Virtual Private Cloud

Guia de usuário

Edição 01

Data 2025-02-26

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Marcas registadas e permissões

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

Aviso

Os produtos, os serviços e as funcionalidades adquiridos são estipulados pelo contrato estabelecido entre a Huawei Cloud e o cliente. Os produtos, os serviços e as funcionalidades descritos neste documento, no todo ou em parte, podem não estar dentro do âmbito de aquisição ou do âmbito de uso. Salvo especificação em contrário no contrato, todas as declarações, informações e recomendações neste documento são fornecidas "TAL COMO ESTÃO" sem garantias ou representações de qualquer tipo, sejam expressas ou implícitas.

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

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 determinar 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.

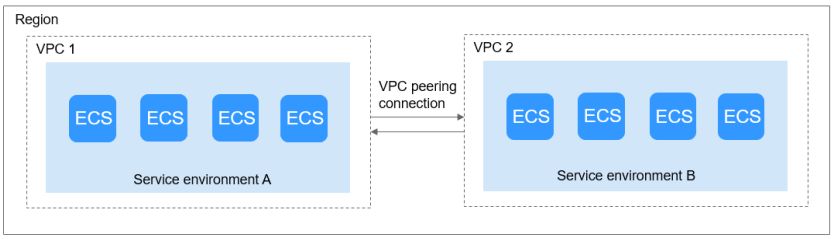
Única VPC

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 network ACLs 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.

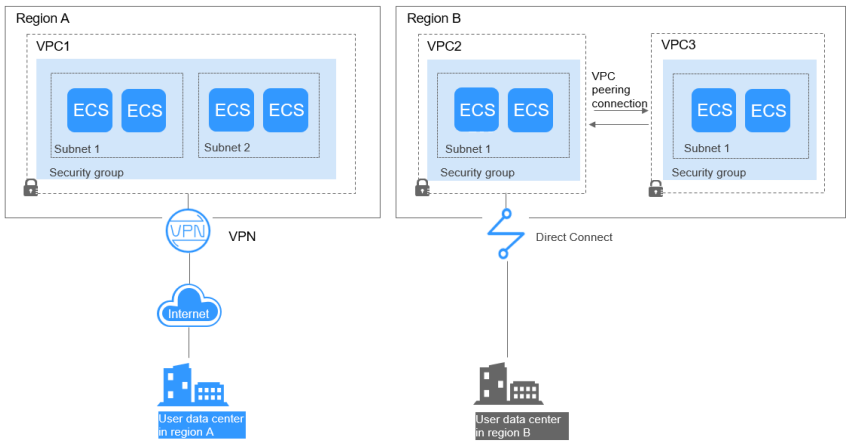
- Se não for necessário controlar explicitamente como cada sub-rede roteia o tráfego de entrada e saída, você poderá usar a tabela de rotas padrão.
- Se você precisar controlar explicitamente como cada sub-rede roteia o tráfego de entrada e saída em uma VPC, adicione rotas personalizadas à tabela de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

Como faço para me 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 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 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 NAT para seus ECSs. Com os gateways NAT, você não precisa atribuir um EIP a cada ECS. Os gateways NAT reduzem os custos, pois você não precisa de tantos EIPs. Os gateways 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. Ela mapeia portas de EIP para portas de 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 aplicação de negócios. O ELB é implementado no modo de cluster. Ele fornece tolerância a falhas para suas aplicações 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**.

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. Faça logon no console de gerenciamento.
2. Na página inicial do console, em **Rede**, clique em **Virtual Private Cloud**.
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

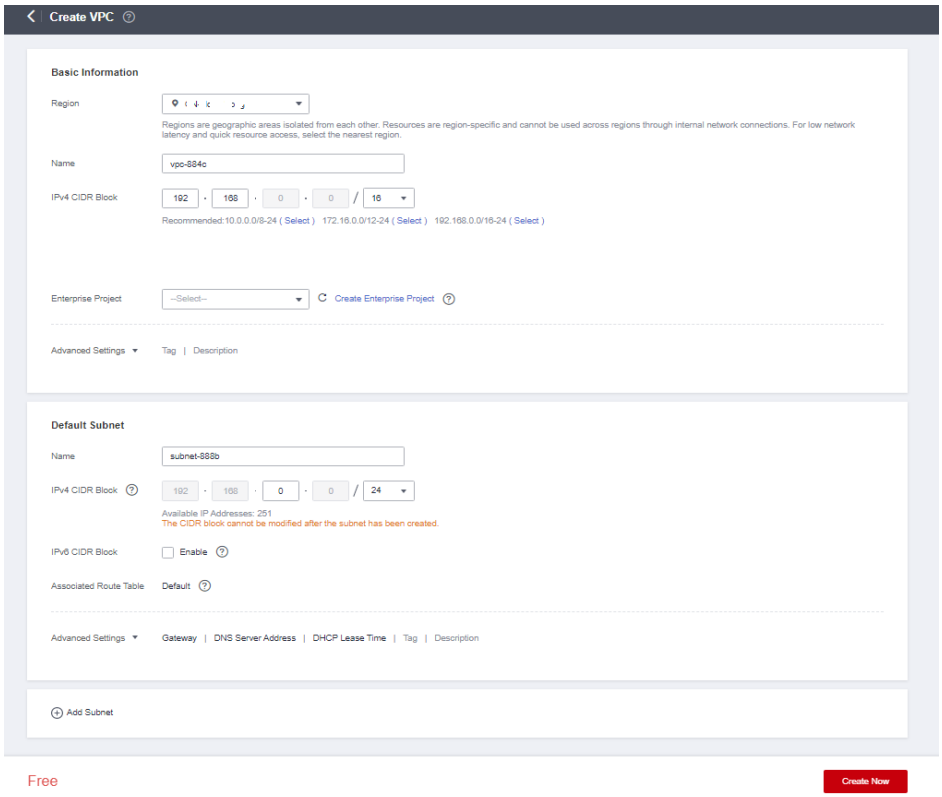


Tabela 1-1 Descrições de parâmetros da VPC

Parâmetro	Descrição	Exemplo de valor
Region	As regiões são áreas geográficas fisicamente isoladas umas das outras. As redes dentro de diferentes regiões não estão conectadas umas às outras, 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

Parâmetro	Descrição	Exemplo de valor
Name	O nome 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.	VPC-test
CIDR Block ou 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
Enterprise Project	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**.	default
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: 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/D

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 ser 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
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**.	Mantenha as configurações padrão.

Parâmetro	Descrição	Exemplo de valor
Gateway	O endereço de gateway da sub-rede. Esse endereço IP é usado para se comunicar com outras sub-redes.	192.168.0.1
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
Domain Name	Insira nomes de domínio (), separados por espaços. São permitidos no máximo 254 caracteres. Um nome de domínio pode consistir em vários rótulos (máx. 63 caracteres cada). Para acessar um nome de domínio, você só precisa digitar o prefixo do nome de domínio. Os ECSs na sub-rede correspondem automaticamente ao sufixo de nome de domínio configurado. Se os nomes de domínio forem alterados, os ECSs recém-adicionados a essa sub-rede usarão os novos nomes de domínio. Se um ECS existente nessa sub-rede precisar usar os novos nomes de domínio, reinicie o ECS ou execute um comando para reiniciar o serviço de cliente de DHCP ou o serviço de rede. **NOTA** O comando para atualizar a configuração de DHCP depende do SO do ECS. Os comandos a seguir servem como referência. ● Reiniciar o serviço de cliente de DHCP: **service dhcpd restart** ● Reiniciar o serviço de rede: **service network restart**	test.com

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 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: 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/D

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

Parâmetro	Requisitos	Exemplo de valor
Key	● Não pode ser deixado em branco. ● Deve ser exclusiva para cada VPC e pode ser a mesma 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**.

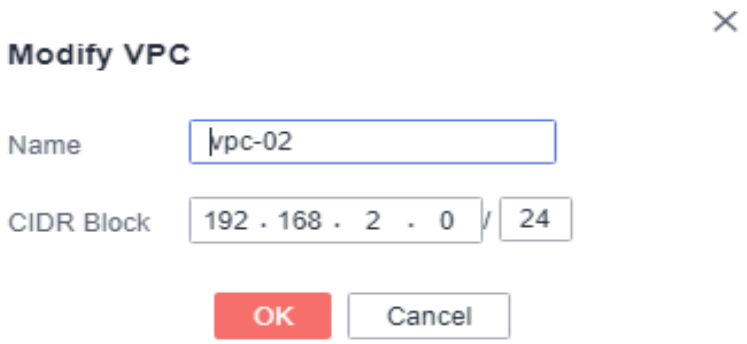
> **NOTA**
>
> Se uma VPC tiver uma sub-rede em seu bloco CIDR secundário, o bloco CIDR secundário não poderá ser modificado no console ou usando APIs.

- 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. Faça logon no console de gerenciamento.
2. Na página inicial do console, em **Rede**, clique em **Virtual Private Cloud**.
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.

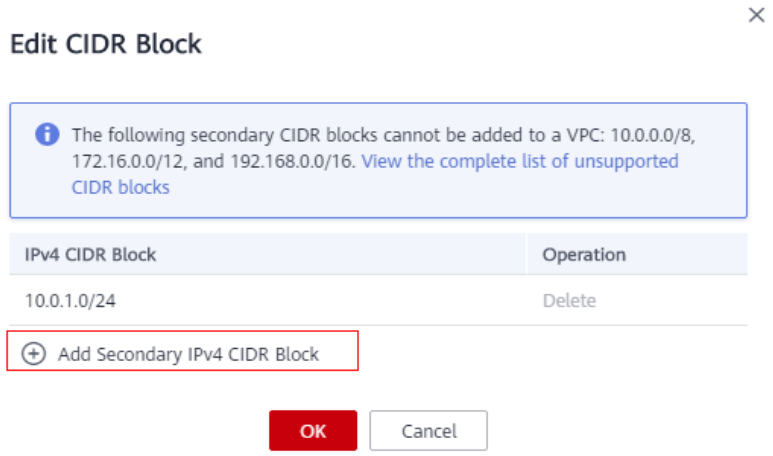
Tabela 1-5 Blocos CIDR secundários restritos

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, em **Rede**, clique em **Virtual Private Cloud**.
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, em **Rede**, clique em **Virtual Private Cloud**.
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 consigo excluir minhas VPCs e sub-redes?**

Procedimento

1. Faça logon no console de gerenciamento.
2. Na página inicial do console, em **Rede**, clique em **Virtual Private Cloud**.
3. No painel de navegação à esquerda, clique em **Virtual Private Cloud**.
4. 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.
5. 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 consigo 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 deixado em branco. ● Deve ser exclusiva para cada VPC e pode ser a mesma 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. 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, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, clique em **Virtual Private Cloud**.
5. Na caixa de pesquisa acima da lista de VPC, clique na caixa de pesquisa.
   a. Clique em **Tag**.
   b. Selecione as tags de destino e clique em **OK**.
      O sistema filtra recursos com base nas tags selecionadas.

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

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, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, clique em **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.
   – Ver 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. 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, em **Rede**, clique em **Virtual Private Cloud**.
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. Elas serão exportadas 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. 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, em **Rede**, clique em **Virtual Private Cloud**.
4. Na lista da VPC, clique no nome da VPC para a qual a topologia será exibida.

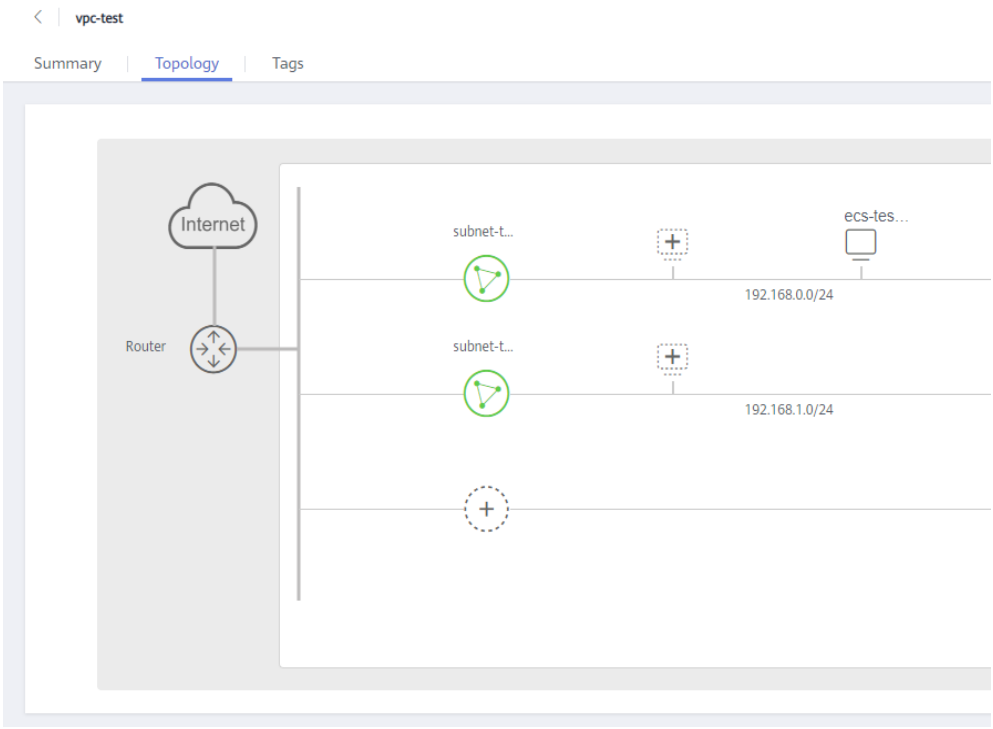
   A página de detalhes da VPC é exibida.
5. Clique na guia **Topology** para exibir a topologia da VPC.

   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. 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, em **Rede**, clique em **Virtual Private Cloud**.
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.	-
Name	O nome da sub-rede. O nome pode conter no máximo 64 caracteres, que podem ser letras, dígitos, sublinhados (_), hifens (-) e pontos (.). O nome não pode conter espaços.	Subnet
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**. 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 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/ 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
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
Advanced Settings/ Domain Name	Insira nomes de domínio (), separados por espaços. São permitidos no máximo 254 caracteres. Um nome de domínio pode consistir em vários rótulos (máx. 63 caracteres cada). Para acessar um nome de domínio, você só precisa digitar o prefixo do nome de domínio. Os ECSs na sub-rede correspondem automaticamente ao sufixo de nome de domínio configurado. Se os nomes de domínio forem alterados, os ECSs recém-adicionados a essa sub-rede usarão os novos nomes de domínio. Se um ECS existente nessa sub-rede precisar usar os novos nomes de domínio, reinicie o ECS ou execute um comando para reiniciar o serviço de cliente de DHCP ou o serviço de rede. **NOTA** O comando para atualizar a configuração de DHCP depende do SO do ECS. Os comandos a seguir servem como referência. ● Reiniciar o serviço de cliente de DHCP: **service dhcpd restart** ● Reiniciar o serviço de rede: **service network restart**	test.com

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 (< ou >).	-

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: o 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. 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, em **Rede**, clique em **Virtual Private Cloud**.
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-redes, localize a sub-rede de destino e clique em seu nome.

   A página de detalhes da sub-rede é exibida.
7. 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 ser letras, dígitos, sublinhados (_), hifens (-) e pontos (.). O nome não pode conter espaços.	Subnet
DNS Server Address	Por padrão, dois endereços de servidor DNS são configurados. Você pode alterá-las conforme necessário. Um máximo de dois endereços de servidor DNS são suportados. Use vírgulas (,) para separar cada dois endereços. 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
Domain Name	Insira nomes de domínio (), separados por espaços. São permitidos no máximo 254 caracteres. Um nome de domínio pode consistir em vários rótulos (máx. 63 caracteres cada). Para acessar um nome de domínio, você só precisa digitar o prefixo do nome de domínio. Os ECSs na sub-rede correspondem automaticamente ao sufixo de nome de domínio configurado. Se os nomes de domínio forem alterados, os ECSs recém-adicionados a essa sub-rede usarão os novos nomes de domínio. Se um ECS existente nessa sub-rede precisar usar os novos nomes de domínio, reinicie o ECS ou execute um comando para reiniciar o serviço de cliente de DHCP ou o serviço de rede. **NOTA** O comando para atualizar a configuração de DHCP depende do SO do ECS. Os comandos a seguir servem como referência. ● Reiniciar o serviço de cliente de DHCP: **service dhcpd restart** ● Reiniciar o serviço de rede: **service network restart**	test.com

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 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 esse parâmetro for deixado vazio, você não adicionar um endereço IP do servidor NTP. Um máximo de quatro endereços IP exclusivos do servidor NTP podem ser configurados. Vários endereços IP devem ser separados usando uma vírgula (,). 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 (< ou >).	-

8. 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. 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, em **Rede**, clique em **Virtual Private Cloud**.
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 caixa de pesquisa acima da lista de sub-rede, clique na caixa de pesquisa.
   a. Clique em **Tag**.
   b. Selecione as tags de destino e clique em **OK**.

      O sistema filtra recursos com base nas tags selecionadas.

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

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, em **Rede**, clique em **Virtual Private Cloud**.
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-redes, localize a sub-rede de destino e clique em seu nome.
7. Na página de detalhes da sub-rede, 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 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. 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, em **Rede**, clique em **Virtual Private Cloud**.
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 NAT.

AVISO

Depois de excluir todos os recursos em uma sub-rede consultando esta seção, a mensagem "Delete the resource that is using the subnet and then delete the subnet." é exibida quando você excluir a sub-rede, você pode consultar **Visualização de endereços IP em uma sub-rede**.

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, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Subnets**.

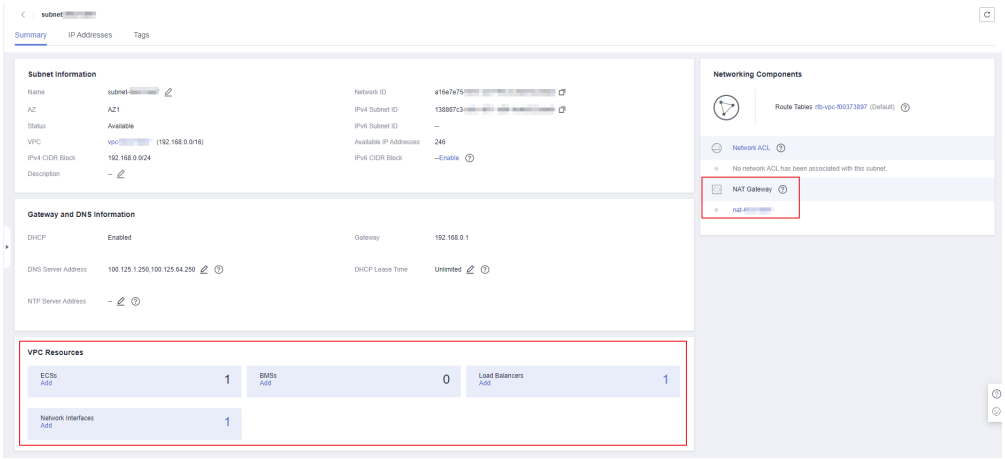
   A página **Subnets** é exibida.
5. Localize a sub-rede de destino e clique em seu nome.

   A página de detalhes da sub-rede é exibida.
6. Na página **Summary**, exiba os recursos na sub-rede.

   a. Na área **VPC Resources**, exiba os ECSs, BMSs, interfaces de rede e balanceadores de carga na sub-rede.

   b. Na área **Networking Components**, veja os gateways NAT na sub-rede.

Figura 1-7 Visualizar recursos em uma sub-rede



7. Exclua recursos da sub-rede.

Tabela 1-10 Exibição e exclusão de 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**.

Recurso	Referência
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 **VPC 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 NAT	Você pode alternar diretamente para gateways NAT na página de detalhes da sub-rede. 1. Clique no nome do gateway NAT na área **Networking Components**. A página de detalhes do gateway NAT é exibida. 2. Clique em  para retornar à lista de gateways NAT. 3. Localize a linha que contém o gateway NAT a ser excluído e clique em **Delete** na coluna **Operation**. ● **Exclusão ou cancelamento de assinatura de um gateway NAT público** ● **Exclusão de um gateway 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.

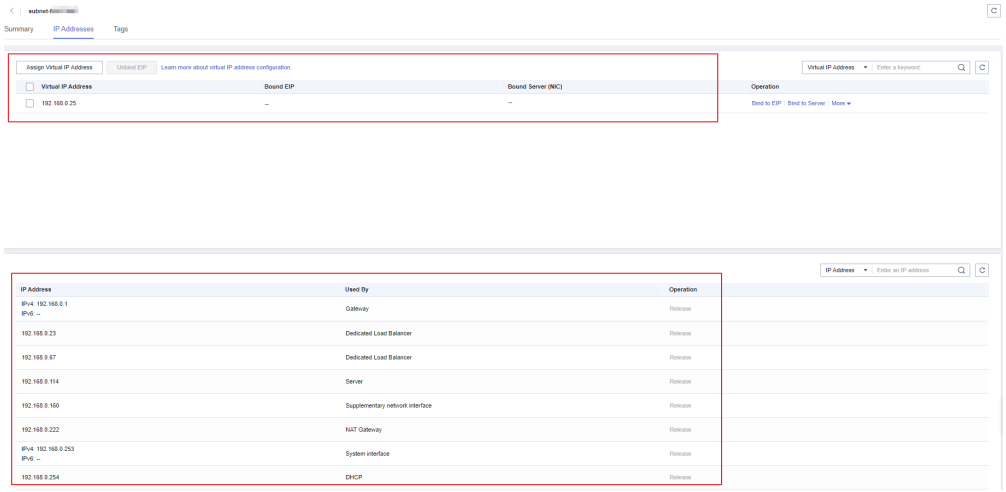
Procedimento

1. 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, em **Rede**, clique em **Virtual Private Cloud**.
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 Visualização de endereços IP em uma sub-rede



Operações de acompanhamento

Se você quiser visualizar e excluir os recursos em uma sub-rede, consulte **Por que não consigo 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. 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, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Subnets**.

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

1.4 Rede de pilha dupla IPv4 e IPv6

O que é uma rede de pilha dupla IPv4/IPv6?

A pilha dupla IPv4 e IPv6 permite que seus recursos, como ECSs, usem os endereços IPv4 e IPv6 para comunicação de rede privada e pública. Por exemplo, se os ECSs usam a rede de pilha dupla IPv4/IPv6:

- Os ECSs podem se comunicar uns com os outros usando endereços IPv4 privados.
- Os ECSs podem se comunicar com a Internet após serem vinculados a EIPs.
- Os ECSs podem se comunicar uns com os outros usando endereços IPv6.
- Os ECSs podem se comunicar com a Internet depois que seus endereços IPv6 são associados a larguras de banda.

NOTA

Se você selecionar **Enable** para **IPv6 CIDR Block** ao criar uma sub-rede, um bloco CIDR IPv6 será automaticamente atribuído à sub-rede.

As operações básicas em redes de pilha dupla IPv4 e IPv6 são as mesmas das redes IPv4, exceto alguns parâmetros. Verifique as páginas do console para obter detalhes.

Observações e restrições

- A função de pilha dupla IPv4/IPv6 é atualmente gratuita, mas será cobrada em uma data posterior (preço ainda a ser determinado).
- Apenas algumas especificações do ECS suportam redes IPv6 e podem usar redes de pilha dupla IPv4/IPv6. Você precisa selecionar esses ECSs nas regiões suportadas.

  Você pode usar um dos métodos a seguir para verificar quais especificações do ECS são compatíveis com IPv6:

  – No console do ECS, clique em **Buy ECS**. Na página exibida, veja as especificações do ECS.

    Se houver o parâmetro **IPv6** com o valor de **Yes**, as especificações do ECS suportarão IPv6.

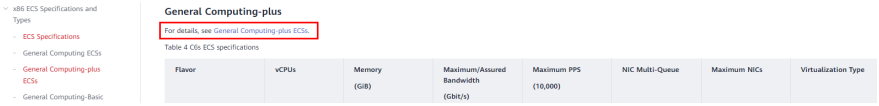
  – Na página **ECS Specifications**, clique no link das especificações do ECS desejadas para verificar se as especificações do ECS são compatíveis com IPv6 na tabela de recursos do ECS.

    Por exemplo, se você quiser verificar se os ECSs de computação geral aprimorada suportam IPv6:

    i. Abra a página **ECS Specifications**.

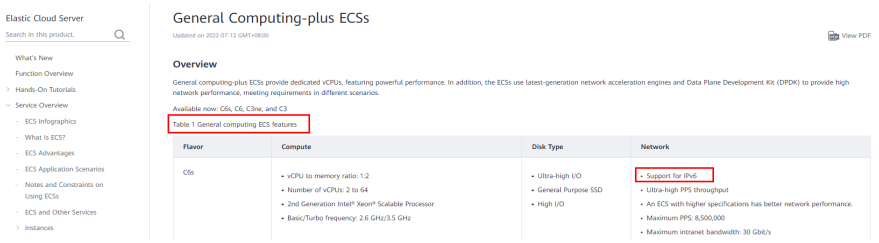
    ii. Em **General Computing-Plus**, clique no link para obter informações detalhadas.

    Figura 1-9 Link para informações detalhadas

    iii. Na página **General Computing-plus ECSs**, verifique se o IPv6 é suportado na tabela de recursos do ECS.

    Figura 1-10 ECSs de computação geral aprimorada

Cenários de aplicação de IPv6

Se o seu ECS oferecer suporte a IPv6, você poderá usar a rede de pilha dupla IPv4/IPv6. **Tabela 1-11** mostra os cenários de aplicação de exemplo.

Tabela 1-11 Cenários de aplicação de pilha dupla IPv4/IPv6

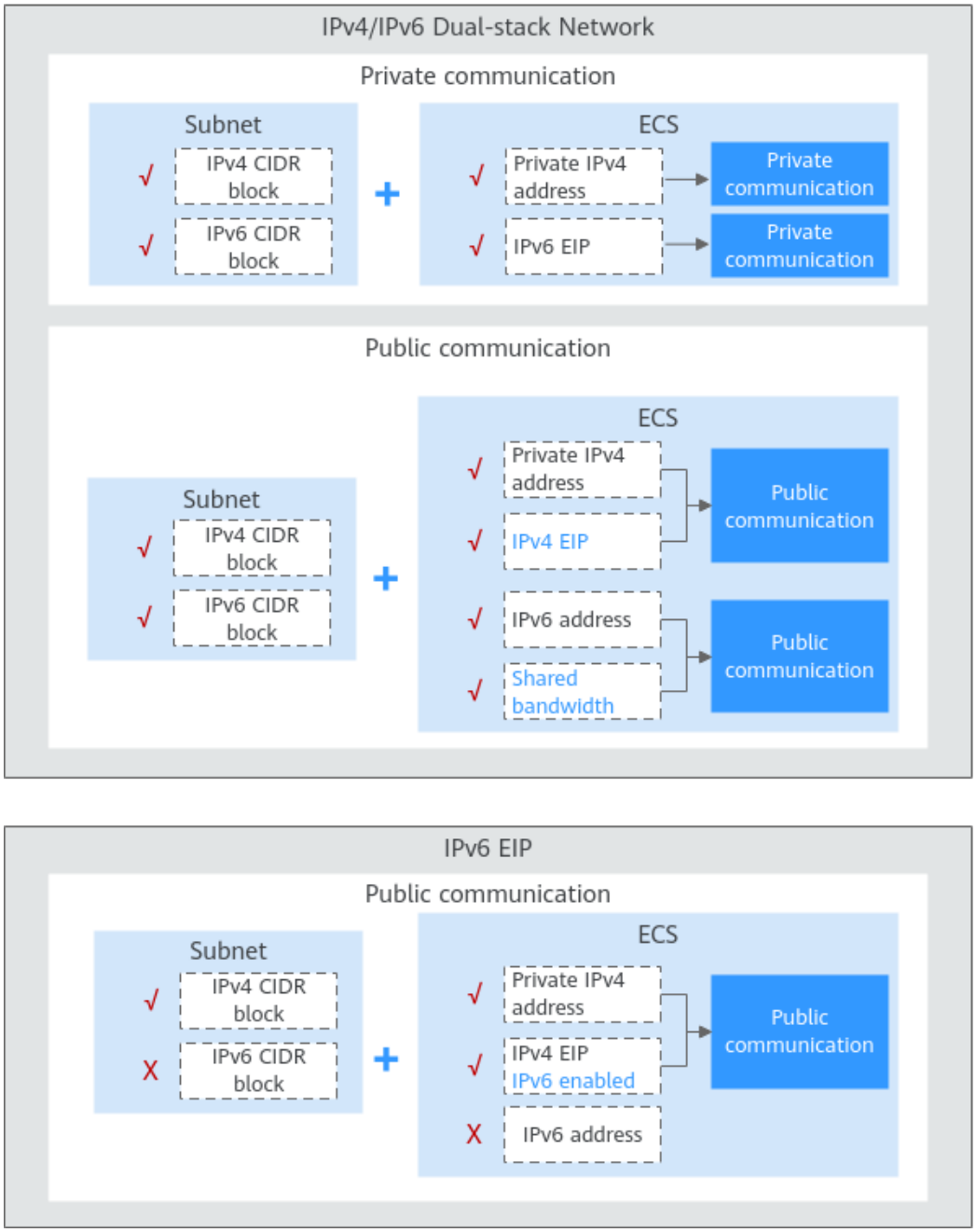
Cenário de aplicação	Descrição	Sub-rede	ECS
Comunicação privada usando endereços IPv6	As suas aplicações implementadas em ECSs precisam se comunicar com outros sistemas (como bancos de dados) por meio de redes privadas usando endereços IPv6.	● Bloco CIDR IPv4 ● Bloco CIDR IPv6	● Endereço IPv4 privado: usado para comunicação privada ● Endereço IPv6: usado para comunicação privada.
Comunicação pública usando endereços IPv6	As suas aplicações implementadas em ECSs precisam fornecer serviços acessíveis da Internet usando endereços IPv6.	● Bloco CIDR IPv4 ● Bloco CIDR IPv6	● Endereço IPv4 privado + EIP IPv4: usados para comunicação de rede pública ● Endereço IPv6 + largura de banda compartilhada: usados para comunicação de rede pública
	As suas aplicações implementadas em ECSs precisam fornecer serviços acessíveis pela Internet e analisar os dados de solicitação de acesso usando endereços IPv6.		

Se o seu flavor do ECS não oferecer suporte a endereços IPv6, você poderá ativar a função EIP IPv6 para permitir comunicações usando endereços IPv6. Para mais detalhes, consulte **Tabela 1-12**.

Tabela 1-12 Cenários de aplicação de EIPs IPv6

Cenário de aplicação	Descrição	Sub-rede	ECS
Comunicação pública usando endereços IPv6	As suas aplicações implementadas em ECSs precisam fornecer serviços acessíveis da Internet usando endereços IPv6.	Bloco CIDR IPv4	● Endereço IPv4 privado ● EIP IPv4 (com função IPv6 ativada): usado para comunicação pública usando IPv4 e EIPs IPv6

Figura 1-11 Cenários de aplicação de redes IPv6



Operações básicas

Criar uma sub-rede IPv6

Crie uma sub-rede IPv6 seguindo as instruções em **Criação de uma sub-rede para a VPC**. Selecione **Enable** para **IPv6 CIDR Block**. Um bloco CIDR IPv6 será automaticamente atribuído à sub-rede. O IPv6 não pode ser desativado após a criação da sub-rede. Atualmente, a personalização do bloco CIDR IPv6 não é suportada.

Visualizar endereços IPv6 em uso

Na lista de sub-redes, clique no nome da sub-rede. Na página exibida, visualize endereços IPv6 em uso na página da guia **IP Addresses**.

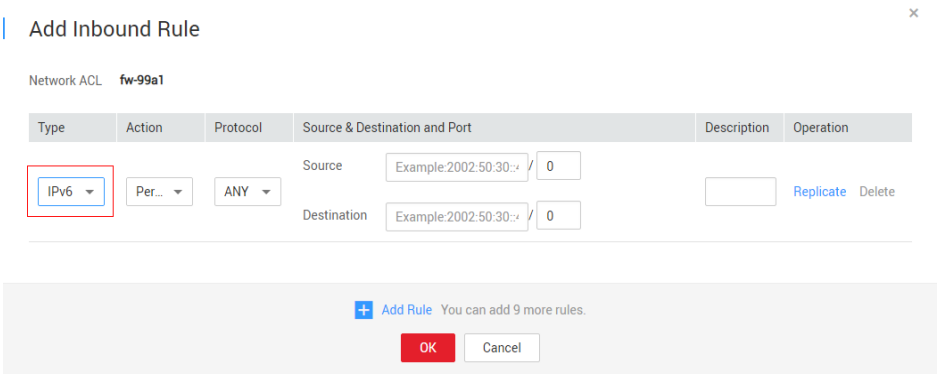
Adicionar uma regra de grupo de segurança (IPv6)

Adicione uma regra de grupo de segurança com **Type** definido como **IPv6** e **Source** ou **Destination** definido como um endereço IPv6 ou bloco CIDR IPv6.

Adicionar uma regra de Network ACL (IPv6)

Adicione uma regra de network ACL com **Type** definido como **IPv6** e **Source** ou **Destination** definido como um endereço IPv6 ou bloco CIDR IPv6.

Figura 1-12 Adicionar uma regra de network ACL (IPv6)



Adicionar uma rota (IPv6)

Adicione uma rota com **Destination** e **Next Hop** definido para um IPv4 ou bloco CIDR IPv6. Para obter detalhes sobre como adicionar uma rota, consulte **Adição de uma rota personalizada**. Se o destino for um bloco CIDR IPv6, o próximo salto só poderá ser um endereço IP na mesma VPC que o bloco CIDR IPv6.

NOTA

Se o destino for um bloco CIDR IPv6, o tipo do próximo salto pode ser apenas um ECS, NIC de extensão ou endereço IP virtual. O próximo salto também deve ter endereços IPv6.

Atribuir endereços IPv6 dinamicamente

Depois que um ECS for criado com êxito, você pode exibir o endereço IPv6 atribuído na página de detalhes do ECS. Você também pode fazer logon no ECS e executar o comando **ifconfig** para exibir o endereço IPv6 atribuído.

Se um endereço IPv6 não for atribuído automaticamente ou a imagem selecionada não suportar a função de atribuição automática de endereços IPv6, manualmente obtenha o endereço IPv6 consultando **Atribuição de endereços IPv6 dinamicamente**.

NOTA

Se um ECS for criado a partir de uma imagem pública:

Antes de ativar a atribuição de endereços IPv6 dinâmicos para uma imagem pública do Linux, verifique se o IPv6 é suportado e, em seguida, verifique se a atribuição de endereços IPv6 dinâmicos foi ativada. Atualmente, todas as imagens públicas do Linux suportam IPv6, e a atribuição de endereços IPv6 dinâmicos está ativada para o Ubuntu 16 por padrão. Você não precisa configurar a atribuição de endereços IPv6 dinâmicos para o sistema operacional Ubuntu 16. Para outras imagens públicas do Linux, você precisa habilitar essa função.

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, contêineres 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.

Assim como as listas brancas, as regras de grupo de segurança funcionam da seguinte maneira:

- As regras de entrada controlam o tráfego de entrada para instâncias no grupo de segurança. Se uma solicitação de entrada corresponder à origem em uma regra de grupo de segurança de entrada com **Action** definida como **Allow**, a solicitação será permitida.

  A menos que especificado de outra forma, você não precisa configurar regras de negação na direção de entrada porque as solicitações que não correspondem a regras de permissão serão negadas.
- As regras de saída controlam o tráfego de saída das instâncias da nuvem no grupo de segurança. Se o destino de uma regra de grupo de segurança de saída com **Action** definida como **Allow** for 0.0.0.0/0, todas as solicitações de saída serão permitidas.

  0.0.0.0/0 representa todos os endereços IPv4.

  ::/0 representa todos os endereços IPv6.

Tabela 2-1 mostra as regras de entrada e saída no grupo de segurança sg-AB.

Tabela 2-1 Regras no grupo de segurança sg-AB

Direção	Ação	Tipo	Protocolo & porta	Origem/ Destino	Descrição
Entrada	Allow	IPv4	Todos	Origem: sg-AB	Essa regra permite que os ECSs do grupo de segurança se comuniquem entre si.
Entrada	Allow	IPv4	TCP: 22	Origem: 0.0.0.0/0	Essa regra permite que todos os endereços IPv4 acessem ECSs no grupo de segurança pela porta SSH 22 para efetuar logon remotamente em ECSs de Linux.
Entrada	Allow	IPv4	TCP: 3389	Origem: 0.0.0.0/0	Essa regra permite que todos os endereços IPv4 acessem ECSs no grupo de segurança pela porta RDP 3389 para efetuar logon remotamente em ECSs do Windows.
Entrada	Allow	IPv4	TCP: 80	Origem: 10.5.6.30/32	Essa regra permite que o endereço IP 10.5.6.30 acesse ECSs no grupo de segurança pela porta 80.
Saída	Allow	IPv4	Todos	Destino: 0.0.0.0/0	Essa regra permite o acesso de ECSs no grupo de segurança a qualquer endereço IPv4 em qualquer porta.
Saída	Allow	IPv6	Todos	Destino: ::/0	Essa regra permite o acesso de ECSs no grupo de segurança a qualquer endereço IPv6 em qualquer porta.
Saída	Allow	IPv4	TCP: 80	Destino: 10.7.6.51/32	Essa regra permite o acesso de ECSs no grupo de segurança ao endereço IP 10.7.6.51 pela porta 80.

O sistema cria automaticamente um grupo de segurança padrão para cada conta. 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

O nome do grupo de segurança padrão é **default**. Os grupos de segurança padrão e personalizados 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 também pode alterar os grupos de segurança associados às instâncias. 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 pode 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 2-3** . Você também pode personalizar regras de grupo de segurança. Para mais detalhes, consulte **Adição de uma regra de grupo de segurança**.

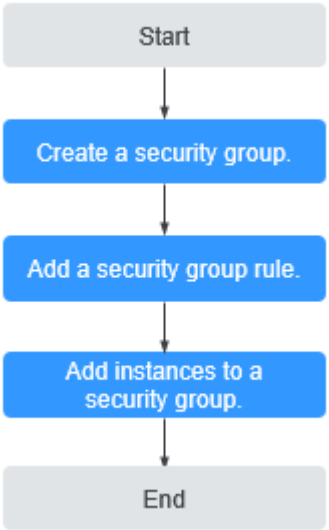
Modelo de grupo de segurança

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, não pode associar mais de cinco grupos de segurança a cada ECS ou NIC de extensão.
- Se um ECS 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 2-2** mostra os detalhes.

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

Configuração da regra	Tipo de ECS
Source ou **Destination** é definido como **IP address group**.	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)
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 flavors de ECS do Kunpeng não oferecem suporte a portas não consecutivas. Se você usar números de porta inconsecutivos em uma regra de grupo de segurança de um ECS de Kunpeng, essa regra e as regras configuradas após essa regra não terão efeito. Se configurar a regra de grupo de segurança A com portas inconsecutivas **22,24** e, em seguida, configurar a regra de grupo de segurança B com a porta 9096, a regra A e a regra B não terão efeito.

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:

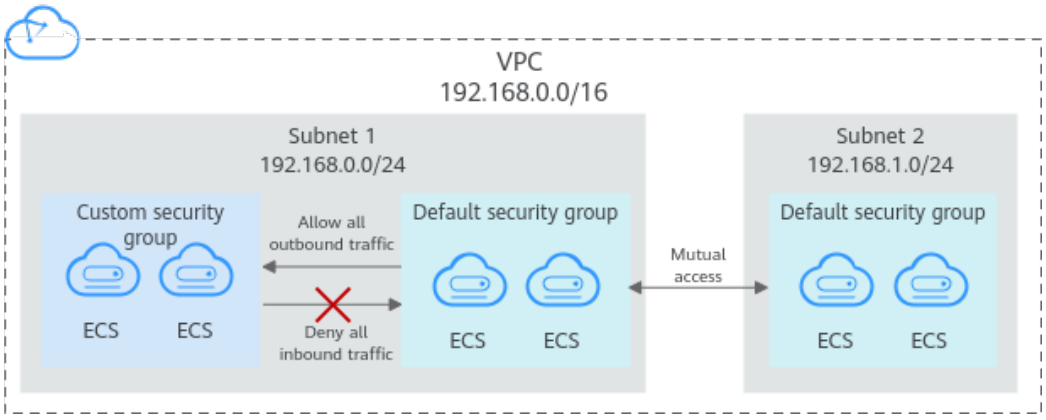
- Defina regras simples de grupo de segurança. Por exemplo, se você adicionar uma instância a vários grupos de segurança, a instância poderá estar em conformidade com centenas de regras de grupo de segurança, e uma alteração em qualquer regra poderá causar desconexão da rede para a instância.
- Antes 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 personalizados 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 de VPC para conectar as duas VPCs.

Tabela 2-3 descreve as regras padrão no grupo de segurança padrão.

Tabela 2-3 Regras no grupo de segurança padrão

Direção	Prioridade	Ação	Protocolo	Porta/Intervalo	Origem/Destino	Descrição
Saída	100	Permitir	Todos	Todos	Destino: 0.0.0.0/0	Permite todo o tráfego de saída.
Entrada	100	Permitir	Todos	Todos	Origem: nome do grupo de segurança atual	Permite comunicações entre ECSs dentro do mesmo grupo de segurança em qualquer porta.
Entrada	100	Permitir	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	Permitir	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.

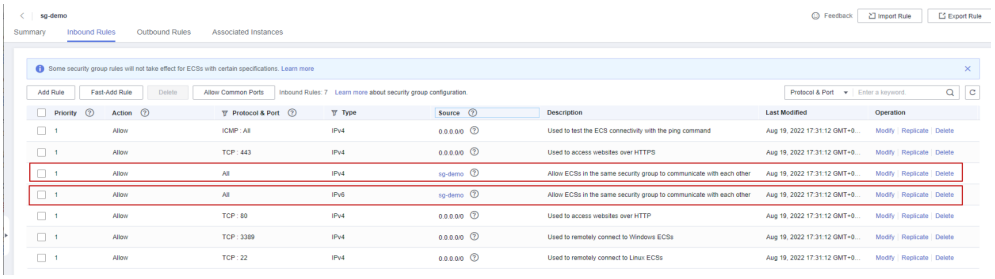
  Você pode adicionar uma regra de entrada aos grupos de segurança que contêm os ECSs para permitir o acesso de ECSs no outro grupo de segurança. A regra exigida é a seguinte.

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

Um grupo de segurança é uma coleção de regras de controle de acesso para controlar o tráfego que tem permissão para alcançar e sair dos recursos de nuvem aos quais está associado. Os recursos de nuvem podem ser servidores de nuvem, contêineres, bancos de dados e muito mais. Um grupo de segurança consiste em regras de entrada e saída.

O sistema fornece vários modelos de grupo de segurança para você criar um grupo de segurança. Um modelo de grupo de segurança tem regras de entrada e saída pré-configuradas. Você pode selecionar um modelo com base em seus requisitos de serviço. **Tabela 2-4** descreve os modelos de grupo de segurança.

Tabela 2-4 Modelos de grupo de segurança

Modelo	Direção	Protocolo /Porta/ Tipo	Origem/ Destino	Descrição	Cenário de aplicação
General-purpose web server	Entrada	TCP: 22 (IPv4)	0.0.0.0/0	Essa regra permite que todos os endereços IPv4 acessem ECSs no grupo de segurança pela porta SSH 22 para efetuar logon remotamente em ECSs de Linux.	● Efetue logon remotamente em ECSs. ● Use o comando ping para testar a conectividade do ECS. ● Os ECSs que funcionam como servidores Web fornecem serviços de acesso ao site.
		TCP: 3389 (IPv4)	0.0.0.0/0	Essa regra permite que todos os endereços IPv4 acessem ECSs no grupo de segurança pela porta RDP 3389 para efetuar logon remotamente em ECSs do Windows.	
		TCP: 80 (IPv4)	0.0.0.0/0	Essa regra permite que todos os endereços IPv4 acessem ECSs no grupo de segurança pela porta HTTP 80 para sites visitados.	
		TCP: 443 (IPv4)	0.0.0.0/0	Essa regra permite que todos os endereços IPv4 acessem ECSs no grupo de segurança pela porta HTTPS 443 para sites visitados.	
		ICMP: todos (IPv4)	0.0.0.0/0	Essa regra permite que todos os endereços IPv4 acessem ECSs no grupo de segurança em qualquer porta para usar o comando ping para testar a conectividade do ECS.	

Modelo	Direção	Protocolo/Porta/Tipo	Origem/Destino	Descrição	Cenário de aplicação
		Todos (IPv4) Todos (IPv6)	sg-xxx	Essa regra permite que os ECSs no grupo de segurança se comuniquem entre si.	
	Saída	Todos (IPv4) Todos (IPv6)	0.0.0.0/0 ::/0	Essa regra permite o acesso de ECSs no grupo de segurança a qualquer endereço IP em qualquer porta.	
All ports open	Entrada	Todos (IPv4) Todos (IPv6)	sg-xxx	Essa regra permite que os ECSs no grupo de segurança se comuniquem entre si.	Abrir todas as portas ECS em um grupo de segurança representa riscos de segurança.
		Todos (IPv4) Todos (IPv6)	0.0.0.0/0 ::/0	Essa regra permite que todos os endereços IP acessem ECSs no grupo de segurança em qualquer porta.	
	Saída	Todos (IPv4) Todos (IPv6)	0.0.0.0/0 ::/0	Essa regra permite o acesso de ECSs no grupo de segurança a qualquer endereço IP em qualquer porta.	
Custom	Entrada	Todos (IPv4) Todos (IPv6)	sg-xxx	Essa regra permite que os ECSs no grupo de segurança se comuniquem entre si.	Esse modelo não permite nenhum acesso de entrada de qualquer porta para ECSs no grupo de segurança. Depois que o grupo de segurança for criado, adicione as regras necessárias consultando **Adição de uma regra de grupo de segurança**.
	Saída	Todos (IPv4) Todos (IPv6)	0.0.0.0/0 ::/0	Essa regra permite o acesso de ECSs no grupo de segurança a qualquer endereço IP em qualquer porta.	

Observações e restrições

Cada ECS deve estar associado a pelo menos um grupo de segurança. Se você não tiver um grupo de segurança ao criar um ECS, o sistema criará automaticamente um grupo de segurança padrão (padrão) para o ECS. Para obter detalhes sobre as regras no grupo de segurança padrão, consulte **Grupos de segurança padrão e regras 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, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **Security Groups**.

   A lista de grupos de segurança é exibida.
5. No canto superior direito, clique em **Create Security Group**.

   A página **Create Security Group** é exibida.
6. Configure os parâmetros conforme solicitado.

Figura 2-3 Criar grupo de segurança

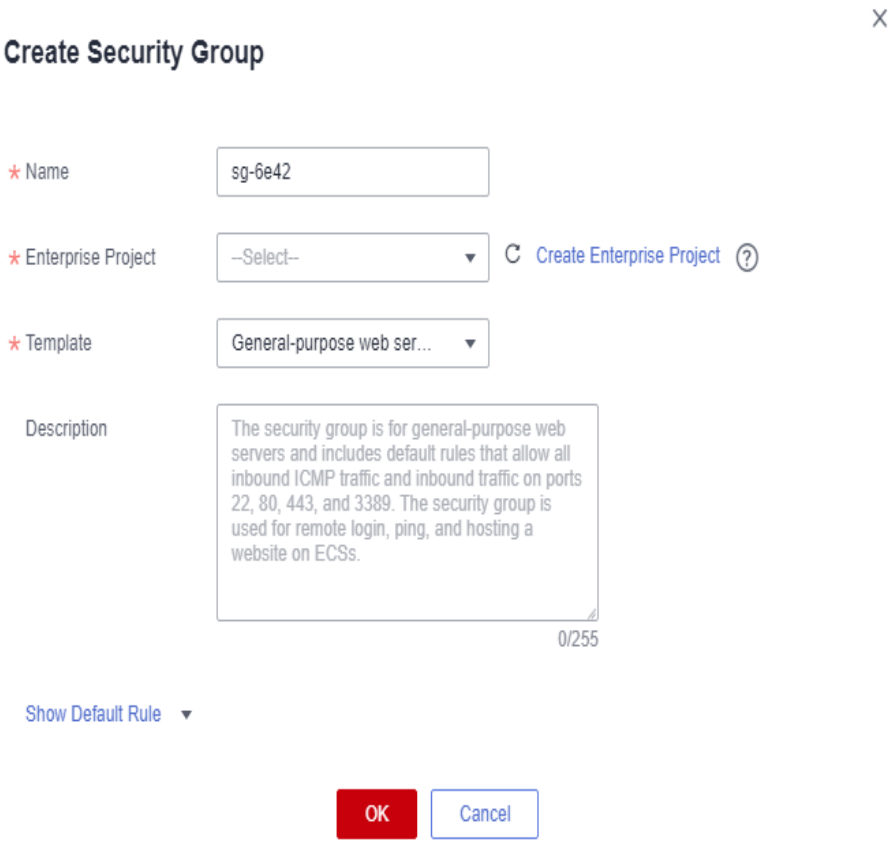


Tabela 2-5 Descrição do parâmetro

Parâmetro	Descrição	Exemplo de valor
Name	Obrigatório Digite o nome do grupo de segurança. 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-AB
Enterprise Project	Obrigatório Ao criar um grupo de segurança, você pode adicionar o grupo de segurança a um projeto empresarial habilitado. 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 da empresa, consulte o **Guia de usuário do Enterprise Management**.	default
Template	Obrigatório O sistema fornece vários modelos de grupo de segurança para você criar um grupo de segurança. Um modelo de grupo de segurança tem regras de entrada e saída pré-configuradas. Você pode selecionar um modelo com base em seus requisitos de serviço. **Tabela 2-4** descreve os modelos de grupo de segurança.	Servidor Web de uso geral
Description	Opcional 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 (< ou >).	N/A

7. Confirme as regras de entrada e saída do modelo e 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 **Adição de instâncias e remoção 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 controlar o tráfego que tem permissão para alcançar e sair dos recursos de nuvem aos quais está associado. Os recursos de nuvem podem ser servidores de nuvem, contêineres, bancos de dados e muito mais. Um grupo de segurança consiste em regras de entrada e saída.

Assim como as listas brancas, as regras de grupo de segurança funcionam da seguinte maneira:

- As regras de entrada controlam o tráfego de entrada para instâncias no grupo de segurança. Se uma solicitação de entrada corresponder à origem em uma regra de grupo de segurança de entrada com **Action** definida como **Allow**, a solicitação será permitida.

  A menos que especificado de outra forma, você não precisa configurar regras de negação na direção de entrada porque as solicitações que não correspondem a regras de permissão serão negadas.
- As regras de saída controlam o tráfego de saída das instâncias da nuvem no grupo de segurança. Se o destino de uma regra de grupo de segurança de saída com **Action** definida como **Allow** for 0.0.0.0/0, todas as solicitações de saída serão permitidas.

  0.0.0.0/0 representa todos os endereços IPv4.

  ::/0 representa todos os endereços IPv6.

Se as regras do grupo de segurança associado à sua instância não puderem atender aos seus requisitos, por exemplo, você precisar permitir o tráfego de entrada em uma porta TCP específica, poderá adicionar uma regra de entrada para permitir o tráfego na porta TCP.

Exemplos de configuração de regra de grupo de segurança

- O sistema fornece um grupo de segurança padrão. Para obter detalhes sobre regras do grupo de segurança padrão, consulte **Grupos de segurança padrão e regras de grupo de segurança**. Se as regras de grupo de segurança padrão não puderem atender aos seus requisitos, você poderá modificá-las.
- Antes de configurar regras de grupo de segurança, você precisa planejar regras para comunicações entre instâncias no grupo de segurança. Para obter mais exemplos de configuração 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, em **Rede**, clique em **Virtual Private Cloud**.
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 **Manage Rule** na coluna **Operation**.

   A página para configurar as regras do grupo de segurança é exibida.

6. Na guia **Inbound Rules**, clique em **Add Rule**.

   A caixa de diálogo **Add Inbound Rule** é exibida.

7. Configure os parâmetros necessários.

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

Figura 2-4 Adicionar regra de entrada

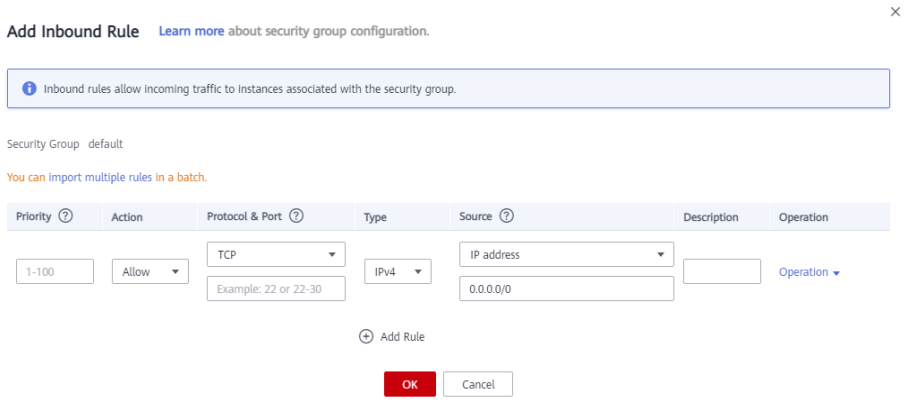


Tabela 2-6 Descrição do parâmetro da regra de entrada

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	Allow ou Deny ● Se a **Action** estiver definida como **Allow**, o acesso da origem será permitido aos ECSs no grupo de segurança nas portas especificadas. ● Se a **Action** estiver definida como **Deny**, o acesso da origem será negado aos ECSs no grupo de segurança nas portas especificadas. As regras de negação têm precedência sobre as regras de permissão da mesma prioridade.	Allow
Type	Versão do endereço IP de origem. Você pode selecionar: ● IPv4 ● IPv6	IPv4

Parâmetro	Descrição	Exemplo de valor
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. Insira portas no seguinte formato: ● Porta individual: digite uma porta, como 22. ● Portas consecutivas: insira um intervalo de portas, como 22-30. ● Portas não consecutivas: 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
Source	A origem em uma regra de entrada é usada para corresponder ao endereço IP ou intervalo de endereços de uma solicitação externa. A origem pode ser: ● **IP address**: – Endereço IP único: endereço/máscara IP Exemplo de endereço IPv4: 192.168.10.10/32 Exemplo de endereço IPv6: 2002:50::44/128 – Intervalo de endereços IP na notação CIDR: endereço/máscara IP Exemplo de intervalo de endereços IPv4: 192.168.52.0/24 Exemplo de intervalo de endereços IPv6: 2407:c080:802:469::/64 – Todos os endereços IP 0.0.0.0/0 representa todos os endereços IPv4. ::/0 representa todos os endereços IPv6. ● **Security group**: a origem é de outro grupo de segurança. Você pode selecionar um grupo de segurança na mesma região sob a conta atual na lista suspensa. Há a instância A no grupo de segurança A e a instância B no grupo de segurança B. Se o grupo de segurança A tiver uma regra de entrada com **Action** definida como **Allow** e **Source** definida como grupo de segurança B, o acesso da instância B será permitido à instância A. ● **IP address group**: um grupo de endereços IP é uma coleção de um ou mais endereços IP. Você pode selecionar um grupo de endereços IP disponível na lista suspensa. Um grupo de endereços IP pode ajudá-lo a gerenciar intervalos de endereços IP e endereços IP com os mesmos requisitos de segurança de uma maneira mais simples.	Endereço 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 (< ou >).	N/A

8. Clique em **OK**.
   A lista de regras de entrada é exibida.
9. Na guia **Outbound Rules**, clique em **Add Rule**.
   A caixa de diálogo **Add Outbound Rule** é exibida.
10. Configure os parâmetros necessários.
    Você pode clicar em +·para adicionar mais regras de saída.

Figura 2-5 Adicionar regra de saída

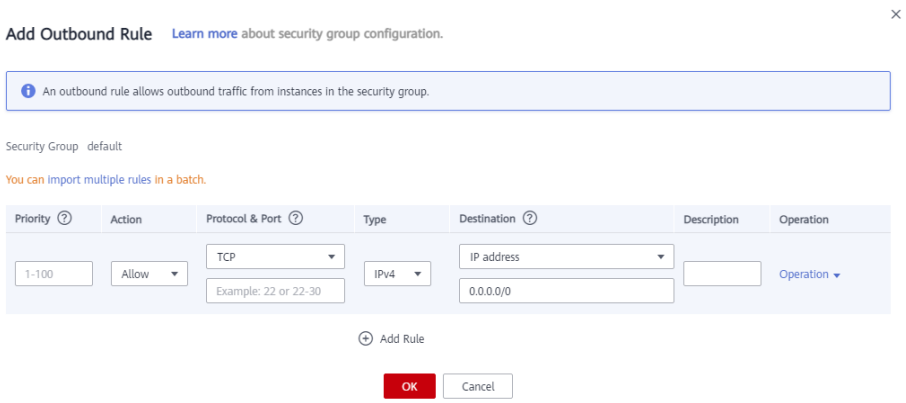


Tabela 2-7 Descrição do parâmetro de regra de saída

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	Allow ou Deny ● Se a **Action** estiver definida como **Allow**, o acesso de ECSs no grupo de segurança será permitido ao destino pelas portas especificadas. ● Se a **Action** estiver definida como **Deny**, o acesso de ECSs no grupo de segurança será negado ao destino nas portas especificadas. As regras de negação têm precedência sobre as regras de permissão da mesma prioridade.	Allow
Type	Versão do endereço IP de destino. Você pode selecionar: ● IPv4 ● IPv6	IPv4
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 em que o tráfego pode sair do ECS. O valor varia de 1 a 65535.	22 ou 22-30

Parâmetro	Descrição	Exemplo de valor
Destination	O destino em uma regra de saída é usado para corresponder ao endereço IP ou intervalo de endereços de uma solicitação interna. O destino pode ser: ● **IP address** – Endereço IP único: endereço/máscara IP Exemplo de endereço IPv4: 192.168.10.10/32 Exemplo de endereço IPv6: 2002:50::44/128 – Intervalo de endereços IP na notação CIDR: endereço/máscara IP Exemplo de intervalo de endereços IPv4: 192.168.52.0/24 Exemplo de intervalo de endereços IPv6: 2407:c080:802:469::/64 – Todos os endereços IP 0.0.0.0/0 representa todos os endereços IPv4. ::/0 representa todos os endereços IPv6. ● **Security group**: o destino é de outro grupo de segurança. Você pode selecionar um grupo de segurança na mesma região sob a conta atual na lista suspensa. Há a instância A no grupo de segurança A e a instância B no grupo de segurança B. Se o grupo de segurança A tiver uma regra de saída com **Action** definida como **Allow** e **Destination** definido como grupo de segurança B, o acesso da instância A será permitido à instância B. ● **IP address group**: um grupo de endereços IP é uma coleção de um ou mais endereços IP. Você pode selecionar um grupo de endereços IP disponível na lista suspensa. Um grupo de endereços IP pode ajudá-lo a gerenciar intervalos de endereços IP e endereços IP com os mesmos requisitos de segurança de uma maneira mais simples.	Endereço 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 (< ou >).	N/A

11. Clique em **OK**.
    A lista de regras de saída é exibida.

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 2-8**.

Tabela 2-8 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 escutada:
   ```
   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

   ```
   tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
   ```
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 escutada:
   ```
   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

   ```
   TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
   ```
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.

2.1.6 Adição rápida de regras de grupo de segurança

Cenários

A função de regra de adição rápida dos grupos de segurança permite adicionar rapidamente regras com portas e protocolos comuns para logon remoto, testes de ping, serviços Web comuns e serviços de banco de dados.

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, em **Rede**, clique em **Virtual Private Cloud**.
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 e clique em **Manage Rule** na coluna **Operation**.

   A página para configurar as regras do grupo de segurança é exibida.
6. Na guia **Inbound Rules**, clique em **Fast-Add Rule**.

   A caixa de diálogo **Fast-Add Inbound Rule** é exibida.
7. Configure os parâmetros necessários.

Figura 2-8 Adição rápida de regra de entrada

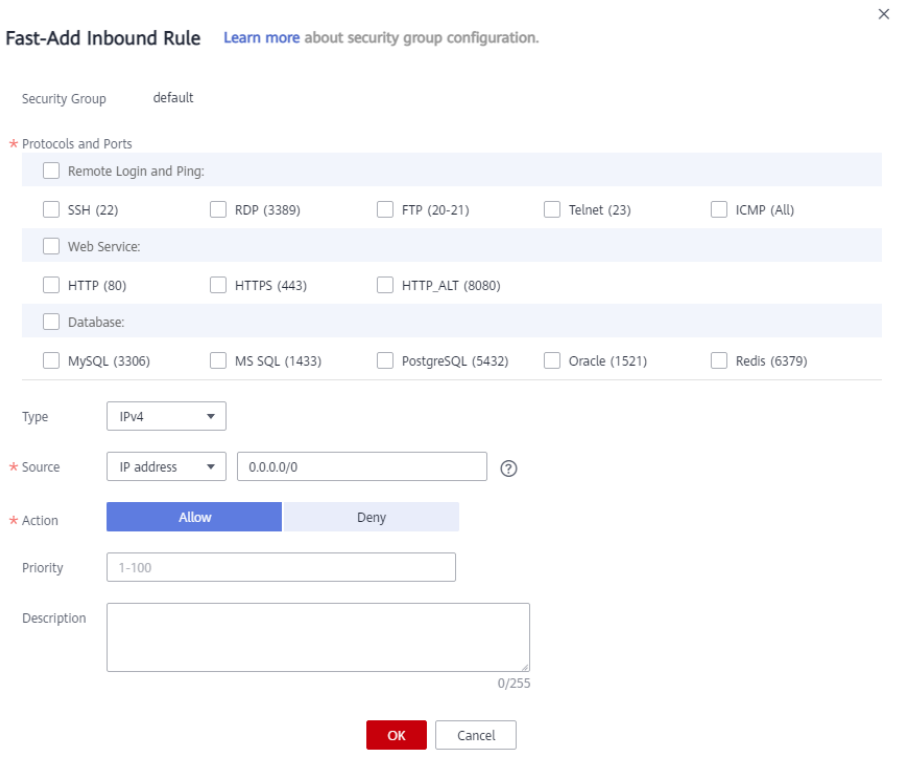


Tabela 2-9 Descrição do parâmetro da regra de entrada

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 de origem. Você pode selecionar: ● IPv4 ● IPv6	IPv4
Source	A origem em uma regra de entrada é usada para corresponder ao endereço IP ou intervalo de endereços de uma solicitação externa. A origem pode ser: ● **IP address**: – Endereço IP único: endereço/máscara IP Exemplo de endereço IPv4: 192.168.10.10/32 Exemplo de endereço IPv6: 2002:50::44/128 – Intervalo de endereços IP na notação CIDR: endereço/máscara IP Exemplo de intervalo de endereços IPv4: 192.168.52.0/24 Exemplo de intervalo de endereços IPv6: 2407:c080:802:469::/64 – Todos os endereços IP 0.0.0.0/0 representa todos os endereços IPv4. ::/0 representa todos os endereços IPv6. ● **Security group**: a origem é de outro grupo de segurança. Você pode selecionar um grupo de segurança na mesma região sob a conta atual na lista suspensa. Há a instância A no grupo de segurança A e a instância B no grupo de segurança B. Se o grupo de segurança A tiver uma regra de entrada com **Action** definida como **Allow** e **Source** definida como grupo de segurança B, o acesso da instância B será permitido à instância A. ● **IP address group**: um grupo de endereços IP é uma coleção de um ou mais endereços IP. Você pode selecionar um grupo de endereços IP disponível na lista suspensa. Um grupo de endereços IP pode ajudá-lo a gerenciar intervalos de endereços IP e endereços IP com os mesmos requisitos de segurança de uma maneira mais simples.	Security group

Parâmetro	Descrição	Exemplo de valor
Action	Allow ou Deny ● Se a **Action** estiver definida como **Allow**, o acesso da origem será permitido aos ECSs no grupo de segurança nas portas especificadas. ● Se a **Action** estiver definida como **Deny**, o acesso da origem será negado aos ECSs no grupo de segurança nas portas especificadas. As regras de negação têm precedência sobre as regras de permissão da mesma prioridade.	Allow
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
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 (< ou >).	-

8. Clique em **OK**.

   A lista de regras de entrada é exibida e você pode exibir sua regra adicionada.
9. Na guia **Outbound Rules**, clique em **Fast-Add Rule**.

   A caixa de diálogo **Fast-Add Outbound Rule** é exibida.
10. Configure os parâmetros necessários.

Figura 2-9 Adição rápida de regra de entrada

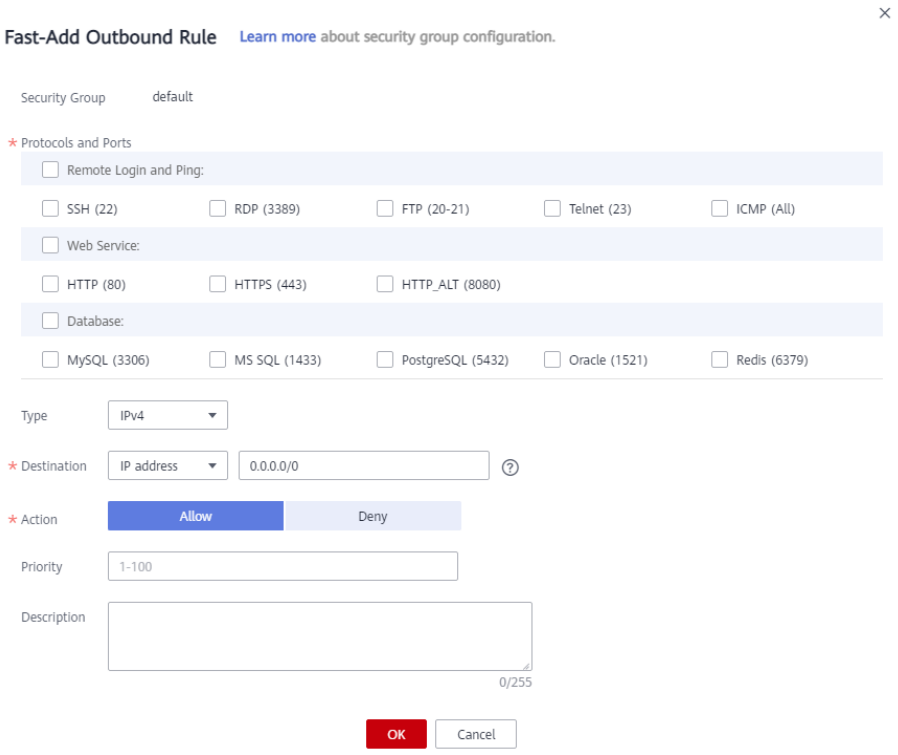


Tabela 2-10 Descrição do parâmetro de regra de saída

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 de origem. Você pode selecionar: ● IPv4 ● IPv6	IPv4

Parâmetro	Descrição	Exemplo de valor
Destination	O destino em uma regra de saída é usado para corresponder ao endereço IP ou intervalo de endereços de uma solicitação interna. O destino pode ser: ● **IP address** – Endereço IP único: endereço/máscara IP Exemplo de endereço IPv4: 192.168.10.10/32 Exemplo de endereço IPv6: 2002:50::44/128 – Intervalo de endereços IP na notação CIDR: endereço/máscara IP Exemplo de intervalo de endereços IPv4: 192.168.52.0/24 Exemplo de intervalo de endereços IPv6: 2407:c080:802:469::/64 – Todos os endereços IP 0.0.0.0/0 representa todos os endereços IPv4. ::/0 representa todos os endereços IPv6. ● **Security group**: o destino é de outro grupo de segurança. Você pode selecionar um grupo de segurança na mesma região sob a conta atual na lista suspensa. Há a instância A no grupo de segurança A e a instância B no grupo de segurança B. Se o grupo de segurança A tiver uma regra de saída com **Action** definida como **Allow** e **Destination** definido como grupo de segurança B, o acesso da instância A será permitido à instância B. ● **IP address group**: um grupo de endereços IP é uma coleção de um ou mais endereços IP. Você pode selecionar um grupo de endereços IP disponível na lista suspensa. Um grupo de endereços IP pode ajudá-lo a gerenciar intervalos de endereços IP e endereços IP com os mesmos requisitos de segurança de uma maneira mais simples.	Security group
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	Allow ou Deny ● Se a **Action** estiver definida como **Allow**, o acesso de ECSs no grupo de segurança será permitido ao destino pelas portas especificadas. ● Se a **Action** estiver definida como **Deny**, o acesso de ECSs no grupo de segurança será negado ao destino nas portas especificadas. As regras de negação têm precedência sobre as regras de permissão da mesma prioridade.	Allow

Parâmetro	Descrição	Exemplo de valor
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 (< ou >).	-

11. Clique em **OK**.

    A lista de regras de saída é exibida e você pode exibir sua regra adicionada.

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. 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, em **Rede**, 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

Você pode modificar a porta, o protocolo e o endereço IP das regras do grupo de segurança conforme necessário para garantir a segurança das suas instâncias.

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, em **Rede**, 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 de 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.

Observações e restrições

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. As regras de grupo de segurança funcionam da seguinte forma:

- Se uma solicitação de entrada corresponder à origem em uma regra de grupo de segurança de entrada com **Action** definida como **Allow**, a solicitação será permitida.
- Se o destino de uma regra de grupo de segurança de saída com **Action** definida como **Allow** for 0.0.0.0/0, todas as solicitações de saída serão permitidas.

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, em **Rede**, 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

- As regras de grupo de segurança a serem importadas devem ser configuradas com base no modelo. Não adicione parâmetros ou altere parâmetros existentes. Caso contrário, a importação falhará.
- Se uma regra de grupo de segurança a ser importada for igual a uma existente, a regra de grupo de segurança não poderá ser importada. Você pode excluir a regra e tentar novamente.

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, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > **Security Groups**.

   A lista de grupos de segurança é exibida.
5. Na lista grupo de segurança, clique no nome do grupo de segurança de destino.

   A página de detalhes do grupo de segurança é exibida.
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 2-11 descreve os parâmetros no modelo para regras de importação.

Tabela 2-11 Parâmetros do modelo

Parâmetro	Descrição	Exemplo de valor
Direction	A direção na qual a regra de grupo de segurança entra em vigor. ● **Inbound**: as regras de entrada controlam o tráfego que flui para os servidores do grupo de segurança. ● **Outbound**: as regras de saída controlam o tráfego de saída dos recursos da nuvem no grupo de segurança.	Inbound
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.	Allow

Parâmetro	Descrição	Exemplo de valor
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	Versão do endereço IP de origem. Você pode selecionar: ● IPv4 ● IPv6	IPv4

Parâmetro	Descrição	Exemplo de valor
Source	A origem em uma regra de entrada é usada para corresponder ao endereço IP ou intervalo de endereços de uma solicitação externa. A origem pode ser: ● **IP address**: – Endereço IP único: endereço/máscara IP Exemplo de endereço IPv4: 192.168.10.10/32 Exemplo de endereço IPv6: 2002:50::44/128 – Intervalo de endereços IP na notação CIDR: endereço/máscara IP Exemplo de intervalo de endereços IPv4: 192.168.52.0/24 Exemplo de intervalo de endereços IPv6: 2407:c080:802:469::/64 – Todos os endereços IP 0.0.0.0/0 representa todos os endereços IPv4. ::/0 representa todos os endereços IPv6. ● **Security group**: a origem é de outro grupo de segurança. Você pode selecionar um grupo de segurança na mesma região sob a conta atual. Há a instância A no grupo de segurança A e a instância B no grupo de segurança B. Se o grupo de segurança A tiver uma regra de entrada com **Action** definida como **Allow** e **Source** definida como grupo de segurança B, o acesso da instância B será permitido à instância A. Um grupo de segurança está no formato de *Nome do grupo de segurança [ID do grupo de segurança]*. Um exemplo é sg-test[96a8a93f-XXX-d7872990c314]. ● **IP address group**: um grupo de endereços IP é uma coleção de um ou mais endereços IP. Você pode selecionar um grupo de endereços IP disponível. Um grupo de endereços IP pode ajudá-lo a gerenciar intervalos de endereços IP e endereços IP com os mesmos requisitos de segurança de uma maneira mais simples. Um grupo de segurança está no formato de *Nome do grupo de endereços IP [ID do grupo de endereços IP]*. Um exemplo é ipGroup-test[96a8a93f-XXX-d7872990c314].	sg-test[96a8a93f-XXX-d7872990c314]

Parâmetro	Descrição	Exemplo de valor
Destination	O destino em uma regra de saída é usado para corresponder ao endereço IP ou intervalo de endereços de uma solicitação interna. O destino pode ser: ● **IP address** – Endereço IP único: endereço/máscara IP Exemplo de endereço IPv4: 192.168.10.10/32 Exemplo de endereço IPv6: 2002:50::44/128 – Intervalo de endereços IP na notação CIDR: endereço/máscara IP Exemplo de intervalo de endereços IPv4: 192.168.52.0/24 Exemplo de intervalo de endereços IPv6: 2407:c080:802:469::/64 – Todos os endereços IP 0.0.0.0/0 representa todos os endereços IPv4. ::/0 representa todos os endereços IPv6. ● **Security group**: o destino é de outro grupo de segurança. Há a instância A no grupo de segurança A e a instância B no grupo de segurança B. Se o grupo de segurança A tiver uma regra de saída com **Action** definida como **Allow** e **Destination** definido como grupo de segurança B, o acesso da instância A será permitido à instância B. Um grupo de segurança está no formato de *Nome do grupo de segurança [ID do grupo de segurança]*. Um exemplo é sg-test[96a8a93f-XXX-d7872990c314]. ● **IP address group**: um grupo de endereços IP é uma coleção de um ou mais endereços IP. Um grupo de endereços IP pode ajudá-lo a gerenciar intervalos de endereços IP e endereços IP com os mesmos requisitos de segurança de uma maneira mais simples. Um grupo de segurança está no formato de *Nome do grupo de endereços IP [ID do grupo de endereços IP]*. Um exemplo é ipGroup-test[96a8a93f-XXX-d7872990c314].	sg-test[96a8a93f-XXX-d7872990c314]
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 (< ou >).	-
Last Modified	A hora em que o grupo de segurança foi modificado.	-

2.1.11 Exclusão de um grupo de segurança

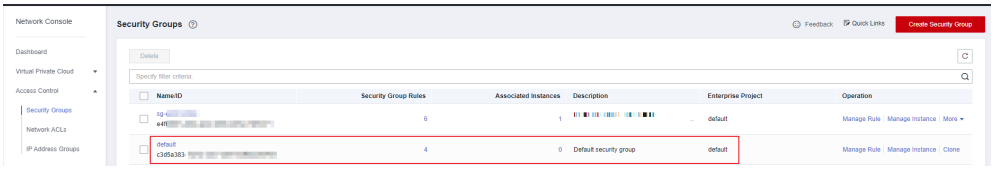
Cenários

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 2-10 Grupo de segurança padrão



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

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

  Se ainda não for possível 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 excluído se for utilizado como origem ou destino 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. 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, em **Rede**, clique em **Virtual Private Cloud**.
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 Adição de instâncias e remoção 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. 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, em **Rede**, 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. 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, em **Rede**, 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. 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, em **Rede**, 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 conforme solicitado.
7. 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 grupo de segurança

Cenários

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

Procedimento

Método 1

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, em **Rede**, 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. 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, em **Rede**, 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

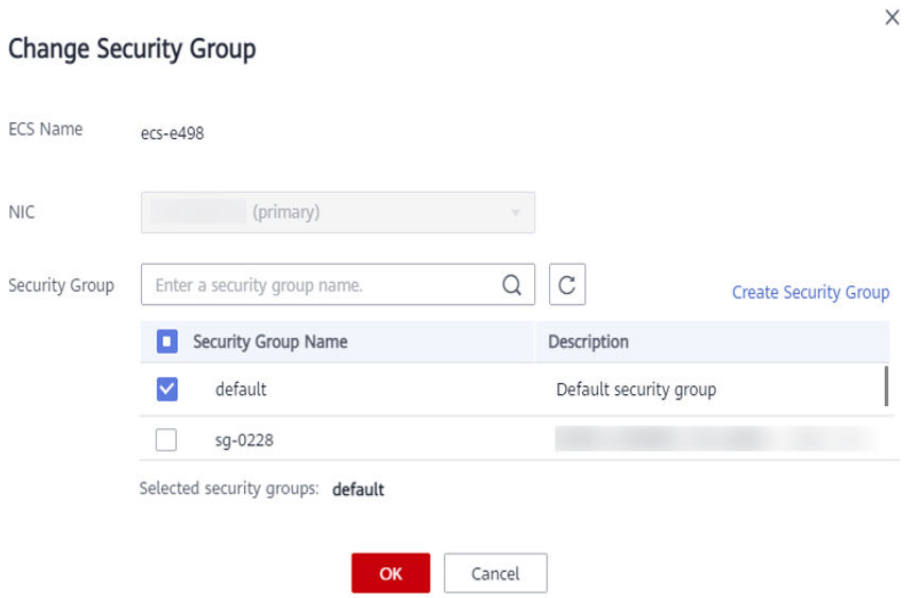
Alterar o grupo de segurança associado a uma NIC do ECS.

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 2-11 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

When adding a security group rule, you must specify the port or port range for communication. When a security group detects an access request, it checks whether the IP address and the port of the device that sends the request are allowed by security group rules. Data communication can be established only when security group rules allow the request.

Tabela 2-12 lists the common ports used by ECSs. You can configure security group rules to allow traffic to and from specified ECS ports. For details, see **Adição de uma regra de grupo de segurança**. For more information about requirements for Windows, see **Service overview and network port requirements for Windows**.

Tabela 2-12 Common ports used by ECSs

Protocol	Port	Description
FTP	21	Used to upload and download files
SSH	22	Used to remotely connect to Linux ECSs
Telnet	23	Used to remotely log in to ECSs using Telnet
SMTP	25	Used to send emails For security purposes, TCP port 25 is disabled in the outbound direction by default.
HTTP	80	Used to access websites over HTTP
POP3	110	Used to receive emails using Post Office Protocol version 3 (POP3)
IMAP	143	Used to receive emails using Internet Message Access Protocol (IMAP)
HTTPS	443	Used to access websites over HTTPS
SQL Server	1433	A TCP port of the SQL Server for providing services
SQL Server	1434	A UDP port of the SQL Server for returning the TCP/IP port number used by the SQL Server
Oracle	1521	Oracle database communications port, which must be enabled on the ECSs where Oracle SQL Server is deployed
MySQL	3306	Used by MySQL databases to provide services
Windows Server Remote Desktop Services	3389	Used to connect to Windows ECSs
Proxy	8080	Proxy port 8080 used in the WWW proxy service for web browsing. If you use port 8080, you need to add **:8080** after the IP address when you visit a website or use a proxy server. After Apache Tomcat is installed, the default service port is 8080.
NetBIOS	137, 138, and 139	NetBIOS is often used for Windows files, printer sharing, and Samba. ● Ports 137 and 138: UDP ports that are used when transferring files using Network Neighborhood (My Network Places) ● Port 139: Connections from this port try to access the NetBIOS/SMB service.

Some Ports Inaccessible

Symptom: Users in certain areas cannot access some ports.

Analysis: Ports listed in the following table are high-risk ports and are blocked by default.

Tabela 2-13 High-risk ports

Protocol	Port
TCP	42, 135, 137, 138, 139, 444, 445, 593, 1025, 1068, 1433, 1434, 3127, 3128, 3129, 3130, 4444, 4789, 5554, 5800, 5900, 8998, 9995, and 9996
UDP	135 to 139, 1026, 1027, 1028, 1068, 1433, 1434, 4789, 5554, 9995, and 9996

Solution: It is recommended that you use ports that are not listed in the table for your services.

2.2 ACLs da rede

2.2.1 ACLs da rede Overview

A ACL da rede is an optional layer of security for your subnets. After you associate one or more subnets with a ACL da rede, you can control traffic in and out of the subnets.

Similar to security groups, ACLs da rede control access to subnets and add an additional layer of defense to your subnets. Security groups only have the "allow" rules, but ACLs da rede have both "allow" and "deny" rules. You can use ACLs da rede together with security groups to implement comprehensive and fine-grained access control.

ACLs da rede Basics

- Your VPC does not come with a ACLs da rede, but you can create a ACLs da rede and associate it with a VPC subnet if required. By default, each ACLs da rede denies all inbound traffic to and outbound traffic from the associated subnet until you add rules.
- You can associate a ACLs da rede with multiple subnets. However, a subnet can only be associated with one ACLs da rede at a time.
- Each newly created ACLs da rede is in the **Inactive** state until you associate subnets with it.
- ACLs da rede are stateful. If the ACLs da rede allows outbound traffic and you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound ACLs da rede rules. Similarly, if inbound traffic is allowed, responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.

  The timeout period of connection tracking varies according to the protocol. The timeout period of a TCP connection in the established state is 600s, and the timeout period of an ICMP connection is 30s. For other protocols, if packets are received in both directions, the connection tracking timeout period is 180s. If one or more packets are received in

one direction but no packet is received in the other direction, the connection tracking timeout period is 30s. For protocols other than TCP, UDP, and ICMP, only the IP address and protocol number are tracked.

Default regra de ACLs da rede

By default, each ACLs da rede has preset rules that allow the following packets:

- Packets whose source and destination are in the same subnet.
- Broadcast packets with the destination 255.255.255.255/32, which is used to configure host startup information.
- Multicast packets with the destination 224.0.0.0/24, which is used by routing protocols.
- Metadata packets with the destination 169.254.169.254/32 and TCP port number 80, which is used to obtain metadata.
- Packets from CIDR blocks that are reserved for public services (for example, packets with the destination 100.125.0.0/16).
- A ACLs da rede denies all traffic in and out of a subnet excepting the preceding packets. **Tabela 2-14** shows the default rules. You cannot modify or delete the default rules.

Tabela 2-14 Default regra de ACLs da rede

Direction	Priority	Action	Protocol	Source	Destination	Description
Inbound	*	Deny	All	0.0.0.0/0	0.0.0.0/0	Denies all inbound traffic.
Outbound	*	Deny	All	0.0.0.0/0	0.0.0.0/0	Denies all outbound traffic.

Rule Priorities

- Each ACLs da rede rule has a priority value where a smaller value corresponds to a higher priority. Any time two rules conflict, the rule with the higher priority is the one that gets applied. The rule whose priority value is an asterisk (*) has the lowest priority.
- If multiple regra de ACLs da rede conflict, only the rule with the highest priority takes effect. If you need a rule to take effect before or after a specific rule, you can insert that rule before or after the specific rule.

Application Scenarios

- If the application layer needs to provide services for users, traffic must be allowed to reach the application layer from all IP addresses. However, you also need to prevent illegal access from malicious users.

  Solution: You can add regra de ACLs da rede to deny access from suspect IP addresses.
- How can I isolate ports with identified vulnerabilities? For example, how do I isolate port 445 that can be exploited by WannaCry worm?

  Solution: You can add regra de ACLs da rede to deny access traffic from a specific port and protocol, for example, TCP port 445.

- No defense is required for the communication within a subnet, but access control is required for communication between subnets.

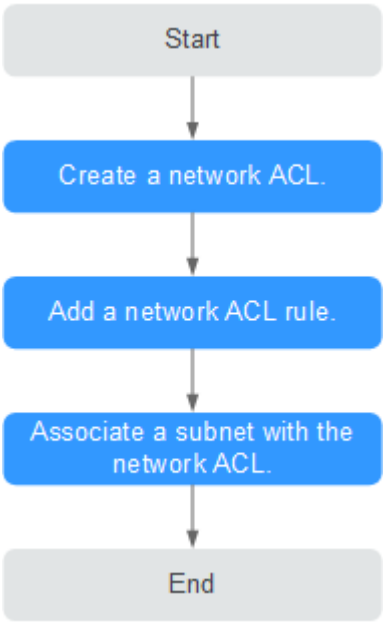
  Solution: You can add regra de ACLs da rede to control traffic between subnets.
- For frequently accessed applications, a security rule sequence may need to be adjusted to improve performance.

  Solution: A ACLs da rede allows you to adjust the rule sequence so that frequently used rules are applied before other rules.

Configuration Procedure

Figura 2-12 shows the procedure for configuring a ACLs da rede.

Figura 2-12 ACLs da rede configuration procedure



1. Create a ACLs da rede by following the steps described in **Criação de uma ACL da rede**.
2. Add regra de ACLs da rede by following the steps described in **Adição uma regra de ACL da rede**.
3. Associate subnets with the ACLs da rede by following the steps described in **Associação de sub-redes com uma ACL da rede**. After subnets are associated with the ACLs da rede, the subnets will be protected by the configured regra de ACLs da rede.

Notes and Constraints

- By default, you can create a maximum of 200 ACLs da rede in your cloud account.
- A ACL da rede can contain no more than 20 rules in one direction, or performance will deteriorate.
- For optimal performance, import no more than 40 regra de ACLs da rede at a time. Existing rules will still be available after new rules are imported. Each rule can be imported only once.

2.2.2 Exemplos de configuração de ACLs da rede

Esta seção fornece exemplos para configurar as ACLs da rede.

- **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 2-15** lista a regra de entrada necessária.

Tabela 2-15 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 regras ACL 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 regras ACL da rede e regras de grupo de segurança para permitir o tráfego.

ACL da rede Configuração **Tabela 2-16** lista a regra de entrada necessária.

Tabela 2-16 Regras de regras ACL 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.
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 2-17 lista as regras de grupo de segurança de entrada e saída necessárias.

Tabela 2-17 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 regras ACL 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

regras ACL 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 regras ACL da rede regra para negar o acesso de alguns endereços IP anormais, por exemplo, 192.168.1.102.

ACL da rede**Tabela 2-18** lista as regras de entrada necessárias.

Tabela 2-18 Regras de regras ACL 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 ACL da rede

Cenários

Você pode criar uma ACL da rede personalizado. Por padrão, uma ACL da rede recém-criada é desabilitada e não tem regras de entrada ou saída, ou quaisquer sub-redes associadas. Cada usuário pode criar até 200 ACL da rede por padrão.

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, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > ACL da rede.

5. No painel direito exibido, clique em **Create ACL da rede**.
6. Na página **Create ACL da rede**, configure os parâmetros conforme solicitado.

Tabela 2-19 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Name	O nome da ACL 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
Enterprise Project	Obrigatório O projeto empresarial ao qual a ACL da rede pertence. Um projeto empresarial facilita o gerenciamento de projeto e o agrupamento de recursos da nuvem e de usuários. O projeto padrão é **default**. Para obter detalhes sobre como criar e gerenciar projetos da empresa, consulte o *Guia de usuário do Enterprise Management*.	default
Description	Informação complementar sobre a ACL da rede. Este parâmetro é opcional. A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	N/D

7. Clique em **OK**.

2.2.4 Adição uma regra de ACL da rede

Cenários

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

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

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, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** >ACL da rede.

5. Localize a regras ACL da rede de destino e clique em seu nome para alternar para a página que mostra detalhes dessa regras ACL 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 regras ACL da rede e clique em **Replicate** na coluna **Operation** para replicar uma regra existente.

Tabela 2-20 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Priority	Prioridade de uma regra de ACL da rede. Um valor de prioridade menor representa uma prioridade mais alta. Cada network ACL inclui uma regra padrão cujo valor de prioridade é um asterisco (*). As regras padrão têm a prioridade mais baixa.	3
Status	Status de uma ACL 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 da ACL 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 no ACL 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 ACL da rede. Este parâmetro é obrigatório. Você pode selecionar um protocolo na lista suspensa. Você pode selecionar **TCP**, **UDP**, **ICMP** ou **All**.	TCP

Parâmetro	Descrição	Exemplo de valor
Source	A origem pode ser: ● **IP address** – Endereço IP único: endereço/máscara IP Exemplo de endereço IPv4: 192.168.10.10/32 Exemplo de endereço IPv6: 2002:50::44/128 – Intervalo de endereços IP na notação CIDR: endereço/máscara IP Exemplo de intervalo de endereços IPv4: 192.168.52.0/24 Exemplo de intervalo de endereços IPv6: 2407:c080:802:469::/64 – Todos os endereços IP 0.0.0.0/0 representa todos os endereços IPv4. ::/0 representa todos os endereços IPv6. ● **IP address group**: um grupo de endereços IP é uma coleção de um ou mais endereços IP. Você pode selecionar um grupo de endereços IP disponível na lista suspensa. Um grupo de endereços IP pode ajudá-lo a gerenciar intervalos de endereços IP e endereços IP com os mesmos requisitos de segurança de uma maneira mais simples. A origem ou o destino de uma regra de network ACL pode usar o grupo de endereços IP. Por exemplo, se a origem usar um grupo de endereços IP, o endereço de destino não poderá usar um grupo de endereços IP.	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 pode ser: ● **IP address** – Endereço IP único: endereço/máscara IP Exemplo de endereço IPv4: 192.168.10.10/32 Exemplo de endereço IPv6: 2002:50::44/128 – Intervalo de endereços IP na notação CIDR: endereço/máscara IP Exemplo de intervalo de endereços IPv4: 192.168.52.0/24 Exemplo de intervalo de endereços IPv6: 2407:c080:802:469::/64 – Todos os endereços IP 0.0.0.0/0 representa todos os endereços IPv4. ::/0 representa todos os endereços IPv6. ● **IP address group**: um grupo de endereços IP é uma coleção de um ou mais endereços IP. Você pode selecionar um grupo de endereços IP disponível na lista suspensa. Um grupo de endereços IP pode ajudá-lo a gerenciar intervalos de endereços IP e endereços IP com os mesmos requisitos de segurança de uma maneira mais simples. A origem ou o destino de uma regra de network ACL pode usar o grupo de endereços IP. Por exemplo, se a origem usar um grupo de endereços IP, o endereço de destino não poderá usar um grupo de endereços IP.	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 ACL da rede. Este parâmetro é opcional. A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	N/D

7. Clique em **OK**.

2.2.5 Associação de sub-redes com uma ACL da rede

Cenários

Na página que mostra os detalhes de ACLs da rede, pode associar as sub-redes desejadas a uma ACLs da rede. Depois que uma regras ACL da rede é associada 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. 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, em **Rede**, 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 página exibida, clique na guia **Associated Subnets**.
7. Na página **Associated Subnets**, clique em **Associate**.
8. Na página exibida, selecione as sub-redes a serem associadas a ACLs da rede e clique em **OK**.

NOTA

As sub-redes com ACLs da rede associadas não serão exibidas na página a ser selecionada. Se quiser associar essa sub-rede a outra ACLs da rede, primeiro você deve desassociar a sub-rede da ACLs da rede original. A associação e a dissociação de sub-rede com um clique não são suportadas atualmente. Uma sub-rede só pode ser associada a uma ACLs da rede.

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. 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, em **Rede**, 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 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 de uma 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. 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, em **Rede**, 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 regra de destino, clique em **More** na coluna **Operation** e selecione **Insert Rule Above** ou **Insert Rule Below**.
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 regras ACL da rede com base nos requisitos de segurança da sua rede.

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, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > ACL 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 **Modify** na coluna **Operation**. Na caixa de diálogo exibida,

configure os parâmetros conforme solicitado. **Tabela 2-21** lista os parâmetros a serem configurados.

Tabela 2-21 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Priority	Prioridade de uma regra de ACL da rede. Um valor de prioridade menor representa uma prioridade mais alta. Cada network ACL inclui uma regra padrão cujo valor de prioridade é um asterisco (*). As regras padrão têm a prioridade mais baixa.	3
Status	Status de uma ACL 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 da ACL 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 no ACL 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 ACL da rede. Este parâmetro é obrigatório. Você pode selecionar um protocolo na lista suspensa. Você pode selecionar **TCP**, **UDP**, **ICMP** ou **All**.	TCP

Parâmetro	Descrição	Exemplo de valor
Source	A origem pode ser: ● **IP address** – Endereço IP único: endereço/máscara IP Exemplo de endereço IPv4: 192.168.10.10/32 Exemplo de endereço IPv6: 2002:50::44/128 – Intervalo de endereços IP na notação CIDR: endereço/máscara IP Exemplo de intervalo de endereços IPv4: 192.168.52.0/24 Exemplo de intervalo de endereços IPv6: 2407:c080:802:469::/64 – Todos os endereços IP 0.0.0.0/0 representa todos os endereços IPv4. ::/0 representa todos os endereços IPv6. ● **IP address group**: um grupo de endereços IP é uma coleção de um ou mais endereços IP. Você pode selecionar um grupo de endereços IP disponível na lista suspensa. Um grupo de endereços IP pode ajudá-lo a gerenciar intervalos de endereços IP e endereços IP com os mesmos requisitos de segurança de uma maneira mais simples. A origem ou o destino de uma regra de network ACL pode usar o grupo de endereços IP. Por exemplo, se a origem usar um grupo de endereços IP, o endereço de destino não poderá usar um grupo de endereços IP.	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 pode ser: ● **IP address** – Endereço IP único: endereço/máscara IP Exemplo de endereço IPv4: 192.168.10.10/32 Exemplo de endereço IPv6: 2002:50::44/128 – Intervalo de endereços IP na notação CIDR: endereço/máscara IP Exemplo de intervalo de endereços IPv4: 192.168.52.0/24 Exemplo de intervalo de endereços IPv6: 2407:c080:802:469::/64 – Todos os endereços IP 0.0.0.0/0 representa todos os endereços IPv4. ::/0 representa todos os endereços IPv6. ● **IP address group**: um grupo de endereços IP é uma coleção de um ou mais endereços IP. Você pode selecionar um grupo de endereços IP disponível na lista suspensa. Um grupo de endereços IP pode ajudá-lo a gerenciar intervalos de endereços IP e endereços IP com os mesmos requisitos de segurança de uma maneira mais simples. A origem ou o destino de uma regra de network ACL pode usar o grupo de endereços IP. Por exemplo, se a origem usar um grupo de endereços IP, o endereço de destino não poderá usar um grupo de endereços IP.	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 ACL da rede. Este parâmetro é opcional. A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	N/D

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. 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, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > ACL 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 **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. 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, em **Rede**, 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 ACLs 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 e, em seguida, importar essas regras para outra 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. A importação de regras duplicadas falhará.

Exportação de regras de ACLs da rede

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, em **Rede**, 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. 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. 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, em **Rede**, 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 regras ACL da rede particular.
6. Clique em .
7. Selecione o arquivo do Excel que contém as regras exportadas de regras ACL da rede e 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. 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, em **Rede**, 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 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 Modificação de uma ACLs da rede.

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, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > Modificação de uma ACLs da rede.
5. Localize a Modificação de uma 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 **Description** 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 **Default regra de ACLs da rede**.

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, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Access Control** > ACL da rede.
5. Localize a linha que contém a ACLs da rede 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 ACLs da rede quando ele não for mais necessário.

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, em **Rede**, 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 no painel direito, clique em **More** na coluna **Operation** e clique em **Delete**.
6. Clique em **Yes**.

   NOTA

   A exclusão de uma ACLs da rede também desassociará suas sub-redes associadas e excluirá as regras de ACLs da rede.

3 Visão geral do grupo de endereços IP

Visão geral do grupo de endereços IP

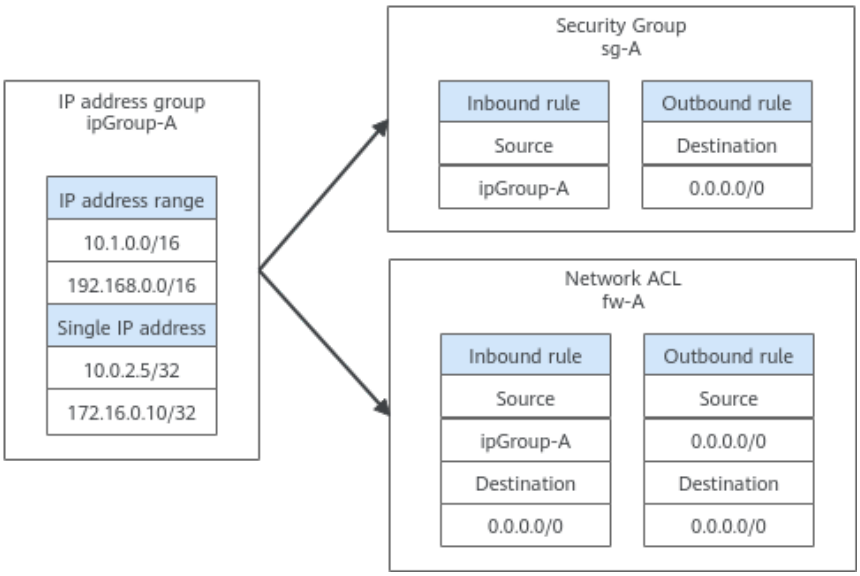
Um grupo de endereços IP é uma coleção de endereços IP. Ele pode ser associado a grupos de segurança e ACLs da rede para simplificar a configuração e o gerenciamento de endereços IP.

Você pode adicionar intervalos de endereços IP e endereços IP que precisam ser gerenciados de maneira unificada a um grupo de endereços IP. Um grupo de endereços IP pode trabalhar em conjunto com diferentes recursos de nuvem. **Tabela 3-1** lista os recursos que podem ser associados a um grupo de endereços IP.

Tabela 3-1 Recursos que podem ser associados a um grupo de endereços IP

Recurso	Descrição	Exemplo
Grupo de segurança	**Source** ou **Destination** de uma regra de grupo de segurança pode ser definida como **IP address group**.	Conforme mostrado em **Figura 3-1**, a regra de entrada do grupo de segurança sg-A usa o grupo de endereços IP ipGroup-A como origem.
ACL da rede	A **Source** ou o **Destination** de uma ACL da rede é definido como **IP address group**.	Conforme mostrado em **Figura 3-1**, a regra de entrada da ACL da rede fw-A usa o grupo de endereços IP ipGroup-A como origem.

Figura 3-1 Usar o grupo de endereços IP



Observações e restrições

- As regras de grupo de segurança associadas a um grupo de endereços IP não entram em vigor para determinados ECSs.
  - 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)
- Se uma regra de regras ACL da rede usar um grupo de endereços IP:
  - A origem ou o destino de uma regra de entrada pode usar o grupo de endereços IP.
  - A origem ou o destino de uma regra de saída pode usar o grupo de endereços IP.

  Por exemplo, se a origem de uma regra de entrada de ACLs da rede estiver definida como um grupo de endereços IP, o destino da regra só poderá ser um endereço IP.

4 Criação de um grupo de endereços IP

Cenários

Esta seção descreve como criar um grupo de endereços IP. Um grupo de endereços IP é uma coleção de endereços IP que pode ser vinculada a grupos de segurança, ACLs da rede para simplificar a configuração e o gerenciamento de endereços IP.

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, em **Rede**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **IP Address Groups**.

   A lista de grupos de endereços IP é exibida.
5. No canto superior direito da lista de grupos de endereços IP, clique em **Create IP Address Group**.

   A página **Create IP Address Group** é exibida.
6. Configure os parâmetros conforme solicitado.

   Para mais detalhes, consulte **Tabela 4-1**.

Tabela 4-1 Parâmetros para criar um grupo de endereços IP

Parâmetro	Descrição	Exemplo de valor
Region	Obrigatório Selecione a região mais próxima de você para garantir a menor latência possível. Um grupo de endereços IP só pode ser associado a recursos na mesma região.	Region A

Parâmetro	Descrição	Exemplo de valor
Name	Obrigatório Digite o nome do grupo de endereços IP. O nome: ● Pode conter de 1 a 64 caracteres. ● Pode conter letras, dígitos, sublinhados (_), hifens (-) e pontos (.). Você pode personalizar o nome de um grupo de endereços IP identificado exclusivamente por seu ID.	ipGroup-A
IP Address Version	Obrigatório Selecione o tipo de endereços IP que podem ser adicionados a um grupo de endereços IP. ● IPv4 ● IPv6	IPv4
IP Addresses	Opcional Insira um endereço IP ou um intervalo de endereços IP em cada linha e pressione **Enter**. Você pode inserir: ● Um intervalo de endereços IPv4, por exemplo, 192.168.0.0/16 ● Um único endereço IPv4, por exemplo, 192.168.10.10/32 ● Um intervalo de endereços IPv6, por exemplo, 2001:db8:a583:6e::/64 ● Um único endereço IPv6, por exemplo, 2001:db8:a583:6e::5c/128	192.168.0.0/16 192.168.10.10/32
Description	Opcional Digite a descrição do grupo de endereços IP na caixa de texto, conforme necessário.	-

7. Clique em **Create Now**.

   A lista de grupos de endereços IP é exibida. O status do grupo de endereços IP criado é **Normal**.

AVISO

Um grupo de endereços IP só entra em vigor depois de ser associado aos recursos correspondentes. Para mais detalhes, consulte **Associação de um grupo de endereços IP a recursos**.

5 Associação de um grupo de endereços IP a recursos

Cenários

Esta seção descreve como associar um grupo de endereços IP a um recurso.

Um grupo de endereços IP pode ser associado a grupos de segurança e ACLs da rede.

Pré-requisitos

- Você criou um grupo de endereços IP foi criado. Para mais detalhes, consulte **Criação de um grupo de endereços IP**.
- Você adicionou endereços IP ao grupo de endereços IP.

Procedimento

Você precisa associar um grupo de endereços IP a recursos. Para mais detalhes, consulte **Tabela 5-1**.

Tabela 5-1 Associar um grupo de endereços IP a recursos

Recurso	Descrição	Referência
Grupo de segurança	A **Source** ou **Destination** da regra de um grupo de segurança pode ser definida como **IP address group**.	**Adição de uma regra de grupo de segurança** ● Regra de entrada: defina **Source** como um grupo de endereços IP. ● Regra de saída: defina **Destination** como um grupo de endereços IP.

Recurso	Descrição	Referência
ACLs da rede	A **Source** ou o **Destination** ACLs da rede é definido como **IP address group**.	**Adição uma regra de ACL da rede** ● Regra de entrada: defina **Source** ou **Destination** como um grupo de endereços IP. A origem ou o destino podem usar o grupo de endereços IP. ● Regra de saída: defina **Source** ou **Destination** como um grupo de endereços IP. A origem ou o destino podem usar o grupo de endereços IP.

6 Modificação de um grupo de endereços IP

Cenários

Esta seção descreve como modificar informações básicas sobre um grupo de endereços IP, incluindo:

- Name
- Description

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, em **Rede**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **IP Address Groups**.

   A lista de grupos de endereços IP é exibida.
5. Na lista de grupos de endereços IP, clique na hiperligação do nome do grupo de endereços IP.

   A página de informações básicas do grupo de endereços IP é exibida.
6. Na página de guia **Basic Information** do grupo de endereços IP, clique em  na direita do parâmetro de destino e modifique o parâmetro conforme solicitado.

   Para mais detalhes, consulte **Tabela 6-1**.

Tabela 6-1 Parâmetros do grupo de endereços IP

Parâmetro	Descrição	Exemplo de valor
Name	Obrigatório Digite o nome do grupo de endereços IP. O nome: ● Pode conter de 1 a 64 caracteres. ● Pode conter letras, dígitos, sublinhados (_), hifens (-) e pontos (.). Você pode personalizar o nome de um grupo de endereços IP identificado exclusivamente por seu ID.	ipGroup-A
Description	Opcional Digite a descrição do grupo de endereços IP na caixa de texto, conforme necessário.	-

7. Clique em .

7 Interface de rede elástica e interface de rede suplementar

7.1 Elastic Network Interface

7.1.1 Visão geral da interface de rede

Uma interface de rede elástica (referida como interface de rede nesta documentação) é uma placa de rede virtual. Você pode criar e configurar interfaces de rede e anexá-las às suas instâncias (ECSs e BMSs) para obter configurações de rede flexíveis e altamente disponíveis.

Tipos de interface de rede

- Uma interface de rede primária é criada junto com uma instância por padrão, que não pode ser desanexada da sua instância.
- Você pode criar interfaces de rede de extensão, anexá-las a uma instância e desanexá-las da instância. O número de interfaces de rede de extensão que você pode anexar a um ECS varia de acordo com o flavor do ECS.

Cenários de aplicação

- Migração flexível

  Você pode desanexar uma interface de rede de uma instância e, em seguida, anexá-la a outra instância. A interface de rede mantém seu endereço IP privado, EIP e regras de grupo de segurança. Dessa forma, o tráfego de serviço na instância defeituosa pode ser migrado rapidamente para a instância em espera, implementando a recuperação rápida do serviço.
- Gerenciamento de tráfego

  Você pode anexar várias interfaces de rede que pertencem a diferentes sub-redes em uma VPC à mesma instância e configurar as interfaces de rede para transportar o tráfego de rede privada, o tráfego de rede pública e o tráfego de rede de gerenciamento da instância. Você pode configurar políticas de controle de acesso e políticas de roteamento para cada sub-rede e configurar regras de grupo de segurança para cada interface de rede para isolar redes e tráfego de serviço.

Observações e restrições

- Uma instância e suas interfaces de rede de extensão devem estar na mesma AZ, VPC e sub-rede. No entanto, elas podem pertencer a diferentes grupos de segurança.

  NOTA

  Uma interface de rede criada usando a API pode estar em uma VPC diferente daquela da sua instância.

- Uma interface de rede primária não pode ser desanexada da sua instância.
- O número de interfaces de rede de extensão que você pode anexar a uma instância varia de acordo com o flavor da instância. Para obter detalhes, consulte **Especificações do ECS**.
- Interfaces de rede elásticas e NICs de extensão não podem ser usadas para acessar diretamente os serviços da Huawei Cloud, como o DNS. Você pode usar o VPCEP para acessar esses serviços. Para obter detalhes, consulte **Compra de um ponto de extremidade da VPC**.

7.1.2 Criação de uma interface de rede

Cenários

Uma interface de rede primária é criada junto com uma instância por padrão. Esta seção descreve como criar uma interface de rede de extensão.

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, em **Rede**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Network Interfaces**.
5. Clique em **Create Network Interface**.
6. Configure parâmetros para a interface de rede, conforme mostrado na **Tabela 7-1**.

Tabela 7-1 Descrições de parâmetro

Parâmetro	Descrição do parâmetro	Exemplo de valor
Name	(Obrigatório) Especifica o nome da interface de rede. O nome pode conter no máximo 64 caracteres, que podem ser letras, dígitos, sublinhados (_), hifens (-) e pontos (.). O nome não pode conter espaços.	networkInterface-891e
VPC	(Obrigatório) Selecione a VPC à qual a interface de rede pertence.	vpc-001

Parâmetro	Descrição do parâmetro	Exemplo de valor
Subnet	(Obrigatório) Selecione a sub-rede à qual a interface de rede pertence.	subnet-001
Private IP Address	Selecione se deseja atribuir automaticamente um endereço IP privado.	-
Security Group	Selecione o grupo de segurança ao qual a interface de rede pertence.	sg-001

7. Clique em **OK**.

7.1.3 Exibição de informações básicas sobre uma interface de rede

Cenários

Você pode visualizar informações básicas sobre a interface de rede no console de gerenciamento, incluindo nome, ID, tipo, VPC, instância anexada e grupos de segurança associados.

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, em **Rede**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Network Interfaces**.
5. Na página **Network Interfaces**, clique no nome da interface de rede de destino.

Outras operações

Na página de detalhes da interface de rede, você também pode modificar as seguintes informações:

- Você pode editar o nome da interface de rede, alterar endereços IP e anexar a interface de rede ou desanexá-la da instância.
- Exclusão dependente da instância
  - **Instance-dependent Deletion** está desabilitada por padrão. A interface de rede não será excluída se for desanexada da instância ou se a instância for excluída. Você pode anexar a interface de rede à outra instância.
  - Se **Instance-dependent Deletion** tiver sido ativada, a interface de rede será excluída após ser desanexada da instância.

7.1.4 Anexação de uma interface de rede a uma instância

Cenários

Você pode anexar uma interface de rede a um ECS ou a um BMS para obter configurações de rede flexíveis e de alta disponibilidade.

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, em **Rede**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Network Interfaces**.
5. Na lista de interface de rede, localize a linha que contém a interface de rede de destino, clique em **Attach Instance** na coluna **Operation** e selecione a instância a ser anexada.
6. Clique em **OK**.

Operações relacionadas

Depois que uma interface de rede é anexada a uma instância, recomenda-se ativar a multifila de NIC para melhorar o desempenho da rede. Para obter detalhes, consulte **Ativação de multifila de NIC**.

7.1.5 Vinculação de uma interface de rede a um EIP

Cenários

Você pode vincular um EIP a uma interface de rede para obter redes mais flexíveis e escaláveis.

Cada interface de rede tem um endereço IP privado. Depois que a interface de rede é vinculada a um EIP, a interface de rede tem um endereço IP privado e um endereço IP público. A vinculação entre uma interface de rede e um EIP não será alterada mesmo depois que a interface de rede for desanexada de uma instância. Depois que uma interface de rede é migrada de uma instância para outra, seu endereço IP privado e o EIP serão migrados juntos ao mesmo tempo.

Uma instância pode ter várias interfaces de rede anexadas. Se cada interface de rede tiver um EIP vinculado, a instância terá vários EIPs e poderá fornecer serviços de acesso flexíveis.

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, em **Rede**, clique em **Virtual Private Cloud**.

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

4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Network Interfaces**.
5. Na lista de interface de rede, localize a linha que contém a interface de rede de destino, clique em **Bind EIP** na coluna **Operation** e selecione o EIP a ser vinculado.
6. Clique em **OK**.

7.1.6 Vinculação de uma interface de rede a um endereço IP virtual

Cenários

Você pode vincular uma interface de rede a um endereço IP virtual para que possa acessar a instância anexada à interface de rede usando o endereço IP virtual.

Apenas uma interface de rede com uma instância anexada pode ser vinculada a um endereço IP virtual.

Para obter mais informações sobre endereços IP virtuais, consulte **Visão geral do endereço IP virtual**.

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, em **Rede**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Network Interfaces**.
5. Na lista de interface de rede, localize a linha que contém a interface de rede de destino e escolha **More** > **Bind Virtual IP Address** na coluna **Operation**.

   A página **IP Addresses** será exibida.
6. Localize a linha que contém o endereço IP virtual de destino e clique em **Bind to Server** na coluna **Operation**.
7. Selecione o servidor e a NIC e clique em **OK**.

7.1.7 Desanexação de uma interface de rede de uma instância ou desvinculação um EIP de uma interface de rede

Cenários

Esta seção descreve como desanexar uma interface de rede de uma instância ou desvincular uma interface de rede de um EIP.

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, em **Rede**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Network Interfaces**.
5. Na lista de interface de rede, localize a linha que contém a interface de rede de destino e clique em **Detach Instance** ou **Unbind EIP** na coluna **Operation**.
6. Clique em **Yes**.

   Se você não precisar mais de um EP, poderá liberar o EIP após desvinculá-lo.

7.1.8 Alteração de grupos de segurança associados a uma interface de rede

Cenários

Você pode alterar os grupos de segurança associados a uma interface de rede na página da lista de interfaces de rede ou na página de detalhes da interface de rede.

Procedimento

Alterar o grupo de segurança associado a uma interface de rede na página da lista de interfaces de rede

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, em **Rede**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Network Interfaces**.
5. Na lista de interface de rede, localize a linha que contém a interface de rede de destino e escolha **More** > **Change Security Group** na coluna **Operation**.
6. Na página **Change Security Group**, selecione os grupos de segurança a serem associados e clique em **OK**.

Alterar grupo de segurança associado a uma interface de rede na página de detalhes da interface de rede

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, em **Rede**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Network Interfaces**.
5. Clique no nome da interface de rede de destino.
6. Clique na guia **Associated Security Groups**. Em seguida, clique em **Change Security Group**.
7. Na página **Change Security Group**, selecione os grupos de segurança a serem associados e clique em **OK**.

Outras operações

Na página de detalhes da interface de rede, clique na guia **Associated Security Groups** e, em seguida, clique em **Manage Rule**. Para obter detalhes sobre como configurar regras de grupo de segurança, consulte **Adição de uma regra de grupo de segurança**.

7.1.9 Exclusão de uma interface de rede

Cenários

Esta seção descreve como excluir uma interface de rede.

Uma interface de rede que tenha uma instância anexada não pode ser excluída.

Observações e restrições

Para excluir uma interface de rede com uma instância anexada, você precisa excluir a instância primeiro.

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, em **Rede**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Network Interfaces**.
5. Localize a linha que contém a interface de rede, clique em **More** na coluna **Operation** e clique em **Delete**.

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

7.2 Interfaces de rede suplementares

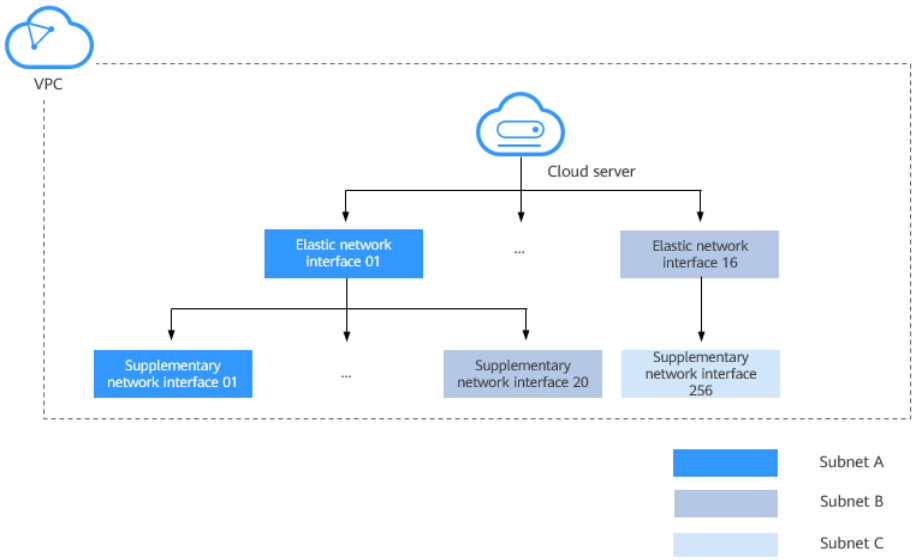
7.2.1 Visão geral da interface de rede suplementar

Interfaces de rede suplementares são um complemento para interfaces de rede elásticas. Se o número de interfaces de rede elásticas que podem ser anexadas ao seu ECS não puder atender aos seus requisitos, você poderá usar interfaces de rede suplementares, que podem ser anexadas a subinterfaces VLAN de interfaces de rede elásticas.

Cenários de aplicação

As interfaces de rede suplementares são anexadas às subinterfaces VLAN de interfaces de rede elásticas. **Figura 7-1** mostra o diagrama de rede.

Figura 7-1 Diagrama de rede suplementar da interface de rede



O número de interfaces de rede elásticas que podem ser anexadas a cada ECS é limitado. Se esse limite não puder atender aos seus requisitos, você poderá anexar interfaces de rede suplementares a interfaces de rede elásticas.

- Você pode anexar interfaces de rede suplementares que pertençam a diferentes sub-redes na mesma VPC a um ECS. Cada interface de rede suplementar tem seu endereço IP privado e EIP para comunicação privada ou pela Internet.
- Você pode regras de grupo de segurança para interfaces de rede suplementares para isolamento de rede.

Observações e restrições

- Um máximo de 256 interfaces de rede suplementares podem ser anexadas a um ECS de determinados flavors. O número de interfaces de rede suplementares que podem ser anexadas a um ECS varia de acordo com o flavor do ECS. As especificações do ECS que suportam interfaces de rede suplementares são as seguintes:

  ECS: séries C7, S7 e M7. Para obter detalhes, consulte **Especificações do ECS**.

  Contêiner de nuvem: c6ne
- As interfaces de rede suplementares e sua interface de rede elástica devem estar na mesma VPC, mas podem pertencer a diferentes sub-redes e grupos de segurança.
- Atualmente, somente o grupo de segurança associado a uma interface de rede suplementar pode ser alterado.
- Os logs de fluxo da VPC de uma interface de rede suplementar são gerados junto com sua interface de rede elástica anexada.
- Antes de usar uma interface de rede suplementar, você precisa criar uma subinterface VLAN em sua NIC do ECS e configurar rotas.
- Um ECS não pode usar o Cloud-Init por meio dos endereços IP privados de suas interfaces de rede suplementares.
- Uma interface de rede suplementar não pode ter um endereço IP virtual vinculado.

7.2.2 Criação de uma interface de rede suplementar

Cenários

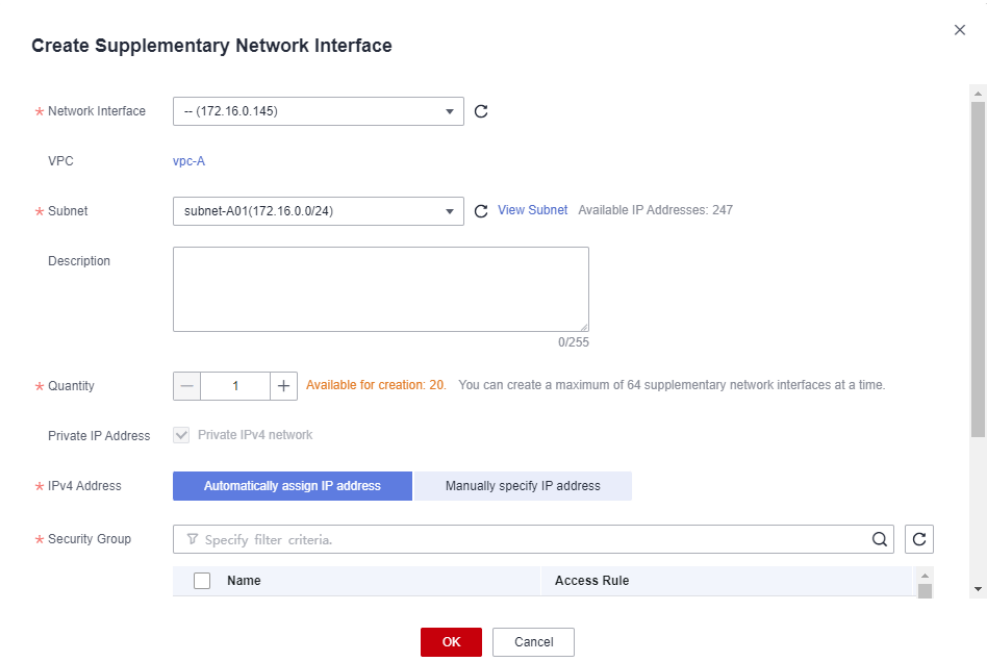
O número de interfaces de rede elásticas que podem ser anexadas a cada ECS é limitado. Se esse limite não puder atender aos seus requisitos, você poderá usar interfaces de rede suplementares.

Criação de uma interface de rede suplementar

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, em **Rede**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Network Interfaces**.
5. No canto superior direito da página, clique em **Create Supplementary Network Interface**.

   Figura 7-2 Criar interface de rede suplementar



6. Configure os parâmetros com base em **Tabela 7-2**.

Tabela 7-2 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Network Interface	Interface de rede elástica à qual a interface de rede suplementar será anexada. Selecione uma interface de rede elástica na lista suspensa.	--(172.16.0.145)
VPC	VPC à qual a interface de rede suplementar pertence. Você não precisa definir esse parâmetro.	vpc-A
Subnet	Selecione a sub-rede para a interface de rede suplementar.	subnet-A01
Description	(Opcional) Digite a descrição da interface de rede suplementar na caixa de texto, conforme necessário. A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	-
Quantity	Número de interfaces de rede suplementares a serem criadas. O valor varia de 1 a 20.	1
Private IP Address	Se atribuir um endereço IPv4 privado à interface de rede suplementar. Este parâmetro não pode ser desmarcado na versão atual.	-
IPv4 Address	Selecione um modo de atribuição de endereço IP virtual. ● **Automatically assign IP address**: o sistema atribui um endereço IP automaticamente. ● **Manually specify IP address**: o sistema atribui um endereço IP especificado por você. Se você selecionar **Manually specify IP address**, insira um endereço IPv4 privado.	Automatically assign IP address
Security Group	Selecione o grupo de segurança ao qual a interface de rede suplementar pertence.	sg-001

7. Clique em **OK**.

Configurar uma interface de rede suplementar

Depois que uma interface de rede suplementar é criada, você precisa criar uma subinterface VLAN e configurar um endereço IP privado e rotas padrão para a interface.

Você precisa obter as informações sobre a interface de rede suplementar, conforme mostrado na **Tabela 7-3**.

Tabela 7-3 Informações suplementares da interface de rede

Informação	Como obter	Descrição
VLAN	Console de gerenciamento	Obtenha o valor da lista de interface de rede suplementar. Para mais detalhes, consulte **Exibição de informações básicas sobre uma interface de rede suplementar**.
Endereço MAC		
Endereço IP privado		
Gateway		Obtenha o valor na página de detalhes da sub-rede à qual a interface de rede suplementar pertence.

O seguinte descreve como criar uma subinterface VLAN no eth0 de um ECS (o CentOS 8.2 é usado como um exemplo. Para obter detalhes sobre outros sistemas operacionais, consulte a documentação do sistema operacional).

Neste exemplo:

- VLAN: 2110
- Endereço IP privado: 192.168.0.2/24
- Gateway: 192.168.0.1
- Endereço MAC: fa:16:3e:a1:b2:**

Procedimento

1. Efetue logon no ECS.

   Para obter detalhes, consulte **Logon em um ECS do Linux**.
2. Crie uma subinterface VLAN para eth0.

   ip link add link *eth0* **name** *eth0.2110* **type vlan id** *2110*
3. Crie um namespace **ns2110**.

   ip netns add *ns2110*
4. Adicione a subinterface VLAN **eth0.2110** ao namespace **ns2110**.

   ip link set *eth0.2110* **netns** *ns2110*
5. Altere o endereço MAC da subinterface VLAN para **fa:16:3e:a1:b2:****.

   ip netns exec *ns2110* **ifconfig** *eth0.2110* **hw ether** *fa:16:3e:a1:b2:***
6. Habilite a subinterface VLAN.

   ip netns exec *ns2110* **ifconfig** *eth0.2110* **up**
7. Configure o endereço IP privado **192.168.0.2/24** para a subinterface VLAN.

   ip netns exec *ns2110* **ip addr add** *192.168.0.2/24* **dev** *eth0.2110*
8. Configure a rota padrão para a subinterface VLAN. 192.168.0.1 é o gateway da sub-rede que a interface de rede suplementar trabalha.

ip netns exec *ns2110* **ip route add default via** *192.168.0.1*

Verificação

1. Acesse outros endereços IP privados na mesma VPC a partir do namespace para verificar se a configuração na interface de rede suplementar entra em vigor.

   ip netns exec *ns2110* **ping** *a.b.c.d*

   Figura 7-3 Exemplo de sucesso

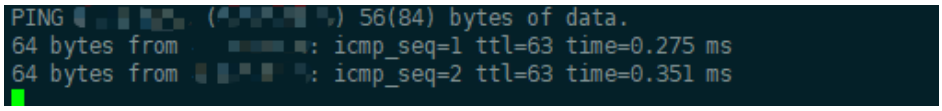
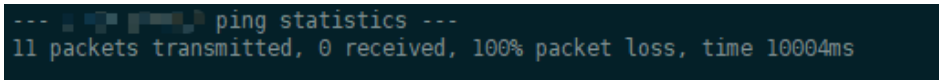
   

   Figura 7-4 Exemplo de falha

7.2.3 Exibição de informações básicas sobre uma interface de rede suplementar

Cenários

Você pode visualizar informações básicas sobre sua interface de rede suplementar no console de gerenciamento, incluindo seu ID, interface de rede, ID da VLAN, VPC, sub-rede, endereço IP privado, EIP, endereço MAC e grupos 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, em **Rede**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Network Interfaces**.
5. Na página **Network Interfaces**, clique na guia **Supplementary Network Interfaces**.
6. Clique no endereço IP privado da interface de rede suplementar cujos detalhes você deseja exibir.
   - Na guia **Summary**, você pode exibir seu ID, interface de rede, ID da VLAN, VPC, sub-rede, endereço IP privado, EIP e endereço MAC.
   - Na guia **Associated Security Groups**, você pode exibir seus grupos de segurança associados e suas regras.

Outras operações

Na página de detalhes da interface de rede suplementar, você também pode modificar as seguintes informações:

- Na guia **Summary**, você pode modificar a descrição da interface e alterar seu EIP vinculado.
- Na guia **Associated Security Groups**, você pode alterar os grupos de segurança associados da interface. Para mais detalhes, consulte **Alteração de grupos de segurança que estão associados a uma interface de rede suplementar**.

7.2.4 Vinculação ou desvinculação de uma interface de rede suplementar de ou para um EIP

Cenários

Você pode vincular uma interface de rede suplementar a um EIP.

Uma interface de rede suplementar tem um endereço IP privado. Você também pode vincular um EIP à interface. A vinculação entre uma interface de rede suplementar e um EIP não é alterada quando a interface de rede da interface de rede suplementar é desanexada de um ECS e, em seguida, anexada a outro ECS. A interface de rede suplementar ainda tem seu endereço IP privado e EIP.

Uma interface de rede pode ter várias interfaces de rede suplementares anexadas. Se cada interface de rede suplementar tiver um EIP, o ECS com a interface de rede anexada poderá ter vários EIPs para acesso flexível à Internet.

Se você não precisar de um EIP ou quiser excluir uma interface de rede suplementar, poderá desvincular o EIP da interface.

Vincular uma interface de rede suplementar a um EIP

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, em **Rede**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Network Interfaces**.
5. Na página **Network Interfaces**, clique na guia **Supplementary Network Interfaces**.
6. Localize a linha que contém a interface de rede suplementar, clique em **Bind EIP** na coluna **Operation** e selecione o EIP a ser vinculado.
7. Clique em **OK**.

Desvincular uma interface de rede suplementar de um EIP

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, em **Rede**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Network Interfaces**.
5. Na página **Network Interfaces**, clique na guia **Supplementary Network Interfaces**.

6. Localize a linha que contém a interface de rede suplementar e clique em **Unbind EIP** na coluna **Operation**.
7. Clique em **Yes**.

7.2.5 Alteração de grupos de segurança que estão associados a uma interface de rede suplementar

Cenários

Depois que uma interface de rede suplementar é criada, você pode alterar seu grupo de segurança.

Você pode alterar o grupo de segurança de uma interface de rede suplementar:

- Na página da lista de interfaces de rede suplementares.
- Na página de detalhes de uma interface de rede suplementar.

Procedimento

Alterar o grupo de segurança associado a uma interface de rede suplementar na página da lista de interfaces de rede suplementares

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, em **Rede**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Network Interfaces**.
5. Na página **Network Interfaces**, clique na guia **Supplementary Network Interfaces**.
6. Localize a linha que contém a interface de rede suplementar e clique em **Change Security Group** na coluna **Operation**.
7. Na página **Change Security Group**, selecione o grupo de segurança a ser associado.
8. Clique em **OK**.

Alterar o grupo de segurança associado a uma interface de rede suplementar na página de detalhes da interface de rede suplementar

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, em **Rede**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Network Interfaces**.
5. Na página **Network Interfaces**, clique na guia **Supplementary Network Interfaces**.
6. Clique no endereço IP privado da interface de rede suplementar cujo grupo de segurança deve ser alterado.
7. Clique na guia **Associated Security Groups**. Em seguida, clique em **Change Security Group**.

8. Na página **Change Security Group**, selecione o grupo de segurança a ser associado.
9. Clique em **OK**.

7.2.6 Exclusão de uma interface de rede suplementar

Cenários

Se você quiser excluir uma interface de rede suplementar com um EIP vinculado, primeiro será necessário desvincular o EIP da interface.

Para desvincular um EIP, você pode consultar **Vinculação ou desvinculação de uma interface de rede suplementar de ou para um EIP**.

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, em **Rede**, clique em **Virtual Private Cloud**.

   A página **Virtual Private Cloud** é exibida.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Network Interfaces**.
5. Na página **Network Interfaces**, clique na guia **Supplementary Network Interfaces**.
6. Localize a linha que contém a interface de rede suplementar e clique em **Delete** na coluna **Operation**.
7. Clique em **Yes** na caixa de diálogo exibida.

   A exclusão de uma interface de rede suplementar também excluirá as subinterfaces VLAN configuradas no ECS.

8 Elastic IP

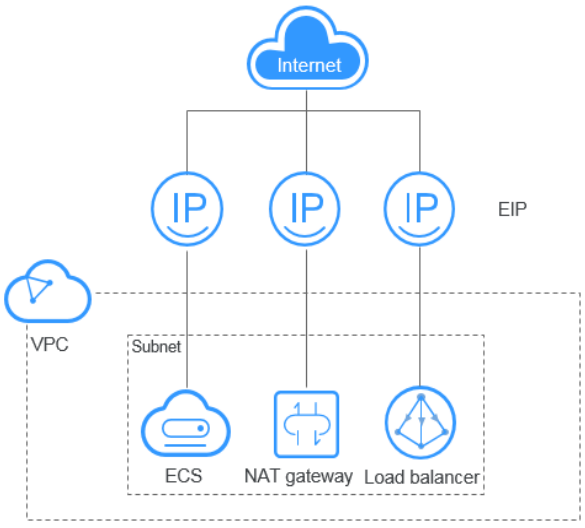
8.1 Visão geral do EIP

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 8-1 Acessar a Internet usando um EIP



Vantagens

- Flexibilidade

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

- Pagamento flexível

  Os EIPs estão disponíveis com base em pagamento por uso (uso da largura de banda ou a quantidade de tráfego faturada). O modo de cobrança anual/mensal é mais preferencial.

- 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

Se você quiser enviar um tíquete de serviço, consulte **Envio de um tíquete de serviço**.

8.2 Atribuição de um EIP e vinculação dele a um ECS

Cenários

You can assign an EIP and bind it to an ECS so that the ECS can access the Internet.

Atribuir um EIP

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, em **Rede**, clique em **Elastic IP**.
4. Na página exibida, clique em **Buy EIP**.
5. Defina os parâmetros conforme solicitados.

Tabela 8-1 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Billing Mode	Os seguintes modos de cobrança estão disponíveis: ● Yearly/Monthly ● Pay-per-use	Pay-per-use

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). Para obter detalhes, consulte **Quais são as diferenças entre BGP estático e BGP dinâmico?**	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
Enterprise Project	O projeto empresarial ao qual o EIP 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**.	default
Advanced Settings	Clique na seta suspensa para configurar parâmetros, incluindo o nome da largura de banda e a tag.	-
Bandwidth Name	O nome da largura de banda.	bandwidth
Tag	As tags de EIP. Cada tag contém um par de chave e valor.	● Chave: Ipv4_key1 ● Valor: 3005eip

Parâmetro	Descrição	Exemplo de valor
Monitoring	Usado para monitorar o EIP e ativado 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 8-2 Requisitos da tag do EIP

Parâmetro	Requisito	Exemplo de valor
Key	● Não pode ser deixado 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 hifens (-).	3005eip

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**.

NOTA

Um EIP e seu recurso de nuvem vinculado podem usar diferentes modos de cobrança.

8.3 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 o liberar, o EIP continuará a ser cobrado e o preço incluirá 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. 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, em **Rede**, 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. 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, em **Rede**, 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. 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, em **Rede**, clique em **Elastic IP**.
4. Na página exibida, selecione os EIPs a serem desvinculados.
5. Clique no botão **Unbind** localizado acima da lista do EIP.
6. Clique em **Yes** na caixa de diálogo exibida.

Liberação de vários EIPs de uma só vez

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, em **Rede**, clique em **Elastic IP**.
4. Na página exibida, selecione os EIPs a serem liberados.
5. Clique no botão **Release** localizado acima da lista do EIP.
6. Clique em **Yes** na caixa de diálogo exibida.

8.4 Modificação de uma largura de banda do EIP

Cenários

Não importa qual modo de cobrança seja usado, se o seu EIP não for adicionado a uma largura de banda compartilhada, ele usará uma largura de banda dedicada.

Esta seção descreve como aumentar ou diminuir uma largura de banda dedicada.

Quando você altera o tamanho da largura de banda, o preço da largura de banda e o tempo efetivo dependem do modo de cobrança, que se aplica a larguras de banda dedicadas e compartilhadas. Para obter detalhes, consulte **Tabela 8-3**.

NOTA

A diminuição das larguras de banda pode causar perda de pacotes.

Tabela 8-3 Impacto na cobrança após a alteração do tamanho da largura de banda

Modo de cobrança	Cobrado por	Alteração	Impacto
Anual/ Mensal	Largura de banda	Aumentar a largura de banda	A alteração entrará em vigor imediatamente. O aumento da largura de banda será cobrado de acordo.
	Largura de banda	Diminuir a largura de banda após a renovação	A alteração não entrará em vigor imediatamente. Você precisa selecionar um novo tamanho de largura de banda e uma duração de renovação. A alteração entrará em vigor no primeiro ciclo de cobrança após uma renovação bem-sucedida. ● O pedido pode ser cancelado antes que a largura de banda entre em vigor. ● A largura de banda não pode ser modificada no primeiro ciclo de cobrança.
Pagamento por uso	Largura de banda	Aumentar ou diminuir a largura de banda	A alteração entrará em vigor imediatamente.
	Tráfego	Aumentar ou diminuir a largura de banda	A alteração entrará em vigor imediatamente. O tamanho da largura de banda que você define é usado apenas para limitar a taxa máxima de transferência de dados.

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, em **Rede**, clique em **Elastic IP**.
4. Localize a linha que contém o EIP de destino na lista do EIP, clique em **More** na coluna **Operation** e selecione **Modify Bandwidth**.
5. Modifique os parâmetros de largura de banda conforme solicitado.

Figura 8-2 Modificação da largura de banda de um EIP do pagamento por uso

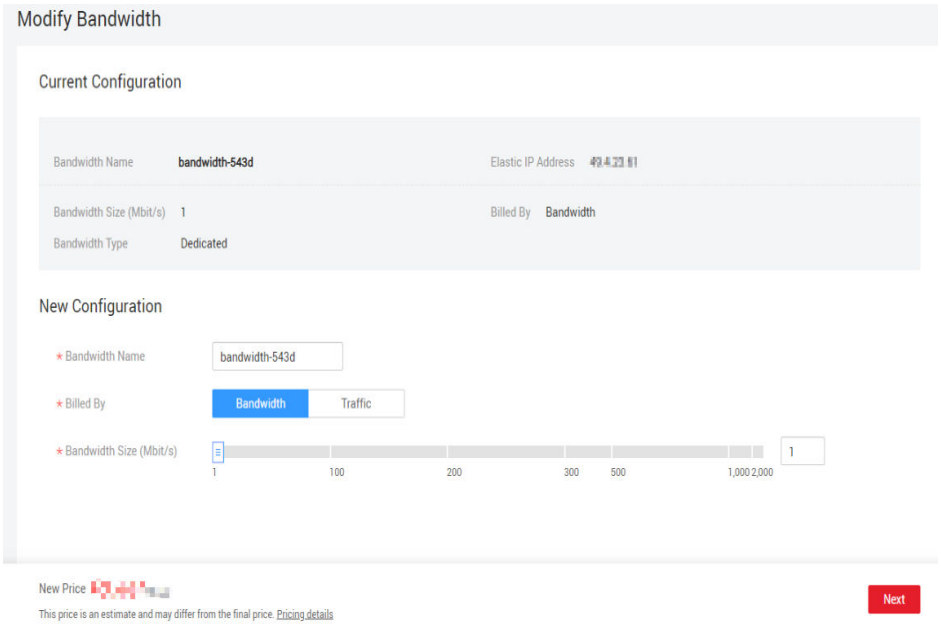
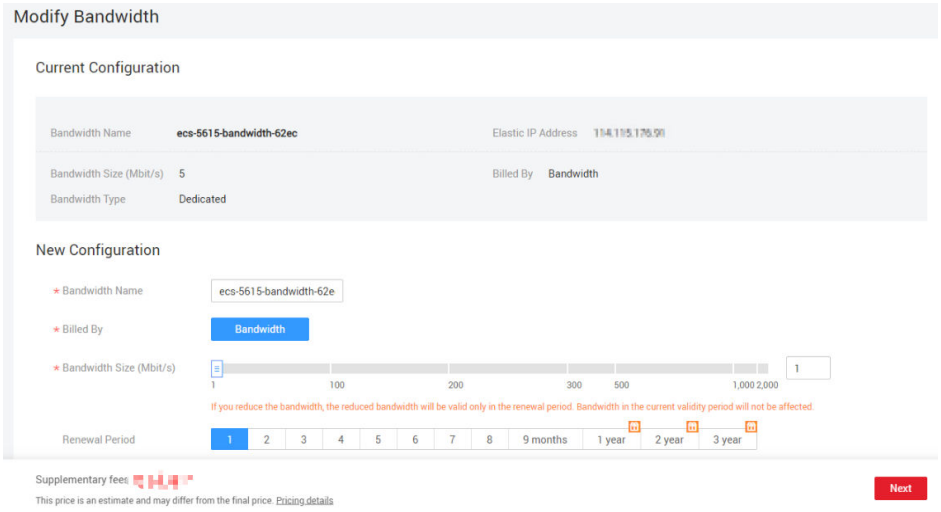


Figura 8-3 Modificação da largura de banda mensal/anual



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

Links úteis

- **Como alterar a opção de cobrança do EIP de largura de banda para tráfego ou de tráfego para largura de banda?**
- **O que são largura de banda de entrada e largura de banda de saída?**
- **Posso aumentar minha largura de banda cobrada anualmente/mensalmente e depois diminuí-la?**

8.5 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 8-4** lista os requisitos de chave e valor da tag.

Tabela 8-4 Requisitos da tag do EIP

Parâmetro	Requisito	Exemplo de valor
Key	● Não pode ser deixado 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 hifens (-).	3005eip

Procedimento

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

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, em **Rede**, clique em **Elastic IP**.
4. Clique na caixa de pesquisa e, em seguida, clique em **Tag** na lista suspensa.
5. Selecione a chave e o valor de tag do EIP.

   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.
6. Clique em **OK**.

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

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

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, em **Rede**, 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.
   - Visualizar as tags.

     Na guia **Tags**, você pode visualizar 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 você deseja editar e clique em **Edit** na coluna **Operation**. Insira o novo valor de tag e clique em **OK**.

     A chave de tag não pode ser modificada.
   - Excluir uma tag.

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

8.6 EIP IPv6

Visão geral

Ambos os EIPs IPv4 e IPv6 estão disponíveis. Você pode atribuir um EIP IPv6 ou mapear um EIP IPv4 existente para um EIP IPv6.

Depois que a função de EIP IPv6 estiver ativada, você obterá um EIP IPv4 e seu EIP IPv6 correspondente. Endereços IPv6 externos podem acessar recursos de nuvem por meio desse EIP IPv6.

EIPs IPv4 são cobrados. Atualmente, os EIPs IPv6 são gratuitos, mas serão cobrados posteriormente (preço ainda a ser determinado).

Cenários de aplicação de pilha dupla IPv4/IPv6

Se o seu ECS for compatível com IPv6, você poderá usar a pilha dupla IPv4/IPv6. **Tabela 8-5** mostra os cenários de aplicação de exemplo.

Tabela 8-5 Cenários de aplicação de pilha dupla IPv4/IPv6

Cenário de aplicação	Descrição	Requisito	Sub-rede IPv4 ou IPv6	ECS
Comunicação IPv4 privada	Suas aplicações em ECSs precisam se comunicar com outros sistemas (como bancos de dados) por meio de redes privadas usando endereços IPv4.	● O IPv6 não está habilitado para a sub-rede de VPC. ● Nenhum EIP foi vinculado aos ECSs.	Bloco CIDR IPv4	**Endereço IPv4 privado**: usado para comunicação IPv4 privada.
Comunicação IPv4 pública	Suas aplicações em ECSs precisam se comunicar com outros sistemas (como bancos de dados) por meio de endereços IPv4 públicos.	● O IPv6 não está habilitado para a sub-rede de VPC. ● Os EIPs foram vinculados aos ECSs.	Bloco CIDR IPv4	● **Endereço IPv4 privado**: usado para comunicação IPv4 privada. ● **Endereço IPv4 público**: usado para comunicação IPv4 pública.

Cenário de aplicação	Descrição	Requisito	Sub-rede IPv4 ou IPv6	ECS
Comunicação IPv6 privada	Suas aplicações em ECSs precisam se comunicar com outros sistemas (como bancos de dados) por meio de endereços IPv6 privados.	• O IPv6 foi habilitado para a sub-rede de VPC. • A rede foi configurada para os ECSs da seguinte forma: – **Flavor**: qualquer flavor de ECS que ofereça suporte à rede IPv6. Para obter detalhes sobre o flavor de ECS compatível com a rede IPv6, consulte a seção "Especificações e tipos de ECS x86" no **Guia de usuário do Elastic Cloud Server**. – **VPC and Subnet**: sub-rede habilitada para IPv6 e VPC. – **Self-assigned IPv6 address**: selecionado. – **Shared Bandwidth**: selecione **Do not configure**.	• Bloco CIDR IPv4 • Bloco CIDR IPv6	• **Endereço IPv4 privado + EIP IPv4**: vincule um EIP IPv4 à instância para permitir a comunicação IPv4 pública. • **Endereço IPv4 privado**: não vincule nenhum EIP IPv4 à instância e use apenas o endereço IPv4 privado para permitir a comunicação IPv4 privada. • **Endereço IPv6**: não configure a largura de banda compartilhada para o endereço IPv6 para permitir a comunicação IPv6 privada.

Cenário de aplicação	Descrição	Requisito	Sub-rede IPv4 ou IPv6	ECS
Comunicação IPv6 pública	Uma rede IPv6 é necessária para que o ECS acesse o serviço IPv6 na Internet.	• O IPv6 foi habilitado para a sub-rede de VPC. • A rede foi configurada para os ECSs da seguinte forma: – **Flavor**: qualquer flavor de ECS que ofereça suporte à rede IPv6. Para obter detalhes sobre o flavor de ECS compatível com a rede IPv6, consulte a seção "Especificações e tipos de ECS x86" no **Guia de usuário do Elastic Cloud Server**. – **VPC and Subnet**: sub-rede habilitada para IPv6 e VPC. – **Self-assigned IPv6 address**: selecionado. – **Shared Bandwidth**: selecione uma largura de banda compartilhada. **NOTA** Para obter detalhes, consulte **Configuração de uma rede IPv6**.	• Bloco CIDR IPv4 • Bloco CIDR IPv6	• **Endereço IPv4 privado + EIP IPv4**: vincule um EIP IPv4 à instância para permitir a comunicação IPv4 pública. • **Endereço IPv4 privado**: não vincule nenhum EIP IPv4 à instância e use apenas o endereço IPv4 privado para permitir a comunicação IPv4 privada. • **Endereço IPv6 + largura de banda compartilhada**: permita comunicação IPv6 privada e comunicação IPv6 pública.

Para obter detalhes, consulte **Rede de pilha dupla IPv4 e IPv6**.

Cenários de aplicação de EIP IPv6

Se você deseja que um ECS forneça serviços IPv6, mas o ECS não oferece suporte a redes IPv6 ou não deseja criar uma rede IPv6, pode usar o EIP IPv6 para atender rapidamente às

suas necessidades. Para obter detalhes sobre cenários de aplicações e planejamento de recursos, consulte **Tabela 8-6**.

Tabela 8-6 Cenários de aplicações e planejamento de recursos de um EIP de rede IPv6 (com EIP IPv6 habilitado)

Cenário de aplicação	Descrição	Requisito	Sub-rede IPv4 ou IPv6	ECS
Comunicação IPv6 pública	Você deseja permitir que um ECS forneça serviços IPv6 para clientes na Internet sem configurar uma rede IPv6.	• Um EIP foi vinculado ao ECS. • O EIP IPv6 foi habilitado.	Bloco CIDR IPv4	• **Endereço IPv4 privado**: usado para comunicação IPv4 privada. • **EIP IPv4 (com EIP IPv6 ativado)**: usado para comunicação de rede pública através de endereços IPv4 e IPv6.

Cenários de aplicações e planejamento de recursos de redes IPv6

Figura 8-4 Cenários de aplicações e planejamento de recursos de redes IPv6

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 dele 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.

- Método 2:

  Se desejar um EIP IPv6 além de um EIP IPv4 existente, localize a linha que contém o EIP IPv4 de destino, clique em **More** na coluna **Operation** e selecione **Enable IPv6 EIP**. Em seguida, um correspondente EIP IPv6 será atribuído.

  Depois que o EIP IPv6 estiver habilitado, você obterá um EIP IPv4 e um EIP IPv6. Endereços IPv6 externos podem acessar recursos de nuvem por meio desse EIP IPv6.

NOTA

Não há impacto adverso nos recursos de nuvem vinculados aos EIPs IPv4 existentes.

Configuração de grupos de segurança

Depois que o EIP IPv6 estiver habilitado, adicione regras de grupo de segurança de entrada e saída para permitir pacotes de e para o intervalo de endereços IP **198.19.0.0/16**. **Tabela 8-7** mostra as regras do grupo de segurança. O EIP IPv6 usa o NAT64 para converter o endereço IP de origem na direção de entrada em um endereço IPv4 no intervalo de endereços IP 198.19.0.0/16. A porta de origem pode ser aleatória, o endereço IP de destino é o endereço IPv4 privado do seu servidor local e a porta de destino permanece inalterada.

Para obter detalhes, consulte **Guia de usuário da Virtual Private Cloud**.

Tabela 8-7 Regras de grupos de segurança

Direção	Protocolo	Origem ou destino
Entrada	Todos	Origem: 198.19.0.0/16
Saída	Todos	Destino: 198.19.0.0/16

Desativação do EIP IPv6

Se você não precisar do EIP IPv6, localize a linha que contém o EIP IPv4 correspondente, clique em **More** na coluna **Operation** e selecione **Disable IPv6 EIP**. Em seguida, o EIP IPv6 será liberado. Você terá apenas o EIP IPv4.

9 Largura de banda compartilhada

9.1 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.

NOTA

- 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.

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 pagamento por uso (exceto EIPs **5_gray** de balanceadores de carga dedicados) a uma largura de banda compartilhada ou removê-los, independentemente do tipo de instâncias às quais eles estão vinculados.

- Modos de cobrança flexíveis

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

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 você quiser aumentar uma largura de banda compartilhada paga por uso maior que 1 Gbit/s, o aumento mínimo é de 500 Mbit/s.
- 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.
- Antes de excluir uma largura de banda compartilhada, remova os EIPs da largura de banda compartilhada primeiro, se houver.
- 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.
- Se você quiser enviar um tíquete de serviço, consulte **Envio de um tíquete de serviço**.

9.2 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. 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, em **Rede**, 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 9-1 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Billing Mode	Uma largura de banda compartilhada pode ser faturada em uma base anual/mensal ou pagamento por uso. ● **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 especificar uma largura de banda compartilhada a ser cobrada 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 empresarial facilita o gerenciamento de projeto e o agrupamento de recursos da nuvem e de usuários. O nome do projeto padrão é **default**.	default
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**.

9.3 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.
- Se for uma largura de banda compartilhada padrão, você pode adicionar EIPs de BGP dinâmicos e NICs de IPv6 a ela. Se for uma largura de banda compartilhada premium, você pode adicionar EIPs de BGP premium e NICs de IPv6 a ela.

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, em **Rede**, 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 Public IP Address** e selecione os EIPs a serem adicionados.
6. Clique em **OK**.

Links úteis

Quais são as diferenças entre uma largura de banda dedicada e uma largura de banda compartilhada? Uma largura de banda dedicada pode ser alterada para uma largura de banda compartilhada ou o contrário?

9.4 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. 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, em **Rede**, 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**.

9.5 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 **Modificação de uma 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.

Se você quiser alterar o modo de cobrança de uma largura de banda compartilhada, consulte **Como alterar o modo de cobrança do meu EIP de pagamento por uso para anual/mensal?**

Modificação de uma largura de banda compartilhada (pagamento por uso)

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, em **Rede**, 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 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.

Aumento de uma largura de banda compartilhada (anual/mensal)

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, em **Rede**, 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.

Diminuição de uma largura de banda compartilhada (anual/mensal)

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, em **Rede**, 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.

9.6 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. Só pode ser cancelada.
- Se você quiser excluir uma largura de banda compartilhada com EIPs adicionados, você tem que remover os EIPs da largura de banda compartilhada primeiro.

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. 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, em **Rede**, 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**.

10 Pacote de dados compartilhados

10.1 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

- Pacotes de dados compartilhados exigem um pagamento único e entram em vigor imediatamente após a compra. Não é possível especificar a data de efetivação.
- Pacotes de dados compartilhados não podem ser cancelados uma vez comprados e não podem ser renovados após a expiração.
- Pacotes de dados compartilhados são cobrados por mês ou ano. Uma vez expirada, a cota de pacote restante não pode mais ser usada.
- Pacotes de dados compartilhados só podem ser usados pela largura de banda de pagamento por uso cobrada pelo tráfego. Dois tipos de pacotes de dados compartilhados estão disponíveis: BGP estático (para largura de banda de BGP estático) e BGP dinâmico (para largura de banda de BGP dinâmico).

- Um pacote de dados compartilhado não pode ser usado para a largura de banda de um EIP específico.
- Um pacote de dados compartilhado não pode ser usado para uma largura de banda compartilhada.
- Um pacote de dados compartilhado não pode ser usado por EIPs do tipo de BGP premium.
- Se você tem um pedido que não foi pago dentro do prazo de pagamento, você precisa cancelar ou pagar o pedido primeiro. Em seguida, você pode comprar um pacote de dados compartilhado.

10.2 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

- Pacotes de dados compartilhados exigem um pagamento único e entram em vigor imediatamente após a compra. Não é possível especificar a data de efetivação.
- Pacotes de dados compartilhados não podem ser cancelados uma vez comprados e não podem ser renovados após a expiração.
- Pacotes de dados compartilhados são cobrados por mês ou ano. Uma vez expirada, a cota de pacote restante não pode mais ser usada.
- Pacotes de dados compartilhados só podem ser usados pela largura de banda de pagamento por uso cobrada pelo tráfego. Dois tipos de pacotes de dados compartilhados estão disponíveis: BGP estático (para largura de banda de BGP estático) e BGP dinâmico (para largura de banda de BGP dinâmico).
- Um pacote de dados compartilhado não pode ser usado para a largura de banda de um EIP específico.
- Um pacote de dados compartilhado não pode ser usado para uma largura de banda compartilhada.
- Um pacote de dados compartilhado não pode ser usado por EIPs do tipo de BGP premium.
- Se você tem um pedido que não foi pago dentro do prazo de pagamento, você precisa cancelar ou pagar o pedido primeiro. Em seguida, você pode comprar um pacote de dados compartilhado.

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, em **Rede**, 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 10-1 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
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: ● Dynamic BGP: 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. ● Static BGP: 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.	Static BGP
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
Duração de uso	O período de validade do pacote de dados compartilhados.	Padrão

6. Clique em **Next**.

11 Tabelas de rotas

11.1 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, 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.
- Ao criar uma conexão da 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**.

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: essas 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.

  – O destino da rota de 100.64.0.0/10 ou 198.19.128.0/20 é usado por serviços de rede, como DNS e VPCEP na nuvem.

  – O destino da rota de 127.0.0.0/8 é o endereço de loopback local.

  – A rota com destino de um bloco CIDR de sub-rede é usada para comunicação entre sub-redes em uma VPC.

- Rotas personalizadas: 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 11-1** 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 próximos tipos de salto sejam diferentes, porque o destino determina a prioridade da rota. 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 11-1 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 rota padrão ● Tabela de rota personalizada
Gateway de VPN	O tráfego destinado ao destino é encaminhado para um gateway de VPN.	Tabela de rota personalizada

Tipo de próximo salto	Descrição	Tabela de rotas suportadas
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 rota padrão ● Tabela de rota personalizada
Gateway de NAT	O tráfego destinado ao destino é encaminhado para um gateway de NAT.	● Tabela de rota 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 rota 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 rota padrão ● Tabela de rota personalizada
Ponto de extremidade da VPC	O tráfego destinado ao destino é encaminhado para um ponto de extremidade da VPC.	● Tabela de rota padrão ● Tabela de rota personalizada
Contêiner em nuvem	O tráfego endereçado ao destino é encaminhado para um contêiner em nuvem.	● Tabela de rota padrão ● Tabela de rota personalizada
Roteador empresarial	O tráfego endereçado ao destino é encaminhado para um roteador empresarial.	● Tabela de rota padrão ● Tabela de rota personalizada
Firewall em nuvem	O tráfego endereçado ao destino é encaminhado para um firewall em nuvem.	● Tabela de rota padrão ● Tabela de rota personalizada

NOTA

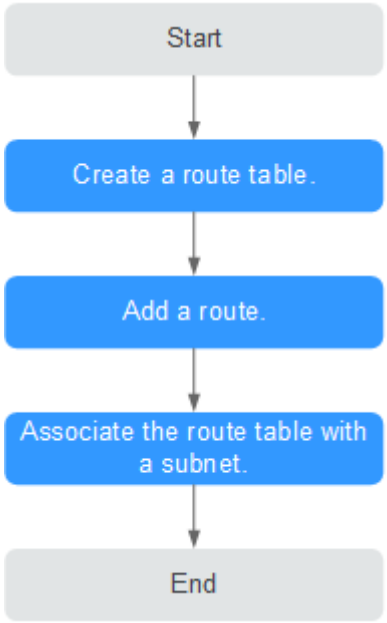
Se você especificar o destino ao criar um recurso, uma rota do sistema será entregue. Se você não especificar um destino ao criar um recurso, uma rota personalizada que pode ser modificada ou excluída será entregue.

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 por padrão). Nesse caso, você pode alterar o destino. No entanto, quando você cria um gateway de VPN, 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 11-1 mostra o processo de criação e configuração de uma tabela de rotas personalizada.

Figura 11-1 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.

11.2 Criação de uma tabela de rota personalizada

Cenários

Se sua tabela de rotas padrão não puder atender aos requisitos de serviço, você poderá criar uma tabela de rotas personalizada seguindo as instruções fornecidas nesta seção.

Observações e restrições

- Cada VPC pode ter no máximo 10 tabelas de rotas, incluindo a tabela de rota padrão.
- Quando você cria uma VPC, 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**.

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, em **Rede**, clique em **Virtual Private Cloud**.
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 11-2 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**.

11.3 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.

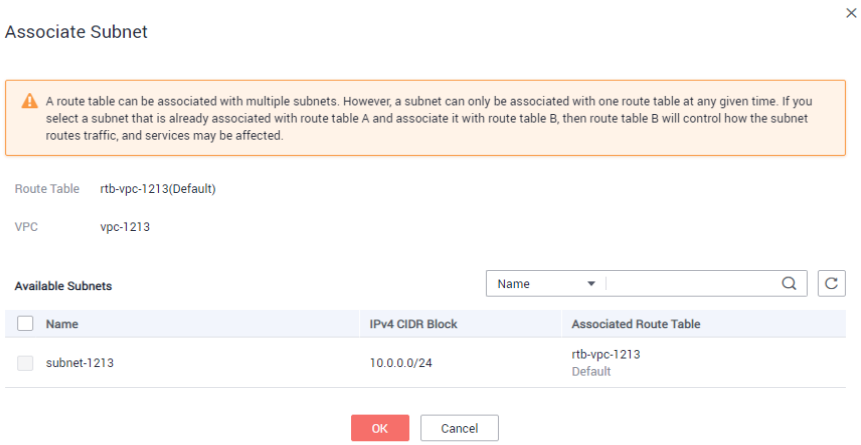
Observações e restrições

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

Procedimento

1. 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, em **Rede**, clique em **Virtual Private Cloud**.
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 11-2 Associar sub-rede



7. Clique em **OK**.

11.4 Alteração da 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. 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, em **Rede**, clique em **Virtual Private Cloud**.
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.

11.5 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.

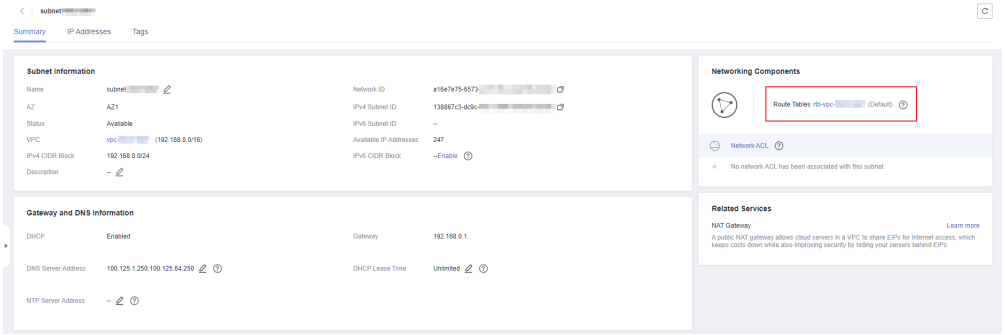
Procedimento

1. 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, em **Rede**, clique em **Virtual Private Cloud**.
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.

   Figura 11-3 Exibição da 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.

11.6 Exibição de informações da 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. 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, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Route Tables**.
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.

11.7 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. 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, em **Rede**, clique em **Virtual Private Cloud**.
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.

11.8 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.

  No entanto, a exclusão de uma VPC também excluirá sua tabela de rotas padrão. Ambas as tabelas de rotas padrão e personalizadas são gratuitas.
- Uma tabela de rotas personalizada com uma sub-rede associada não pode ser excluída diretamente.

  Se você quiser excluir essa tabela de rotas, poderá associar a sub-rede a outra tabela de rotas primeiro consultando a **Alteração da tabela de rota associada a uma sub-rede**.

Procedimento

1. Faça logon no console de gerenciamento.
1. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
2. Na página inicial do console, em **Rede**, clique em **Virtual Private Cloud**.
3. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Route Tables**.
4. 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.

5. Clique em **Yes**.

11.9 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 também pode adicionar rotas personalizadas conforme necessário para encaminhar o tráfego destinado ao destino para o próximo salto especificado.

Observações e restrições

Um máximo de 200 rotas podem ser adicionadas a cada tabela de rotas.

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, em **Rede**, clique em **Virtual Private Cloud**.
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.

Tabela 11-3 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Destination Type	Obrigatório O destino pode ser: ● IP address: endereço IP único ou intervalo de endereços IP ● IP address group: selecione um grupo de endereços IP que contenha um ou mais endereços IP.	IP address

Parâmetro	Descrição	Exemplo de valor
Destination	Obrigatório Insira o destino da rota. ● Se **Destination Type** estiver definido como **IP address**, insira um único endereço IP ou um intervalo de endereços IP na notação CIDR. ● Se **Destination Type** estiver definido como **IP address group**, selecione um grupo de endereços IP que contenha um ou mais endereços IP. **AVISO** ● O destino de cada rota em uma tabela de rotas deve ser exclusivo. ● Se um grupo de endereços IP contiver um intervalo de endereços IP no formato *Endereço IP inicial-Endereço IP final*, o grupo de endereços IP não é suportado. Por exemplo, um grupo de endereços IP não pode conter 192.168.0.1-192.168.0.62. Você precisa alterar 192.168.0.1-192.168.0.62 para 192.168.0.0/26.	192.168.0.0/24
Next Hop Type	Obrigatório Defina o tipo do próximo salto. Para obter detalhes sobre os tipos de recursos suportados, consulte **Tabela 11-1**. **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**.	VPC peering connection
Next Hop	Obrigatório Defina o próximo salto. Os recursos na caixa de listagem suspensa são exibidos com base no tipo de próximo salto selecionado.	peer-AB
Description	Opcional Insira a descrição da rota na caixa de texto, conforme necessário.	-

7. Clique em **OK**.

11.10 Modificação de uma rota

Cenários

Esta seção descreve como modificar uma rota personalizada numa tabela de rotas.

Observações e restrições

- As rotas do sistema não podem ser modificadas.
- Ao criar uma conexão da VPN, Cloud Connect ou Direct Connect, a tabela de rotas padrão fornece automaticamente uma rota que não pode ser excluída ou modificada.
- Rotas com o tipo de próximo salto de contêiner de nuvem não podem ser modificadas ou excluídas.
- As rotas com o tipo de próximo salto do ponto de extremidade da VPC não podem ser modificadas ou excluídas.

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, em **Rede**, clique em **Virtual Private Cloud**.
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 11-4 Descrições de parâmetro

Parâmetro	Descrição	Exemplo de valor
Destination Type	Obrigatório O destino pode ser: ● IP address: endereço IP único ou intervalo de endereços IP ● IP address group: selecione um grupo de endereços IP que contenha um ou mais endereços IP.	IP address

Parâmetro	Descrição	Exemplo de valor
Destination	Obrigatório Insira o destino da rota. ● Se **Destination Type** estiver definido como **IP address**, insira um único endereço IP ou um intervalo de endereços IP na notação CIDR. ● Se **Destination Type** estiver definido como **IP address group**, selecione um grupo de endereços IP que contenha um ou mais endereços IP. **AVISO** ● O destino de cada rota em uma tabela de rotas deve ser exclusivo. ● Se um grupo de endereços IP contiver um intervalo de endereços IP no formato *Endereço IP inicial-Endereço IP final*, o grupo de endereços IP não é suportado. Por exemplo, um grupo de endereços IP não pode conter 192.168.0.1-192.168.0.62. Você precisa alterar 192.168.0.1-192.168.0.62 para 192.168.0.0/26.	192.168.0.0/24
Next Hop Type	Obrigatório Defina o tipo do próximo salto. Para obter detalhes sobre os tipos de recursos suportados, consulte **Tabela 11-1**. **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**.	VPC peering connection
Next Hop	Obrigatório Defina o próximo salto. Os recursos na caixa de listagem suspensa são exibidos com base no tipo de próximo salto selecionado.	peer-AB
Description	Opcional Insira a descrição da rota na caixa de texto, conforme necessário.	-

8. Clique em **OK**.

11.11 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 11-5 mostra se rotas de tipos diferentes podem ser replicadas para tabelas de rotas padrão ou personalizadas.

Por exemplo, se o próximo salto de uma rota for um servidor, essa rota poderá ser replicada para ambas 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 11-5 Replicação de rotas

Tipo de próximo salto	Pode ser replicado para a tabela de rota padrão	Pode ser replicado para tabela de rota personalizada
Local	Não	Não
Server	Sim	Sim
Extension NIC	Sim	Sim
BMS user-defined network	Não	Sim
VPN gateway	Não	Sim
Direct Connect gateway	Não	Sim
Cloud connection	Não	Sim
Supplementary network interface	Sim	Sim
NAT gateway	Sim	Sim
VPC peering connection	Sim	Sim
Virtual IP address	Sim	Sim
VPC endpoint	Não	Não
Cloud container	Não	Não
Enterprise router	Sim	Sim
Cloud firewall	Sim	Sim

NOTA

- Se o serviço Direct Connect estiver ativado por chamada ou e-mail, as rotas entregues à tabela de rotas padrão não poderão ser replicadas para uma tabela de rotas personalizada.

Procedimento

1. Faça logon no console de gerenciamento.

1. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
2. Na página inicial do console, em **Rede**, clique em **Virtual Private Cloud**.
3. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Route Tables**.
4. Na lista da tabela de rotas, localize a linha que contém a tabela de rotas da qual você deseja replicar rotas e clique em **Replicate Route** na coluna **Operation**.
5. Selecione a tabela de rotas de destino para a qual você deseja replicar a rota e as rotas a serem replicadas conforme solicitado.

   As rotas listadas 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.
6. Clique em **OK**.

11.12 Exclusão de uma rota

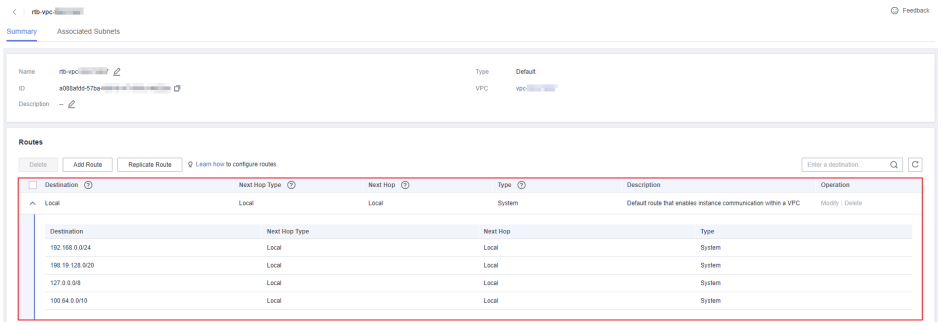
Cenários

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

Observações e restrições

- As rotas do sistema não podem ser excluídas.

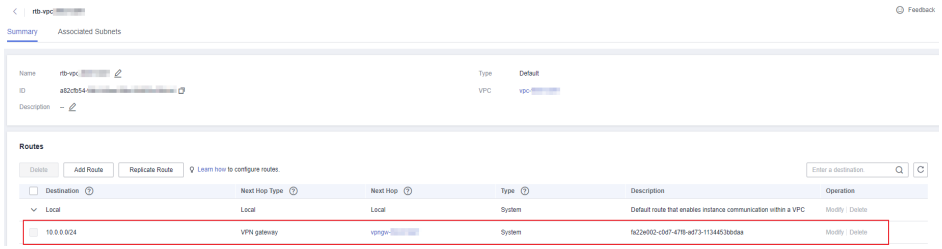
  Figura 11-4 Rotas do sistema



- As rotas entregues automaticamente por VPN, Cloud Connect, ou Cloud Connect para a tabela de rotas padrão não podem ser excluídas. Os próximos tipos de salto de tais rotas são:
  - VPN gateway
  - Direct Connect gateway
  - 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 11-5 Rota entregue por VPN



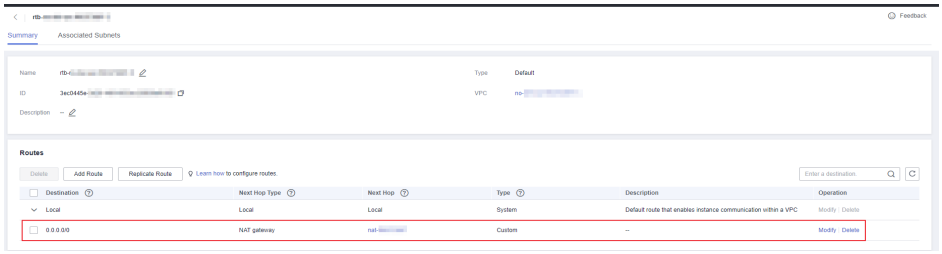
- Rotas com o tipo de próximo salto de contêiner de nuvem não podem ser modificadas ou excluídas.
- As rotas com o tipo de próximo salto do ponto de extremidade da VPC não podem ser modificadas ou excluídas.

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, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Route Tables**.
5. Localize a tabela de rotas de destino e clique em seu nome.

   A página de detalhes da tabela de rotas é exibida.

Figura 11-6 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**.

11.13 Configuração de um servidor SNAT

Scenarios

Together with VPC route tables, you can configure SNAT on an ECS to enable other ECSs that have no EIPs bound in the same VPC to access the Internet through this ECS.

The configured SNAT takes effect for all subnets in a VPC.

Prerequisites

- You have an ECS where SNAT is to be configured.
- The ECS where SNAT is to be configured runs Linux.
- The ECS where SNAT is to be configured has only one network interface card (NIC).

Differences Between SNAT ECSs and NAT Gateways

The NAT Gateway service provides network address translation (NAT) for servers, such as ECSs, BMSs and Workspace desktops, in a VPC or servers from an on-premises data center that connects to a VPC through Direct Connect or VPN. A NAT gateway allows these servers to share an EIP to access the Internet or provide services accessible from the Internet.

The NAT Gateway service is easier to configure and use than SNAT. This service can be flexibly deployed across subnets and AZs and has different NAT gateway specifications. You can click **NAT Gateway** under **Rede** on the management console to try this service.

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, 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 dele 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 de resposta iptables no ECS em que a SNAT está configurada e configurar 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 support.huawei.com
PING www.XXX.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 de 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:

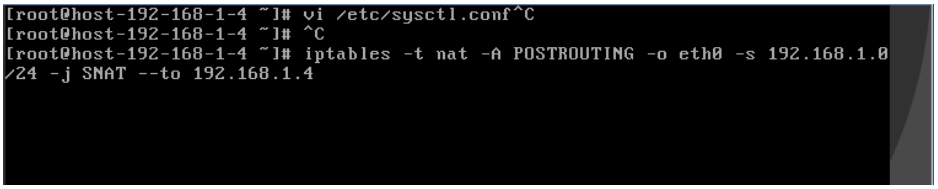
    sysctl -p /etc/sysctl.conf

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 11-7 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

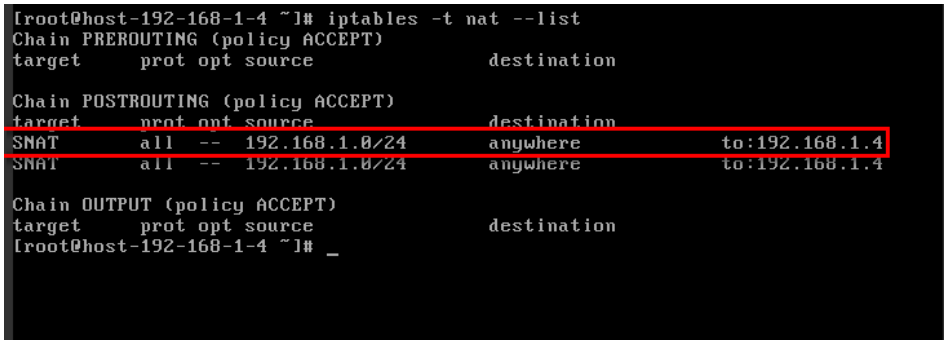
4. Adicione as permissões de execução para o arquivo **rc.local**:

   # chmod +x /etc/rc.local

15. Verifique se a configuração foi bem-sucedida. Se informações semelhantes a **Figura 11-8** (por exemplo, 192.168.1.0/24) forem exibidas, a configuração foi bem-sucedida.

    iptables -t nat --list

Figura 11-8 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 implementada. 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 ACLs da rede para ver se o tráfego necessário é permitido.

12 Conexão de emparelhamento de VPC

12.1 Visão geral da conexão de emparelhamento de VPC

O que é uma conexão de emparelhamento de VPC?

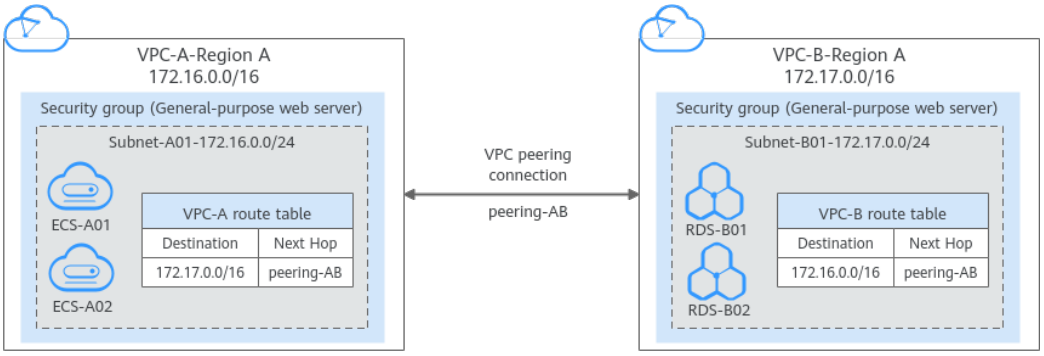
Uma conexão de emparelhamento de VPC é uma conexão de rede entre duas VPCs e permite que elas se comuniquem usando endereços IP privados. As VPCs a serem emparelhadas podem estar na mesma conta ou em contas diferentes, mas devem estar na mesma região.

- Se você quiser conectar VPCs em regiões diferentes, use **Cloud Connect**.
- Você pode usar conexões de emparelhamento de VPC para criar redes diferentes. Para obter detalhes, consulte **Exemplos de uso de conexão de emparelhamento de VPC**.

Figura 12-1 mostra um cenário de aplicação de conexões de emparelhamento de VPC.

- Há duas VPCs (VPC-A e VPC-B) na região A que não são conectados.
- Os servidores de serviço (ECS-A01 e ECS-A02) estão no VPC-A e os servidores de banco de dados (RDS-B01 e RDS-B02) estão no VPC-B. Os servidores de serviço e os servidores de banco de dados não podem se comunicar uns com os outros.
- Você precisa criar uma conexão de emparelhamento de VPC (emparelhamento-AB) entre a VPC-A e a VPC-B para que os servidores de serviço e os servidores de banco de dados possam se comunicar uns com os outros.

Figura 12-1 Diagrama de rede de conexão de emparelhamento de VPC



AVISO

Atualmente, as conexões de emparelhamento de VPC são gratuitas.

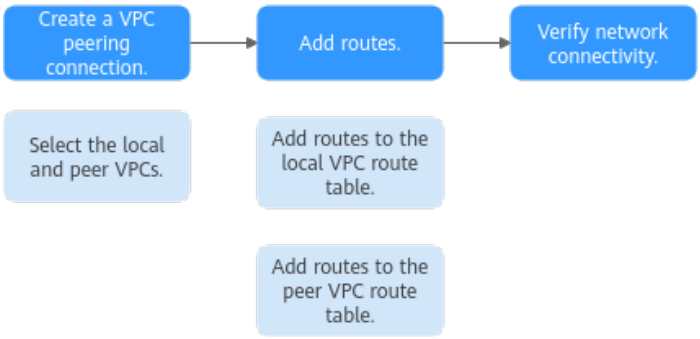
Processo de criação de conexão de emparelhamento de VPC

Uma conexão de emparelhamento de VPC só pode conectar VPCs na mesma região.

- Se duas VPCs estiverem na mesma conta, o processo de criação de uma conexão de emparelhamento de VPC será mostrado em **Figura 12-2**.

  Para obter detalhes sobre como criar uma conexão de emparelhamento de VPC, consulte **Criação de uma conexão de emparelhamento de VPC com uma outra VPC na sua conta.**.

  Figura 12-2 Processo de criação de uma conexão de emparelhamento de VPC entre VPCs na mesma conta

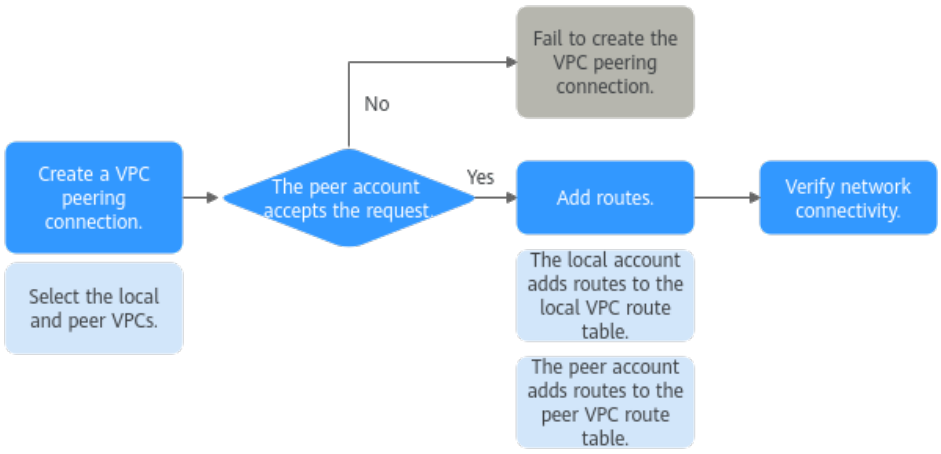
  

- Se duas VPCs estiverem em contas diferentes, o processo de criação de uma conexão de emparelhamento de VPC será mostrado em **Figura 12-3**.

  Para obter detalhes sobre como criar uma conexão de emparelhamento de VPC, consulte **Criação de uma conexão de emparelhamento de VPC com uma VPC em outra conta**.

  Se a conta A iniciar uma solicitação para criar uma conexão de emparelhamento da VPC com uma VPC na conta B, a conexão de emparelhamento da VPC entrará em vigor somente depois que a conta B aceitar a solicitação.

  Figura 12-3 Processo de criação de uma conexão de emparelhamento de VPC entre VPCs em contas diferentes

Observações e restrições

- Uma conexão de emparelhamento de VPC só pode conectar VPCs na mesma região.
  - Se você quiser conectar VPCs em regiões diferentes, use **Cloud Connect**.
  - Se você precisar de apenas alguns ECSs em regiões diferentes para se comunicar, poderá **atribuir e vincular EIPs aos ECSs**.
- Se as VPCs locais e de par tiverem blocos CIDR sobrepostos, a conexão de emparelhamento da VPC pode não ter efeito.

  Neste caso, você pode consultar **exemplos de configuração de rede**.
- Uma conexão de emparelhamento de VPC pode permitir que uma VPC criada no site da Huawei Cloud da China continental e outra criada no site da Huawei Cloud Internacional se comuniquem, mas as VPCs devem estar na mesma região. Por exemplo, uma VPC no site do China continental está na região CN-Hong Kong, e a outra VPC no site Internacional também está na região CN-Hong Kong.
- Por padrão, se a VPC A estiver emparelhada com a VPC B que tenha EIPs, a VPC A não poderá usar EIPs na VPC B para acessar a Internet. Para habilitar isso, você pode usar o serviço NAT Gateway ou configurar um servidor SNAT. Para obter detalhes, consulte **Habilitação da conectividade com a Internet para um ECS sem um EIP**.

12.2 Exemplos de uso da conexão de emparelhamento de VPC

Uma conexão de emparelhamento de VPC é uma conexão de rede entre duas VPCs e permite que elas se comuniquem. **Tabela 12-1** lista diferentes cenários de uso de conexões de emparelhamento VPC.

Tabela 12-1 Exemplos de uso de conexão de emparelhamento de VPC

Localização	Bloco CIDR	Descrição
VPCs na mesma região	• Os blocos CIDR da VPC não se sobrepõem. • Blocos CIDR de sub-rede de VPCs não se sobrepõem.	Você pode criar conexões de emparelhamento de VPC para conectar blocos CIDR inteiros de VPCs. Em seguida, todos os recursos nas VPCs podem se comunicar uns com os outros.
VPCs na mesma região	• Os blocos CIDR da VPC se sobrepõem. • Alguns blocos CIDR de sub-rede se sobrepõem.	Você pode criar conexões de emparelhamento de VPC para conectar sub-redes específicas ou ECSs de VPCs diferentes. • Para conectar sub-redes específicas de duas VPCs, os blocos CIDR da sub-rede não podem se sobrepor. • Para conectar ECSs específicos de duas VPCs, cada ECS deve ter um endereço IP privado exclusivo.

Localização	Bloco CIDR	Descrição

Os blocos CIDR da VPC sesobrepõem. Todos os blocos CIDR desu

Localização	Bloco CIDR	Descrição

b-redes esobrepõem.

AVISO

Uma conexão de emparelhamento de VPC só pode conectar VPCs na mesma região. Se suas VPCs estiverem em regiões diferentes, use **Cloud Connect**.

Emparelhamento de duas ou mais VPCs

- Duas VPCs emparelhadas: a **Figura 12-4** mostra o diagrama de rede de uma conexão de emparelhamento de VPC que conecta VPC-A e VPC-B.

Figura 12-4 Diagrama de rede (IPv4)

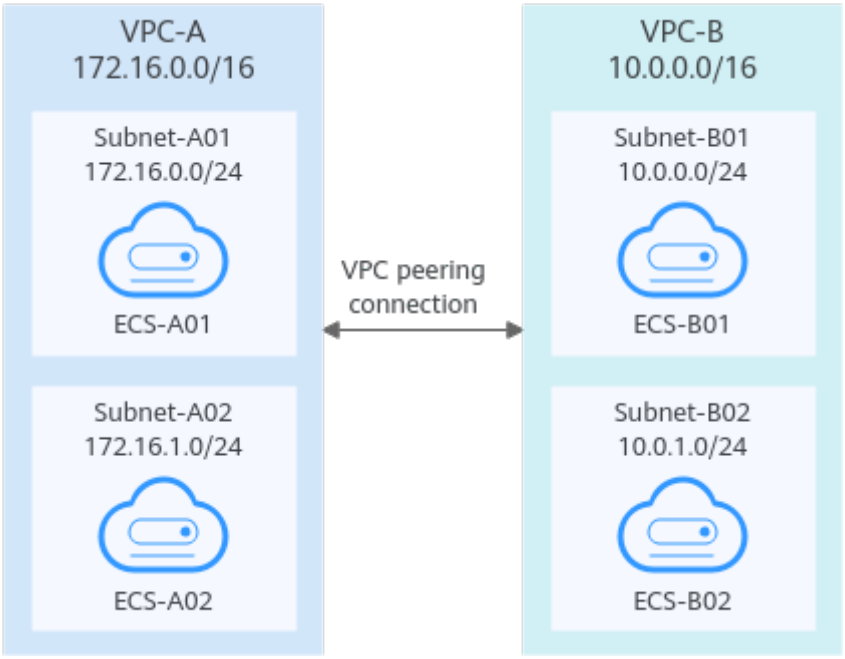


Tabela 12-2 Relações de emparelhamento (IPv4)

Relação de emparelhamento	Nome da conexão de emparelhamento	VPC local	VPC de par
VPC-A é emparelhada com a VPC-B.	Peering-AB	VPC-A	VPC-B

Tabela 12-3 Tabelas de rotas de VPC (IPv4)

Tabela de rotas	Destino	Próximo salto	Tipo de rota	Descrição
rtb-VPC-A	10.0.0.0/16	Peering-AB	Personalizado	Adicione uma rota com o bloco CIDR de VPC-B como o destino e Peering-AB como o próximo salto.
rtb-VPC-B	172.16.0.0/16	Peering-AB	Personalizado	Adicione uma rota com o bloco CIDR de VPC-A como o destino e Peering-AB como o próximo salto.

- Várias VPCs emparelhadas: a **Figura 12-5** mostra o diagrama de rede das conexões de emparelhamento VPC que conectam VPC-A, VPC-B e VPC-C.

Figura 12-5 Diagrama de rede (IPv4)

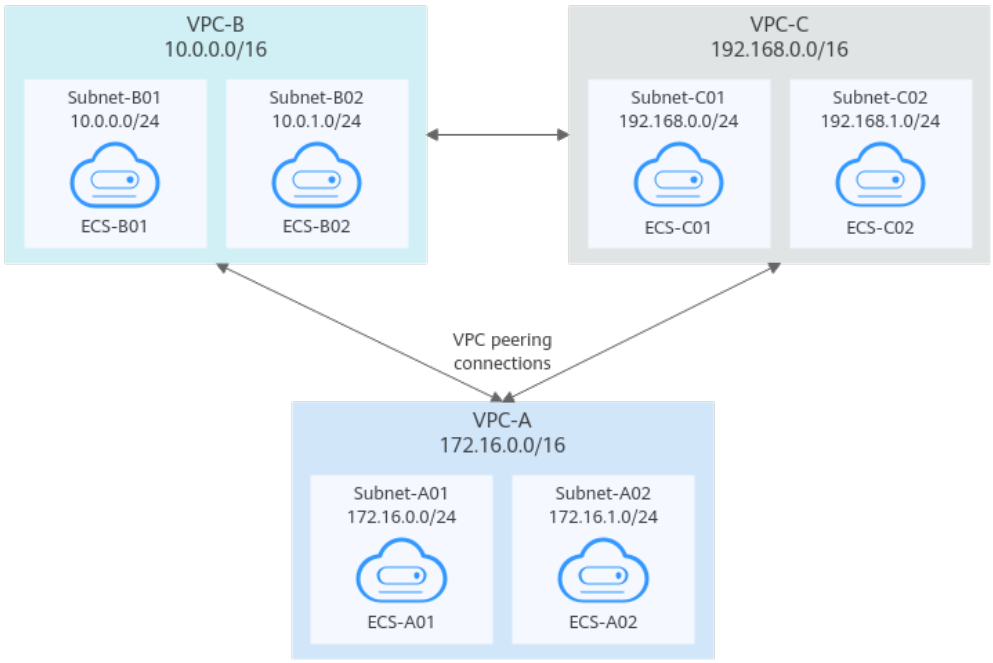


Tabela 12-4 Relações de emparelhamento (IPv4)

Relação de emparelhamento	Nome da conexão de emparelhamento	VPC local	VPC de par
VPC-A é emparelhada com a VPC-B.	Peering-AB	VPC-A	VPC-B
VPC-A é emparelhada com a VPC-C.	Peering-AC	VPC-A	VPC-C
VPC-B é emparelhada com a VPC-C.	Peering-BC	VPC-B	VPC-C

Tabela 12-5 Tabelas de rotas de VPC (IPv4)

Tabela de rotas	Destino	Próximo salto	Tipo de rota	Descrição
rtb-VPC-A	10.0.0.0/16	Peering-AB	Personalizado	Adicione uma rota com o bloco CIDR de VPC-B como o destino e Peering-AB como o próximo salto.

Tabela de rotas	Destino	Próximo salto	Tipo de rota	Descrição
	192.168.0.0/16	Peering-AC	Personalizado	Adicione uma rota com o bloco CIDR de VPC-C como o destino e Peering-AC como o próximo salto.
rtb-VPC-B	172.16.0.0/16	Peering-AB	Personalizado	Adicione uma rota com o bloco CIDR de VPC-A como o destino e Peering-AB como o próximo salto.
	192.168.0.0/16	Peering-BC	Personalizado	Adicione uma rota com o bloco CIDR de VPC-C como o destino e Peering-BC como o próximo salto.
rtb-VPC-C	172.16.0.0/16	Peering-AC	Personalizado	Adicione uma rota com o bloco CIDR de VPC-A como o destino e Peering-AC como o próximo salto.
	10.0.0.0/16	Peering-BC	Personalizado	Adicione uma rota com o bloco CIDR de VPC-B como o destino e Peering-BC como o próximo salto.

NOTA

Se um grande número de VPCs, por exemplo, 10 VPCs, precisar se comunicar entre si, a rede para estabelecer conexões de emparelhamento de VPC entre elas será complexa. Nesse caso, recomenda-se um roteador corporativo. Você pode conectar todas as VPCs a um roteador corporativo para permitir que elas se comuniquem. Para obter detalhes, consulte **Uso de um roteador corporativo para permitir a comunicação entre VPCs na mesma região**.

Emparelhamento de uma VPC central com várias VPCs

A **Figura 12-6** mostra o diagrama de rede das conexões de emparelhamento VPC que conectam VPC-B, VPC-C, VPC-D, VPC-E, VPC-F, VPC-G e VPC-A central.

Figura 12-6 Diagrama de rede (IPv4)

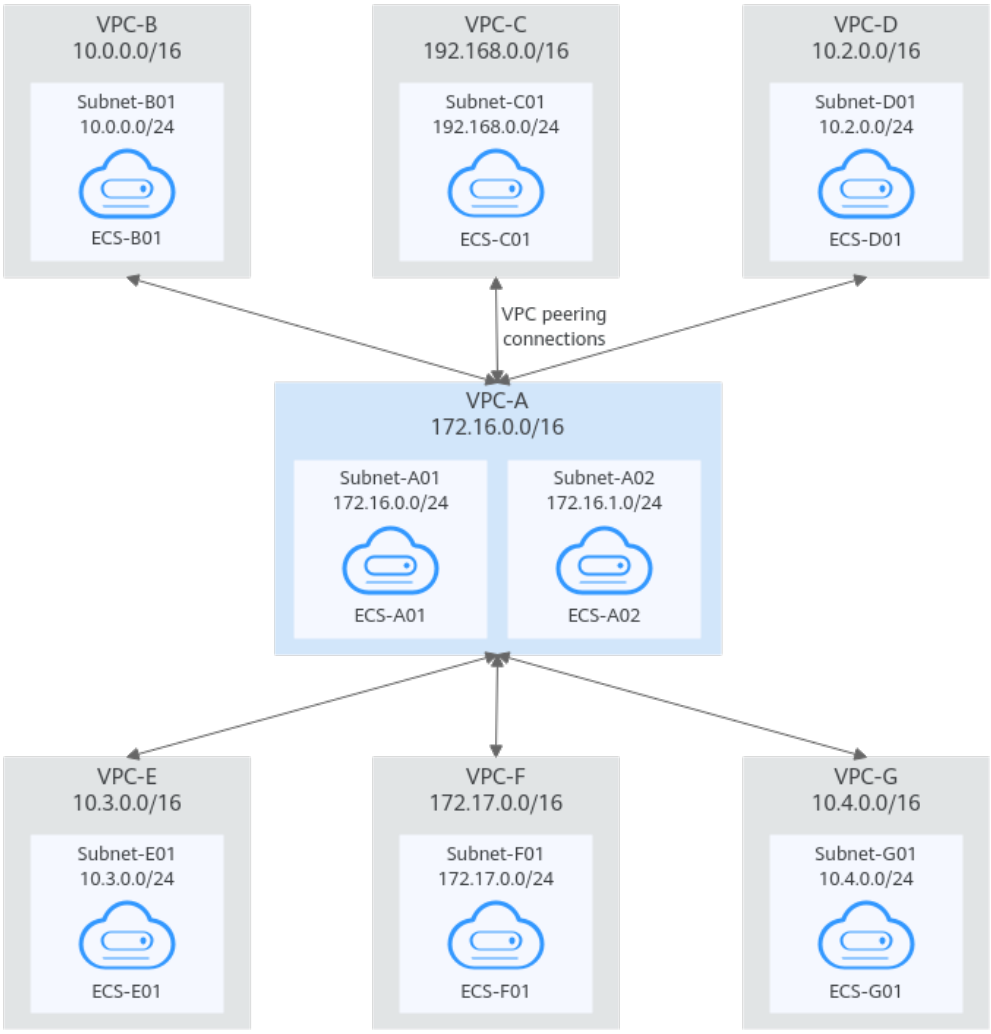


Tabela 12-6 Relações de emparelhamento (IPv4)

Relação de emparelhamento	Nome da conexão de emparelhamento	VPC local	VPC de par
VPC-A é emparelhada com a VPC-B.	Peering-AB	VPC-A	VPC-B
VPC-A é emparelhada com a VPC-C.	Peering-AC	VPC-A	VPC-C
VPC-A é emparelhada com a VPC-D.	Peering-AD	VPC-A	VPC-D
VPC-A é emparelhada com a VPC-E.	Peering-AE	VPC-A	VPC-E

Relação de emparelhamento	Nome da conexão de emparelhamento	VPC local	VPC de par
VPC-A é emparelhada com a VPC-F.	Peering-AF	VPC-A	VPC-F
VPC-A é emparelhada com a VPC-G.	Peering-AG	VPC-A	VPC-G

Tabela 12-7 Detalhes da tabela de rotas de VPC (IPv4)

Tabela de rotas	Destino	Próximo salto	Tipo de rota	Descrição
rtb-VPC-A	10.0.0.0/16	Peering-AB	Personalizado	Adicione uma rota com o bloco CIDR de VPC-B como o destino e Peering-AB como o próximo salto.
	192.168.0.0/16	Peering-AC	Personalizado	Adicione uma rota com o bloco CIDR de VPC-C como o destino e Peering-AC como o próximo salto.
	10.2.0.0/16	Peering-AD	Personalizado	Adicione uma rota com o bloco CIDR de VPC-D como o destino e Peering-AD como o próximo salto.
	10.3.0.0/16	Peering-AE	Personalizado	Adicione uma rota com o bloco CIDR de VPC-E como o destino e Peering-AE como o próximo salto.
	172.17.0.0/16	Peering-AF	Personalizado	Adicione uma rota com o bloco CIDR de VPC-F como o destino e Peering-AF como o próximo salto.
	10.4.0.0/16	Peering-AG	Personalizado	Adicione uma rota com o bloco CIDR de VPC-G como o destino e Peering-AG como o próximo salto.
rtb-VPC-B	172.16.0.0/16	Peering-AB	Personalizado	Adicione uma rota com o bloco CIDR de VPC-A como o destino e Peering-AB como o próximo salto.
rtb-VPC-C	172.16.0.0/16	Peering-AC	Personalizado	Adicione uma rota com o bloco CIDR de VPC-A como o destino e Peering-AC como o próximo salto.
rtb-VPC-D	172.16.0.0/16	Peering-AD	Personalizado	Adicione uma rota com o bloco CIDR de VPC-A como o destino e Peering-AD como o próximo salto.

Tabela de rotas	Destino	Próximo salto	Tipo de rota	Descrição
rtb-VPC-E	172.16.0.0/16	Peering-AE	Personalizado	Adicione uma rota com o bloco CIDR de VPC-A como o destino e Peering-AE como o próximo salto.
rtb-VPC-F	172.16.0.0/16	Peering-AF	Personalizado	Adicione uma rota com o bloco CIDR de VPC-A como o destino e Peering-AF como o próximo salto.
rtb-VPC-G	172.16.0.0/16	Peering-AG	Personalizado	Adicione uma rota com o bloco CIDR de VPC-A como o destino e Peering-AG como o próximo salto.

Emparelhamento de duas VPCs com blocos CIDR sobrepostos

Como mostrado em **Figura 12-7**, VPC-A e VPC-B têm sobreposição de blocos CIDR, e sua Subnet-A01 e Subnet-B01 também têm sobreposição de blocos CIDR. Nesse caso, uma conexão de emparelhamento de VPC pode conectar sua Subnet-A02 e Subnet-B02 que não se sobrepõem.

Figura 12-7 Diagrama de rede (IPv4)

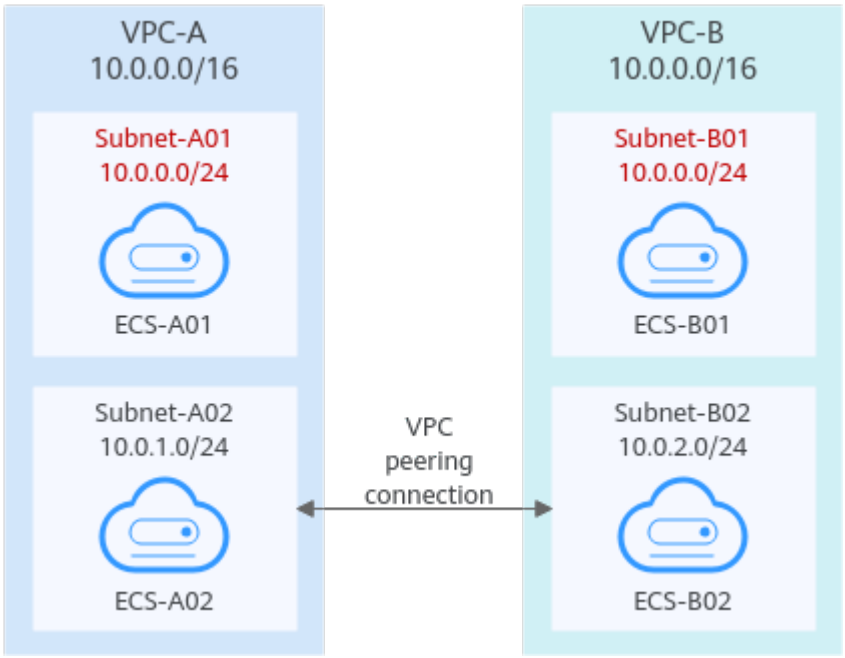


Tabela 12-8 Relações de emparelhamento (IPv4)

Relação de emparelhamento	Nome da conexão de emparelhamento	VPC local	VPC de par
VPC-A é emparelhada com a VPC-B.	Peering-AB	VPC-A	VPC-B

Tabela 12-9 Detalhes da tabela de rotas da VPC (IPv4)

Tabela de rotas	Destino	Próximo salto	Tipo de rota	Descrição
rtb-VPC-A	10.0.2.0/24	Peering-AB	Personalizado	Adicione uma rota com o bloco CIDR de Subnet-B02 como o destino e emparelhamento-AB como o próximo salto.
rtb-VPC-B	10.0.1.0/24	Peering-AB	Personalizado	Adicione uma rota com o bloco CIDR de Subnet-A02 como o destino e Peering-AB como o próximo salto.

Emparelhamento de ECSs em uma VPC central com ECSs em duas outras VPCs

Como mostrado em **Figura 12-8**, VPC-B e VPC-C têm blocos CIDR sobrepostos, e suas Subnet-B01 e Subnet-C01 têm blocos CIDR sobrepostos. Nesse caso, a conexão de emparelhamento VPC pode conectar ECSs em Subnet-B01 e Subnet-A01 e ECSs em Subnet-C01 e Subnet-A01.

Figura 12-8 Diagrama de rede (IPv4)

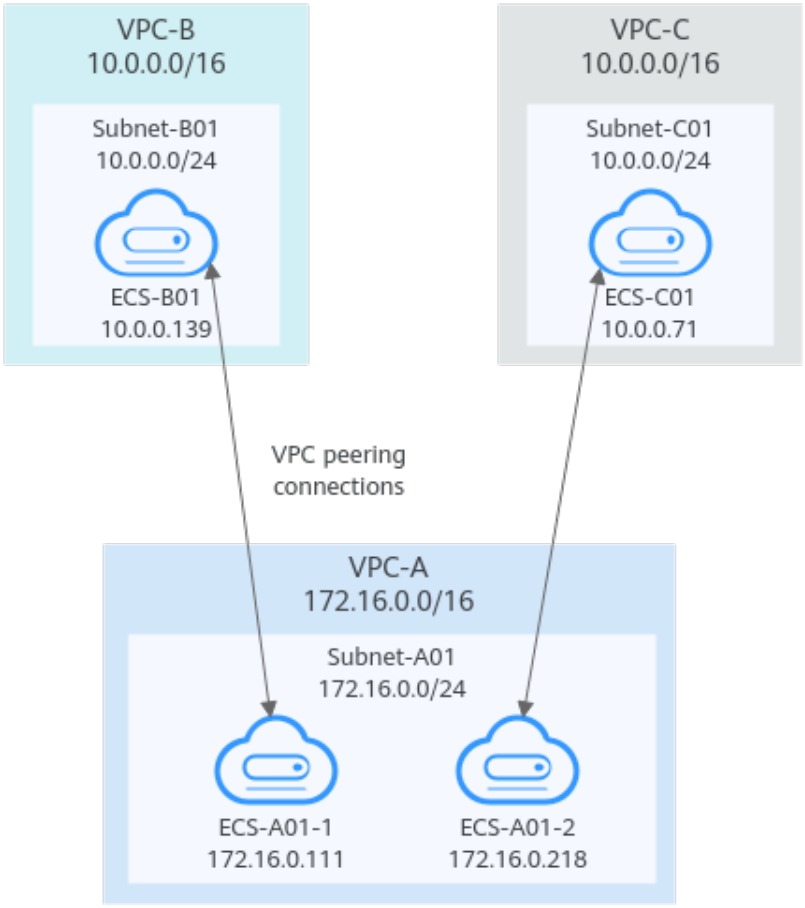


Tabela 12-10 Relações de emparelhamento (IPv4)

Relação de emparelhamento	Nome da conexão de emparelhamento	VPC local	VPC de par
O ECS-A01-1 na VPC-A é emparelhado com o ECS-B01 na VPC-B.	Peering-AB	VPC-A	VPC-B
ECS-A01-2 na VPC-A é emparelhado com ECS-C01 na VPC-C.	Peering-AC	VPC-A	VPC-C

Tabela 12-11 Detalhes da tabela de rotas da VPC (IPv4)

Tabela de rotas	Destino	Próximo salto	Tipo de rota	Descrição
rtb-VPC-A	10.0.0.139/32	Peering-AB	Personalizado	Adicione uma rota com o endereço IP privado de ECS-B01 como o destino e Peering-AB como o salto seguinte.
	10.0.0.71/32	Peering-AC	Personalizado	Adicione uma rota com o endereço IP privado de ECS-C01 como o destino e Peering-AC como o salto seguinte.
rtb-VPC-B	172.16.0.111/32	Peering-AB	Personalizado	Adicione uma rota com o endereço IP privado de ECS-A01-1 como o destino e Peering-AB como o salto seguinte.
rtb-VPC-C	172.16.0.218/32	Peering-AC	Personalizado	Adicione uma rota com o endereço IP privado de ECS-A01-2 como o destino e Peering-AC como o salto seguinte.

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

Cenários

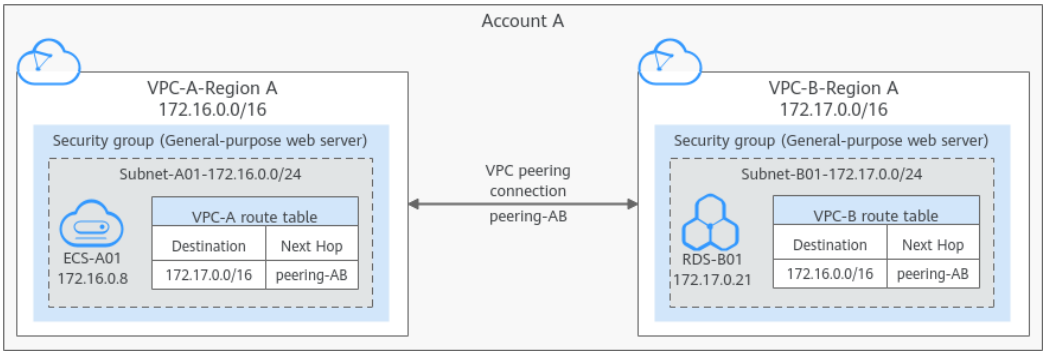
Se duas VPCs da mesma região não puderem se comunicar entre si, você poderá usar uma conexão de emparelhamento de VPC. Esta seção descreve como criar uma conexão de emparelhamento de VPC entre duas VPCs na mesma conta.

A seguir, descrevemos como criar uma conexão de emparelhamento de VPC entre VPC-A e VPC-B na conta A para habilitar as comunicações entre o ECS-A01 e o RDS-B01.

Procedimento:

1. **Passo 1: criar uma conexão de emparelhamento de VPC.**
2. **Passo 2: adicionar rotas para a conexão de emparelhamento de VPC**
3. **Passo 3: verificar a conectividade da rede**

Figura 12-9 Diagrama de rede de uma conexão de emparelhamento de VPC entre VPCs na mesma conta



AVISO

Atualmente, as conexões de emparelhamento de VPC são gratuitas.

Observações e restrições

- Apenas uma conexão de emparelhamento de VPC pode ser criada entre duas VPCs ao mesmo tempo.
- Uma conexão de emparelhamento de VPC só pode conectar VPCs na mesma região.
  - Se você quiser conectar VPCs em regiões diferentes, use **Cloud Connect**.
  - Se você precisar de apenas alguns ECSs em regiões diferentes para se comunicar, poderá **atribuir e vincular EIPs aos ECSs**.
- Se as VPCs locais e de par tiverem blocos CIDR sobrepostos, a conexão de emparelhamento da VPC pode não ter efeito.

  Neste caso, você pode consultar **exemplos de configuração de rede**.

Pré-requisitos

Você tem duas VPCs na mesma região. Se você quiser criar um, veja **Criação de uma VPC**.

Passo 1: criar uma conexão de emparelhamento de VPC.

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, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **VPC Peering Connections**.

   A lista de conexões de emparelhamento de VPC é exibida.
5. No canto superior direito da página, clique em **Create VPC Peering Connection**.

   A caixa de diálogo **Create VPC Peering Connection** é exibida.
6. Configure os parâmetros conforme solicitado.

   Para mais detalhes, consulte **Tabela 12-12**.

Figura 12-10 Criar conexão de emparelhamento de VPC

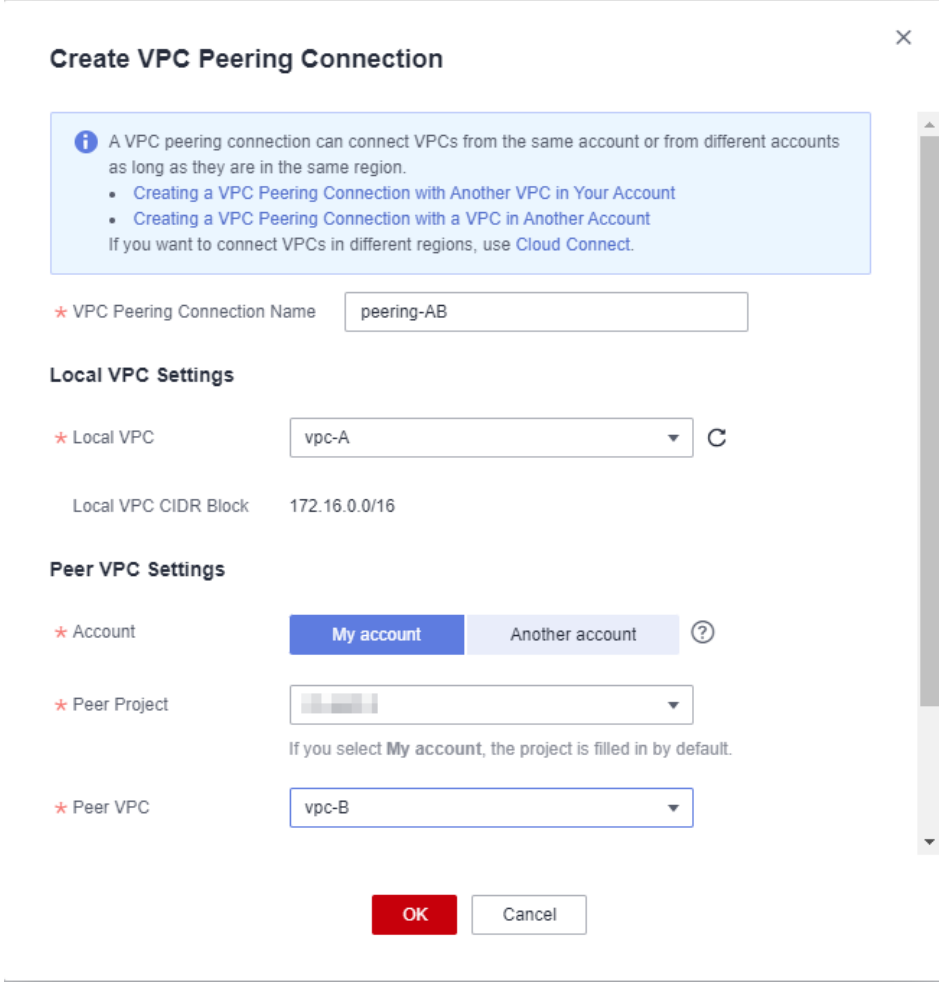


Tabela 12-12 Parâmetros para criar uma conexão de emparelhamento de VPC

Parâmetro	Descrição	Exemplo de valor
VPC Peering Connection Name	Obrigatório Insira um nome para a conexão de emparelhamento da VPC. O nome pode conter no máximo 64 caracteres Unicode, incluindo letras, dígitos, hifens (-) e sublinhados (_).	peering-AB
Local VPC	Obrigatório VPC em uma extremidade da conexão de emparelhamento VPC. Você pode selecionar uma na lista suspensa.	VPC-A
Bloco CIDR do VPC local	Bloco CIDR da VPC local selecionada	172.16.0.0/16

Parâmetro	Descrição	Exemplo de valor
Account	Obrigatório ● Opções: **My account** e **Another account** ● Selecione **My account**.	My account
Peer Project	O sistema preenche o projeto correspondente por padrão porque **My account** está definida como **Account**. Por exemplo, se VPC-A e VPC-B estiverem na conta A e na região A, o sistema preencherá o projeto correspondente da conta A na região A por padrão.	ab-cdef-1
Peer VPC	Esse parâmetro é obrigatório se **Account** estiver definido como **My account**. VPC na outra extremidade da conexão de emparelhamento de VPC. Você pode selecionar uma na lista suspensa.	VPC-B
Peer VPC CIDR Block	Bloco CIDR da VPC de par selecionada Se as VPCs locais e de par tiverem blocos CIDR sobrepostos, a conexão de emparelhamento da VPC pode não ter efeito. Para obter detalhes, consulte **Exemplos de uso da conexão de emparelhamento de VPC**.	172.17.0.0/16
Description	Opcional Insira a descrição da conexão de emparelhamento da VPC na caixa de texto, conforme necessário.	peering-AB conecta VPC-A e VPC-B.

7. Clique em **OK**.

   Uma caixa de diálogo para adicionar rotas é exibida.

8. Clique em **Add Route** ou **Add Later**.

   Se você clicar em **Add Route**, a página **Local Routes** será exibida. Então, vá para **Passo 2: adicionar rotas para a conexão de emparelhamento de VPC**.

AVISO

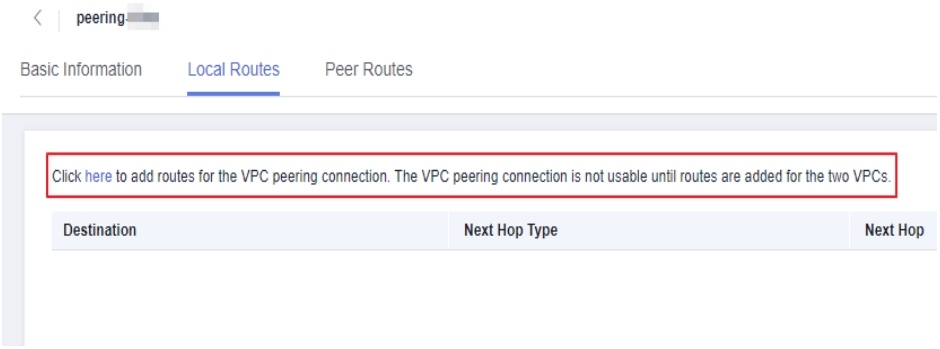
Depois que uma conexão de emparelhamento de VPC é criada, você deve adicionar rotas às tabelas de rotas das VPCs locais e de par. Caso contrário, a conexão de emparelhamento da VPC não terá efeito.

Passo 2: adicionar rotas para a conexão de emparelhamento de VPC

1. Adicione rotas à tabela de rotas da VPC local:
   a. Na guia **Local Routes** da conexão de emparelhamento da VPC, clique no hiperlink **Route Tables**.

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

      Figura 12-11 Hiperlink para a tabela de rotas-VPC local

   b. Clique em **Add Route**.

      Tabela 12-13 descreve os parâmetros de rota.

      Tabela 12-13 Descrição do parâmetro

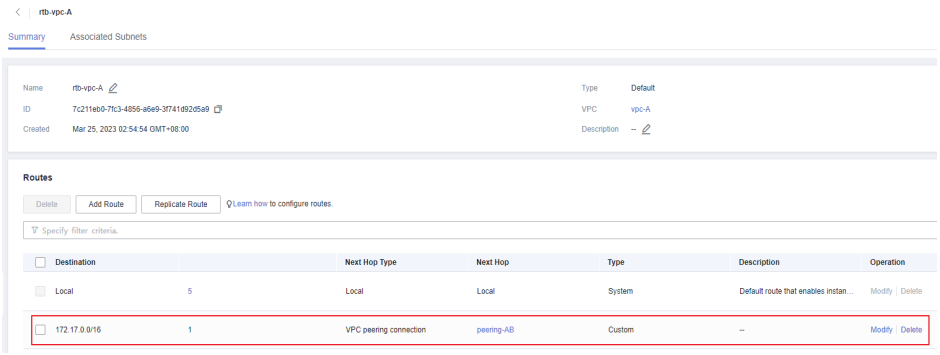
Parâmetro	Descrição	Exemplo de valor
Destination Type	O destino pode ser: ● **IP address**: selecione esta opção se quiser inserir um endereço IP ou um intervalo de endereços IP. ● **IP address group**: selecione esta opção se desejar selecionar um grupo de endereços IP que contenha um ou mais endereços IP.	IP address
Destination	O bloco CIDR da VPC de par, o bloco CIDR da sub-rede ou o endereço IP do ECS. Para mais detalhes, consulte **Exemplos de uso da conexão de emparelhamento de VPC**.	Bloco CIDR da VPC-B: 172.17.0.0/16
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 de VPC atual.	peering-AB
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 >).	-

c. Clique em **OK**.

Você pode visualizar a rota na lista de rotas.

Figura 12-12 Rota para a VPC local

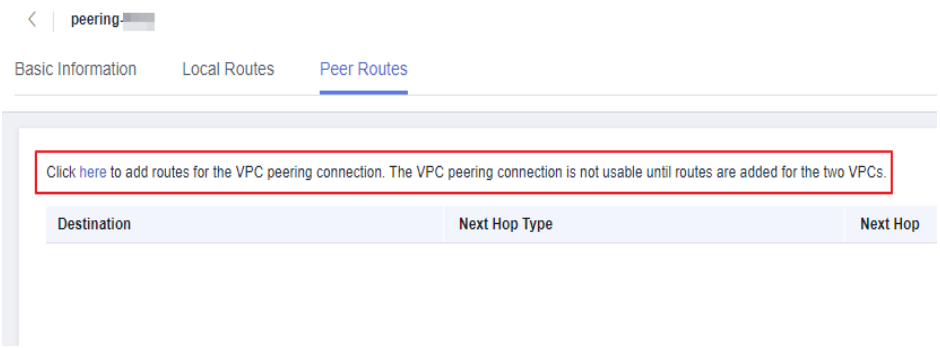


2. Adicione rotas à tabela de rotas da VPC par:

a. Na guia **Peer Routes** da conexão de emparelhamento da VPC, clique no hiperlink **Route Tables**.

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

Figura 12-13 Hiperlink para tabela de rotas-VPC de par



b. Clique em **Add Route**.

Tabela 12-14 descreve os parâmetros de rota.

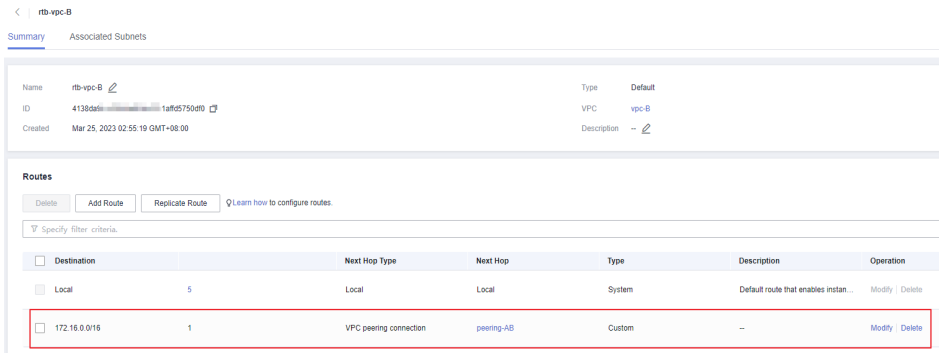
Tabela 12-14 Descrição do parâmetro

Parâmetro	Descrição	Exemplo de valor
Destination Type	O destino pode ser: ● **IP address**: selecione esta opção se quiser inserir um endereço IP ou um intervalo de endereços IP. ● **IP address group**: selecione esta opção se desejar selecionar um grupo de endereços IP que contenha um ou mais endereços IP.	IP address
Destination	O bloco CIDR da VPC local, bloco CIDR da sub-rede ou endereço IP do ECS. Para mais detalhes, consulte **Exemplos de uso da conexão de emparelhamento de VPC**.	Bloco CIDR da VPC-A: 172.16.0.0/16
Next Hop Type	O tipo de próximo 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-AB
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 >).	-

c. Clique em **OK**.

Você pode visualizar a rota na lista de rotas.

Figura 12-14 Rota para a VPC par



Passo 3: verificar a conectividade da rede

Depois de adicionar rotas para a conexão de emparelhamento da VPC, verifique a comunicação entre as VPCs locais e de par.

1. Efetue logon no ECS-A01 na VPC local.
2. Verifique se o ECS-A01 pode se comunicar com o RDS-B01.

   Ping *endereço IP do RDS-B01*

   Exemplo de comando:

   ping 172.17.0.21

   Se informações semelhantes às seguintes forem exibidas, o ECS-A01 e o RDS-B01 poderão se comunicar entre si e a conexão de emparelhamento da VPC entre a VPC-A e a VPC-B será criada com êxito.

```
[root@ecs-A02 ~]# ping 172.17.0.21
PING 172.17.0.21 (172.17.0.21) 56(84) bytes of data.
64 bytes from 172.17.0.21: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.17.0.21: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.17.0.21: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.17.0.21: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.17.0.21 ping statistics ---
```

AVISO

- Neste exemplo, o ECS-A01 e o RDS-B01 estão no mesmo grupo de segurança. Se as instâncias em grupos de segurança diferentes, você precisa adicionar regras de entrada para permitir o acesso do grupo de segurança de par. Para mais detalhes, consulte **Ativar ECSs em diferentes grupos de segurança para se comunicarem entre si por meio de uma rede interna**.
- Se as VPCs conectadas por uma conexão de emparelhamento da VPC não puderem se comunicar entre si, consulte **Por que a comunicação falhou entre VPCs que foram conectadas por uma conexão de emparelhamento de VPC**

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

Cenários

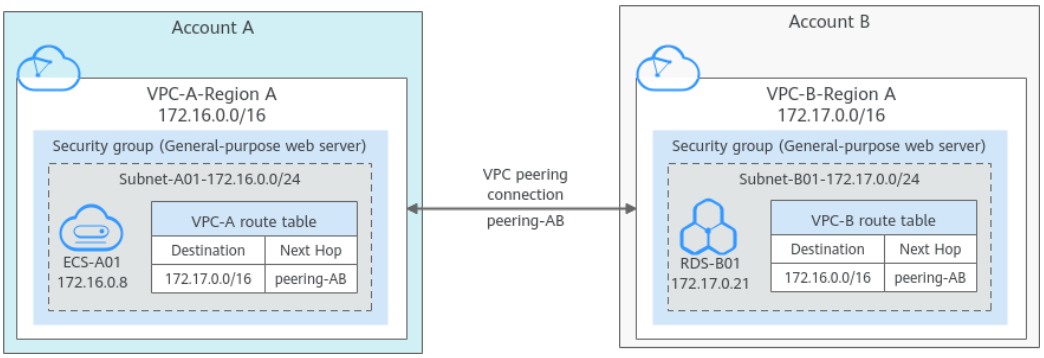
Se duas VPCs da mesma região não puderem se comunicar, você poderá usar uma conexão de emparelhamento de VPC. Esta seção descreve como criar uma conexão de emparelhamento de VPC entre duas VPCs em contas diferentes.

A seguir, descrevemos como criar uma conexão de emparelhamento de VPC entre a VPC-A na conta A e a VPC-B na conta B para habilitar a comunicação entre o ECS-A01 e o RDS-B01.

Procedimento:

1. **Passo 1: criar uma conexão de emparelhamento de VPC.**
2. **Passo 2: a conta de par aceita a solicitação de conexão de emparelhamento da VPC**
3. **Passo 3: adicionar rotas para a conexão de emparelhamento da VPC**
4. **Passo 4: verificar conectividade de rede**

Figura 12-15 Diagrama de rede de uma conexão de emparelhamento de VPC entre VPCs em diferentes contas



AVISO

Atualmente, as conexões de emparelhamento de VPC são gratuitas.

Observações e restrições

- Apenas uma conexão de emparelhamento de VPC pode ser criada entre duas VPCs ao mesmo tempo.
- Uma conexão de emparelhamento de VPC só pode conectar VPCs na mesma região.
  - Se você quiser conectar VPCs em regiões diferentes, use **Cloud Connect**.
  - Se você precisar de apenas alguns ECSs em regiões diferentes para se comunicar, poderá **atribuir e vincular EIPs aos ECSs**.
- Se as VPCs locais e de par tiverem blocos CIDR sobrepostos, a conexão de emparelhamento da VPC pode não ter efeito.

  Neste caso, você pode consultar **exemplos de configuração de rede**.
- Para uma conexão de emparelhamento de VPC entre VPCs em contas diferentes:
  - Se a conta A iniciar uma solicitação para criar uma conexão de emparelhamento da VPC com uma VPC na conta B, a conexão de emparelhamento da VPC entrará em vigor somente depois que a conta B aceitar a solicitação.
  - Para garantir a segurança da rede, não aceite conexões de emparelhamento de VPC de contas desconhecidas.

Pré-requisitos

Você tem duas VPCs na mesma região. Se você quiser criar um, veja **Criação de uma VPC**.

Passo 1: criar uma conexão de emparelhamento de VPC.

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, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **VPC Peering Connections**.

A lista de conexões de emparelhamento de VPC é exibida.

5. No canto superior direito da página, clique em **Create VPC Peering Connection**.

   A caixa de diálogo **Create VPC Peering Connection** é exibida.

6. Configure os parâmetros conforme solicitado.

   Para mais detalhes, consulte **Tabela 12-15**.

Figura 12-16 Criar conexão de emparelhamento de VPC

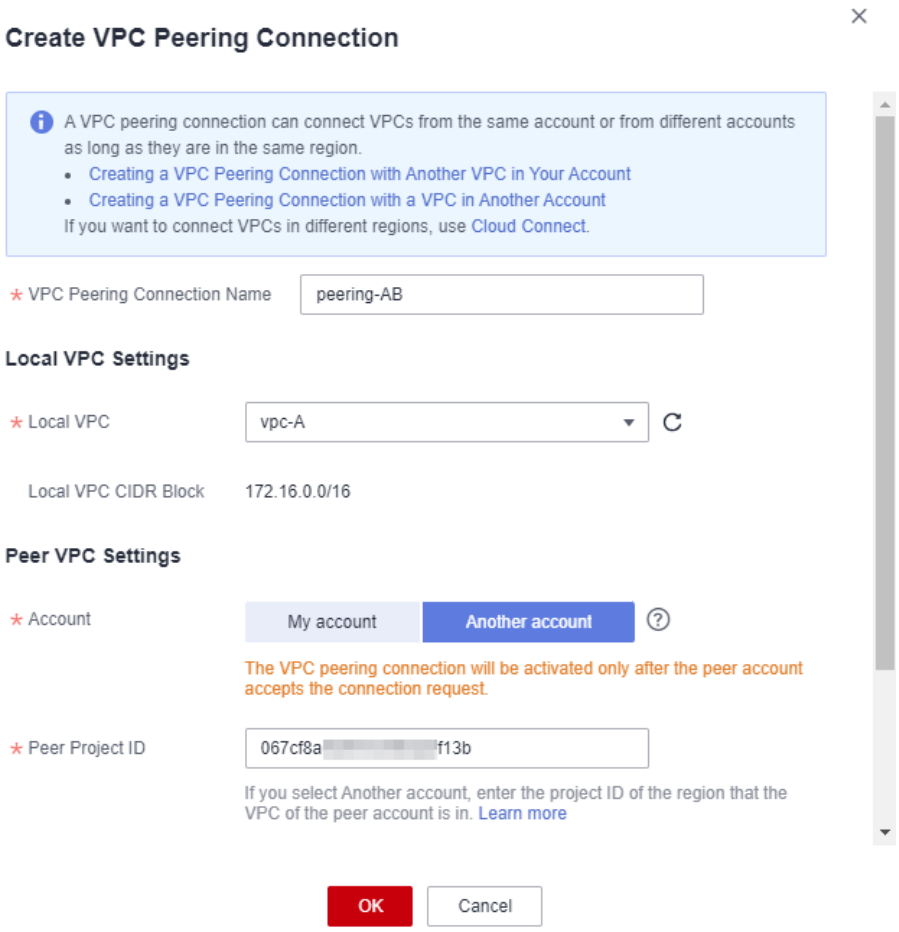


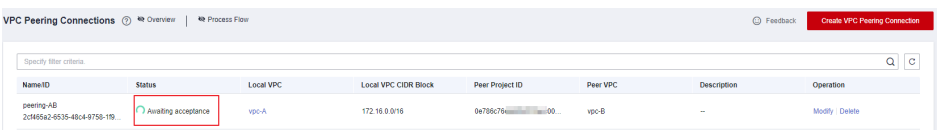
Tabela 12-15 Parâmetros para criar uma conexão de emparelhamento de VPC

Parâmetro	Descrição	Exemplo de valor
VPC Peering Connection Name	Obrigatório Insira um nome para a conexão de emparelhamento da VPC. O nome pode conter no máximo 64 caracteres Unicode, incluindo letras, dígitos, hifens (-) e sublinhados (_).	peering-AB

Parâmetro	Descrição	Exemplo de valor
Local VPC	Obrigatório VPC em uma extremidade da conexão de emparelhamento de VPC. Você pode selecionar uma na lista suspensa.	VPC-A
Local VPC CIDR Block	Bloco CIDR da VPC local selecionada	172.16.0.0/16
Account	Obrigatório ● Opções: **My account** e **Another account** ● Selecione **Another account**.	Another account
Peer Project ID	Este parâmetro é obrigatório porque **Account** está definida como **Another account**.	ID do projeto da VPC-B na região A: 067cf8aecf3XXX08322f13b
Peer VPC ID	Este parâmetro é obrigatório porque **Account** está definida como **Another account**.	ID da VPC-B: 17cd7278-XXX-530c952dcf35
Description	Opcional Insira a descrição da conexão de emparelhamento da VPC na caixa de texto, conforme necessário. A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >).	peering-AB conecta VPC-A e VPC-B.

7. Clique em **OK**.
   - Se a mensagem "Invalid VPC ID and project ID." for exibida, verifique se o código do projeto e o código da VPC estão corretos.
     - ID do projeto do par: o valor deve ser o ID do projeto da região em que a VPC do par reside.
     - As VPCs locais e de par devem estar na mesma região.
   - Se o status da conexão de emparelhamento da VPC criada for **Awaiting acceptance**, vá para **Passo 2: a conta de par aceita a solicitação de conexão de emparelhamento da VPC**.

Figura 12-17 Aguardar aceitação



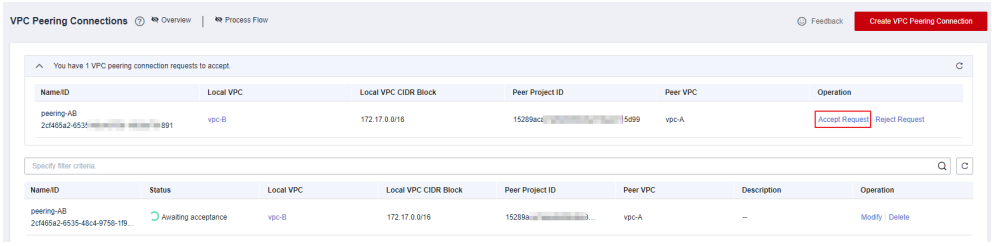
Passo 2: a conta de par aceita a solicitação de conexão de emparelhamento da VPC

Depois de criar uma conexão de emparelhamento de VPC com uma VPC em outra conta, você precisa entrar em contato com a conta de emparelhamento para aceitar a solicitação de conexão de emparelhamento de VPC. Neste exemplo, a conta A notifica a conta B para aceitar a solicitação. A conta B precisa:

1. Faça logon no console de gerenciamento.
2. Na página inicial do console, em **Rede**, clique em **Virtual Private Cloud**.
3. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **VPC Peering Connections**.

   A lista de conexões de emparelhamento de VPC é exibida.
4. Na parte superior da lista de conexões de emparelhamento de VPC, localize a solicitação de conexão de emparelhamento de VPC a ser aceita.

   Figura 12-18 Aceitar solicitação



5. Localize a linha que contém a conexão de emparelhamento da VPC de destino e clique em **Accept Request** na coluna **Operation**.

   Depois que o status da conexão de emparelhamento da VPC for alterado para **Accepted**, a conexão de emparelhamento da VPC será criada.
6. Vá para **Passo 3: adicionar rotas para a conexão de emparelhamento da VPC**.

AVISO

Depois que uma conexão de emparelhamento de VPC é criada, você deve adicionar rotas às tabelas de rotas das VPCs locais e de peer. Caso contrário, a conexão de emparelhamento da VPC não terá efeito.

Passo 3: adicionar rotas para a conexão de emparelhamento da VPC

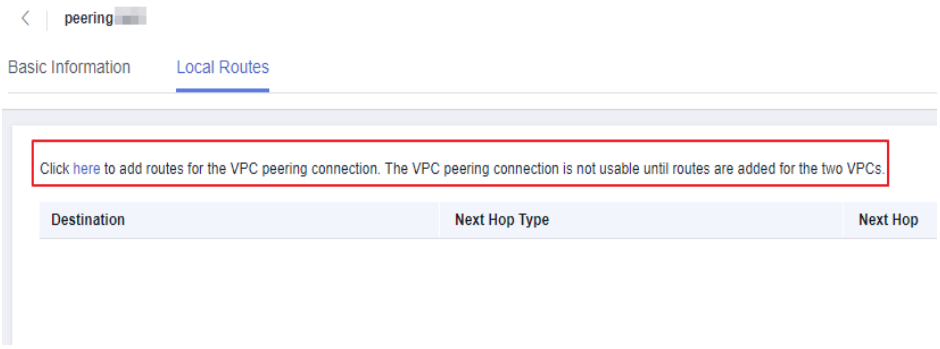
Ambas as contas precisam adicionar uma rota à tabela de rotas de sua VPC. Neste exemplo, a conta A adiciona uma rota à tabela de rotas do VPC-A e a conta B adiciona uma rota à tabela de rotas do VPC-B.

1. Adicione rotas à tabela de rotas da VPC local:
   a. Na lista de conexões de emparelhamento VPC da conta local, clique no nome da conexão de emparelhamento VPC de destino.

      A guia **Basic Information** da conexão de emparelhamento da VPC é exibida.
   b. Na guia **Local Routes** da conexão de emparelhamento da VPC, clique no hiperlink **Route Tables**.

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

Figura 12-19 Hiperlink para a tabela de rotas-VPC local



c. Clique em **Add Route**.

Tabela 12-16 descreve os parâmetros de rota.

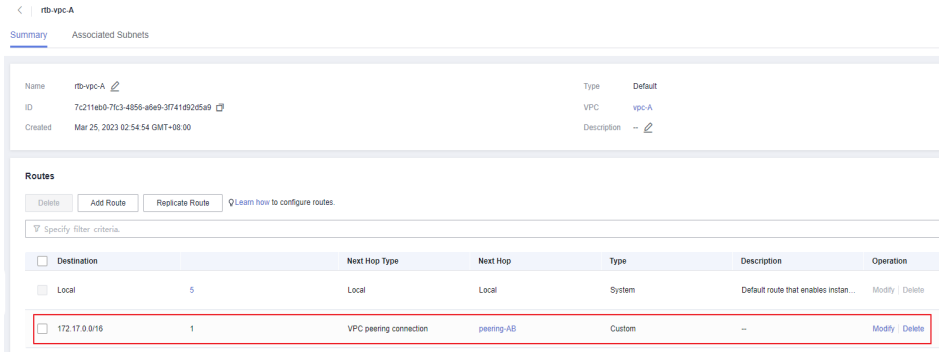
Tabela 12-16 Descrição do parâmetro

Parâmetro	Descrição	Exemplo de valor
Destination Type	O destino pode ser: ● **IP address**: selecione esta opção se quiser inserir um endereço IP ou um intervalo de endereços IP. ● **IP address group**: selecione esta opção se desejar selecionar um grupo de endereços IP que contenha um ou mais endereços IP.	IP address
Destination	O bloco CIDR da VPC de par, o bloco CIDR da sub-rede ou o endereço IP do ECS. Para mais detalhes, consulte **Exemplos de uso da conexão de emparelhamento de VPC**.	Bloco CIDR da VPC-B: 172.17.0.0/16
Next Hop Type	O tipo de próximo 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-AB
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 >).	-

d. Clique em **OK**.

Você pode visualizar a rota na lista de rotas.

Figura 12-20 Rota para a VPC local



2. Adicione rotas à tabela de rotas da VPC de par:

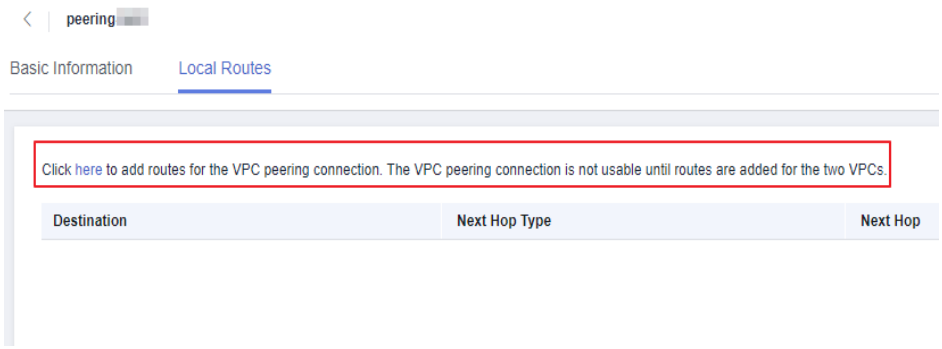
   a. Na lista de conexões de emparelhamento de VPC da conta de par, clique no nome da conexão de emparelhamento de VPC de destino.

      A guia **Basic Information** da conexão de emparelhamento da VPC é exibida.

   b. Na guia **Local Routes** da conexão de emparelhamento da VPC, clique no hiperlink **Route Tables**.

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

Figura 12-21 Hiperlink para tabela de rotas-VPC de par



   c. Clique em **Add Route**.

      Tabela 12-17 descreve os parâmetros de rota.

Tabela 12-17 Descrição do parâmetro

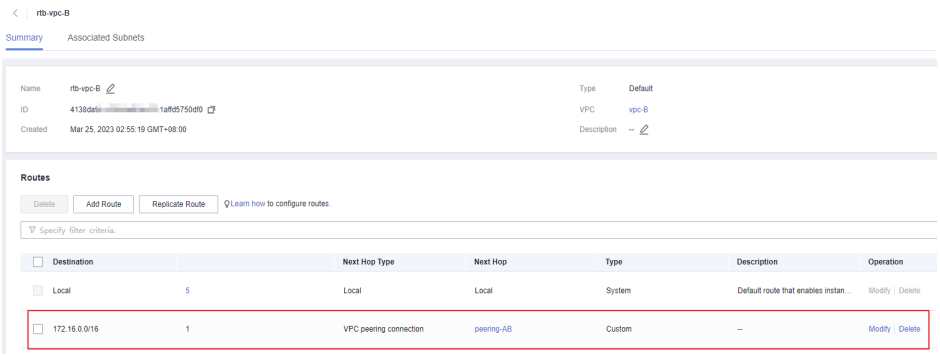
Parâmetro	Descrição	Exemplo de valor
Destination Type	O destino pode ser: ● **IP address**: selecione esta opção se quiser inserir um endereço IP ou um intervalo de endereços IP. ● **IP address group**: selecione esta opção se desejar selecionar um grupo de endereços IP que contenha um ou mais endereços IP.	IP address

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 **Exemplos de uso da conexão de emparelhamento de VPC**.	Bloco CIDR da VPC-A: 172.16.0.0/16
Next Hop Type	O tipo de próximo 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-AB
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 >).	-

d. Clique em **OK**.

Você pode visualizar a rota na lista de rotas.

Figura 12-22 Rota para a VPC par



Passo 4: verificar conectividade de rede

Depois de adicionar rotas para a conexão de emparelhamento da VPC, verifique a comunicação entre as VPCs locais e de par.

1. Efetue logon no ECS-A01 na VPC local.
2. Verifique se o ECS-A01 pode se comunicar com o RDS-B01.

   Ping *endereço IP do RDS-B01*

   Exemplo de comando:

   ping 172.17.0.21

   Se informações semelhantes às seguintes forem exibidas, o ECS-A01 e o RDS-B01 poderão se comunicar entre si e a conexão de emparelhamento da VPC entre a VPC-A e a VPC-B será criada com êxito.

```
[root@ecs-A02 ~]# ping 172.17.0.21
PING 172.17.0.21 (172.17.0.21) 56(84) bytes of data.
```



```
64 bytes from 172.17.0.21: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.17.0.21: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.17.0.21: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.17.0.21: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.17.0.21 ping statistics ---
```

AVISO

- Neste exemplo, o ECS-A01 e o RDS-B01 estão no mesmo grupo de segurança. Se as instâncias em grupos de segurança diferentes, você precisa adicionar regras de entrada para permitir o acesso do grupo de segurança de par. Para mais detalhes, consulte **Ativar ECSs em diferentes grupos de segurança para se comunicarem entre si por meio de uma rede interna**.
- Se as VPCs conectadas por uma conexão de emparelhamento da VPC não puderem se comunicar entre si, consulte **Por que a comunicação falhou entre VPCs que foram conectadas por uma conexão de emparelhamento de VPC**

12.5 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. 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 **Rede** , 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**.

12.6 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. 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 **Rede**, 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.

12.7 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. 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 **Rede**, 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.

12.8 Exibição de rotas configuradas para uma conexão de emparelhamento de VPC

Cenários

Esta seção descreve como exibir as rotas adicionadas às tabelas de rotas de VPCs locais e de par de uma conexão de emparelhamento de VPC.

- **Exibir rotas de uma conexão de emparelhamento de VPC entre VPCs na mesma conta**
- **Exibir rotas de uma conexão de emparelhamento de VPC entre VPCs em contas diferentes**

Se duas VPCs não puderem se comunicar por meio de uma conexão de emparelhamento de VPC, você poderá verificar as rotas adicionadas para as VPCs locais e de par seguindo as instruções fornecidas nesta seção.

Exibir rotas de uma conexão de emparelhamento de VPC entre VPCs na mesma conta

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, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **VPC Peering Connections**.

   A lista de conexões de emparelhamento de VPC é exibida.
5. Na lista de conexões de emparelhamento de VPC, clique no nome da conexão de emparelhamento de VPC de destino.

   A página que mostra os detalhes da conexão de emparelhamento da VPC é exibida.
6. Exiba as rotas adicionadas para a conexão de emparelhamento da VPC:
   a. Clique na guia **Local Routes** para visualizar a rota local adicionada para a conexão de emparelhamento da VPC.
   b. Clique na guia **Peer Routes** para visualizar a rota de par adicionada para a conexão de emparelhamento da VPC.

Exibir rotas de uma conexão de emparelhamento de VPC entre VPCs em contas diferentes

Somente o proprietário da conta de uma VPC em uma conexão de emparelhamento da VPC pode visualizar as rotas adicionadas para a conexão.

1. Faça logon no console de gerenciamento usando a conta da VPC local e exiba a rota da VPC local:
   a. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.

b. Na página inicial do console, em **Rede**, clique em **Virtual Private Cloud**.

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

A lista de conexões de emparelhamento de VPC é exibida.

d. Na lista de conexões de emparelhamento de VPC, clique no nome da conexão de emparelhamento de VPC de destino.

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

e. Clique na guia **Local Routes** para visualizar a rota local adicionada para a conexão de emparelhamento da VPC.

2. Faça logon no console de gerenciamento usando a conta da VPC de par e exiba a rota da VPC de par referindo-se a **1**.

12.9 Exclusão de rotas configuradas para uma conexão de emparelhamento de VPC

Cenários

Esta seção descreve como excluir rotas das tabelas de rotas das VPCs locais e de par conectadas por uma conexão de emparelhamento de VPC.

- **Exclusão de rotas de uma conexão de emparelhamento de VPC entre VPCs na mesma conta**
- **Excluindo rotas de uma conexão de emparelhamento de VPC entre VPCs em contas diferentes**

Exclusão de rotas de uma conexão de emparelhamento de VPC entre VPCs na mesma conta

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, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **VPC Peering Connections**.

   A lista de conexões de emparelhamento de VPC é exibida.
5. Na lista de conexões de emparelhamento de VPC, clique no nome da conexão de emparelhamento de VPC de destino.

   A página que mostra os detalhes da conexão de emparelhamento da VPC é exibida.
6. 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**.

   Uma caixa de diálogo de confirmação é exibida.

   c. Clique em **Yes**.

7. 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**.

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

Excluindo rotas de uma conexão de emparelhamento de VPC entre VPCs em contas diferentes

Somente o proprietário da conta de uma VPC em uma conexão de emparelhamento da VPC pode excluir as rotas adicionadas para a conexão.

1. Faça logon no console de gerenciamento usando a conta da VPC local e exclua a rota da VPC local:
   a. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
   b. Na página inicial do console, em **Rede**, clique em **Virtual Private Cloud**.
   c. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **VPC Peering Connections**.

      A lista de conexões de emparelhamento de VPC é exibida.
   d. Na lista de conexões de emparelhamento de VPC, clique no nome da conexão de emparelhamento de VPC de destino.

      A página que mostra os detalhes da conexão de emparelhamento da VPC é exibida.
   e. Exclua a rota adicionada à tabela de rotas da VPC local:
      i. 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.
      ii. 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.
      iii. Clique em **Yes**.
2. Faça logon no console de gerenciamento usando a conta da VPC de par e exclua a rota da VPC de par referindo-se a **1**.

13 Log de fluxo de VPC

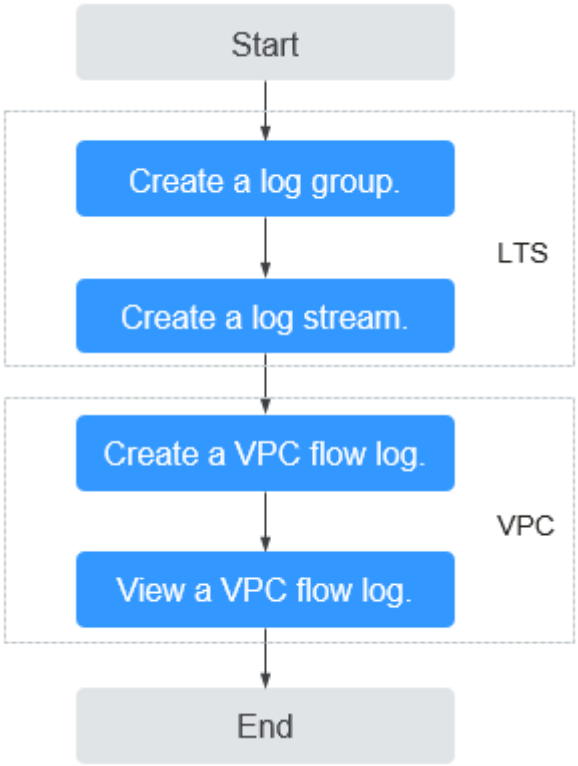
13.1 Visão geral de log de fluxo de VPC

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 ACLs da rede requerem modificação.

Atualmente, a função de log 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 13-1** mostra o processo de configuração dos logs de fluxo de VPC.

Figura 13-1 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.

Notes and Constraints

- 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.

13.2 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. 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, em **Rede**, 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 13-1 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.	All
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**.

13.3 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. 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, em **Rede**, 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: o seguinte é um exemplo de registro de log 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 ACCEPT 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: o seguinte 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: o seguinte é um exemplo de um registro de log de fluxo no qual os dados foram ignorados durante a janela de captura:

```
1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd - - -
- - - - 1431280876 1431280934 - SKIPDATA
```

Tabela 13-2 descreve os campos de um registro de log de fluxo.

Tabela 13-2 Descrição do campo de log

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 registrado.	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 rede. ● **REJECT**: o tráfego registrado foi permitido pelos grupos de segurança ou ACLs da rede.	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.

13.4 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. 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, em **Rede**, 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**.

13.5 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. 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, em **Rede**, 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.

14 Endereço IP virtual

14.1 Visão geral do endereço IP virtual

O que é um endereço IP virtual?

Um endereço IP virtual pode ser compartilhado entre múltiplos ECSs. Um ECS pode ter endereços IP privados e virtuais, e você pode acessar o ECS por meio de qualquer endereço IP. Um endereço IP virtual tem os mesmos recursos de acesso à rede que um endereço IP privado, incluindo comunicação de camada 2 e camada 3 em VPCs, acesso entre VPCs usando conexões de emparelhamento de VPC, bem como acesso por meio de EIPs, conexões de VPN e conexões Direct Connect.

Você pode vincular ECSs implementados no modo ativo/em espera com o mesmo endereço IP virtual e, em seguida, vincular um EIP ao endereço IP virtual. Os endereços IP virtuais podem trabalhar em conjunto com o Keepalived para garantir alta disponibilidade e recuperação de desastres. Se o ECS ativo estiver com defeito, o ECS em espera assumirá automaticamente os serviços do ativo.

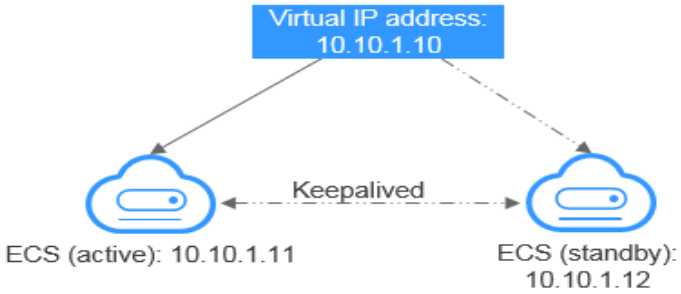
Rede

Os endereços IP virtuais são usados para alta disponibilidade e podem trabalhar em conjunto com o Keepalived para tornar possível a alternância do ECS ativo/em espera. Dessa forma, se um ECS for desativado por algum motivo, o outro poderá assumir o controle e os serviços continuarão ininterruptos. Os ECSs podem ser configurados para alta disponibilidade ou como clusters de balanceamento de carga.

- **Modo de rede 1**: alta disponibilidade

  Se você quiser melhorar a disponibilidade do serviço e evitar pontos únicos de falha, poderá implementar ECSs no modo ativo/em espera ou implementar um ECS ativo e vários ECSs em espera. Nesse arranjo, todos os ECSs usam o mesmo endereço IP virtual. Se o ECS ativo se tornar defeituoso, um ECS em espera assumirá os serviços do ECS ativo e os serviços continuarão ininterruptos.

Figura 14-1 Diagrama de rede do modo de alta disponibilidade

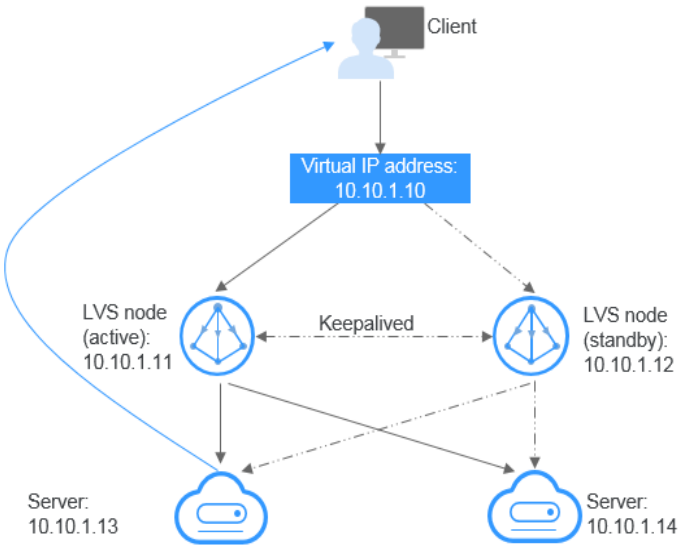


- Nessa configuração, um único endereço IP virtual é vinculado a dois ECSs na mesma sub-rede.
- Em seguida, o Keepalived é usado para configurar os dois ECSs para funcionar no modo ativo/em espera. Siga os padrões do setor para configurar o Keepalived. Os detalhes não estão incluídos aqui.

- **Modo de rede 2**: cluster de balanceamento de carga de alta disponibilidade

  Se você quiser criar um cluster de balanceamento de carga de alta disponibilidade, use o Keepalived e configure os nós do LVS como roteadores diretos.

  Figura 14-2 cluster de balanceamento de carga de alta disponibilidade



  - Vincule um único endereço IP virtual a dois ECSs.
  - Configure os dois ECSs como nós do LVS funcionando como roteadores diretos e use o Keepalived para configurar os nós no modo ativo/em espera. Os dois ECSs encaminharão solicitações uniformemente para servidores back-end diferentes.
  - Configure mais dois ECSs como servidores back-end.
  - Desative a verificação de origem/destino para os dois servidores back-end.
  - Verifique se a verificação de origem/destino está desativada nos ECSs LVS ativos e em espera. Para mais detalhes, consulte **Desativação da verificação de origem e destino (cenário de cluster de balanceamento de carga HA)**.

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.

Siga os padrões do setor para configurar o Keepalived. Os detalhes não estão incluídos aqui.

Cenários de aplicação

- Acesso ao endereço IP virtual por meio de um EIP

  Se a sua aplicação tiver requisitos de alta disponibilidade e precisar fornecer serviços pela Internet, é recomendável vincular um EIP a um endereço IP virtual.
- Uso de uma conexão de emparelhamento de VPN, Direct Connect ou VPC para acessar um endereço IP virtual

  Para garantir alta disponibilidade e acesso à Internet, use uma VPN para segurança e Direct Connect para uma conexão estável. A conexão de emparelhamento de VPC é necessária para que as VPCs na mesma região possam se comunicar entre si.

Observações e restrições

- Os endereços IP virtuais não são recomendados quando várias NICs na mesma sub-rede são configuradas em um ECS. É muito fácil haver conflitos de rota no ECS, o que causaria falha de comunicação usando o endereço IP virtual.
- Um endereço IP virtual só pode ser vinculado a ECSs na mesma sub-rede.
- O encaminhamento de IP deve ser desativado no ECS em espera. Para mais detalhes, consulte **Desativação de encaminhamento IP no ECS em espera**.
- Recomenda-se que não mais de oito endereços IP virtuais sejam vinculados a um ECS.
- Recomenda-se que não mais de 10 ECSs sejam vinculados a um endereço IP virtual.
- Os endereços IP virtuais e as NICs de extensão não podem ser usados para acessar diretamente os serviços da Huawei Cloud, como o DNS. Você pode usar o VPCEP para acessar esses serviços. Para obter detalhes, consulte **Compra de um ponto de extremidade de VPC**.

14.2 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. 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, em **Rede**, clique em **Virtual Private Cloud**.
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.

14.3 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. 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, em **Rede**, clique em **Virtual Private Cloud**.
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:

```
[[redacted] ~]#nmcli connection
NAME                UUID                                  TYPE      DEVICE
Wired connection 1  5e72ec5a-6165-3bd6-a34b-ce43981acb27  ethernet  eth0
docker0             cd351a91-c5eb-4b69-83eb-df092a2ccf6b  bridge    docker0
```


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.addresses172.16.0.125**
- Adicionar vários endereços IP virtuais: **nmcli connection modify "Wired connection 1" ipv4.addresses172.16.0.125,172.16.0.126**

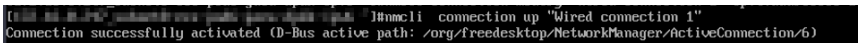
c. Execute o seguinte comando para que a configuração entre em vigor:

nmcli connection up "*CONNECTION***"**

Neste exemplo, execute o seguinte comando:

nmcli connection up "Wired connection 1"

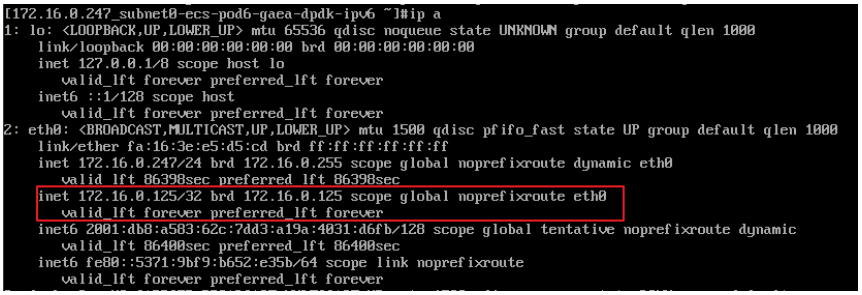
Informação semelhante à seguinte foi exibida:



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 **Network and Sharing Center** e clique na conexão local correspondente.

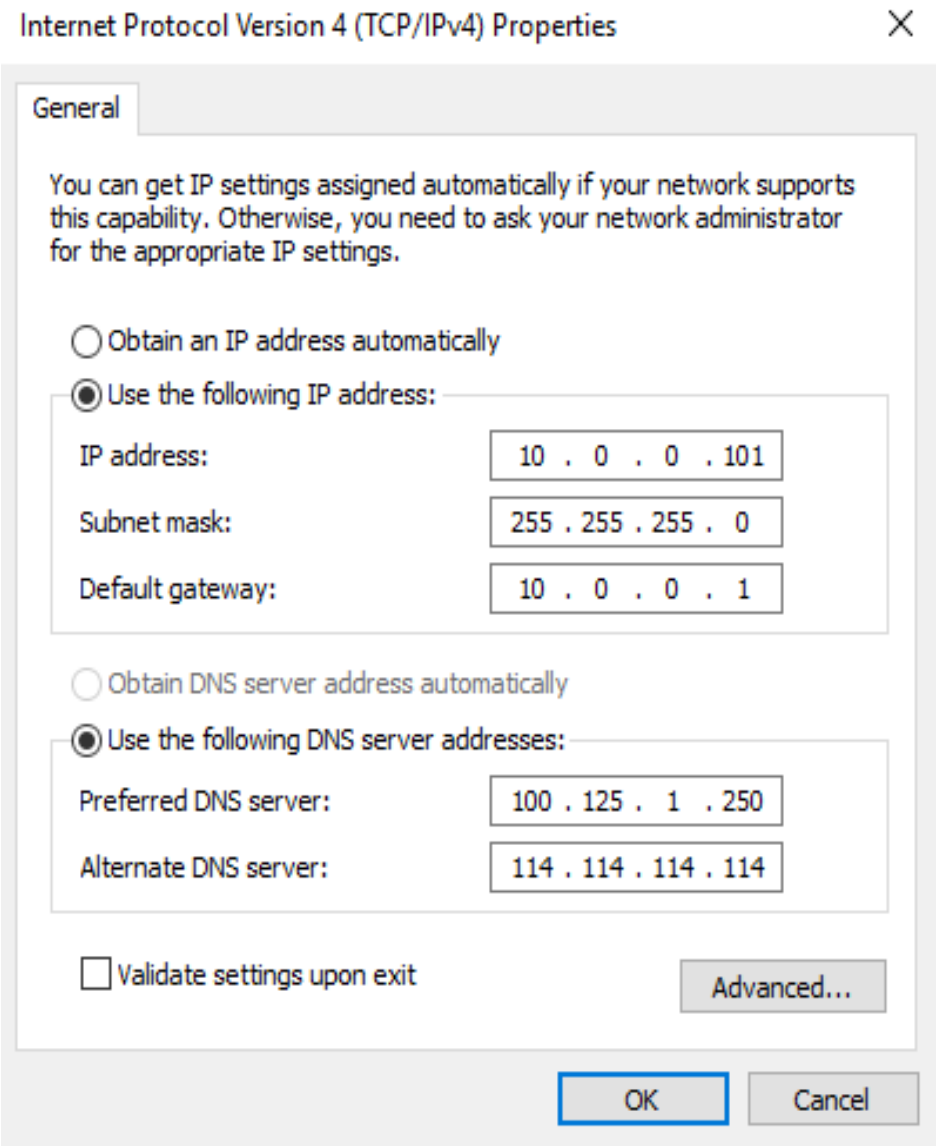
b. Na página exibida, clique em **Properties**.

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 14-3 Configurar o endereço IP privado

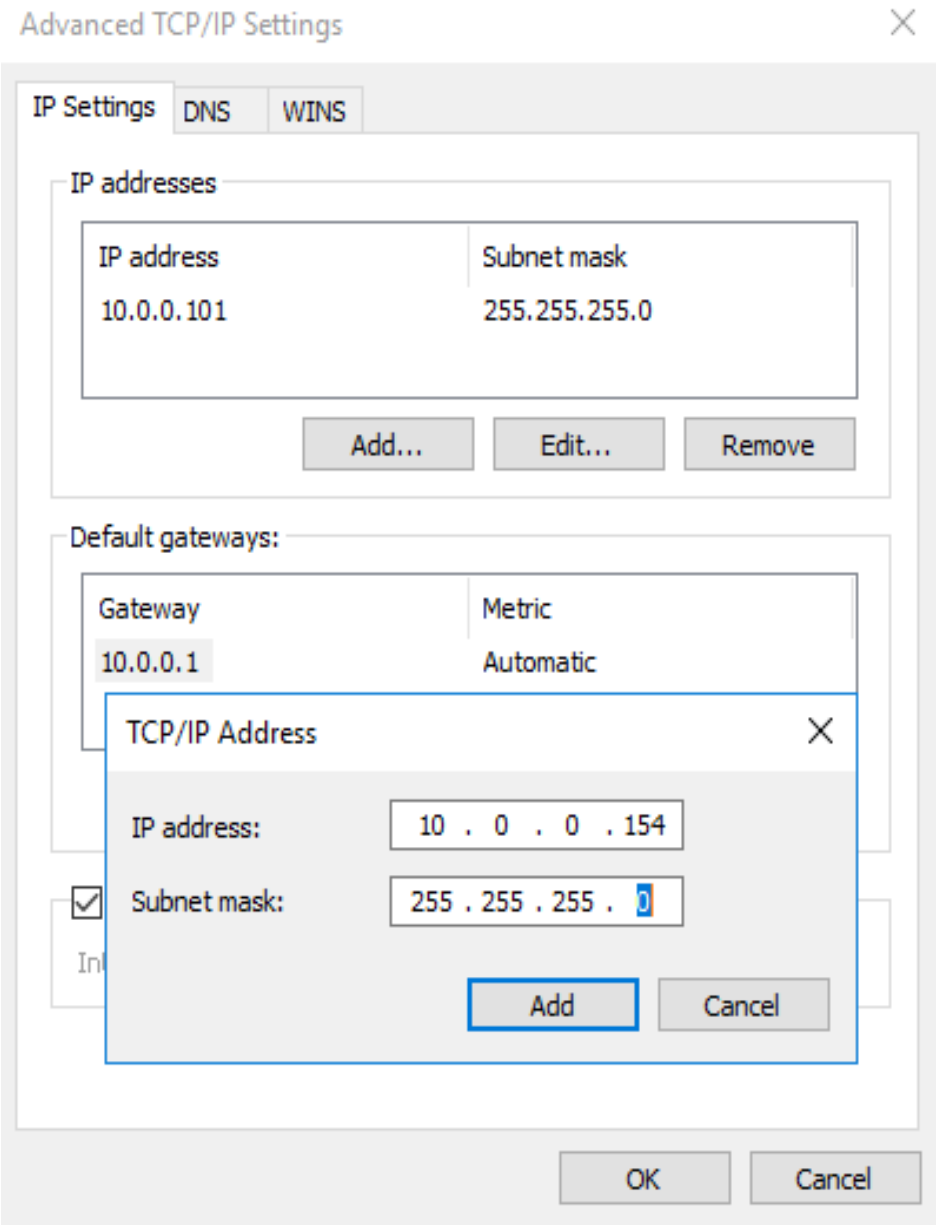


f. Clique em **Advanced**.

g. Na guia **IP Settings**, clique em **Add** na área **IP addresses**.

Adicione o endereço IP virtual. Por exemplo, 10.0.0.154.

Figura 14-4 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.

Links úteis

- **Por que o endereço IP virtual não pode ser pingado após ser vinculado a uma NIC do ECS?**
- **Quais são as diferenças entre EIP, endereço IP privado e endereço IP virtual?**

- **Desvinculação de um endereço IP virtual de um EIP**

14.4 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 **Rede** 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 **Rede**, 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**.

14.5 Acesso de um endereço IP virtual usando uma VPN

Procedimento

1. Configure a rede do ECS com base em **Rede**.
2. Crie uma VPN.

A VPN pode ser usada para acessar o endereço IP virtual do ECS.

14.6 Uso de uma conexão Direct Connect para acessar o endereço IP virtual

Procedimento

1. Configure a rede do ECS com base em **Rede**.
2. Crie uma conexão Direct Connect.

A conexão Direct Connect criada pode ser usada para acessar o endereço IP virtual do ECS.

14.7 Uso de uma conexão de emparelhamento de VPC para acessar o endereço IP virtual

Procedimento

1. Configure a rede do ECS com base em **Rede**.
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.

14.8 Desativação de encaminhamento IP no ECS em espera

Para um ECS do Linux:

1. Faça logon no ECS em espera e execute o seguinte comando para verificar se o encaminhamento de IP 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 a saída do comando for **1**, execute **2** e **3** para desabilitar o encaminhamento de IP.

   – Se a saída do comando for **0**, nenhuma ação adicional será necessária.
2. Use o editor vi para abrir o arquivo **/etc/sysctl.conf**, altere o valor de **net.ipv4.ip_forward** para **0** e insira **:wq** para salvar a alteração e sair. Você também pode usar o comando **sed** para modificar a configuração. Um exemplo de comando é o seguinte:

   sed -i '/net.ipv4.ip_forward/s/1/0/g' /etc/sysctl.conf
3. Execute o seguinte comando para que a alteração tenha efeito:

   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**.

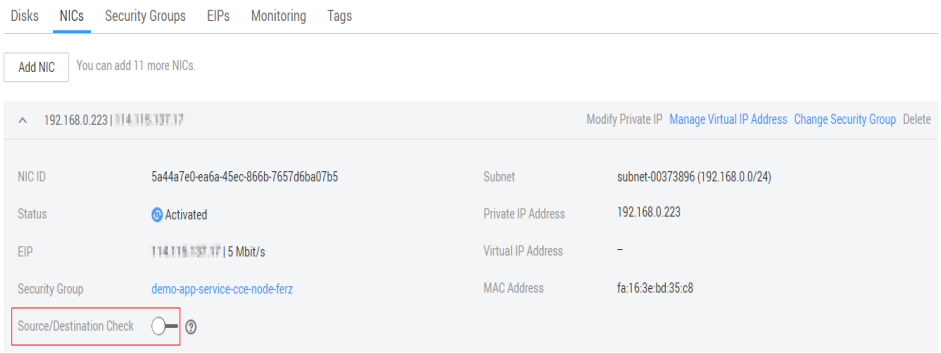
   – Se o valor for definido como **0**, o encaminhamento IP será desativado.

   – Se o valor for definido como **1**, o encaminhamento IP será ativado.

14.9 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 14-5 Desativar a verificação de origem/destino



14.10 Desvinculação de um endereço IP virtual de uma instância

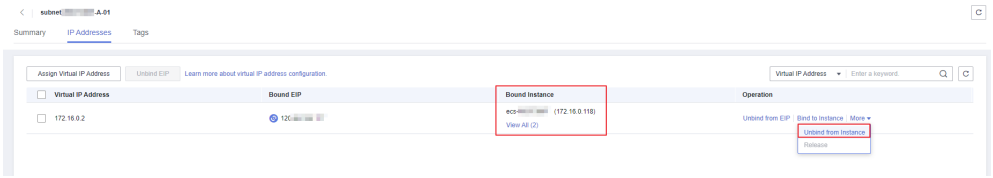
Cenários

Esta seção descreve como desvincular um endereço IP virtual de uma instância, como um ECS ou uma conexão de Camada 2.

Procedimento

1. 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, em **Rede**, clique em **Virtual Private Cloud**.
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.

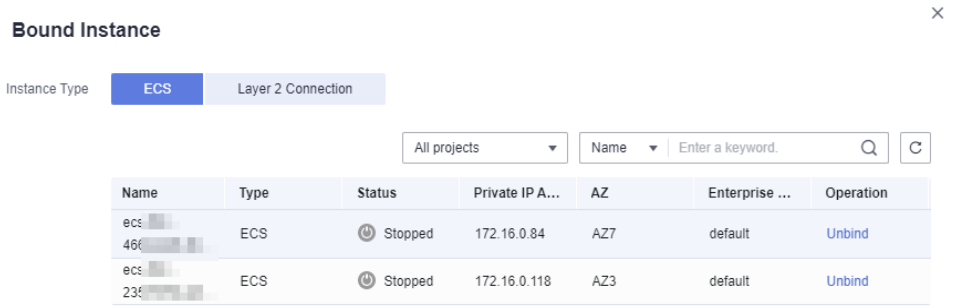
Figura 14-6 Endereços IP virtuais



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 14-7 Vincular instância



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**.

14.11 Desvinculação de um endereço IP virtual de um EIP

Cenários

Esta seção descreve como desvincular um endereço IP virtual de um EIP.

Procedimento

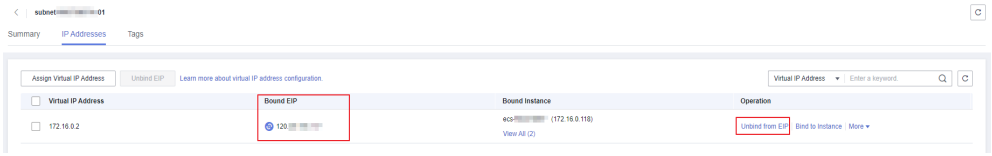
1. Faça logon no console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Na página inicial do console, em **Rede**, clique em **Virtual Private Cloud**.
4. No painel de navegação à esquerda, escolha **Virtual Private Cloud** > **Subnets**.

   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 14-8 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**.

14.12 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 14-1**.

Tabela 14-1 Liberar um endereço IP virtual que está sendo usado por um recurso

Mensagens	Análise de causa e solução
Figura 14-9: 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, uma conexão de camada 2 ou um ECS. Libere o endereço IP virtual.
Figura 14-10: 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 do RDS: **documentação do RDS** ● Instância do CCE: **documentação do CCE** ● Gateway de API: **documentação do gateway de API**

Figura 14-9 Cenário 1—O endereço IP virtual não pode ser excluído

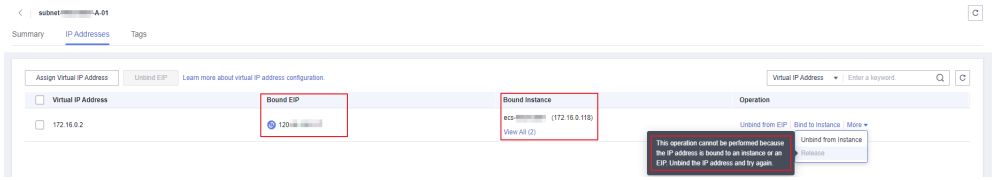
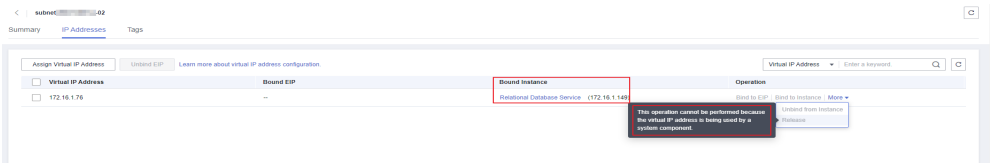


Figura 14-10 Cenário 2—O endereço IP virtual não pode ser excluído



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, em **Rede**, clique em **Virtual Private Cloud**.
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 14-11 Liberação de um endereço IP virtual

7. Confirme as informações e clique em **Yes**.

15 Interconexão com o CTS

15.1 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 15-1 lista as operações de VPC que podem ser gravadas pelo CTS.

Tabela 15-1 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

15.2 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.

16 Monitoramento

16.1 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 16-1 Métricas de EIP e largura de banda

ID	Nome	Descrição	Intervalo de valor	Objeto monitorado	Intervalo de monitoramento (dados brutos)
upstream_bandwidth	Outbound Bandwidth	Taxa de rede de tráfego de saída (anteriormente chamada de "Upstream Bandwidth") Unidade: bit/s	≥ 0 bit/s	Largura de banda ou EIP	1 minuto

ID	Nome	Descrição	Intervalo de valor	Objeto monitorado	Intervalo de monitoramento (dados brutos)
downstream_bandwidth	Inbound Bandwidth	Taxa de rede de tráfego de entrada (anteriormente chamada de "Downstream Bandwidth") Unidade: bit/s	≥ 0 bit/s	Largura de banda ou EIP	1 minuto
upstream_bandwidth_usage	Outbound Bandwidth Usage	Uso de largura de banda de saída na unidade de porcentagem.	0% a 100%	Largura de banda ou EIP	1 minuto
up_stream	Outbound Traffic	Tráfego de rede saindo da plataforma de nuvem em um minuto (anteriormente chamado de "Tráfego upstream") Unidade: byte	≥ 0 bytes	Largura de banda ou EIP	1 minuto
down_stream	Inbound Traffic	Tráfego de rede entrando na plataforma de nuvem em um minuto (anteriormente chamado de "Downstream Traffic") Unidade: byte	≥ 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
- Query monitoring metrics in batches:

  "dimensions": [

  {

  "name": "bandwidth_id",

  "value": "530cd6b0-86d7-4818-837f-935f6a27414d"

  }

  {

  "name": "publicip_id",

  "value": "3773b058-5b4f-4366-9035-9bbd9964714a"

  }

  ],

16.2 Exibição de métricas

Cenários

Você pode ver a largura de banda e o uso do EIP.

Você pode exibir a largura de banda de entrada, largura de banda de saída, uso da largura de banda de entrada, uso da largura de banda de saída, tráfego de entrada e tráfego de saída em um período especificado.

Procedimento (console do Cloud Eye)

1. Faça logon no 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. 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.

16.3 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. Faça logon no 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.

17 Gerenciamento de permissões

17.1 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 o pessoal com base na estrutura organizacional da sua empresa. Cada usuário do IAM tem suas próprias credenciais de identidade para acessar os recursos da VPC.
- Conceder aos usuários apenas as permissões necessárias para executar uma determinada tarefa com base em suas responsabilidades de trabalho.
- Confiar uma HUAWEI ID ou serviço de nuvem para executar O&M eficiente em seus recursos da VPC.

Se a sua HUAWEI ID cumprir os seus requisitos de permissões, pode ignorar esta secção.

Figura 17-1 mostra o fluxo do processo de concessão de permissões.

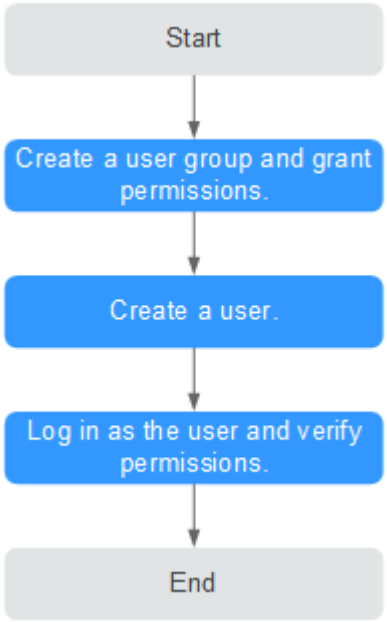
Pré-requisitos

Antes de conceder permissões a grupos de usuários, saiba mais sobre permissões (**Gerenciamento de permissões**) para VPC.

Para conceder permissões para outros serviços, saiba mais sobre todas as **permissões definidas pelo sistema** compatíveis com o IAM.

Fluxo do processo

Figura 17-1 Processo para conceder permissões da VPC



1. No console do IAM, **crie um grupo de usuários e atribua permissões a ele** (**VPC ReadOnlyAccess** como um exemplo).
2. **crie um grupo de usuários e atribua permissões a ele**.
3. **Efetue logon como o usuário do IAM** and verify permissions.

   Na região autorizada, execute as seguintes operações:

   – 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.

17.2 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 **Permissions Policies and Supported Actions**.

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 rascunho ou com base em uma política existente.

Para obter detalhes da operação, consulte **Criação de uma política personalizada**. 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:vpcs:list
                 "
            ]
        }
    ]
}
```

- Exemplo 2: negar a exclusão do 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"
        }
    ]
}
```

