Virtual Private Cloud

Perguntas frequentes

Edição 01

Data 2024-09-14

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Marcas registadas e permissões

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

Aviso

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

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

Índice

1 Perguntas gerais

1.1 O que é uma cota?

O que é uma cota?

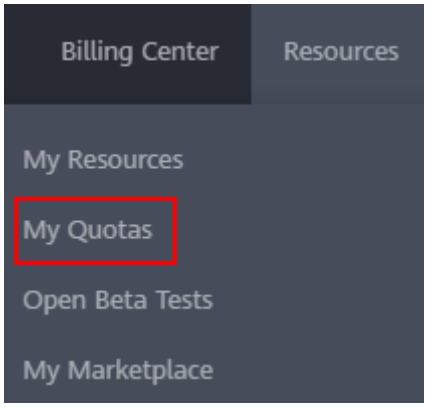
Uma cota limita a quantidade de um recurso disponível para os usuários, evitando picos no uso do recurso. Por exemplo, uma cota de VPC limita o número de VPCs que podem ser criadas.

Você também pode solicitar uma cota aumentada se a cota existente não puder atender às suas necessidades de serviço.

Como fazer para ver minhas cotas?

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. No canto superior direito da página, escolha **Resources** > **My Quotas**.
   A página **Service Quota** é exibida.

   Figura 1-1 Minhas cotas

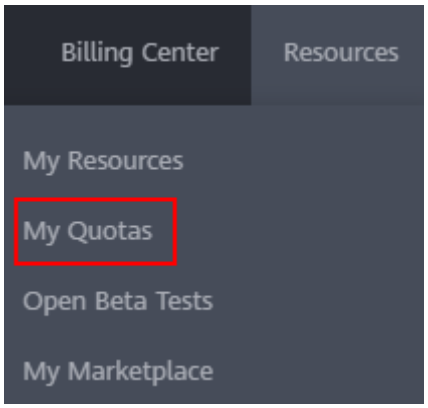
4. Visualize a cota usada e total de cada tipo de recursos na página exibida.
   Se uma cota não puder atender aos requisitos de serviço, solicite uma cota mais alta.

Como fazer para solicitar uma cota mais alta?

1. Acesse o console de gerenciamento.
2. No canto superior direito da página, escolha **Resources** > **My Quotas**.

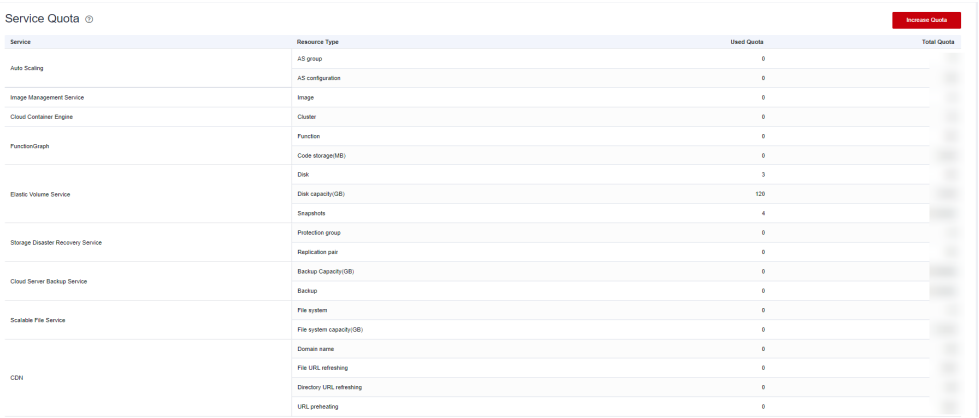
   A página **Service Quota** é exibida.

   Figura 1-2 Minhas cotas

3. Clique em **Increase Quota**.

   Figura 1-3 Increasing quota

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

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

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

2 Cobrança e pagamentos

2.1 Serei cobrado pelo uso do serviço de VPC?

O serviço VPC é gratuito, mas o EIP e a largura de banda usados em conjunto com uma VPC serão cobrados com base no preço padrão.

2.2 Como um EIP é cobrado?

Os EIPs podem ser cobrados em uma base anual/mensal ou de pagamento por uso. As opções de cobrança e os itens de cobrança dependem do modo de cobrança.

- **Figura 2-1**
- **Tabela 2-1**

Figura 2-1 Cobrança de EIP

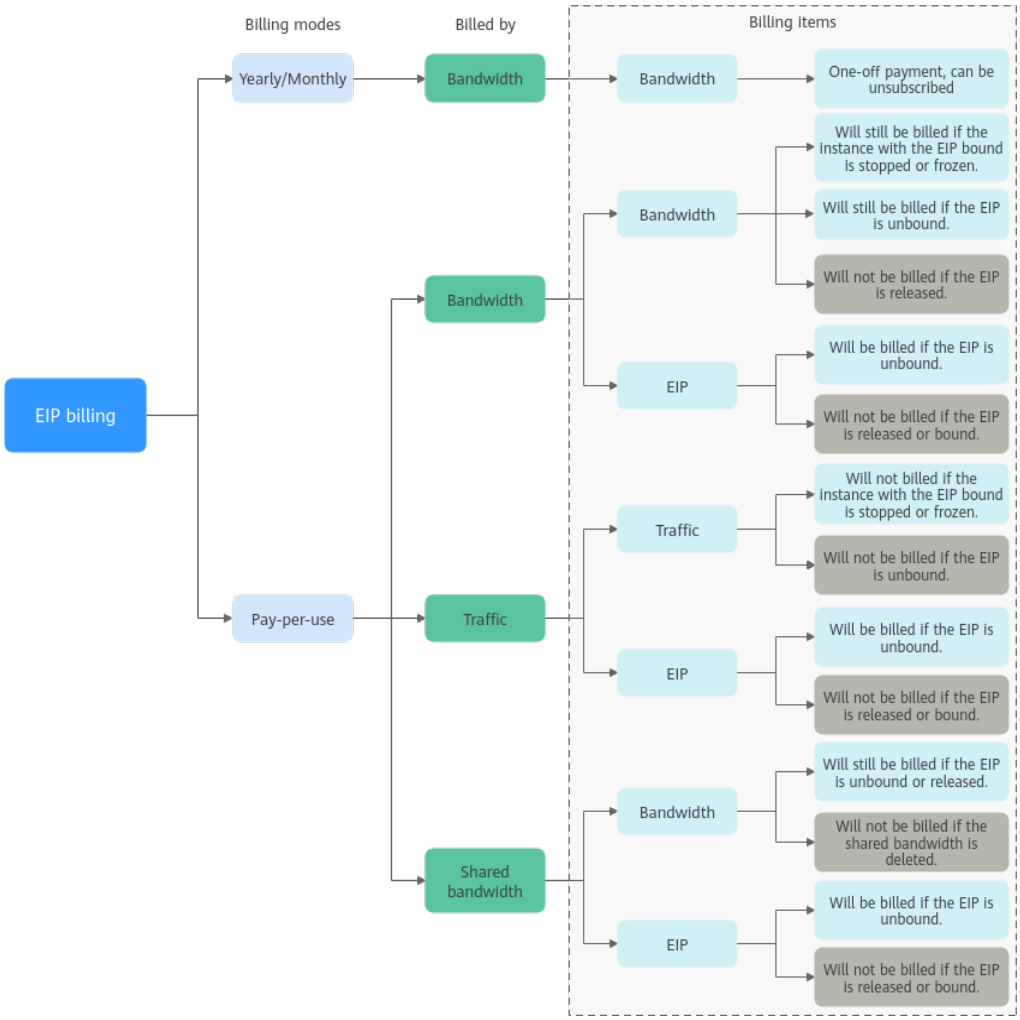


Tabela 2-1 Descrição da cobrança de EIP

Modo de cobrança	Cobrado por	Item cobrado	Descrição do item de cobrança	Impacto das operações de EIP nos itens de cobrança
Anual/Mensal	Largura de banda	Largura de banda	Se você comprar um EIP anual/mensal, precisará pagar apenas pela largura de banda incluída na assinatura. Você é cobrado com base no tamanho da largura de banda e na duração de uso especificados. Não há limite de quanto tráfego você pode usar.	Você pode cancelar a assinatura de uma assinatura anual/mensal. Sua taxa de uso real e algumas taxas preferenciais serão deduzidas do valor do reembolso.

Modo de cobrança	Cobrado por	Item cobrado	Descrição do item de cobrança	Impacto das operações de EIP nos itens de cobrança
Pagamento por uso	Largura de banda	• Largura de banda • EIP	Se um EIP de pagamento por uso for cobrado por largura de banda: • Largura de banda: você é cobrado com base no tamanho da largura de banda e na duração de uso especificados. Não há limite de quanto tráfego você pode usar. Depois que o EIP for comprado, você poderá alterar o tamanho da largura de banda especificada. A largura de banda que você usa não excederá a largura de banda especificada. • Retenção de EIP: se um EIP não for liberado, ele continuará sendo cobrado mesmo que não esteja vinculado a uma instância.	Após a compra de um EIP: • Se o EIP não estiver vinculado a nenhuma instância, tanto o EIP quanto sua largura de banda serão cobrados. • Se o EIP estiver vinculado a uma instância, somente a largura de banda será faturada. **A largura de banda será cobrada independentemente de a instância vinculada ao EIP estar em execução ou não.** • **Depois que o EIP for desvinculado de uma instância, a largura de banda continuará a ser cobrada. A menos que seja liberado, o EIP ainda será cobrado.** • Se o EIP for liberado, tanto o EIP quanto sua largura de banda não serão cobrados.

Modo de cobrança	Cobrado por	Item cobrado	Descrição do item de cobrança	Impacto das operações de EIP nos itens de cobrança
	Tráfego	● Tráfego ● EIP	Se um EIP de pagamento por uso for cobrado por tráfego: ● Tráfego: você é cobrado com base no seu tipo de EIP e na quantidade total de tráfego saindo da nuvem. O tamanho da largura de banda que você define é usado apenas para limitar a taxa máxima de transferência de dados. Para evitar altas taxas causadas pelo tráfego de intermitência, especifique um tamanho de largura de banda adequado ao comprar um EIP. ● Retenção de EIP: se um EIP não for liberado, ele continuará sendo cobrado mesmo que não esteja vinculado a uma instância.	Após a compra de um EIP: ● Se o EIP não estiver vinculado a uma instância, você será cobrado pelo próprio EIP, mas não pelo tráfego. ● Se o EIP estiver vinculado a uma instância, somente o tráfego usado será cobrado. **Se a instância vinculada ao EIP parar de ser executada e não houver tráfego gerado, não haverá taxas de tráfego nem de EIP.** ● **Depois que o EIP for desvinculado de uma instância, o tráfego não será cobrado, mas o EIP ainda será cobrado.** ● Se o EIP for liberado, o EIP não será cobrado.

Modo de cobrança	Cobrado por	Item cobrado	Descrição do item de cobrança	Impacto das operações de EIP nos itens de cobrança
	Largura de banda compartilhada	• Largura de banda compartilhada • EIP	Se um EIP de pagamento por uso for adicionado a uma largura de banda compartilhada: • Largura de banda compartilhada: somente a largura de banda compartilhada será cobrada. Não haverá custos adicionais de largura de banda ou tráfego para EIPs adicionados à largura de banda compartilhada. • Retenção de EIP: se um EIP não for liberado, ele continuará sendo cobrado mesmo que não esteja vinculado a uma instância.	Após a compra de um EIP: • Largura de banda compartilhada – Nenhuma operação no EIP afetará a cobrança de uma largura de banda compartilhada. Por exemplo, se você liberou o EIP, mas não excluiu a largura de banda compartilhada, a largura de banda compartilhada ainda será cobrada. – Depois que uma largura de banda compartilhada for excluída, ela não será mais cobrada. • EIP – Se o EIP não estiver vinculado a uma instância, o EIP ainda será cobrado. – Se o EIP for desvinculado de uma instância, ele será cobrado para mantê-lo alocado à sua conta, a menos que seja liberado. – Se o EIP for liberado ou vinculado a uma instância, o EIP não será cobrado.

Para economizar dinheiro, você pode adicionar vários EIPs na mesma região a uma largura de banda compartilhada. Uma largura de banda compartilhada pode ser cobrada em uma base

anual/mensal ou de pagamento por uso. Para obter detalhes, consulte **Tabela 2-2**. Atualmente, apenas EIPs de pagamento por uso podem ser adicionados a uma largura de banda compartilhada.

- Você pode adicionar um EIP a uma largura de banda compartilhada ao comprar o EIP.
- Você também pode adicionar um EIP existente a uma largura de banda compartilhada. Depois que o EIP é adicionado a uma largura de banda compartilhada, não haverá largura de banda adicional ou custo de tráfego. Você será cobrado apenas pela largura de banda compartilhada.

Tabela 2-2 Detalhes de cobrança de largura de banda compartilhada

Modo de cobrança	Cobrado por	Item cobrado	Descrição do item de cobrança
Anual/ Mensal	Largura de banda	Largura de banda	Se você comprar uma largura de banda compartilhada anual/mensal, será cobrado com base no tamanho da largura de banda especificada e na duração de uso. Não há limite de quanto tráfego você pode usar.
Pagamento por uso	Largura de banda	Largura de banda	você é cobrado com base no tamanho da largura de banda e na duração de uso especificados. Não há limite de quanto tráfego você pode usar. Depois que uma largura de banda compartilhada é comprada, você pode alterar o tamanho da largura de banda especificada. A largura de banda que você usa não excederá a largura de banda especificada.

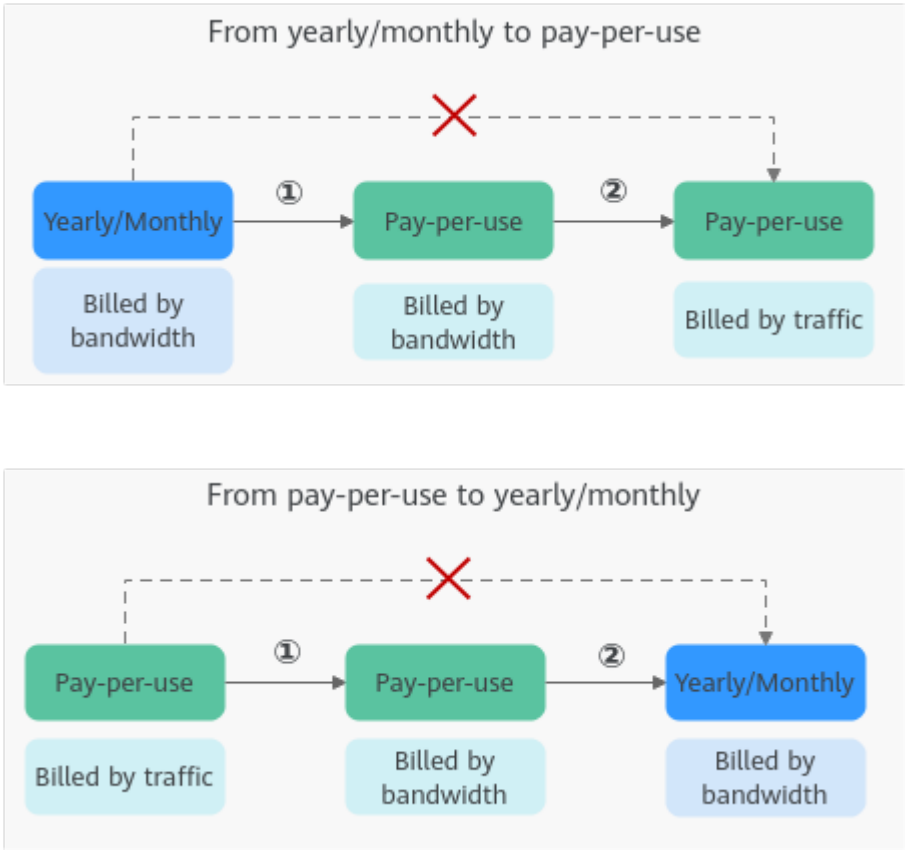
Consulte **Cobrança**.

2.3 Como alterar meu modo de cobrança do EIP de pagamento por uso para anual/mensal?

Tabela 2-3 Descrição da alteração do modo de cobrança

Alteração	Descrição
De anual/mensal para pagamento por uso	● Um EIP cobrado em uma base anual/mensal pode ser alterado diretamente para ser cobrado por largura de banda em uma base de pagamento por uso. ● Um EIP cobrado em uma base anual/mensal não pode ser alterado diretamente para ser cobrado pelo tráfego em uma base de pagamento por uso. Para alterar isso: 1. Primeiro, altere o EIP cobrado em uma base anual/mensal para ser cobrado por largura de banda em uma base de pagamento por uso. 2. Em seguida, altere o EIP cobrado por largura de banda em uma base de pagamento por uso para ser cobrado por tráfego em uma base de pagamento por uso. O novo modo de cobrança só entra em vigor após a expiração da cobrança anual/mensal.
De pagamento por uso a anual/mensal	● Um EIP que é cobrado por largura de banda em uma base de pagamento por uso pode ser alterado diretamente para ser cobrado em uma base anual/mensal. ● Um EIP que é cobrado por tráfego em uma base de pagamento por uso não pode ser alterado diretamente para ser cobrado em uma base anual/mensal. Para alterar isso: 1. Primeiro, altere o EIP cobrado pelo tráfego em uma base de pagamento por uso para ser cobrado por largura de banda em uma base de pagamento por uso. 2. Em seguida, altere o EIP cobrado por largura de banda em uma base de pagamento por uso para ser cobrado anualmente/mensalmente. Depois que a alteração for bem-sucedida, o novo modo de cobrança entrará em vigor imediatamente.

Figura 2-2 Alteração do modo de faturamento do EIP



De anual/mensal para pagamento por uso na expiração (cobrado por largura de banda)

1. Faça logon no console de gerenciamento.
2. No canto superior direito da página, escolha **Billing & Costs** > **Renewal**.
3. Na lista de recursos, procure o EIP cujo modo de cobrança precisa ser alterado.
4. Localize a linha que contém o EIP e escolha **More** > **Change to Pay-per-Use After Expiration** na coluna **Operation**.
5. Confirme as configurações e clique em **Change to Pay-per-Use**.

   Após a conclusão da operação, o EIP anual/mensal é alterado para ser cobrado por largura de banda em uma base de pagamento por uso.

2.4 Como alterar um EIP de pagamento por uso de cobrança por largura de banda para tráfego ou de cobrança por tráfego para largura de banda?

Tabela 2-4 Descrição da mudança

Alteração	Descrição
EIP de pagamento por uso: da cobrança por tráfego para por largura de banda	Um EIP de pagamento por uso cobrado pelo tráfego pode ser alterado diretamente para ser cobrado pela largura de banda. Depois que a alteração for bem-sucedida, o novo modo de cobrança entrará em vigor imediatamente.
EIP de pagamento por uso: da cobrança por largura de banda até por tráfego	Um EIP de pagamento por uso cobrado pela largura de banda pode ser alterado diretamente para ser cobrado pelo tráfego. Depois que a alteração for bem-sucedida, o novo modo de cobrança entrará em vigor imediatamente.

De cobrado por tráfego a por largura de banda (EIP de pagamento por uso)

1. Faça logon no console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione a região e o projeto desejados.
3. Em **Rede**, clique em **Elastic IP**.
4. Na lista de EIP, localize a linha que contém o EIP, clique em **More** na coluna **Operation** e clique em **Modify Bandwidth**.
5. Na página **Modify Bandwidth**, altere a opção de cobrança conforme solicitado.
   Você também pode alterar o nome e o tamanho da largura de banda.
6. Clique em **Next**.
7. Na página exibida, confirme as configurações e clique em **Submit**.

NOTA

- Alterar as opções de cobrança não altera os EIPs nem interrompe seu uso.
- Os seguintes cenários de alteração aplicam-se apenas a EIPs **pay-per-use**.
- Os EIPs **Yearly/monthly** não podem ser alterados diretamente para EIPs de pagamento por uso cobrados pelo tráfego. Se a mudança for necessária, consulte **Como alterar meu modo de cobrança do EIP de pagamento por uso para anual/mensal?**

2.5 Por que ainda estou sendo cobrado depois que todas as VPCs foram excluídas?

Sintoma

As cobranças são geradas mesmo que todas as VPCs tenham sido excluídas.

Possíveis causas

As VPCs são gratuitas, mas você ainda é cobrado pelos EIPs usados em conjunto com uma VPC.

- EIPs podem estar em uso em outros projetos ou regiões. Você pode exibir todos os EIPs na central de cobrança, localizar o EIP e alternar para o projeto ou região onde o EIP está localizado e liberá-lo.
- As informações na fatura são do seu período de liquidação anterior. Geralmente, as taxas não são deduzidas da sua conta imediatamente após a liberação dos EIPs de pagamento por uso. Em vez disso, as contas são geradas e as taxas são deduzidas da sua conta somente após o término do período de liquidação.

3 VPCs e sub-redes

3.1 O que é Virtual Private Cloud?

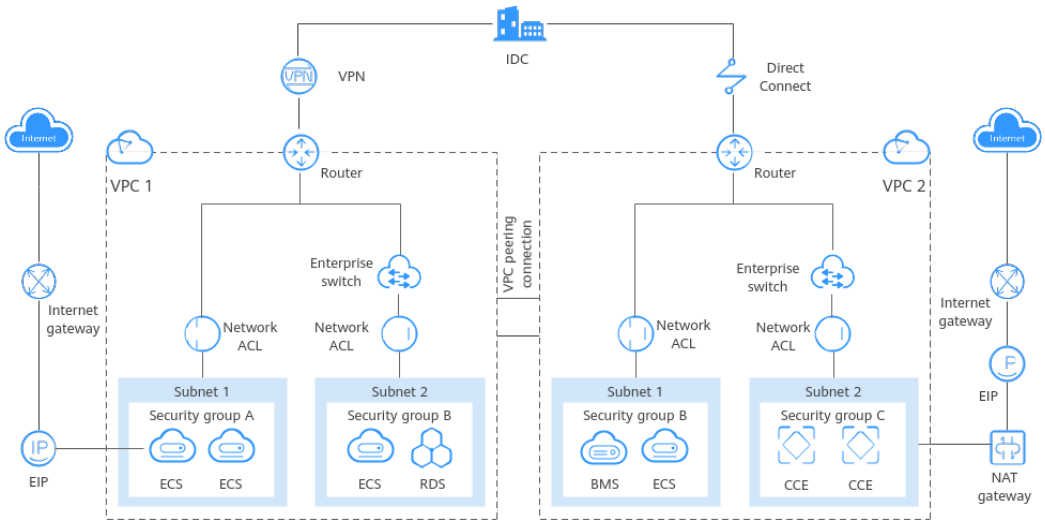
O serviço Virtual Private Cloud (VPC) permite provisionar redes virtuais logicamente isoladas para recursos de nuvem, como servidores de nuvem, contêineres e bancos de dados. Você pode criar sub-redes personalizadas, grupos de segurança, network ACLs e atribuir EIPs e larguras de banda. Com a Direct Connect ou a Virtual Private Network (VPN), você pode conectar suas VPCs a um data center local.

O serviço VPC usa tecnologias de virtualização de rede, como redundância de links, clusters de gateway distribuídos e implementação em várias AZs, para garantir a segurança, a estabilidade e a disponibilidade da rede.

Arquitetura do produto

A arquitetura do produto consiste em componentes da VPC, recursos de segurança e opções de conectividade da VPC.

Figura 3-1 Arquitetura



Visão geral da tabela de rotas

Componentes da VPC

Cada VPC consiste em um bloco CIDR privado, tabelas de rotas e pelo menos uma sub-rede.

- Bloco CIDR privado: ao criar uma VPC, é necessário especificar o bloco CIDR privado utilizado pela VPC. O serviço VPC é compatível com seguintes blocos CIDR: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255 e 192.168.0.0 – 192.168.255.255
- Sub-redes: recursos em nuvem (como servidores e bancos de dados em nuvem) devem ser implementados em sub-redes. Depois de criar uma VPC, você pode dividi-la em uma ou mais sub-redes. Cada sub-rede deve estar dentro da VPC. Para mais informações, consulte **Sub-rede**.
- Tabelas de rotas: quando você cria uma VPC, o sistema gera automaticamente uma tabela de rotas predefinida. A tabela de rotas garante que todas as sub-redes na mesma VPC possam se comunicar entre si. Se as rotas na tabela de rotas padrão não puderem atender aos requisitos da aplicação (por exemplo, se houver um ECS sem um endereço IP elástico (EIP) vinculado que precisa acessar a Internet), você pode criar uma tabela de rotas personalizada. Para obter mais informações, consulte **Visão geral da tabela de rotas**.

Recursos de segurança

Grupos de segurança e network ACLs garantem a segurança dos recursos de nuvem implantados em uma VPC. Um grupo de segurança atua como um firewall virtual para fornecer regras de acesso para instâncias que têm os mesmos requisitos de segurança e são mutuamente confiáveis em uma VPC. Para mais informações, consulte **Visão geral de grupo de segurança**. Uma network ACL pode ser associada a sub-redes que tenham os mesmos requisitos de controle de acesso. Você pode adicionar regras de entrada e saída para controlar com precisão o tráfego de entrada e saída no nível da sub-rede. Para mais informações, consulte **Visão geral de Network ACL**.

Conectividade de VPC

Huawei Cloud oferece várias opções de conectividade VPC para atender a diferentes requisitos. Para obter detalhes, consulte **Cenários de aplicação**.

- O emparelhamento de VPC permite que duas VPCs na mesma região se comuniquem usando endereços IP privados.
- Elastic IP ou NAT Gateway permite que os ECSs em uma VPC se comuniquem com a Internet.
- Virtual Private Network (VPN), Cloud Connect ou Direct Connect podem conectar uma VPC ao seu data center.

3.2 Quais blocos CIDR estão disponíveis para o serviço VPC?

A tabela a seguir lista os blocos CIDR privados que você pode especificar ao criar uma VPC. Considere o seguinte ao selecionar um bloco CIDR de VPC:

- Número de endereços IP: reserve endereços IP suficientes em caso de crescimento do negócio.
- Intervalo de endereços IP: evite conflitos de endereço IP se precisar conectar uma VPC a um data center local ou conectar duas VPCs.

O serviço VPC é compatível com seguintes blocos CIDR:

Bloco CIDR da VPC	Intervalo de endereços IP	Número máximo de endereços IP
10.0.0.0/8-24	10.0.0.0-10.255.255.255	2^24-2=16777214
172.16.0.0/12-24	172.16.0.0-172.31.255.255	2^20-2=1048574
192.168.0.0/16-24	192.168.0.0-192.168.255.255	2^16-2=65534

3.3 Quantas VPCs posso criar?

Por padrão, você pode criar no máximo cinco VPCs na sua conta. Se o número de VPCs não atender às suas necessidades de serviço, **envie um tíquete de serviço**.

3.4 As sub-redes podem se comunicar umas com as outras?

Sub-redes na mesma VPC podem se comunicar entre si, mas aqueles em diferentes VPCs não podem fazer o mesmo por padrão. No entanto, você pode criar conexões de emparelhamento de VPC para permitir que sub-redes em diferentes VPCs se comuniquem entre si.

NOTA

Se as sub-redes tiverem ACLs da rede associadas, regra de ACL da rede deve permitir a comunicação entre as sub-redes.

3.5 Que blocos CIDR de sub-rede estão disponíveis?

Um bloco CIDR de sub-rede deve ser incluído em seu bloco CIDR da VPC. Os blocos CIDR da VPC compatíveis são **10.0.0.0/8–24**, **172.16.0.0/12–24** e **192.168.0.0/16–24**. O tamanho de bloco permitido de uma sub-rede está entre a máscara de rede de seu bloco CIDR de VPC e a máscara de rede /28.

3.6 Posso modificar o bloco CIDR de uma sub-rede?

Você pode modificar o bloco CIDR de uma sub-rede somente quando estiver criando a sub-rede. Depois que a sub-rede é criada, você não pode modificar seu bloco CIDR.

3.7 Quantas sub-redes posso criar?

Por padrão, você pode criar um máximo de 100 sub-redes em sua conta de nuvem. Se o número de sub-redes não puder atender aos requisitos de serviço, **envie um tíquete de serviço** para solicitar um aumento de cota.

3.8 Como fazer com que o tempo de concessão de DHCP alterado de uma sub-rede entre em vigor imediatamente?

Cenários

Depois que você alterar o tempo de concessão de DHCP no console, os ECSs existentes não usarão a nova concessão de DHCP até que a concessão atual precise ser renovada. Uma concessão é renovada quando metade do tempo de concessão tiver decorrido. Por exemplo, se um contrato de 30 dias for definido em 1º de janeiro, o contrato será renovado em 15 de janeiro.

Se você precisar fazer com que o novo tempo de concessão de DHCP entre em vigor imediatamente para ECSs na sub-rede, consulte o procedimento a seguir.

NOTA

Se você renovar a concessão de DHCP manualmente, os endereços IP atuais dos ECSs serão liberados. Os ECSs não têm endereços IP até que a nova versão entre em vigor e sejam atribuídos a novos endereços IP, o que pode causar interrupção do serviço.

Você também pode reiniciar diretamente os ECSs para que a nova versão do DHCP entre em vigor imediatamente.

Procedimento

Para um ECS do Windows:

1. Depois que você altera o tempo de concessão de DHCP no console, faça logon no ECS cuja concessão você deseja atualizar.
2. Escolha **Start** > **Run**. Digite cmd para abrir o prompt de comando.
3. Veja o tempo de expiração da concessão de DHCP atual:

   ipconfig /all

4. Atualize a concessão de DHCP:

   ipconfig /release && ipconfig /renew

5. Verifique o novo tempo de expiração da concessão de DHCP:

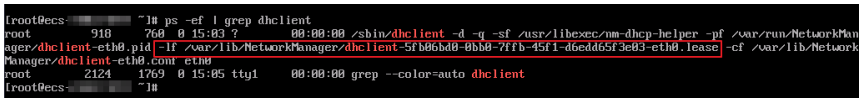
   ipconfig /all

Para um ECS do Linux:

1. Depois que você altera o tempo de concessão de DHCP no console, faça logon no ECS cuja concessão você deseja atualizar.
2. Verifique se o cliente que fornece o serviço DHCP é **dhclient**:

   ps -ef | grep dhclient

   – Se informações semelhantes às seguintes forem exibidas, o processo **dhclient** existe e o cliente é **dhclient**. O arquivo **lease** que segue o parâmetro **-lf** contém informações de concessão.



– Se o processo de **dhclient** não existir, este procedimento pode não ser aplicável. Neste caso, você precisa procurar os comandos de operação do cliente de DHCP correspondente.

3. Libere o endereço IP do ECS:

   dhclient -r

4. Obtenha a nova concessão de DHCP:

   killall dhclient && systemctl restart NetworkManager

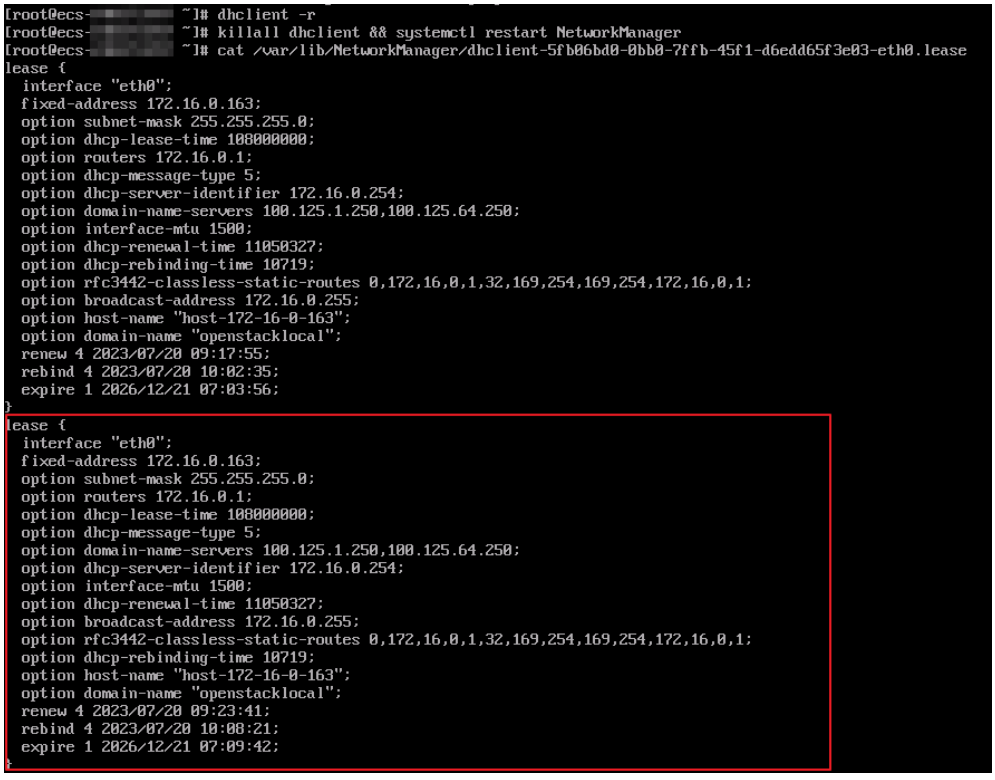
5. Exibir as informações de concessão de DHCP mais recentes no arquivo **lease** obtido em **2**:

   cat *lease* *File name*

   Exemplo de comando:

   cat /var/lib/NetworkManager/dhclient-5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03-eth0.lease

   Informação semelhante à seguinte foi exibida. O arquivo **lease** contém informações históricas de concessão de DHCP e as informações após a última **lease** são sobre a concessão de DHCP mais recente.



3.9 Como fazer com que um nome de domínio em uma sub-rede entre em vigor imediatamente após ser alterado?

Ao criar uma sub-rede, você também pode configurar nomes de domínio. Para acessar um nome de domínio, você só precisa inserir o prefixo do nome de domínio e os ECSs na sub-rede corresponderão automaticamente ao sufixo do nome de domínio. Depois que uma sub-rede é criada, você pode alterar os nomes de domínio configurados. **Tabela 3-1** descreve como fazer a alteração entrar em vigor.

Tabela 3-1 Políticas eficazes de nome de domínio

ECS	Política eficaz
Novos ECSs na sub-rede	Os ECSs recém-adicionados a uma sub-rede usarão os novos nomes de domínio automaticamente. Não é necessária configuração adicional.
ECSs existentes em uma sub-rede	Para usar os novos nomes de domínio, você pode usar um dos seguintes métodos: ● Reiniciar o ECS. ● Reiniciar o serviço de cliente de DHCP: **service dhcpd restart** ● Reiniciar o serviço de rede: **service network restart** **NOTA** O comando para atualizar a configuração de DHCP depende do SO do ECS. Os comandos aqui são para sua referência.

3.10 Por que não consigo excluir minhas VPCs e sub-redes?

Se VPCs e sub-redes estiverem sendo usadas por outros recursos, você precisará primeiro excluir esses recursos com base nos prompts no console antes de excluir as VPCs e as sub-redes. A seguir, fornece prompts de exclusão detalhados e o guia de exclusão correspondente.

- **Exclusão de sub-redes**
- **Exclusão de VPCs**

AVISO

As VPCs e as sub-redes são gratuitas.

Exclusão de sub-redes

Você pode consultar **Tabela 3-2** para excluir sub-redes.

Tabela 3-2 Excluir sub-redes

Prompts	Causa	Solução
Você não tem permissão para realizar essa operação.	Sua conta não tem permissões para excluir sub-redes.	Entre em contato com o administrador da conta para conceder permissões à sua conta e exclua a sub-rede. **Gerenciamento de permissões**

Prompts	Causa	Solução
Exclua rotas personalizadas da tabela de rotas associada da sub-rede e, em seguida, exclua a sub-rede.	A tabela de rotas tem rotas personalizadas com o seguinte tipo de salto seguinte: ● Servidor ● NIC de extensão ● Virtual IP address ● NAT gateway	Exclua a rota personalizada da tabela de rotas e, em seguida, exclua a sub-rede. 1. **Exibição da tabela de rotas associada a uma sub-rede** 2. **Exclusão de uma rota**
Libere quaisquer endereços IP virtuais configurados na sub-rede e, em seguida, exclua a sub-rede.	A sub-rede tem endereços IP virtuais configurados.	Libere os endereços IP virtuais da sub-rede e, em seguida, exclua a sub-rede. **Liberação de um endereço IP virtual**
Libere quaisquer endereços IP privados configurados na sub-rede e, em seguida, exclua a sub-rede.	A sub-rede tem endereços IP virtuais que não são usados por nenhuma instância.	Na guia **IP Addresses**, visualize e libere esses endereços IP privados e exclua a sub-rede. 1. **Visualização de endereços IP em uma sub-rede** 2. Na lista de endereços IP privados, localize o endereço IP que não está sendo usado e clique em **Release** na coluna **Operation**. **AVISO** Se você quiser liberar um endereço IP privado em uso, precisará excluir o recurso que usa o endereço IP primeiro.
Exclua o recurso (ECS ou balanceador de carga) que está usando a sub-rede e, em seguida, exclua a sub-rede.	A sub-rede está sendo usada por um ECS ou um balanceador de carga.	Exclua o ECS ou o balanceador de carga e, em seguida, exclua a sub-rede. **Exibição e exclusão de recursos em uma sub-rede**

Prompts	Causa	Solução
Exclua o balanceador de carga que está usando a sub-rede e, em seguida, exclua a sub-rede.	A sub-rede está sendo usada por um balanceador de carga.	Exclua o balanceador de carga e, em seguida, exclua a sub-rede. **Exibição e exclusão de recursos em uma sub-rede**
Exclua o gateway de NAT que está usando a sub-rede e, em seguida, exclua a sub-rede.	A sub-rede está sendo usada por um gateway de NAT.	Exclua o gateway de NAT e, em seguida, exclua a sub-rede. **Exibição e exclusão de recursos em uma sub-rede**
Exclua o recurso que está usando a sub-rede e exclua a sub-rede.	A sub-rede está sendo usada pelos recursos da nuvem.	Na guia **IP Addresses**, visualize o uso do endereço IP, localize o recurso que está usando o endereço IP, exclua o recurso e exclua a sub-rede. 1. **Visualização de endereços IP em uma sub-rede** 2. Localize o recurso com base no uso do endereço IP, referindo-se a **Pesquisar recursos na nuvem**. 3. Exclua o recurso e, em seguida, exclua a sub-rede.

Excluir VPCs

Antes de excluir uma VPC, verifique se todas as sub-redes da VPC foram excluídas. Você pode consultar **Tabela 3-3** para excluir VPCs.

Tabela 3-3 Excluir VPCs

Mensagens	Causa	Solução
Você não tem permissão para realizar essa operação.	Sua conta não tem permissões para excluir VPCs.	Entre em contato com o administrador da conta para conceder permissões à sua conta e excluir a VPC. **Gerenciamento de permissões**

Mensagens	Causa	Solução
Exclua o serviço de ponto de extremidade da VPC ou a rota configurada para o serviço da tabela de rotas da VPC e, em seguida, exclua a VPC.	A tabela de rotas da VPC tem rotas personalizadas.	Exclua as rotas personalizadas e, em seguida, exclua a VPC. 1. Na lista de VPC, localize a linha que contém a VPC e clique no número na coluna **Route Tables**. A lista da tabela de rotas é exibida. 2. **Exclusão de uma rota**
	A VPC está sendo usada por um serviço de ponto de extremidade da VPC.	Pesquise o serviço de ponto de extremidade da VPC no console de serviço de ponto de extremidade da VPC e exclua-o. **Exclusão de um serviço do ponto de extremidade da VPC**
A VPC não pode ser excluída, porque há recursos vinculados.	A VPC está sendo usada pelos seguintes recursos: ● Sub-rede ● Conexão de emparelhamento de VPC ● Tabela de rota personalizada	Clique no hiperlink do nome do recurso conforme solicitado para excluir o recurso. ● **Tabela 3-2** ● **Exclusão de uma conexão de emparelhamento de VPC** ● **Exclusão de uma tabela de rotas**
Exclua o gateway virtual que está usando a VPC e, em seguida, exclua a VPC.	A VPC está sendo usada por um gateway virtual da Direct Connect.	No console da Direct Connect, localize o gateway virtual e exclua-o. **Exclusão de um gateway virtual**
Exclua o gateway da VPN que está usando a VPC e, em seguida, exclua a VPC.	A VPC está sendo usada por um gateway da VPN.	No console da VPN, localize o gateway da VPN e exclua-o. **Exclusão de um gateway de VPN**
Remova a VPC da conexão de nuvem e exclua a VPC.	A VPC está sendo usada por uma conexão da Cloud Connect.	No console da Cloud Connect, localize a conexão e remova a VPC dela. **Remoção de uma instância de rede**

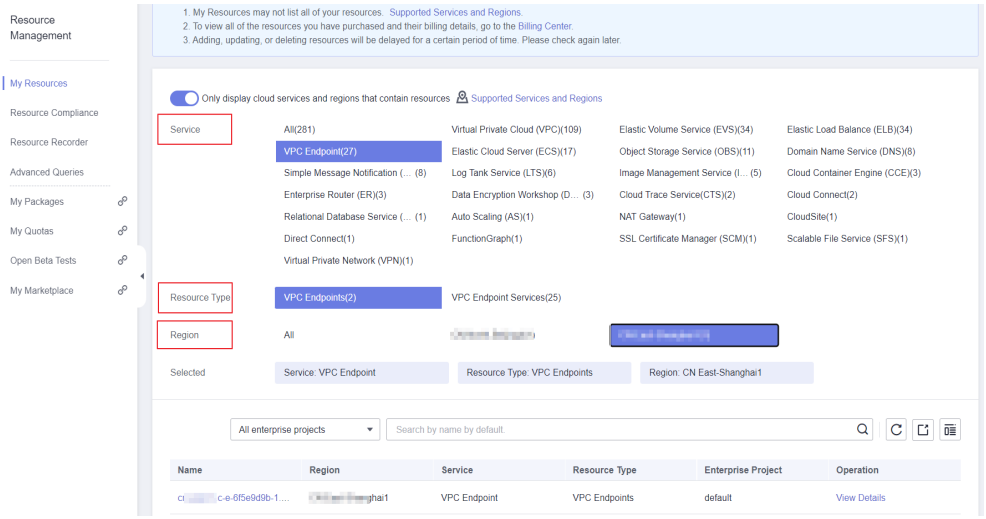
Mensagens	Causa	Solução
Exclua todos os grupos de segurança personalizados nessa região e exclua essa última VPC.	Na região atual, essa é a última VPC e há grupos de segurança personalizados. **AVISO** Você só precisa excluir os grupos de segurança personalizados. O grupo de segurança padrão não afeta a exclusão de VPCs.	Exclua todos os grupos de segurança personalizados e, em seguida, exclua a VPC. **Exclusão de um grupo de segurança**
Libere todos os EIPs nessa região e exclua essa última VPC.	Na região atual, esta é a última VPC e há EIPs.	Libere todos os EIPs e exclua a VPC. **Liberação de um EIP**

Pesquisar recursos na nuvem

1. Faça logon no console de gerenciamento.
2. No canto superior direito do console, escolha **More** > **Resources** > **My Resources**.

   A página **My Resources** é exibida.

   Figura 3-2 Meus recursos



3. Na página **My Resources**, defina critérios de pesquisa para encontrar rapidamente os recursos na sub-rede.
   - **Service**: selecione um serviço que tenha recursos em sub-redes.

     Tabela 3-4 lista alguns recursos comuns. Se você tiver outros recursos, verifique-os.

- **Resource Type**: verifique os tipos de recursos.
- **Region**: selecione a região em que a VPC e a sub-rede estão localizadas para filtrar recursos na mesma região. As VPCs e as sub-redes podem ser usadas apenas por recursos de sua mesma região.

Tabela 3-4 Recursos comuns em sub-redes

Categoria de produto	Serviço
Computação	Elastic Cloud Server (ECS)
	Bare Metal Server (BMS)
	Cloud Container Engine (CCE)
	Cloud Container Instance (CCI)
Contêineres	Application Service Mesh (ASM)
Redes	Elastic Load Balance (ELB)
	NAT Gateway
	VPC Endpoint (VPCEP)
Bancos de dados	GaussDB
	Relational Database Service (RDS)
	Document Database Service (DDS)
	GaussDB NoSQL
	Distributed Database Middleware (DDM)
Middleware	Distributed Cache Service (DCS) ● Instância do Redis ● Instância do Memcached
	Distributed Message Service (DMS) ● Instância de Kafka ● Instância do RabbitMQ
EI	MapReduce Service (MRS)
	Data Warehouse Service (DWS)
	Cloud Search Service (CSS)

Se você não puder excluir uma sub-rede mesmo depois de excluir todos os recursos que ela contém, **envie um tíquete de serviço**.

3.11 Posso alterar a VPC de um ECS?

Sim.

Você pode clicar em **Change VPC** na coluna **Operation** na página **Elastic Cloud Server**.

Para obter detalhes, consulte **Alteração de uma VPC**.

3.12 Por que o endereço IP do ECS é perdido depois que a hora do sistema é alterada?

Causa: isso ocorre porque a diferença de tempo entre a hora antiga e a nova é maior do que o tempo de concessão DHCP. O tempo de concessão de DHCP predefinido definido quando cria uma sub-rede é de 365 dias. Se você alterar manualmente a hora do sistema do ECS e a diferença de hora entre a antiga e a nova for maior que 365 horas, a concessão de DHCP não será renovada e o endereço IP do ECS será perdido.

Solução: se você precisar alterar a hora do sistema ECS e a diferença de tempo for maior do que a hora de liberação do DHCP, altere o modo de atribuição de endereço IP do ECS para estático antes de alterar a hora do sistema ECS.

3.13 Como alterar o endereço do servidor do DNS de um ECS?

Cenários

Esta seção descreve como alterar o endereço do servidor do DNS de um ECS e fazer com que o novo endereço do servidor do DNS entre em vigor imediatamente no ECS.

As operações necessárias são as seguintes:

Alterar servidores do DNS para o ECS

Conhecimento de fundo

Os ECSs usam servidores do DNS privados para resolução de nomes de domínio em VPCs. Os servidores do DNS privados não afetam a resolução de nomes de domínio para que os ECSs acessem a Internet. Além disso, você pode usar os servidores do DNS privados para acessar diretamente os endereços IP privados dos serviços em nuvem, como OBS e SMN. Em comparação com o acesso através da Internet, este acesso apresenta alto desempenho e baixa latência.

Antes de os nomes de domínio privados estarem disponíveis, as sub-redes da VPC usam o servidor do DNS público (114.114.114.114). Para permitir que os ECSs nessas VPCs acessem nomes de domínio privados, você pode alterar o servidor do DNS público para os servidores do DNS privados configurados para as sub-redes da VPC. Para obter instruções sobre como obter um endereço de servidor do DNS privado, consulte **Quais são os servidores do DNS privados fornecidos pelo serviço DNS da Huawei Cloud?**

Alterar servidores do DNS para o ECS

Depois que você alterar os endereços de servidor do DNS de uma sub-rede da VPC, os endereços de servidor do DNS dos ECSs na sub-rede não entrarão em vigor imediatamente.

Para que os endereços de servidor do DNS entrem em vigor imediatamente, faça o seguinte:

- Reinicie o sistema operacional. Em seguida, o ECS obterá os novos endereços de servidor do DNS do servidor DHCP.

  AVISO

  Reiniciar o SO interromperá os serviços no ECS. Portanto, realize esta operação fora dos horários de pico.

  Como alternativa, aguarde até que a concessão DHCP expire, que é de 365 dias por padrão. Depois que o tempo de concessão expira, o servidor DHCP aloca outro endereço IP e atualiza os endereços do servidor do DNS para o ECS.

- Obtenha os novos endereços de servidor do DNS.

  a. Efetue logon no ECS.

  b. Execute o seguinte comando para exibir o endereço do servidor do DNS do ECS:

     cat /etc/resolv.conf

     Se informações semelhantes às seguintes forem exibidas, 114.114.114.114 é o endereço do servidor do DNS do ECS.

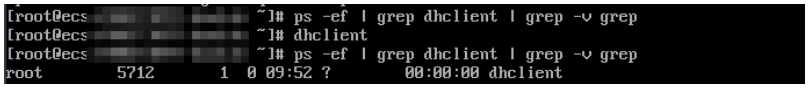
     

  c. Execute o seguinte comando para verificar se o processo **dhclient** existe:

     ps -ef | grep dhclient | grep -v grep

     Se informações semelhantes às seguintes forem exibidas, nenhum processo existe (o CentOS 8.1 é usado como exemplo).

     Neste caso, execute o comando **dhclient** para iniciar o processo e verificar se o processo **dhclient** existe.

     Se informações semelhantes às seguintes forem exibidas, o processo existe (o CentOS 7.2 é usado como exemplo).

  d. Execute o seguinte comando para liberar o endereço do servidor do DNS atual:

     dhclient -r

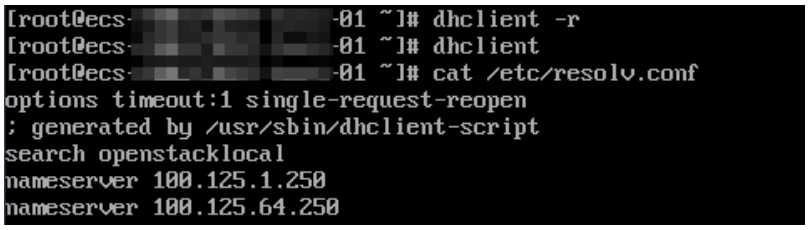
  e. Execute o seguinte comando para reiniciar o processo **dhclient** e obter novos endereços de servidor do DNS:

     dhclient

  f. Execute o comando a seguir para exibir os novos endereços de servidor do DNS do ECS:

     cat /etc/resolv.conf

     Se informações semelhantes às seguintes forem exibidas, 100.125.1.250 e 100.125.64.250 serão os novos endereços de servidor do DNS do ECS.



4 EIPs

4.1 Como atribuir ou recuperar um EIP específico?

Se você quiser recuperar um EIP que você lançou ou atribuir um EIP específico, você pode usar APIs definindo o valor de **ip_address** para aquele que você deseja atribuir. Para obter detalhes, consulte **Referência da API do Elastic IP**.

NOTA

- Se o EIP tiver sido atribuído a outro usuário, você não conseguirá atribuir o EIP necessário.
- Você não pode usar o console de gerenciamento para atribuir um EIP específico.

4.2 Quais são as diferenças entre EIP, endereço IP privado e endereço IP virtual?

Diferentes tipos de endereços IP têm diferentes funções.

Figura 4-1 Arquitetura do endereço IP

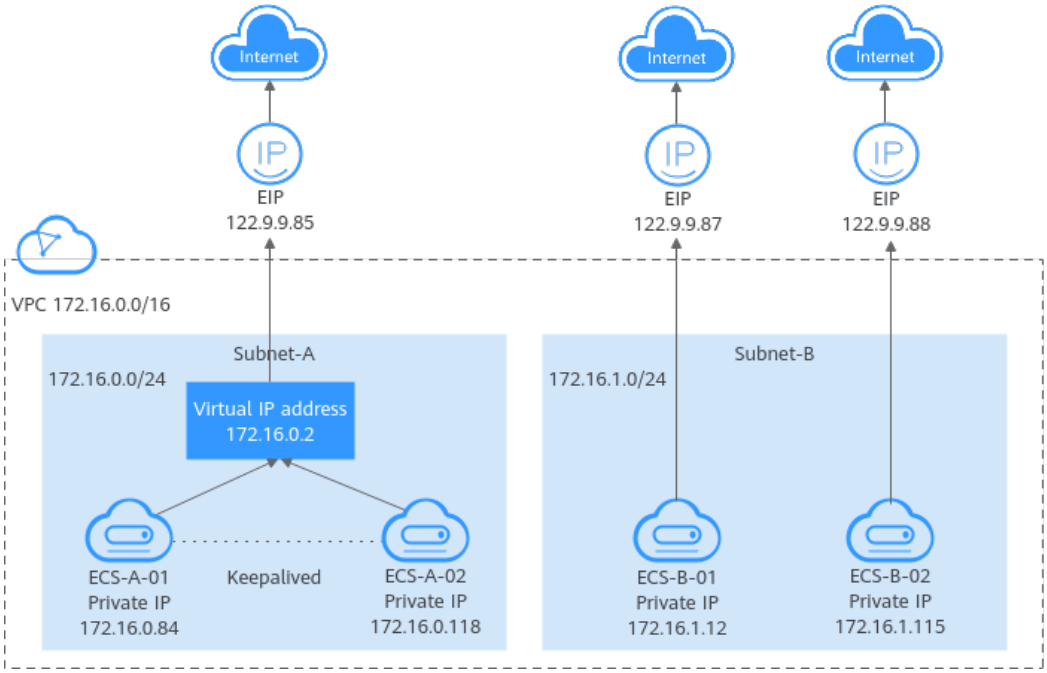


Tabela 4-1 Funções de diferentes tipos de endereços IP

Tipo do endereço IP	Descrição	Exemplo de valor
Endereço IP privado	Os endereços IP privados vêm com seus ECSs e pertencem às sub-redes da VPC dos ECSs. Eles são usados para comunicação privada na nuvem.	● Endereço IP privado do ECS-A-01: 172.16.0.84 ● Endereço IP privado do ECS-B-01: 172.16.1.12
Endereço IP virtual	Um endereço IP virtual pode ser compartilhado entre vários ECSs. Dois ECSs podem funcionar como um par ativo e em espera para obter alta disponibilidade usando um endereço IP virtual e o Keepalived. Se o ECS ativo estiver defeituoso, o endereço IP virtual poderá ser alternado dinamicamente para o ECS em espera para continuar fornecendo serviços. Para obter mais informações sobre endereços IP virtuais, consulte **Visão geral do endereço IP virtual**.	Vincule o endereço IP virtual (172.16.0.2) ambos ECS-A-01 e ECS-A-02. A alternância ativa/em espera do ECS-A-01 e do ECS-A-02 pode ser implementada usando o Keepalived.

Tipo do endereço IP	Descrição	Exemplo de valor
EIP	EIPs podem ser usados por recursos de nuvem para acesso à Internet. ● Você pode vincular um EIP a um endereço IP virtual para permitir que os ECSs com o endereço IP virtual vinculado acessem a Internet. ● Você pode vincular um EIP a um ECS para permitir que o ECS acesse a Internet. Cada EIP pode ser vinculado a apenas um ECS por vez. Para obter mais informações, consulte **Visão geral do EIP**.	● Vincule o EIP (122.9.9.85) ao endereço IP virtual (172.16.0.2) para permitir que o ECS-A-01 e o ECS-A-02 acessem a Internet. ● Vincule o EIP (122.9.9.87) ao ECS-B-01 para permitir que o ECS-B-01 acesse a Internet.

4.3 Como acessar a Internet usando um EIP vinculado a uma NIC de extensão?

1. Depois que um EIP for vinculado a uma NIC de extensão, efetue logon no ECS e use o comando **route** para consultar a rota.

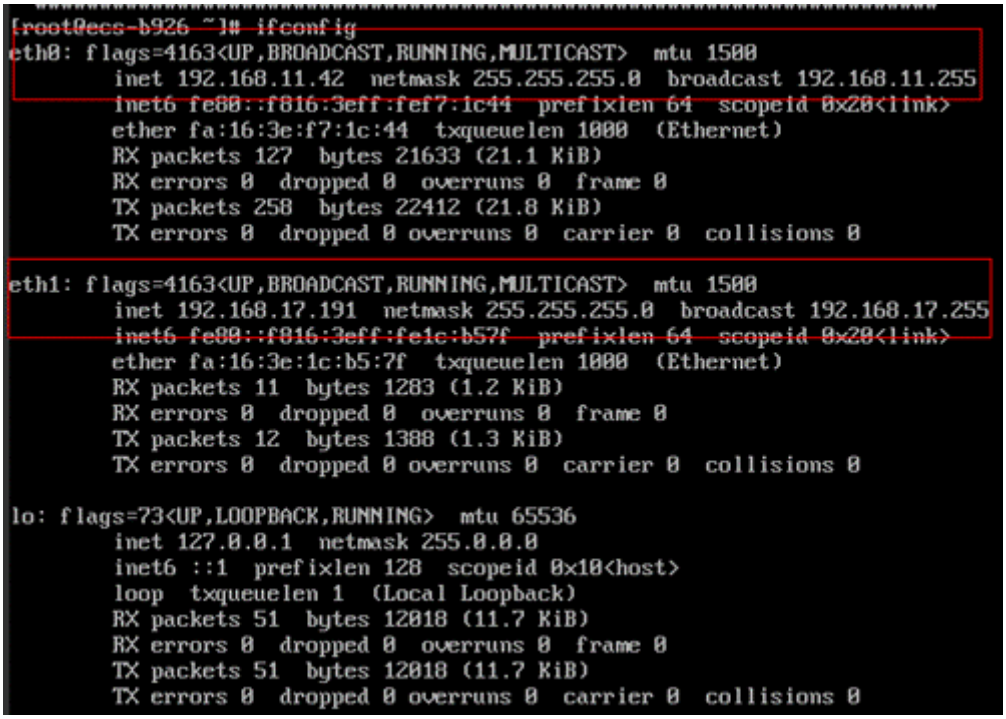
   Você pode executar o **route --help** para saber mais sobre o comando **route**.

   Figura 4-2 Visualização de informações da rota

   ```
   [root@ecs-b926 ~]# route -n
   Kernel IP routing table
   Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
   0.0.0.0         192.168.11.1    0.0.0.0         UG    0      0        0 eth0
   169.254.0.0     0.0.0.0         255.255.0.0     U     1002   0        0 eth0
   169.254.0.0     0.0.0.0         255.255.0.0     U     1003   0        0 eth1
   169.254.169.254 192.168.11.1    255.255.255.255 UGH   0      0        0 eth0
   192.168.11.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
   192.168.17.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
   [root@ecs-b926 ~]#
   ```

2. Execute o comando **ifconfig** para exibir as informações da NIC.

Figura 4-3 Exibir informações da NIC



3. Por padrão, habilite o acesso à Internet por meio da NIC de extensão.

   a. Execute o seguinte comando para excluir a rota padrão da NIC primária:

   route del -net 0.0.0.0 gw 192.168.11.1 dev eth0

   192.168.11.1 é o gateway da sub-rede em que a NIC serve. Você pode exibir o gateway na página de guia **Summary** da sub-rede no console de gerenciamento.

   NOTA

   Essa operação interromperá a comunicação do ECS. Recomenda-se que você execute a configuração seguindo a etapa 4.

   b. Execute o seguinte comando para configurar a rota padrão para a NIC de extensão:

   route add default gw 192.168.17.1

4. Configure o acesso à Internet a partir da NIC da extensão com base no endereço de destino.

   Execute o seguinte comando para configurar o acesso a um bloco CIDR especificado (por exemplo, *xx.xx*.0.0/16) por meio da NIC de extensão:

   Você pode configurar o bloco CIDR conforme necessário.

   route add -net xx.xx.0.0 netmask 255.255.0.0 gw 192.168.17.1

4.4 Quais são as diferenças entre as NICs primárias e de extensão dos ECSs?

As diferenças são as seguintes:

- Geralmente, as rotas padrão do SO usam preferencialmente as NICs primárias. Se as rotas padrão do SO usarem as NICs de extensão, a comunicação de rede será

interrompida. Em seguida, você pode verificar a configuração da rota para corrigir o erro de comunicação de rede.

- As NICs primários podem se comunicar com a zona de serviço público (zona onde PaaS e os serviços DNS são implementados). As NICs de extensão não podem comunicar esta região.

4.5 Um EIP que usa largura de banda dedicada pode ser alterado para usar largura de banda compartilhada?

Sim. Um EIP de pagamento por uso que usa a largura de banda dedicada pode ser alterado para usar a largura de banda compartilhada. No entanto, um EIP anual/mensal que usa a largura de banda dedicada não pode ser alterado para usar a largura de banda compartilhada.

4.6 Posso vincular um EIP a vários ECSs?

Cada EIP pode ser vinculado a apenas um ECS por vez.

Vários ECSs não podem compartilhar o mesmo EIP. Um ECS e seu EIP vinculado devem estar na mesma região. Se você quiser que vários ECSs na mesma VPC compartilhem um EIP, use um gateway NAT. Para obter mais informações, consulte **Guia de usuário do NAT Gateway**.

4.7 Como acessar um ECS com um EIP vinculado pela Internet?

Cada ECS é adicionado automaticamente a um grupo de segurança após ser criado para garantir sua segurança. O grupo de segurança nega o tráfego de acesso da Internet por padrão (exceto tráfego TCP da porta 22 através do SSH para um ECS do Linux e tráfego TCP da porta 3389 através do RDP para um ECS do Windows). Para permitir acesso externo a ECSs no grupo de segurança, adicione uma regra de entrada ao grupo de segurança.

Você pode definir **Protocol** como **TCP**, **UDP**, **ICMP** ou **All** conforme necessário na página para criar uma regra de grupo de segurança.

- Se o ECS precisar estar acessível pela Internet e você souber o endereço IP usado para acessar o ECS, defina **Source** como o intervalo de endereços IP que contém o endereço IP.
- Se o ECS precisar estar acessível pela Internet, mas você não souber o endereço IP usado para acessar o ECS, mantenha a configuração padrão 0.0.0.0/0 para **Source** e defina as portas permitidas para melhorar a segurança da rede.

  A origem padrão **0.0.0.0/0** indica que todos os endereços IP podem acessar ECSs no grupo de segurança.
- Alocar ECSs que têm diferentes requisitos de acesso à Internet a diferentes grupos de segurança.

4.8 O que é a política de atribuição de EIP?

Por padrão, os EIPs são atribuídos aleatoriamente.

Se um EIP for liberado por engano, o sistema atribuirá preferencialmente um EIP que você liberou nas últimas 24 horas.

Se você quiser um EIP específico que tenha sido liberado há mais de 24 horas, consulte **Como atribuir ou recuperar um EIP específico?**

Se você não quiser um EIP que tenha liberado, é recomendável que você compre outro EIP primeiro e, em seguida, libere o que não deseja.

4.9 Posso vincular um EIP de um ECS a outro ECS?

Sim.

Você pode desvincular o EIP do ECS original. Para obter detalhes, consulte **Desvinculação de um EIP de uma instância**.

Em seguida, vincule o EIP ao ECS de destino. Para obter detalhes, consulte **Vinculação de um EIP a uma instância**.

Se você quiser alterar um EIP para o seu ECS, consulte **Alteração de um EIP**.

4.10 Posso comprar um EIP específico?

Por padrão, os EIPs são atribuídos aleatoriamente. Se você tiver liberado EIPs, o sistema preferencialmente atribuirá EIPs daqueles que você liberou.

Você pode atribuir um EIP específico apenas chamando uma API. Para obter detalhes, consulte **Atribuição de um EIP**.

4.11 Como consultar a região dos meus EIPs?

Você pode visitar **https://en.ipip.net/ip.html** para consultar a região de seus EIPs.

- A região de um EIP identificada usando um site de terceiros pode ser diferente da região à qual o EIP pertence.
- Se a região identificada usando outro site de terceiros for diferente daquela identificada usando **https://en.ipip.net/ip.html**, use a região identificada usando **https://en.ipip.net/ip.html**.
- Se a região identificada usando **https://en.ipip.net/ip.html** for diferente da selecionada ao comprar o EIP, use a região selecionada durante a compra do EIP.

  NOTA

  A localização geográfica de um EIP comprado em CN North-Ulanqab1 é Pequim.
- Se o serviço for afetado negativamente porque a região do seu EIP não pode ser determinada, **envie um tíquete de serviço**.

Para saber mais sobre a região de EIPs, **envie um tíquete de serviço**.

4.12 Como alterar um EIP para uma instância?

Cenário 1: alterar um EIP para um ECS

1. Desvincule um EIP.
   a. Faça logon no console de gerenciamento.
   b. Clique em ☰ no canto superior esquerdo e escolha **Rede** > **Elastic IP**.
   c. Na página exibida, localize a linha que contém o EIP de destino e clique em **Unbind**.
   d. Clique em **Yes**.
2. Atribua um EIP.
   a. Faça logon no console de gerenciamento.
   b. Clique em ☰ no canto superior esquerdo e escolha **Rede** > **Elastic IP**.
   c. Na página exibida, clique em **Buy EIP**.
   d. Defina os parâmetros conforme solicitados.
   e. Clique em **Next**.
3. Vincule o novo EIP ao ECS.
   a. Faça logon no console de gerenciamento.
   b. Clique em ☰ no canto superior esquerdo e escolha **Rede** > **Elastic IP**.
   c. Na página **EIPs**, localize a linha que contém o EIP de destino e clique em **Bind**.
   d. Selecione o ECS desejado.
   e. Clique em **OK**.
4. Libere o EIP que foi substituído.
   a. Faça logon no console de gerenciamento.
   b. Clique em ☰ no canto superior esquerdo e escolha **Rede** > **Elastic IP**.
   c. Na lista de EIP, localize a linha que contém o EIP de destino e clique em **Release**.
   d. Clique em **Yes**.

Cenário 2: alterar um EIP para um balanceador de carga

1. Desvincule um EIP.
   a. Faça logon no console de gerenciamento.
   b. Clique em **Service List**. Em **Networking**, clique em **Elastic Load Balance**.
   c. Na lista de balanceadores de carga, localize o balanceador de carga de destino e escolha **More** > **Unbind EIP** na coluna **Operation**.
   d. Clique em **Yes**.
2. Atribua um EIP referindo-se a **2**.
3. Vincule o novo EIP ao balanceador de carga.
   a. Faça logon no console de gerenciamento.

b. Clique em **Service List**. Em **Networking**, clique em **Elastic Load Balance**.
c. Na lista de balanceadores de carga, localize o balanceador de carga de destino e escolha **More** > **Bind EIP** na coluna **Operation**.
d. Na caixa de diálogo **Bind EIP**, selecione o EIP a ser vinculado e clique em **OK**.

4. Libere o EIP que foi substituído. Para mais detalhes, consulte **4**.

Cenário 3: alterar um EIP para um gateway NAT

1. Atribua um EIP referindo-se a **2**.
2. Modifique uma regra SNAT.

   Para obter detalhes, consulte **Modificação de uma regra SNAT**. Na lista de EIP, selecione o novo EIP e desmarque o EIP existente.
3. Modifique uma regra DNAT.

   Para obter detalhes, consulte **Modificação de uma regra DNAT**.
4. Libere o EIP que foi substituído. Para mais detalhes, consulte **4**.

4.13 Posso vincular um EIP a um recurso de nuvem em outra região?

Não. Os EIPs e seus recursos de nuvem associados devem estar na mesma região.

4.14 Posso alterar a região do meu EIP?

A região de um EIP não pode ser alterada.

Se você atribuiu um EIP na região A, mas precisa de um EIP na região B, não é possível alterar diretamente a região do EIP atribuído de A para B. Em vez disso, você deve atribuir um EIP na região B.

5 Conexões de emparelhamento de VPC

5.1 Quantas conexões de emparelhamento de VPC posso criar em uma conta?

Se você usar uma conexão de emparelhamento de VPC para conectar VPCs na mesma região, poderá fazer logon no console de gerenciamento para visualizar sua cota de conexão de emparelhamento de VPC. Para mais detalhes, consulte **O que é uma cota?**.

- Número de conexões de emparelhamento de VPC que você pode criar em cada região entre VPCs na mesma conta: sujeito à cota real
- Número de conexões de emparelhamento de VPC que você pode criar em cada região entre VPCs em contas diferentes: as conexões de emparelhamento de VPC aceitas usam as cotas de ambas as contas. As conexões de emparelhamento VPC a serem aceitas usam apenas as cotas de contas que solicitam as conexões.

  Uma conta pode criar conexões de emparelhamento de VPC com contas diferentes se a conta tiver cota suficiente.

5.2 Uma conexão de emparelhamento de VPC pode conectar VPCs em diferentes regiões?

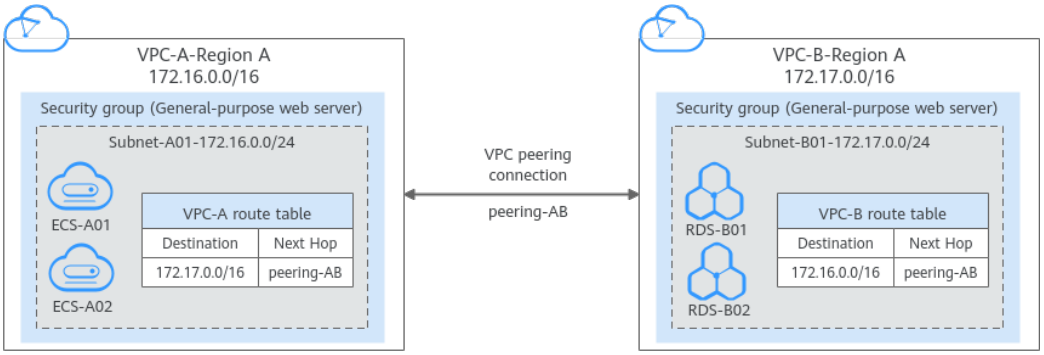
Uma conexão de emparelhamento de VPC só pode conectar VPCs na mesma região.

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

Figura 5-1 mostra um cenário de aplicação de conexões de emparelhamento de VPC.

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

Figura 5-1 Diagrama de rede de conexão de emparelhamento de VPC



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

Sintoma

Depois que uma conexão de emparelhamento de VPC é criada, as VPCs local e de par não podem se comunicar umas com as outras.

Solução de problemas

Os problemas aqui são descritos em ordem de probabilidade de ocorrer.

Tabela 5-1 Causas possíveis e soluções:

Nº	Possível causa	Solução
1	Blocos CIDR sobrepostos de VPCs locais e de par ● Todos os seus blocos CIDR de sub-rede se sobrepõem. ● Alguns de seus blocos de sub-rede CIDR se sobrepõem.	Consulte **Blocos CIDR sobrepostos de VPCs locais e de par**.
2	Configuração de rota incorreta para as VPCs locais e de par ● Nenhuma rota é adicionada. ● Rotas incorretas são adicionadas. ● Os destinos das rotas se sobrepõem aos configurados para conexões Direct Connect ou VPN.	Consulte **Configuração de rota incorreta para VPCs locais e de par**.

Nº	Possível causa	Solução
3	Configuração de rede incorreta ● As regras do grupo de segurança dos ECSs que precisam se comunicar negam o tráfego de entrada uns dos outros. ● O firewall da NIC do ECS bloqueia o tráfego. ● As regras de network ACL das sub-redes conectadas pela conexão de emparelhamento da VPC negam o tráfego de entrada. ● Verifique a configuração de roteamento baseada em políticas de um ECS com várias NICs.	Consulte **Configuração de rede incorreta**.
4	Falha na rede do ECS	Consulte **Falha na rede do ECS**.

AVISO

Se o problema persistir, **envie um tíquete de serviço**.

Blocos CIDR sobrepostos de VPCs locais e de par

Se os blocos CIDR de VPCs conectados por uma conexão de emparelhamento de VPC se sobrepuserem, a conexão pode não ter efeito devido aos conflitos de rota.

Tabela 5-2 Blocos CIDR sobrepostos de VPCs locais e de par

Cenário	Descrição	Solução
As VPCs com blocos CIDR sobrepostos também incluem sub-redes que se sobrepõem.	Os blocos CIDR de VPC-A e VPC-B se sobrepõem, e todas as suas sub-redes se sobrepõem. ● Blocos CIDR sobrepostos de VPC-A e VPC-B: 10.0.0.0/16 ● Blocos CIDR sobrepostos de Sub-rede-A01 em VPC-A e Sub-rede-B01 em VPC-B: 10.0.0.0/24 ● Blocos CIDR sobrepostos de Sub-rede-A02 em VPC-A e Sub-rede-B02 em VPC-B: 10.0.1.0/24	VPC-A e VPC-B não podem ser conectados usando uma conexão de emparelhamento de VPC. Replaneje a rede.

Cenário	Descrição	Solução
Duas VPCs têm blocos CIDR sobrepostos, mas algumas de suas sub-redes não se sobrepõem.	Os blocos CIDR de VPC-A e VPC-B se sobrepõem, e algumas de suas sub-redes se sobrepõem. ● Blocos CIDR sobrepostos de VPC-A e VPC-B: 10.0.0.0/16 ● Blocos CIDR sobrepostos de Sub-rede-A01 em VPC-A e Sub-rede-B01 em VPC-B: 10.0.0.0/24 ● CIDR blocos de Sub-rede-A02 em VPC-A e Sub-rede-B02 em VPC-B não se sobrepõem.	● Uma conexão de emparelhamento de VPC não pode conectar as VPCs inteiras, VPC-A e VPC-B. ● Uma conexão pode conectar suas sub-redes (Sub-rede-A02 e Sub-rede-B02) que não se sobrepõem. .

Se os blocos CIDR de VPCs se sobrepuserem e algumas de suas sub-redes se sobrepuserem, você poderá criar uma conexão de emparelhamento de VPC entre suas sub-redes com blocos CIDR não sobrepostos. **Tabela 5-3** descreve as rotas necessárias.

Tabela 5-3 Rotas necessárias para a conexão de emparelhamento de VPC entre Sub-rede-A02 e Sub-rede-B02

Tabela de rotas	Destino	Próximo salto	Descrição
Tabela de rotas da VPC-A	10.0.2.0/24	Emparelhamento-AB	Adicione uma rota com o bloco CIDR de Sub-rede-B02 como o destino e Emparelhamento-AB como o próximo salto.
Tabela de rotas da VPC-B	10.0.1.0/24	Emparelhamento-AB	Adicione uma rota com o bloco CIDR de Sub-rede-A02 como o destino e Emparelhamento-AB como o próximo salto.

AVISO

Se duas VPCs quiserem usar seus blocos CIDR IPv6 para comunicação por meio de uma conexão de emparelhamento de VPC, mas seus blocos CIDR IPv4 ou sub-redes se sobrepuserem, a conexão não será utilizável.

Configuração de rota incorreta para VPCs locais e de par

Verifique as rotas nas tabelas de rotas das VPCs locais e de par consultando a **Visualização de rotas configuradas para uma conexão de emparelhamento de VPC**. **Tabela 5-4** lista os itens que você precisa verificar.

Tabela 5-4 Itens de verificação de rota

Item	Solução
Verifique se as rotas são adicionadas às tabelas de rotas das VPCs locais e de par.	Se as rotas não forem adicionadas, adicione rotas referindo-se a: ● **Criação de uma conexão de emparelhamento de VPC com outra VPC na sua conta**. ● **Criação de uma conexão de emparelhamento de VPC com uma VPC na outra conta**
Verifique os destinos das rotas adicionadas às tabelas de rotas das VPCs locais e de par. ● Na tabela de rotas da VPC local, verifique se o destino da rota é o bloco CIDR, o bloco CIDR de sub-rede ou o endereço IP privado relacionado da VPC de par. ● Na tabela de rotas da VPC de par, verifique se o destino da rota é o bloco CIDR, o bloco CIDR de sub-rede ou o endereço IP privado relacionado da VPC local.	Se o destino da rota estiver incorreto, altere-o consultando **Modificação de rotas configuradas para uma conexão de emparelhamento VPC**.
Os destinos das rotas se sobrepõem aos configurados para conexões Direct Connect ou VPN.	Verifique se alguma das VPCs conectadas pela conexão de emparelhamento da VPC também tem uma conexão VPN ou Direct Connect conectada. Se o fizerem, verifique os destinos de suas rotas. Se os destinos das rotas se sobrepuserem, a conexão de emparelhamento da VPC não terá efeito. Nesse caso, replaneje a conexão de rede.

Configuração de rede incorreta

1. Verifique se as regras do grupo de segurança dos ECSs que precisam se comunicar permitem o tráfego de entrada uns dos outros consultando a **Exibição do grupo de segurança de um ECS**.
   - Se os ECSs estiverem associados ao mesmo grupo de segurança, você não precisará verificar suas regras.
   - Se os ECSs estiverem associados a grupos de segurança diferentes, adicione uma regra de entrada para permitir o acesso uns dos outros consultando a **Habilitação da comunicação de ECSs entre si em diferentes grupos de segurança por meio de uma rede interna**.
2. Verifique se o firewall da NIC do ECS bloqueia o tráfego.

   Se o firewall bloquear o tráfego, configure o firewall para permitir o tráfego de entrada.
3. Verifique se as regras de network ACL das sub-redes conectadas pela conexão de emparelhamento de VPC negam o tráfego de entrada.

   Se as regras de network ACL negarem o tráfego de entrada, configure as regras para permitir o tráfego.

4. Se um ECS tiver mais de uma NIC, verifique se o roteamento baseado em política correto foi configurado para o ECS e se os pacotes com endereços IP de origem diferentes correspondem às suas próprias rotas de cada NIC.

   Se um ECS tiver duas NICs (eth0 e eth1):

   – Endereço IP de eth0: 192.168.1.10; gateway de sub-rede: 192.168.1.1
   – Endereço IP de eth1: 192.168.2.10; gateway de sub-rede: 192.168.2.1

   Formato do comando:

   – **ping -I** *Endereço IP de eth0 endereço de gateway de sub-rede de eth0*
   – **ping -I** *Endereço IP de eth1 endereço de gateway de sub-rede de eth1*

   Execute os seguintes comandos:

   – **ping -I 192.168.1.10 192.168.1.1**
   – **ping -I 192.168.2.10 192.168.2.1**

   Se a comunicação de rede for normal, as rotas das NICs estão configuradas corretamente.

   Caso contrário, será necessário configurar o roteamento baseado em políticas para o ECS com várias NICs consultando **Como configurar rotas baseadas em políticas para um ECS com várias NICs?**

Falha na rede do ECS

1. Efetue logon no ECS.
2. Verifique se a NIC do ECS tem um endereço IP atribuído.
   – ECS do Linux: use o comando **ifconfig** ou **ip address** para exibir o endereço IP da NIC.
   – ECS do Windows: na caixa de pesquisa, digite **cmd** e pressione **Enter**. No prompt de comando exibido, execute o comando **ipconfig**.

   Se a NIC do ECS não tiver um endereço IP atribuído, consulte **Por que meu ECS falha ao obter um endereço IP?**
3. Verifique se o gateway de sub-rede do ECS pode sofrer ping.
   a. Na lista do ECS, clique no nome do ECS.

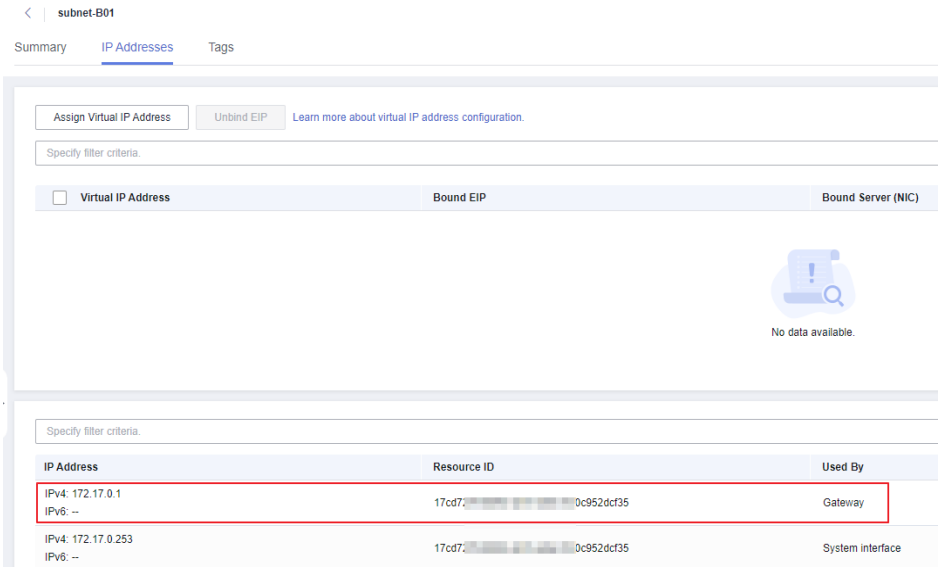
      A página de detalhes do ECS é exibida.
   b. Na página de detalhes do ECS, clique no hiperlink da VPC.

      A página **Virtual Private Cloud** é exibida.
   c. Na lista da VPC, localize a VPC de destino e clique no número na coluna **Subnets**.

      A página **Subnets** é exibida.
   d. Na lista de sub-redes, clique no nome da sub-rede.

      A página de detalhes da sub-rede é exibida.
   e. Clique na guia **IP Addresses** e visualize o endereço de gateway da sub-rede.

Figura 5-2 Endereço de gateway.



f. Verifique se a comunicação do gateway está normal:

Ping*Endereço de gateway de sub-rede*

Exemplo de comando: **ping 172.17.0.1**

Se o endereço de gateway não puder ser pingado, consulte **Por que meu ECS falha ao se comunicar em uma rede da camada 2 ou da camada 3?**

6 Endereços IP virtuais

6.1 Por que não é possível fazer ping no endereço IP virtual depois que ele é vinculado a uma NIC do ECS?

Sintoma

Depois de vincular um endereço IP virtual a uma NIC do ECS, você não poderá executar ping no endereço IP virtual.

Solução de problema

Os problemas aqui são descritos em ordem de probabilidade de ocorrer.

Solucione o problema descartando as causas descritas aqui, uma por uma.

Figura 6-1 Solução de problema

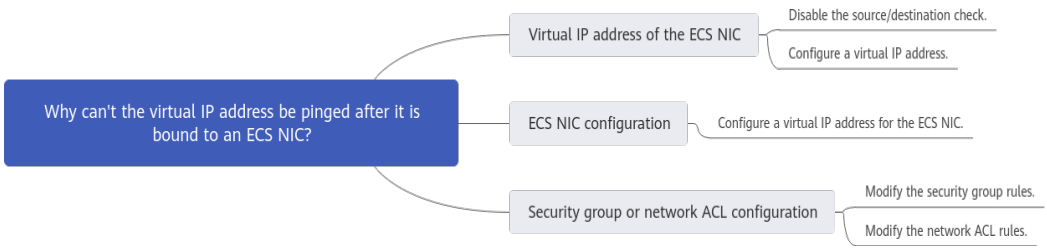


Tabela 6-1 Solução de problema

Possível causa	Solução
Endereço IP virtual da NIC do ECS	Veja **Endereço IP virtual da NIC do ECS**
Endereço IP virtual da NIC interna do ECS	Veja **Endereço IP virtual da NIC interna do ECS**
Configuração do grupo de segurança ou network ACL	Veja **Configuração do grupo de segurança ou network ACL**

Endereço IP virtual da NIC do ECS

Verifique se a verificação de origem/destino da NIC está desabilitada e se um endereço IP virtual está vinculado à NIC.

1. Faça logon no console de gerenciamento.
2. Clique em **Service List** e clique em **Elastic Cloud Server** em **Computing**.
3. Na lista de ECS, clique no nome do ECS.
4. Na página de detalhes do ECS exibida, clique na guia **Network Interfaces**.
5. Verifique de que a **Source/Destination Check** esteja desativada.
6. Certifique-se de que um endereço IP seja exibido para **Virtual IP Address** na página de detalhes da NIC.

   Se não houver um endereço IP virtual, clique em **Manage Virtual IP Address**. Na guia **IP Addresses** exibida, clique em **Assign Virtual IP Address**.

NOTA

Para verificar se um endereço IP virtual foi configurado, **ifconfig** não funcionará. Use **ip address** em vez disso. Para obter mais informações, consulte **Vinculação de um endereço IP virtual a um EIP ou ECS**.

Endereço IP virtual da NIC interna do ECS

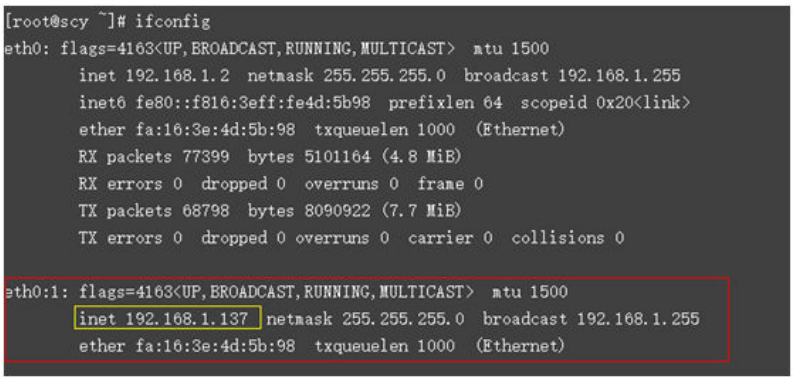
A seguir, os ECSs do Linux e do Windows são usados como exemplos para descrever como verificar se uma NIC do ECS tem um endereço IP virtual.

Para um ECS do Linux:

1. Verifique se há uma NIC **eth***X:X*:

   ifconfig

   Figura 6-2 Verificar NIC **eth***X:X*



   A saída do comando na figura anterior contém uma NIC **eth***X:X*. **192.168.1.137** é o seu endereço IP virtual.

   – Se a NIC **eth***X:X* estiver lá, a NIC do ECS está configurada corretamente.
   – Se a NIC **eth***X:X* não puder ser encontrada, execute as seguintes operações:

2. Se a saída do comando não contiver uma NIC **eth***X*:*X*, mude para o diretório **/etc/sysconfig/network-scripts**:

   cd /etc/sysconfig/network-scripts

3. Execute o seguinte comando para criar e modificar o arquivo **ifcfg-eth0:1**:

   vi ifcfg-eth0:1

   Adicione as seguintes informações da NIC ao arquivo:

   ```
   BOOTPROTO=static
   DEVICE=eth0:1
   HWADDR=fa:16:3e:4d:5b:98
   IPADDR=192.168.1.137
   GATEWAY=192.168.1.1
   NETMASK=255.255.255.0
   ONBOOT=yes
   ONPARENT=yes
   ```

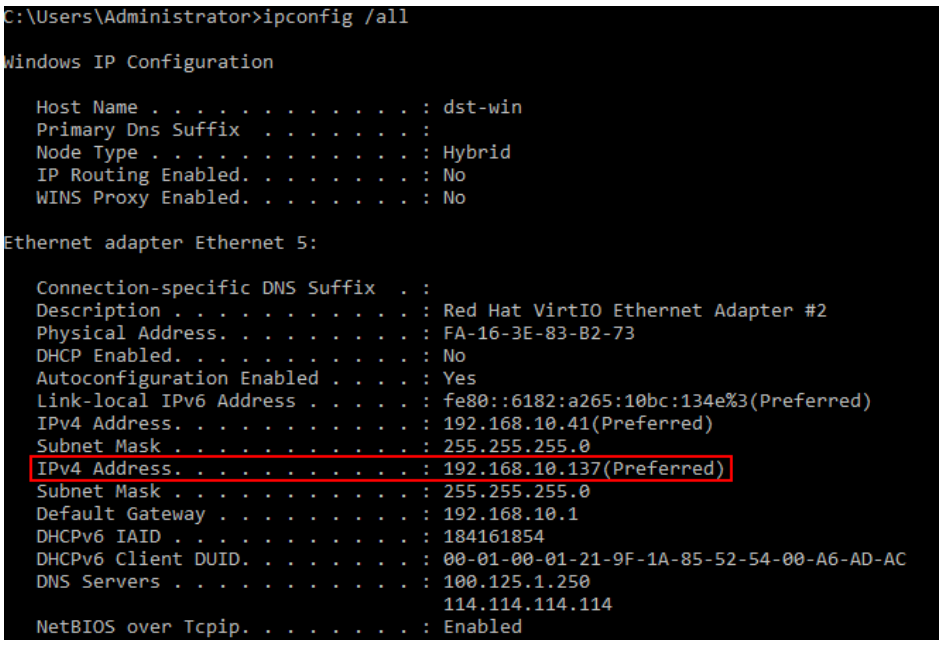
4. Pressione **Esc**, insira **:wq!**, salve o arquivo e saia.
5. Reinicie o ECS e execute o comando **ifconfig** para verificar se o endereço IP virtual foi configurado para o ECS.

Para um ECS do Windows:

1. No menu **Start**, abra a janela de linha de comando do Windows e execute o seguinte comando para verificar se o endereço IP virtual foi configurado:

   ipconfig /all

   Figura 6-3 Verificar se o endereço IP virtual foi configurado

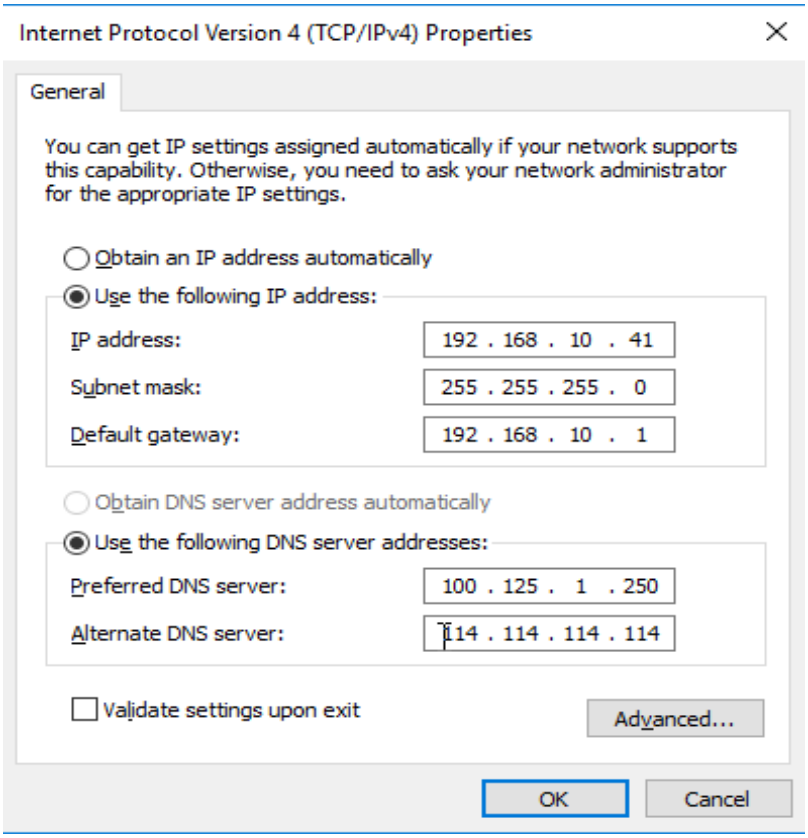
   Na saída de comando anterior, verifique se o valor do **IPv4 Address** (192.168.10.137) é o endereço IP da NIC do ECS.

   – Se sim, o endereço IP virtual foi configurado para a NIC do ECS.
   – Se não, execute as seguintes operações:

2. Escolha **Control Panel** > **Network and Internet** > **Network Connections**. Clique com o botão direito do mouse na ligação local correspondente e, em seguida, clique em **Properties**.

3. Na página de guia **Network**, selecione **Internet Protocol Version 4 (TCP/IPv4)**.
4. Clique em **Properties**.
5. Selecione **Use the following IP address** e defina **IP address** como o endereço IP privado exibido em **Figura 6-3**. Por exemplo, 192.168.10.41

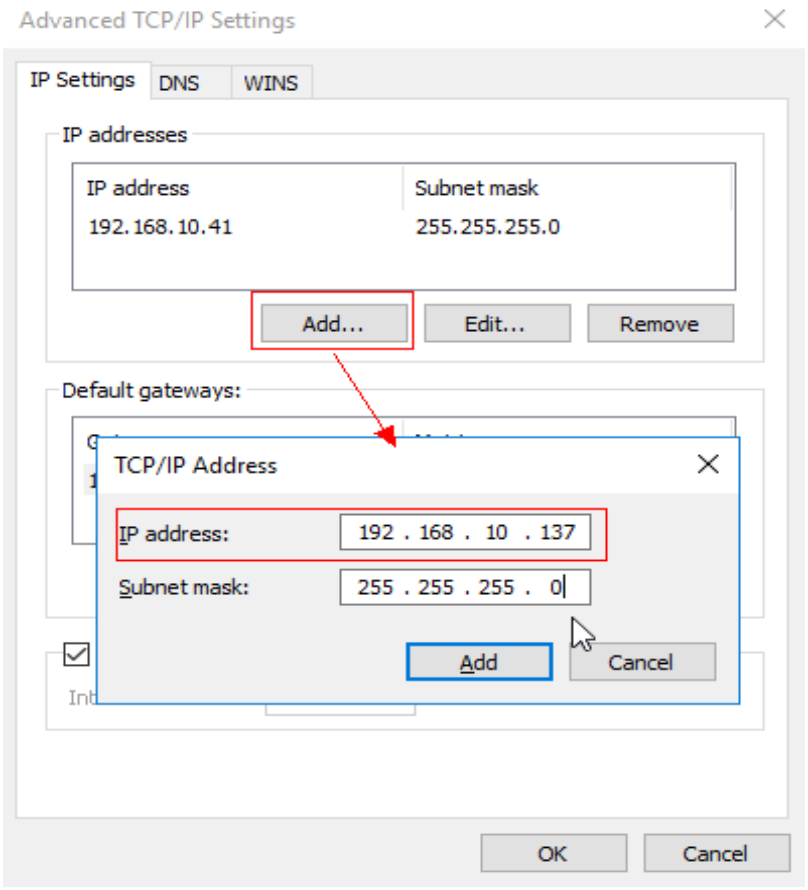
Figura 6-4 Configurar um endereço IP privado



6. Clique em **Advanced**.
7. Na guia **IP Settings**, clique em **Add** na área **IP addresses**.

   Adicione o endereço IP virtual configurado em **Figura 6-3**. Por exemplo, 192.168.10.137

Figura 6-5 Configurar o endereço IP virtual



Configuração do grupo de segurança ou network ACL

Verifique se os grupos de segurança do ECS e network ACLs associadas à sub-rede usada pela NIC do ECS estão bloqueando o tráfego.

1. Na página de detalhes do ECS, clique na guia **Security Groups** e confirme se as regras de grupo de segurança necessárias foram configuradas para o endereço IP virtual. Se as regras de grupo de segurança necessárias não tiverem sido configuradas, clique em **Change Security Group** ou **Modify Security Group Rule** para alterar o grupo de segurança ou modificar as regras de grupo de segurança.
2. Clique em **Service List**. Em **Rede**, clique em **Virtual Private Cloud**. No painel de navegação à esquerda do console de rede, clique em **Network ACLs** e verifique se as regras de network ACL associadas à sub-rede usada pela NIC do ECS estão bloqueando o acesso ao endereço IP virtual.

Submissão de um tíquete de serviço

Se o problema persistir, **envie um tíquete de serviço**.

6.2 Como vincular um endereço IP virtual na Huawei Cloud a um servidor em um data center local?

Pré-requisitos

- Você atribuiu endereços IP virtuais. Para obter detalhes, consulte **Atribuição de um IP virtual**.
- Você criou uma conexão de Camada 2 para a sub-rede onde reside o endereço IP virtual. Para obter detalhes, consulte **Compra de um switch corporativo**.

Procedimento

1. Acesse o console de gerenciamento.
2. Na página inicial do console, em **Rede**, clique em **Virtual Private Cloud**.
3. Na árvore de navegação à esquerda, escolha **Enterprise Switch**.
4. Clique em **Manage Virtual IP Address** à direita de **Layer 2 Connection Topology**.
5. Na lista de endereços IP, localize a linha que contém o endereço IP virtual de destino e clique em **Bind to Instance** na coluna **Operation**.
6. Na página **Bind to Instance**, defina **Instance Type** como **Layer 2 Connection**, selecione a conexão da Camada 2 de destino e clique em **OK**.

6.3 Por que a rede é desconectada entre servidores usando um endereço IP virtual após uma alternância ativa/em espera?

Para um cluster de alta disponibilidade configurado usando endereços IP virtuais e Keepalived, se você descobrir que a rede entre o cliente e o servidor é desconectada após uma alternância ativa/em espera, a causa possível é que a alternância é realizada manualmente. Como resultado, a tabela ARP no cliente não é atualizada, você pode executar as seguintes operações para atualizar a tabela ARP:

1. Faça logon no sistema para o cliente
2. Atualize a tabela ARP no cliente.
   - Método 1: acionar o cliente para aprender o novo endereço MAC correspondente ao endereço IP virtual:

     ping *Virtual IP address*

     Exemplo de comando: **ping 192.168.3.22**
   - Método 2: limpar as entradas residuais na tabela ARP do endereço IP virtual para acionar o cliente para aprender a nova tabela ARP:

     arp -d *Virtual IP address*

     Exemplo de comando: **arp -d 192.168.3.22**

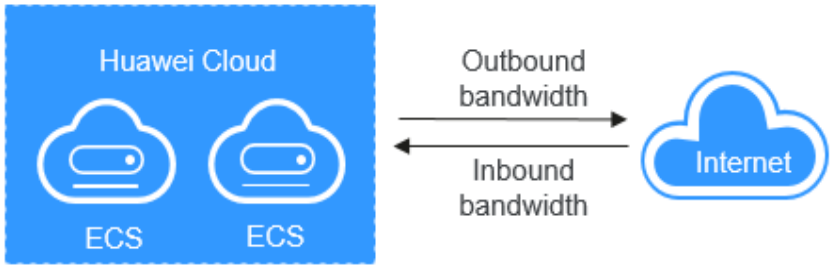
7 Largura de banda

7.1 O que são largura de banda de entrada e largura de banda de saída?

A largura de banda de entrada é a largura de banda consumida quando os dados são transferidos da Internet para a Huawei Cloud. Por exemplo, quando os recursos são baixados da Internet para ECSs, isso consome a largura de banda de entrada.

A largura de banda de saída é a largura de banda consumida quando os dados são transferidos da Huawei Cloud para a Internet. Por exemplo, quando os ECSs fornecem serviços acessíveis da Internet e usuários externos baixam recursos dos ECSs, isso consome a largura de banda de saída.

Figura 7-1 Largura de banda de entrada e largura de banda de saída



A Huawei Cloud cobra apenas pela largura de banda de saída.

NOTA

- Em 31 de julho de 2020, 00:00:00 GMT + 08:00, as regras que limitam as larguras de banda públicas foram alteradas nas regiões da China continental, incluindo CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN Southwest-Guiyang1 e CN North-Ulanqab1.

  Em 10 de dezembro de 2021, 00:00:00 GMT+08:00, as regras que limitam as larguras de banda públicas foram alteradas em CN-Hong Kong, AP-Bangkok, AP-Singapore, AF-Johannesburg, LA-Mexico City2, LA-Sao Paulo1 e LA-Santiago.

  Após a mudança:

  - Se a banda comprada ou modificada de até 10 Mbit/s, a largura de banda de entrada será de 10 Mbit/s, e a largura de banda de saída será a mesma que a largura de banda comprada ou modificada.
  - Se a largura de banda comprada ou modificada de mais de 10 Mbit/s, as larguras de banda nas direções de entrada e saída serão as mesmas que a largura de banda comprada ou modificada.

7.2 Como saber se meu limite de largura de banda do EIP foi excedido?

Sintoma

O tamanho da largura de banda configurado quando você compra uma largura de banda dedicada ou compartilhada é o limite superior da largura de banda de saída. Se um ECS que executa suas aplicações Web não puder ser acessado sem problemas pela Internet, verifique se a largura de banda de saída do EIP vinculado ao ECS é maior do que o tamanho da largura de banda configurado.

NOTA

Se a largura de banda de saída exceder o tamanho de largura de banda configurado, pode haver perda de pacotes. Para evitar a perda de dados, recomenda-se que você monitore a largura de banda.

Solução de problemas

Os problemas aqui são descritos em ordem de probabilidade de ocorrer.

Solucione o problema descartando as causas descritas aqui, uma por uma.

Figura 7-2 Solução de problemas

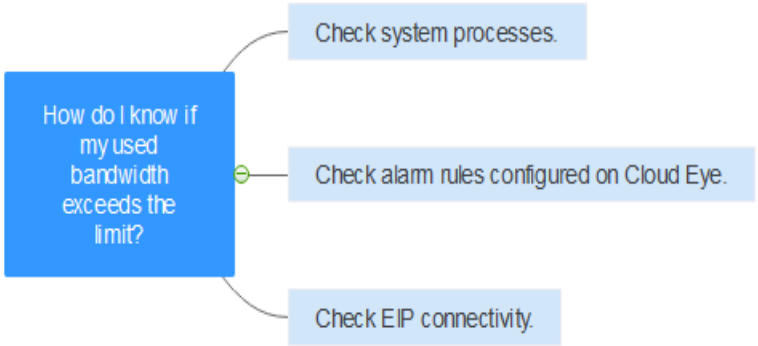


Tabela 7-1 Solução de problemas

Possível causa	Descrição	Solução
Processos do sistema que levam a alta largura de banda	Se alguns processos de sistema pesados ou aplicações em execução no ECS estiverem causando a alta largura de banda ou o uso da CPU, o ECS será executado lentamente ou poderá ficar inacessível inesperadamente.	Veja **Processos do sistema que levam ao uso de alta largura de banda**
Regras impróprias de alarme do Cloud Eye	Se você criou regras de alarme para o uso de largura de banda no console do Cloud Eye, onde o limite de largura de banda de saída ou o período de alarme é definido muito pequeno, o sistema pode gerar alarmes excessivos.	Veja **Regras impróprias de alarme do Cloud Eye**
Falha na conexão do EIP	Um ECS com um EIP vinculado não pode acessar a Internet.	Consulte **Por que meu ECS não consegue acessar a Internet mesmo depois que um EIP está vinculado?**

Processos do sistema que levam ao uso de alta largura de banda

Se alguns processos de sistema pesados ou aplicações em execução no ECS estiverem causando a alta largura de banda ou o uso da CPU, o ECS será executado lentamente ou poderá ficar inacessível inesperadamente.

Você pode consultar o seguinte para localizar os processos que levaram a uma largura de banda excessivamente alta ou uso da CPU e otimizar ou interromper os processos.

- **Por que meu ECS do Windows está lento?**
- **Por que meu ECS do Linux está lento?**

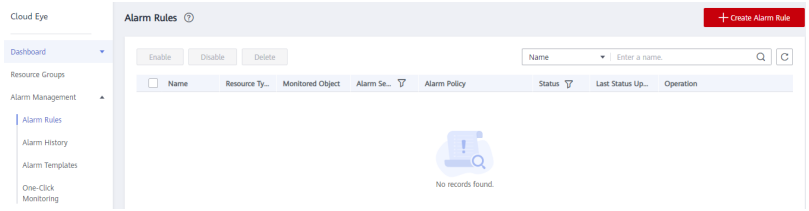
Regras impróprias de alarme do Cloud Eye

Se você criou regras de alarme para o uso de largura de banda no console do Cloud Eye, onde o limite de largura de banda de saída ou o período de alarme é definido muito pequeno, o sistema pode gerar alarmes excessivos.

Você precisa definir uma regra de alarme apropriada com base na largura de banda comprada. Por exemplo, se a largura de banda adquirida for de 5 Mbit/s, você pode criar uma regra de alarme para relatar um alarme quando a largura de banda máxima de saída atingir 4,8 Mbit/s três períodos seguidos. Você também pode **aumentar sua largura de banda**.

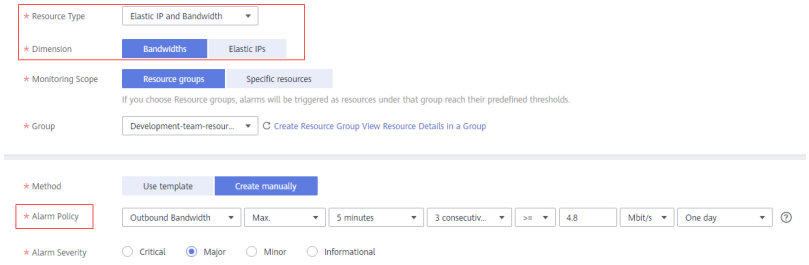
1. Faça logon no console de gerenciamento, em **Management & Deployment**, clique em **Cloud Eye**. No console do **Cloud Eye**, escolha **Alarm Management** > **Alarm Rules**.

Figura 7-3 Regras de alarme



2. Clique em **Create Alarm Rule** e configure uma regra de alarme para gerar alarmes quando a largura de banda exceder o limite configurado.

Figura 7-4 Criar uma regra de alarme



Enviar um tíquete de serviço

Se o problema persistir, **envie um tíquete de serviço**.

7.3 Quais são as diferenças entre largura de banda do EIP e largura de banda de rede privada?

As larguras de banda do EIP são usadas pelos ECSs para acessar a Internet por meio de EIPs. As larguras de banda do EIP usadas serão cobradas.

A largura de banda privada refere-se à largura de banda usada pelos ECSs em VPCs. A largura de banda privada e a velocidade máxima de transferência de dados (em PPS) permitidas para um ECS são determinadas com base nas especificações do ECS.

Para obter detalhes, consulte **Tipos de ECS**.

7.4 Qual é a faixa de tamanho de largura de banda?

A faixa de largura de banda é de 1 Mbit/s a 2000 Mbit/s.

7.5 Quais tipos de largura de banda estão disponíveis?

Há largura de banda dedicada e largura de banda compartilhada. Uma largura de banda dedicada só pode ser usada por um EIP, mas uma largura de banda compartilhada pode ser usada por vários EIPs.

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

Uma largura de banda dedicada só pode ser usada por um EIP. Um EIP só pode ser usado por um recurso de nuvem, como um ECS, um gateway NAT ou um balanceador de carga.

Uma largura de banda compartilhada pode ser compartilhada por vários EIPs de pagamento por uso. Adicionar um EIP a ou remover um EIP de uma largura de banda compartilhada não afeta suas cargas de trabalho.

Uma largura de banda dedicada não pode ser alterada para uma largura de banda compartilhada ou vice-versa. Você pode comprar uma largura de banda compartilhada para seus EIPs de pagamento por uso.

- Depois de adicionar um EIP a uma largura de banda compartilhada, o EIP usará a largura de banda compartilhada.
- Depois de remover um EIP de uma largura de banda compartilhada, o EIP usará a largura de banda dedicada.

7.7 Como comprar uma largura de banda compartilhada?

1. Acesse o console de gerenciamento.
2. No painel de navegação à esquerda, escolha **Elastic IP and Bandwidth** > **Shared Bandwidths**.
3. No canto superior direito, clique em **Buy Shared Bandwidth**. Na página exibida, configure os parâmetros conforme solicitado para comprar uma largura de banda compartilhada.

7.8 Existe um limite para o número de EIPs que podem ser adicionados a cada largura de banda compartilhada?

Um máximo de 20 EIPs pode ser adicionado a cada largura de banda compartilhada. Se você quiser adicionar mais EIPs a cada largura de banda compartilhada, **envie um tíquete de serviço** para solicitar um aumento de cota.

7.9 Posso aumentar minha largura de banda faturada em base anual/mensal e depois diminuí-la?

Você pode aumentar a largura de banda para um EIP anual/mensal sempre que quiser, e a alteração entra em vigor imediatamente. Mas você só pode diminuí-lo quando renovar a assinatura EIP, e a largura de banda reduzida não terá efeito até o próximo ciclo de faturamento. Para obter detalhes, consulte **Modificação de uma largura de banda de EIP**.

7.10 Qual é a relação entre largura de banda e taxa de upload/download?

A largura de banda é medida em bit/s, mas a taxa de download é medida em byte/s.

1 byte = 8 bits, ou seja, taxa de download = largura de banda/8

Devido a vários problemas, como desempenho do computador, qualidade do dispositivo de rede, uso de recursos e horários de pico da rede, se a largura de banda for de 1 Mbit/s, a taxa real de upload ou download é geralmente menor que 125 kByte/s (1 Mbit/s = 1.000 Kbit/s, taxa de upload ou download = 1.000/8 = 125 kByte/s).

7.11 Quais são as diferenças entre BGP estático, BGP dinâmico e BGP premium?

As diferenças entre BGP estático, BGP dinâmico e BGP premium são as seguintes:

Tabela 7-2 Diferenças entre BGP estático, BGP dinâmico e BGP premium

Item	BGP estático	BGP dinâmico	BGP premium
Definição	As rotas estáticas são configuradas manualmente e devem ser reconfiguradas manualmente sempre que a topologia da rede ou o status do link mudarem.	O BGP dinâmico fornece failover automático e escolhe o caminho ideal com base nas condições de rede em tempo real, bem como nas políticas predefinidas.	o BGP premium escolhe o caminho ideal e garante redes de baixa latência e alta qualidade. O BGP é usado para interconectar com linhas de várias operadoras principais. Conexões de rede pública que apresentam baixa latência e alta qualidade são estabelecidas diretamente entre a China continental e Hong Kong (China). **NOTA** O BGP premium agora está disponível apenas na região CN-Hong Kong.

Item	BGP estático	BGP dinâmico	BGP premium
Garantia	Quando as mudanças ocorrem em uma rede que use o BGP estático, a configuração manual toma algum tempo e a alta disponibilidade não pode ser garantida. **NOTA** Se você selecionar o BGP estático, seu sistema de aplicativo deverá ter configurações de recuperação de desastres em vigor.	Quando ocorre uma falha no link de uma operadora, o BGP dinâmico selecionará rapidamente outro caminho ideal para assumir os serviços, garantindo a disponibilidade do serviço. Atualmente, as operadoras na China que suportam roteamento BGP dinâmico incluem a China Telecom, a China Mobile, a China Unicom, a China Education and Research Network (CERNET), a National Radio and Television Administration e o Dr. Peng Group.	O BGP premium tem a mesma capacidade de garantia do BGP dinâmico. Além disso, o BGP premium garante maior qualidade de rede e menor latência. Atualmente, as operadoras convencionais em Hong Kong (China) são suportadas.
Disponibilidade do serviço	99%	99,95%	99,95%
Cobrança	Seu preço do menos ao mais caro: BGP estático, BGP dinâmico e BGP premium.		

NOTA

Para obter mais informações sobre a disponibilidade do serviço, consulte **Acordo de nível de serviço da Huawei Cloud**.

8 Conectividade

8.1 Se uma VPN permite comunicação entre as duas VPCs?

Se as duas VPCs estiverem na mesma região, você poderá usar uma conexão de emparelhamento de VPC para permitir a comunicação entre elas.

Se as duas VPCs estiverem em regiões diferentes, você poderá usar uma VPN para permitir a comunicação entre as VPCs. Os blocos CIDR das duas VPCs são as sub-redes locais e remotas, respectivamente.

8.2 Por que os nomes de domínio internos ou da Internet na nuvem são inacessíveis por meio de nomes de domínio quando meu ECS tem várias NICs?

Quando um ECS tiver mais de uma NIC, se diferentes endereços de servidor DNS estiverem configurados para as sub-redes usadas pelas NICs, o ECS não poderá acessar a Internet ou os nomes de domínio na nuvem.

Você pode resolver esse problema configurando o mesmo endereço de servidor DNS para as sub-redes usadas pelo mesmo ECS. Você pode executar as seguintes etapas para modificar endereços de servidor DNS de sub-redes em uma VPC:

1. Faça logon no console de gerenciamento.
2. Na página inicial do console, em **Rede**, clique em **Virtual Private Cloud**.
3. No painel de navegação à esquerda, clique em **Virtual Private Cloud**.
4. Na página **Virtual Private Cloud**, localize a VPC à qual uma sub-rede será modificada e clique no nome da VPC.
5. Na lista de sub-redes, localize a linha que contém a sub-rede a ser modificada e clique em **Modify**. Na página exibida, altere o endereço do servidor DNS conforme solicitado.
6. Clique em **OK**.

8.3 Quais são as prioridades da rota personalizada e do EIP se ambos estiverem configurados para um ECS para permitir que o ECS acesse a Internet?

A prioridade de um EIP é maior do que a de uma rota personalizada em uma tabela de rotas da VPC. Por exemplo:

A tabela de rotas de VPC de um ECS tem uma rota personalizada com 0.0.0.0/0 como destino e gateway NAT como próximo salto.

Se um ECS na VPC tiver um EIP vinculado, a tabela de rotas da VPC terá uma rota baseada em política com 0.0.0.0/0 como destino, que tem uma prioridade mais alta do que sua rota personalizada. Nesse caso, o tráfego é encaminhado para o EIP e não pode alcançar o gateway NAT.

8.4 Por que há interrupções intermitentes quando um host local acessa um site criado em um ECS?

Sintoma

Depois de criar um site em um ECS, alguns usuários ocasionalmente não conseguem acessar o site por meio da rede local.

Solução de problemas

1. Verifique a rede local do usuário.

   Se o host local se comunicar com o ECS usando NAT, esse problema poderá ocorrer.
2. Execute o seguinte comando para verificar se **tcp_tw_recycle** está ativado no ECS:

   sysctl -a|grep tcp_tw_recycle

   Se o valor de **tcp_tw_recycle** for **1**, a função é ativada.
3. Execute o seguinte comando para verificar o número de pacotes perdidos do ECS:

   cat /proc/net/netstat | awk '/TcpExt/ { print $21,$22 }'

   Se o valor de **ListenDrops** não for **0**, haverá perda de pacotes, ou seja, a rede está com defeito.

Procedimento

Esse problema pode ser resolvido modificando os parâmetros do kernel do ECS.

- Execute o seguinte comando para modificar temporariamente os parâmetros (os parâmetros serão alterados após uma reinicialização):

  sysctl -w net.ipv4.tcp_tw_recycle=0
- Execute as seguintes operações para modificar permanentemente os parâmetros:

  a. Execute o seguinte comando e modifique o arquivo **/etc/sysctl.conf**:

  vi /etc/sysctl.conf

  Adicione o seguinte conteúdo ao arquivo:

net.ipv4.tcp_tw_recycle=0

b. Pressione **Esc**, insira **:wq!**, salve o arquivo e saia.

c. Execute o seguinte comando para que a modificação tenha efeito:

sysctl -p

8.5 Por que os ECSs que usam endereços IP privados na mesma sub-rede suportam apenas comunicação unidirecional?

Sintoma

Dois ECSs (**ecs01** e **ecs02**) estão na mesma sub-rede em uma VPC. Seus endereços IP são 192.168.1.141 e 192.168.1.40.

O **ecs01** pode fazer ping de **ecs02** através de um endereço IP privado com êxito, mas **ecs02** não pode fazer ping de **ecs01** por meio de um endereço IP privado.

Solução de problemas

1. Faça ping em **ecs01** de **ecs02** por meio do EIP. Se **ecs01** pode ser pingado, a NIC de **ecs01** está funcionando corretamente.
2. Execute o comando **arp -n** em **ecs02** para verificar se a saída do comando contém o endereço MAC de **ecs01**. Se a saída do comando não contiver o endereço MAC de **ecs01**, **ecs02** falhará em aprender o endereço MAC de **ecs01** ao usar o endereço IP privado para executar o ping de **ecs01**.
3. Execute o comando **ip a** no **ecs01** para verificar a configuração de NIC do **ecs01**. A figura a seguir apresenta um exemplo.

Figura 8-1 Exibir a configuração da NIC do **ecs01**

```
[root@bd-slave1 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether fa:16:3e:62:1d:d5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.141/24 brd 192.168.1.255 scope global eth0
    inet 192.168.1.40/32 scope global eth0
    inet6 fe80::f816:3eff:fe62:1dd5/64 scope link
       valid_lft forever preferred_lft forever
```

O endereço IP 192.168.1.40/32 não deve ser configurado com base na saída do comando. Como resultado, o **ecs01** falha ao enviar pacotes para o **ecs02**.

Procedimento

Modifique a configuração de NIC de **ecs01**. Execute o seguinte comando para excluir o endereço IP redundante, por exemplo, 192.168.1.40/32, configurado na NIC **eth0**:

ip a del 192.168.1.40/32 dev eth0

8.6 Por que a comunicação falha entre dois ECSs na mesma VPC ou perda de pacotes ocorre quando eles se comunicam?

Sintoma

Dois ECSs na mesma VPC não podem se comunicar uns com os outros ou há perda de pacotes quando eles se comunicam.

Solução de problemas

Os problemas aqui são descritos em ordem de probabilidade de ocorrer.

Solucione o problema descartando as causas descritas aqui, uma por uma.

Figura 8-2 Solução de problemas

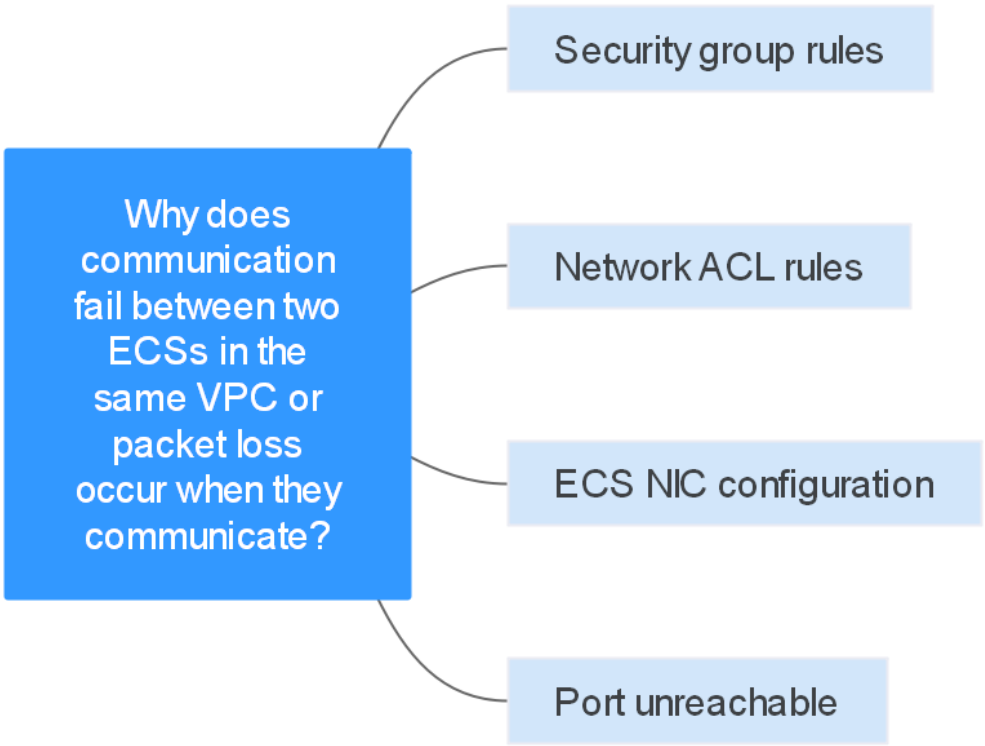


Tabela 8-1 Solução de problemas

Possível causa	Solução
Regras de grupo de segurança	Veja **Regras de grupos de segurança**
Regras de ACL de rede	Veja **Regras de ACL de rede**

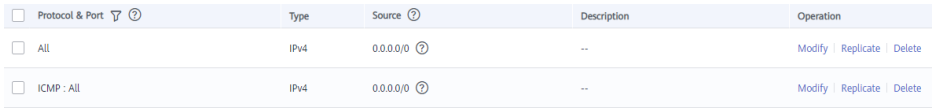
Possível causa	Solução
Configuração da NIC do ECS	Veja **Configuração da NIC do ECS**
Porta inacessível	Veja **Porta inacessível**

Regras de grupos de segurança

Verifique se o grupo de segurança da NIC do ECS permite o tráfego ICMP de saída e de entrada.

Tome a direção de entrada como exemplo. As regras do grupo de segurança devem conter pelo menos uma das seguintes regras.

Figura 8-3 Regra de grupo de segurança de entrada



Se pacotes de outros protocolos forem testados, configure as regras do grupo de segurança para permitir o tráfego de protocolo correspondente. Por exemplo, se os pacotes UDP forem testados, verifique se o grupo de segurança permite o tráfego UDP de entrada.

Regras de ACL de rede

1. Verifique se a sub-rede da NIC do ECS tem uma ACL de rede associada.
2. Verifique o status da ACL de rede na lista de ACLs da rede.
   - Se **Disabled** for exibido na coluna **Status**, a ACL da rede foi desabilitada. Vá para **3**.
   - Se **Enabled** for exibido na coluna **Status**, a ACL da rede foi ativada. Vá para **4**.
3. Clique no nome da ACL de rede e configure regras nas guias **Inbound Rules** e **Outbound Rules** para permitir o tráfego ICMP.
4. Se a ACL de rede estiver desabilitada, todos os pacotes nas direções de entrada e de saída serão descartados por padrão. Neste caso, exclua a ACL de rede ou habilite a ACL de rede e permita o tráfego ICMP.

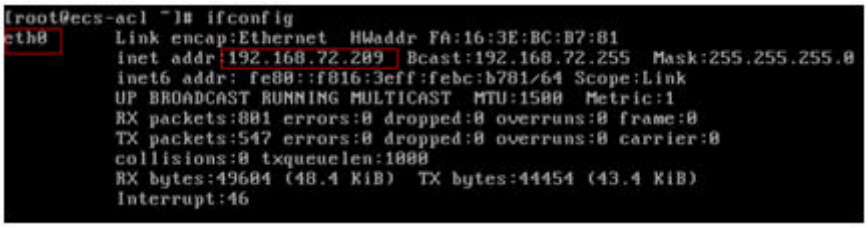
Configuração da NIC do ECS

O procedimento a seguir usa um ECS Linux como exemplo. Para um ECS Windows, verifique as restrições de firewall.

1. Verifique se várias NICs estão configuradas para o ECS. Se o ECS tiver várias NICs e o EIP estiver vinculado a uma NIC de extensão, configure o roteamento baseado em políticas para o ECS. Para mais detalhes, consulte **Como configurar rotas baseadas em políticas para um ECS com várias NICs?**
2. Faça logon no ECS e execute o seguinte comando para verificar se a NIC foi criada e se obteve um endereço IP privado. Se não houver informações da NIC ou o endereço IP privado não puder ser obtido, entre em contato com o suporte técnico.

ifconfig

Figura 8-4 Endereço IP da NIC



3. Se o uso da CPU exceder 80%, a comunicação do ECS poderá ser afetada negativamente. Execute o seguinte comando para verificar se o uso da CPU do ECS é muito alto:

   top

4. Execute o comando a seguir para verificar se o ECS tem restrições nas regras de grupo de segurança:

   iptables-save

5. Execute o seguinte comando para verificar se o arquivo **/etc/hosts.deny** contém os endereços IP que limitam a comunicação:

   vi /etc/hosts.deny

   Se o arquivo **hosts.deny** contiver o endereço IP de outro ECS, exclua o endereço IP do arquivo **hosts.deny** e salve o arquivo.

Porta inacessível

1. Se uma porta do ECS não puder ser alcançada, verifique se as regras de grupo de segurança e as regras de ACL de rede habilitam a porta.
2. No ECS Linux, execute o seguinte comando para verificar se o ECS escuta na porta: se o ECS não escutar na porta, a comunicação do ECS poderá ser afetada negativamente.

   netstat -na | grep <*Port number*>

Enviar um tíquete de serviço

Se o problema persistir, **envie um tíquete de serviço**.

8.7 Por que meu ECS não pode usar o Cloud-init?

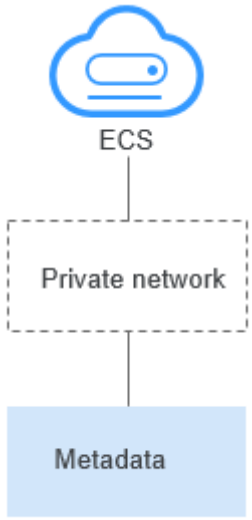
Sintoma

Um ECS não pode usar Cloud-init.

Solução de problemas

Figura 8-5 mostra o processo para que um ECS obtenha metadados usando o Cloud-init.

Figura 8-5 Processo para obtenção de metadados



Verifique as seguintes possíveis causas.

Figura 8-6 Possíveis causas

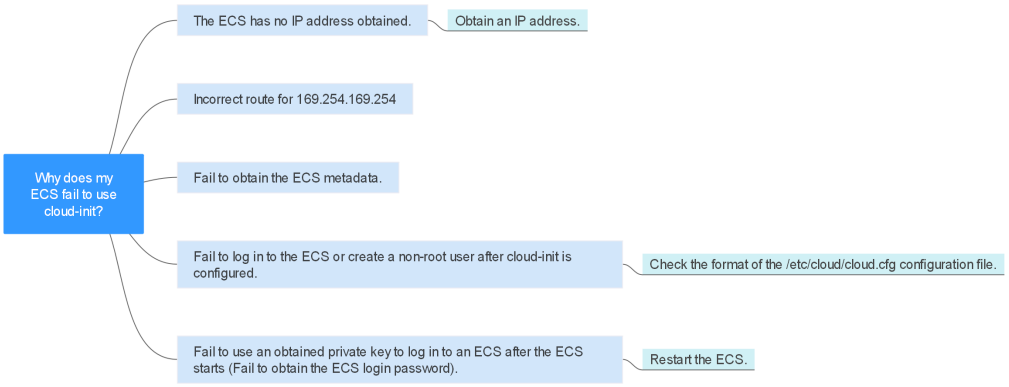


Tabela 8-2 Possíveis causas

Possível causa	Solução
O ECS não obteve nenhum endereço IP.	Veja **O ECS não obteve endereço IP**
Rota incorreta para 169.254.169.254	Veja **Rota incorreta para 169.254.169.254**
Falha ao obter os metadados do ECS.	Veja **Não obteve os metadados do ECS**

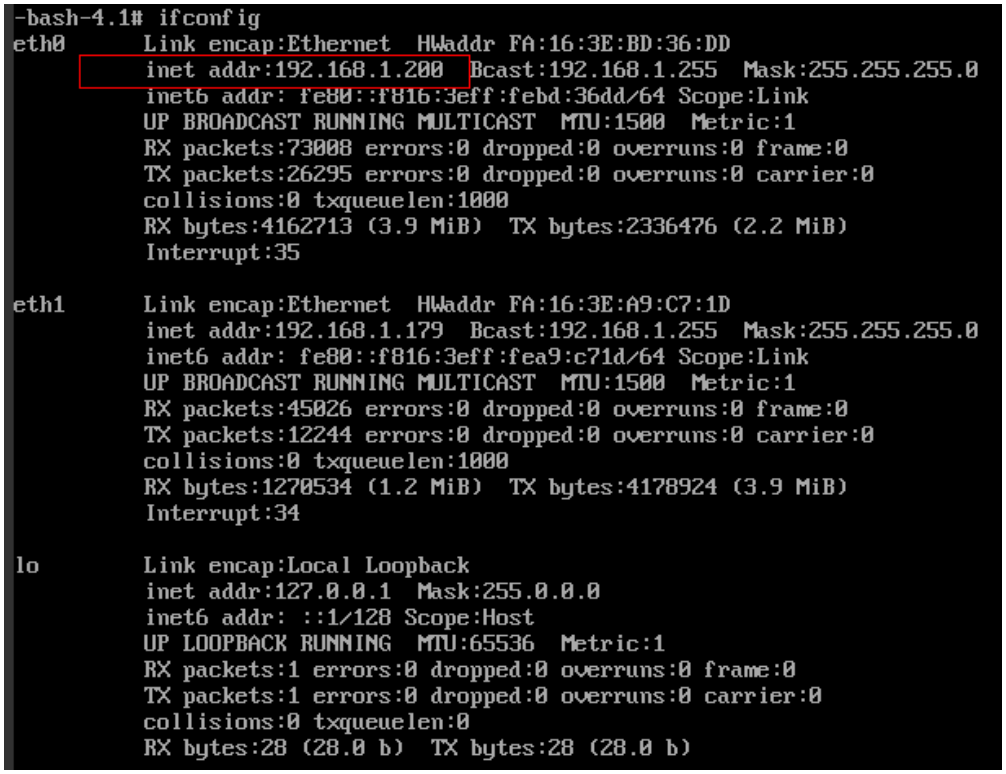
Possível causa	Solução
Falha ao efetuar logon no ECS ou criar um usuário não-raiz após a configuração do Cloud-init.	Verifique o formato do arquivo de configuração **/etc/cloud/cloud.cfg**. Para mais detalhes, consulte **Não é possível efetuar logon no ECS ou criar um usuário não raiz após a configuração do Cloud-init**.
Falha ao usar uma chave privada obtida para efetuar logon em um ECS após o início do ECS (Falha ao obter a senha de logon do ECS).	Reinicie o ECS e tente novamente.

O ECS não obteve endereço IP

Verifique se o ECS obteve um endereço IP.

Se nenhum endereço IP for obtido, execute o comando **dhclient** para obter o endereço IP (esse comando varia dependendo dos SOs do ECS). Como alternativa, você pode executar o comando **ifdown *ethx*** para desativar a porta de rede e, em seguida, executar o comando **ifup *ethx*** para permitir que a NIC do ECS obtenha automaticamente um endereço IP novamente.

Figura 8-7 Endereço IP de ECS



Rota incorreta para 169.254.169.254

Faça ping de **169.254.169.254/32** do ECS. Se o endereço IP não puder receber ping, execute as seguintes etapas:

1. Verifique a rota exata configurada no ECS para o endereço IP **169.254.169.254/32**.

   Na maioria dos casos, o próximo salto da rota exata para o endereço IP **169.254.169.254/32** é o mesmo que o da rota padrão para o endereço IP.

   Figura 8-8 Rota para o endereço IP **169.254.169.254/32**

   ```
   -bash-4.1# ip route
   169.254.169.254 via 192.168.1.1 dev eth0  proto static
   192.168.1.0/24 dev eth0  proto kernel  scope link  src 192.168.1.200
   192.168.1.0/24 dev eth1  proto kernel  scope link  src 192.168.1.179
   169.254.0.0/16 dev eth0  scope link  metric 1002
   default via 192.168.1.1 dev eth0  proto static
   -bash-4.1#
   ```

2. Se não houver uma rota exata para o endereço IP **169.254.169.254/32**, a causa é a seguinte:

   Imagens com sistemas operacionais de CentOS 5 não são compatíveis com Cloud-init. Para usar o Cloud-init, selecione um sistema operacional diferente.

3. Se o próximo salto da rota exata para o endereço IP **169.254.169.254/32** for diferente da rota padrão para o endereço IP:
   - Se o ECS tiver sido criado antes da ativação do Cloud-init, execute **service network restart** para obter a rota correta.
   - Se o ECS tiver sido criado recentemente, **envie um tíquete de serviço** ou entre em contato com o suporte técnico.

Não obteve os metadados do ECS

Execute o seguinte comando no ECS para obter os metadados:

curl http://169.254.169.254/openstack/latest/meta_data.json

Se forem exibidas informações semelhantes às mostradas em **Figura 8-9**, o ECS obtém os metadados com êxito.

Figura 8-9 Saída do comando

Não é possível efetuar logon no ECS ou criar um usuário não raiz após a configuração do Cloud-init

Verifique se o formato do arquivo de configuração **/etc/cloud/cloud.cfg** está correto. Para obter detalhes, consulte os requisitos de formato de arquivo para diferentes distribuições de

Linux. A figura a seguir mostra um exemplo de arquivo de configuração **/etc/cloud/cloud.cfg** para o Ubuntu.

Figura 8-10 Arquivo de configuração

```
system_info:
  # This will affect which distro class gets used
  distro: rhel
  # Default user name + that default users groups (if added/used)
  default_user:
    name: linux  // Specifies the username for login.
    lock_passwd: False  // The value False indicates that the password login mode is enabled. For some OSs, the value 0 indicates that the password login mode is enabled.
    gecos: Cloud User
    groups: users  // Specifies whether the user will be added to a group. This parameter is optional. The groups parameter value must be an existing group under /etc/group in the system.
    passwd: $6$I63DBVKK$Zh4lchiJR7HuIvtJHsYBQJIg5RoQCRL51X2Hsgj2s5JwXI7KUO1we8WYcwbzea52VHpRmNo28vmxxCyU6LwoD0
    sudo: ["ALL=(ALL) NOPASSWD:ALL"]  // Specifies that all permissions of user root will be granted to the user.
    shell: /bin/bash  // Specifies that the bash shell is used.
  # Other config here will be given to the distro class and/or path classes
  paths:
     cloud_dir: /var/lib/cloud/
     templates_dir: /etc/cloud/templates/
  ssh_svcname: sshd
```

Chave privada obtida não pode ser usada para efetuar logon em um ECS após o início do ECS (falha ao obter a senha de logon do ECS)

Reinicie o ECS para corrigir a falha.

Submissão de um tíquete de serviço

Se o EIP ainda falhar em usar Cloud-init após executar as etapas anteriores, **envie um tíquete de serviço**.

Forneça as seguintes informações ao engenheiro de suporte técnico.

Item	Descrição	Exemplo	Valor
Bloco CIDR da VPC	Necessário para a configuração do gateway do cliente	Exemplo: 10.0.0.0/16	N/D
ID da VPC	N/D	Exemplo: 120b71c7-94ac-45b8-8ed6-30aafc8fbdba	N/D
Bloco CIDR da sub-rede 1 (pode ser o mesmo que o bloco CIDR da VPC)	N/D	Exemplo: 10.0.1.0/24	N/D
ID do ECS	N/D	N/D	N/D
Endereço IP de ECS	N/D	Exemplo: 192.168.1.192/24	N/D
Informações de rota do ECS	N/D	N/D	-

8.8 Por que meu ECS não consegue acessar a Internet mesmo depois que um EIP é vinculado?

Sintoma

Um ECS com um EIP vinculado não pode acessar a Internet.

Solução de problemas

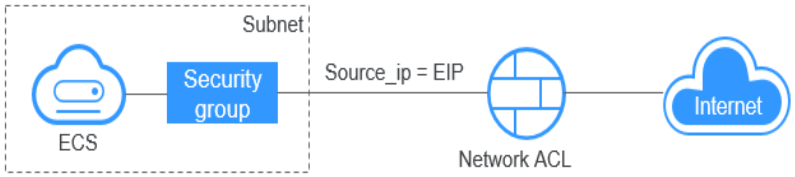
Verificar se os EIPs estão bloqueados ou congelados

- Verifique se o EIP está bloqueado. Para obter detalhes, consulte **Como desbloquear um EIP?**
- Verifique se o EIP está congelado. Para obter detalhes, consulte **Por que meus EIPs estão congelados? Como descongelar meus EIPs?**

Verificar a conectividade do EIP

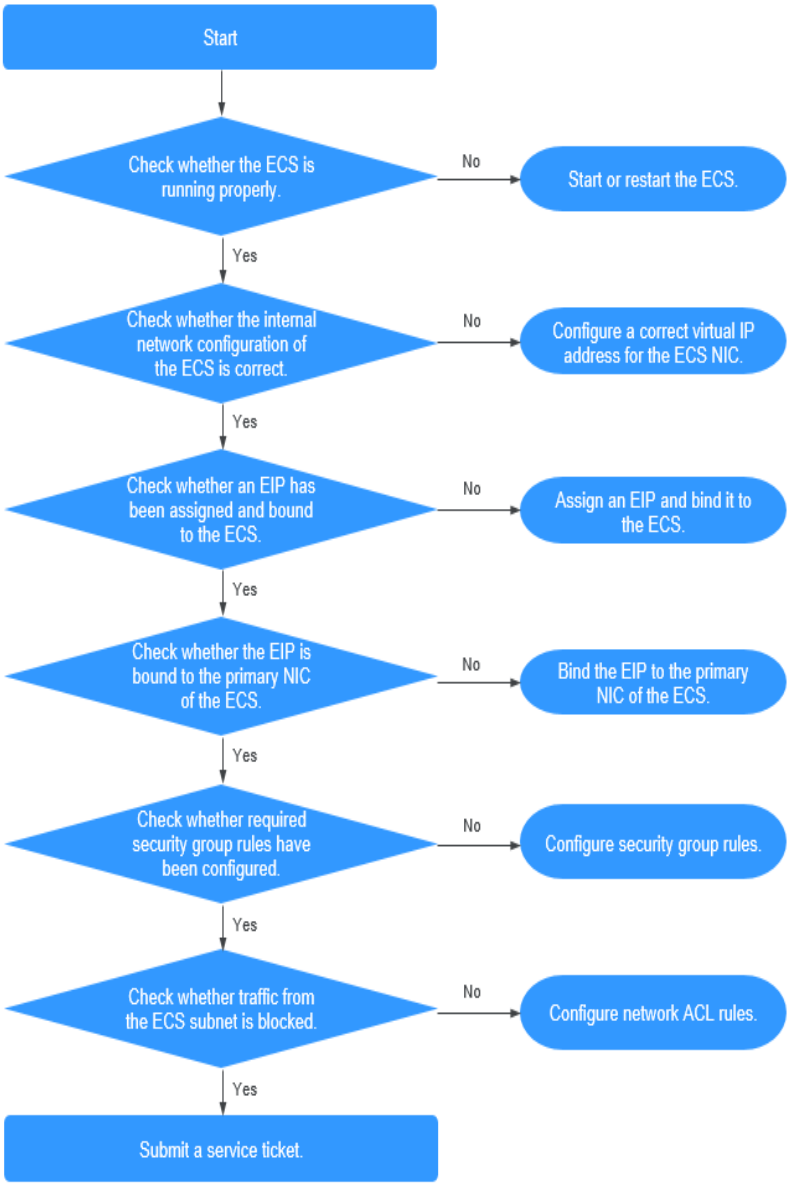
Figura 8-11 mostra o diagrama de rede para um ECS acessar a Internet usando um EIP.

Figura 8-11 Diagrama de rede do EIP



Localize a falha com base no procedimento a seguir.

Figura 8-12 Procedimento de solução de problemas



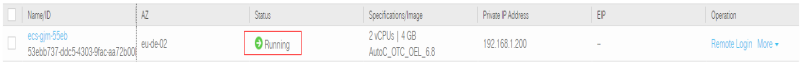
1. **Passo 1: verificar se o ECS está funcionando corretamente**
2. **Passo 2: verificar se a configuração de rede do ECS está correta**
3. **Passo 3: verificar se um EIP foi atribuído e vinculado ao ECS**
4. **Passo 4: verificar se um EIP está vinculado à NIC primária do ECS**
5. **Passo 5: verificar se as regras do grupo de segurança necessárias foram configuradas.**
6. **Passo 6: verificar se o tráfego da sub-rede do ECS está bloqueado**

Passo 1: verificar se o ECS está funcionando corretamente

Verifique o estado do ECS.

Se o estado do ECS não for **Running**, inicie ou reinicie o ECS.

Figura 8-13 Estado do ECS



Passo 2: verificar se a configuração de rede do ECS está correta

1. Verifique se a NIC do ECS tem um endereço IP atribuído.

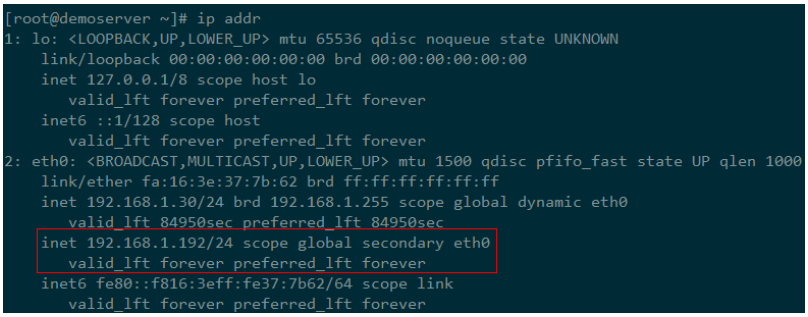
   Faça logon no ECS, e execute **ifconfig** ou **ip address** para verificar o endereço IP da NIC do ECS.

   Se as NICs primária e de extensão de um ECS tiverem um EIP vinculado, verifique se o ECS tem rotas baseadas em políticas configuradas. Se o ECS executar Windows, execute **ipconfig**.

2. Verifique se a NIC do ECS tem um endereço IP virtual.

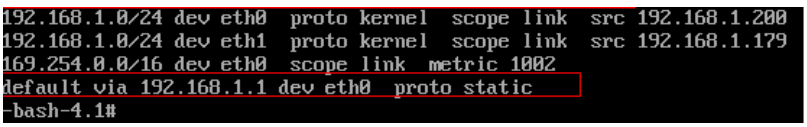
   Faça logon no ECS e execute **ifconfig** ou **ip address** para verificar se a NIC do ECS tem um endereço IP virtual. Se a NIC do ECS não tiver um endereço IP virtual, execute o comando **ip addr add** *virtual IP address* **eth0** para configurar um endereço IP para a NIC do ECS.

   Figura 8-14 Endereço IP virtual de uma NIC

   Verifique se a NIC do ECS tem uma rota padrão. Se não houver uma rota padrão, execute **ip route add** para adicionar uma.

   Figura 8-15 Rota predefinida

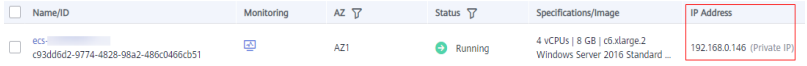
   

Passo 3: verificar se um EIP foi atribuído e vinculado ao ECS

Verifique se um EIP foi atribuído e vinculado ao ECS. Se nenhum EIP tiver sido atribuído, atribua um EIP e vincule-o ao ECS.

O ECS mostrado na **Figura 8-16** não tem nenhum EIP vinculado. Ele só tem um endereço IP privado vinculado.

Figura 8-16 Status do EIP



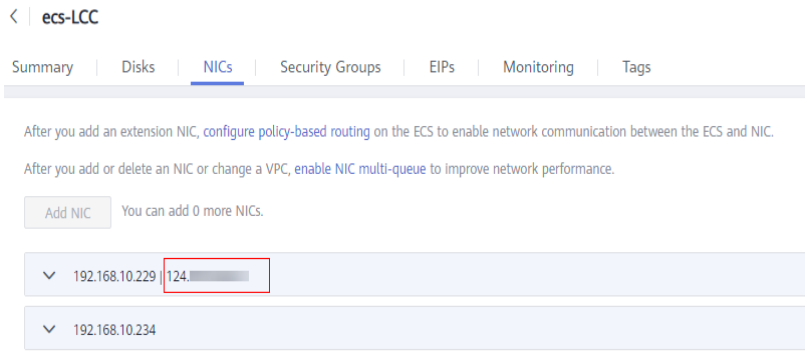
Passo 4: verificar se um EIP está vinculado à NIC primária do ECS

Verifique se um EIP está vinculado à NIC primária do ECS. Se não houver nenhum EIP vinculado à NIC primária do ECS, vincule um.

Você pode exibir os detalhes da NIC clicando na guia **NICs** na página de detalhes do ECS. Por padrão, o primeiro registro na lista é a NIC primária.

Como mostrado em **Figura 8-17**, o EIP está vinculado à NIC primária.

Figura 8-17 Verificar se o EIP está vinculado à NIC primária do ECS



Passo 5: verificar se as regras do grupo de segurança necessárias foram configuradas.

Para obter detalhes sobre como adicionar regras de grupo de segurança, consulte **Adição de uma regra de grupo de segurança**.

Se as regras do grupo de segurança não tiverem sido configuradas, configure-as com base nas suas necessidades de serviço. (O endereço IP remoto indica o endereço IP permitido e **0.0.0.0/0** indica que todos os endereços IP são permitidos.)

Passo 6: verificar se o tráfego da sub-rede do ECS está bloqueado

Verifique se a ACL da rede da sub-rede da NIC bloqueia determinado tráfego da sub-rede.

Você pode configurar a ACL da rede no console da VPC. Certifique-se de que as regras de ACL da rede permitem o tráfego da sub-rede do ECS.

Submissão de um tíquete de serviço

Se o EIP ainda não puder se comunicar com a Internet depois de executar todas as etapas acima, **envie um tíquete de serviço**.

Forneça as seguintes informações ao suporte técnico.

Item	Descrição	Exemplo	Valor
Bloco CIDR da VPC	Necessário para configuração de gateway	Exemplo: 10.0.0.0/16	N/D

Item	Descrição	Exemplo	Valor
ID da VPC	N/D	Exemplo: 120b71c7-94ac-45b8-8ed6-30aafc8fbdba	N/D
Bloco CIDR da sub-rede 1 (pode ser o mesmo que o bloco CIDR da VPC)	N/D	Exemplo: 10.0.1.0/24	N/D
ID do ECS	N/D	N/D	N/D
Endereço IP de ECS	N/D	Exemplo: 192.168.1.192/24	N/D
Informações de rota do ECS	N/D	N/D	N/D
EIP	Necessário para que o ECS acesse a Internet	Exemplo: 10.154.55.175	N/D
Largura de banda de EIP	Tamanho máximo da largura de banda usada pelo ECS para acessar a Internet	Exemplo: 1 Mbit/s	N/D
ID do EIP	N/D	Exemplo: b556c80e-6345-4003-b512-4e6086abbd48	N/D

8.9 Por que meu ECS não consegue se comunicar em uma rede de Camada 2 ou de Camada 3?

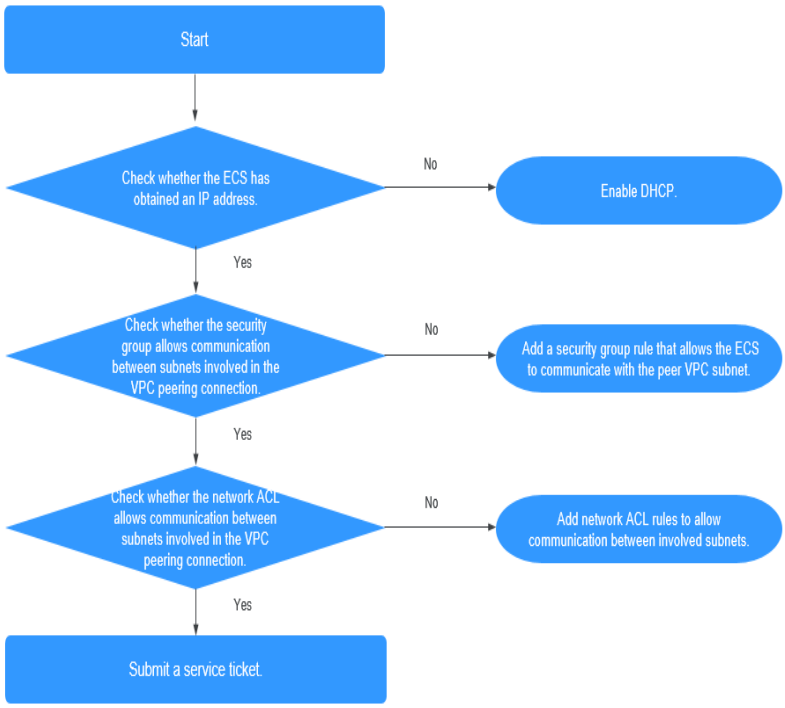
Sintoma

Um ECS não pode executar ping no gateway da sub-rede em que o ECS reside.

Solução de problemas

Localize a falha com base no procedimento a seguir.

Figura 8-18 Procedimento de solução de problemas



1. **Verificar se o ECS obteve um endereço IP**
2. **Verificar se o grupo de segurança permite a comunicação entre sub-redes envolvidas na conexão de emparelhamento da VPC**
3. **Verificar se a ACL de rede permite comunicação entre sub-redes envolvidas na conexão de emparelhamento da VPC**

Verificar se o ECS obteve um endereço IP

Faça logon no ECS, e execute **ifconfig** ou **ip address** para verificar o endereço IP da NIC do ECS. Se um ECS executar o Windows, use **ipconfig**.

Se o ECS não tiver um endereço IP, verifique se o DHCP foi habilitado para a sub-rede necessária.

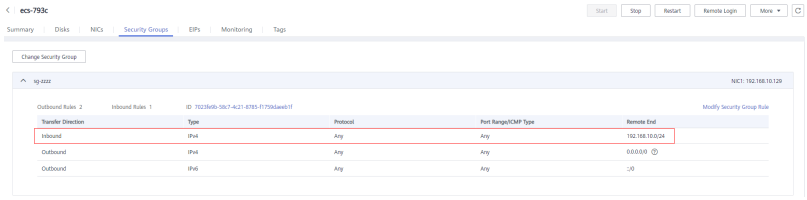
Alterne para a página de detalhes da sub-rede e verifique se a função DHCP foi ativada.

Para mais detalhes, consulte **Por que meu ECS não consegue obter um endereço IP?**

Verificar se o grupo de segurança permite a comunicação entre sub-redes envolvidas na conexão de emparelhamento da VPC

Você pode exibir o grupo de segurança na página de detalhes do ECS. Verifique se uma regra de grupo de segurança foi configurada para permitir que o ECS se comunique com a sub-rede da VPC de mesmo nível.

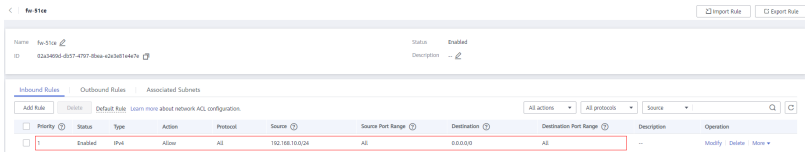
Figura 8-19 Regra de grupo de segurança



Verificar se a ACL de rede permite comunicação entre sub-redes envolvidas na conexão de emparelhamento da VPC

No painel de navegação à esquerda do console da VPC, escolha **Network ACLs**. Na página exibida, selecione a ACL de rede associada às sub-redes da conexão de emparelhamento da VPC. Na página de detalhes da ACL de rede, verifique se as regras da ACL de rede permitem a comunicação entre as sub-redes envolvidas na conexão de emparelhamento da VPC.

Figura 8-20 Regra de ACL de rede



Enviar um tíquete de serviço

Se o problema persistir, **envie um tíquete de serviço**.

8.10 Como lidar com uma falha de rede do BMS?

1. Execute o seguinte comando para verificar se as portas de rede do BMS foram vinculadas:

   ifconfig

   Figura 8-21 Verificar a vinculação

```
[root@bms2 rhel]# ifconfig
bond0     Link encap:Ethernet  HWaddr FA:16:3E:E9:B0:8A
          inet addr:192.168.2.46  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::f816:3eff:fee9:b08a/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MASTER MULTICAST  MTU:8888  Metric:1
          RX packets:188108 errors:0 dropped:0 overruns:0 frame:0
          TX packets:112119 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:42689694 (40.7 MiB)  TX bytes:82939564 (79.0 MiB)

bond0.2966 Link encap:Ethernet  HWaddr FA:16:3E:60:9C:CF
          inet addr:192.168.4.113  Bcast:192.168.4.255  Mask:255.255.255.0
          inet6 addr: fe80::f816:3eff:fe60:9ccf/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:8888  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:660 (660.0 b)  TX bytes:720 (720.0 b)

eth0      Link encap:Ethernet  HWaddr FA:16:3E:E9:B0:8A
          UP BROADCAST RUNNING SLAVE MULTICAST  MTU:8888  Metric:1
          RX packets:174667 errors:0 dropped:0 overruns:0 frame:0
          TX packets:112119 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:41874228 (39.9 MiB)  TX bytes:82939564 (79.0 MiB)

eth1      Link encap:Ethernet  HWaddr FA:16:3E:E9:B0:8A
          UP BROADCAST RUNNING SLAVE MULTICAST  MTU:8888  Metric:1
          RX packets:13441 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:815466 (796.3 KiB)  TX bytes:0 (0.0 b)
```


Se nenhuma informação de vinculação for obtida, as portas de rede BMS não serão vinculadas. Entre em contato com o suporte técnico.

2. Execute o seguinte comando para verificar se as informações de rota do BMS estão corretas:

   route –n

   Figura 8-22 Verificar informações de rota do BMS

   ```
   [root@bms2 rhel]# route -n
   Kernel IP routing table
   Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
   169.254.169.254 192.168.2.1     255.255.255.255 UGH   0      0        0 bond0
   192.168.4.0     0.0.0.0         255.255.255.0   U     0      0        0 bond0.2966
   192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 bond0
   169.254.0.0     0.0.0.0         255.255.0.0     U     1006   0        0 bond0
   169.254.0.0     0.0.0.0         255.255.0.0     U     1007   0        0 bond0.2966
   0.0.0.0         192.168.2.1     0.0.0.0         UG    0      0        0 bond0
   [root@bms2 rhel]#
   ```

   Verifique se a rota padrão (com um destino de 0.0.0.0/0) existe.

   Figura 8-23 Verificar a rota padrão

   ```
   0.0.0.0         192.168.2.1     0.0.0.0         UG    0      0        0 bond0
   [root@bms2 rhel]#
   ```

   Verifique se existe uma rota para **169.254.169.254**.

   Figura 8-24 Verificar a rota para o intervalo de endereços IP **169.254.169.254**

   ```
   Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
   169.254.169.254 192.168.2.1     255.255.255.255 UGH   0      0        0 bond0
   ```

   Se as rotas necessárias não estiverem lá, entre em contato com o suporte técnico.

3. Se os BMSs em uma VPC não puderem se comunicar uns com os outros ou um BMS com um EIP vinculado não puder acessar a Internet, corrija a falha com base nas perguntas frequentes relacionadas.

4. Se a falha não puder ser corrigida depois de executar essas operações, entre em contato com o suporte técnico.

   Obtenha as informações sobre VPC e BMS no console de gerenciamento e forneça ao engenheiro de suporte técnico as seguintes informações.

Item	Descrição	Exemplo	Valor
ID da VPC 1	ID da VPC 1	Exemplo: fef65559-c154-4229-afc4-9ad0314437ea	N/D
ID do BMS 1	ID do BMS 1 na VPC 1	Exemplo: f7619b12-3683-4203-9271-f34f283cd740	N/D

Item	Descrição	Exemplo	Valor
ID do BMS 2	ID do BMS 2 na VPC 1	Exemplo: f75df766-68aa-4ef3-a493-06cdc26ac37a	N/D

8.11 Por que meu ECS não consegue obter um endereço IP?

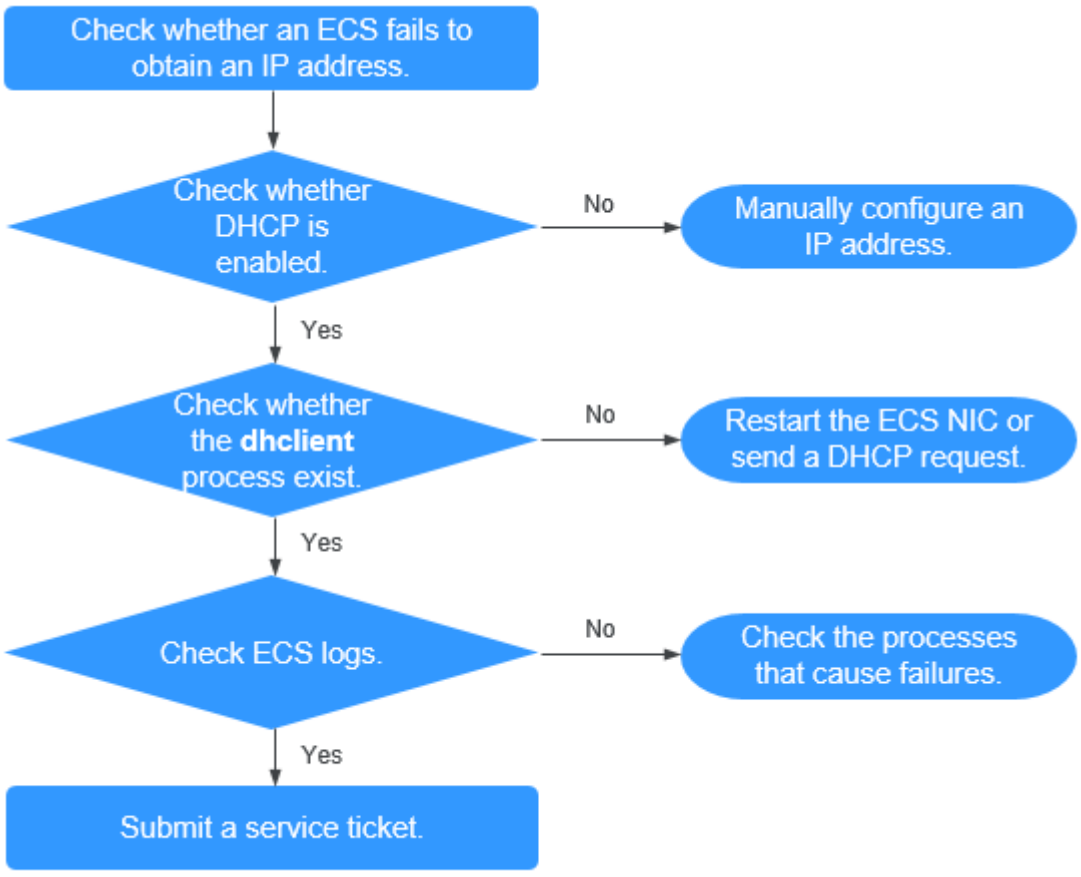
Sintoma

Não foi possível obter o endereço IP privado do ECS.

Solução de problemas

Localize a falha com base no procedimento a seguir.

Figura 8-25 Processo de solução de problemas



1. **Verificar se o DHCP está habilitado**
2. **Verificar se o processo dhclient existe**
3. **Verificar logs do ECS**

Verificar se o DHCP está habilitado

Verifique se a função DHCP da sub-rede está ativada (ativada por padrão).

Alterne para a página de detalhes da sub-rede. Se o DHCP estiver desabilitado, você deverá configurar manualmente um endereço IP estático para o ECS consultando a etapa **3**.

Verificar se o processo dhclient existe

1. Verifique se o processo **dhclient** existe:

   ps -ef | grep dhclient

2. Se o processo **dhclient** não existir, efetue logon no ECS e reinicie a NIC do ECS ou envie uma solicitação DHCP.
   - Linux:

     Execute o comando **dhclient ethx**. Se os comandos **dhclient** forem suportados, execute o comando **ifdown ethx;ifup ethx**. No comando, *ethx* indica a NIC do ECS, por exemplo, **eth0** e **eth1**.
   - Windows:

     Desconecte a conexão de rede e conecte-a.
3. Se o cliente de DHCP não enviar solicitações por um longo período de tempo, por exemplo, a falha ocorrer novamente após o reinício da NIC, você poderá usar o seguinte método para configurar o endereço IP estático.
   - Linux:
     i. Execute o seguinte comando para abrir o arquivo **/etc/sysconfig/network-scripts/ifcfg-eth0**:

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

     ii. Modifique os seguintes itens de configuração no arquivo **/etc/sysconfig/network-scripts/ifcfg-eth0**.

        BOOTPROTO=static

        IPADDR=192.168.1.100 #IP address

        NETMASK=255.255.255.0 #Subnet mask

        GATEWAY=192.168.1.1 #Gateway address

     iii. Execute o seguinte comando para reiniciar o serviço da rede:

        service network restart
   - Windows:

     Na guia **Local Area Connection Status**, clique em **Properties**. Na área exibida, selecione **Internet Protocol Version 4 (TCP/IPv4)** e clique em **Properties**. Na área exibida, insira o endereço IP, a máscara de sub-rede e o endereço de gateway padrão.

Verificar logs do ECS

Verifique o log de **messages** do ECS no diretório **/var/log/messages**.

Procure o endereço MAC da NIC e verifique se há algum processo que cause falhas na obtenção de endereços IP por DHCP.

Enviar um tíquete de serviço

Se o problema persistir, **envie um tíquete de serviço**.

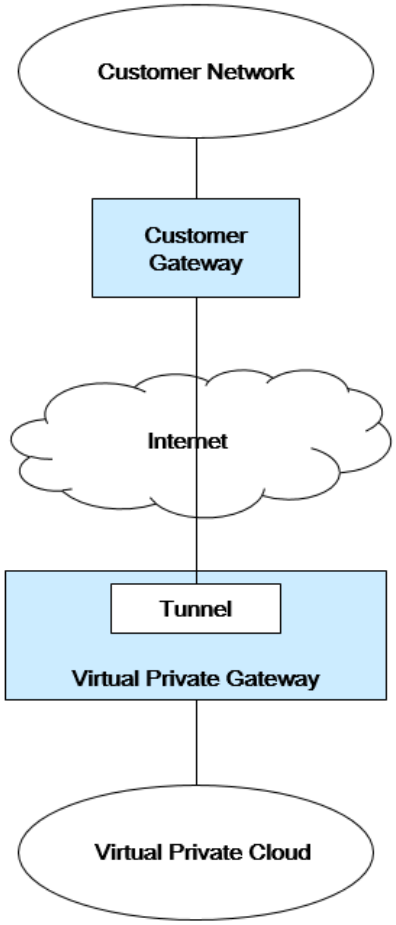
Forneça ao atendimento ao cliente o ID do ECS, o ID da sub-rede usada pelo ECS e o ID da VPC usada pelo ECS.

8.12 Como lidar com uma falha de rede VPN ou da Direct Connect?

Rede VPN

Figura 8-26 mostra sua rede, o gateway do cliente, a VPN e a VPC.

Figura 8-26 Rede VPN



Orientação de autoverificação do cliente

1. Forneça as informações da sua rede.

   Obter informações listadas em **Tabela 8-3**. Esta tabela lista valores de exemplo. Você pode determinar os valores reais com base nos valores de exemplo. Você deve obter todos os valores reais do seu projeto.

   NOTA

   Você pode imprimir esta tabela e preencher seus valores.

   Tabela 8-3 Informações da rede

Item	Descrição	Exemplo	Valor
Bloco CIDR da VPC	Necessário para a configuração do gateway do cliente	Exemplo: 10.0.0.0/16	N/D
ID da VPC	N/D	N/D	N/D
Bloco CIDR da sub-rede 1 (pode ser o mesmo que o bloco CIDR da VPC)	N/D	Exemplo: 10.0.1.0/24	N/D
ID do ECS	N/D	N/D	N/D
Tipo de gateway do cliente (por exemplo, Cisco)	N/D	N/D	N/D
Endereço IP público usado pelo gateway do cliente	N/D	O valor deve ser estático.	N/D

2. Forneça as informações de configuração do gateway.

   Você pode verificar os problemas de conectividade do gateway com base nas seguintes etapas:

   Você deve levar em consideração as regras de IKE, IPsec, ACL e a seleção de rotas. Você pode corrigir a falha em qualquer sequência desejada. No entanto, é recomendável que você verifique a falha na seguinte sequência: Regras de IKE, IPsec, ACL e seleção de rotas.

   a. Obtenha a política de IKE usada pelo dispositivo de gateway.
   b. Obtenha a política de IPsec utilizada pelo dispositivo de gateway.
   c. Obtenha a regra de ACL usada pelo seu dispositivo de gateway.
   d. Verifique se o dispositivo de gateway pode se comunicar com os dispositivos de gateway na nuvem.

   NOTA

   Os comandos usados em diferentes dispositivos de gateway são diferentes. Você pode executar os comandos baseados em seu dispositivo de gateway (como o dispositivo Cisco, H3C, AR ou Fortinet) para obter as informações necessárias anteriores.

Operações de O&M que exigem assistência

Você deve enviar solicitações de comunicação dos ECSs para o dispositivo remoto.

Método:

Faça logon em um ECS e faça o ping de um endereço IP no data center local.

8.13 Por que meu servidor pode ser acessado a partir da Internet, mas não pode acessar a Internet?

Sintoma

O servidor pode ser acessado, mas não pode acessar a Internet.

Solução de problemas

Verifique as seguintes possíveis causas.

Figura 8-27 Possíveis causas

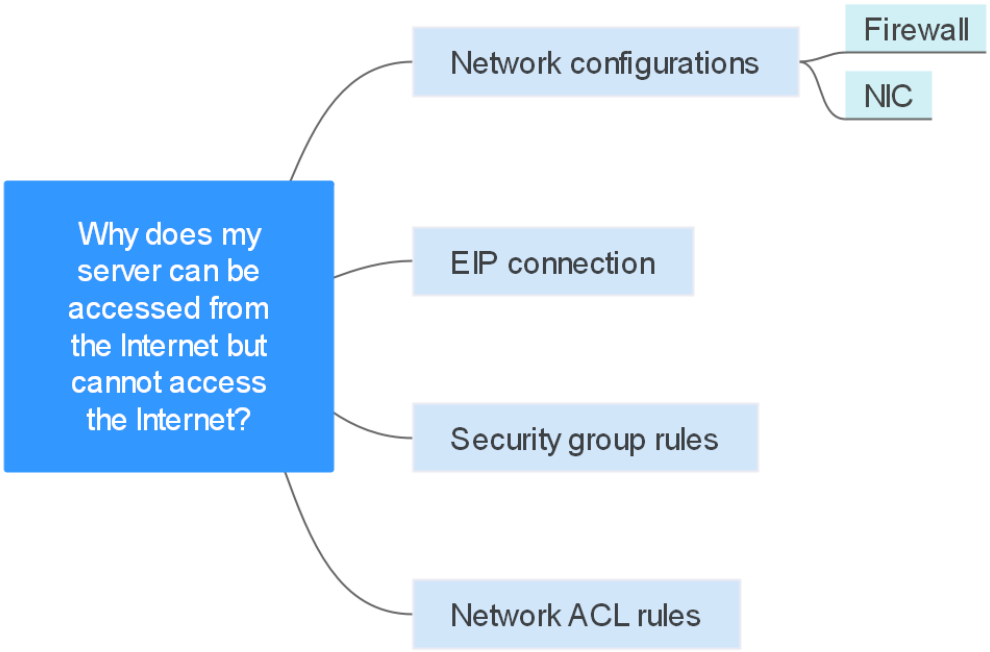


Tabela 8-4 Possíveis causas

Possível causa	Solução
Configurações de rede	Verifique as configurações de firewall e NIC. Veja **Configurações de rede**.
Conexão do EIP	Consulte **Por que o acesso à Internet falha mesmo se meu ECS estiver vinculado a um EIP?**

Possível causa	Solução
Regras de grupos de segurança	Veja **Regras de grupos de segurança**
Regras da network ACL	Veja **Regras da network ACL**

Configurações de rede

- Firewall

  Desative as regras de firewall para o ECS e verifique se a conectividade com a Internet foi restaurada:

  – ECS do Linux: **verificar a configuração do firewall**.

  – ECS do Windows: **verificar a configuração do firewall**.

- NIC

  Verifique as configurações de NIC e DNS.

  – ECS do Linux: **verificar a configuração da NIC**.

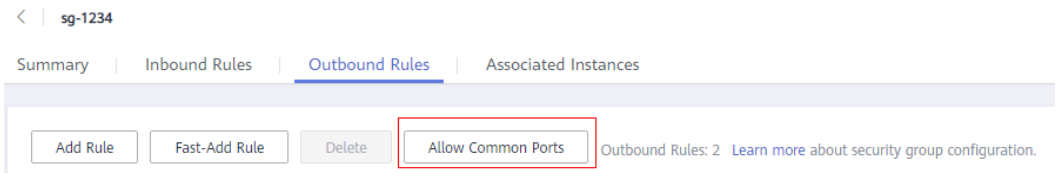
  – ECS do Windows: **verificar a configuração da NIC**.

Regras de grupos de segurança

Verifique se há uma regra de grupo de segurança para o servidor que nega o tráfego de saída.

Por padrão, um grupo de segurança permite todo o tráfego de saída. Se o tráfego de saída for negado, pode **configurar regras de grupo de segurança** ou clique em **Allow Common Ports**.

Figura 8-28 Permitir portas comuns

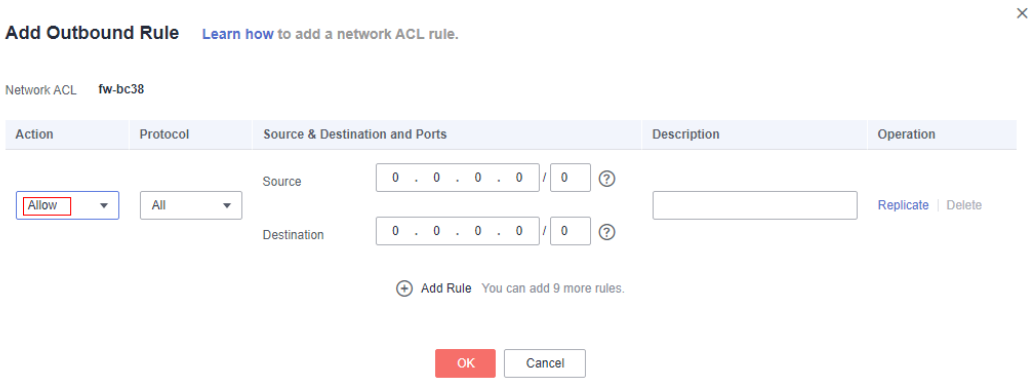


Regras da network ACL

Verifique se a network ACL da sub-rede à qual o servidor pertence nega o tráfego de saída.

Por padrão, uma network ACL nega todo o tráfego de saída. Você precisa adicionar uma regra de saída com **Action** definida como **Allow** à network ACL associada ao servidor.

Figura 8-29 Permitir tráfego de saída



Enviar um tíquete de serviço

Se o problema persistir, **envie um tíquete de serviço**.

8.14 Por que não consigo acessar sites usando endereços IPv6 após a configuração da pilha dual IPv4/IPv6?

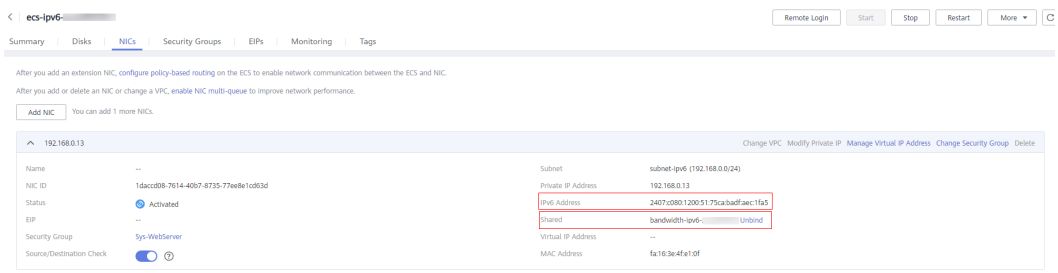
Sintoma

Você ativou a pilha dual IPv4/IPv6 para um ECS, mas o ECS não pode acessar sites usando endereços IPv6.

Solução de problemas

- Verifique se a pilha dual IPv4/IPv6 está configurada corretamente e se a NIC de pilha dual do ECS obteve um endereço IPv6.
- Verifique se o endereço IPv6 obtido da NIC de pilha dual foi adicionado a uma largura de banda compartilhada.
- Se o ECS tiver várias NICs, verifique se as rotas baseadas em políticas foram configuradas para essas NICs.

Figura 8-30 Detalhes da NIC



Solução

- Ao comprar um ECS, selecione **Automatically-assigned IPv6 address** para **Network**.

Se um endereço IPv6 não for atribuído automaticamente ou a imagem selecionada não for compatível com a alocação automática de endereços IPv6, obtenha manualmente o endereço IPv6 consultando **Atribuição dinâmica de endereços IPv6**.

NOTA

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

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

- Por padrão, os endereços IPv6 só podem ser usados para comunicação de rede privada. Se você quiser usar um endereço IPv6 para acessar a Internet ou quiser que ele seja acessado por clientes de IPv6 na Internet, será necessário adicionar o endereço IPv6 a uma largura de banda compartilhada. Para obter detalhes, consulte **Compra de uma largura de banda compartilhada e adição do endereço IPv6 a ela**.

  Se você já tiver uma largura de banda compartilhada, adicione o endereço IPv6 a ela.
- 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.

8.15 Por que meu ECS não se comunica com outros depois de ter o firewall instalado?

Sintoma

Um ECS tem uma única NIC e não consegue se comunicar com outras pessoas depois que o ECS tem um firewall instalado. Um cenário de exemplo é o seguinte:

Em uma VPC, há três ECSs. Os serviços são implementados no ECS 1 e no ECS 2, e um firewall de terceiros é instalado no ECS X. O tráfego do ECS 1 e do ECS 2 precisa ser filtrado pelo firewall do ECS X.

Localização de falha

Os problemas aqui são descritos em ordem de probabilidade de ocorrer.

Solucione o problema descartando as causas descritas aqui, uma por uma.

Tabela 8-5 Localização de falha

Possível causa	Solução
Regras de grupos de segurança	Veja **Se as regras do grupo de segurança estão configuradas**
Verificação de origem/destino	Veja **Se a verificação de origem/destino está desabilitada**

Possível causa	Solução
Rotas personalizadas da VPC	Veja **Se as rotas personalizadas da VPC são adicionadas**

Se as regras do grupo de segurança estão configuradas

As sub-redes na mesma VPC podem se comunicar entre si. Se o serviço de ECS não puder se comunicar com o ECS que tem firewall instalado, verifique se eles estão no mesmo grupo de segurança.

Se os ECSs estiverem em grupos de segurança diferentes, você precisará adicionar regras aos grupos de segurança para permitir o acesso uns dos outros.

Para obter detalhes, consulte **Adição de uma regra de grupo de segurança**.

Se a verificação de origem/destino está desabilitada

Verifique se a função de verificação de origem/destino está desabilitada na NIC do ECS com firewall instalado.

Se as rotas personalizadas da VPC são adicionadas

Verifique se a tabela de rotas de sub-rede do serviço VPC tem uma rota apontando para o ECS com firewall instalado.

Se não houver essa rota, adicione uma rota personalizada com o próximo salto definido para o ECS e o destino definido para o ECS com o firewall instalado.

Para obter detalhes, consulte **Adição de uma rota personalizada**.

Submissão de um tíquete de serviço

Se o problema persistir, **envie um tíquete de serviço**.

9 Roteamento

9.1 Como configurar rotas baseadas em políticas para um ECS com várias NICs?

Guia de operação

Este documento descreve como configurar rotas baseadas em políticas para ECSs do Linux e Windows. Para mais detalhes, consulte **Tabela 9-1**.

Tabela 9-1 Instruções de operação

Tipo de SO	Versão do endereço IP	Procedimento
Linux	IPv4	Tome um ECS executando o CentOS 8.0 (64-bit) como exemplo.
	IPv6	
Windows	IPv4	Tome um ECS executando o Windows Server 2012 (64-bit) como exemplo.
	IPv6	

Operações relacionadas

Se quiser acessar a Internet usando uma NIC de extensão, consulte **Como acessar a Internet usando um EIP vinculado a uma NIC de extensão?**

9.2 Uma tabela de rota pode abranger várias VPCs?

Uma tabela de rotas não pode abranger várias VPCs.

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. Uma VPC tem uma tabela de rotas padrão e pode ter várias tabelas de rotas personalizadas.

Cada sub-rede em uma VPC deve estar associada a uma tabela de rotas. Uma sub-rede só pode ser associada a uma tabela de rotas de cada vez, mas você pode associar várias sub-redes em uma VPC à mesma tabela de rotas.

9.3 Quantas rotas uma tabela de rotas pode conter?

Cada tabela de rotas pode conter um máximo de rotas200 por padrão, incluindo rotas adicionadas para conexões Direct Connect e de emparelhamento de VPC.

9.4 Existem restrições ao usar uma tabela de rotas?

- Um ECS que fornece SNAT deve ter **Unbind IP from MAC** habilitado.
- O destino de cada rota em uma tabela de rotas deve ser exclusivo. O próximo salto deve ser um endereço IP privado ou um endereço IP virtual na VPC. Caso contrário, a tabela de rotas não terá efeito.
- Se um endereço IP virtual for definido como o próximo salto em uma rota, os EIPs vinculados ao endereço IP virtual na VPC se tornarão inválidos.

9.5 As mesmas prioridades de roteamento se aplicam a conexões da Direct Connect e rotas personalizadas na mesma VPC?

Não. As conexões da Direct Connect e as rotas personalizadas são usadas em cenários diferentes, portanto, as prioridades de roteamento são diferentes.

9.6 Existem diferentes prioridades de roteamento da VPN e rotas personalizadas na mesma VPC?

Não. A prioridade de roteamento das rotas personalizadas e a das VPNs são as mesmas.

10 Segurança

10.1 As regras do grupo de segurança são consideradas iguais se todos os parâmetros, exceto sua descrição, forem iguais?

Sim. Não é possível adicionar ou importar uma regra de grupo de segurança que tenha os mesmos parâmetros, mas uma descrição diferente de uma regra existente no grupo de segurança.

10.2 Quais são os requisitos para excluir um grupo de segurança?

- Antes de excluir um grupo de segurança, verifique se o grupo de segurança não está sendo usado por nenhum recurso de nuvem, como servidores de nuvem, contêineres e bancos de dados. Se o grupo de segurança for usado por um recurso de nuvem, libere o recurso de nuvem ou altere o grupo de segurança usado pelo recurso de nuvem e, em seguida, exclua o grupo de segurança.
- Se o grupo de segurança que você deseja excluir estiver associado a regras de outro grupo de segurança (**Source**), exclua ou modifique as regras de grupo de segurança associadas e, em seguida, exclua o grupo de segurança.

  NOTA

  - O grupo de segurança padrão não pode ser excluído.
  - Se um grupo de segurança estiver associado a recursos diferentes de servidores e NICs de extensão, o grupo de segurança não poderá ser excluído.

10.3 Por que o acesso de saída na porta TCP 25 é bloqueado?

Sintoma

Não é possível acessar um endereço externo na porta TCP 25. Por exemplo, a execução do comando **Telnet smtp.***.com 25** falha.

Causa

Por motivos de segurança, a porta TCP 25 está desabilitada na direção de saída por padrão.

Você não precisa habilitar a porta TCP 25, a menos que queira implementar um serviço de e-mail na nuvem.

Esta seção aplica-se apenas a **CN-Hong Kong**.

Solução

- Use a porta 465 suportada pelo provedor de serviços de e-mail de terceiros.
- Aplique para ativar a porta TCP 25 na direção de saída.

  Se você precisar ativar a porta TCP 25 no ECS para comunicações externas, envie uma solicitação.

AVISO

Antes de enviar sua inscrição, você deve concordar e garantir que a porta TCP 25 seja usada apenas para se conectar a servidores de Simple Mail Transfer Protocol (SMTP) de terceiros e que os e-mails sejam enviados usando os servidores SMTP de terceiros. Se você usar o EIP especificado no tíquete de serviço para enviar e-mails diretamente por SMTP, a porta TCP 25 será permanentemente desativada e você não poderá mais usá-la ou solicitar que seja ativada.

1. Na página **Create Service Ticket**, escolha **Products** > **Elastic Cloud Server**.
2. Clique em **Open Port 25** em **Select Subtype** e crie um tíquete de serviço.

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

10.4 Como saber as instâncias associadas a um grupo de segurança?

Um grupo de segurança pode ser associado a instâncias quando ou depois de criadas. Para excluir esse grupo de segurança, você precisa desassociar as instâncias do grupo de segurança primeiro.

Você pode efetuar logon no console de gerenciamento para verificar as instâncias associadas mostradas em **Tabela 10-1** exceto servidores, NICs de extensão e interfaces de rede suplementares.

Se você não puder excluir um grupo de segurança mesmo depois de excluir todas as instâncias associadas, **envie um tíquete de serviço**.

Tabela 10-1 Lista de verificação

Categoria de produto	Produto
Banco de dados	GaussDB
	RDS
	DDS
	GaussDB NoSQL
	DDM
Middleware	Redis/Memcached
	Kafka
	RabbitMQ
	DMS (for RocketMQ)
	API Gateway
Big Data	DataArts Studio
	DWS
	CSS

10.5 Posso alterar o grupo de segurança de um ECS?

Sim. Faça logon no console do ECS, alterne para a página que mostra os detalhes do ECS e altere o grupo de segurança do ECS.

Para obter detalhes, consulte **Alteração de um grupo de segurança**.

10.6 Quantos grupos de segurança posso criar?

Cada conta pode ter até 100 grupos de segurança e 5000 regras de grupo de segurança.

Ao criar um ECS, você pode selecionar vários grupos de segurança, mas é recomendável selecionar não mais do que cinco.

10.7 Como configurar um grupo de segurança para protocolos multicanais?

Configuração do ECS

O daemon TFTP determina se um arquivo de configuração especifica o intervalo de portas. Se você usar um arquivo de configuração TFTP que permita que as portas do canal de dados sejam configuráveis, é uma boa prática configurar um intervalo pequeno de portas que não sejam escutadas.

Configuração do grupo de segurança

Você pode configurar a porta 69 e configurar portas de canal de dados usadas pelo TFTP para o grupo de segurança. No RFC1350, o protocolo TFTP especifica que as portas disponíveis para canais de dados variam de 0 a 65535. No entanto, nem todas essas portas são usadas pelos processos daemon TFTP de diferentes aplicações. Você pode configurar um intervalo menor de portas para o daemon TFTP.

A figura a seguir fornece um exemplo da configuração da regra de grupo de segurança se as portas usadas pelos canais de dados variarem de 60001 a 60100.

Figura 10-1 Regras de grupos de segurança

Type	Protocol	Port/Range	Source
IPv4	All	All	sg-test
IPv4	UDP	60001-60100	0.0.0.0/0

10.8 Uma regra de grupo de segurança ou uma regra de ACL da rede imediatamente tem efeito para conexões existentes depois de ser modificada?

- Depois que uma regra de grupo de segurança é modificada, a nova regra entra em vigor imediatamente para seu tráfego original. Os grupos de segurança são com status. As respostas ao tráfego de saída podem entrar na instância independentemente das regras do grupo de segurança de entrada e vice-versa. Os grupos de segurança usam o rastreamento de conexão para rastrear o tráfego de e para instâncias. Se uma regra de grupo de segurança for adicionada, excluída ou modificada, ou uma instância no grupo de segurança for criada ou excluída, o rastreamento de conexão para todas as instâncias no grupo de segurança será automaticamente limpo. Nesse caso, o tráfego de entrada ou saída da instância será considerado como novas conexões, que precisam corresponder às regras do grupo de segurança de entrada ou saída para garantir que as regras entrem em vigor imediatamente e garantam a segurança do tráfego de entrada.
- Uma ACL da rede de regra modificada não entrará em vigor imediatamente para suas conexões existentes. Demora cerca de 120 segundos para a nova regra entrar em vigor, e o tráfego será interrompido durante esse período. Para garantir que o tráfego seja imediatamente interrompido após a alteração da regra, é recomendável configurar regras de grupo de segurança.

10.9 Por que algumas portas são inacessíveis?

Symptom: Users in certain areas cannot access some ports.

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

Tabela 10-2 High-risk ports

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

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

10.10 Por que o acesso de um endereço IP específico ainda é permitido depois que uma regra de ACL da rede que nega o acesso do endereço IP foi adicionada?

As regras de network ACL têm prioridades. Um valor de prioridade menor representa uma prioridade mais alta. Cada network ACL inclui uma regra padrão cujo valor de prioridade é um asterisco (*). As regras padrão têm a prioridade mais baixa.

Se as regras entrarem em conflito, a regra com a prioridade mais alta entra em vigor.

Se você precisar que uma regra entre em vigor antes ou depois de uma regra específica, poderá inserir essa regra antes ou depois da regra específica. Por exemplo, se a prioridade da regra A é 1, mas você precisa que a regra B tenha prioridade sobre a regra A, insira a regra B antes da regra A. Então, a regra B terá prioridade 1 e a regra A será 2. Da mesma forma, se a regra B é menos importante que a regra A, insira a regra B depois da regra A.

Quando uma regra que nega o acesso de um endereço IP especificado é adicionada, insira as regras que permitem o acesso de todos os endereços IP no final. Em seguida, a regra que nega o acesso do endereço IP especificado terá prioridade sobre as outras regras e será efetiva. Para obter detalhes, consulte **Alteração da sequência de uma regra de network ACL**.

10.11 Por que minhas regras de grupo de segurança não entram em vigor?

Sintoma

As regras de grupo de segurança configuradas para um ECS não entraram em vigor.

Solução de problemas

Os problemas aqui são descritos em ordem de probabilidade de ocorrer.

Solucione o problema descartando as causas descritas aqui, uma por uma.

Figura 10-2 Solução de problemas

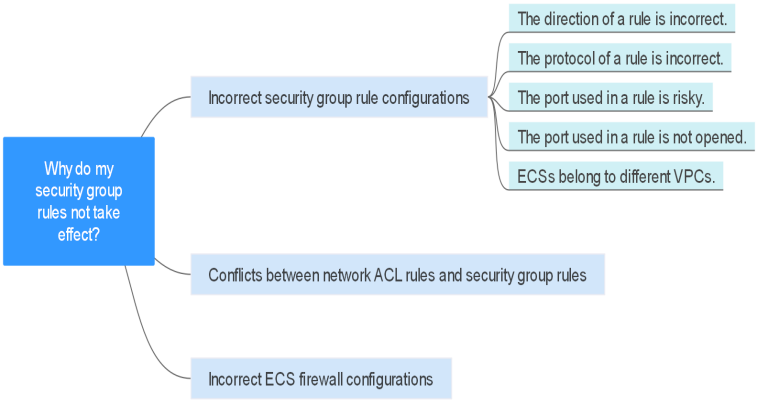


Tabela 10-3 Solução de problemas

Possível causa	Solução
Configurações de regra de grupo de segurança incorretas	Veja **Configuração de regra de grupo de segurança incorreta**
Conflitos entre as regras da network ACL e as regras do grupo de segurança	Veja **Conflitos entre as regras da network ACL e as regras do grupo de segurança**
Configurações incorretas do firewall do ECS	Veja **Configurações incorretas do firewall do ECS**

Configuração de regra de grupo de segurança incorreta

Se as regras do grupo de segurança estiverem incorretamente configuradas, os ECSs não poderão ser protegidos. Verifique as regras do grupo de segurança com base nas seguintes causas:

1. A direção de uma regra está incorreta.
2. O protocolo de uma regra está incorreto.
3. A porta usada em uma regra é arriscada e não pode ser acessada. Para obter detalhes sobre portas comuns e portas arriscadas, consulte **Portas comuns usadas pelos ECSs**.
4. A porta usada em uma regra não está aberta. Você pode executar as etapas a seguir para verificar se uma porta está sendo ouvida no servidor.

   Por exemplo, você implementou um site em ECSs. Os usuários precisam acessar seu site através de TCP (porta 80), e você adicionou a regra de grupo de segurança mostrada em **Tabela 10-4**.

Tabela 10-4 Regra de grupo de segurança

Direção	Protocolo	Porta	Origem
Entrada	TCP	80	0.0.0.0/0

ECS do Linux

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

a. Efetue logon no ECS.

b. Execute o seguinte comando para verificar se a porta TCP 80 está sendo escutada:

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

Se a saída do comando mostrada em **Figura 10-3** for exibida, a porta TCP 80 está sendo escutada.

Figura 10-3 Saída de comando para o ECS do Linux

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

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

ECS do Windows

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

a. Efetue logon no ECS.

b. Escolha **Start** > **Accessories** > **Command Prompt**.

c. Execute o seguinte comando para verificar se a porta TCP 80 está sendo escutada:

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

Se a saída do comando mostrada em **Figura 10-4** for exibida, a porta TCP 80 está sendo escutada.

Figura 10-4 Saída de comando para o ECS do Windows

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

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

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

Você pode **adicionar uma regra de grupo de segurança** ou **modificar uma regra de grupo de segurança** para selecionar a direção correta, protocolo e abrir as portas.

Conflitos entre as regras da network ACL e as regras do grupo de segurança

Os grupos de segurança operam ao nível do ECS, enquanto as network ACLs operam ao nível da sub-rede.

Por exemplo, se configurar uma regra de grupo de segurança de entrada para permitir o acesso através da porta 80 e uma regra de network ACL para negar o acesso através da porta 80, a regra de grupo de segurança não terá efeito.

Você pode **adicionar uma regra de network ACL** ou **modificar uma regra de network ACL** para permitir o tráfego da porta de protocolo correspondente.

Configurações incorretas do firewall do ECS

Verifique se o firewall do ECS abre as portas necessárias.

For details, see **Disabling a Windows ECS Firewall and Adding a Port Exception on a Windows ECS Firewall** or **Disabling a Linux ECS Firewall and Adding a Port Exception on a Linux ECS Firewall**.

Enviar um tíquete de serviço

Se o problema persistir, **envie um tíquete de serviço**.

