

Virtual Private Cloud

Melhores práticas

Edição 01
Data 2024-09-20



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. Todos os direitos reservados.

Nenhuma parte deste documento pode ser reproduzida ou transmitida em qualquer forma ou por qualquer meio sem consentimento prévio por escrito da Huawei Cloud Computing Technologies Co., Ltd.

Marcas registadas e permissões



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

Aviso

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Índice

1 Planejamento de rede.....	1
2 Conectividade de VPC.....	5
3 Acesso de rede privada.....	9
4 Acesso de rede pública.....	13
5 Custos de rede mais baixos.....	18
6 Uso de um firewall de terceiros para limpar o tráfego de VPCs conectadas por conexões de emparelhamento de VPC.....	20
7 Uso de firewalls de terceiros ao conectar um data center local à nuvem.....	30
8 Implementação de contêineres que podem se comunicar uns com os outros em ECSs.....	35
9 Configuração de rotas baseadas em políticas para um ECS com várias NICs.....	39
9.1 Visão geral.....	39
9.2 Coleta de informações de rede do ECS.....	40
9.3 Configuração de rotas baseadas em políticas para um ECS do Linux com várias NICs (IPv4/IPv6).....	44
9.4 Configuração de rotas baseadas em políticas para um ECS do Windows com várias NICs (IPv4/IPv6).....	54

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.

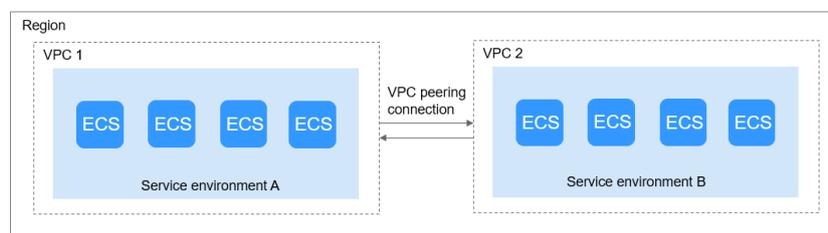
Única VPC

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.

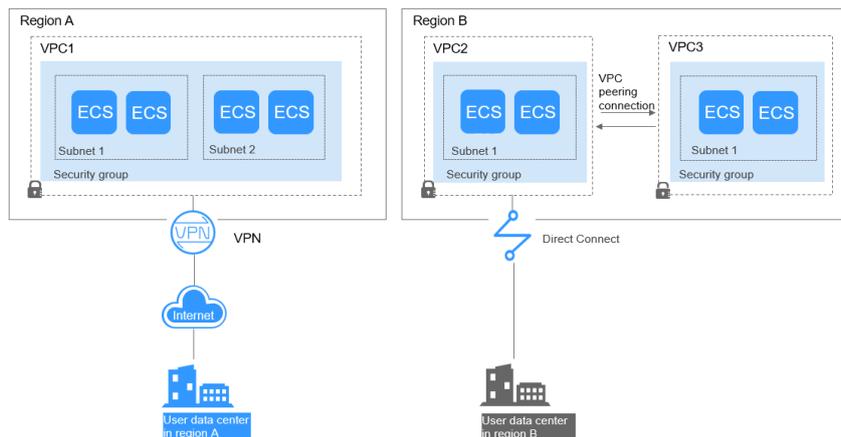
- Se não for necessário controlar explicitamente como cada sub-rede roteia o tráfego de entrada e saída, você poderá usar a tabela de rotas padrão.
- Se você precisar controlar explicitamente como cada sub-rede roteia o tráfego de entrada e saída em uma VPC, adicione rotas personalizadas à tabela de 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 [Guia de usuário do Elastic Load Balance](#).

2 Conectividade de VPC

Acessar a Internet

Os recursos de nuvem em uma VPC podem usar os seguintes serviços de nuvem para se conectar à Internet.

Tabela 2-1 Acessar a Internet

Serviço de nuvem	Cenários de aplicação	Descrição	Referência
EIP	Um único ECS acessa a Internet.	<p>Um EIP é um endereço IP estático que pode ser acessado diretamente através da Internet ou fornecer serviços acessíveis a partir da Internet.</p> <p>Um EIP pode ser vinculado a um ECS para permitir o acesso à Internet ou não vinculado para desativar o acesso.</p> <p>Larguras de banda compartilhadas e pacotes de dados compartilhados podem ser usados para reduzir custos.</p>	Configuração da VPC de ECSs que acessam a Internet usando EIPs

Serviço de nuvem	Cenários de aplicação	Descrição	Referência
NAT Gateway	Vários ECSs compartilham um EIP para acessar a Internet.	Um gateway da NAT oferecem tradução de endereço de rede de origem (SNAT) e tradução de endereço de rede de destino (DNAT). A SNAT permite que vários ECSs na mesma VPC compartilhem EIPs para acessar a Internet. Dessa forma, você pode reduzir os custos de gerenciamento e evitar que os EIPs dos ECSs sejam expostos à Internet. DNAT implementa o encaminhamento de dados em nível de porta. Ela mapeia portas EIP para portas ECS para que os ECSs em uma VPC possam compartilhar o mesmo EIP e largura de banda para fornecer serviços acessíveis pela Internet. No entanto, a DNAT não equilibra o tráfego.	Uso da SNAT para acessar a Internet Uso da DNAT para fornecer serviços acessíveis a partir da Internet
ELB	Use balanceadores de carga fornecidos pelo serviço ELB para distribuir uniformemente o tráfego de entrada entre vários ECSs em cenários de alta concorrência, como comércio eletrônico.	Os balanceadores de carga distribuem o tráfego entre vários ECSs de back-end, equilibrando a carga de trabalho em cada ECS (na Camada 4 ou na Camada 7). Você pode vincular EIPs a ECSs para permitir o acesso da Internet. O ELB expande os recursos de serviço das aplicações e melhora a disponibilidade eliminando pontos únicos de falha.	O que é ELB?

Conecta-se a VPCs

Você pode conectar VPCs usando os seguintes serviços de nuvem.

Tabela 2-2 Conecta-se a VPCs

Serviço de nuvem	Cenários de aplicação	Descrição	Referência
Emparelhamento de VPC	Conectar VPCs na mesma região.	Você pode solicitar uma conexão de emparelhamento de VPC com outra VPC na sua conta ou em outra conta, mas as duas VPCs devem estar na mesma região. As conexões de emparelhamento de VPC são gratuitas.	Criação de uma conexão de emparelhamento de VPC com uma outra VPC na sua conta Criação de uma conexão de emparelhamento de VPC com uma VPC em outra conta
VPN	Usar a VPN para conectar VPCs entre regiões a baixo custo.	A VPN usa um túnel de comunicação criptografado para conectar VPCs em diferentes regiões e enviar tráfego pela Internet. É barata, fácil de configurar e fácil de usar. No entanto, as conexões de VPN serão afetadas pela qualidade da Internet.	Conexão a uma VPC por meio de uma VPN

Conectar-se a um data center no local (IDC)

Se você tiver um data center local e não quiser migrar todos os seus serviços para a nuvem, poderá criar uma nuvem híbrida para manter os dados principais em seu data center.

Tabela 2-3 Conectar-se a um data center local

Serviço de nuvem	Cenários de aplicação	Descrição	Referência
VPN	Usar a VPN para conectar uma VPC a um data center local a baixo custo.	A VPN usa um túnel de comunicação criptografado para conectar uma VPC na nuvem a um data center local e enviar tráfego pela Internet. É barata, fácil de configurar e fácil de usar. No entanto, as conexões de VPN serão afetadas pela qualidade da Internet.	Conexão a uma VPC por meio de uma VPN

Serviço de nuvem	Cenários de aplicação	Descrição	Referência
Direct Connect	Usar uma conexão física para conectar uma VPC a um data center local.	A Direct Connect fornece conexões físicas entre VPCs e data centers. Possui baixa latência e é muito seguro. A Direct Connect é uma boa escolha se você tiver requisitos rigorosos sobre a qualidade e segurança de transmissão de rede.	Acesso de várias VPCs usando uma conexão

3 Acesso de rede privada

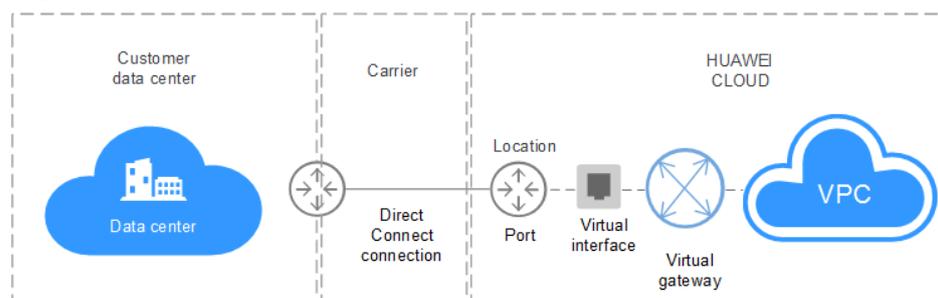
Conectar-se a um data center local

Você pode conectar uma VPC ao seu data center local. Depois de estabelecer essa conexão segura e confiável, você poderá migrar em escala para a Huawei Cloud, uma nuvem com recursos de computação, armazenamento e rede massivos. Com a Huawei Cloud, você não será afetado por flutuações súbitas na demanda por serviços. Tanto a Direct Connect quanto a VPN são compatíveis com as conexões entre seu data center e suas VPCs na nuvem.

- Direct Connect

A Direct Connect fornece conexões de rede dedicadas de alta velocidade, estáveis e seguras que conectam seus data centers a VPCs. Com a Direct Connect, você pode conectar computadores em seu data center local a servidores em nuvem ou servidores de hospedagem na Huawei Cloud. Ela maximiza as capacidades de computação em nuvem e as instalações de TI existentes para construir um ambiente de computação em nuvem híbrida flexível e escalável.

Figura 3-1 Conectar-se a um data center local com uma conexão Direct Connect



- VPN

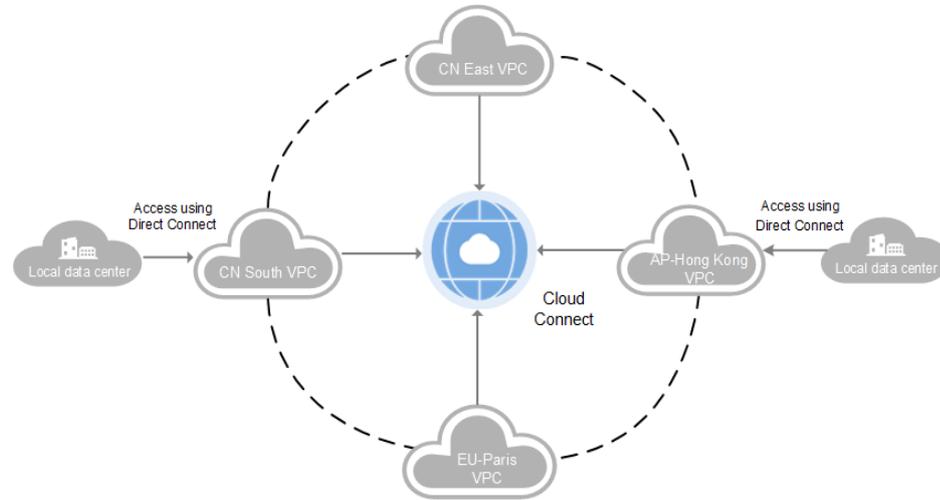
VPN estabelece um túnel de comunicações seguro e criptografado entre seu data center local e sua VPC na Huawei Cloud. Com a VPN, você pode se conectar a uma VPC e acessar os recursos implementados nela.

Conectar VPCs e data centers com a Cloud Connect

A Cloud Connect permite que você crie rapidamente redes de alta qualidade que possam conectar VPCs em regiões e trabalhar com a Direct Connect para conectar VPCs e data centers locais.

Com a Cloud Connect, você pode construir uma rede de nuvem globalmente conectada com capacidade de escalabilidade e comunicação de classe empresarial.

Figura 3-2 Conectar VPCs e data centers com a Cloud Connect



Conectar VPCs

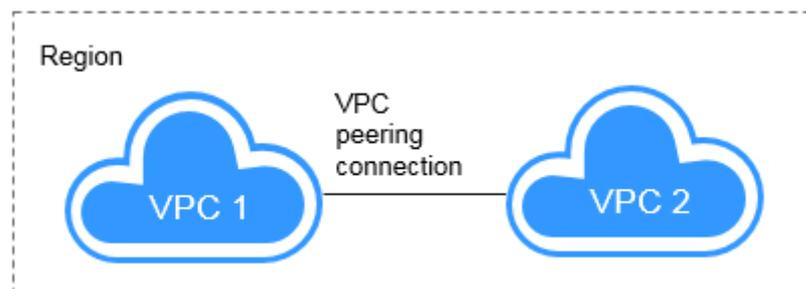
Se você quiser conectar VPCs na mesma região, use conexões de emparelhamento de VPC.

Se você quiser conectar VPCs em regiões diferentes e criar uma rede de serviços entre regiões, use a Direct Connect, VPN ou Cloud Connect.

- **Emparelhamento de VPC**

Você pode usar conexões de emparelhamento de VPC para conectar VPCs na mesma região.

Figura 3-3 Conectar VPCs na mesma região com uma conexão de emparelhamento de VPC

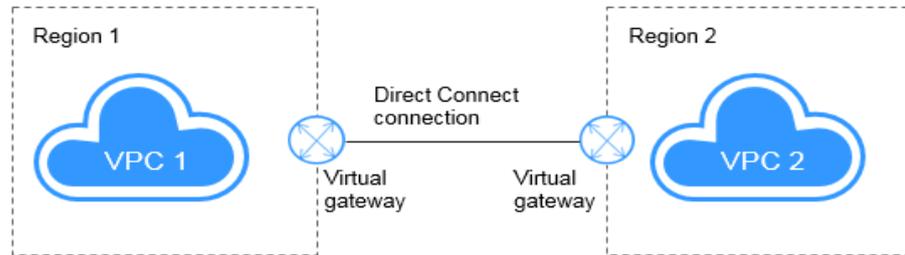


- **Direct Connect**

A Direct Connect fornece conexões de rede dedicadas de alta velocidade, estáveis e seguras que conectam seus data centers a VPCs. Com a Direct Connect, você pode conectar computadores em seu data center local a servidores em nuvem ou servidores de hospedagem na Huawei Cloud. Ela maximiza as capacidades de computação em nuvem e as instalações de TI existentes para construir um ambiente de computação em nuvem

híbrida flexível e escalável. A Direct Connect também pode ser usado para conectar VPCs em diferentes regiões.

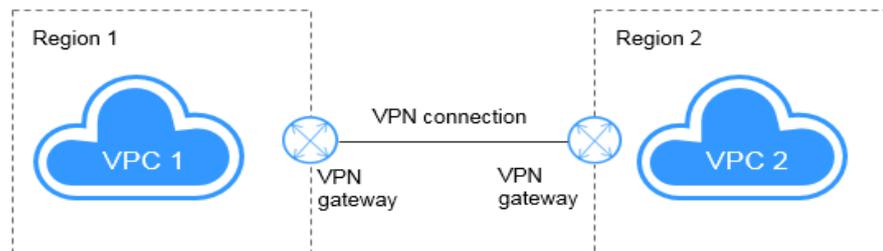
Figura 3-4 Conectar VPCs em diferentes regiões com a Direct Connect



- VPN

VPN estabelece um túnel de comunicações seguro e criptografado entre seu data center local e sua VPC na Huawei Cloud. Com a VPN, você pode se conectar a uma VPC e acessar os recursos implantados nela. A VPN pode conectar VPCs em diferentes regiões.

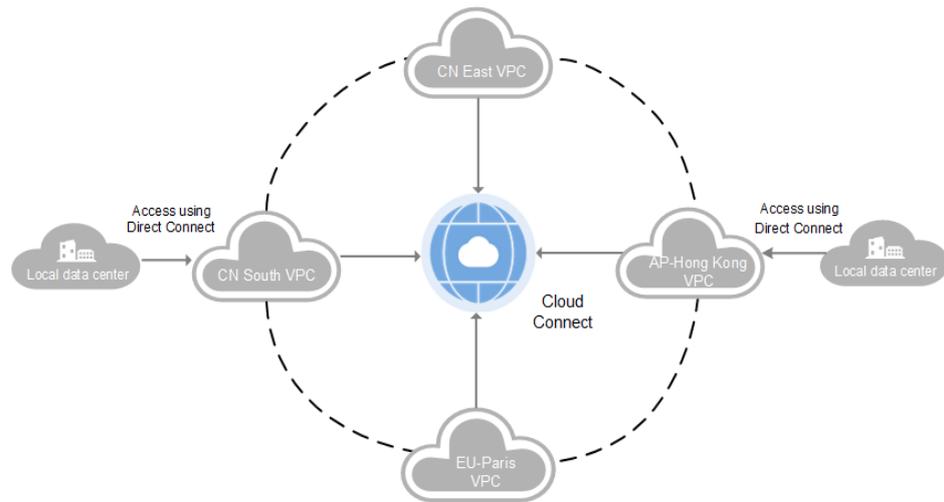
Figura 3-5 Conectar VPCs em diferentes regiões com VPN



- Cloud Connect

A Cloud Connect permite que você crie rapidamente redes de alta qualidade que possam conectar VPCs em regiões e trabalhe com a Direct Connect para conectar VPCs e data centers locais. Com a Cloud Connect, você pode construir uma rede de nuvem globalmente conectada com capacidade de escalabilidade e comunicação de classe empresarial.

Figura 3-6 Conectar VPCs em diferentes regiões com a Cloud Connect



4 Acesso de rede pública

Produtos

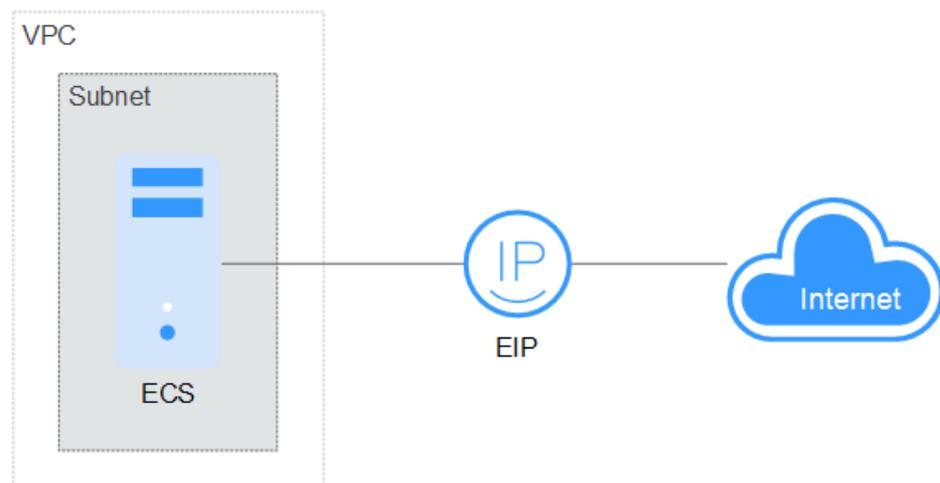
Serviços de nuvem, como EIP, NAT Gateway e ELB, podem ser usados para se conectar à Internet.

- EIP
O serviço EIP fornece endereços IP públicos independentes e largura de banda para o acesso à Internet. Os EIPs 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.
- ELB
O ELB distribui o tráfego de acesso entre vários ECSs para equilibrar a carga de aplicação, melhorando a tolerância a falhas e expandindo as capacidades de serviço das aplicações. Você pode criar um balanceador de carga, configurar um protocolo de escuta e uma porta e adicionar servidores de back-end a um balanceador de carga. Você também pode verificar o estado de execução dos servidores de back-end para garantir que as solicitações sejam enviadas apenas para servidores saudáveis.
- NAT Gateway
NAT Gateway fornece SNAT e DNAT para seus recursos em uma VPC, e permite que os servidores na sua VPC acessem ou ofereçam serviços acessíveis pela Internet.

Fornecer serviços acessíveis a partir da Internet

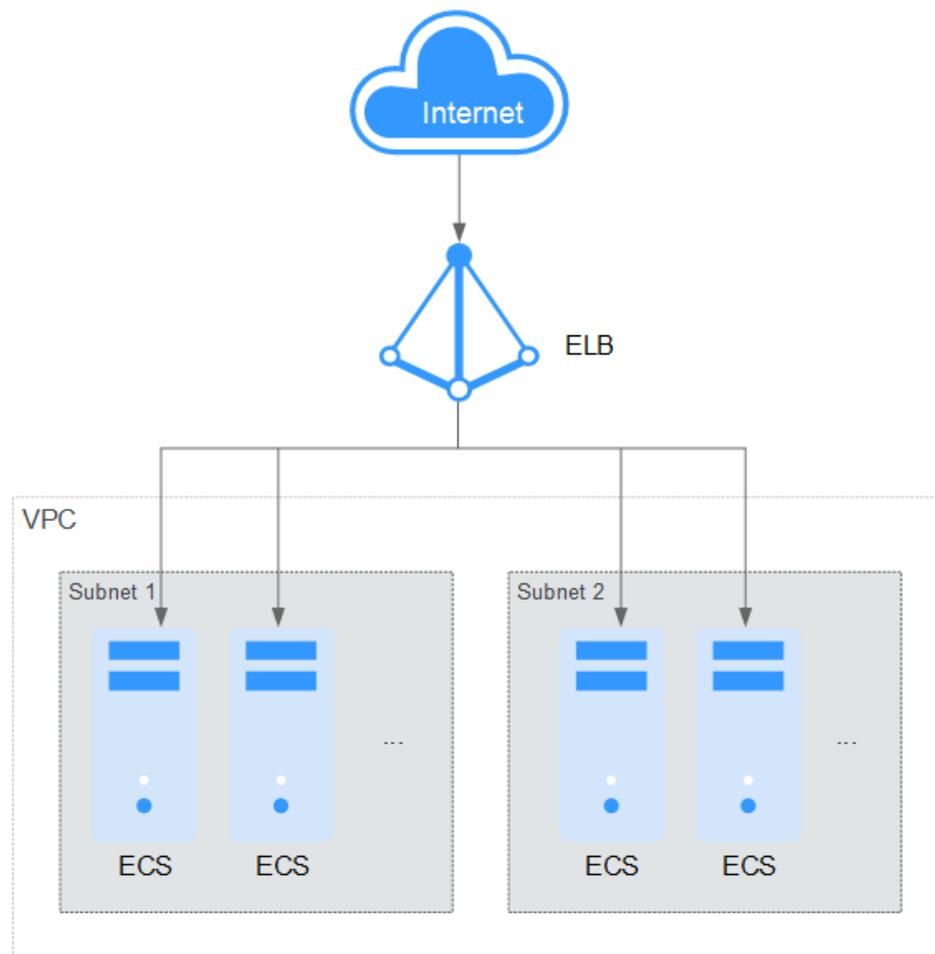
- O ECS único fornece serviços acessíveis a partir da Internet.
Se você tiver apenas uma aplicação e o tráfego de serviço for pequeno, poderá atribuir um EIP e vinculá-lo ao ECS para que o ECS possa fornecer serviços acessíveis pela Internet.

Figura 4-1 EIP



- Vários ECSs equilibram cargas de trabalho.
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 se integra profundamente ao serviço Auto Scaling (AS), que permite o dimensionamento automático com base no tráfego do serviço e garante a estabilidade e a confiabilidade do serviço.

Figura 4-2 ELB

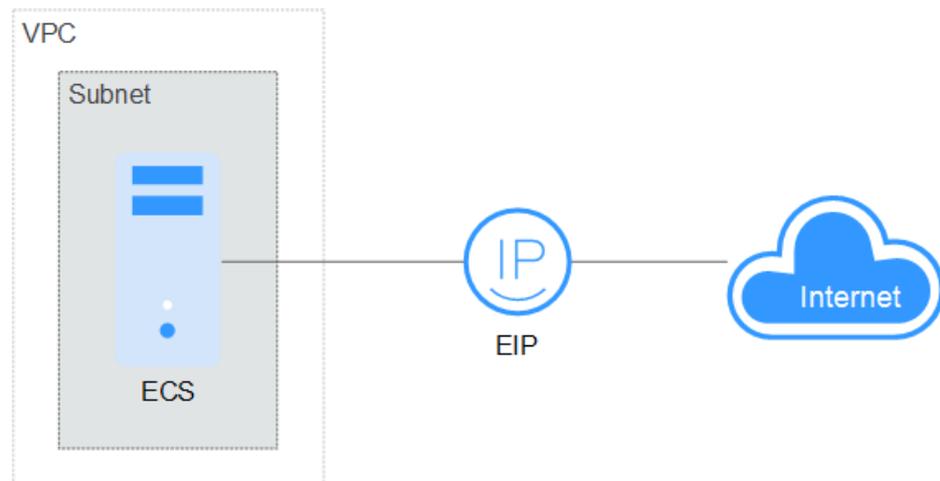


Acessar a Internet

- Um único ECS acessa a Internet.

Quando um ECS precisa acessar a Internet, você pode vincular um EIP ao ECS para que o ECS possa acessar a Internet. A Huawei Cloud permite que seu EIP seja cobrado com base no uso da largura de banda ou na quantidade de tráfego. Se você não precisar usar o EIP, poderá desvinculá-lo de forma flexível.

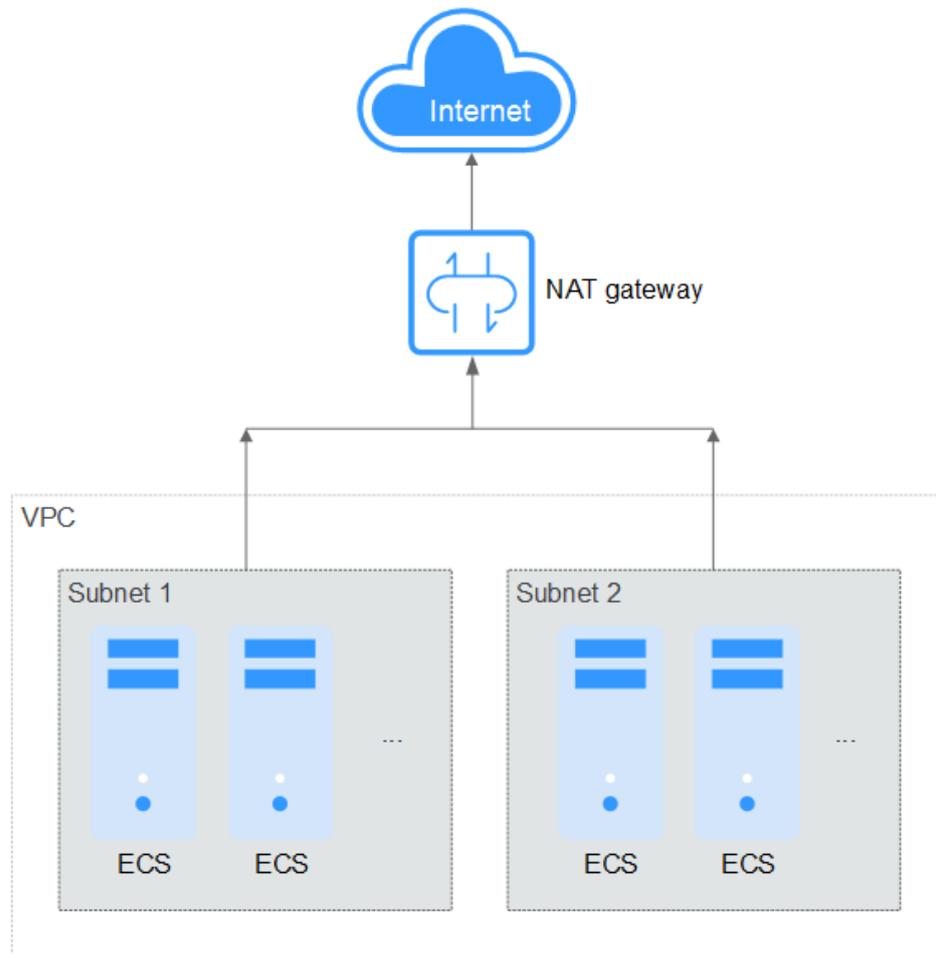
Figura 4-3 EIP



- Vários ECSs acessam a Internet.

Se vários ECSs na VPC precisarem acessar a Internet, você poderá usar um gateway NAT e configurar regras SNAT por sub-rede para permitir que os ECSs na VPC acessem a Internet. Se você acessar a Internet usando um EIP, mas sem regras de DNAT configuradas, os usuários externos não poderão acessar diretamente o endereço de rede pública do gateway NAT pela Internet, garantindo a segurança do ECS.

Figura 4-4 Gateway NAT



5 Custos de rede mais baixos

Você pode selecionar um produto adequado e modo de faturamento com base em seus requisitos de serviço.

Largura de banda dedicada

Se você quiser garantir a largura de banda disponível para um determinado EIP, é aconselhável comprar largura de banda dedicada. A largura de banda dedicada só pode ser usada para um único EIP específico. A largura de banda dedicada não é afetada por outros serviços.

Um EIP pode ser cobrado por largura de banda ou por tráfego:

- Largura de banda se seus serviços usam uma grande quantidade de tráfego, mas são estáveis, um EIP cobrado por largura de banda é recomendado.
- Tráfego: se seus serviços usam apenas uma quantidade relativamente pequena de tráfego, um EIP cobrado por tráfego combinado com um pacote de dados compartilhado é recomendado por um preço mais favorável.

Se o seu tráfego é estável, a cobrança anual/mensal com base na largura de banda é mais rentável.

Largura de banda compartilhada

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. Vários EIPs cujo modo de cobrança é pagamento por uso podem ser adicionados a uma largura de banda compartilhada. Você pode vincular EIPs a produtos como ECSs, gateways NAT e balanceadores de carga para que esses produtos possam usar a largura de banda compartilhada.

Pacote de dados compartilhado

Um pacote de dados compartilhado é um pacote pré-pago para tráfego de rede pública. O preço do pacote é menor do que o do faturamento pós-pago por tráfego. Pacotes de dados compartilhados reduzem muito o custo do tráfego em uma rede pública. Um pacote de dados compartilhado entra em vigor imediatamente após a compra e nenhuma operação adicional é

necessária. Se você se inscreveu em EIPs de pagamento por uso usando largura de banda cobrada por tráfego em uma região e comprou um pacote de dados compartilhado na mesma região, os EIPs usarão o pacote de dados compartilhados.

- Quando usar um pacote de dados compartilhado

Depois que um pacote de dados compartilhado entra em vigor para uma largura de banda faturada pelo tráfego, o tráfego usado pela largura de banda é deduzido do pacote de dados compartilhados primeiro. Depois que o pacote de dados compartilhado é usado, a largura de banda é faturada pela quantidade de tráfego usada. Um pacote de dados compartilhado economiza mais se a quantidade de tráfego usada for enorme.

- Observações adicionais sobre pacotes de dados compartilhados

- Somente o tráfego gerado na região selecionada quando o pacote de dados compartilhado é comprado pode ser deduzido.
- Pacotes de dados compartilhados dinâmicos e estáticos são usados para deduzir o tráfego gerado pelos EIPs do BGP dinâmico e BGP estático, respectivamente.
- Um pacote de dados compartilhados tem um período de validade de um mês ou um ano a partir da data da compra. Após esse período expirar, o tráfego não utilizado também expira e não pode ser usado. É aconselhável avaliar o tamanho de um pacote de dados compartilhados necessário com base no histórico de uso.
- Se você ativar a função de renovação automática para um pacote de dados compartilhado, o sistema tentará renovar automaticamente a assinatura dentro de sete dias antes que o pacote de dados compartilhado expire. Após a renovação ser bem-sucedida, o tráfego restante no pacote de dados compartilhado pode ser usado dentro do novo período de validade.
- Depois que um pacote de dados compartilhado é usado, seu serviço não será interrompido automaticamente. O sistema fatura automaticamente com base no tráfego, garantindo a disponibilidade do sistema de serviço.

6

Uso de um firewall de terceiros para limpar o tráfego de VPCs conectadas por conexões de emparelhamento de VPC

Cenário de aplicação

A VPC permite configurar e gerenciar redes virtuais. Você pode usar grupos de segurança e network ACLs para controlar o acesso à rede. Você também pode usar firewalls de terceiros para garantir a segurança dos serviços em nuvem.

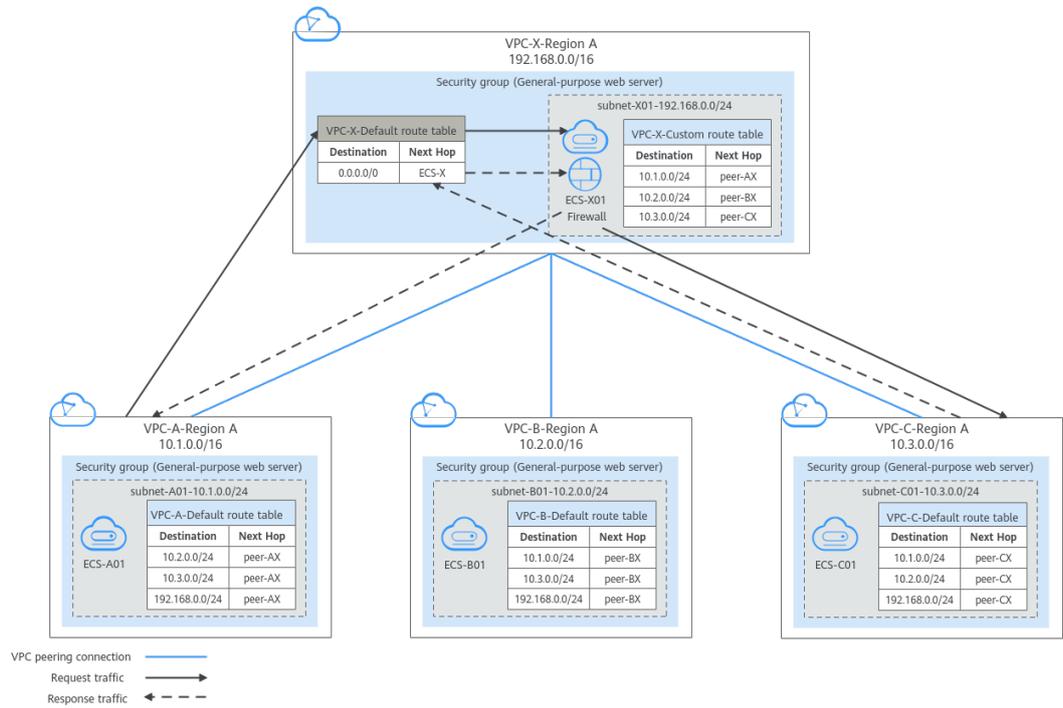
Esta seção descreve como usar um firewall para limpar o tráfego entre VPCs conectadas usando conexões de emparelhamento de VPC.

Arquitetura

Neste exemplo, os serviços são implementados em VPC-A, VPC-B e VPC-C, e o firewall é implantado em VPC-X. Essas VPCs se comunicam entre si por meio de conexões de emparelhamento de VPC. O tráfego entre VPC-A, VPC-B e VPC-C deve fluir através do firewall no VPC-X. A tabela de rotas padrão do VPC-X direciona todo o tráfego de entrada para o firewall. Depois de ser limpo pelo firewall, o tráfego é enviado para uma VPC de serviço com base na tabela de rotas personalizada.

Figura 6-1 mostra como o ecs-A01 acessa o ecs-C01. Você pode ver os caminhos de tráfego de solicitação e resposta.

Figura 6-1 Planejamento de rede quando um firewall de terceiros é usado para limpar o tráfego entre VPCs



Planejamento de recursos

Neste exemplo, você precisa criar VPCs, ECSs e conexões de emparelhamento de VPC. Para obter detalhes sobre os recursos necessários, consulte [Tabela 6-1](#).

NOTA

Os seguintes detalhes de planejamento de recursos são apenas exemplos para sua referência. Você precisa planejar recursos com base nos requisitos reais de serviço.

Tabela 6-1 Recursos necessários

Recurso	Descrição
VPC	<p>Tabela 6-2 mostra detalhes sobre as VPCs necessárias.</p> <p>Neste exemplo, há quatro VPCs, incluindo três VPCs em que os serviços são implantados e uma VPC em que o firewall é implantado. Essas VPCs são da mesma região e seus blocos CIDR de sub-rede não se sobrepõem.</p> <ul style="list-style-type: none"> ● Os serviços são implantados em VPC-A, VPC-B e VPC-C, e o firewall é implantado em VPC-X. Essas VPCs se comunicam entre si por meio de conexões de emparelhamento de VPC. ● VPC-A, VPC-B, VPC-C e VPC-X têm uma sub-rede. ● As sub-redes de VPC-A, VPC-B, VPC-C estão associadas à sua tabela de rotas padrão. ● A VPC X tem uma tabela de rota padrão e uma tabela de rota personalizada. A sub-rede da VPC X é associada à tabela de rotas personalizada. <p>A tabela de rotas padrão controla o tráfego de entrada para a VPC-X e a tabela de rotas personalizada controla o tráfego de saída da VPC-X.</p> <p>AVISO Os blocos CIDR de sub-rede das VPCs que precisam se comunicar entre si por meio de uma conexão de emparelhamento de VPC não podem se sobrepor. Caso contrário, a conexão de emparelhamento da VPC não terá efeito.</p>
ECS	<p>Tabela 6-3 mostra detalhes sobre os ECSs necessários.</p> <p>Os quatro ECSs estão em VPCs diferentes. Se os ECSs estiverem em grupos de segurança diferentes, adicione regras aos grupos de segurança para permitir o acesso entre eles.</p>
Conexão de emparelhamento de VPC	<p>Tabela 6-4 mostra detalhes sobre as conexões de emparelhamento de VPC necessárias.</p> <p>Há três conexões de emparelhamento de VPC.</p> <ul style="list-style-type: none"> ● peer-AX: conecta VPC-A e VPC-X ● peer-BX: conecta VPC-B e VPC-X ● peer-CX: conecta VPC-C e VPC-X <p>As conexões de emparelhamento de VPC são transitivas. Depois que as rotas são configuradas, VPC-A, VPC-B e VPC-C podem se comunicar entre si por meio do VPC-X.</p>

Tabela 6-2 Detalhes da VPC

Nome da VPC	Bloco CIDR da VPC	Nome da sub-rede	Bloco CIDR da sub-rede	Tabela de rotas	A sub-rede é usada para implementar
VPC-A	10.1.0.0/16	subnet-A01	10.1.0.0/24	Tabela de rota padrão	Serviços

Nome da VPC	Bloco CIDR da VPC	Nome da sub-rede	Bloco CIDR da sub-rede	Tabela de rotas	A sub-rede é usada para implementar
VPC-B	10.2.0.0/16	subnet-B01	10.2.0.0/24	Tabela de rota padrão	Serviços
VPC-C	10.3.0.0/16	subnet-C01	10.3.0.0/24	Tabela de rota padrão	Serviços
VPC-X	192.168.0.0/16	subnet-X01	192.168.0.0/24	Tabela de rota personalizada	Firewall

Tabela 6-3 Detalhes do ECS

Nome do ECS	Nome da VPC	Nome da sub-rede	Endereço IP privado	Imagem	Grupo de segurança	ECS é usado para implementar
ecs-A01	VPC-A	subnet-A01	10.1.0.139	Imagem pública: CentOS 8.2 64bit	sg-demo: servidor Web de uso geral	Serviços
ecs-B01	VPC-B	subnet-B01	10.2.0.93			Serviços
ecs-C01	VPC-C	subnet-C01	10.3.0.220			Serviços
ecs-X01	VPC-X	subnet-X01	192.168.0.5			Firewall

Tabela 6-4 Detalhes da conexão de emparelhamento de VPC

Nome da conexão	VPC local	VPC de par
peer-AX	VPC-A	VPC-X
peer-BX	VPC-B	VPC-X
peer-CX	VPC-C	VPC-X

Configuração da rota

Você precisa adicionar rotas às tabelas de rotas da VPC para permitir a comunicação entre VPCs e limpar o tráfego por meio do firewall. Para mais detalhes, consulte [Tabela 6-5](#).

 **NOTA**

As rotas a seguir são apenas exemplos para sua referência. Você precisa planejar rotas com base nos requisitos reais de serviço.

Tabela 6-5 Tabelas de rotas necessárias

Tabela de rotas	Descrição
Tabelas de rotas de VPCs de serviço	<p>Tabela 6-6 mostra detalhes sobre tabelas de rotas de VPCs de serviço. As tabelas de rotas padrão de VPC-A, VPC-B e VPC-C têm rotas com destinos definidos para outras sub-redes da VPC e com o próximo salto definido para conexão de emparelhamento de VPC.</p>
Tabelas de roteamento do firewall de VPC	<p>Tabela 6-6 mostra detalhes sobre tabelas de rotas do firewall de VPC-X.</p> <ol style="list-style-type: none">Na tabela de rotas padrão da VPC-X:<ul style="list-style-type: none">Se o firewall for implementado em um ECS, adicione uma rota com destino definido como 0.0.0.0/0 e o próximo salto definido como ecs-X01 para direcionar o tráfego para o ECS com o firewall implementado.Se o firewall for implantado em dois ECSs e os ECSs se comunicarem com sistemas externos por meio de um endereço IP virtual, o endereço IP virtual será alternado dinamicamente para o ECS em espera para continuar fornecendo serviços quando o ECS ativo estiver com defeito e não puder fornecer serviços. Nesse cenário, adicione uma rota com o destino definido como 0.0.0.0/0 e o próximo salto definido como o endereço IP virtual para direcionar o tráfego para o ECS com o firewall implementado.<p>Neste exemplo, o firewall é implementado em um ECS. O tráfego na VPC-A, VPC-B e VPC-C precisa passar pela VPC-X e ser direcionado ao firewall para anulação.</p>Na tabela de rotas personalizadas do VPC-X, adicione rotas com destino definido para VPCs de blocos de serviço CIDR de sub-rede (VPC-A, VPC-B e VPC-C) e o próximo salto definido para a conexão de emparelhamento de VPC.

Tabela 6-6 Detalhes sobre tabelas de rotas de VPCs de serviço

N o m e d a V P C	Tabela de rotas	Destino	Tipo de próximo salto	Próximo salto	Tipo de rota	Função de rota
VPC-A	Tabela de rotas padrão: rtb-vpc-A	10.2.0.0/24	Conexão de emparelhamento de VPC	peer-AX	Personalizada	<ul style="list-style-type: none"> ● Destino: subnet-B01 na VPC-B ● Conecta a subnet-A01 à subnet-B01
		10.3.0.0/24	Conexão de emparelhamento de VPC	peer-AX	Personalizada	<ul style="list-style-type: none"> ● Destino: subnet-C01 na VPC-C ● Conecta a subnet-A01 à subnet-C01
		192.168.0.0/24	Conexão de emparelhamento de VPC	peer-AX	Personalizada	<ul style="list-style-type: none"> ● Destino: subnet-X01 na VPC-X ● Conecta a subnet-A01 à subnet-X01
VPC-B	Tabela de rotas padrão: rtb-vpc-B	10.1.0.0/24	Conexão de emparelhamento de VPC	peer-BX	Personalizada	<ul style="list-style-type: none"> ● Destino: subnet-A01 na VPC-A ● Conecta a subnet-A01 à subnet-B01
		10.3.0.0/24	Conexão de emparelhamento de VPC	peer-BX	Personalizada	<ul style="list-style-type: none"> ● Destino: subnet-C01 na VPC-C ● Conecta a subnet-B01 à subnet-C01
		192.168.0.0/24	Conexão de emparelhamento de VPC	peer-BX	Personalizada	<ul style="list-style-type: none"> ● Destino: subnet-X01 na VPC-X ● Conecta a sub-rede-B01 à sub-rede-X01
VPC-C	Tabela de rotas padrão: rtb-vpc-C	10.1.0.0/24	Conexão de emparelhamento de VPC	peer-CX	Personalizada	<ul style="list-style-type: none"> ● Destino: subnet-A01 na VPC-A ● Conecta a subnet-A01 à subnet-C01

Nome da VPC	Tabela de rotas	Destino	Tipo de próximo salto	Próximo salto	Tipo de rota	Função de rota
		10.2.0.0/24	Conexão de emparelhamento de VPC	peer-CX	Personalizada	<ul style="list-style-type: none"> ● Destino: subnet-B01 na VPC-B ● Conecta a subnet-B01 à subnet-C01
		192.168.0.0/24	Conexão de emparelhamento de VPC	peer-CX	Personalizada	<ul style="list-style-type: none"> ● Destino: subnet-X01 na VPC-X ● Conecta a subnet-C01 à subnet-X01

Tabela 6-7 Detalhes sobre tabelas de rotas do firewall de VPC

Nome da VPC	Tabela de rotas	Destino	Tipo de próximo salto	Próximo salto	Tipo de rota	Função de rota
VPC-X	Tabela de rotas padrão: rtb-vpc-X	0.0.0.0/0	Servidor	ECS-X	Personalizada	<ul style="list-style-type: none"> ● Destino: ecs-X com firewall implementado ● Tráfego de entrada direto da VPC-X para o firewall. <p>Se o firewall estiver implementado em vários ECSs e esses ECSs se comunicarem com redes externas por meio de um endereço IP virtual, defina o próximo salto da rota para o endereço IP virtual.</p>
	Tabela de rotas personalizada: rtb-vpc-custom-X	10.1.0.0/24	Conexão de emparelhamento de VPC	peer-AX	Personalizada	<ul style="list-style-type: none"> ● Destino: subnet-A01 na VPC-A ● Conecta a subnet-A01 à subnet-X01

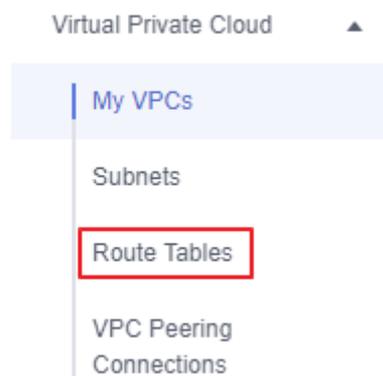
No me da VPC	Tabela de rotas	Destino	Tipo de próximo salto	Próximo salto	Tipo de rota	Função de rota
		10.2.0.0/24	Conexão de emparelhamento de VPC	peer-BX	Personalizada	<ul style="list-style-type: none"> ● Destino: subnet-B01 na VPC-B ● Conecta a subnet-B01 à subnet-X01
		10.3.0.0/24	Conexão de emparelhamento de VPC	peer-CX	Personalizada	<ul style="list-style-type: none"> ● Destino: subnet-C01 na VPC-C ● Conecta a subnet-C01 à subnet-X01

Observações e restrições

- Uma conexão de emparelhamento de VPC só pode permitir a comunicação entre VPCs na mesma região.
- Os blocos CIDR de sub-rede das VPCs que precisam se comunicar entre si por meio de uma conexão de emparelhamento de VPC não podem se sobrepor. Caso contrário, a conexão de emparelhamento da VPC não terá efeito.
- A sub-rede em que o ECS implementado com um firewall de terceiros reside precisa ser associada a uma tabela de rotas personalizada. Certifique-se de que a região onde seus recursos estão localizados oferece suporte a tabelas de rotas personalizadas.

Se **Route Tables** for exibida no painel esquerdo do console de rede, tabelas de rotas personalizadas são compatíveis.

Figura 6-2 Tabelas de rotas



Procedimento

Passo 1 Crie quatro VPCs e suas sub-redes na região A.

Para obter detalhes, consulte [Criação de uma VPC](#).

Para obter detalhes sobre VPCs e suas sub-redes, consulte [Tabela 6-2](#).

Passo 2 Crie uma tabela de rotas personalizada no VPC-X e associe a subnet-X01 à tabela de rotas personalizada.

1. Crie uma tabela de rotas personalizada no VPC-X.

Para obter detalhes, consulte [Criação de uma tabela de rotas personalizada](#).

2. Associe a subnet-X01 à tabela de rotas personalizada criada em [Passo 2.1](#).

Depois que o subnet-X01 é criado, ele é automaticamente associado à tabela de rotas padrão da VPC-X. Você precisa associar a tabela de rota personalizada criada em [Passo 2.1](#) à subnet-X01.

Para obter detalhes, consulte [Alteração da tabela de rotas associada a uma sub-rede](#).

Passo 3 Crie um ECS em cada VPC.

Para obter detalhes, consulte [Compra de um ECS](#).

Passo 4 Configure a NIC do ecs-X e instale o firewall de terceiros no ecs-X.

1. Desabilite a verificação de origem/destino para a NIC do ecs-X.
2. Instale um firewall de terceiros no ecs-X.

Passo 5 (Opcional) Configure um endereço IP virtual para ECSs.

Você pode criar dois ECSs na VPC-X e vinculá-los ao mesmo endereço IP virtual para que possam trabalhar no modo ativo e em espera. Se o ECS ativo estiver com defeito e não puder fornecer serviços, o endereço IP virtual será alternado dinamicamente para o ECS em espera para continuar fornecendo serviços. Ignore esta etapa se o ECS em que o firewall é implementado não precisar funcionar no modo ativo/em espera.

1. Atribua um endereço IP virtual na sub-rede da VPC-X.

Para obter detalhes, consulte [Atribuição de um IP virtual](#).

2. Vincule o endereço IP virtual aos ECSs ativos e em espera nos quais o firewall é implementado.

Para obter detalhes, consulte [Vinculação de um endereço IP virtual a um EIP ou ECS](#).

Passo 6 Crie três conexões de emparelhamento de VPC e configure rotas.

1. Crie três conexões de emparelhamento de VPC.

– Se suas VPCs estiverem na mesma conta, consulte [Criação de uma conexão de emparelhamento de VPC com outra VPC na sua conta](#).

– Se suas VPCs estiverem em contas diferentes, consulte [Criação de uma conexão de emparelhamento de VPC com uma VPC em outra conta](#).

Para obter detalhes sobre conexões de emparelhamento de VPC, consulte [Tabela 6-4](#).

2. Nas tabelas de rotas padrão das três VPCs de serviço, adicione rotas com destino definido para as outras três VPCs e com o próximo salto definido para a conexão de emparelhamento da VPC.

Para obter detalhes, consulte [Adição de uma rota personalizada](#).

Neste exemplo, adicione as rotas planejadas em [Tabela 6-6](#) para tabelas de rotas da VPC-A, VPC-B e VPC-C.

3. Adicione rotas às tabelas de rotas padrão e personalizada da VPC do firewall.

Para obter detalhes, consulte [Adição de uma rota personalizada](#).

Neste exemplo, adicione as rotas planejadas em [Tabela 6-7](#) às tabelas de rotas padrão e personalizada da VPC-X.

Passo 7 Efetue logon no ECS e verifique se o firewall tem efeito.

Vários métodos estão disponíveis para efetuar logon em um ECS. Para obter detalhes, consulte [Logon em um ECS](#).

Neste exemplo, use o VNC fornecido no console de gerenciamento para fazer logon em um ECS.

1. Efetue logon no ecs-A01 e verifique a conectividade de rede entre a VPC-A e a VPC-B.

ping *Private IP address of ecs-B01*

Exemplo de comando:

ping 10.2.0.93

Se informações semelhantes às seguintes forem exibidas, as duas VPCs poderão se comunicar uma com a outra.

```
[root@ecs-A01 ~]# ping 10.2.0.93
PING 10.2.0.93 (10.2.0.93) 56(84) bytes of data.
64 bytes from 10.2.0.93: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 10.2.0.93: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 10.2.0.93: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 10.2.0.93: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 10.2.0.93 ping statistics ---
```

2. Mantenha a conectividade de rede entre a VPC-A e a VPC-B em [Passo 7.1](#) e efetue logon no ecs-X01 para verificar se o tráfego da VPC-A para a VPC-B flui pelo ecs-X01.
3. Em ecs-X01, verifique a alteração de tráfego em eth0.

Execute o seguinte comando pelo menos duas vezes consecutivamente para verificar se os valores dos pacotes RX e dos pacotes TX mudam:

ifconfig eth0

Se os pacotes mudam, o tráfego flui através do ecs-X01 e é eliminado pelo firewall.

```
[root@ecs-X01 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.5 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::f816:3eff:feb6:a632 prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:b6:a6:32 txqueuelen 1000 (Ethernet)
    RX packets 726222 bytes 252738526 (241.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 672597 bytes 305616882 (291.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@ecs-X01 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.5 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::f816:3eff:feb6:a632 prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:b6:a6:32 txqueuelen 1000 (Ethernet)
    RX packets 726260 bytes 252748508 (241.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 672633 bytes 305631756 (291.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

4. Repita [Passo 7.1](#) a [Passo 7.3](#) para verificar a comunicação entre outras VPCs.

----Fim

7

Uso de firewalls de terceiros ao conectar um data center local à nuvem

Cenários

Seu data center local se comunica com a Huawei Cloud por meio da Direct Connect ou VPN. Um firewall virtual de terceiros é implementado na nuvem para filtrar o tráfego.

Esta seção descreve como usar um firewall virtual de terceiros ao conectar seu data center local a várias VPCs.

Vantagens

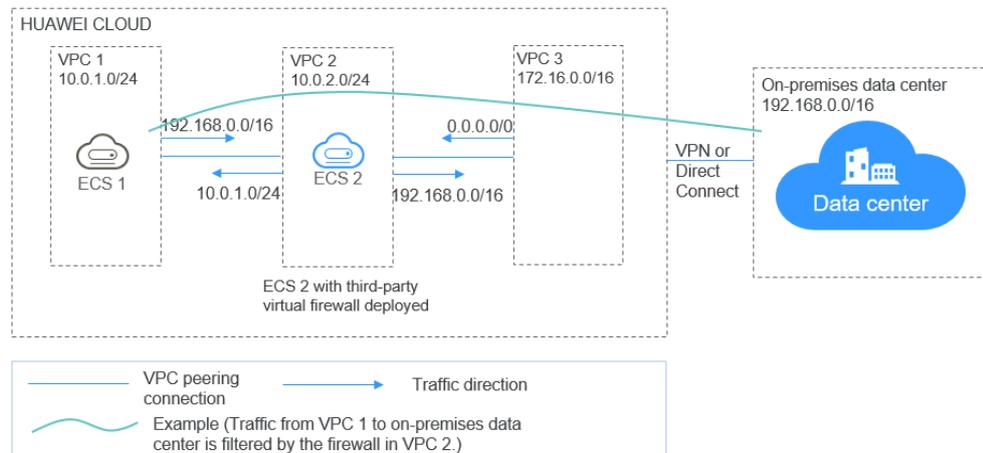
- Você pode usar firewalls de terceiros.
- O tráfego entre a nuvem e o data center local passará pelo firewall virtual de terceiros.
- Você pode definir regras de segurança conforme necessário.

Topologia típica

Suponha que seus serviços estejam implantados em VPC 1, VPC 2, VPC 3 e seu data center local, e você precisa usar um firewall virtual de terceiros na nuvem. Você pode configurar o firewall virtual no ECS 2 na VPC 2 e usar conexões de emparelhamento da VPC e configurar rotas para permitir a comunicação entre as VPCs. Além disso, você precisa criar uma conexão da Direct Connect para permitir a comunicação entre a VPC 3 e o data center local.

O diagrama de implementação é o seguinte:

Figura 7-1 Diagrama de implementação



Pré-requisitos

Os blocos CIDR de sub-rede da VPC 1, VPC 2 e VPC 3 não podem se sobrepor. Caso contrário, a comunicação por meio de conexões de emparelhamento VPC falhará.

Procedimento

Passo 1 Criar VPCs.

Crie VPC 1, VPC 2 e VPC 3.

Para obter detalhes, consulte [Criação de uma VPC](#).

📖 NOTA

Os blocos CIDR da VPC 1, VPC 2 e VPC 3 não podem se sobrepor. Por exemplo, o bloco CIDR da VPC 1 é 10.0.1.0/24, o da VPC 2 é 10.0.2.0/24 e o do VPC 3 é 172.16.0.0/16.

Passo 2 Criar ECSs.

1. Crie o ECS 1 e o ECS 2, que pertencem à sub-rede da VPC 1 e à sub-rede da VPC 2, respectivamente.

Para obter detalhes, consulte [Compra de um ECS](#).

📖 NOTA

A verificação de origem/destino deve ser desabilitada para a NIC do ECS 2.

2. Implemente um firewall virtual de terceiros no ECS 2.

Passo 3 Criar conexões de emparelhamento de VPC.

Crie conexões de emparelhamento de VPC entre VPC 1 e VPC 2, VPC 2 e VPC 3 para permitir a comunicação entre elas.

Ao criar uma conexão de emparelhamento de VPC, não configure rotas para as extremidades local e de par. Configurar rotas em [Passo 7](#).

Para obter detalhes sobre criar conexões de emparelhamento de VPC, consulte [Criação de uma conexão de emparelhamento de VPC com outra VPC na sua conta](#).

Passo 4 Criar uma tabela de rotas para uma sub-rede.

Crie uma tabela de rotas personalizada e associe-a à sub-rede da VPC 2 para controlar o tráfego de saída.

Para obter detalhes, consulte [Criação de uma tabela de rotas personalizada](#).

Passo 5 (Opcional) Atribuir um endereço IP virtual e vincule-o a ECSs.

Você pode criar dois ECSs na VPC 2 e vinculá-los ao mesmo endereço IP virtual para que possam funcionar no modo ativo e em espera. Se o ECS ativo estiver com defeito e não puder fornecer serviços, o endereço IP virtual será alternado dinamicamente para o ECS em espera para continuar fornecendo serviços. Ignore esta etapa se o ECS em espera não for necessário.

1. Atribua um endereço IP virtual na sub-rede da VPC 2.

Para obter detalhes, consulte [Atribuição de um IP virtual](#).

2. Vincule o endereço IP virtual ao ECS 2.

Para obter detalhes, consulte [Vinculação de um endereço IP virtual a um EIP ou ECS](#).

Passo 6 Criar uma conexão Direct Connect.

Use uma conexão Direct Connect para habilitar a comunicação entre a VPC 3 e o data center local. Para obter detalhes, consulte [Criar uma conexão](#).

Passo 7 Configurar rotas.

Você pode configurar rotas para encaminhar o tráfego para um próximo salto e, finalmente, para um destino.

1. Adicione a rota a seguir à tabela de rotas padrão da VPC 1:

Adicione uma rota para encaminhar o tráfego da VPC 1 para o data center local, defina o destino da rota para o bloco CIDR do data center local, e o próximo salto da rota para a conexão de emparelhamento da VPC entre a VPC 1 e a VPC 2.

[Figura 7-2](#) é para referência.

Figura 7-2 Rotas na tabela de rotas padrão da VPC 1

Destination	Next Hop Type	Next Hop	Type	Description
Local	Local	Local	System	Default route that enables Instance ...
192.168.0.0/16	VPC peering connection	VPC1-VPC2	Custom	--

2. Adicione a rota a seguir à tabela de rotas padrão da VPC 2:

Defina o destino da rota para 0.0.0.0/0 e o próximo salto da rota para o ECS 2.

Se houver dois ECSs que usam o mesmo endereço IP virtual para trabalhar no modo ativo e em espera, o próximo salto deverá ser o endereço IP virtual.

[Figura 7-3](#) é para referência.

Figura 7-3 Rotas na tabela de rotas padrão da VPC 2

Destination	Next Hop Type	Next Hop	Type
0.0.0.0	Server	ecs2	Custom

3. Adicione as seguintes rotas à tabela de rotas da sub-rede da VPC 2:
 - a. Adicione uma rota para encaminhar o tráfego da VPC 2 para a VPC 1, defina o destino da rota para o bloco CIDR da VPC 1 e o próximo salto da rota para a conexão de emparelhamento da VPC entre a VPC 1 e a VPC 2.
 - b. Adicione uma rota para encaminhar o tráfego da VPC 2 para o data center local, defina o destino da rota para o bloco CIDR do data center local, e o próximo salto da rota para a conexão de emparelhamento da VPC entre a VPC 2 e a VPC 3.

Figura 7-4 é para referência.

Figura 7-4 Rotas na tabela de rotas da sub-rede da VPC 2

Destination	Next Hop Type	Next Hop	Type	Description
10.0.1.0/24	VPC peering connection	VPC1-VPC2	Custom	--
192.168.0.0/16	VPC peering connection	VPC2-VPC3	Custom	--

4. Adicione a rota a seguir à tabela de rotas padrão da VPC 3:
Defina o destino da rota como 0.0.0.0/0 e o próximo salto da rota para a conexão de emparelhamento da VPC entre a VPC 2 e a VPC 3.

Figura 7-5 é para referência.

Figura 7-5 Rotas na tabela de rotas padrão da VPC 3

Destination	Next Hop Type	Next Hop	Type
0.0.0.0/0	VPC peering connection	VPC2-VPC3	Custom
192.168.0.0/24	Direct Connect gateway	vgw-0704-01	System

Uma conexão Direct Connect foi criada em **Passo 6**. Assim, uma rota para a conexão Direct Connect será entregue automaticamente pelo sistema.

---Fim

Verificação

Faça logon no ECS 1 e acesse seu data center local a partir do ECS 1. Verifique se o ECS 2 pode receber pacotes enviados do ECS 1 para o data center. Verifique se os pacotes passam e são filtrados pelo firewall no ECS 2.

8 Implementação de contêineres que podem se comunicar uns com os outros em ECSs

Cenários

Você pode implantar contêineres que não são da Huawei Cloud em ECSs da Huawei Cloud e permitir que os contêineres em ECSs diferentes, mas na mesma sub-rede, se comuniquem entre si.

Vantagens

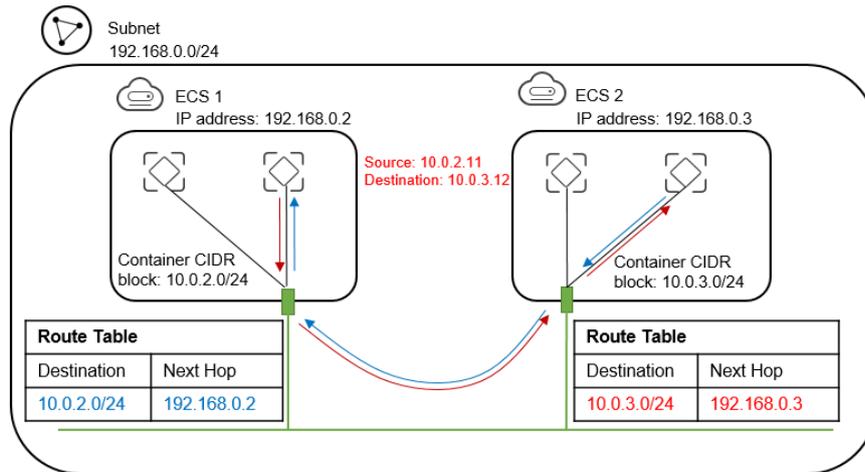
- Os contêineres implementados em ECSs podem usar blocos CIDR que não são daqueles das VPCs às quais os ECSs pertencem, mas usam rotas adicionadas a tabelas de rotas da VPC para encaminhamento de dados.
- Você só precisa adicionar rotas às tabelas de rotas para permitir comunicações entre os contêineres, o que é flexível e conveniente.

Topologia típica

Os requisitos de topologia de rede são os seguintes:

- Os ECSs estão na mesma sub-rede. Conforme mostrado na figura a seguir, a sub-rede da VPC é 192.168.0.0/24, e os endereços IP do ECS 1 e do ECS 2 são 192.168.0.2 e 192.168.0.3, respectivamente.
- Os contêineres estão em blocos CIDR que não pertencem às sub-redes da VPC às quais os ECSs pertencem. Os contêineres no mesmo ECS estão no mesmo bloco CIDR, mas os contêineres em ECSs diferentes usam blocos CIDR diferentes. Conforme mostrado na figura a seguir, o bloco CIDR de contêineres no ECS 1 é 10.0.2.0/24 e o bloco no ECS 2 é 10.0.3.0/24.
- O próximo salto dos pacotes de dados enviados para um contêiner é o ECS onde o contêiner está localizado. Conforme mostrado na figura a seguir, o próximo salto dos pacotes enviados ao bloco CIDR 10.0.2.0/24 é 192.168.0.2, e o dos pacotes enviados ao bloco CIDR 10.0.3.0/24 é 192.168.0.3.

Figura 8-1 Topologia de rede



Procedimento

Passo 1 Crie VPCs.

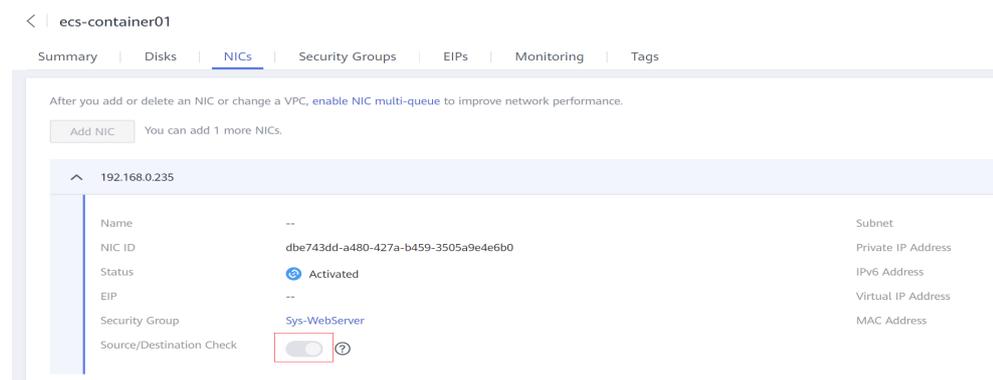
Para obter detalhes, consulte [Criação de uma VPC](#).

Passo 2 Crie ECSs.

Para obter detalhes, consulte [Compra de um ECS](#).

Depois que o ECS for criado, desative a verificação de origem/destino na NIC do ECS, conforme mostrado na [Figura 8-2](#).

Figura 8-2 Desativar a verificação de origem/destino



Passo 3 Implemente contêineres em ECSs.

Você pode usar o Docker CE para implementar contêineres. Para obter detalhes, consulte a documentação do Docker CE.

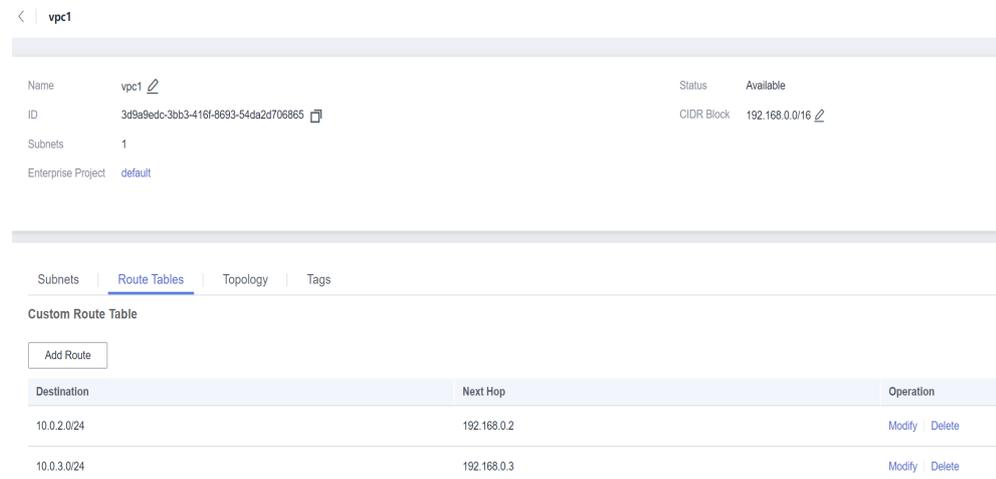
📖 NOTA

Os contêineres no mesmo ECS devem estar no mesmo bloco CIDR e os blocos CIDR de contêineres em ECSs diferentes não podem se sobrepor.

Passo 4 Adicione rotas à tabela de rotas da VPC.

Defina o próximo salto dos pacotes enviados para o bloco CIDR 10.0.2.0/24 para 192.168.0.2, e defina o próximo salto dos pacotes enviados para o bloco CIDR 10.0.3.0/24 para 192.168.0.3.

Figura 8-3 Adicionar rotas



NOTA

- Por padrão, uma VPC suporta contêineres de no máximo 50 blocos CIDR diferentes. Se contêineres de mais blocos CIDR diferentes precisarem ser implantados em uma VPC, solicite mais tabelas de rotas para a VPC.
- Depois que um contêiner é migrado para outro ECS, você precisa adicionar rotas à tabela de rotas do ECS da VPC.

Passo 5 Adicione regras ao grupo de segurança.

Para usar os comandos ping e traceroute para verificar as comunicações entre contêineres, adicione as regras mostradas em **Tabela 8-1** ao grupo de segurança dos ECSs para permitir o tráfego ICMP e UDP.

Para obter detalhes, consulte [Adição de uma regra de grupo de segurança](#).

Tabela 8-1 Regras de grupos de segurança

Direção	Protocolo	Porta	Origem
Entrada	ICMP	Todas	0.0.0.0/0
Entrada	UDP	Todas	0.0.0.0/0

----Fim

Verificação

Use o comando ping para verificar se os contêineres implantados em dois ECSs diferentes podem se comunicar entre si.

Execute os comandos a seguir para criar uma conexão de rede **my-net** no ECS 1, defina o bloco CIDR a ser usado por um contêiner no ECS 1 como 10.0.2.0/24 e crie o contêiner que usa **my-net**.

```
$ docker network create --subnet 10.0.2.0/24 my-net  
$ docker run -d --name nginx --net my-net -p 8080:80 nginx:alpine
```

Execute os comandos a seguir para criar uma conexão de rede e um contêiner no ECS 2 e defina o bloco CIDR a ser usado pelo contêiner como 10.0.3.0/24.

```
$ docker network create --subnet 10.0.3.0/24 my-net  
$ docker run -d --name nginx --net my-net -p 8080:80 nginx:alpine
```

Execute o seguinte comando para definir a política padrão da cadeia FORWARD na tabela de filtros do iptables no ECS para ACCEPT.

NOTA

Essa operação é necessária porque o Docker define a política padrão da cadeia FORWARD na tabela de filtros do iptables para DROP para fins de segurança.

```
$ iptables -P FORWARD ACCEPT
```

Faça ping e traceroute de 10.0.3.2 de 10.0.2.2. As operações de ping e traceroute são bem sucedidas, e o pacote é rastreado na seguinte sequência: 10.0.2.2 -> 10.0.2.1 -> 192.168.0.3 -> 10.0.3.2, que é consistente com as regras de encaminhamento de rota configuradas.

```
[root@ecs1 ~]# docker exec -it nginx /bin/sh  
/ # traceroute -d 10.0.3.2  
traceroute to 10.0.3.2 (10.0.3.2), 30 hops max, 46 byte packets  
 1 10.0.2.1 (10.0.2.1)  0.007 ms  0.004 ms  0.007 ms  
 2 192.168.0.3 (192.168.0.3)  0.232 ms  0.165 ms  0.248 ms  
 3 10.0.3.2 (10.0.3.2)  0.366 ms  0.308 ms  0.158 ms  
/ # ping 10.0.3.2  
PING 10.0.3.2 (10.0.3.2): 56 data bytes  
64 bytes from 10.0.3.2: seq=0 ttl=62 time=0.570 ms  
64 bytes from 10.0.3.2: seq=1 ttl=62 time=0.343 ms  
64 bytes from 10.0.3.2: seq=2 ttl=62 time=0.304 ms  
64 bytes from 10.0.3.2: seq=3 ttl=62 time=0.319 ms
```

9 Configuração de rotas baseadas em políticas para um ECS com várias NICs

9.1 Visão geral

Conhecimento de fundo

Se um ECS tiver várias NICs, a NIC primária poderá se comunicar com redes externas por padrão, mas as NICs de extensão não. Para habilitar as NICs de extensão para se comunicar com trabalhos externos, você precisa configurar rotas baseadas em políticas para essas NICs.

Cenários

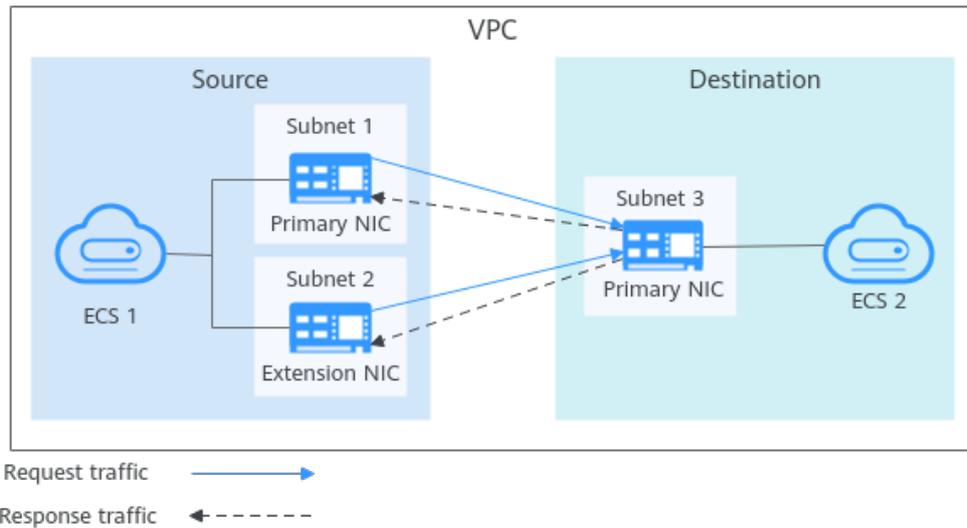
Este exemplo descreve como configurar rotas baseadas em políticas para um ECS com duas NICs. [Figura 9-1](#) mostra a rede. Os detalhes são os seguintes:

- As NICs primárias e de extensão no ECS de origem estão em sub-redes diferentes da mesma VPC.
- Os ECSs de origem e de destino estão em sub-redes diferentes da mesma VPC e os dois ECSs podem se comunicar entre si por meio de NICs principais sem configurar rotas baseadas em políticas.
- Depois que as rotas baseadas em políticas são configuradas para as duas NICs do ECS de origem, as NICs primária e de extensão podem se comunicar com o ECS de destino.

AVISO

Você pode selecionar um endereço IP de destino com base nos requisitos de serviço. Antes de configurar rotas baseadas em políticas, certifique-se de que o ECS de origem possa usar sua NIC primária para se comunicar com o ECS de destino.

Figura 9-1 Rede de ECS de NIC dupla



Guia de operação

Você pode seguir as seguintes operações para configurar rotas baseadas em políticas para ECSs de Linux e Windows. Para mais detalhes, consulte [Tabela 9-1](#).

Tabela 9-1 Instruções de operação

SO	Versão do endereço IP	Descrição
Linux	IPv4	Tome um ECS executando o CentOS 8.0 (64-bit) como exemplo. Configuração de rotas baseadas em políticas para um ECS do Linux com várias NICs (IPv4/IPv6)
	IPv6	
Windows	IPv4	Tome um ECS executando o Windows Server 2012 (64-bit) como exemplo. Configuração de rotas baseadas em políticas para um ECS do Windows com várias NICs (IPv4/IPv6)
	IPv6	

9.2 Coleta de informações de rede do ECS

Cenários

Antes de configurar rotas baseadas em políticas para um ECS de várias NICs, você precisa coletar informações de rede sobre o ECS.

- [Tabela 9-2](#) lista as informações a serem coletadas para um ECS de Linux usando IPv4.

Tabela 9-2 ECS de Linux usando IPv4

EC S	NIC primária	NIC de extensão	Como obter
Ori ge m	<ul style="list-style-type: none"> ● Endereço de NIC: 10.0.0.115 ● Sub-rede: 10.0.0.0/24 ● Gateway de sub-rede: 10.0.0.1 	<ul style="list-style-type: none"> ● Endereço de NIC: 10.0.1.183 ● Sub-rede: 10.0.1.0/24 ● Gateway de sub-rede: 10.0.1.1 	<ul style="list-style-type: none"> ● Obtenção de endereços de NIC do ECS ● Obtenção de blocos CIDR de sub-rede e endereços de gateway
De sti no	Endereço de NIC: 10.0.2.12	N/D	

- **Tabela 9-3** lista as informações a serem coletadas para um ECS de Linux usando IPv6.

Tabela 9-3 ECS de Linux usando IPv6

EC S	NIC primária	NIC de extensão	Como obter
Ori ge m	<ul style="list-style-type: none"> ● Endereço IPv4: 10.0.0.102 ● Endereço IPv6: 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9 ● Sub-rede IPv6: 2407:c080:1200:1dd8::/64 ● Gateway de sub-rede IPv6: 2407:c080:1200:1dd8::1 	<ul style="list-style-type: none"> ● Endereço IPv4: 10.0.1.191 ● Endereço IPv6: 2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8 ● Sub-rede IPv6: 2407:c080:1200:1a9c::/64 ● Gateway de sub-rede IPv6: 2407:c080:1200:1a9c::1 	<ul style="list-style-type: none"> ● Obtenção de endereços de NIC do ECS ● Obtenção de blocos CIDR de sub-rede e endereços de gateway
De stin o	<ul style="list-style-type: none"> ● Endereço IPv4: 10.0.2.3 ● Endereço IPv6: 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044 	N/D	

- **Tabela 9-4** lista as informações a serem coletadas para um ECS de Windows usando IPv4.

Tabela 9-4 ECS do Windows usando IPv4

EC S	NIC primária	NIC de extensão	Como obter
Ori ge m	<ul style="list-style-type: none"> ● Endereço de NIC: 10.0.0.59 ● Gateway de sub-rede: 10.0.0.1 	<ul style="list-style-type: none"> ● Endereço de NIC: 10.0.1.104 ● Gateway de sub-rede: 10.0.1.1 	<ul style="list-style-type: none"> ● Obtenção de endereços de NIC do ECS ● Obtenção de blocos CIDR de sub-rede e endereços de gateway
De sti no	Endereço de NIC: 10.0.2.12	N/D	

- **Tabela 9-5** lista as informações a serem coletadas para um ECS de Windows usando IPv6.

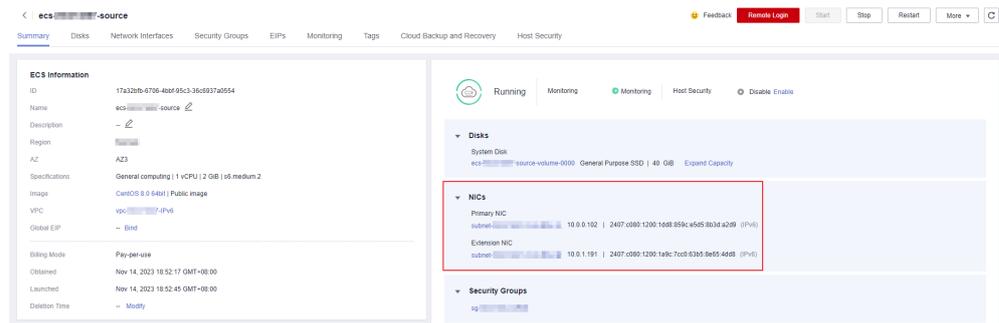
Tabela 9-5 ECS do Windows usando IPv6

EC S	NIC primária	NIC de extensão	Como obter
Ori ge m	Endereço de NIC: 2407:c080:802:aba:6788:fb9 4:d71f:8deb	Endereço de NIC: 2407:c080:802:be6:71c8:42 e0:d44e:eeb4	Obtenção de endereços de NIC do ECS
De sti no	Endereço de NIC: 2407:c080:802:be7:c2e6:d99 c:b685:c6c8	N/D	

Obtenção de endereços de NIC do ECS

1. Faça logon no console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Clique em **Service List** e escolha **Compute > Elastic Cloud Server**.
4. Na lista do ECS, clique no nome do ECS de destino.
A página de guia **Summary** do ECS é exibida.
5. Na área **NICs**, visualize os endereços IP das NICs primárias e de extensão.
Você pode ver os endereços IPv4 e IPv6 das NICs.

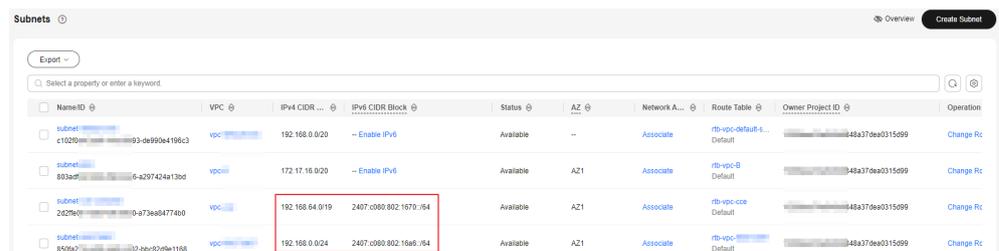
Figura 9-2 Endereços IPv4 e IPv6 de NICs



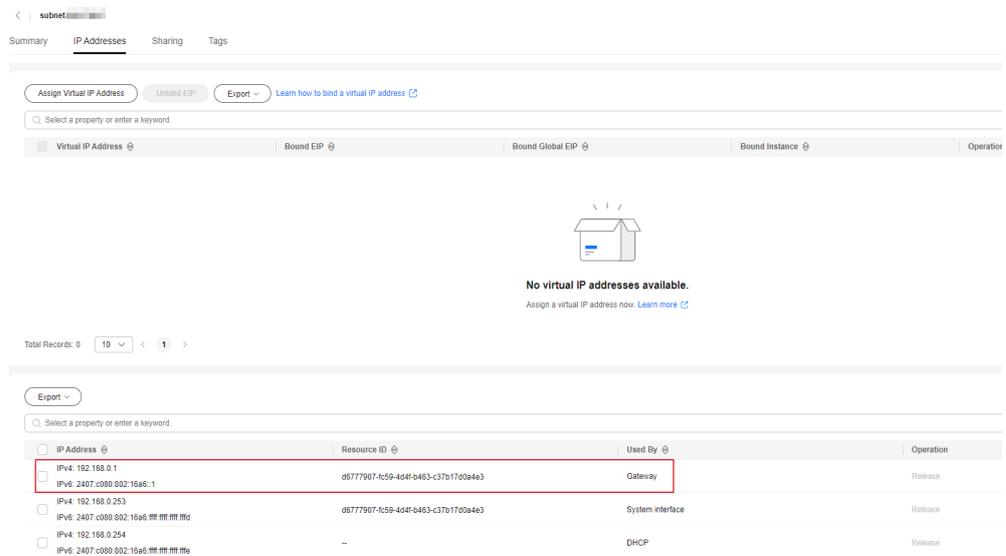
Obtenção de blocos CIDR de sub-rede e endereços de gateway

1. Faça login no console de gerenciamento.
2. Clique em  no canto superior esquerdo e selecione a região e o projeto desejados.
3. Clique em **Service List** e escolha **Compute > Elastic Cloud Server**.
4. Na lista do ECS, clique no nome do ECS de destino.
A página de guia **Summary** do ECS é exibida.
5. Na área **ECS Information**, clique no hyperlink da VPC.
A página **Virtual Private Cloud** é exibida.
6. Localize a VPC de destino e clique no número na coluna **Subnets**.
A página **Subnets** é exibida.
7. Na lista de sub-redes, visualize os blocos CIDR das sub-redes.
Você pode exibir os blocos CIDR IPv4 e IPv6 de sub-redes.

Figura 9-3 Blocos CIDR IPv4 e IPv6 de sub-redes



8. Na lista de sub-redes, clique no nome da sub-rede.
A página **Summary** é exibida.
9. Clique na guia **IP Addresses** e visualize os endereços de gateway da sub-rede.
Você pode ver os endereços IPv4 e IPv6 de um gateway.

Figura 9-4 Endereços IPv4 e IPv6 de um gateway

9.3 Configuração de rotas baseadas em políticas para um ECS do Linux com várias NICs (IPv4/IPv6)

Cenários

Esta seção descreve como configurar rotas baseadas em política para um ECS de NIC dupla executando o CentOS 8.0 (64-bit).

- IPv4: [Procedimento \(ECS de Linux usando IPv4\)](#)
- IPv6: [Procedimento \(ECS de Linux usando IPv6\)](#)

Para obter detalhes sobre o conhecimento de fundo e a rede de ECSs de NIC dupla, consulte [Visão geral](#).

Procedimento (ECS de Linux usando IPv4)

1. Colete as informações de rede do ECS necessárias para configurar rotas baseadas em políticas.
Para mais detalhes, consulte [Coleta de informações de rede do ECS](#).
2. Efetue login em um ECS.
Vários métodos estão disponíveis para efetuar login em um ECS. Para obter detalhes, consulte [Logon em um ECS](#).
3. Verifique se o ECS de origem pode usar sua NIC primária para se comunicar com o ECS de destino:

ping -I *IP address of the primary NIC on the source ECS* *IP address of the destination ECS*

Neste exemplo, execute o seguinte comando:

ping -I 10.0.0.115 10.0.2.12

Se informações semelhantes às seguintes forem exibidas, o ECS de origem poderá usar sua NIC primária para se comunicar com o ECS de destino.

```
[root@ecs-resource ~]# ping -I 10.0.0.115 10.0.2.12
PING 10.0.2.12 (10.0.2.12) from 10.0.0.115 : 56(84) bytes of data.
64 bytes from 10.0.2.12: icmp_seq=1 ttl=64 time=0.775 ms
64 bytes from 10.0.2.12: icmp_seq=2 ttl=64 time=0.268 ms
64 bytes from 10.0.2.12: icmp_seq=3 ttl=64 time=0.220 ms
64 bytes from 10.0.2.12: icmp_seq=4 ttl=64 time=0.167 ms
^C
--- 10.0.2.12 ping statistics ---
```

📖 NOTA

Antes de configurar rotas baseadas em políticas, certifique-se de que o ECS de origem possa usar sua NIC primária para se comunicar com o ECS de destino.

4. Consulte os nomes da NIC do ECS:

ifconfig

Procure o nome da NIC com base no endereço da NIC.

- 10.0.0.115 é o endereço IP da NIC primária e o nome da NIC é eth0.
- 10.0.1.183 é o endereço IP da NIC da extensão e o nome da NIC é eth1.

```
[root@ecs-resource ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.115 netmask 255.255.255.0 broadcast 10.0.0.255
    inet6 fe80::f816:3eff:fe92:6e0e prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:92:6e:0e txqueuelen 1000 (Ethernet)
    RX packets 432288 bytes 135762012 (129.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 1655
    TX packets 423744 bytes 106716932 (101.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.1.183 netmask 255.255.255.0 broadcast 10.0.1.255
    inet6 fe80::f816:3eff:febf:5818 prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:bf:58:18 txqueuelen 1000 (Ethernet)
    RX packets 9028 bytes 536972 (524.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 1915
    TX packets 6290 bytes 272473 (266.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

5. Configure rotas temporárias para o ECS.

AVISO

As rotas temporárias entram em vigor imediatamente após a configuração e serão perdidas após o reinício do ECS. Para evitar interrupções de rede depois que o ECS for reiniciado, execute 6 após esta etapa para configurar rotas persistentes.

a. Configure rotas baseadas em política para NICs primária e de extensão:

■ NIC primária

```
ip route add default via Subnet gateway dev NIC name table Route table name
```

```
ip route add Subnet CIDR block dev NIC name table Route table name
```

```
ip rule add from NIC address table Route table name
```

■ NIC de extensão

```
ip route add default via Subnet gateway dev NIC name table Route table name
```

```
ip route add Subnet CIDR block dev NIC name table Route table name
```

ip rule add from *NIC address table Route table name*

Configure os parâmetros da seguinte forma:

- NIC name: digite o nome obtido em [4](#).
- Route table name: personalize um nome de tabela de rota usando um número.
- Other network information: insira os endereços IP coletados em [1](#).

Neste exemplo, execute os seguintes comandos:

- NIC primária
ip route add default via 10.0.0.1 dev eth0 table 10
ip route add 10.0.0.0/24 dev eth0 table 10
ip rule add from 10.0.0.115 table 10
- NIC de extensão
ip route add default via 10.0.1.1 dev eth1 table 20
ip route add 10.0.1.0/24 dev eth1 table 20
ip rule add from 10.0.1.183 table 20

 **NOTA**

Se o ECS tiver várias NICs, configure as rotas baseadas em políticas para todas as NICs, uma a uma.

- b. Verifique se as rotas baseadas em políticas foram adicionadas com sucesso.

ip rule**ip route show table** *Route table name of the primary NIC***ip route show table** *Route table name of the extension NIC*

O nome da tabela de rotas é personalizado em [5.a](#).

Neste exemplo, execute os seguintes comandos:

ip rule**ip route show table 10****ip route show table 20**

Se informações semelhantes às seguintes forem exibidas, as rotas baseadas em políticas foram adicionadas.

```
[root@ecs-resource ~]# ip rule
0:      from all lookup local
32764:  from 10.0.1.183 lookup 20
32765:  from 10.0.0.115 lookup 10
32766:  from all lookup main
32767:  from all lookup default
[root@ecs-resource ~]# ip route show table 10
default via 10.0.0.1 dev eth0
10.0.0.0/24 dev eth0 scope link
[root@ecs-resource ~]# ip route show table 20
default via 10.0.1.1 dev eth1
10.0.1.0/24 dev eth1 scope link
```

- c. Verifique se o ECS de origem e o ECS de destino podem se comunicar entre si.

ping -I *IP address of the primary NIC on the source ECS IP address of the destination ECS***ping -I** *IP address of the extension NIC on the source ECS IP address of the destination ECS*

Neste exemplo, execute os seguintes comandos:

```
ping -I 10.0.0.115 10.0.2.12
```

```
ping -I 10.0.1.183 10.0.2.12
```

Se informações semelhantes às seguintes forem exibidas, ambas as NICs do ECS de origem poderão se comunicar com o ECS de destino.

```
[root@ecs-resource ~]# ping -I 10.0.0.115 10.0.2.12
PING 10.0.2.12 (10.0.2.12) from 10.0.0.115 : 56(84) bytes of data.
64 bytes from 10.0.2.12: icmp_seq=1 ttl=64 time=0.775 ms
64 bytes from 10.0.2.12: icmp_seq=2 ttl=64 time=0.268 ms
64 bytes from 10.0.2.12: icmp_seq=3 ttl=64 time=0.220 ms
64 bytes from 10.0.2.12: icmp_seq=4 ttl=64 time=0.167 ms
^C
--- 10.0.2.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 102ms
rtt min/avg/max/mdev = 0.167/0.357/0.775/0.244 ms
[root@ecs-resource ~]# ping -I 10.0.1.183 10.0.2.12
PING 10.0.2.12 (10.0.2.12) from 10.0.1.183 : 56(84) bytes of data.
64 bytes from 10.0.2.12: icmp_seq=1 ttl=64 time=2.84 ms
64 bytes from 10.0.2.12: icmp_seq=2 ttl=64 time=0.258 ms
64 bytes from 10.0.2.12: icmp_seq=3 ttl=64 time=0.234 ms
64 bytes from 10.0.2.12: icmp_seq=4 ttl=64 time=0.153 ms
^C
--- 10.0.2.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 92ms
rtt min/avg/max/mdev = 0.153/0.871/2.840/1.137 ms
```

6. Configure rotas persistentes para o ECS.

- a. Execute o seguinte comando para abrir o arquivo `/etc/rc.local`:

```
vi /etc/rc.local
```

- b. Pressione `i` para entrar no modo de edição.

- c. Adicione o seguinte conteúdo ao final do arquivo:

```
# wait for nics up
sleep 5
# Add v4 routes for eth0
ip route flush table 10
ip route add default via 10.0.0.1 dev eth0 table 10
ip route add 10.0.0.0/24 dev eth0 table 10
ip rule add from 10.0.0.115 table 10
# Add v4 routes for eth1
ip route flush table 20
ip route add default via 10.0.1.1 dev eth1 table 20
ip route add 10.0.1.0/24 dev eth1 table 20
ip rule add from 10.0.1.183 table 20
# Add v4 routes for cloud-init
ip rule add to 169.254.169.254 table main
```

Os parâmetros são descritos da seguinte forma:

- `wait for nics up`: tempo de inicialização do arquivo. Defina o valor para ser o mesmo das configurações anteriores.
 - `Add v4 routes for eth0`: rotas baseadas em políticas da NIC primária. Defina o valor para ser o mesmo que o configurado em [5.a](#).
 - `Add v4 routes for eth1`: rotas baseadas em políticas da NIC da extensão. Defina o valor para ser o mesmo que o configurado em [5.a](#).
 - `Add v4 routes for cloud-init`: configure o endereço de Cloud-Init. Defina o valor para ser o mesmo das configurações anteriores.
- d. Pressione `ESC` para sair e digite `:wq!` para salvar a configuração.
 - e. Execute o seguinte comando para atribuir permissões de execução ao arquivo `/etc/rc.local`:

```
chmod +x /etc/rc.local
```

NOTA

Se o seu sistema operacional for Red Hat ou EulerOS, execute o seguinte comando depois de executar [6.e](#):

```
chmod +x /etc/rc.d/rc.local
```

- f. Execute o seguinte comando para reiniciar o ECS:

```
reboot
```

AVISO

As rotas baseadas em políticas adicionadas ao arquivo `/etc/rc.local` entram em vigor somente depois que o ECS é reiniciado. Certifique-se de que as cargas de trabalho no ECS não serão afetadas antes de reiniciar o ECS.

- g. Repita [5.b](#) a [5.c](#) para verificar se as rotas baseadas em políticas foram adicionadas e se o ECS de origem e o ECS de destino podem se comunicar entre si.

Procedimento (ECS de Linux usando IPv6)

1. Colete as informações de rede do ECS necessárias para configurar rotas baseadas em políticas.
Para mais detalhes, consulte [Coleta de informações de rede do ECS](#).
2. Efetue logon em um ECS.
Vários métodos estão disponíveis para efetuar logon em um ECS. Para obter detalhes, consulte [Logon em um ECS](#).
3. Verifique se um ECS tem IPv6 habilitado e pode obter endereços IPv6.

AVISO

Execute esta etapa para os ECSs de origem e de destino para garantir que os ECSs tenham obtido endereços IPv6. Caso contrário, os ECSs não poderão se comunicar uns com os outros usando endereços IPv6.

Os ECSs neste exemplo executam o CentOS 8.0 (64-bit). Para obter detalhes sobre como obter endereços IPv6 para ECSs executando outros sistemas operacionais, consulte [Atribuição dinâmica de endereços IPv6](#).

- a. Execute o seguinte comando para verificar se o ECS tem endereços IPv6:

```
ip addr
```

Na saída do comando a seguir, `eth0` e `eth1` são as NICs do ECS. Cada NIC tem um `inet6` seguido de um endereço IP que começa com `fe80`. Isso indica que o ECS tem IPv6 habilitado, mas não obteve endereços IPv6. Neste caso, execute [3.b](#) a [3.g](#) para obter endereços IPv6.

```
[root@ecs-resource ~]# ip addr
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
UP group default qlen 1000
    link/ether fa:16:3e:22:22:88 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.102/24 brd 10.0.0.255 scope global dynamic noprefixroute
eth0
    valid_lft 107943256sec preferred_lft 107943256sec
```

```
inet6 fe80::f816:3eff:fe22:2288/64 scope link
    valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
UP group default qlen 1000
    link/ether fa:16:3e:22:23:e1 brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.191/24 brd 10.0.1.255 scope global dynamic noprefixroute
eth1
    valid_lft 107943256sec preferred_lft 107943256sec
inet6 fe80::f816:3eff:fe22:23e1/64 scope link
    valid_lft forever preferred_lft forever
```

- b. Consulte os nomes da NIC do ECS:

ifconfig

Procure o nome da NIC com base no endereço da NIC.

- 10.0.0.102 é o endereço IP da NIC primária e o nome da NIC é eth0.
- 10.0.1.191 é o endereço IP da NIC da extensão e o nome da NIC é eth1.

```
[root@ecs-resource ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.102 netmask 255.255.255.0 broadcast 10.0.0.255
    inet6 fe80::f816:3eff:fe22:2288 prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:22:22:88 txqueuelen 1000 (Ethernet)
    RX packets 135116 bytes 132321802 (126.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 60963 bytes 23201005 (22.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.1.191 netmask 255.255.255.0 broadcast 10.0.1.255
    inet6 fe80::f816:3eff:fe22:23e1 prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:22:23:e1 txqueuelen 1000 (Ethernet)
    RX packets 885 bytes 97676 (95.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 47 bytes 4478 (4.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- c. Configure o arquivo **ifcfg** da NIC primária.

- i. Execute o seguinte comando para abrir o arquivo **ifcfg** da NIC primária:

```
vi /etc/sysconfig/network-scripts/ifcfg-Primary NIC name
```

O nome da NIC primária é obtido em **3.b**.

Neste exemplo, execute o seguinte comando:

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

- ii. Pressione **i** para entrar no modo de edição.

- iii. Adicione o seguinte conteúdo ao final do arquivo:

```
IPV6INIT="yes"
DHCPV6C="yes"
```

- iv. Pressione **ESC** para sair e digite **:wq!** para salvar a configuração.

- d. Configure o arquivo **ifcfg** da NIC da extensão.

- i. Execute o seguinte comando para abrir o arquivo **ifcfg** da NIC da extensão:

```
vi /etc/sysconfig/network-scripts/ifcfg-Extension NIC name
```

O nome da NIC de extensão é obtido em **3.b**.

Neste exemplo, execute o seguinte comando:

```
vi /etc/sysconfig/network-scripts/ifcfg-eth1
```

- ii. Pressione **i** para entrar no modo de edição.

- iii. Adicione o seguinte conteúdo ao final do arquivo:

```
IPV6INIT="yes"
DHCPV6C="yes"
```

- iv. Pressione **ESC** para sair e digite **:wq!** para salvar a configuração.
- e. Edite o arquivo **/etc/sysconfig/network**.
 - i. Execute o seguinte comando para abrir o arquivo **/etc/sysconfig/network**:
vi /etc/sysconfig/network
 - ii. Pressione **i** para entrar no modo de edição.
 - iii. Adicione o seguinte conteúdo ao final do arquivo:

```
NETWORKING_IPV6="yes"
```
 - iv. Pressione **ESC** para sair e digite **:wq!** para salvar a configuração.
- f. Execute o seguinte comando para reiniciar o serviço de rede para que a configuração entre em vigor:
systemctl restart NetworkManager
- g. Execute o seguinte comando para verificar se o ECS tem endereços IPv6:

ip addr

Na saída do comando a seguir, cada NIC tem mais um **inet6** seguido por um endereço IP que começa com **2407**, além do seguido por um endereço IP que começa com **fe80**. Nesse caso, o ECS obteve endereços IPv6.

```
[root@ecs-resource ~]# ip addr
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether fa:16:3e:22:22:88 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.102/24 brd 10.0.0.255 scope global dynamic noprefixroute eth0
        valid_lft 107999994sec preferred_lft 107999994sec
    inet6 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9/128 scope global dynamic noprefixroute
        valid_lft 7195sec preferred_lft 7195sec
    inet6 fe80::f816:3eff:fe22:2288/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether fa:16:3e:22:23:e1 brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.191/24 brd 10.0.1.255 scope global dynamic noprefixroute eth1
        valid_lft 107999994sec preferred_lft 107999994sec
    inet6 2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8/128 scope global dynamic noprefixroute
        valid_lft 7198sec preferred_lft 7198sec
    inet6 fe80::f816:3eff:fe22:23e1/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

4. Verifique se o ECS de origem pode usar sua NIC primária para se comunicar com o ECS de destino:

ping6 -I IP address of the primary NIC on the source ECS IP address of the destination ECS

Neste exemplo, execute o seguinte comando:

**ping6 -I 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9
2407:c080:1200:1dd9:16a7:fe7a:8f71:7044**

Se informações semelhantes às seguintes forem exibidas, o ECS de origem poderá usar sua NIC primária para se comunicar com o ECS de destino.

```
[root@ecs-resource ~]# ping6 -I 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044
PING
2407:c080:1200:1dd9:16a7:fe7a:8f71:7044 (2407:c080:1200:1dd9:16a7:fe7a:8f71:7044) from 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9 : 56 data bytes
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=1 ttl=64
time=0.635 ms
```

```
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=2 ttl=64
time=0.320 ms
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=3 ttl=64
time=0.287 ms
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=4 ttl=64
time=0.193 ms
^C
--- 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3074ms
rtt min/avg/max/mdev = 0.193/0.358/0.635/0.167 ms
```

NOTA

Antes de configurar rotas baseadas em políticas, certifique-se de que o ECS de origem possa usar sua NIC primária para se comunicar com o ECS de destino.

5. Configure rotas temporárias para o ECS.

AVISO

As rotas temporárias entram em vigor imediatamente após a configuração e serão perdidas após o reinício do ECS. Para evitar interrupções de rede depois que o ECS for reiniciado, execute **6** após esta etapa para configurar rotas persistentes.

- a. Configure rotas baseadas em política para NICs primária e de extensão:
 - NIC primária
 - ip -6 route add default via Subnet gateway dev NIC name table Route table name**
 - ip -6 route add Subnet CIDR block dev NIC name table Route table name**
 - ip -6 rule add from NIC address table Route table name**
 - NIC de extensão
 - ip -6 route add default via Subnet gateway dev NIC name table Route table name**
 - ip -6 route add Subnet CIDR block dev NIC name table Route table name**
 - ip -6 rule add from NIC address table Route table name**

Configure os parâmetros da seguinte forma:

- NIC name: digite o nome obtido em **3.b**.
- Route table name: personalize um nome de tabela de rota usando um número.
- Other network information: insira os endereços IP coletados em **1**.

Neste exemplo, execute os seguintes comandos:

- NIC primária
 - ip -6 route add default via 2407:c080:1200:1dd8::1 dev eth0 table 10**
 - ip -6 route add 2407:c080:1200:1dd8::/64 dev eth0 table 10**
 - ip -6 rule add from 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9 table 10**
- NIC de extensão
 - ip -6 route add default via 2407:c080:1200:1a9c::1 dev eth1 table 20**
 - ip -6 route add 2407:c080:1200:1a9c::/64 dev eth1 table 20**
 - ip -6 rule add from 2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8 table 20**

 **NOTA**

Se o ECS tiver várias NICs, configure as rotas baseadas em políticas para todas as NICs, uma a uma.

- b. Verifique se as rotas baseadas em políticas foram adicionadas com sucesso.

ip -6 rule**ip -6 route show table** *Route table name of the primary NIC***ip -6 route show table** *Route table name of the extension NIC*

O nome da tabela de rotas é personalizado em [5.a](#).

Neste exemplo, execute os seguintes comandos:

ip -6 rule**ip -6 route show table 10****ip -6 route show table 20**

Se informações semelhantes às seguintes forem exibidas, as rotas baseadas em políticas foram adicionadas.

```
[root@ecs-resource ~]# ip -6 rule
0:      from all lookup local
32764:  from 2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8 lookup 20
32765:  from 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9 lookup 10
32766:  from all lookup main
[root@ecs-resource ~]# ip -6 route show table 10
2407:c080:1200:1dd8::/64 dev eth0 metric 1024 pref medium
default via 2407:c080:1200:1dd8::1 dev eth0 metric 1024 pref medium
[root@ecs-resource ~]# ip -6 route show table 20
2407:c080:1200:1a9c::/64 dev eth1 metric 1024 pref medium
default via 2407:c080:1200:1a9c::1 dev eth1 metric 1024 pref medium
```

- c. Verifique se o ECS de origem e o ECS de destino podem se comunicar entre si.

ping -6 -I *IP address of the primary NIC on the source ECS IP address of the destination ECS***ping -6 -I** *IP address of the extension NIC on the source ECS IP address of the destination ECS*

Neste exemplo, execute os seguintes comandos:

ping -6 -I 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9
2407:c080:1200:1dd9:16a7:fe7a:8f71:7044**ping -6 -I 2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8**
2407:c080:1200:1dd9:16a7:fe7a:8f71:7044

Se informações semelhantes às seguintes forem exibidas, ambas as NICs do ECS de origem poderão se comunicar com o ECS de destino.

```
[root@ecs-resource ~]# ping -6 -I
2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9
2407:c080:1200:1dd9:16a7:fe7a:8f71:7044
PING
2407:c080:1200:1dd9:16a7:fe7a:8f71:7044 (2407:c080:1200:1dd9:16a7:fe7a:8f7
1:7044) from 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9 : 56 data bytes
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=1 ttl=64
time=0.770 ms
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=2 ttl=64
time=0.295 ms
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=3 ttl=64
time=0.245 ms
^C
--- 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2080ms
rtt min/avg/max/mdev = 0.245/0.436/0.770/0.237 ms
[root@ecs-resource ~]# ping -6 -I
```

```
2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8
2407:c080:1200:1dd9:16a7:fe7a:8f71:7044
PING
2407:c080:1200:1dd9:16a7:fe7a:8f71:7044 (2407:c080:1200:1dd9:16a7:fe7a:8f7
1:7044) from 2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8 : 56 data bytes
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=1 ttl=64
time=0.922 ms
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=2 ttl=64
time=0.307 ms
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=3 ttl=64
time=0.174 ms
^C
--- 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2059ms
rtt min/avg/max/mdev = 0.174/0.467/0.922/0.326 ms
```

6. Configure rotas persistentes para o ECS.

- a. Execute o seguinte comando para abrir o arquivo **/etc/rc.local**:

```
vi /etc/rc.local
```

- b. Pressione **i** para entrar no modo de edição.

- c. Adicione o seguinte conteúdo ao final do arquivo:

```
# wait for nics up
sleep 5
# Add v6 routes for eth0
ip -6 route flush table 10
ip -6 route add default via 2407:c080:1200:1dd8::1 dev eth0 table 10
ip -6 route add 2407:c080:1200:1dd8::/64 dev eth0 table 10
ip -6 rule add from 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9 table 10
# Add v6 routes for eth1
ip -6 route flush table 20
ip -6 route add default via 2407:c080:1200:1a9c::1 dev eth1 table 20
ip -6 route add 2407:c080:1200:1a9c::/64 dev eth1 table 20
ip -6 rule add from 2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8 table 20
```

Os parâmetros são descritos da seguinte forma:

- **wait for nics up**: tempo de inicialização do arquivo. Defina o valor para ser o mesmo das configurações anteriores.
 - **Add v6 routes for eth0**: rotas baseadas em políticas da NIC primária. Defina o valor para ser o mesmo que o configurado em **5.a**.
 - **Add v6 routes for eth1**: rotas baseadas em políticas da NIC da extensão. Defina o valor para ser o mesmo que o configurado em **5.a**.
- d. Pressione **ESC** para sair e digite **:wq!** para salvar a configuração.
- e. Execute o seguinte comando para atribuir permissões de execução ao arquivo **/etc/rc.local**:

```
chmod +x /etc/rc.local
```

 **NOTA**

Se o seu sistema operacional for Red Hat ou EulerOS, execute o seguinte comando depois de executar **6.e**:

```
chmod +x /etc/rc.d/rc.local
```

- f. Execute o seguinte comando para reiniciar o ECS:

```
reboot
```

AVISO

As rotas baseadas em políticas adicionadas ao arquivo `/etc/rc.local` entram em vigor somente depois que o ECS é reiniciado. Certifique-se de que as cargas de trabalho no ECS não serão afetadas antes de reiniciar o ECS.

- g. Repita [5.b](#) a [5.c](#) para verificar se as rotas baseadas em políticas foram adicionadas e se o ECS de origem e o ECS de destino podem se comunicar entre si.

9.4 Configuração de rotas baseadas em políticas para um ECS do Windows com várias NICs (IPv4/IPv6)

Cenários

Esta seção descreve como configurar rotas baseadas em políticas para um ECS de NIC dupla executando o Windows Server 2012 (64-bit).

- IPv4: [Procedimento \(ECS de Windows usando IPv4\)](#)
- IPv6: [Procedimento \(ECS de Windows usando IPv6\)](#)

Para obter detalhes sobre o conhecimento de fundo e a rede de ECSs de NIC dupla, consulte [Visão geral](#).

Procedimento (ECS de Windows usando IPv4)

1. Colete as informações de rede do ECS necessárias para configurar rotas baseadas em políticas.

Para mais detalhes, consulte [Coleta de informações de rede do ECS](#).

2. Efetue logon em um ECS.

Vários métodos estão disponíveis para efetuar logon em um ECS. Para obter detalhes, consulte [Logon em um ECS](#).

3. Verifique se o ECS de origem pode usar sua NIC primária para se comunicar com o ECS de destino:

ping -S *IP address of the primary NIC on the source ECS* *IP address of the destination ECS*

Neste exemplo, execute o seguinte comando:

ping -S 10.0.0.59 10.0.2.12

Se informações semelhantes às seguintes forem exibidas, o ECS de origem poderá usar sua NIC primária para se comunicar com o ECS de destino.

```
C:\Users\Administrator>ping -S 10.0.0.59 10.0.2.12
Pinging 10.0.2.12 from 10.0.0.59 with 32 bytes of data:
Reply from 10.0.2.12: bytes=32 time<1ms TTL=64
```

 **NOTA**

Antes de configurar rotas baseadas em políticas, certifique-se de que o ECS de origem possa usar sua NIC primária para se comunicar com o ECS de destino.

4. Configure uma rota baseada em política para a NIC da extensão.

route add -p 0.0.0.0 mask 0.0.0.0 Subnet gateway of the extension NIC metric Route priority

Configure os parâmetros da seguinte forma:

- **0.0.0.0/0**: Default route. não mude isso.
- Subnet gateway of the extension NIC: insira o endereço IP coletado em [1](#).
- Route priority: defina seu valor para 261. A prioridade da NIC de extensão deve ser menor que a da NIC primária. Um valor maior indica uma prioridade mais baixa.

Neste exemplo, execute o seguinte comando:

route add -p 0.0.0.0 mask 0.0.0.0 10.0.1.1 metric 261

 **NOTA**

- A NIC primária já tem rotas baseadas em políticas e você não precisa configurar novamente.
 - Se o ECS tiver várias NICs de extensão, configure rotas baseadas em políticas para todas as NICs de extensão, uma a uma.
5. Verifique se a rota baseada em políticas foi adicionada com sucesso.

route print

Se informações semelhantes às seguintes forem exibidas, a rota baseada em políticas foi adicionada. A rota é persistente e não será perdida depois que o ECS for reiniciado.

```
C:\Users\Administrator>route print
=====
Interface List
19...fa 16 3e fc 7b 76 .....Red Hat VirtIO Ethernet Adapter #3
14...fa 16 3e 5d 3e b6 .....Red Hat VirtIO Ethernet Adapter
1.....Software Loopback Interface 1
16...00 00 00 00 00 00 e0 Microsoft ISA/ATP Adapter #2
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          10.0.1.1         10.0.1.104       266
0.0.0.0                    0.0.0.0          10.0.0.1         10.0.0.59        5
10.0.0.0                   255.255.255.0   On-link         10.0.0.59        261
10.0.0.59                  255.255.255.255 On-link         10.0.0.59        261
10.0.0.255                 255.255.255.255 On-link         10.0.0.59        261
10.0.1.0                   255.255.255.0   On-link         10.0.1.104       261
10.0.1.104                 255.255.255.255 On-link         10.0.1.104       261
10.0.1.255                 255.255.255.255 On-link         10.0.1.104       261
127.0.0.0                  255.0.0.0       On-link         127.0.0.1        306
127.0.0.1                  255.255.255.255 On-link         127.0.0.1        306
127.255.255.255           255.255.255.255 On-link         127.0.0.1        306
169.254.169.254           255.255.255.255 10.0.0.254      10.0.0.59        6
224.0.0.0                  240.0.0.0       On-link         127.0.0.1        306
224.0.0.0                  240.0.0.0       On-link         10.0.0.59        261
224.0.0.0                  240.0.0.0       On-link         10.0.1.104       261
255.255.255.255           255.255.255.255 On-link         127.0.0.1        306
255.255.255.255           255.255.255.255 On-link         10.0.0.59        261
255.255.255.255           255.255.255.255 On-link         10.0.1.104       261
=====
Persistent Routes:
Network Address            Netmask          Gateway Address  Metric
0.0.0.0                    0.0.0.0          10.0.1.1         261
=====

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1      306   ::1/128                    On-link
14     261   fe80::/64                  On-link
19     261   fe80::/64                  On-link
19     261   fe80::197b:3504:e05:5a4d/128
                                           On-link
14     261   fe80::e115:8e6a:5dcc:6715/128
                                           On-link
1      306   ff00::/8                   On-link
14     261   ff00::/8                   On-link
19     261   ff00::/8                   On-link
=====
Persistent Routes:
None
=====
```

6. Verifique se o ECS de origem e o ECS de destino podem se comunicar entre si.

ping -S *IP address of the primary NIC on the source ECS* *IP address of the destination ECS*

ping -S *IP address of the extension NIC on the source ECS* *IP address of the destination ECS*

Neste exemplo, execute os seguintes comandos:

ping -S 10.0.0.59 10.0.2.12

ping -S 10.0.1.104 10.0.2.12

Se informações semelhantes às seguintes forem exibidas, ambas as NICs do ECS de origem poderão se comunicar com o ECS de destino.

```
C:\Users\Administrator>ping -S 10.0.0.59 10.0.2.12

Pinging 10.0.2.12 from 10.0.0.59 with 32 bytes of data:
Reply from 10.0.2.12: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.2.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping -S 10.0.1.104 10.0.2.12

Pinging 10.0.2.12 from 10.0.1.104 with 32 bytes of data:
Reply from 10.0.2.12: bytes=32 time=4ms TTL=64
Reply from 10.0.2.12: bytes=32 time<1ms TTL=64
Reply from 10.0.2.12: bytes=32 time<1ms TTL=64
Reply from 10.0.2.12: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.2.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms
```

Procedimento (ECS de Windows usando IPv6)

1. Colete as informações de rede do ECS necessárias para configurar rotas baseadas em políticas.
Para mais detalhes, consulte [Coleta de informações de rede do ECS](#).
2. Efetue logon em um ECS.
Vários métodos estão disponíveis para efetuar logon em um ECS. Para obter detalhes, consulte [Logon em um ECS](#).
3. Execute o comando a seguir para verificar se o ECS tem IPv6 habilitado e pode obter endereços IPv6.

ipconfig

Se informações semelhantes às seguintes forem exibidas, cada NIC terá um endereço IPv6 começando com 2407, o que indica que o ECS pode obter endereços IPv6.

```
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 4:

    Connection-specific DNS Suffix . : openstacklocal
    IPv6 Address. . . . . : 2407:c080:802:be6:ec23:ec4:c886:cc1
    Link-local IPv6 Address . . . . . : fe80::8836:ab73:1b03:a17d%19
    IPv4 Address. . . . . : 192.168.1.12
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::f816:3eff:fe3e:1e1e%19

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix . : openstacklocal
    IPv6 Address. . . . . : 2407:c080:802:aba:8999:5e61:e19:cf7e
    Link-local IPv6 Address . . . . . : fe80::180d:f3b5:27ac:2acb%14
    IPv4 Address. . . . . : 192.168.0.57
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::f816:3eff:fede:c837%14
    192.168.0.1

Tunnel adapter isatap.openstacklocal:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : openstacklocal

C:\Users\Administrator>_
```

AVISO

Execute esta etapa para os ECSs de origem e de destino para garantir que os ECSs tenham obtido endereços IPv6. Caso contrário, os ECSs não poderão se comunicar uns com os outros usando endereços IPv6.

Os ECSs neste exemplo executam o Windows Server 2012 (64-bit). Nenhuma configuração adicional é necessária para esses ECSs porque eles podem obter endereços IPv6 automaticamente. Se o ECS não conseguir obter endereços IPv6 automaticamente, consulte [Atribuição dinâmica de endereços IPv6](#).

4. Verifique se os ECSs de origem e destino podem se comunicar entre si.

ping -6 -S *IP address of the primary NIC on the source ECS* *IP address of the destination ECS*

ping -6 -S *IP address of the extension NIC on the source ECS* *IP address of the destination ECS*

Neste exemplo, execute os seguintes comandos:

```
ping -6 -S 2407:c080:802:aba:8999:5e61:e19:cf7e 2407:c080:802:be7:c2e6:d99c:b685:c6c8
```

```
ping -6 -S 2407:c080:802:be6:ec23:ec4:c886:cc1 2407:c080:802:be7:c2e6:d99c:b685:c6c8
```

Se informações semelhantes às seguintes forem exibidas, ambas as NICs do ECS de origem poderão se comunicar com o ECS de destino.

```
C:\Users\Administrator>ping -6 -S 2407:c080:802:aba:8999:5e61:e19:cf7e 2407:c080:802:be7:c2e6:d99c:b685:c6c8

Pinging 2407:c080:802:be7:c2e6:d99c:b685:c6c8 from 2407:c080:802:aba:8999:5e61:e19:cf7e with 32 bytes of data:
Reply from 2407:c080:802:be7:c2e6:d99c:b685:c6c8: time<1ms
Reply from 2407:c080:802:be7:c2e6:d99c:b685:c6c8: time<1ms
Reply from 2407:c080:802:be7:c2e6:d99c:b685:c6c8: time<1ms
Reply from 2407:c080:802:be7:c2e6:d99c:b685:c6c8: time<1ms

Ping statistics for 2407:c080:802:be7:c2e6:d99c:b685:c6c8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping -6 -S 2407:c080:802:be6:ec23:ec4:c886:cc1 2407:c080:802:be7:c2e6:d99c:b685:c6c8

Pinging 2407:c080:802:be7:c2e6:d99c:b685:c6c8 from 2407:c080:802:be6:ec23:ec4:c886:cc1 with 32 bytes of data:
Reply from 2407:c080:802:be7:c2e6:d99c:b685:c6c8: time=3ms
Reply from 2407:c080:802:be7:c2e6:d99c:b685:c6c8: time<1ms
Reply from 2407:c080:802:be7:c2e6:d99c:b685:c6c8: time<1ms
Reply from 2407:c080:802:be7:c2e6:d99c:b685:c6c8: time<1ms

Ping statistics for 2407:c080:802:be7:c2e6:d99c:b685:c6c8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

AVISO

Os ECSs neste exemplo executam o Windows Server 2012 (64-bit). Você não precisa configurar rotas baseadas em políticas para esses ECSs porque ambas as NICs de um ECS podem se comunicar com outras pessoas usando IPv6.