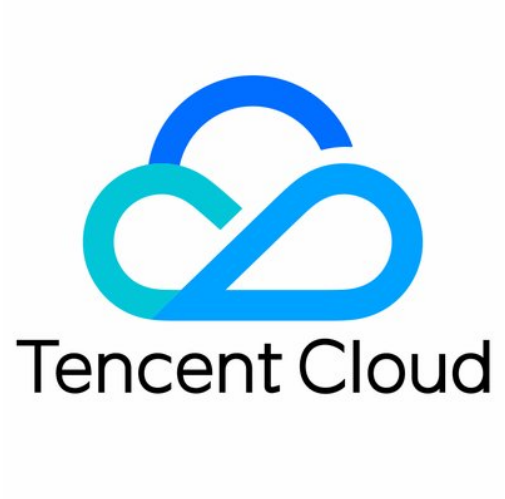
Virtual Private Cloud

Guia de operação

Product Documentation



Contents

Guia de operação
Topologia de rede

Last updated：2024-01-24 17:48:52

O mapa de topologia da rede exibe todos os recursos do VPC, para que você possa obter implantações e conexões do VPC em tempo real.

Instruções

1. Faça login no Console do VPC.
2. Clique em **Network Topology Map (Mapa de topologia da rede)** na barra lateral esquerda.
3. Selecione uma região e VPC para exibir os recursos de nuvem do VPC, como CVM, CLB, TencentDB e NoSQL, e sua relação de topologia de rede.
Nas duas sub-redes do VPC de exemplo, conforme mostrado abaixo, a sub-rede `test6` contém duas instâncias do CLB. Esse VPC se comunica com a internet por meio do NAT Gateway e da rede pública do CLB. Ele se comunica com o VPC oposto por meio do Peering Connection.

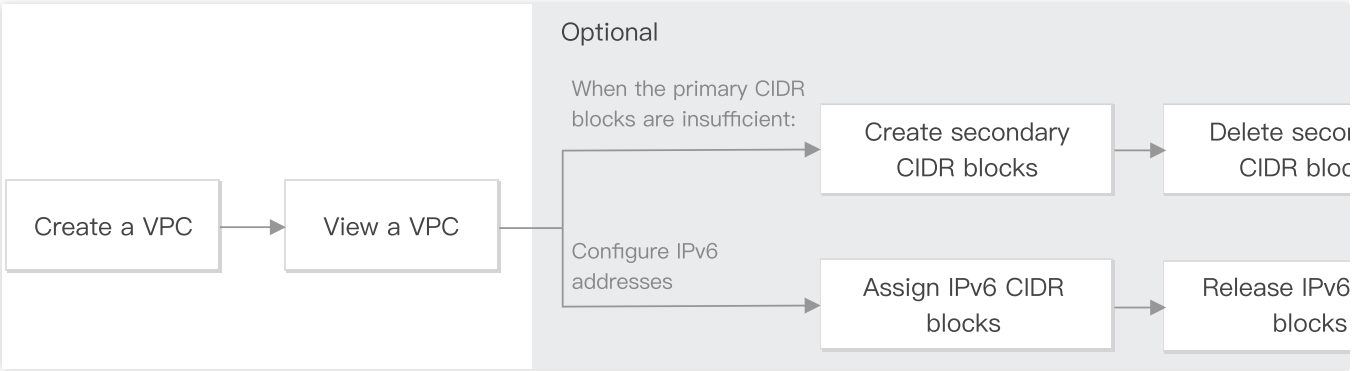
Virtual Private Cloud (VPC)
Visão geral

Last updated：2024-01-24 17:48:51

Um VPC é uma rede virtual isolada logicamente que você pode usar exclusivamente e planejar de forma independente no Tencent Cloud. Para usar qualquer recurso do Tencent Cloud, é necessário criar um VPC e uma sub-rede. Uma sub-rede é um espaço de rede no VPC. Você pode dividir um VPC em pelo menos uma sub-rede. O VPC é regional, já a sub-rede é específica da zona de disponibilidade. As sub-redes no mesmo VPC podem se comunicar entre si por meio de uma rede privada, por padrão.
Todos os recursos de nuvem, como os CVMs e os CLBs em um VPC, devem ser implantados em uma sub-rede.

Ciclo de vida do VPC

O ciclo de vida do VPC varia com as necessidades, conforme mostrado abaixo:



1. Criação de um VPC: é necessário planejar sua rede cuidadosamente antes de criar um VPC. Os blocos CIDR de VPCs e sub-redes não podem ser modificados após a criação.
2. Exibição de um VPC: é possível exibir as informações básicas de um VPC, sua associação ao CCN e os recursos que ele contém.
3. (Opcional) Escolha as operações que se aplicam aos seus casos de uso:
Quando o bloco CIDR principal for insuficiente, consulte Edição de blocos CIDR IPv4:
Criação de blocos CIDR secundários: é possível criar blocos CIDR secundários para atender às demandas reais da rede.
Exclusão de blocos CIDR secundários: é possível excluir os blocos CIDR secundários se não precisar mais deles.
4. Exclusão de um VPC: após um VPC for excluído, suas sub-redes e tabelas de rota também serão excluídas.

Limites

Last updated：2024-01-24 17:48:51

Limites de uso

Não é possível modificar os intervalos de IP da VPC e da sub-rede após a criação.
Para cada sub-rede, a Tencent Cloud reserva os seus dois primeiros IPs e o último para as redes de IP. Por exemplo, se o bloco CIDR da sub-rede for `172.16.0.0/24`, então `172.16.0.0`, `172.16.0.1` e `172.16.0.255` serão reservados pela Tencent Cloud.
Ao adicionar uma CVM a uma VPC, a instância será atribuída aleatoriamente a um IP privado de uma sub-rede especificada. Você pode reatribuir um IP privado a ele depois que a instância for criada.
Em uma VPC, um IP privado da CVM corresponde a um endereço IP público.
As CVMs baseadas na rede clássica não podem se interconectar com os recursos de nuvem no bloco CIDR secundário.
Um Peering Connection não aceita blocos CIDR secundários.
O Cloud Connect Network, o gateway do VPN e o gateway do Direct Connect padrão aceitam os blocos CIDR secundários.

Limites de cota

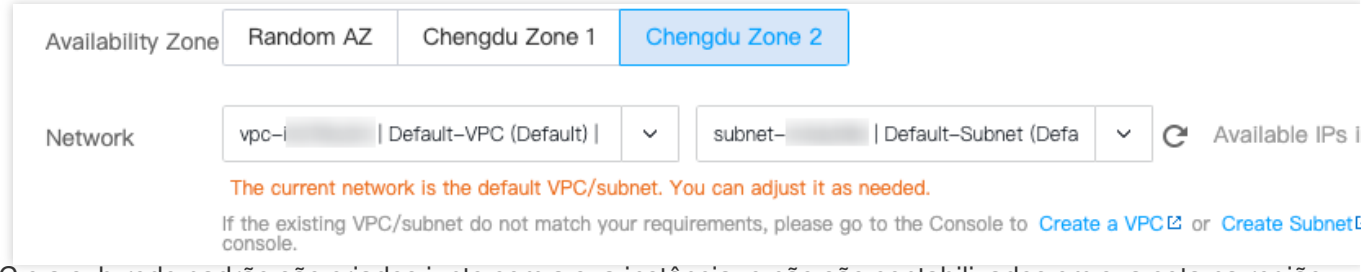
Recurso	Limites
Quantidade de instâncias da VPC por região e conta	20
Quantidade de sub-redes por VPC	100
Quantidade de blocos CIDR secundários por VPC	5

Nota:
Se você quiser aumentar a cota, envie um tíquete para solicitar.

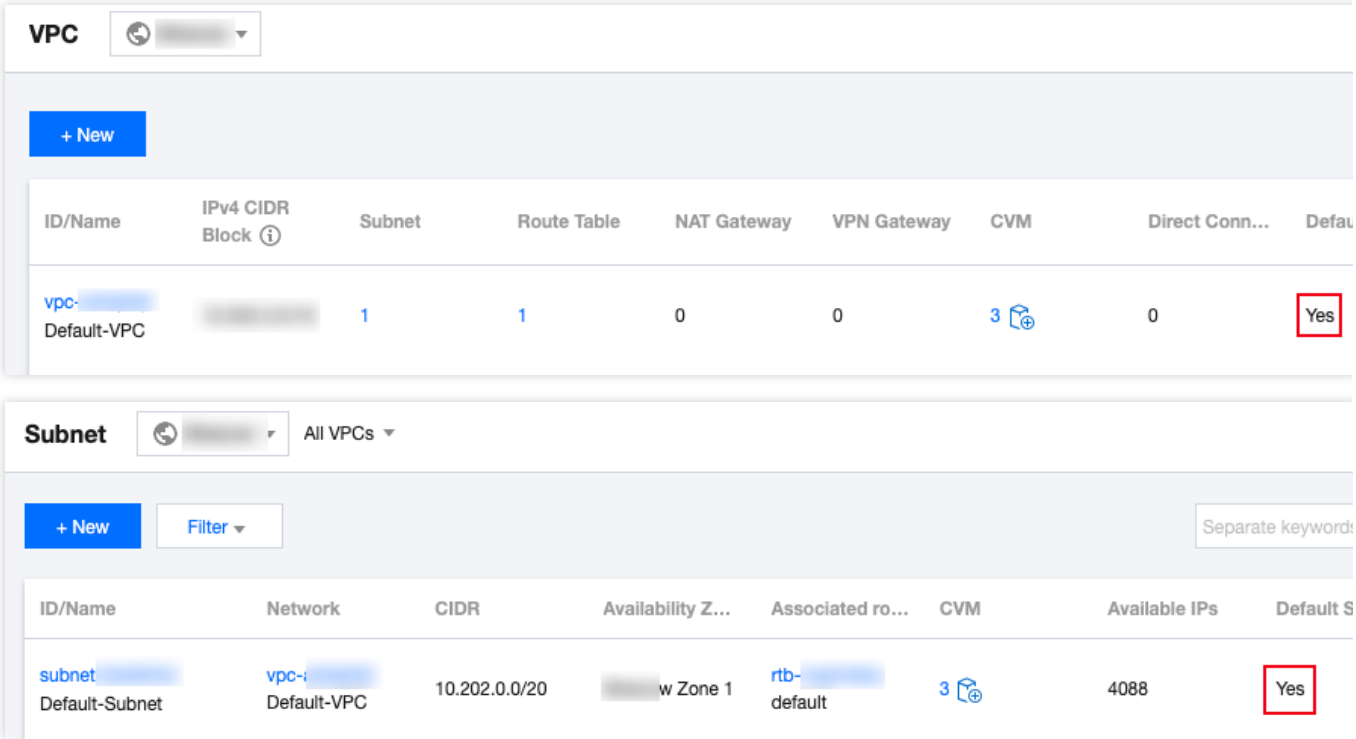
Criação de VPCs

Last updated：2024-01-24 17:48:51

Os Virtual Private Clouds (VPCs) são a base para o uso dos serviços do Tencent Cloud. Ao adquirir uma instância como CVM, CLB ou TencentDB em uma região que não tem VPCs existentes, um VPC e uma sub-rede padrão serão criados automaticamente.



O VPC e a sub-rede padrão são criados junto com a sua instância, e não são contabilizados em sua cota na região. Eles funcionam da mesma forma que os criados manualmente. Só pode haver um VPC e uma sub-rede padrão em cada região. É possível excluir o VPC e a sub-rede padrão se não precisar mais deles.



Você pode consultar este documento para criar uma instância do VPC no console se a instância padrão ou existente não for adequada.

Instruções

1. Faça login no Console do VPC.
2. Selecione uma região na parte superior da página **VPC**, e clique em **+ Novo (+New)**.
3. Insira as informações do VPC e da sub-rede no pop-up **Create VPC (Criar VPC)**.

Nota:

Os blocos CIDR do VPC e da sub-rede não podem ser modificados após a criação.

O bloco CIDR do VPC pode ser qualquer um dos seguintes intervalos de IP. Para que os VPCs se comuniquem entre si por meio de uma rede privada, seus blocos CIDR não devem se sobrepor.

`10.0.0.0` - `10.255.255.255` (intervalo de máscara entre 16 e 28)

`172.16.0.0` - `172.31.255.255` (intervalo de máscara entre 16 e 28)

`192.168.0.0` - `192.168.255.255` (intervalo de máscara entre 16 e 28)

O bloco CIDR da sub-rede deve estar dentro ou ser igual ao bloco CIDR do VPC.

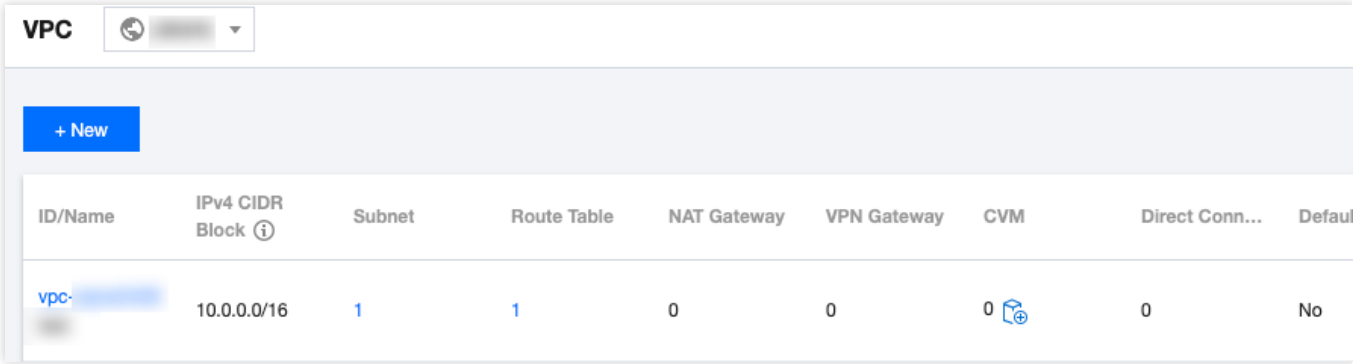
Por exemplo, se o intervalo de IP do VPC for `10.0.0.0/16`, então seu intervalo de IP da sub-rede pode ser `10.0.0.0/16`, `10.0.0.0/24`, etc.

Availability zone (Zona de disponibilidade): uma sub-rede é específica da zona de disponibilidade. Selecione uma zona de disponibilidade na qual a sub-rede está localizada. Um VPC permite sub-redes em diferentes zonas de disponibilidade e essas sub-redes podem se comunicar umas com as outras por meio de uma rede privada por padrão.

Associated route table (Tabela de rotas associada): a sub-rede deve ser associada a uma tabela de rotas para encaminhamento de tráfego. Uma tabela de rotas padrão será associada para garantir a interconexão da rede privada no VPC.

Advanced options (Opções avançadas): é possível adicionar tags para melhorar o gerenciamento das permissões de recursos de subusuários e colaboradores.

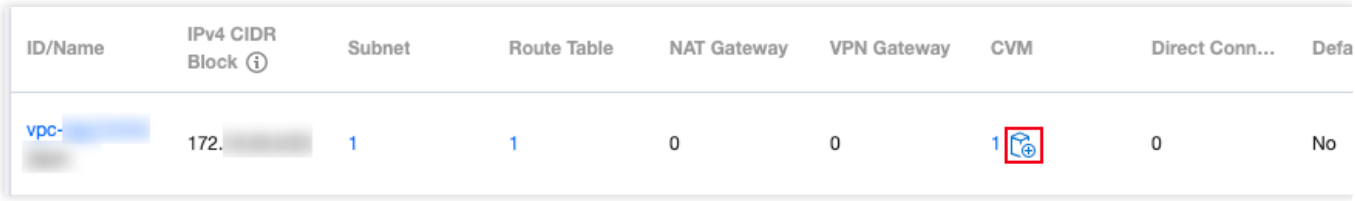
4. Ao concluir a configuração, clique em **OK**. Um VPC criado será exibido na lista, conforme mostrado abaixo. Um novo VPC tem uma sub-rede e uma tabela de rotas padrão.



Operação posterior

Depois que o VPC e a sub-rede forem criados, é possível implantar recursos, incluindo o CVM e o CLB no VPC. Clique no ícone conforme mostrado abaixo para adquirir diretamente um CVM na página de aquisição do CVM. Para

obter mais informações, consulte Criação de um VPC IPv4.



Exibição de VPCs

Last updated：2024-01-24 17:48:51

É possível consultar todos os recursos do VPC por meio do console do VPC, como os recursos de nuvem e as conexões em um VPC.

Instruções

1. Faça login no Console do VPC.
2. Selecione a região do VPC na parte superior da página **VPC**. É possível verificar as informações de todos os VPC nesta região na lista.

Coluna	Descrição
ID/Name (ID/Nome)	O ID e o nome do VPC. O nome pode ser modificado.
IPv4 CIDR Block (Bloco CIDR IPv4)	O bloco CIDR IPv4 do VPC. Ele não pode ser modificado.
IPv6 CIDR Block (Bloco CIDR IPv6)	O bloco CIDR IPv6 do VPC. Atualmente, essa funcionalidade está em beta. Para usá-la, envie um tíquete.
Subnet (Sub-rede)	O número das sub-redes no VPC. Clique no número para acessar a página Sub-rede.
Tabela de rotas	O número das tabelas de rotas no VPC. Clique no número para acessar a página Tabela de rotas.
NAT Gateway	O número dos NAT Gateways no VPC. Clique no número para acessar a página NAT Gateway.
VPN Gateway	O número dos VPN Gateways no VPC. Clique no número para acessar a página VPN Gateway.
CVM	O número dos CVMs no VPC. Clique no número para acessar a página do CVM. Clique no ícone do CVM para redirecionar para a página de aquisição do CVM.
Classiclink	O número das instâncias do CVM baseadas na rede clássica associadas a este VPC. Um CVM baseado na rede clássica só pode ser associado a um VPC.
Gateway do Direct Connect	O número dos gateways do Direct Connect no VPC. Clique no número para acessar a página Gateway do Direct Connect.
VPC padrão	Indica se o VPC é o VPC padrão da região. Só pode haver um VPC padrão em

	uma região. O VPC padrão é criado automaticamente quando você adquire recursos como o CVM. Ele funciona da mesma forma que os criados manualmente.
Hora de criação	A hora em que o VPC foi criado.
Operação	As operações compatíveis do VPC. Apenas um VPC sem nenhum recurso pode ser excluído. Você pode clicar em More (Mais) para editar o bloco CIDR IPv4 e o bloco CIDR IPv6, se aplicável.

3. Clique no ID do VPC para exibir os detalhes, incluindo as informações básicas, a associação do CCN e os recursos associados. Clique no número ao lado de um recurso para acessar a página de gerenciamento do recurso.
4. Retorne à lista do VPC e clique na caixa de pesquisa do canto superior direito para filtrar o VPC por diferentes atributos de recursos.
5. Clique no ícone de configuração no canto superior direito para personalizar as colunas de exibição.

Edição de blocos CIDR IPv4

Last updated：2024-01-24 17:48:51

Cada VPC pode ter um bloco CIDR principal, que não pode ser modificado após a criação da VPC. Quando os IPs no bloco CIDR principal não atendem às suas necessidades, é possível criar vários blocos CIDR secundários para adicionar intervalos de IP.
Você pode alocar a sub-rede com um intervalo de IP dos blocos CIDR principal ou secundário. Todas as sub-redes da mesma VPC são interconectadas por padrão, independentemente de pertencerem aos blocos CIDR principal ou secundário.

Limites de uso

As CVMs baseadas na rede clássica não podem se interconectar com os recursos de nuvem no bloco CIDR secundário.
Um Peering Connection não aceita blocos CIDR secundários.
O Cloud Connect Network, o gateway do VPN e o gateway do Direct Connect padrão aceitam os blocos CIDR secundários. Atenção aos seguintes limites para um gateway do Direct Connect:
Essa funcionalidade está indisponível nas regiões de nuvem financeira.
Até 10 blocos CIDR secundários podem ser propagados.
Essa funcionalidade está indisponível para um NAT Gateway e gateway do Direct Connect.

Criação de blocos CIDR secundários

1. Faça login no Console da VPC.
2. Selecione a região da VPC na parte superior da página **VPC**.
3. Na lista de VPCs, localize a VPC e selecione **More (Mais)** > **Edit IPv4 CIDR block (Editar bloco CIDR IPv4)** na coluna **Operation (Operação)**.
4. Na caixa de diálogo pop-up, clique em **Add (Adicionar)** para inserir um bloco CIDR secundário.

Atenção:

Um bloco CIDR secundário pode se sobrepor ao intervalo de IP de destino de uma rota personalizada. Observe que o bloco CIDR secundário usa uma rota local, que tem uma prioridade mais alta do que as rotas de sub-rede personalizadas.

5. Clique em **OK**.

Exclusão de blocos CIDR secundários

1. Faça login no Console da VPC.
2. Selecione a região da VPC na parte superior da página **VPC**.
3. Na lista de VPCs, localize a VPC do qual os blocos CIDR secundários serão excluídos e selecione **More (Mais)** > **Edit IPv4 CIDR block (Editar o bloco CIDR IPv4)** na coluna **Operation (Operação)**.
4. Na caixa de diálogo pop-up, clique em **Delete (Excluir)** ao lado do bloco CIDR secundário.
5. Clique em **OK**.

Associação ou desassociação do CCN

Last updated：2024-01-24 17:48:51

O Cloud Connect Network (CCN) faz a ponte dos VPCs do Tencent Cloud e entre VPCs e IDCs locais. Ele fornece interconexão de rede privada multiponto. Para usar essa funcionalidade do CCN, primeiro é necessário adicionar VPCs a um CCN. Este documento descreve como associar um VPC ou desassociá-lo de um CCN.

Associação ao CCN

1. Faça login no Console do VPC.
2. Selecione a região do VPC na parte superior da página **VPC**.
3. Clique no ID do VPC para acessar a página **Basic Information (Informações básicas)**.
4. Clique em **Associate Now (Associar agora)** em **Associate with CCN (Associar ao CCN)** para abrir a caixa de diálogo.
5. Configure os parâmetros da seguinte forma.
Account (Conta): a conta do proprietário da instância do CCN. A instância do VPC e do CCN pode estar na mesma conta ou em contas diferentes. Se você escolher **Other accounts (Outras contas)**, insira o **Account ID (ID da conta)**. O proprietário da conta precisa aceitar o aplicativo do CCN dentro de 7 dias, caso contrário, o aplicativo vai expirar. O proprietário do CCN assume a tarifa de interconexão de rede gerada pelas instâncias que se conectam ao CCN.
CCN ID (ID do CCN): selecione um ID do CCN na lista suspensa para **My Account (Minha conta)** ou insira um ID do CCN para **Other accounts (Outras contas)**.
6. Clique em **OK**. Em seguida, o status estará como **Connected (Conectado)** conforme mostrado abaixo.

Desassociação do CCN

1. Faça login no Console do VPC.
2. Selecione a região do VPC na parte superior da página **VPC**.
3. Localize o VPC para desassociar do CCN e clique no ID do VPC para acessar a página **Basic Information (Informações básicas)**.
4. Clique em **Disassociate (Desassociar)** na seção **Associate with CCN (Associar ao CCN)**.
5. Verifique e confirme os riscos da operação e clique em **Disassociate (Desassociar)**.

Operações relevantes

Modificação do DNS da VPC

Last updated：2024-01-24 17:48:51

As CVMs em uma VPC da Tencent Cloud são compatíveis com o DHCP. As opções configuráveis do DHCP incluem o endereço DNS e o nome de domínio. Este documento descreve como modificar o endereço DNS e o nome de domínio de uma VPC.

Nota:

O protocolo DHCP (Dynamic Host Configuration Protocol) é um protocolo de rede local que define o padrão da transferência de informações de configuração para servidores de rede TCP/IP.

Por enquanto, as VPCs criadas antes de 1º de abril de 2018 não são compatíveis com as funcionalidades do DHCP. Se você não conseguir modificar o endereço DNS e o nome de domínio no console, significa que seu VPC não é compatível com essas funcionalidades.

Observações

As novas configurações entrarão em vigor em todos as CVMs na VPC.

Para as CVMs recém-criadas, as configurações modificadas entram em vigor imediatamente.

Para as CVMs existentes, as configurações modificadas entram em vigor após as CVMs ou os serviços de rede serem reiniciados.

Instruções

1. Faça login no Console da VPC.
2. Selecione a região da VPC na parte superior da página **VPC**.
3. Clique no ID da VPC para acessar a página **Basic Information (Informações básicas)**.
4. Clique no ícone de edição para modificar o DNS e o nome de domínio, respectivamente.

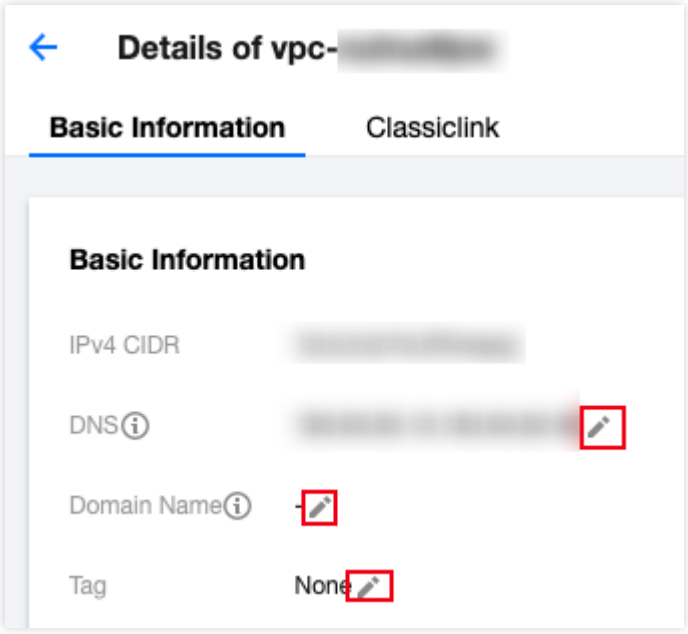
DNS: endereços do servidor DNS

Nota:

O DNS padrão da Tencent Cloud é “183.60.83.19” e “183.60.82.98”. Se o DNS padrão não for usado, os serviços internos como a ativação do Windows, o NTP e o YUM não estarão disponíveis.

O DNS aceita no máximo quatro endereços IP. Separe os IPs com vírgulas. Observe que alguns sistemas operacionais podem não aceitar quatro endereços DNS.

Nome de domínio: sufixo do nome do host da CVM, como “exemplo.com”. Você pode inserir até 60 caracteres ou manter a configuração padrão se não tiver requisitos especiais.



Modificação do nome e da tag da VPC

Last updated：2024-01-24 17:48:51

Este documento descreve como modificar o nome, a tag ou outras informações de uma VPC.

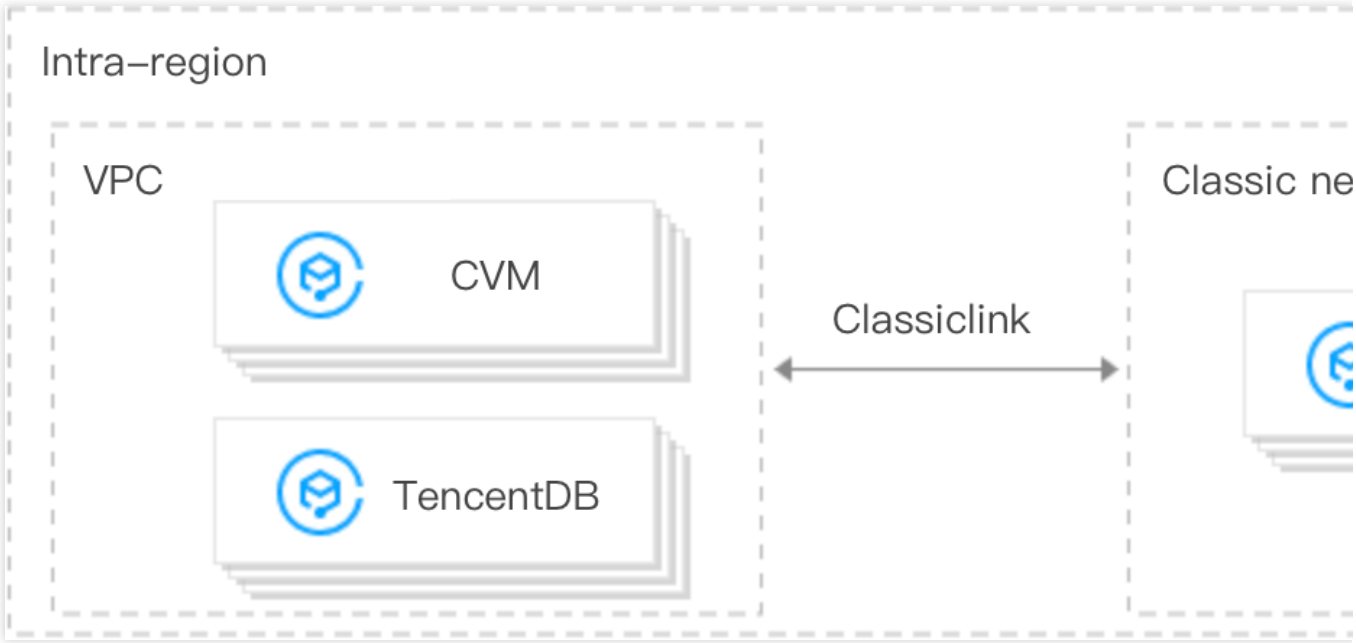
Instruções

1. Faça login no Console da VPC.
2. Selecione a região da VPC na parte superior da página **VPC**.
3. Clique no ícone de edição ao lado de um nome de VPC para modificá-lo.
4. Clique no ID da VPC para acessar a página **Basic Information (Informações básicas)**.
5. As tags são usadas para identificar e gerenciar os recursos. Você pode clicar no ícone de edição para adicionar ou excluir as tags.

Classiclink
Visão geral

Last updated：2024-01-24 17:48:51

A funcionalidade Classiclink permite que os recursos baseados na VPC se comuniquem com as CVMs baseadas na rede clássica. Por exemplo:
As CVMs baseadas na rede clássica podem se comunicar com os recursos da VPC, como a CVM, o TencentDB, o CLB da rede privada, o Redis/CMEM etc.
Os recursos da VPC só podem acessar as CVMs baseadas na rede clássica, mas não outros recursos na rede clássica, como o TencentDB e o CLB.



Limites de uso

Uma VPC só pode ser interconectada com a rede clássica **na mesma região**.
O intervalo de IP da VPC deve estar dentro de `10.0.0.0/16-10.47.0.0/16` (incluindo os subconjuntos); caso contrário, pode haver conflitos de IP que podem causar falha durante a associação e comunicação com as CVMs baseadas na rede clássica.
Uma CVM baseada na rede clássica só pode ser associado a uma VPC por vez.
Uma VPC aceita a associação com até 100 CVMs baseadas na rede clássica.
Depois que as CVMs baseadas na rede clássica são associadas a uma VPC, elas só conseguem se comunicar com os recursos no bloco CIDR principal, e não com os do bloco CIDR secundário da VPC.

As instâncias do CLB em uma VPC não podem ser vinculadas a da CVM baseado na rede clássica que se interconecta com o mesmo VPC.
Em situações com o Classiclink, o tráfego da CVM só pode ser roteado para endereços IP privados dentro da VPC, mas não para destinos fora da VPC.
Nota:
O CVM baseado na rede clássica não consegue acessar os recursos de rede pública ou privada fora da VPC atual por meio de dispositivos de rede, como o gateway do VPN, o gateway do Direct Connect, o gateway público, o Peering Connection e o NAT Gateway. Da mesma forma, o par de um gateway do VPN, do gateway do Direct Connect e do Peering Connection não consegue acessar as CVMs baseadas na rede clássica.

Observações

Alterar o IP privado de da CVM baseado na rede clássica invalidará sua associação com a VPC, e fará com que as configurações se tornem inválidas. Para associá-los, é necessário adicionar um Classiclink novamente no console da VPC.
O Classiclink não será afetado por ações tomadas em relação ao CVM, como o isolamento devido a pagamentos em atraso, o isolamento de segurança, a migração a frio, o failover, a modificação de configuração e a troca de sistema operacional.
O CVM será desassociado automaticamente da VPC se a CVM for retornado.

Referência

Para mais informações sobre o Classiclink, consulte Gerenciamento do Classiclink.

Gerenciamento do Classiclink

Last updated：2024-01-24 17:48:51

Criação de um Classiclink

Um Classiclink associa CVMs baseadas na rede clássica a uma VPC para permitir a interconexão entre a VPC e a rede clássica. Isso permite que as CVMs baseadas na rede clássica se comuniquem com os recursos da VPC.

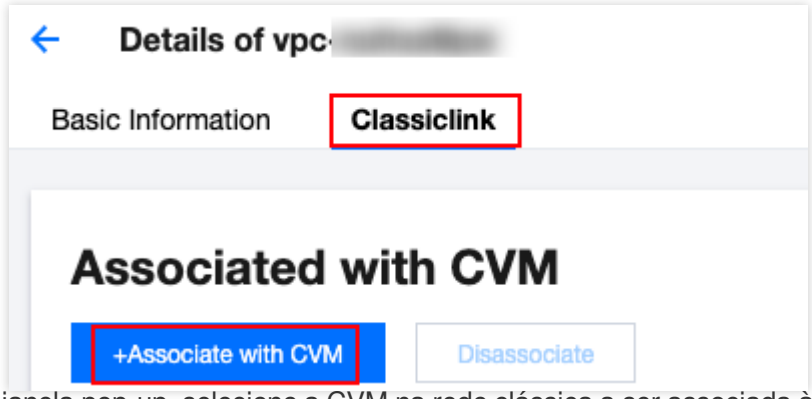
Nota:

Os IPs privados das CVMs baseadas na rede clássica associados serão adicionados automaticamente à política local da tabela de rotas da VPC. Isso permite a interconexão, sem a necessidade de modificar manualmente a política de roteamento da VPC.

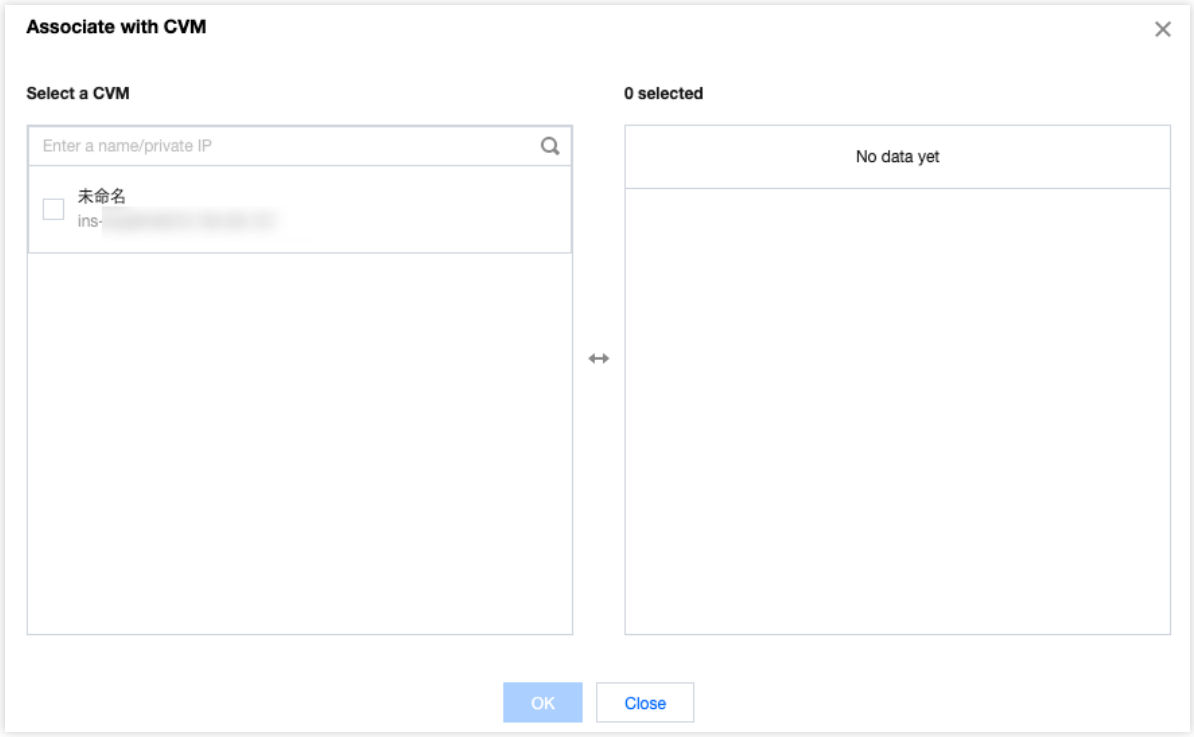
Depois que a CVM baseada na rede clássica for associada a uma VPC, suas configurações de firewall e ACL de rede permanecerão efetivas.

Instruções

1. Faça login no Console da VPC.
2. Selecione a região, e clique no ID da VPC que precisa do Classiclink, para acessar a página de detalhes.
3. Clique na guia **Classiclink** e em **+Associate with CVM (+Associar à CVM)**.



4. Na janela pop-up, selecione a CVM na rede clássica a ser associada à VPC e clique em **OK**.

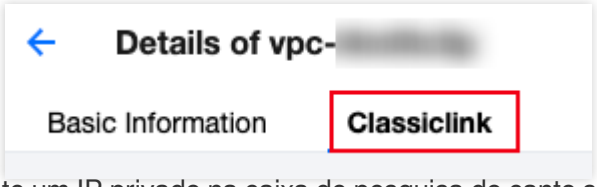


Exibição do Classiclink

É possível exibir a lista de CVMs baseadas na rede clássica que se interconectam com a VPC.

Instruções

1. Faça login no Console da VPC.
2. Selecione a região, e clique no ID da VPC que precisa do Classiclink, para acessar a página de detalhes.
3. Clique na guia **Classiclink** para exibir a lista de CVMs baseadas na rede clássica associadas à VPC.



4. Digite um IP privado na caixa de pesquisa do canto superior direito para localizar a CVM de forma rápida.

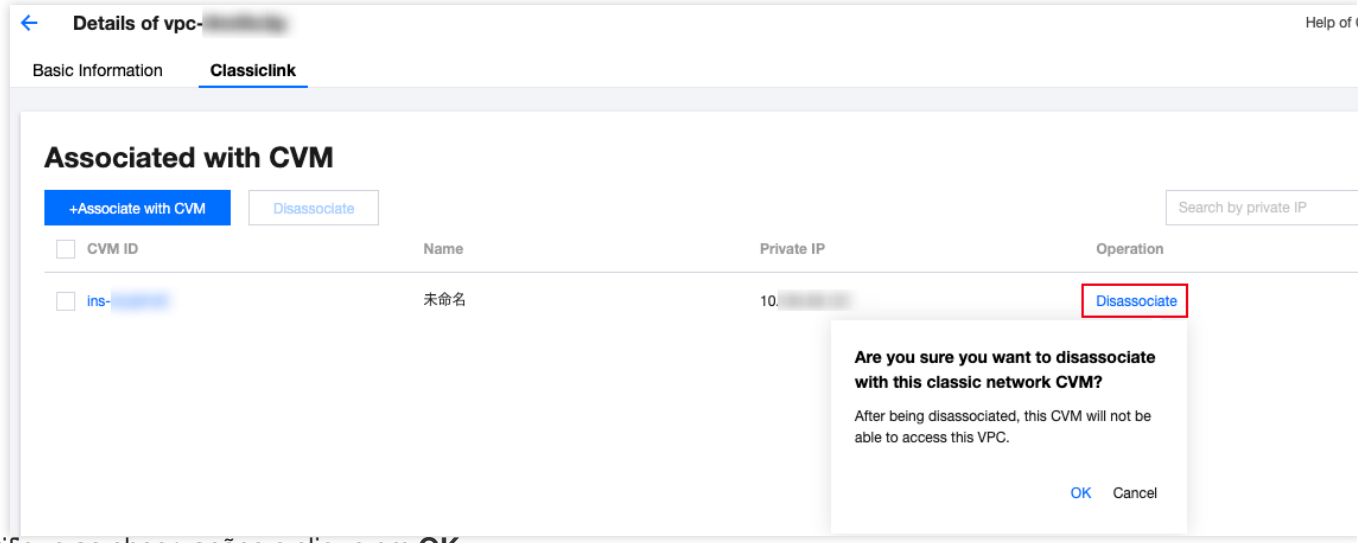
Exclusão de um Classiclink

Essa ação desassocia as CVMs baseadas na rede clássica da VPC e encerra sua interconexão.

Instruções

1. Faça login no Console da VPC.

2. Clique no ID da VPC que precisa do Classiclink, para acessar a página de detalhes.
3. Clique na guia **Classiclink**, selecione a CVM a ser desassociada da lista de CVMs baseadas na rede clássica, e clique em **Disassociate (Desassociar)** na coluna **Operation (Operação)**.



4. Verifique as observações e clique em **OK**.
5. Para desassociar várias CVMs, selecione as CVMs a serem desassociadas e clique em **Disassociate (Desassociar)** acima da lista.

Ativação ou desativação do multicast

Last updated：2024-01-24 17:48:51

Este documento descreve como ativar ou desativar o multicast para os VPCs.

Informações gerais

O broadcast e o multicast são modos de comunicação um para muitos, que podem economizar a largura de banda da rede dos negócios e reduzir a carga da rede por meio da transmissão eficiente de dados ponto a multiponto.
No modo unicast, o servidor inicial envia dados para N servidores separadamente. No modo multicast, o servidor envia os mesmos dados para N servidores de uma vez, o que reduz o consumo de recursos do servidor e também o recurso de largura de banda do backbone da rede.
Nota:
Atualmente, as funcionalidades de broadcast e multicast estão em teste beta. Se você precisar usá-las, envie uma solicitação.
No momento, as regiões que aceitam multicast e broadcast são: Pequim, Xangai, Guangzhou, Chengdu, Chongqing, Nanjing, Hong Kong da China, Singapura, Seul, Tóquio, Bangkok, Toronto, Vale do Silício, Virgínia, Frankfurt e Moscou.
Multicast: a Tencent Cloud aceita o multicast no âmbito da VPC.
Broadcast: a Tencent Cloud aceita o broadcast no âmbito da sub-rede.

Visão geral

O multicast e o broadcast são usados principalmente nos setores financeiro e de jogos:
Serviços de broadcast ou dados de mercado do setor financeiro. Por exemplo, depois de obter os preços das ações e outros dados em tempo real, os corretores podem transmitir dados de ações para vários clientes em tempo real, reduzindo muito a carga da rede.
Para o setor de jogos, o broadcast e o multicast são usados principalmente para manter a conexão entre vários servidores.

Instruções

Ativação do multicast

1. Faça login no Console da VPC.

2. Na lista de VPCs, localize a VPC desejada e ative o **Multicast**.

Desativação do multicast

1. Faça login no Console da VPC.
2. Na lista de VPCs, localize a VPC desejada e desative o **Multicast**.

Referências

Para mais informações sobre o broadcast no nível de sub-redes, consulte Ativação ou desativação do broadcast.

Exclusão de VPCs

Last updated：2024-01-24 17:48:51

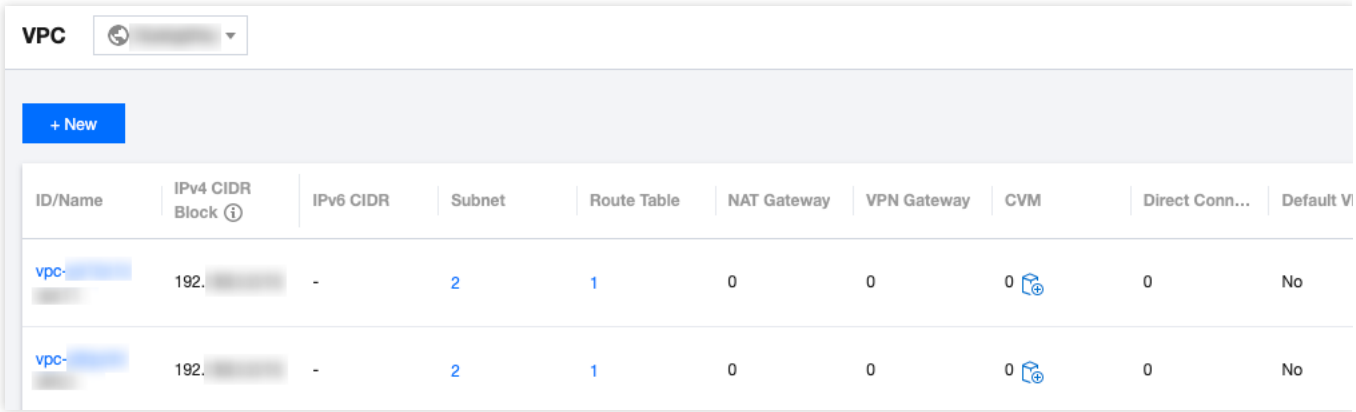
Quando uma VPC não está mais em uso e não tem outros recursos (Peering Connections, ClassicLink, NAT Gateway, gateway do VPN, gateway do Direct Connect, CCN e conexão privada), exceto sub-redes vazias, tabelas de roteamento e ACLs de rede, ela pode ser excluída.

Nota:

Uma sub-rede vazia se refere a uma sub-rede que não usa nenhum IP; ou seja, quando há apenas sub-redes vazias, tabelas de roteamento e ACLs de rede em uma VPC, a VPC pode ser excluída; quando há uso de IP em uma sub-rede, a VPC não pode ser excluída.

Instruções

1. Faça login no Console da VPC.
2. Selecione a região da VPC na parte superior da página **VPC**.
3. Na lista de VPCs, localize a VPC a ser excluída, clique em **Delete (Excluir)** na coluna **Operation (Operação)** e confirme a exclusão.



Sub-redes

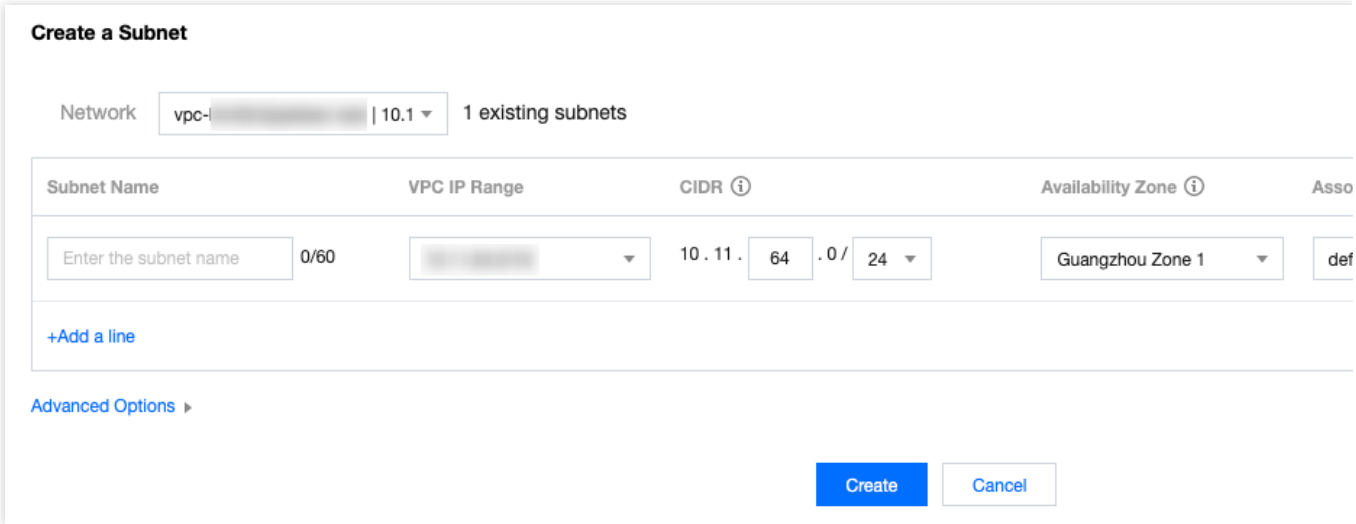
Criação de sub-redes

Last updated：2024-01-24 17:48:51

Uma sub-rede é um espaço de rede em um VPC, que carrega todas as implantações de recursos em nuvem. Um VPC possui pelo menos uma sub-rede. Uma sub-rede será criada junto com o VPC. Também é possível criar mais sub-redes em um VPC de acordo com suas necessidades empresariais.
Uma sub-rede é específica de uma zona de disponibilidade. Um VPC permite sub-redes em diferentes zonas de disponibilidade, e, por padrão, essas sub-redes podem se comunicar umas com as outras por meio de uma rede privada. Este documento lhe orientará sobre como criar uma sub-rede em um VPC.

Instruções

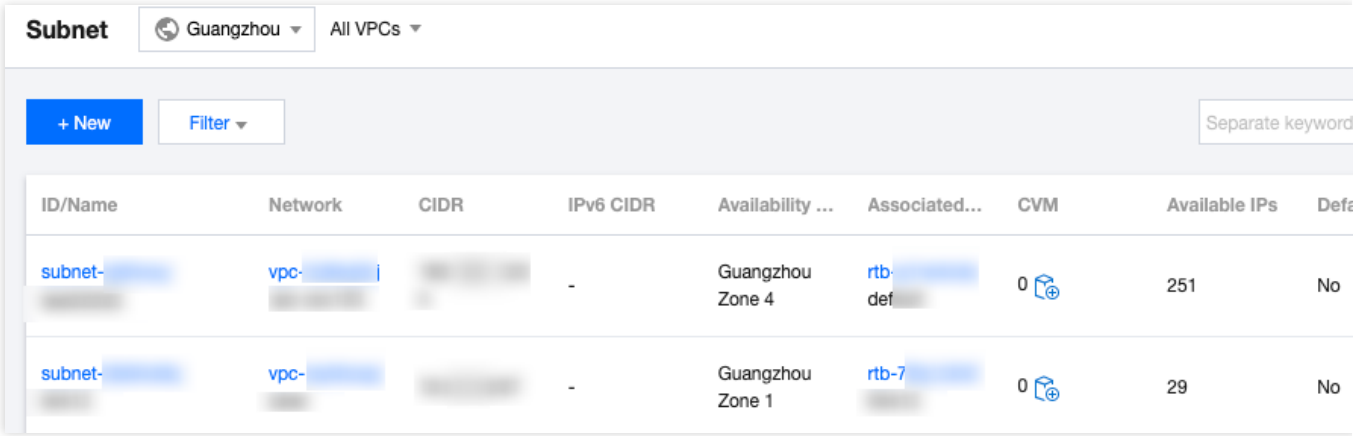
1. Faça login no Console do VPC.
2. Clique em **Subnet (Sub-rede)** na barra lateral esquerda para acessar a página de gerenciamento.
3. Selecione a região e o VPC em que a sub-rede será criada e clique em **+New (+Novo)**.
4. Configure os parâmetros da sub-rede na caixa de diálogo pop-up.



Network (Rede): o VPC onde a sub-rede está localizada. O VPC selecionado na Etapa 3 será exibido automaticamente. Como alternativa, você pode selecionar um VPC na lista suspensa.
Subnet Name (Nome da sub-rede): insira um nome de sub-rede personalizado com 60 caracteres.
VPC IP Range (Intervalo de IP do VPC): o bloco CIDR do VPC selecionado será exibido automaticamente.
CIDR: defina o bloco CIDR da sub-rede, que deve fazer parte do bloco CIDR do VPC e não pode se sobrepor ao bloco CIDR de outras sub-redes existentes no VPC.
Nota:

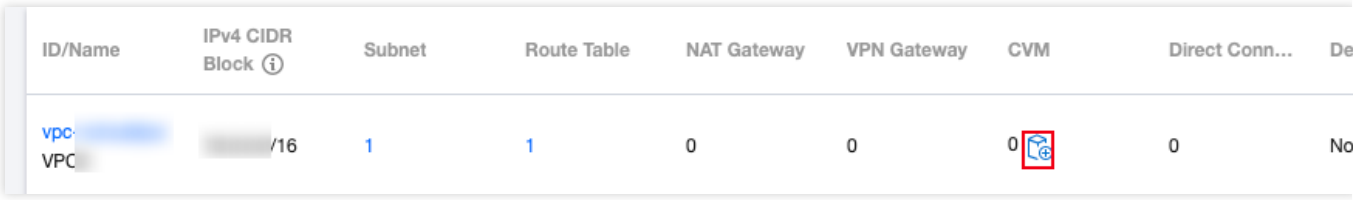
Planeje intervalos de IP de sub-rede adequados à escala da sua empresa. Um endereço IP privado dentro da sub-rede especificada será atribuído automaticamente à instância do CVM que você está criando. O IP privado principal de um CVM pode ser modificado.
Availability Zone (Zona de disponibilidade): selecione uma zona de disponibilidade na qual a sub-rede está localizada.
Associated route table (Tabela de rotas associada): selecione uma tabela de rotas a ser associada. A sub-rede deve ser associada a uma tabela de rotas para controlar o tráfego de saída. Por padrão, a tabela de rotas padrão do VPC será associada para garantir a interconexão da rede privada no VPC. Você também pode selecionar outra tabela de rotas no VPC.
Add a line (Adicionar uma linha): clique em **Add a line (Adicionar uma linha)** para criar várias sub-redes de uma vez. Clique em

para excluir as configurações de sub-rede selecionadas.
Advanced Options (Opções avançadas): você pode opcionalmente definir tags para a sub-rede para gerenciar melhor os recursos da sub-rede. Clique em **Add (Adicionar)** para definir várias tags de uma vez. Você pode clicar no ícone na coluna **Operation (Operação)** para excluir as configurações de tag selecionadas.
5. Ao concluir a configuração, clique em **Create (Criar)**. Em seguida, as sub-redes criadas serão exibidas na lista, conforme mostrado abaixo.



Operação posterior

Após criar uma sub-rede, você pode implantar recursos, incluindo o CVM e o CLB nela.
Clique no ícone conforme mostrado abaixo para adquirir diretamente um CVM na página de aquisição do CVM. Para obter mais informações, consulte Criação de um VPC IPv4.



ID/Name	IPv4 CIDR Block	Subnet	Route Table	NAT Gateway	VPN Gateway	CVM	Direct Conn...	De
vpc- VPC	/16	1	1	0	0	0	0	No

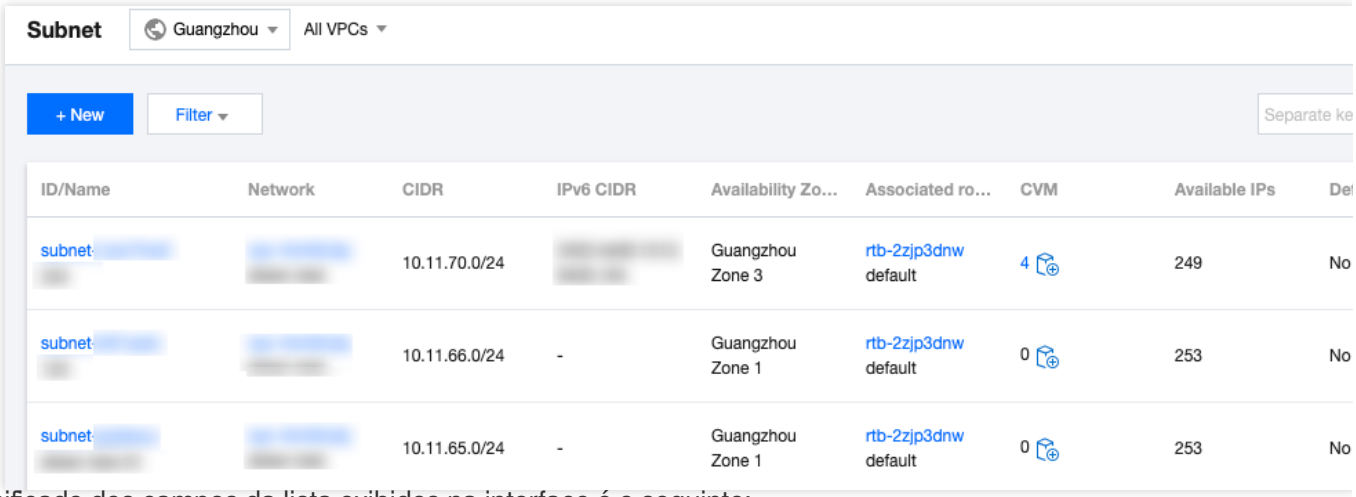
Exibição de uma sub-rede

Last updated：2024-01-24 17:48:51

É possível exibir os recursos de todas as sub-redes no VPC no console do VPC, por exemplo, os recursos de nuvem implantados na sub-rede, a tabela de rotas associada à sub-rede e as regras de ACL vinculadas à sub-rede.

Instruções

1. Faça login no Console do VPC.
2. Selecione **Subnet (Sub-rede)** na barra lateral esquerda para acessar a página de gerenciamento de sub-rede.
3. Na parte superior da página **Subnet (Sub-rede)**, selecione a região e o VPC aos quais a sub-rede pertence. Se você mantiver o valor padrão, ou seja, **All VPCs (Todos os VPCs)**, poderá exibir todas as sub-redes de todos os VPCs nesta região, conforme mostrado abaixo:



O significado dos campos da lista exibidos na interface é o seguinte:

ID/Name (ID/Nome): exibe o ID e o nome da sub-rede. Todas as sub-redes recebem um ID quando são criadas e o nome delas pode ser modificado em tempo real.

Network (Rede): o VPC ao qual a sub-rede pertence.

CIDR: o intervalo de IP do bloco CIDR da sub-rede. O bloco CIDR da sub-rede não pode ser modificado.

Availability Zone (Zona de disponibilidade): exibe a zona de disponibilidade na qual a sub-rede está localizada.

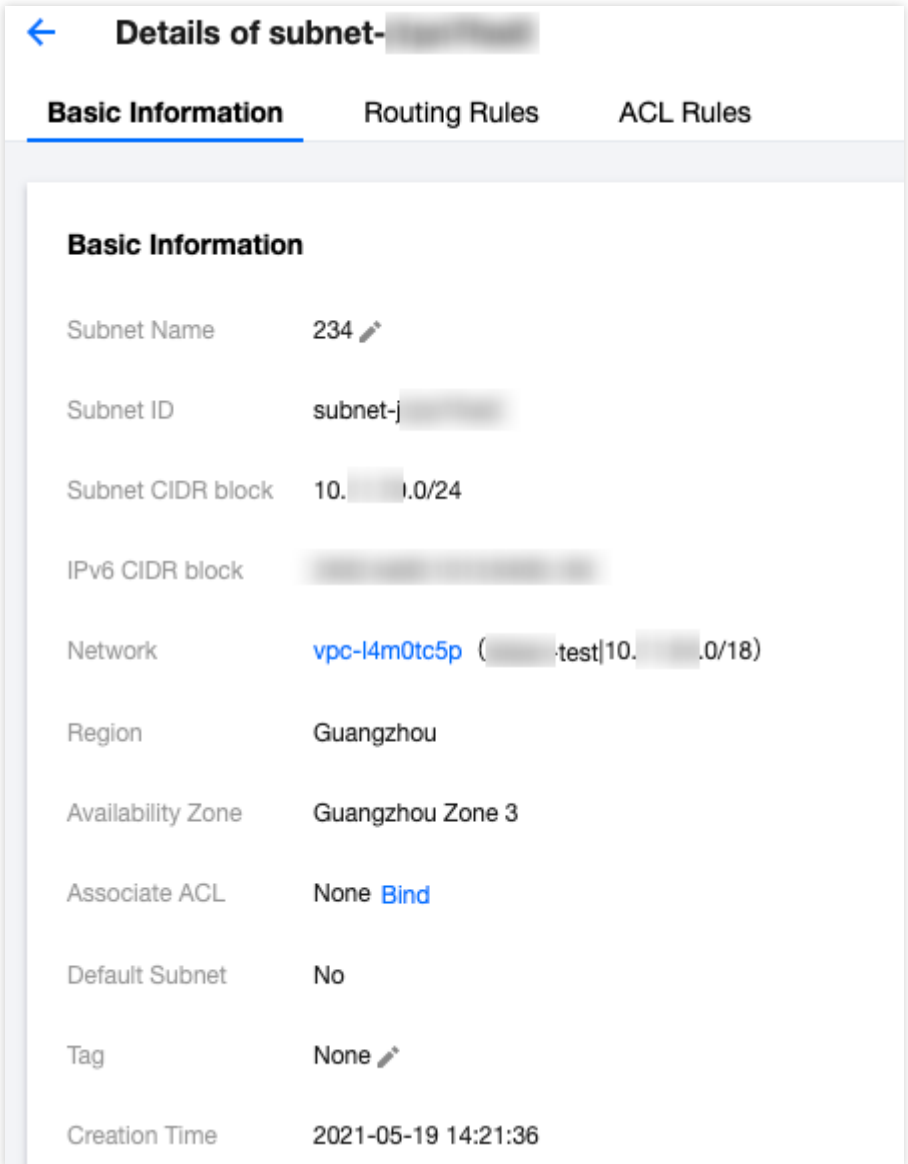
Associated Route Table (Tabela de rotas associada): a tabela de rotas associada à sub-rede.

CVM: exibe os números dos CVMs implantados na sub-rede.

Available IPs (IPs disponíveis): o número dos endereços IP disponíveis no intervalo de blocos CIDR da sub-rede.

Default Subnet (Sub-rede padrão): para as sub-redes criadas pelo usuário na página **Subnet (Sub-rede)** no console VPC, que não são as sub-redes padrão, o campo de valor exibirá **No (Não)**. Se você selecionar o VPC e a sub-rede

padrão criados automaticamente pelo Tencent Cloud na página de aquisição do CVM, aqui será exibido **Yes (Sim)**. Só pode haver um único VPC e sub-rede padrão em uma determinada região.
Creation Time (Hora de criação): a hora de criação da sub-rede.
Operation (Operação): as operações executáveis para a sub-rede. Você pode excluir a sub-rede sem recursos ou clicar em **More (Mais)** > **Change Route Table (Alterar a tabela de rotas)** para substituir a tabela de rotas associada à sub-rede.
4. Clique no ID da sub-rede para exibir os detalhes dos recursos da sub-rede. Alterne a guia para exibir as regras de roteamento e as regras de ACL.



5. Clique no ID do VPC da rede à qual a sub-rede pertence ou no ID da tabela de rotas associada, para exibir as informações detalhadas do recurso correspondente.
6. Clique no número dos CVMs para acessar a página da instância do CVM. Se a quantidade for 0, clique no ícone do CVM para acessar a página de aquisição do CVM.
7. Na parte superior da página, clique em **Filter (Filtrar)** para exibir a lista de sub-redes na zona disponível especificada.

8. Clique na caixa de pesquisa no canto superior direito da página para consultar rapidamente por **subnet ID (ID da sub-rede)**, **Subnet Name (Nome da sub-rede)**, **Tag** e **IPv4 CIDR Block (Bloco CIDR IPv4)**.
9. Clique no ícone de Configuração no canto superior direito para personalizar os campos exibidos.

Alteração da tabela de rotas da sub-rede

Last updated：2024-01-24 17:48:51

Cada sub-rede deve ser associada a uma tabela de rotas, que é usada para controlar a direção do tráfego de saída da sub-rede. Você pode alterar a tabela de rotas associada da sub-rede na página **VPC -> Subnet (Sub-rede)** de acordo com as necessidades de roteamento da sub-rede. Se você precisar criar uma tabela de rotas, consulte Criação de uma tabela de rotas personalizada.

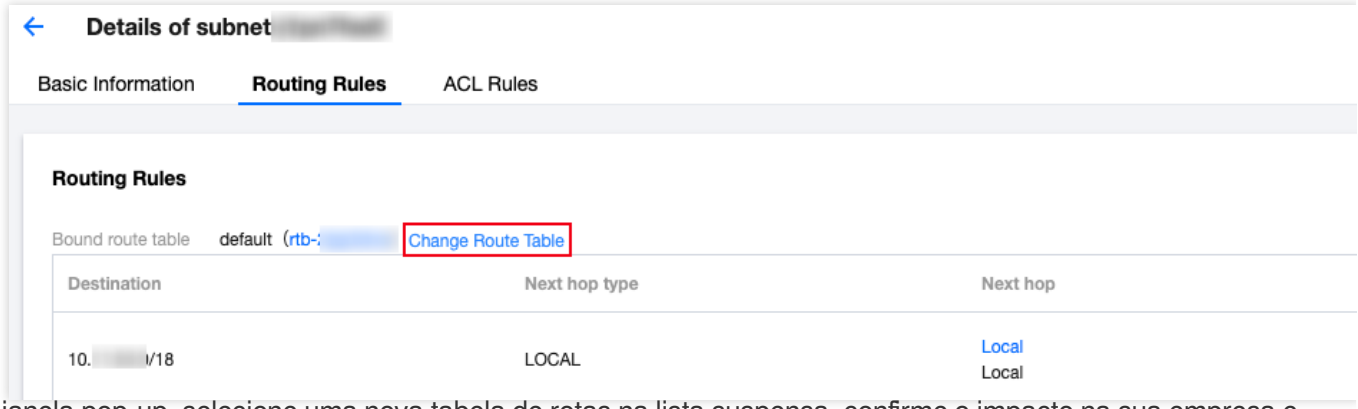
Impacto nos sistemas

Considerando que a tabela de rotas impacta diretamente o fluxo de tráfego na sub-rede, quaisquer alterações como a associação da tabela de rotas ou as entradas de rotas devem ser cuidadosamente consideradas de acordo com as necessidades empresariais dos fluxos de rede.

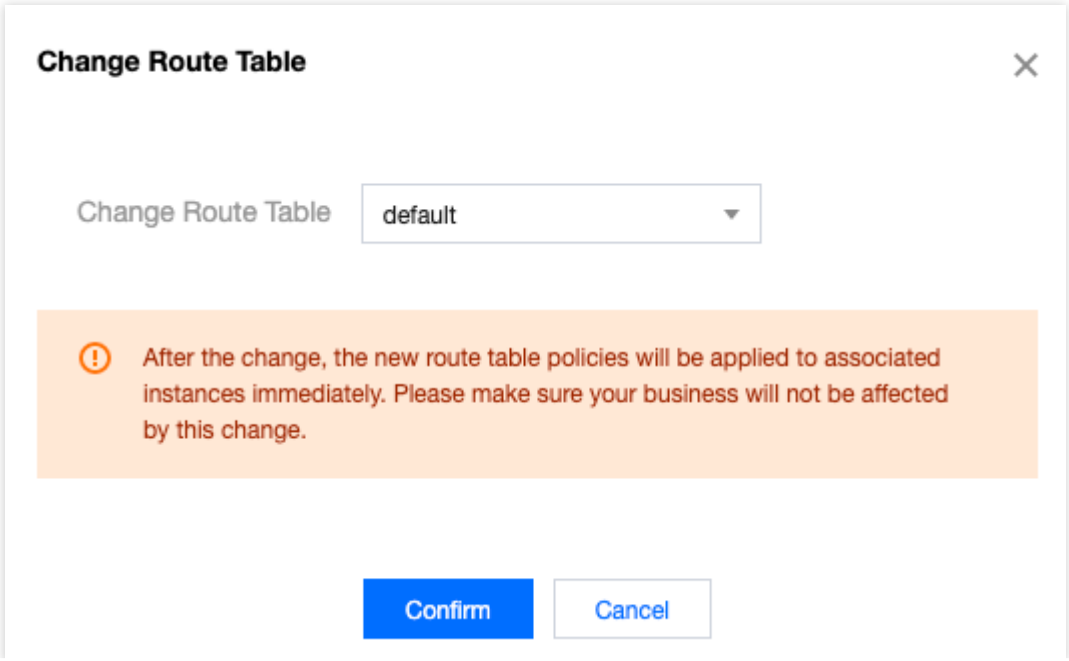
Instruções

1. Faça login no Console do VPC.
2. Selecione **Subnet (Sub-rede)** na barra lateral esquerda para acessar a página de gerenciamento de sub-rede.
3. O sistema fornece dois métodos para alterar a tabela de rotas associada à sub-rede.
Clique em **More (Mais)** > **Change Route Table (Alterar tabela de rotas)** na coluna **Operation (Operação)** no lado direito da sub-rede que precisa alterar a tabela de rotas.

Clique no ID da sub-rede que precisa alterar a tabela de rotas para acessar a página de detalhes, mude para a guia **Routing Rules (Regras de roteamento)** e clique em **Change Route Table (Alterar a tabela de rotas)**.



4. Na janela pop-up, selecione uma nova tabela de rotas na lista suspensa, confirme o impacto na sua empresa e clique em **Confirm (Confirmar)**.



Gerenciamento de regras de ACL

Last updated：2024-01-24 17:48:51

A Regra de ACL é uma camada de segurança opcional que opera no nível das sub-redes. Ela é usada para controlar os fluxos de dados de entrada e saída das sub-redes, que podem ser conforme o protocolo e a granularidade da porta, para obter um controle preciso do tráfego das sub-redes. É possível associar a mesma ACL de rede a sub-redes que requerem o mesmo nível de controle de tráfego de rede.
Esta seção descreve como vincular, desvincular e alterar as regras de ACL por meio do console do VPC.

Instruções

1. Faça login no Console do VPC.
2. Selecione **Subnet (Sub-rede)** na barra lateral esquerda para acessar a página de gerenciamento de sub-rede.
3. Clique em um ID de sub-rede para acessar a sua página de detalhes. É possível realizar a vinculação, a desvinculação ou a alteração da ACL nas seguintes páginas.
No campo **Associate ACL (Associar ACL)** na guia **Basic Information (Informações básicas)**
Na guia **ACL Rules (Regras de ACL)**
4. Execute as seguintes operações com base nas necessidades empresariais. As capturas de tela a seguir consideram as operações em **ACL Rules (Regras de ACL)** como exemplo.
Se a sub-rede atual não estiver vinculada à regra de ACL, você pode clicar em **Bind (Vincular)** para selecionar uma regra de ACL apropriada e clicar em **OK** para concluir a vinculação. A vinculação entrará em vigor imediatamente. No momento, apenas o tráfego de entrada e saída da sub-rede a qual a regra é **Allow (Permitir)** pode avançar.
Se a regra de ACL vinculada à sub-rede atual não atender aos requisitos de fluxo de rede, clique em **Change (Alterar)** para alterar a regra de ACL, que entrará em vigor imediatamente.
Se a sub-rede atual estiver vinculada a uma regra de ACL, mas você não precisar mais controlar o tráfego de entrada e saída da sub-rede, clique em **Unbind (Desvincular)** para desvincular a regra de ACL. A desvinculação será feita de imediato e isso causará o levantamento da restrição da regra de ACL no tráfego de entrada e saída da sub-rede.

Ativação ou desativação do broadcast

Last updated：2024-01-24 17:48:51

Informações gerais

O multicast e o broadcast são modos de comunicação um para muitos, que podem ajudar as empresas a reduzir o consumo de largura de banda da rede e a carga da rede por meio da transmissão eficiente de dados ponto a multiponto.
No modo unicast, o servidor inicial envia dados para N servidores separadamente. No modo multicast, o servidor envia os mesmos dados para N servidores de uma vez, o que reduz o consumo de recursos do servidor e também o recurso de largura de banda do backbone da rede.
Multicast: a Tencent Cloud aceita o multicast no âmbito da VPC.
Broadcast: a Tencent Cloud aceita o broadcast no âmbito da sub-rede.
Nota:
Atualmente, as funcionalidades de broadcast e multicast estão em teste beta. Se você precisar usá-las, envie uma solicitação.
No momento, as regiões que aceitam multicast e broadcast são: Pequim, Xangai, Guangzhou, Chengdu, Chongqing, Nanjing, Hong Kong da China, Singapura, Seul, Tóquio, Bangkok, Toronto, Vale do Silício, Virgínia, Frankfurt e Moscou.

Visão geral

O multicast e o broadcast são usados principalmente nos setores financeiro e de jogos:
Serviços de broadcast ou dados de mercado do setor financeiro. Por exemplo, depois de obter os preços das ações e outros dados em tempo real, os corretores podem transmitir dados de ações para vários clientes em tempo real, reduzindo muito a carga da rede.
Para o setor de jogos, o broadcast e o multicast são usados principalmente para manter a conexão entre vários servidores.
Este documento descreve como ativar ou desativar o broadcast para sub-redes.

Instruções

Ativação do broadcast

1. Faça login no Console da VPC.

2. Clique em **Subnet (Sub-rede)** na barra lateral esquerda, para acessar a página de admin.
3. Na lista de VPCs, localize a VPC em questão e alterne para **Enable (Ativar)** na coluna **Subnet broadcast (Broadcast da sub-rede)**.

Desativação do broadcast

1. Faça login no Console da VPC.
2. Clique em **Subnet (Sub-rede)** na barra lateral esquerda, para acessar a página de admin.
3. Na lista de VPCs, localize a VPC em questão e alterne para **Disable (Desativar)** na coluna **Subnet broadcast (Broadcast da sub-rede)**.

Referências

Para mais informações sobre o multicast no nível da VPC, consulte Ativação ou desativação do multicast.

Exclusão de uma sub-rede

Last updated：2024-01-24 17:48:51

Você pode excluir as sub-redes que não estão mais em uso e não usam nenhum recurso de IP.

Nota:

Atualmente, os recursos da Tencent Cloud que envolvem o uso de IP em sub-redes incluem a CVM, o CLB da rede privada, a ENI, o HAVIP, o SCF, o TKE e o TencentDB (para MySQL, Redis, TDSQL etc.).

Instruções

1. Faça login no Console da VPC.
2. Clique em **Subnet (Sub-rede)** na barra lateral esquerda para acessar a página de gerenciamento.
3. Na parte superior da lista, selecione a região e a VPC aos quais pertence a sub-rede a ser excluída.
4. Na lista, selecione a sub-rede a ser excluída, clique em **Delete (Excluir)** na coluna **Operation (Operação)** e clique em **OK**.

Tabelas de rotas
Visão geral

Last updated：2024-01-24 17:48:52

Uma tabela de rotas consiste em várias políticas de roteamento que controlam a direção do tráfego de saída das sub-redes na VPC. Cada sub-rede só pode ser associada a uma tabela de rotas, já cada tabela de rotas pode ser associada a várias sub-redes. Você pode criar várias tabelas de rotas para sub-redes com rotas de tráfego diferentes.

Tipos

Existem dois tipos de tabelas de rotas: padrão e personalizada.
Tabela de rotas padrão: ao criar uma VPC, o sistema gera automaticamente uma tabela de rotas padrão, que será associada às sub-redes criadas posteriormente se nenhuma tabela de rotas personalizada for selecionada. Você não pode excluir a tabela de rotas padrão, mas pode adicionar, excluir e modificar as políticas de roteamento nela.
Tabela de rotas personalizada: você pode criar ou excluir uma tabela de rotas personalizada na VPC. Essa tabela de rotas personalizada pode ser associada a todas as sub-redes para aplicar a mesma política de roteamento.
Nota:
Você pode associar uma tabela de rotas ao criar uma sub-rede ou alterar a tabela de rotas após a criação de uma sub-rede.

Política de roteamento

Uma tabela de rotas controla as rotas de tráfego usando políticas de roteamento. Uma política de roteamento consiste no destino, tipo do próximo salto e próximo salto.
Destination (Destino): especifica o intervalo de IP de destino para o qual você deseja encaminhar o tráfego. Deve ser um intervalo de IP. Se você quiser inserir um único endereço IP, defina a máscara para `32` (por exemplo, `172.16.1.1/32`). O destino não pode ser um intervalo de IP da VPC onde reside a tabela de rotas, pois a rota local já permite a interconexão de rede privada neste VPC.
Nota:
Se você implantou um serviço TKE na VPC, o destino configurado na política de roteamento da sub-rede da VPC não pode estar dentro do bloco CIDR da VPC nem conter o intervalo de IP do TKE.
Por exemplo, se o bloco CIDR da VPC for `172.168.0.0/16` e o bloco CIDR do TKE for `192.168.0.0/16`, o

intervalo de IP de destino não pode estar dentro de `172.168.0.0/16`, ou conter `192.168.0.0/16`, quando você configurar a política de roteamento para uma sub-rede da VPC.
Next-hop type (Tipo do próximo salto): indica a saída de pacotes de dados para a VPC. O tipo do próximo salto da VPC aceita **NAT Gateway**, **Peering Connection**, **VPN Gateway (Gateway do VPN)**, **Direct Connect Gateway (Gateway do Direct Connect)**, **CVM** e outros.
Next hop (Próximo salto): especifica a instância do próximo salto (identificada pelo ID do próximo salto) para a qual o tráfego é encaminhado, como um NAT Gateway em uma VPC.

Prioridade das políticas de roteamento

Quando há várias políticas de roteamento em uma tabela de rotas, a seguinte prioridade de roteamento se aplica, de alta para baixa:
Tráfego dentro da VPC: o tráfego dentro da VPC é correspondido primeiro.
Rota de correspondência exata (a correspondência de prefixo mais longa): quando há várias rotas na tabela de rotas que podem corresponder ao IP de destino, a rota com a máscara mais longa (exata) é correspondida para determinar o próximo salto.
IP público: se nenhuma política de roteamento for correspondida, uma instância da CVM pode acessar a Internet por meio de seu endereço IP público.
Caso de uso:
Quando uma sub-rede está associada a um NAT Gateway, e a CVM na sub-rede possui um IP público (ou EIP), a CVM acessa a Internet por meio do NAT Gateway por padrão (porque a prioridade da rota de correspondência exata é maior que a do IP público). No entanto, você pode definir uma política de roteamento para permitir que a CVM acesse a Internet usando seu endereço IP público. Para mais detalhes, consulte Ajuste das prioridades dos NAT Gateways e EIPs.

ECMP

O Roteamento de vários caminhos de custo igual (ECMP, na sigla em inglês) significa que existem várias rotas de igual custo para um único destino. A tecnologia de roteamento tradicional usa apenas um caminho para transferir pacotes para o mesmo destino, enquanto os demais caminhos estão no estado de espera ou inválido. Quando o caminho falha, leva tempo para usar outro caminho. Por outro lado, o ECMP usa várias rotas de custos iguais no ambiente de rede para aumentar a largura de banda de transmissão, equilibrar o tráfego em várias rotas e obter backup com links redundantes.
O VPC aceita o ECMP para o mesmo tipo de rota, conforme detalhado abaixo.

Tipo do próximo salto	Aceita o ECMP (mesmo tipo de rota)	Quantidade máxima de ECMPs
NAT Gateway	Não	N/A
IP público da CVM	Não	N/A

CVM	Sim	8
Peering Connection	Não	N/A
Gateway do Direct Connect	Sim	8
CCN	Não	N/A
HAVIP	Sim	8
Gateway do VPN	Sim	8

Nota:
O CCN aceita um ECMP com gateway do Direct Connect ou Peering Connection.

Casos de uso

O ECMP é frequentemente usado para equilibrar a carga de tráfego em gateways com largura de banda limitada. Suponha que você precise de 2.000 Mbps para interconectar seus negócios baseados na VPC e IDC, mas a largura de banda máxima atual do VPN é de 1.000 Mbps. Para atingir o objetivo, você pode criar dois gateways do VPN de 1.000 Mbps e dois túneis VPN.

Rotas principal/secundária

As rotas principal/secundária referem-se a dois ou mais caminhos para o mesmo destino, com um caminho ativo e caminhos em espera ou inválidos. Suponha que haja duas rotas da VPC para o IDC, ou seja, caminho A e caminho B. Todos os pacotes são enviados ao destino pelo caminho A, enquanto o caminho B fica inválido ou em espera. Quando o caminho A sofre falhas de ligação, você pode ativar o caminho B para assumir o tráfego do caminho A, garantindo assim a disponibilidade da aplicação. Nesse caso, os caminhos A e B são chamados de rotas principal e secundária.
O tipo do próximo salto determina a prioridade das rotas. Ao adicionar uma política de roteamento à tabela de rotas da VPC, você pode configurar diferentes tipos de gateways para atuar como rotas principal e secundária para um único destino. Depois, a investigação de rede da VPC pode ser usada para verificar a qualidade e a acessibilidade da ligação. Após configurar uma política de alarme, você pode detectar prontamente qualquer exceção de ligação e alternar com rapidez entre as rotas principal e secundária para atender aos requisitos de alta disponibilidade.
Nota:
Atualmente, a funcionalidade de prioridade de rotas está na versão beta. Para usá-la, envie um tíquete.
O tipo do próximo salto determina a prioridade da rota na tabela de rotas da VPC. Por padrão, a prioridade de rota de alta para baixa é CCN, gateway do Direct Connect, gateway do VPN e outros.
Atualmente, você não pode ajustar a prioridade das rotas no console. Se necessário, envie um tíquete.

A tabela a seguir descreve se as rotas principal/secundária são aceitas em diferentes tipos de rotas da VPC.

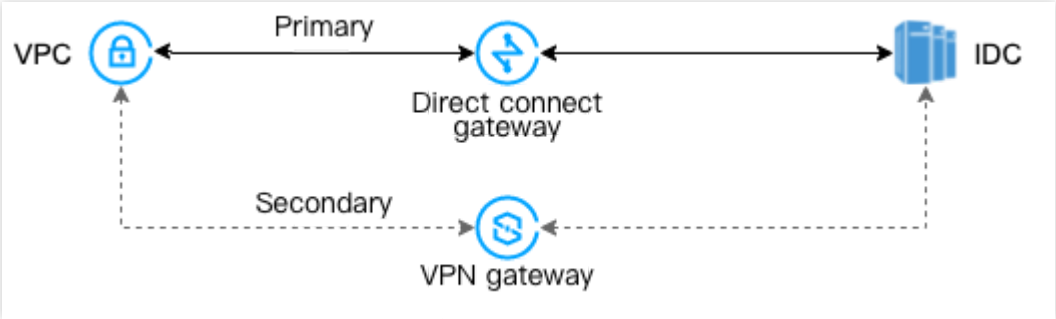
Tipo do próximo salto	Aceita rotas principal/secundária
NAT Gateway	Não
IP público da CVM	Não
CVM	Sim, com CCN, gateway do VPN, gateway do Direct Connect ou HAVIP
Peering Connection (intrarregião)	Não
Peering Connection (entre regiões)	Não
Gateway do Direct Connect	Sim, com CCN, gateway do VPN, HAVIP ou CVM
CCN	Sim, com gateway do VPN, gateway do Direct Connect, HAVIP ou CVM
HAVIP	Sim, com CCN, gateway do VPN, gateway do Direct Connect ou CVM
Gateway do VPN	Sim, com CCN, gateway do Direct Connect, HAVIP ou CVM

Casos de uso

As rotas principal/secundária são frequentemente usadas para encaminhar o tráfego continuamente quando uma ligação de gateway falha.

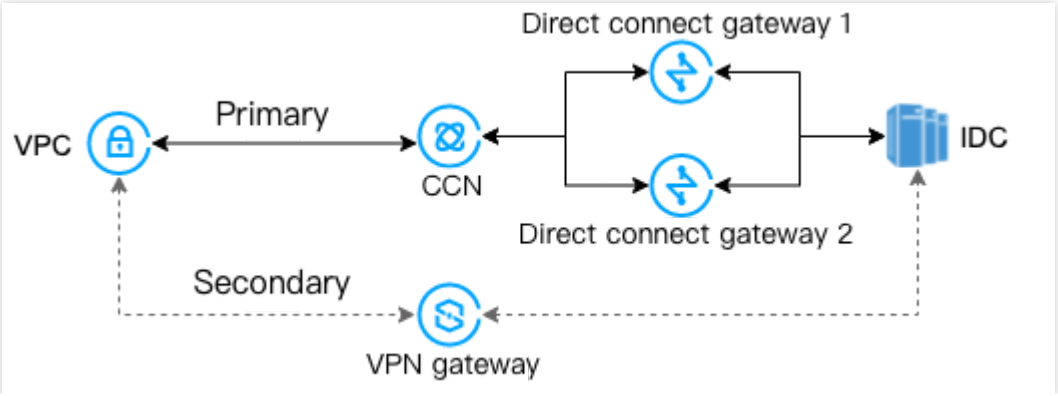
Gateway do Direct Connect baseado na VPC (principal) e gateway do VPN para a VPC (secundária)

Cenário: interconecte uma VPC da Tencent Cloud e um IDC local por meio de um gateway do Direct Connect baseado na VPC. Enquanto isso, crie túneis VPN por meio de um gateway do VPN para atuar como o vínculo de comunicação secundário entre o IDC e a VPC.



Gateway do Direct Connect baseado no CCN (principal) e gateway do VPN para a VPC (secundária)

Cenário: interconecte uma VPC da Tencent Cloud e um IDC local por meio de uma instância do CCN. Enquanto isso, crie túneis VPN por meio de um gateway do VPN para atuar como o vínculo de comunicação secundário entre o IDC e a VPC.



Observações

Last updated：2024-01-24 17:48:51

Não é possível excluir a tabela de rotas padrão de uma VPC.
Após criar uma VPC, sua tabela de rotas será fornecida automaticamente com uma rota padrão, indicando que todos os recursos nessa VPC estão interconectados por meio da rede privada. Não é possível modificar nem excluir essa política de roteamento.

Destino	Tipo do próximo salto	Próximo salto
Local	Local	Local

Os protocolos de roteamento dinâmico, como o BGP e o OSPF, não são aceitos.
As rotas podem ser publicadas no CCN. As seguintes rotas podem ser publicadas no CCN.

Tipo do próximo salto	Publicação no CCN por padrão	Publicar ou retirar manualmente	Descrição
Local	Compatível	Não compatível	Atribuído pelo sistema. O intervalo de IP da VPC conectada ao CCN será publicado automaticamente no CCN, incluindo os blocos CIDR principal e secundário (exceto para intervalos de IP do TKE).
CVM	Não compatível	Compatível	Uma rota personalizada para a CVM. Quando o intervalo de IP for todo 0 ou a política de roteamento estiver desativada, a rota não poderá ser publicada no CCN.
HAVIP	Não compatível	Compatível	Rota personalizada para o HAVIP. Quando o intervalo de IP for todo 0 ou a política de roteamento estiver desativada, as rotas não poderão ser publicadas no CCN.

Nota:
Uma rota personalizada desativada não pode ser publicada no CCN.
Primeiro, uma rota personalizada deve ser retirada antes de poder ser desativada, se tiver sido publicada em um CCN.

Limites de cota

Recurso	Limite
Quantidade de tabelas de rotas por VPC	10
Quantidade de tabelas de rotas associadas a cada sub-rede	1
Quantidade de políticas de roteamento por tabela de rotas	50

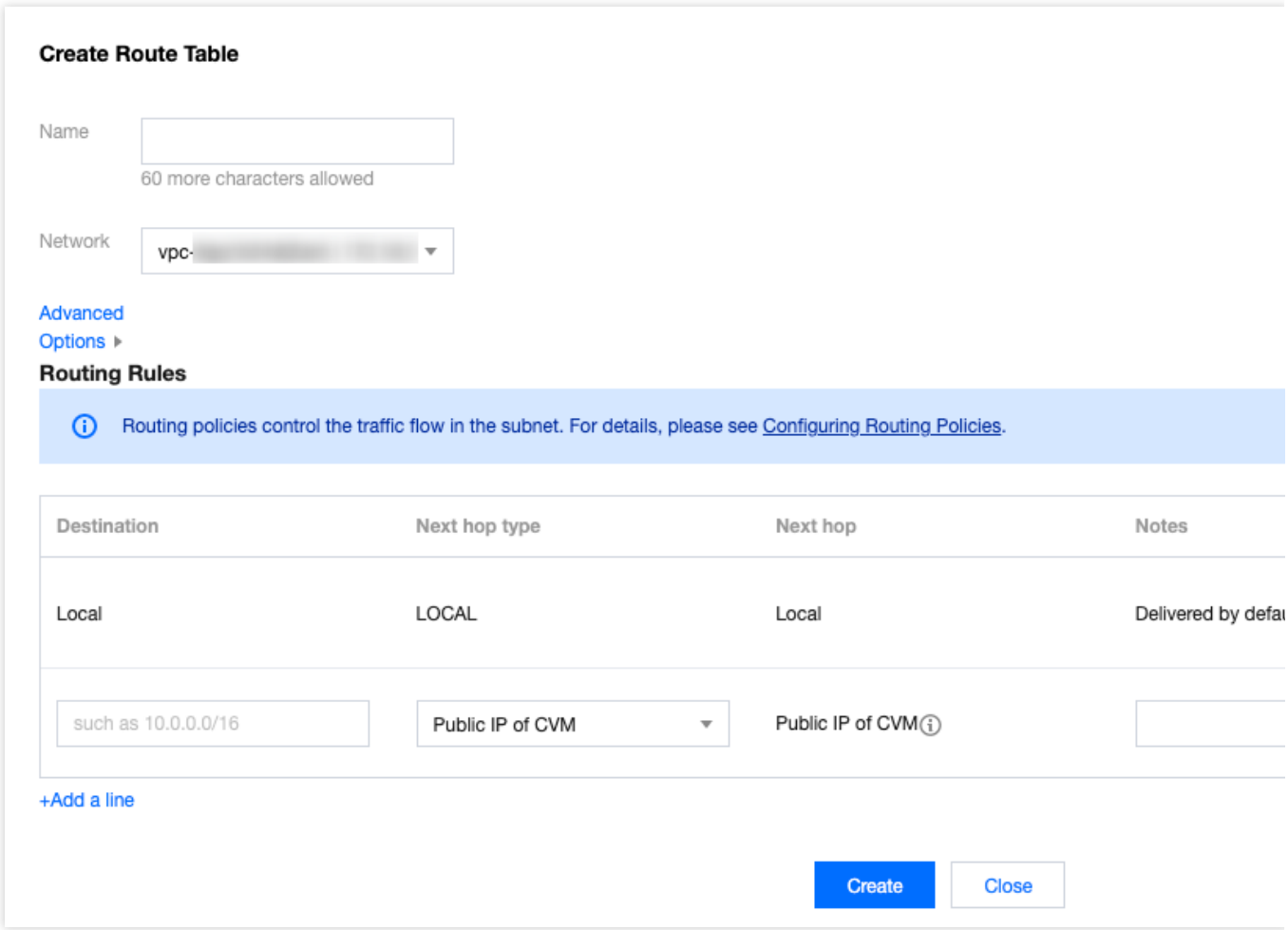
Criação de tabelas de rotas personalizadas

Last updated：2024-01-24 17:48:51

Uma tabela de rotas é usada para controlar o tráfego de saída da sub-rede. Ela pode conter várias políticas de roteamento. Existem tabelas de rotas padrão e personalizadas. A tabela de rotas padrão (rota local) permite a interconexão da rede privada no VPC, que não pode ser excluída, mas pode ser configurada com políticas de roteamento da mesma forma que você configura uma tabela de rotas personalizada. Este documento descreve como criar e configurar uma tabela de rotas personalizada.

Instruções

1. Faça login no Console do VPC.
2. Clique em **Route Tables (Tabelas de rotas)** na barra lateral esquerda para acessar a página de gerenciamento.
3. Clique em **+ New (+ Novo)**.
4. Na caixa de diálogo pop-up, insira o nome da tabela de rotas, selecione o VPC ao qual ela pertence e configure as políticas de roteamento.



Nota:

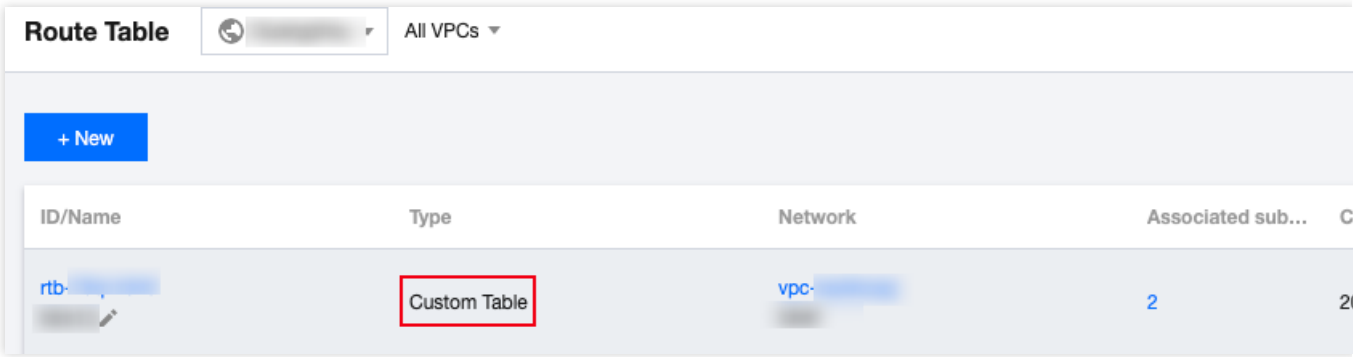
É possível configurar as políticas de roteamento ao criar uma tabela de rotas. Como alternativa, depois que uma tabela de rotas for criada, você poderá clicar na ID dela para acessar a página **Basic Information (Informações básicas)** e clicar em **+ New routing policies (+ Novas políticas de roteamento)**, para configurar as políticas de roteamento.

Configuração de uma política de roteamento :

Parâmetro	Descrição
Destino	O intervalo de IP de destino para o qual o tráfego será encaminhado. A configuração deve atender aos seguintes requisitos: Insira um intervalo de IP. Se você quiser inserir um único IP, defina a máscara para 32 (por exemplo, `172.16.1.1/32`). O destino não pode ser um intervalo de IP do VPC onde a tabela de rotas está localizada, porque a rota local já permite a interconexão de rede privada neste VPC. **Observação**: se você tiver implantado um serviço TKE no VPC, o destino que você configurar na política da tabela de rotas da sub-rede do VPC não poderá estar dentro do bloco CIDR do VPC ou conter o intervalo de IP do TKE. Por exemplo, se o bloco CIDR do VPC for `172.168.0.0/16` e o bloco CIDR do TKE for `192.168.0.0/16`, o intervalo de IP de

	destino não deve estar dentro de `172.168.0.0/16`, ou conter `192.168.0.0/16`, quando você configurar a política de roteamento para uma sub-rede do VPC.
Next hop type (Tipo de próximo salto)	A saída dos pacotes de dados do VPC. Os seguintes tipos são compatíveis: NAT Gateway: o tráfego direcionado para um intervalo de IP de destino é encaminhado para um NAT Gateway. Peering Connections: o tráfego direcionado para um intervalo de IP de destino é encaminhado para um VPC na outra extremidade de um Peering Connection. Gateway do Direct Connect: o tráfego direcionado para um intervalo de IP de destino é encaminhado para um gateway do Direct Connect. IP virtual de alta disponibilidade: o tráfego direcionado para um intervalo de IP de destino é encaminhado para um HAVIP. VPN Gateway: o tráfego direcionado para um intervalo de IP de destino é encaminhado para um VPN Gateway. IP público do CVM: o tráfego direcionado para um intervalo de IP de destino é encaminhado para o IP público (incluindo EIPs) de uma instância do CVM em um VPC. CVM: o tráfego direcionado para um intervalo de IP de destino é encaminhado para uma instância do CVM em um VPC.
Próximo salto	Especifica a instância do próximo salto para a qual o tráfego é redirecionado, como o gateway ou IP do CVM.
Observações	Descreve o propósito da rota para gerenciamento de recursos. Esse parâmetro é opcional.
Adicionar uma linha	Configura várias políticas de roteamento, se necessário. Você pode clicar no ícone de exclusão na coluna **Operation (Operação)** para excluir as políticas de roteamento desnecessárias. Uma tabela de rotas personalizada deve conter pelo menos uma política de roteamento.

5. Ao concluir a configuração, clique em **Create (Criar)**. Em seguida, a tabela de rotas será exibida na lista.

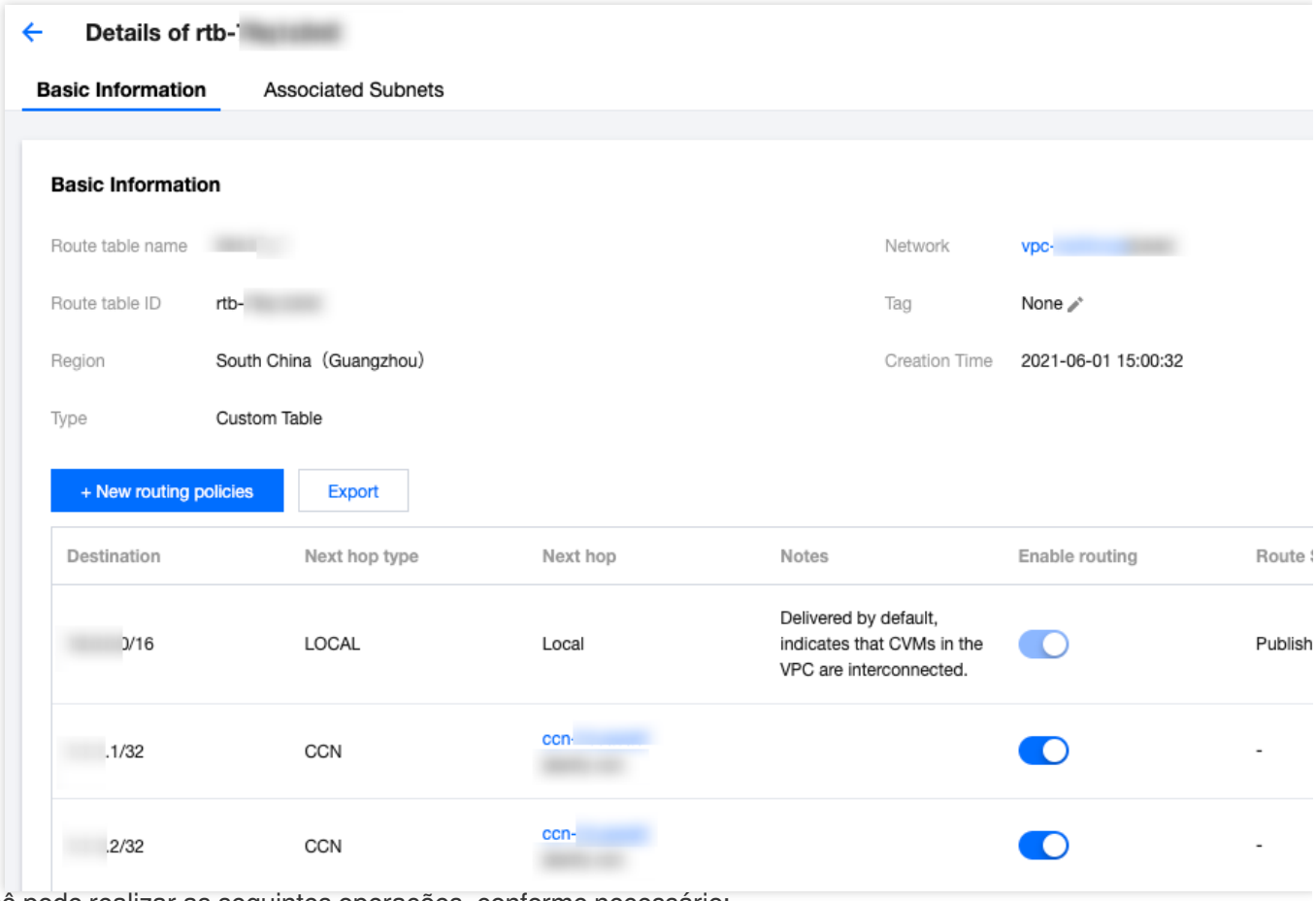


Configuração do HAVIP

Atualmente, apenas as políticas de roteamento cujo **Next hop type (Tipo de próximo salto)** é **High Availability Virtual IP (IP virtual de alta disponibilidade)**, **VPN Gateway** ou **CVM** nas tabelas de rotas padrão ou

personalizadas podem ser publicadas manualmente ou retiradas do CCN.

1. Clique na ID da tabela de rotas para acessar a página de detalhes.



2. Você pode realizar as seguintes operações, conforme necessário:

Clique em **Publish to CCN (Publicar no CCN)** para publicar uma política de roteamento habilitada para o CCN.

Clique em **Withdraw from CCN (Retirar do CCN)** para retirar uma política de roteamento personalizada que foi publicada no CCN.

Clique em **Edit (Editar)** para modificar a política de roteamento.

Clique em **Delete (Excluir)** para excluir uma política de roteamento desativada.

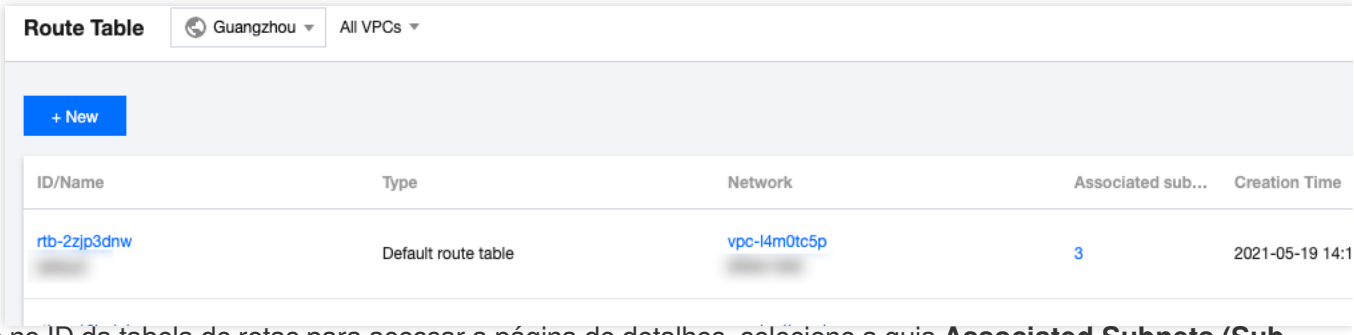
Associação ou desassociação da sub-rede

Last updated：2024-01-24 17:48:51

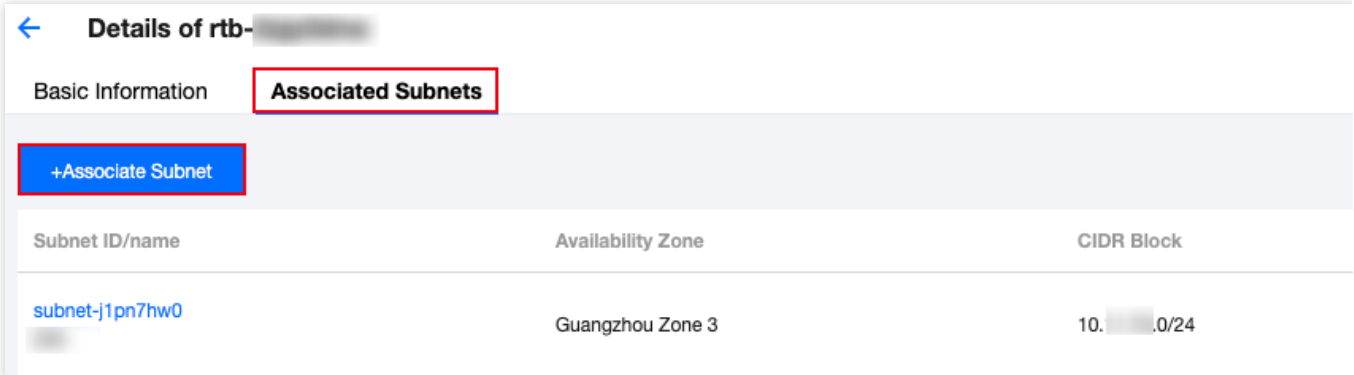
Depois que a tabela de rotas for criada, ela precisará ser associada à sub-rede para controlar o tráfego de saída da sub-rede. Este documento descreve como associar a tabela de rotas ou desassociá-la da sub-rede.

Associação à sub-rede

1. Faça login no Console do VPC.
2. Selecione **Route Tables (Tabelas de rotas)** na barra lateral esquerda para acessar a página de gerenciamento.
3. Existem dois métodos para associar à sub-rede:
Na lista, selecione a tabela de rotas que precisa ser associada à sub-rede e clique em **More (Mais)** > **Associated Subnets (Sub-redes associadas)** na coluna **Operation (Operação)**.



Clique no ID da tabela de rotas para acessar a página de detalhes, selecione a guia **Associated Subnets (Sub-redes associadas)** e clique em **+Associate Subnet (+Associar sub-rede)**.



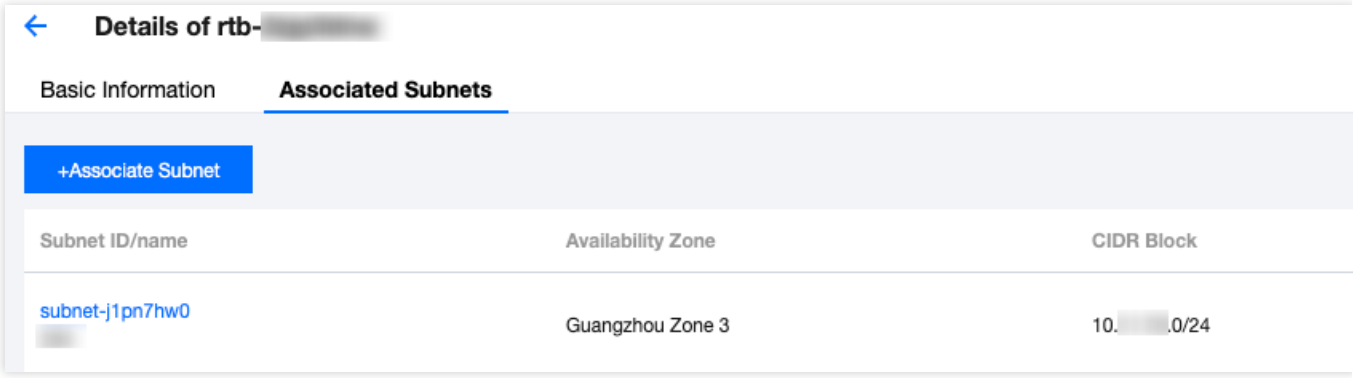
4. Na janela pop-up, selecione a sub-rede a ser associada (uma tabela de rotas pode ser associada a várias sub-redes ao mesmo tempo e é possível filtrar rapidamente por ID/nome da sub-rede). Avalie o impacto comercial da associação na sub-rede. Confirme o impacto e clique em **OK**.

Atenção:

Depois que a tabela de rotas for associada à sub-rede, a tabela de rotas original associada à sub-rede será substituída pela nova, e o tráfego de saída da sub-rede será executado de acordo com as políticas na nova tabela de rotas. Avalie cuidadosamente o impacto na empresa.

Desassociação da sub-rede

1. Faça login no Console do VPC.
2. Selecione **Route Tables (Tabelas de rotas)** na barra lateral esquerda para acessar a página de gerenciamento.
3. Clique no ID da tabela de rotas para acessar a página de detalhes, alterne para a guia **Associated Subnets (Sub-redes associadas)** e clique em **Disassociate (Desassociar)**.



4. Na janela pop-up, selecione uma nova tabela de rotas para a sub-rede a ser desassociada e clique em **OK** para completar a dissociação da tabela de rotas atual da sub-rede. A política de tráfego de saída da sub-rede será executada com base na nova tabela de rotas selecionada para ela.

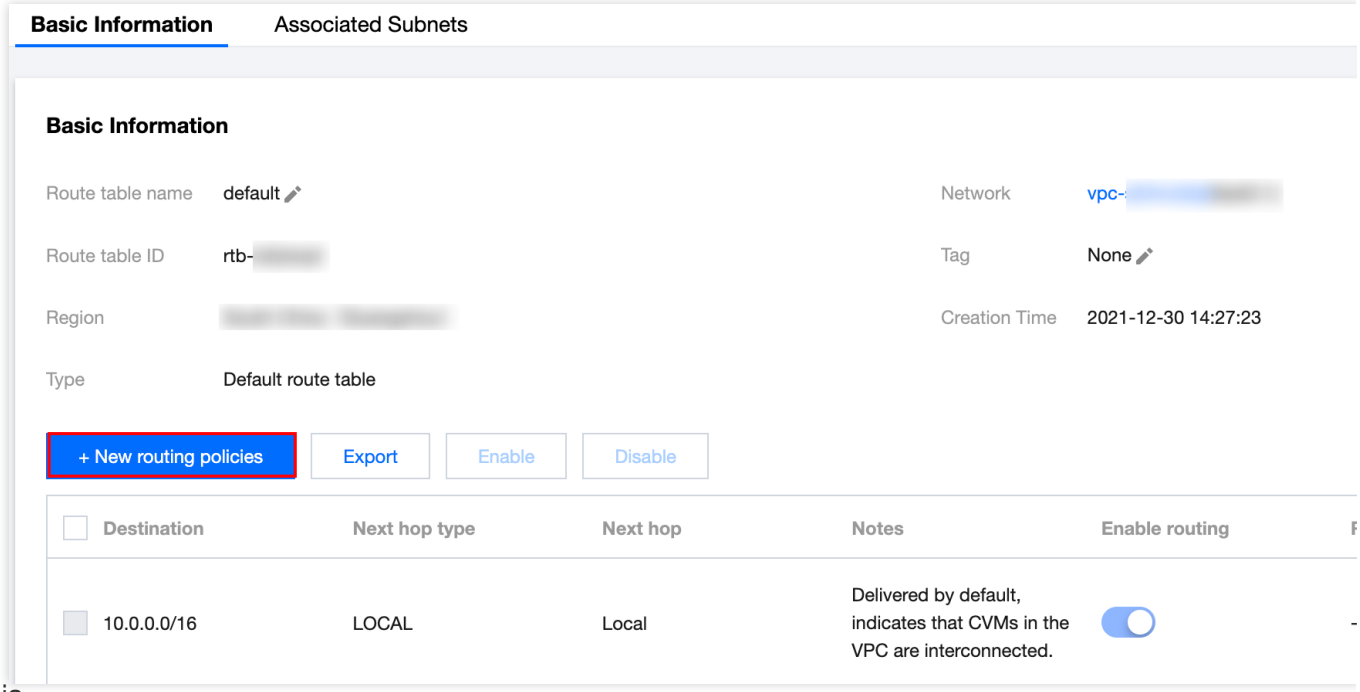
Gerenciamento de políticas de roteamento

Last updated：2024-01-24 17:48:51

Este documento descreve as operações relacionadas com as políticas de roteamento.

Adição de uma política de roteamento

1. Faça login no Console da VPC e acesse a página **Route Table (Tabela de rotas)**.
2. Clique no **ID/Name (ID/Nome)** da tabela de rotas a ser modificada para acessar sua página de detalhes.
3. Clique em **+New routing policies (+Novas políticas de roteamento)**.



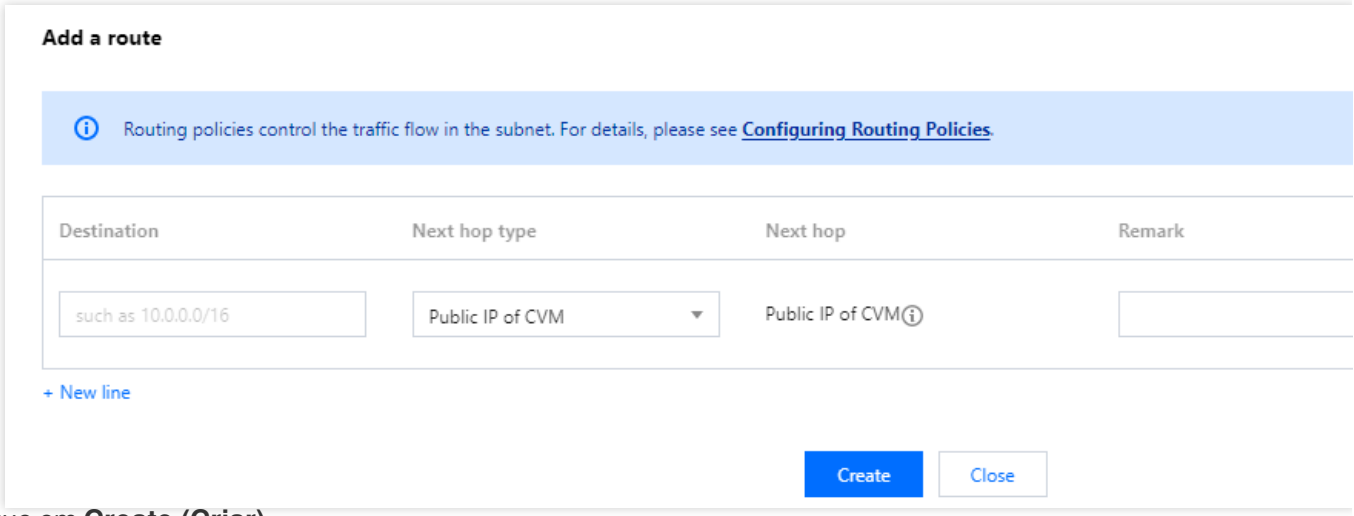
4. Na janela pop-up, configure a política de roteamento.

Nota:

Se você implantou um serviço TKE na VPC, o destino que você configura na política de roteamento da sub-rede da VPC não pode se sobrepor ao bloco CIDR da VPC ou ao intervalo de IP do TKE. Por exemplo, se o bloco CIDR da VPC for `172.168.0.0/16` e o bloco CIDR do TKE for `192.168.0.0/16`, o intervalo de IP de destino não pode estar dentro de `172.168.0.0/16` nem conter `192.168.0.0/16`.

Item de configuração	Descrição
Destination (Destino)	Especifica o intervalo de IP de destino para o qual você deseja encaminhar o tráfego de saída da sub-rede. Os requisitos para um destino são os seguintes:

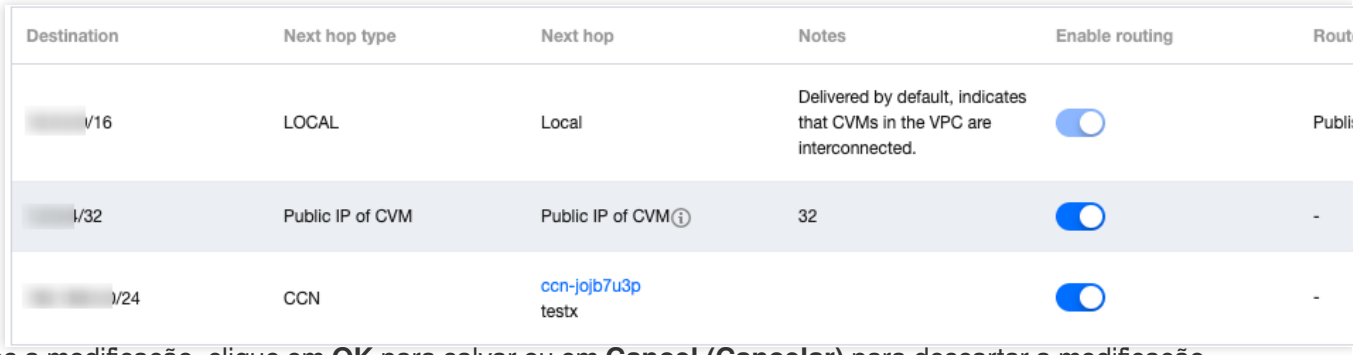
	Insira um intervalo de IP. Se você quiser inserir um único IP, defina a máscara para `32` (por exemplo, `172.16.1.1/32`). O destino não pode ser um intervalo de IP da VPC onde reside a tabela de rotas, pois a rota local já permite interconexão de rede privada neste VPC.
Next hop type (Tipo do próximo salto)	Indica a saída de pacotes de dados para a VPC. Tipos aceitos: NAT Gateway: o tráfego direcionado para um intervalo de IP de destino é encaminhado para um NAT Gateway. Peering Connections: o tráfego direcionado para um intervalo de IP de destino é encaminhado para o par da VPC de um Peering Connection. Direct Connect Gateway (Gateway do Direct Connect): o tráfego direcionado para um intervalo de IP de destino é encaminhado para um gateway do Direct Connect. High Availability Virtual IP (IP virtual de alta disponibilidade): o tráfego direcionado para um intervalo de IP de destino é encaminhado para um HAVIP. VPN Gateway (Gateway do VPN): o tráfego direcionado para um intervalo de IP de destino é encaminhado para um gateway do VPN. Public IP of CVM (IP público da CVM): o tráfego direcionado para um intervalo de IP de destino é encaminhado para o IP público (incluindo EIPs) de uma instância da CVM na VPC. CVM: o tráfego direcionado para um intervalo de IP de destino é encaminhado para uma instância da CVM na VPC.
Next hop (Próximo salto)	Especifica a instância do próximo salto para a qual o tráfego é redirecionado, como o gateway ou o IP da CVM.
Notes (Observações)	(Opcional) Você pode inserir a descrição da rota para gerenciamento de recursos.
Add a line (Adicionar uma linha)	Você pode clicar em +Add a line (+Adicionar uma linha) para configurar várias políticas de roteamento ou clicar no ícone de exclusão na coluna Operation (Operação) para excluir as políticas de roteamento desnecessárias.



5. Clique em **Create (Criar)**.

Edição de uma política de roteamento

1. Faça login no Console da VPC e acesse a página **Route Table (Tabela de rotas)**.
2. Na lista, clique no **ID/Name (ID/Nome)** da tabela de rotas em questão para acessar sua página de detalhes.
3. Clique em **Edit (Editar)** na coluna **Operation (Operação)** da política de roteamento para modificá-la.



4. Após a modificação, clique em **OK** para salvar ou em **Cancel (Cancelar)** para descartar a modificação.

Publicação/Retirada de uma política de roteamento do/para o CCN

As rotas de uma VPC associada a um CCN são publicadas no CCN por padrão. Para as novas políticas de roteamento personalizadas que não são publicadas, você precisa publicá-las manualmente. Você também pode retirar uma política de roteamento do CCN.

Atualmente, apenas as políticas de roteamento cujo **Next hop type (Tipo de próximo salto)** é **High Availability Virtual IP (IP virtual de alta disponibilidade)** ou **CVM** nas tabelas de rotas padrão ou personalizadas podem ser publicadas manualmente ou retiradas do CCN.

Pré-requisitos

A VPC onde reside o HAVIP ou CVM está associada a uma instância do CCN.

Instruções

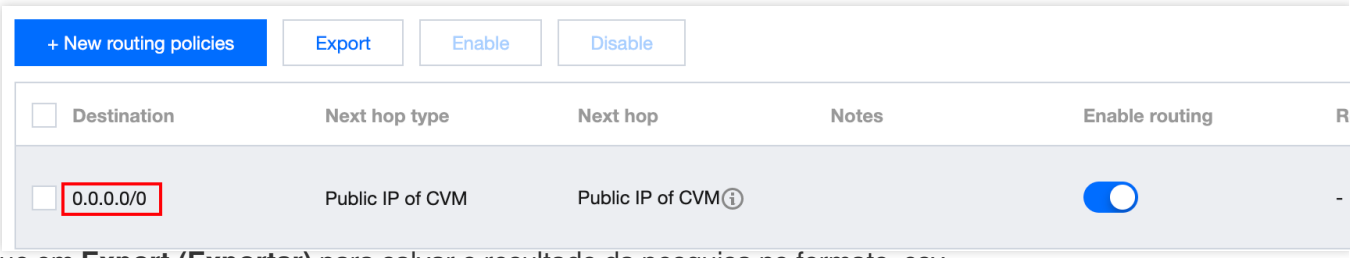
1. Faça login no Console da VPC e acesse a página **Route Table (Tabela de rotas)**.
2. Clique no **ID/Name (ID/Nome)** da tabela de rotas a ser modificada para acessar sua página de detalhes.
3. Execute as seguintes operações conforme necessário:
Clique em **Publish to CCN (Publicar no CCN)** para publicar manualmente uma política de roteamento personalizada no CCN.
Clique em **Withdraw from CCN (Retirar do CCN)** para retirar uma política de roteamento personalizada que foi publicada no CCN.

Atenção:

Uma política de roteamento desativada não pode ser publicada no CCN.
Uma política de roteamento não pode ser desativada depois de publicada no CCN.

Consulta e exportação de uma política de roteamento

1. Faça login no Console da VPC e acesse a página **Route Table (Tabela de rotas)**.
2. Clique no **ID/Name (ID/Nome)** da tabela de rotas em questão para acessar sua página de detalhes. Nessa página, você pode exibir as políticas de roteamento nesta tabela de rotas.
3. Na caixa de pesquisa superior direita, consulte as políticas de roteamento inserindo um endereço de destino.



4. Clique em **Export (Exportar)** para salvar o resultado da pesquisa no formato .csv.

Ativação/Desativação de uma política de roteamento

Uma política de roteamento personalizada pode ser ativada ou desativada.

Instruções

1. Faça login no Console da VPC e acesse a página **Route Table (Tabela de rotas)**.

2. Clique no **ID/Name (ID/Nome)** da tabela de rotas em questão para acessar sua página de detalhes. Verifique o status da política de roteamento:

: ativada

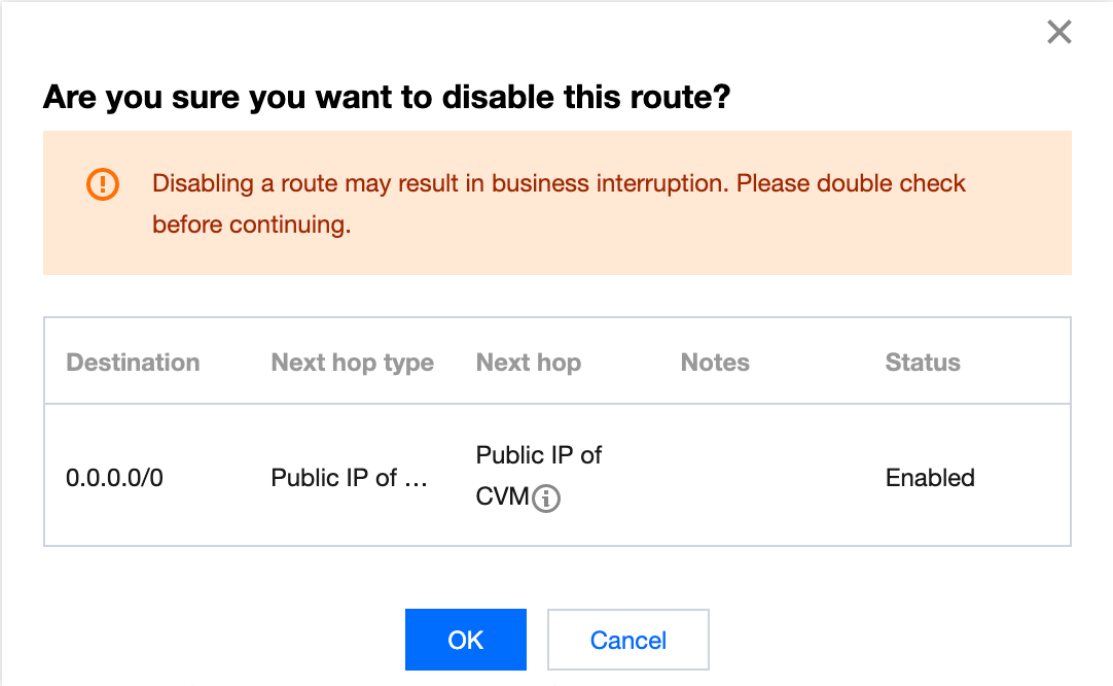
: desativada

3. Para desativar uma política de roteamento: clique no ícone

ao lado de uma política de roteamento para desativá-la.

Atenção:

Desativar uma rota pode resultar na interrupção dos negócios. Confirme antes de continuar.



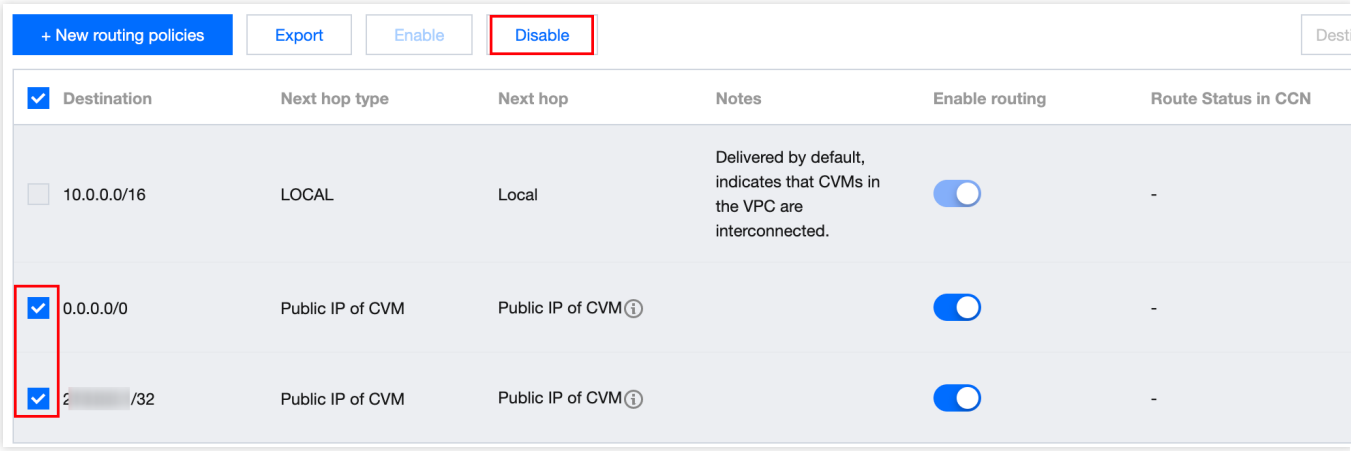
4. Para ativar uma política de roteamento: clique no ícone

ao lado de uma política de roteamento para ativá-la.

Atenção:

Quando ativada, será utilizada a rota com a máscara mais longa. Isso pode afetar seus negócios atuais. Confirme antes de continuar.

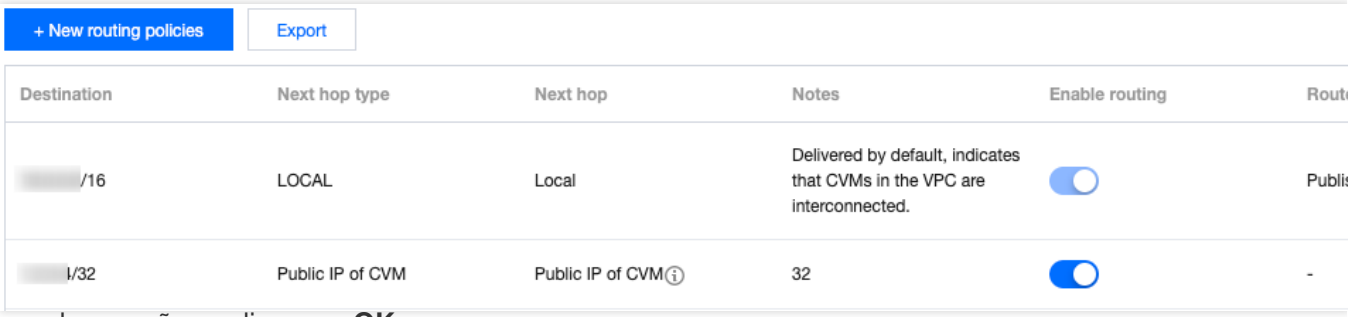
5. Para ativar ou desativar várias políticas de roteamento: selecione as políticas de roteamento em questão e clique em **Enable (Ativar)** ou **Disable (Desativar)** acima da lista.



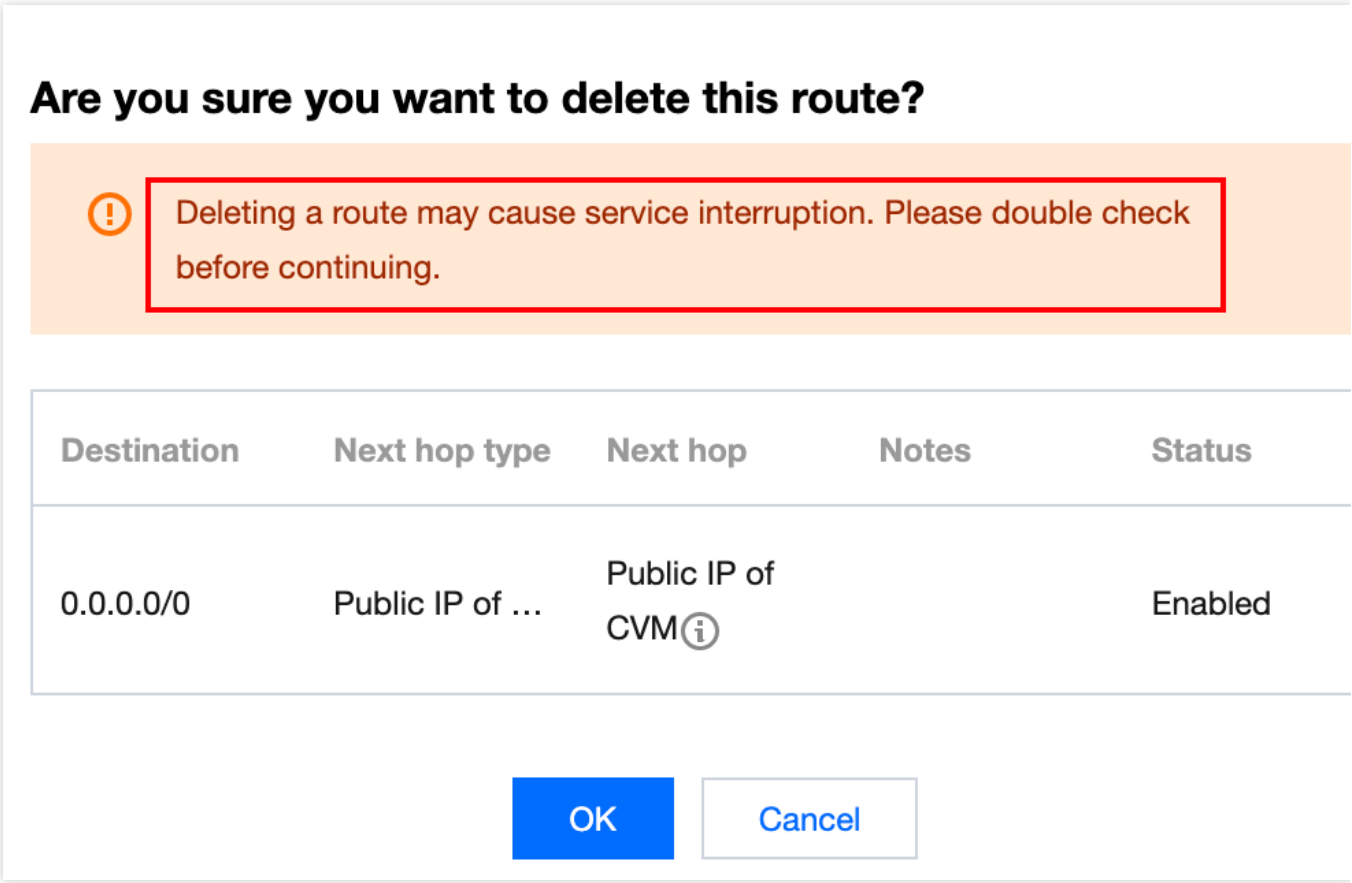
Exclusão de uma política de roteamento

Você pode excluir as políticas de roteamento não utilizadas. Só é possível excluir as políticas de roteamento personalizadas.

1. Faça login no Console da VPC e acesse a página **Route Table (Tabela de rotas)**.
2. Clique no **ID/Name (ID/Nome)** da tabela de rotas a ser modificada para acessar sua página de detalhes.
3. Selecione a política de roteamento a ser excluída e clique em **Delete (Excluir)** na coluna **Operation (Operação)**.



4. Leia as observações e clique em **OK**.



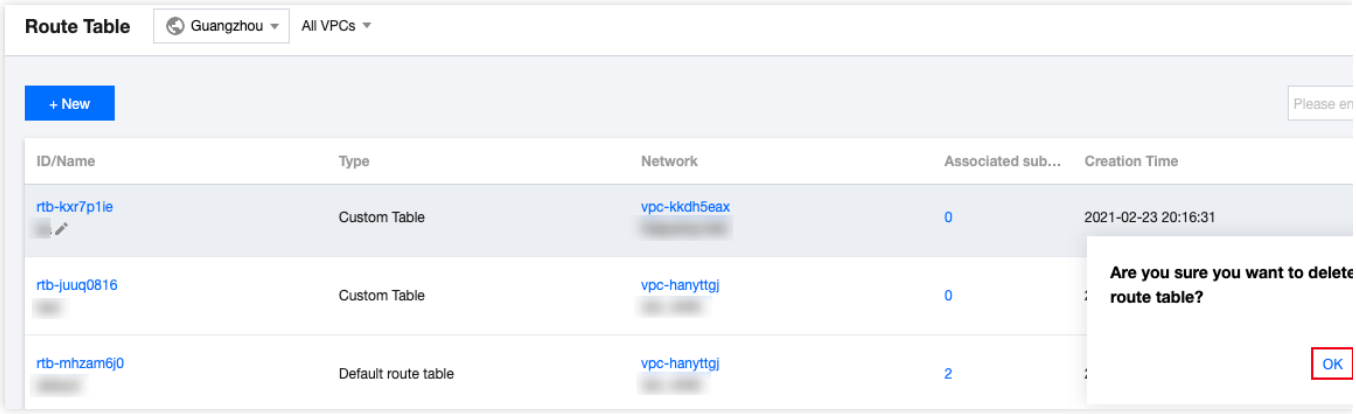
Exclusão de uma tabela de rotas

Last updated：2024-01-24 17:48:51

É possível excluir a tabela de rotas que não estiver associada a nenhuma sub-rede. Diferente da tabela de rotas padrão que é gerada automaticamente pelo sistema, apenas as tabelas de rotas personalizadas podem ser excluídas.

Instruções

1. Faça login no Console VPC e selecione **Route Tables (Tabelas de rotas)**.
2. Na lista, selecione a tabela de rotas a ser excluída. Clique em **Delete (Excluir)** na coluna **Operation (Operação)**.



IPs e ENIs
IP elástico

Last updated：2024-01-24 17:48:51

IP elástico (EIP): um EIP é um endereço IP estático desenvolvido para computação em nuvem dinâmica. Ele também é um endereço IP público que permanece inalterado em uma região. Com os EIPs, é possível remapear rapidamente um endereço para outra instância ou uma instância do NAT Gateway em sua conta para proteger contra as falhas da instância.

Você pode manter o EIP na sua conta até que seja liberado. Embora o IP público só possa ser liberado com o CVM, o EIP pode ser dissociado do ciclo de vida do CVM e operar de forma independente como um recurso em nuvem. Por exemplo, caso precise manter um IP público que esteja fortemente relacionado à sua empresa, você pode convertê-lo em um EIP e mantê-lo em sua conta.

Para acessar os procedimentos detalhados dos EIPs, consulte a seção “Direções” em IP elástico.

HAVIPs
Visão geral

Last updated：2024-01-24 17:48:51

Um IP virtual de alta disponibilidade (HAVIP, na sigla em inglês) é um endereço IP privado atribuído do bloco CIDR de uma sub-rede da VPC. Geralmente, é usado em conjunto com software de alta disponibilidade, como Keepalived e cluster de failover do Windows Server, para criar um cluster principal/secundário altamente disponível.

Nota:

Atualmente, o HAVIP está em versão beta, e podem levar 10 segundos para alternar entre os servidores principal/secundário. Para testá-lo, inscreva-se para ser um usuário beta.

Para garantir a alta disponibilidade da CVM em um cluster principal/secundário, recomendamos atribuir CVMs a hosts diferentes usando grupos de posicionamento. Para mais informações sobre grupos de posicionamento, consulte Grupo de posicionamento.

O software de alta disponibilidade deve permitir o envio de mensagens ARP.

Funcionalidades

É possível solicitar vários endereços HAVIP no console para cada VPC.

Você deve vincular o HAVIP no arquivo de configuração da CVM.

Arquitetura e princípio

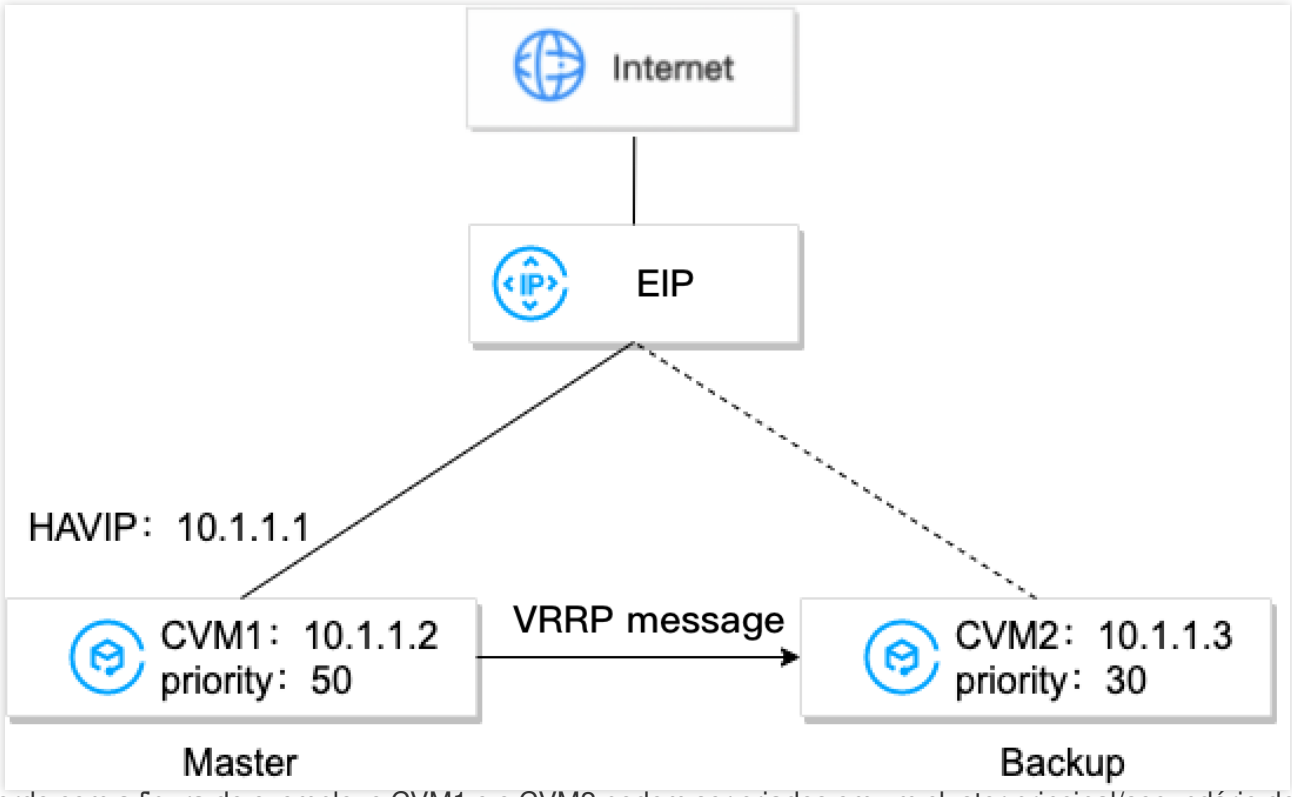
Normalmente, um cluster principal/secundário de alta disponibilidade consiste em dois servidores: um servidor principal ativo e um servidor secundário em espera. Os dois servidores compartilham o mesmo VIP (IP virtual). O VIP só pode trabalhar em um servidor principal ao mesmo tempo. Quando o servidor principal falhar, o servidor secundário assumirá o VIP para continuar fornecendo serviços.

Em redes físicas tradicionais, o status principal/secundário pode ser negociado com o protocolo VRRP do Keepalived. O dispositivo principal envia periodicamente mensagens ARP gratuitas para limpar a tabela MAC ou a tabela ARP do terminal da troca de uplink, de modo a acionar a migração VIP para o dispositivo principal.

Em uma VPC, um cluster principal/secundário de alta disponibilidade também pode ser implementado ao implantar o Keepalived em CVMs. No entanto, uma instância da CVM geralmente não pode obter um IP privado por meio de anúncio ARP por motivos de segurança, como falsificação de ARP. O VIP deve ser um HAVIP solicitado da Tencent Cloud, que é específico da sub-rede. Portanto, o HAVIP só pode ser vinculado a um servidor na mesma sub-rede por meio de anúncio.

Nota:

O Keepalived é um software de alta disponibilidade baseado em VRRP. Para usar o Keepalived, primeiro conclua sua configuração no arquivo `Keepalived.conf` .
A figura a seguir mostra a arquitetura do HAVIP.



De acordo com a figura de exemplo, o CVM1 e o CVM2 podem ser criados em um cluster principal/secundário de alta disponibilidade com as seguintes etapas:
1. Instale o Keepalived no CVM1 e no CVM2, configure o HAVIP como VIP do VRRP e defina as prioridades dos servidores principal e secundário. Valores maiores representam prioridades mais altas.
2. O Keepalived usa o protocolo VRRP para comparar as prioridades iniciais de CVM1 e CVM2, e determina o CVM1 como o servidor principal devido à sua prioridade mais alta.
3. O servidor principal envia mensagens ARP, anuncia o VIP (um HAVIP) e atualiza o VIP para os mapeamentos MAC. Neste caso, o CVM1 é o servidor principal e fornece serviços utilizando o IP privado (HAVIP) para comunicação. Você pode ver que o HAVIP está vinculado ao servidor principal do CVM1 no console do HAVIP.
4. (Opcional) Vincule um EIP ao HAVIP no console para implementar a comunicação na rede pública.
5. O servidor principal envia mensagens VRRP ao servidor secundário de forma periódica. Se o servidor principal não conseguir enviar mensagens VRRP dentro de um determinado período, o servidor secundário será definido como principal e enviará mensagens de atualização ARP que carregam seu endereço MAC. Nesse caso, o CVM2 passa a ser o servidor principal para fornecer serviços de comunicação e tratar solicitações de acesso externo. Você verá que a CVM vinculado ao HAVIP muda para o CVM2 no console do HAVIP.

Casos de uso comuns

Alta disponibilidade do Cloud Load Balancer

Para implantar o Cloud Load Balancer (CLB), você geralmente usará alta disponibilidade (HA, na sigla em inglês) entre instâncias do CLB e configurará servidores reais como um cluster. Portanto, você deve implantar e usar o HAVIP como um IP virtual entre dois servidores do CLB.

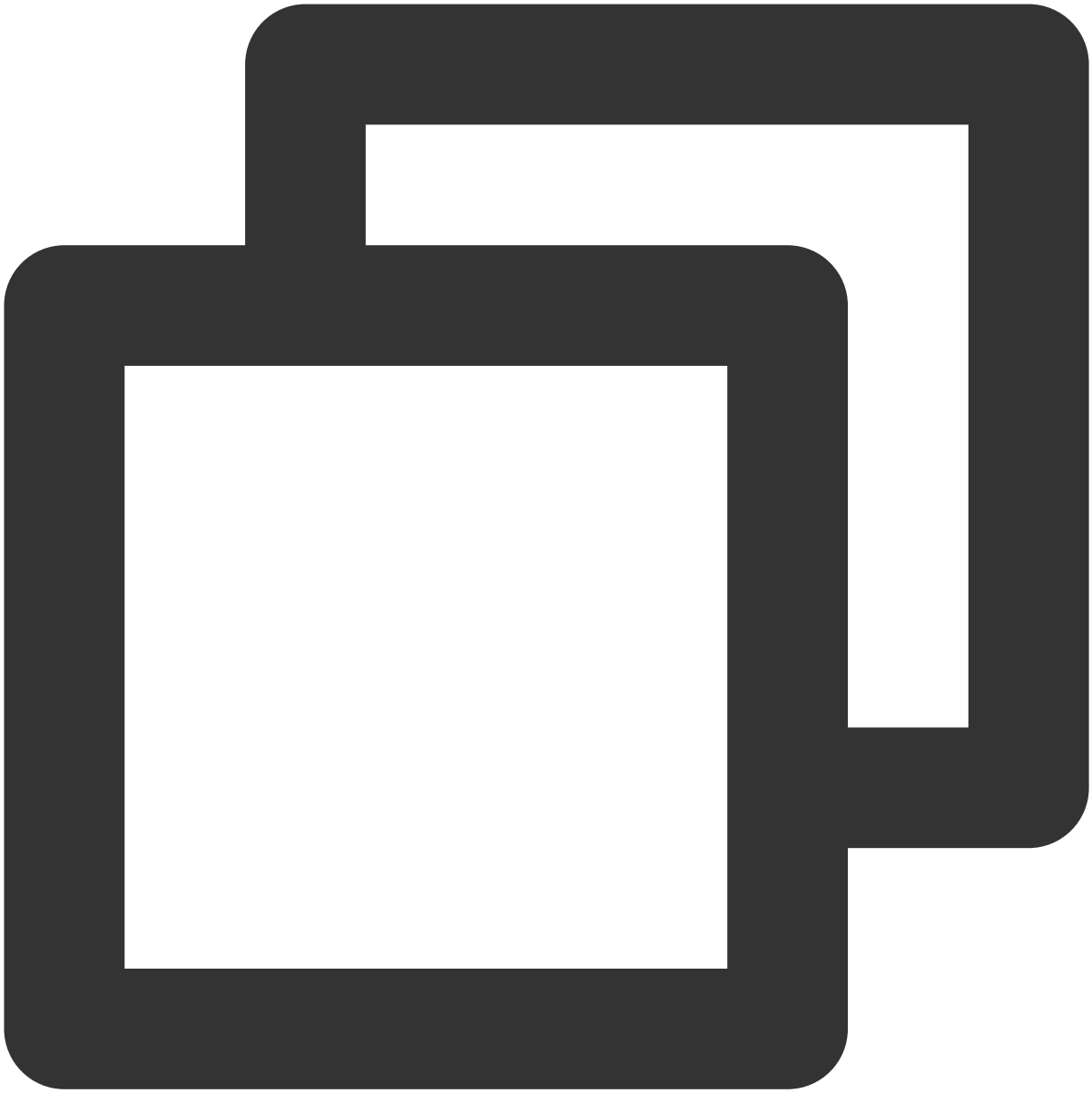
Banco de dados relacional principal/secundário

Se o Keepalived ou o cluster de failover do Windows Server forem usados entre dois bancos de dados para criar um cluster principal/secundário altamente disponível, use o HAVIP como um IP virtual. Para mais informações, consulte Criação de cluster principal/secundário de alta disponibilidade usando HAVIP + Keepalived e Criação de um banco de dados de alta disponibilidade usando HAVIP + cluster de failover do Windows Server em Práticas recomendadas.

Perguntas frequentes

Por que devo usar o HAVIP junto com o Keepalived em uma VPC?

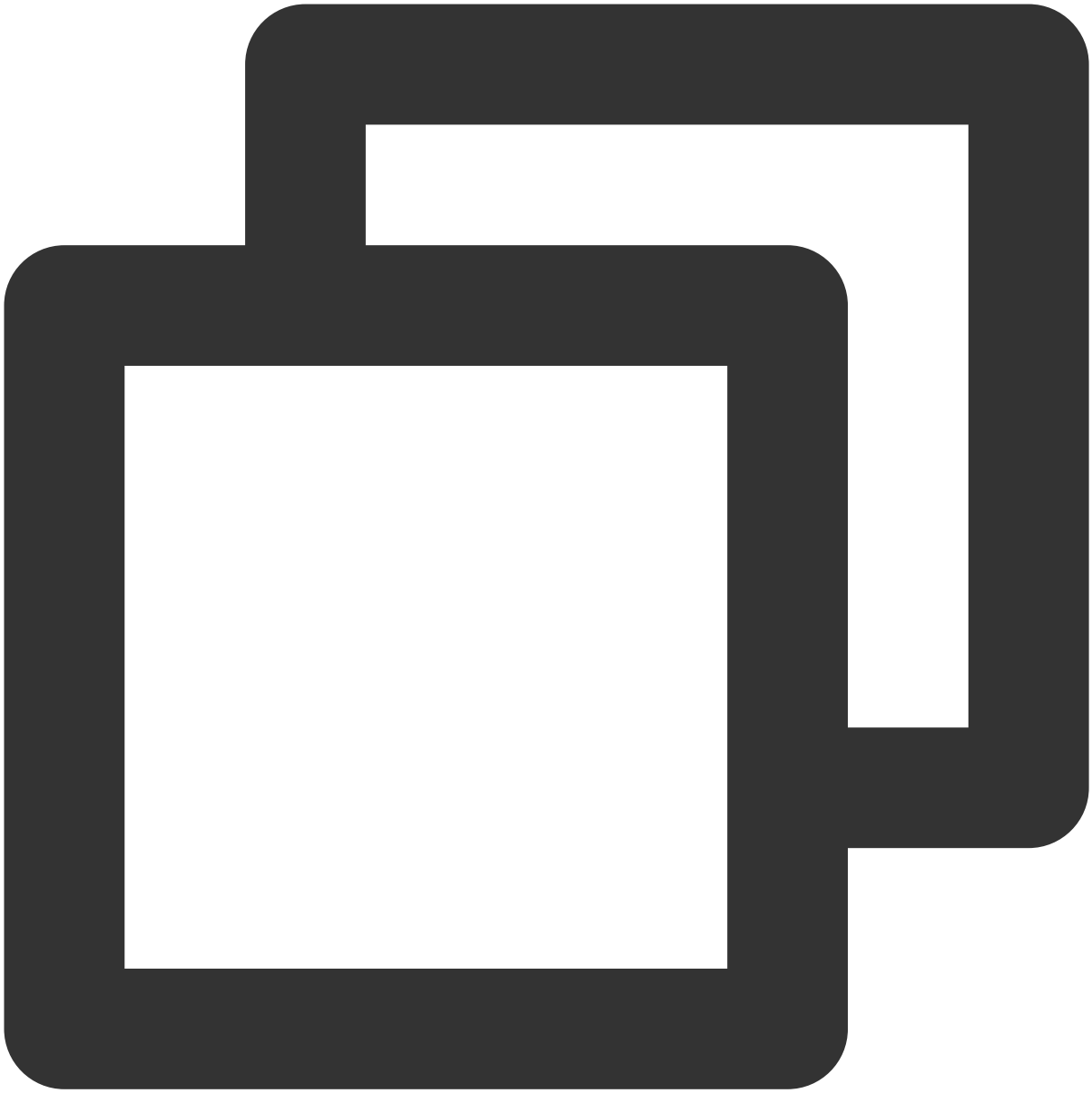
Alguns fornecedores de nuvem pública não aceitam vincular um IP privado ao CVM por meio do anúncio ARP por motivos de segurança, como falsificação de ARP. Se você usar diretamente um IP privado como o IP virtual no arquivo “Keepalived.conf”, o Keepalived não conseguirá atualizar o mapeamento de IP para MAC durante a alternância de IP virtual do servidor principal/secundário. Neste caso, você deve chamar uma API para alternar o IP. Usando a configuração do Keepalived como exemplo, as configurações de IP são as seguintes:



```
vrrp_instance VI_1 {
    state BACKUP            #Dispositivo secundário
    interface eth0           #Nome da ENI
    virtual_router_id 51
    nopreempt                    #Modo Non-preempt
    #preempt_delay 10
    priority 80
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass 1111
```

```
    }
    unicast_src_ip 172.17.16.7 #IP privado do dispositivo local
    unicast_peer{
        172.17.16.13           #Endereço IP do dispositivo de par, por exemplo: 10.
    }

    virtual_ipaddress {

        172.17.16.3  #Insira o endereço HAVIP que você solicitou no console.

    }

    garp_master_delay 1
    garp_master_refresh 5

    track_interface {
        eth0
    }

    track_script {
        checkhaproxy
    }
}
```

Se não houver HAVIP, a seção a seguir do arquivo de configuração será inválida.



```
virtual_ipaddress {
   172.17.16.3 #Insira o endereço HAVIP que você solicitou no console.
}
```

Referência

Para mais informações sobre os limites de uso do HAVIP, consulte Limites.

Para mais informações sobre o guia de operação do HAVIP, consulte Gerenciamento de HAVIP.

Limites

Last updated：2024-01-24 17:48:51

Limites de uso

A ocupação de um HAVIP pode ser declarada pelo back-end do CVM, mas você não pode vincular os HAVIPs manualmente a um servidor especificado no console (a experiência é consistente com a de uma máquina física tradicional).
O RS de back-end, mas não o HAVIP, determina se a migração deve ser feita com base na negociação do arquivo de configuração.
Apenas as instâncias do VPC são compatíveis, e a rede básica não é compatível.
A detecção de pulsação deve ser feita por um aplicativo no CVM, mas não pelo HAVIP, que serve apenas como um endereço IP flutuante declarado pelo ARP (a experiência é a mesma de uma máquina física tradicional).

Limites de cota

Recurso	Limite
Cota HAVIP padrão em cada VPC	10

Gerenciamento de HAVIP

Last updated：2024-01-24 17:48:52

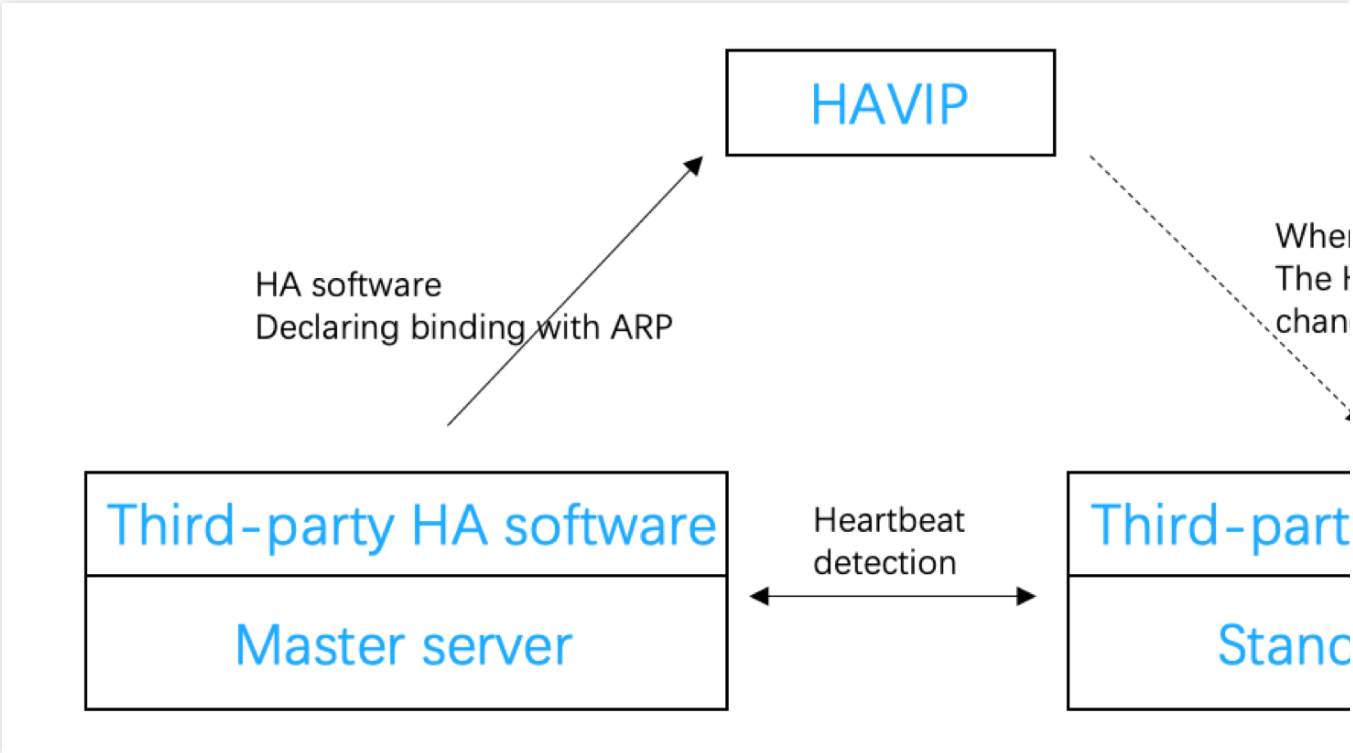
Este documento descreve como criar um HAVIP no console e configurá-lo em um software de terceiros.

Instruções

1. Faça login no Console do VPC e selecione **IP and Interface (IP e interface)** > **HAVIP** na barra lateral esquerda.
2. Selecione a região em questão na página de gerenciamento do HAVIP e clique em **Apply (Solicitar)**.
3. Na caixa de diálogo pop-up, configure os parâmetros do HAVIP.
Name (Nome): insira um nome para o HAVIP.
Virtual Private Cloud: selecione um VPC no qual o HAVIP a ser criado está localizado.
Subnet (Sub-rede): selecione uma sub-rede específica para o HAVIP.
IP address (Endereço IP): o endereço IP do HAVIP pode ser atribuído automaticamente ou especificado de forma manual. Se você escolher **Automatic Assignment (Atribuição automática)**, um endereço IP da sub-rede será atribuído automaticamente. Se você escolher **Enter manually (Inserir manualmente)**, certifique-se de que o endereço IP inserido esteja no intervalo de IP da sub-rede e não seja um endereço IP reservado do sistema. Por exemplo, se o intervalo de IP da sub-rede for `10.0.0.0/24`, o endereço IP privado inserido deve estar dentro de `10.0.0.2-10.0.0.254`.
4. Clique em **OK**. Depois que o HAVIP for criado, ele será exibido na lista e seu status será **Not bound with CVM yet (Ainda não vinculado ao CVM)**.

Configuração de um HAVIP

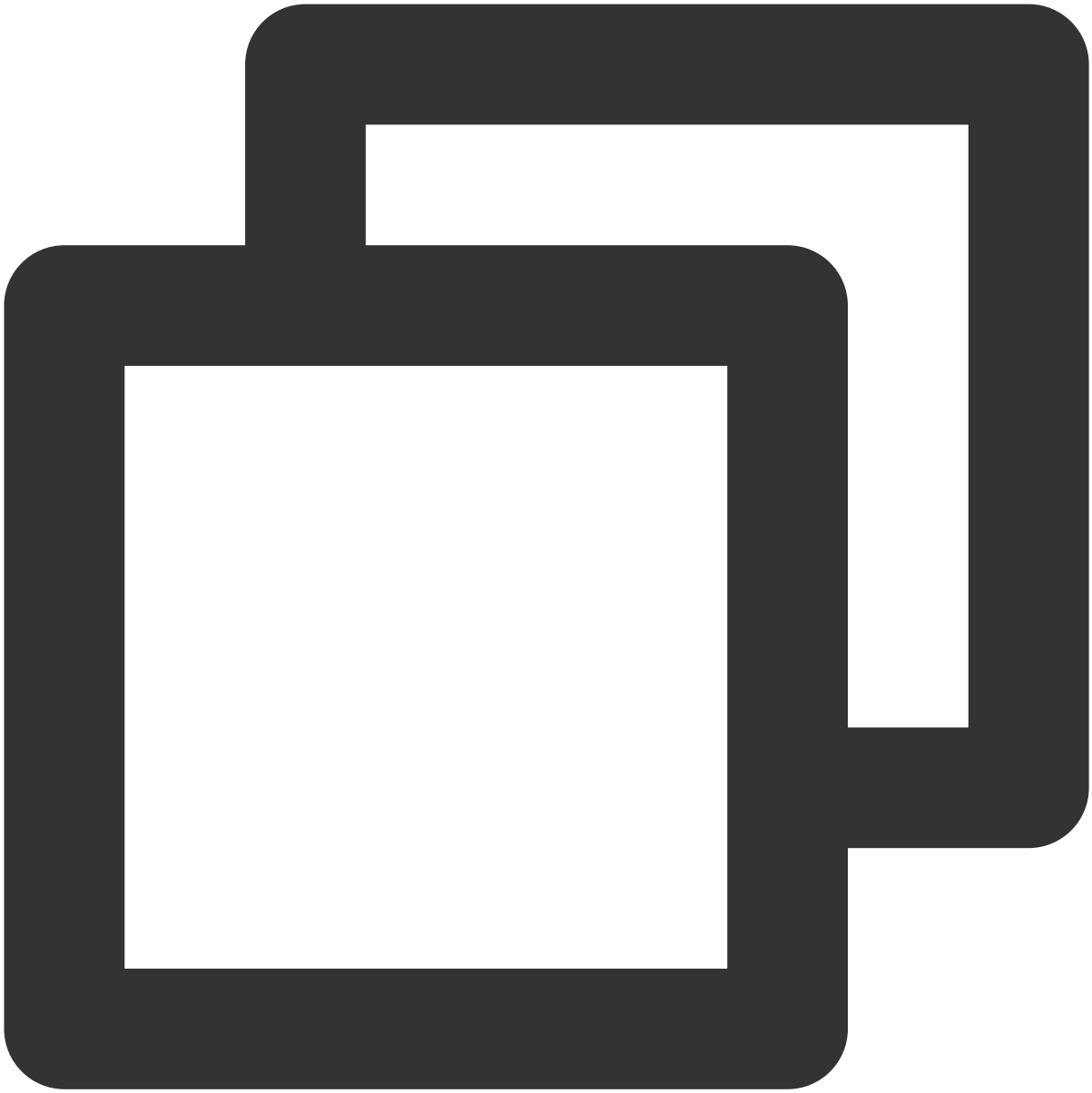
Um HAVIP é projetado para ser usado junto com um software de alta disponibilidade (HA, na sigla em inglês) de terceiros, que deve ser configurado no software de HA de terceiros. Um HAVIP é apenas um objeto de operação e um endereço IP privado que pode ser vinculado por meio de anúncio. Portanto, a vinculação e a desvinculação de HAVIP a CVMs não são feitas no console do Tencent Cloud. Em vez disso, basta especificar o HAVIP como um endereço IP virtual (VIP) flutuante no software de HA de terceiros, que por sua vez especifica um ENI a ser vinculado ao HAVIP por meio do ARP. Veja abaixo como vincular ou desvincular um HAVIP:



Em um ambiente de dispositivo físico tradicional, todos os endereços IP privados são vinculados a ENIs por meio do ARP, por padrão, e podem ser especificados como endereços IP flutuantes no software de HA. Em um ambiente de nuvem pública, um IP privado não pode usar o ARP ou ser especificado como um endereço IP flutuante no software de HA. Portanto, é necessário seguir as mesmas etapas do software de terceiros para especificar o HAVIP como um endereço IP flutuante.

Nota:

Programas de software de HA comuns incluem: o Linux HeartBeat, o Keepalived, o Pacemaker e o Windows MSCS. Ao especificar um VIP no arquivo de configuração do software de HA, basta inserir o HAVIP que você criou:



```
vrrp_instanceVI_1 {
# Selecione os parâmetros adequados para os CVMs principais e secundários.
    state MASTER                #Defina o status inicial como `Backup`.
    interface eth0               #O ENI (tais como `eth0`) usado para vincular um VI
    virtual_router_id 51         #O valor `virtual_router_id` para o cluster
        nopreempt                    #Modo Non-preempt
        preempt_delay 10            #Defina o atraso de preempção para 10 minutos
    priority 100                #Prioridade. Quanto maior o valor, maior a prioridad
    advert_int 1                #Intervalo de verificação. O valor padrão é 1 segund
    authentication {            #Autenticação
        auth_type PASS           #Método de autenticação
```

```
        auth_pass 1111          #Senha de autenticação
    }
        unicast_src_ip 172.16.16.5 #Endereço IP privado do dispositivo local
        unicast_peer{
        172.16.16.6               #Endereço IP do dispositivo de par
        }
    virtual_ipaddress {
        172.16.16.12              #HAVIP
    }
    }
```

Depois que as configurações forem concluídas no software de HA do CVM, o status do HAVIP mudará para **Bound with CVM (Vinculado ao CVM)** no console.

Consulte os seguintes casos para realizar as suas configurações:

Criação de cluster principal/secundário de alta disponibilidade usando HAVIP + Keepalived

Criação de um banco de dados de alta disponibilidade usando HAVIP + cluster de failover do Windows Server

Documentação

Semelhante a um IP privado, um HAVIP também pode ser vinculado ou desvinculado de um EIP no console. Se você precisar de comunicação de rede pública, consulte Vinculação ou desvinculação de EIP.

Vinculação ou desvinculação de EIP

Last updated：2024-01-24 17:48:52

Semelhante a um IP privado, a vinculação do HAVIP também pode ser configurada no console. Vincular um HAVIP refere-se a operações de EIP. Você pode pular esta seção se nenhuma conexão de rede pública for necessária.

Vinculação de um EIP

1. Faça login no Console do VPC e selecione **IP and Interface (IP e interface)** > **HAVIP** na barra lateral esquerda.
2. Selecione a região em questão na página de gerenciamento do HAVIP.
3. Selecione o HAVIP a ser vinculado ao EIP e clique em **Bind (Vincular)** na coluna **Operation (Operação)**.
4. Na caixa de diálogo pop-up, selecione um EIP a ser vinculado.

Atenção:

Um HAVIP só pode ser vinculado a um EIP. Se nenhum EIP estiver disponível, primeiro você deve criar um EIP no console.

Se o HAVIP não estiver vinculado a uma instância do CVM, o EIP correspondente ficará inativo e incorrerá em uma taxa de inatividade. Configure o HAVIP corretamente e vincule-o a uma instância, referindo-se aos seguintes casos:

Criação de cluster principal/secundário de alta disponibilidade usando HAVIP + Keepalived em Práticas recomendadas

Criação de um banco de dados de alta disponibilidade usando HAVIP + cluster de failover do Windows Server em Práticas recomendadas

5. Clique em **OK**.

Desvinculação de um EIP

1. Faça login no Console do VPC e selecione **IP and Interface (IP e interface)** > **HAVIP** na barra lateral esquerda.
2. Selecione a região em questão na página de gerenciamento do HAVIP.
3. Selecione o HAVIP do qual o EIP será desvinculado e clique em **Unbind (Desvincular)** na coluna **Operation (Operação)**.
4. No pop-up, leia as observações e clique em **OK** para desvincular o EIP.

Atenção:

Seu negócio de rede pública pode ser afetado após a desvinculação do EIP. Prepare-se com antecedência.

Depois de ser desvinculado, o EIP ficará inativo e incorrerá em uma taxa de inatividade. Você pode liberar os EIPs não utilizados diretamente para evitar custos.

Consulta de HAVIPs

Last updated：2024-01-24 17:48:51

É possível exibir todos os detalhes do HAVIP em uma região específica no console dele.

Instruções

1. Faça login no Console do VPC.
2. Selecione **IP and Interface (IP e interface)** > **HAVIP** na barra lateral esquerda para acessar a página de gerenciamento do HAVIP.
3. Selecione uma região de destino para exibir os detalhes de todos os HAVIPs que você solicitou.
A descrição do campo é a seguinte:
ID/Name (ID/Nome): ID refere-se ao ID gerado do HAVIP automaticamente depois de ser criado. Você pode clicar nela para exibir as informações básicas do HAVIP. O nome é definido pelo usuário quando o HAVIP é criado.
Status: indica se o HAVIP está especificado como um endereço IP flutuante no arquivo de configuração do software de HA no CVM. Um HAVIP configurado com êxito estará com o status **Bound with CVM (Vinculado ao CVM)**; caso contrário, estará com o status **Not bound with CVM yet (Ainda não vinculado ao CVM)**.
Address (Endereço): endereço HAVIP.
Backend ENI (ENI de back-end): refere-se ao ID do ENI do CVM vinculado. Caso o HAVIP ainda não esteja vinculado ao CVM, este campo será exibido como **-**.
Server (Servidor): refere-se ao ID do CVM vinculado. Caso o HAVIP ainda não esteja vinculado ao CVM, este campo será exibido como **-**.
EIP: refere-se ao EIP vinculado. Caso o HAVIP não esteja vinculado a um EIP, este campo será exibido como **-**.
Virtual Private Cloud: refere-se ao VPC do HAVIP.
Subnet (Sub-rede): refere-se à sub-rede do HAVIP.
Application Time (Hora da solicitação): refere-se à hora em que este HAVIP foi solicitado.
Operation (Operação): refere-se às operações compatíveis, incluindo **Bind (Vincular)**, **Unbind (Desvincular)** e **Release (Liberar)**.
Bind (Vincular): vincula um EIP
Unbind (Desvincular): desvincula um EIP
Release (Liberar): libera o HAVIP
4. Insira o ID, o nome ou o endereço na caixa de pesquisa à direita para pesquisar rapidamente por HAVIPs.
5. Clique no ícone ao lado da caixa de pesquisa para atualizar a página.

Liberação de HAVIPs

Last updated：2024-01-24 17:48:51

Este documento descreve como liberar os HAVIPs não utilizados.

Pré-requisitos

Somente o HAVIP **não vinculado ao CVM** pode ser liberado.

Nota:

Para o HAVIP **vinculado ao CVM**, é preciso desassociar o HAVIP no arquivo de configuração do software de HA de terceiros no CVM, antes de liberá-lo no console.

Instruções

1. Faça login no Console do VPC.
2. Selecione **IP and Interface (IP e interface)** > **HAVIP** na barra lateral esquerda. Na lista de HAVIPs, localize o HAVIP a ser liberado.
3. Clique em **Release (Liberar)** na coluna **Operation (Operação)**.
4. Clique em **Confirm (Confirmar)** na caixa de diálogo pop-up.

ENIs

Last updated：2024-01-24 17:48:51

O Elastic Network Interface (ENI) fica vinculado a um CVM em um VPC e pode ser migrado livremente entre os CVMs. Os ENIs ajudam a configurar redes de gerenciamento e criar soluções de rede altamente confiáveis.
É possível vincular vários ENIs na mesma zona de disponibilidade a um CVM, com base nas especificações do CVM, a fim de garantir uma rede altamente disponível. Também é possível vincular vários endereços IP privados a um ENI para implantar vários endereços IP para um único CVM.
Para acessar os procedimentos comuns de ENI, consulte:

Criação de um ENI
Vinculação e configuração dos CVMs
Desvinculação de um CVM
Exclusão de um ENI
Vinculação de endereços IP privados secundários
Liberação de endereços IP privados secundários
Vinculação de EIPs
Desvinculação de EIPs
Modificação de IPs privados principais
Alteração da sub-rede de um ENI

Consulta de localização de IP

Last updated：2024-01-24 17:48:51

A funcionalidade de consulta de localização de IP te ajuda a obter informações sobre a localização geográfica e o ISP de um endereço IP público.
Por exemplo, a consulta mostra que o endereço IP `123.123.123.123` está localizado em Pequim e é fornecido pela China Unicom.
Nota:
Atualmente, a funcionalidade de consulta de localização de IP está em teste beta. Para testá-la, inscreva-se para a elegibilidade beta.
No momento, essa funcionalidade está disponível gratuitamente, e nenhum SLA pode ser fornecido. Ela será faturada após a comercialização.

Casos de uso

Você pode consultar a localização e o ISP de um endereço IP da CVM de destino e escolher a CVM de origem para se conectar.
Você pode consultar a localização real de um IP público que você adquiriu da Tencent Cloud ou de outras plataformas de nuvem.

Restrições

Atualmente, a consulta de localização de IP está disponível apenas para os endereços IPv4.

Instruções

1. Faça login no Console da VPC.
2. Clique **IP and Interface (IP e interface)** > **IP Location Query (Consulta de localização de IP)** na barra lateral esquerda.
3. Insira um endereço IP para ser consultado e clique em

.

Nota:

Você também pode chamar a API `DescribeIpGeolocationInfos` ou `DescribeIpGeolocationDatabaseUrl` para consultar a localização do IP.

Pacote de largura de banda

Last updated：2024-01-24 17:48:52

O Bandwidth Package (BWP) do Tencent Cloud é um método de faturamento agregado de vários IPs, que reduz significativamente os custos de acesso à internet. Quando as instâncias de rede pública têm picos de tráfego em momentos diferentes, é possível usar o BWP para o faturamento agregado da largura de banda para economizar custos. O BWP aceita os 5 principais mensais e o faturamento do 95º percentil mensal para casos de uso diferentes. O BWP ajuda a reduzir os custos de acesso à internet e aumentar sua eficiência de custos.

Nota:

Atualmente, o BWP está na versão beta. Para testá-lo, envie uma solicitação.

Para ter acesso aos procedimentos comuns do BWP, consulte

Exibição da largura de banda faturável

Alteração do modo de faturamento

Gerenciamento de pacotes de largura de banda de IPs

Gerenciamento de pacotes de largura de banda de dispositivos

Conexão de rede
NAT Gateway

Last updated：2024-01-24 17:48:51

Um NAT Gateway é um serviço que oferece suporte à conversão de endereços IP e fornece recursos SNAT e DNAT. Ele pode fornecer serviço de acesso à internet seguro e de alto desempenho para recursos nos VPCs. Por exemplo, pode fornecer uma saída segura, acessando a rede pública para vários CVMs que ainda não têm acesso à rede pública (internet).

Para acessar os procedimentos comuns do NAT Gateway, consulte:

Introdução

Modificação da configuração do NAT Gateway

Gerenciamento de EIPs do NAT Gateway

Gerenciamento de regras de encaminhamento de portas

Configuração de uma rota que aponta para o NAT Gateway

VPN Connection

Last updated：2024-01-24 17:48:51

O VPN Connection é um serviço de conectividade privada de túnel de rede baseado em IPSEC que fornece uma conexão site a site criptografada e segura entre sites remotos, como IDCs e recursos no Tencent Cloud. O VPN Connection possibilita o acesso e a troca seguros de dados confidenciais em uma infraestrutura de rede compartilhada, como a rede pública (internet).

Para acessar os procedimentos comuns do VPN, consulte:

VPN Gateway

Gateway do cliente

Túnel VPN

Conexão do VPC ao IDC (roteamento baseado em política)

Conexão do IDC ao CCN

Direct Connect

Last updated：2024-01-24 17:48:51

O Direct Connect fornece uma abordagem rápida e segura para conectar as redes do Tencent Cloud com os IDCs locais. Ele é baseado em canais dedicados de TCP/IP de 2ª camada que terminam no gateway do Direct Connect baseado em nuvem. A partir daqui, é possível acessar os recursos do Tencent Cloud em várias regiões, oferecendo um ambiente de nuvem híbrida flexível e confiável.

Para acessar os procedimentos comuns do Direct Connection, consulte:

Início rápido

Gerenciamento de conexões

Gerenciamento dos gateways do Direct Connect

Túneis dedicados

Cloud Connect Network

Last updated：2024-01-24 17:48:51

O Cloud Connect Network (CCN) é um serviço de conectividade privada global em execução no backbone da rede do Tencent Cloud. O CCN permite a conectividade entre VPCs em todas as regiões, entre IDCs por meio de VPN ou links do Direct Connect, e até mesmo entre outros provedores de serviços ou nuvem. O roteamento de vários níveis do CCN tem aprendizado autônomo; portanto, quando a topologia da rede mudar, não será necessário executar os procedimentos tediosos com base na rede.

Para acessar os procedimentos comuns do CCN, consulte:

Interconexão de instância de rede em uma conta

Interconexão de instância de rede entre contas

Gerenciamento de instâncias

Gerenciamento de rotas

Gerenciamento de largura de banda

Gerenciamento de segurança
Grupos de segurança
Visão geral do grupo de segurança

Last updated：2024-01-24 17:55:51

Um grupo de segurança é um firewall virtual e oferece filtragem de pacotes de dados com monitoração de estado. Ele é usado para configurar o controle de acesso à rede da CVM, do Cloud Load Balancer, do TencentDB e de outras instâncias, além de controlar o seu tráfego de saída e de entrada. É um meio importante de isolamento de segurança de rede.
É possível configurar regras de grupo de segurança para permitir ou rejeitar o tráfego de entrada e de saída de instâncias dentro do grupo de segurança.

Funcionalidades

Um grupo de segurança é um grupo lógico. É possível adicionar CVM, ENI, TencentDB e outras instâncias na mesma região com os mesmos requisitos de isolamento de segurança de rede ao mesmo grupo de segurança.
Por padrão, as instâncias no mesmo grupo de segurança não são interconectadas, a menos que você permita especificando regras.
Os grupos de segurança têm estado. O tráfego de entrada que você permitiu pode se tornar automaticamente de saída e vice-versa.
É possível modificar as regras do grupo de segurança a qualquer momento, e as novas regras entrarão em vigor imediatamente.

Limites de uso

Para mais informações sobre as restrições e cotas de grupos de segurança, consulte Visão geral dos limites de uso.

Regras de grupos de segurança

Componentes

Uma regra de grupo de segurança consiste em:
Origem ou destino: o IP de origem para uma regra de entrada ou o IP de destino para uma regra de saída. Pode ser um endereço IP, um intervalo de IP ou um grupo de segurança. Para mais informações, consulte Adição de uma

regra de grupo de segurança.
Tipo de protocolo e porta de protocolo: o tipo de protocolo, como TCP, UDP etc.
Política: permitir ou rejeitar a solicitação de acesso.

Prioridades das regras

As regras em um grupo de segurança são priorizadas de cima para baixo. A regra no topo da lista tem a prioridade mais alta e entrará em vigor primeiro, já a regra na parte inferior tem a prioridade mais baixa e entrará em vigor por último.
Se houver um conflito de regras, a regra com a prioridade mais alta prevalecerá por padrão.
Quando o tráfego entra ou sai de uma instância vinculada a um grupo de segurança, as regras do grupo de segurança serão correspondidas sequencialmente de cima para baixo. Se uma regra for correspondida com êxito e entrar em vigor, as regras posteriores não serão correspondidas.

Vários grupos de segurança

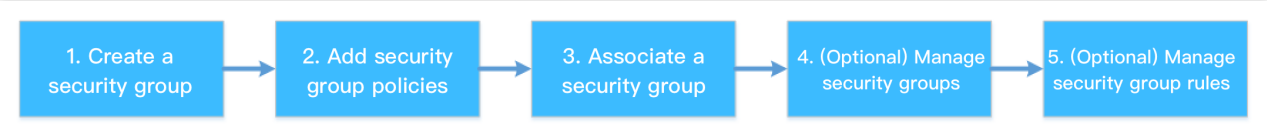
Uma instância pode ser vinculada a um ou vários grupos de segurança. Quando ela está vinculada a vários grupos de segurança, as regras do grupo serão correspondidas sequencialmente de cima para baixo. É possível ajustar as prioridades dos grupos de segurança a qualquer momento.

Modelos de grupos de segurança

Ao criar um grupo de segurança, é possível selecionar um dos dois modelos de grupos de segurança fornecidos pela Tencent Cloud:
Modelo que abre todas as portas: todo o tráfego de entrada e de saída terá permissão para passar.
Modelo que abre as portas principais: a porta TCP 22 (para login por SSH do Linux), as portas 80 e 443 (para serviço web), a porta 3389 (para login remoto do Windows), o protocolo ICMP (para comandos ping) e a rede privada serão abertos para a internet.
Nota:
Se esses modelos não atenderem às suas necessidades reais, é possível criar grupos de segurança personalizados. Para mais informações, consulte Criação de um grupo de segurança e Casos de aplicação de grupos de segurança.
Se for necessário proteger a camada de aplicativos (HTTP/HTTPS), ative o Web Application Firewall (WAF) da Tencent Cloud, que fornece segurança na web na camada de aplicativos para se defender contra vulnerabilidades na web, rastreadores mal-intencionados e ataques CC, protegendo seus sites e aplicativos web.

Como usar um grupo de segurança

A figura a seguir mostra como usar um grupo de segurança:



Práticas recomendadas de grupos de segurança

Criação de um grupo de segurança

Recomendamos que você especifique um grupo de segurança ao adquirir da CVM por API. Caso contrário, o grupo de segurança padrão será usado e não poderá ser excluído.
Se você precisar alterar a política de proteção da instância, recomendamos modificar as regras existentes em vez de criar um grupo de segurança novo.

Gerenciamento de regras

Exporte e faça backup das regras de grupos de segurança antes de modificá-las, para que você possa importá-las e restaurá-las se ocorrer um erro.
Para criar várias regras de grupos de segurança, use o modelo de parâmetros.

Associação de um grupo de segurança

É possível adicionar instâncias com os mesmos requisitos de proteção ao mesmo grupo de segurança, em vez de configurar um grupo de segurança separado para cada instância.
Não é recomendável vincular uma instância a muitos grupos de segurança, porque as regras em diferentes grupos podem entrar em conflito e resultar na desconexão da rede.

Criação de um grupo de segurança

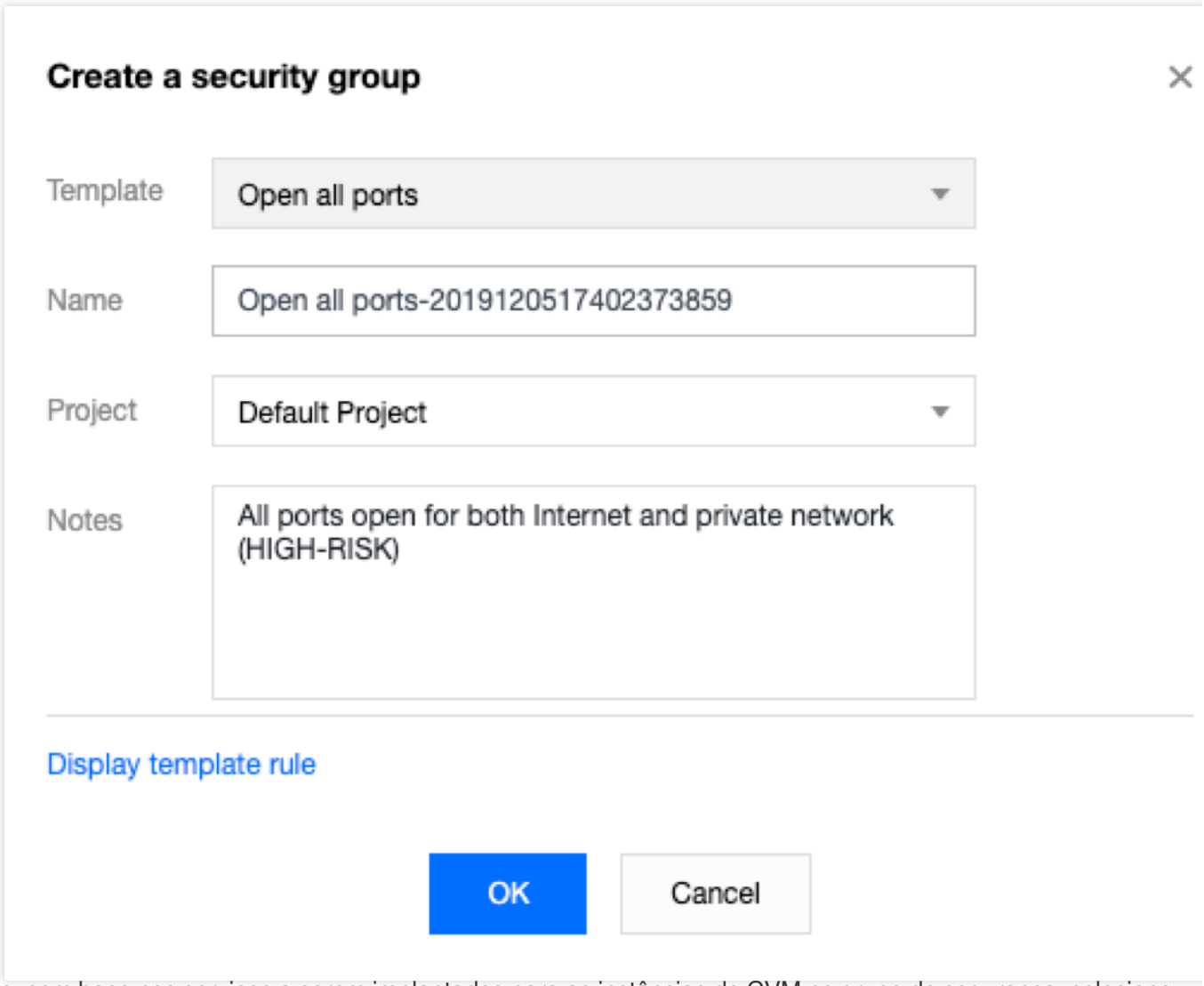
Last updated：2024-01-24 17:55:51

Cenário de operação

Um grupo de segurança é um firewall virtual para instâncias do CVM. Cada instância do CVM deve pertencer a pelo menos um grupo de segurança. O Tencent Cloud oferece dois modelos: **Open all ports to the Internet (Abrir todas as portas para a internet)** e **Open ports 22, 80, 443, and 3389 and ICMP protocol to the Internet (Abrir as portas 22, 80, 443 e 3389 e o protocolo ICMP para a internet)**. Com esses modelos, é possível criar um grupo de segurança padrão durante a criação de uma instância do CVM, caso ainda não o tenha criado.
Se você não deseja que sua instância do CVM se junte ao grupo de segurança padrão, é possível criar outro no console do CVM da seguinte maneira:

Etapas

1. Faça login no Console do CVM.
2. Na barra lateral esquerda, clique em **Security Group (Grupo de segurança)** para ter acesso à pagina de gerenciamento de grupos de segurança.
3. Na página de gerenciamento de grupos de segurança, selecione **Region (Região)** e clique em **+Create (+Criar)**.
4. Na janela **Create a security group (Criar um grupo de segurança)** exibida, conclua a configuração, conforme mostrado na figura abaixo:



Modelo: com base nos serviços a serem implantados para as instâncias do CVM no grupo de segurança, selecione um modelo apropriado para simplificar a configuração das regras do grupo, conforme descrito na tabela a seguir:

Modelo	Descrição	Cenário
Open all ports to the Internet (Abrir todas as portas para a internet)	Por padrão, todas as portas serão abertas para a internet e rede privada; o que, no entanto, pode incorrer em riscos de segurança.	-
Open ports 22, 80, 443, and 3389 and the ICMP protocol to the Internet (Abrir as portas 22, 80, 443 e 3389 e o protocolo ICMP para a internet)	Por padrão, as portas 22, 80, 443 e 3389 e o protocolo ICMP serão abertos para a internet. Além disso, todas as portas serão abertas para a rede privada.	O serviço Web precisa ser implantado para as instâncias no grupo de segurança.
Custom (Personalizado)	Depois de criar um grupo de segurança, você pode adicionar regras a ele conforme necessário. Para obter informações	-

	detalhadas sobre a operação, consulte Adição de regras de grupo de segurança.	

Name (Nome): personalize o nome de um grupo de segurança.

Project (Projeto): **Default project (Projeto padrão)** fica selecionado por padrão. Você também pode especificar outro projeto para facilitar o gerenciamento futuro.

Remarks (Observações): descreve resumidamente o grupo de segurança para facilitar o gerenciamento futuro.

5. Clique em **OK** para finalizar a criação do grupo de segurança.

Se você selecionar o modelo **Custom (Personalizado)** ao criar um grupo de segurança, clique em **Set rules now (Definir as regras agora)** após a criação para adicionar regras de grupo de segurança.

Adição de uma regra de grupos de segurança

Last updated：2024-01-24 17:55:51

Cenário de operação

Os grupos de segurança são usados para determinar se as solicitações de acesso da internet ou de redes privadas devem ser permitidas. Por questões de segurança, a negação de acesso é adotada na direção de entrada na maioria dos casos. Se você selecionar o modelo "Open all ports to the Internet (Abrir todas as portas para a internet)" ou "Open ports 22, 80, 443, and 3389 and the ICMP protocol to the Internet (Abrir as portas 22, 80, 443 e 3389 e o protocolo ICMP para a internet)" ao criar um grupo de segurança, o sistema adicionará automaticamente regras de grupo de segurança para algumas portas de comunicação com base no modelo selecionado.
Este documento descreve como adicionar regras de grupo de segurança para permitir ou proibir CVMs em um grupo de segurança de acessar a internet ou instâncias do VPC.

Observações

As regras de grupo de segurança são divididas em IPv4 e IPv6.
Open all ports (Abrir todas as portas) é aplicável às regras de grupo de segurança IPv4 e IPv6.

Pré-requisitos

Você criou um grupo de segurança.
Você sabe quais solicitações de acesso à internet ou rede privada precisam ser permitidas ou rejeitadas para sua instância do CVM. Para obter mais casos de uso de configurações de regras de grupo de segurança, consulte Casos de uso de grupos de segurança.

Etapas

1. Faça login no Console do CVM.
2. Na barra lateral esquerda, clique em **Security Group (Grupo de segurança)** para ter acesso à pagina de gerenciamento de grupos de segurança.
3. Na página de gerenciamento de grupos de segurança, selecione **Region (Região)** e localize a linha do grupo para o qual deseja definir regras.
4. Na coluna de operação, clique em **Modify Rules (Modificar regras)**.

5. Na
página
a de regras do grupo de segurança, clique em **Inbound rules (Regras de entrada)** e selecione um dos seguintes modos com base em suas necessidades reais para concluir a operação.

Nota：

Os exemplos de operação abaixo usam o modo 2 (adicionar regras).

Modo 1 (abrir todas as portas): é aplicável a cenários em que as regras do protocolo ICMP não precisam ser definidas e as operações podem ser feitas por meio das portas 22, 3389, 80, 443, 20 e 21, assim como do protocolo ICMP.

Modo 2 (adicionar regras): é aplicável a cenários em que vários protocolos de comunicação, como ICMP, precisam ser definidos.

6. Na janela **Add Inbound Rules (Adicionar regras de entrada)** que é exibida, defina as regras.

Os principais parâmetros necessários para adicionar uma regra são os seguintes:

Type (Tipo): o valor padrão é "Custom (Personalizado)". Você também pode selecionar outro modelo de regras de sistema, como "Windows login (Login no Windows)", "Linux login (Login no Linux)", "Ping", "HTTP (80)" ou "HTTPS (443)".

Source (Origem)/Destination (Destino): a origem (regras de entrada) ou o destino (regras de saída) do tráfego. Escolha uma das seguintes opções:

Origem/destino especificados	Descrição
Um endereço IPv4 ou intervalo de endereços IPv4	Especifique-o na notação CIDR (por exemplo, 203.0.113.0, 203.0.113.0/24 ou 0.0.0.0/0, em que 0.0.0.0/0 indica que todos os endereços IPv4 serão correspondidos).
Um endereço IPv6 ou um intervalo de endereços IPv6	Especifique-o na notação CIDR (por exemplo, FF05::B5, FF05:B5::/60, ::/0 ou 0::0/0, em que ::/0 ou 0::0/0 indica que todos os endereços IPv6 serão correspondidos).
Importar ID do grupo de segurança: você pode importar os seguintes IDs de grupos de segurança: ID do grupo de segurança Outro grupo de segurança	O grupo de segurança atual se refere aos CVMs associados ao grupo de segurança. Outro grupo de segurança se refere ao ID de outro grupo de segurança no mesmo projeto e na mesma região.
Importe o objeto de endereço IP ou o objeto de grupo de endereços IP no modelo de parâmetros.	-

Protocol port (Porta de protocolo): insira o tipo de protocolo e intervalo de portas ou importe uma porta de protocolo ou grupo de portas de protocolo no modelo de parâmetros.
Policy (Política): o valor padrão é "Permit (Permitir)".
Permit (Permitir): permite solicitações de acesso pela porta.
Reject (Rejeitar): descarta os pacotes de dados diretamente sem retornar nenhuma resposta.
Remarks (Observações): descreve resumidamente a regra para facilitar o gerenciamento futuro.
7. C
lique em
Finish (Finalizar). As regras de entrada são adicionadas ao grupo de segurança.
8. Na página de regra do grupo de segurança, clique em **Outbound Rules (Regras de saída)** e adicione regras de saída ao grupo de segurança referindo-se a Etapa 5 à Etapa 7.

Associação de instâncias do CVM a grupos de segurança

Last updated：2024-01-24 17:55:51

Cenário de operação

Um grupo de segurança é usado como um importante método de isolamento de segurança de rede para configurar o controle de acesso à rede para um ou mais CVMs. Você pode associar instâncias do CVM a um ou mais grupos de segurança com base nas suas necessidades empresariais. Este documento descreve como associar uma instância do CVM a um grupo de segurança no console.

Pré-requisitos

Uma instância do CVM foi criada.

Etapas

1. Faça login no Console do CVM.
2. Na barra lateral esquerda, clique em **Security Group (Grupo de segurança)** para ter acesso à pagina de gerenciamento de grupos de segurança.
3. Na página de gerenciamento de grupos de segurança, selecione **Region (Região)** e localize a linha do grupo para o qual deseja definir regras.
4. Na coluna de operação, clique em **Manage instance (Gerenciar instância)** para acessar a página **Associate with Instance (Associar à instância)**.
5. Nessa página, clique em **Add Association (Adicionar associação)**.
6. Na janela "Add Instance Association (Adicionar associação da instância)" exibida, selecione a instância a ser vinculada ao grupo de segurança e clique em **OK**.

Operações subsequentes

Para exibir todos os grupos de segurança que você criou em uma região, consulte a lista de grupos de segurança. Para obter informações detalhadas sobre a operação, consulte Exibição de um grupo de segurança.

Se você não deseja que uma instância do CVM pertença a um ou vários grupos de segurança, remova-a deles.
Para obter informações detalhadas sobre a operação, consulte Remoção de um grupo de segurança.
Se sua empresa não precisar mais de um ou vários grupos de segurança, é possível excluí-los. Depois de excluir um grupo de segurança, todas as regras nele também serão excluídas.
Para obter informações detalhadas sobre a operação, consulte Exclusão de um grupo de segurança.

Gerenciamento de grupos de segurança
Exibição de um grupo de segurança

Last updated：2024-01-24 17:55:51

Cenário de operação

Para exibir todos os grupos de segurança que você criou em uma determinada região, conclua as etapas a seguir.

Etapas

Exibição de todos os grupos de segurança

1. Faça login no Console do CVM.
2. Na barra lateral esquerda, clique em **Security Group (Grupo de segurança)** para ter acesso à pagina de gerenciamento de grupos de segurança.
3. Na página de gerenciamento de grupos de segurança, selecione **Region (Região)** para exibir todos os grupos de segurança na região.

Exibição de um grupo de segurança específico

É possível usar a funcionalidade de pesquisa na página de gerenciamento de grupos de segurança para exibir um grupo específico.

1. Faça login no Console do CVM.
2. Na barra lateral esquerda, clique em **Security Group (Grupo de segurança)** para ter acesso à pagina de gerenciamento de grupos de segurança.
3. Na página de gerenciamento de grupos de segurança, selecione **Region (Região)**.
4. No canto superior direito da lista de grupos de segurança da região, clique na caixa de texto de pesquisa e selecione um dos seguintes métodos para consultar o grupo de segurança de destino.

Selecione **Security Group ID (ID do grupo de segurança)**, insira o ID desejado e clique em


para consultar o grupo de segurança correspondente.

Selecione **Security Group Name (Nome do grupo de segurança)**, insira o nome desejado e clique em


para consultar o grupo de segurança correspondente.

Selecione **Label (Rótulo)**, insira o nome do rótulo e clique em


para consultar todos os grupos de segurança com o rótulo.

Outras operações

Para saber mais sobre a sintaxe para exibir um grupo de segurança específico, clique em


na caixa de texto de pesquisa para exibir a sintaxe relevante.

Remoção de um grupo de segurança

Last updated：2024-01-24 17:55:51

Cenário de operação

Você pode remover instâncias do CVM de um grupo de segurança com base nas suas necessidades empresariais.

Pré-requisitos

A instância do CVM a ser removida está associada a dois ou mais grupos de segurança.

Etapas

1. Faça login no Console do CVM.
2. Na barra lateral esquerda, clique em **Security Group (Grupo de segurança)** para ter acesso à pagina de gerenciamento de grupos de segurança.
3. Na página de gerenciamento de grupos de segurança, selecione **Region (Região)** e localize a linha do grupo cujas instâncias você deseja remover.
4. Na coluna de operação, clique em **Manage instances (Gerenciar instâncias)** para acessar a página **Associate with Instance (Associar à instância)**.
5. Nessa página, selecione a instância a ser removida e clique em **Remove from security group (Remover do grupo de segurança)**.
6. Na janela exibida, clique em **OK**.

Clone de um grupo de segurança

Last updated：2024-01-24 17:55:51

Cenário de operação

Pode ser necessário clonar um grupo de segurança nas seguintes situações:
Você criou um grupo de segurança denominado sg-A na região A e deseja aplicar as regras de sg-A às instâncias da região B. Neste caso, você pode clonar sg-A para a região B em vez de criar outro grupo na região B.
Sua empresa precisa executar uma nova regra de grupo de segurança. Nesse caso, você pode clonar o grupo de segurança original para backup.

Observações

Por padrão, apenas as regras de entrada e saída de um grupo de segurança são clonadas, mas não as instâncias associadas ao grupo.
Os grupos de segurança podem ser clonados entre projetos ou regiões.

Etapas

1. Faça login no Console do CVM.
2. Na barra lateral esquerda, clique em **Security Group (Grupo de segurança)** para ter acesso à pagina de gerenciamento de grupos de segurança.
3. Na página de gerenciamento de grupos de segurança, selecione **Region (Região)** e localize a linha do grupo a ser clonado.
4. Na coluna de operação, clique em **More (Mais)** > **Clone (Clonar)**.
5. Na janela "Clone Security Group (Clonar grupo de segurança)" exibida, selecione **Target Project (Projeto de destino)** e **Target Region (Região de destino)** para a clonagem, insira um **New Name (Novo nome)** para o grupo e clique em **OK**.

Exclusão de um grupo de segurança

Last updated：2024-01-24 17:55:51

Cenário de operação

Se sua empresa não precisar mais de um ou vários grupos de segurança, é possível excluí-los. Depois de excluir um grupo de segurança, todas as regras nele também serão excluídas.

Pré-requisitos

O grupo de segurança a ser excluído não está associado a nenhuma instância. Se estiver associado a instâncias, primeiro remova-as do grupo. Caso contrário, o grupo de segurança não poderá ser excluído. Para obter informações detalhadas sobre a operação, consulte Remoção de um grupo de segurança.

Etapas

1. Faça login no Console do CVM.
2. Na barra lateral esquerda, clique em **Security Group (Grupo de segurança)** para ter acesso à pagina de gerenciamento de grupos de segurança.
3. Na página de gerenciamento de grupos de segurança, selecione **Region (Região)** e localize a linha do grupo a ser excluído.
4. Na coluna de operação, clique em **More (Mais)** > **Delete (Excluir)**.
5. Na janela exibida, clique em **OK**.

Ajuste das prioridades dos grupos de segurança

Last updated：2024-01-24 17:55:51

Visão geral

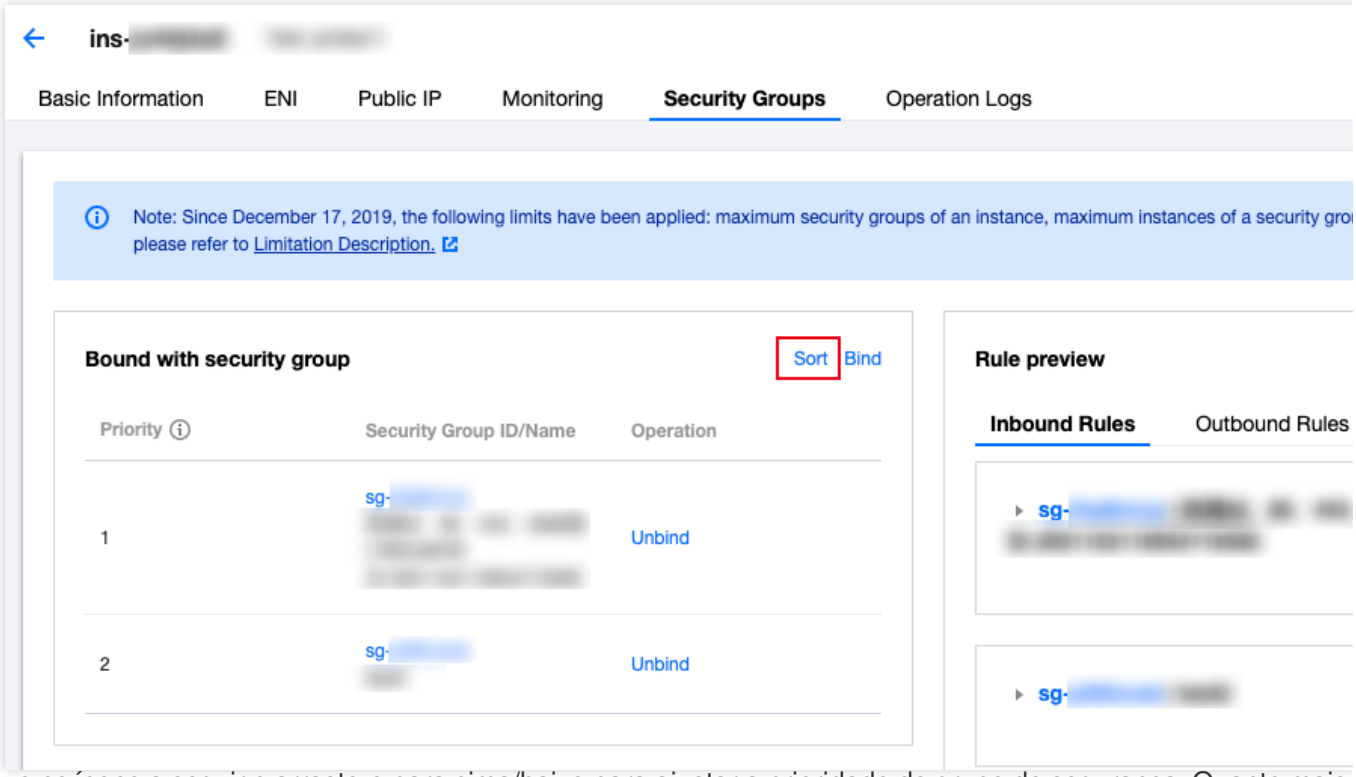
É possível vincular um ou mais grupos de segurança a da CVM. Se você vinculou vários grupos de segurança, eles são executados com base em suas prioridades. É possível ajustar as prioridades da seguinte forma.

Pré-requisitos

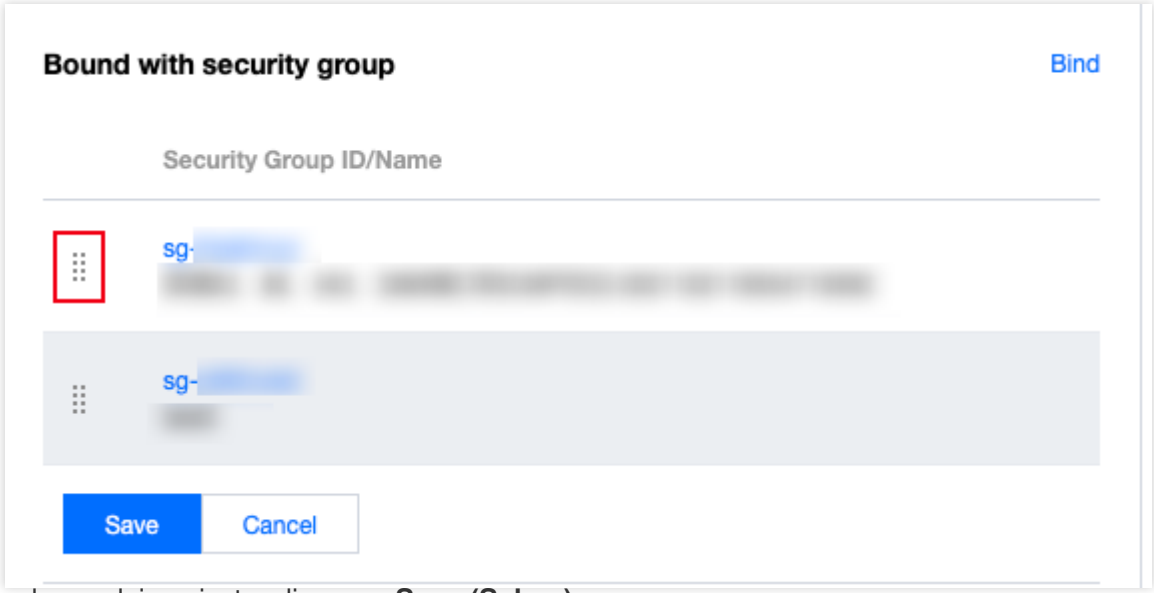
A instância da CVM está associada a dois ou mais grupos de segurança.

Instruções

1. Faça login no Console da CVM.
2. Na página de gerenciamento de instâncias, clique no ID da instância da CVM para acessar a página de detalhes.
3. Clique na guia **Security Groups (Grupos de segurança)** para acessar a página de gerenciamento do grupo de segurança.
4. No módulo **Bound Security Groups (Vincular grupos de segurança)**, clique em **Sort (Classificar)**.



5. Clique no ícone a seguir e arraste-o para cima/baixo para ajustar a prioridade do grupo de segurança. Quanto mais alta a posição, maior a prioridade do grupo de segurança.



6. Quando concluir o ajuste, clique em **Save (Salvar)**.

Gerenciamento de regras de grupo de segurança
Exibição de uma regra de grupos de segurança

Last updated：2024-01-24 17:55:51

Cenário de operação

Depois de adicionar uma regra de grupo de segurança, é possível visualizar seus detalhes no console.

Pré-requisitos

Você criou um grupo de segurança e adicionou regras de grupo de segurança ao grupo.
Para obter informações sobre como criar um grupo de segurança e adicionar regras a ele, consulte Adição de regras de grupo de segurança.

Etapas

1. Faça login no Console do CVM.
2. Na barra lateral esquerda, clique em **Security Group (Grupo de segurança)** para ter acesso à pagina de gerenciamento de grupos de segurança.
3. Na página de gerenciamento de grupos de segurança, selecione **Region (Região)** e localize o grupo cujas regras você deseja exibir.
4. Clique no ID ou nome do grupo de segurança de destino, para acessar a página de regras dele.
5. Na página de regras do grupo de segurança, clique na guia **Inbound Rules or Outbound Rules (Regras de entrada ou Regras de saída)** para exibir as regras de entrada ou saída do grupo.

Modificação de uma regra de grupos de segurança

Last updated：2024-01-24 17:55:51

Cenário de operação

Regras de grupo de segurança definidas incorretamente (por exemplo, aquelas que não restringem o acesso a portas especificadas) podem incorrer em graves riscos de segurança. Nesse caso, é possível modificar essas regras, a fim de garantir a segurança da rede das instâncias do CVM. Este documento descreve como modificar regras de grupo de segurança.

Pré-requisitos

Você criou um grupo de segurança e adicionou regras de grupo de segurança ao grupo.
Para obter informações sobre como criar um grupo de segurança e adicionar regras a ele, consulte Adição de regras de grupo de segurança.

Etapas

1. Faça login no Console do CVM.
2. Na barra lateral esquerda, clique em **Security Group (Grupo de segurança)** para ter acesso à pagina de gerenciamento de grupos de segurança.
3. Na pagina de gerenciamento de grupos de segurança, selecione **Region (Região)** e localize a linha do grupo cujas regras devem ser modificadas.
4. Na coluna de operação, clique em **Modify Rules (Modificar regras)** para acessar a página de regras do grupo de segurança.
5. Na página de regras do grupo de segurança, clique na guia **Inbound Rules or Outbound Rules (Regras de entrada ou Regras de saída)** com base na direção (entrada ou saída) das regras a serem modificadas.
6. Localize a regra que deseja modificar e clique em **Edit (Editar)** na coluna de operação para modificá-la.

Exclusão de uma regra de grupos de segurança

Last updated：2024-01-24 17:55:51

Cenário de operação

Se uma regra de grupo de segurança não for mais necessária, é possível excluí-la.

Pré-requisitos

Você criou um grupo de segurança e adicionou regras de grupo de segurança ao grupo.
Para obter informações sobre como criar um grupo de segurança e adicionar regras a ele, consulte Adição de regras de grupo de segurança.
Você confirmou que sua instância do CVM não precisa permitir ou proibir o acesso à internet ou à rede privada.

Etapas

1. Faça login no Console do CVM.
2. Na barra lateral esquerda, clique em **Security Group (Grupo de segurança)** para ter acesso à pagina de gerenciamento de grupos de segurança.
3. Na página de gerenciamento de grupos de segurança, selecione **Region (Região)** e localize a linha do grupo cujas regras devem ser excluídas.
4. Na coluna de operação, clique em **Modify Rules (Modificar regras)** para acessar a página de regras do grupo de segurança.
5. Na página de regras do grupo de segurança, clique na guia **Inbound Rules or Outbound Rules (Regras de entrada ou Regras de saída)** com base na direção (entrada ou saída) das regras a serem excluídas.
6. Localize a regra do grupo de segurança desejada e clique em **Delete (Excluir)**.
7. Na janela pop-up, clique em **OK**.

Importação de uma regra de grupos de segurança

Last updated：2024-01-24 17:55:51

Cenário de operação

É possível importar um arquivo de regras exportado para um grupo de segurança, a fim de criar ou restaurar rapidamente as regras dele.

Etapas

1. Faça login no Console do CVM.
2. Na barra lateral esquerda, clique em **Security Group (Grupo de segurança)** para ter acesso à pagina de gerenciamento de grupos de segurança.
3. Na página de gerenciamento de grupos de segurança, selecione **Region (Região)** e localize o grupo para o qual deseja importar regras.
4. Clique no ID ou nome do grupo de segurança, para acessar a sua respectiva página de regras.
5. Na página de regras do grupo de segurança, clique na guia **Inbound Rules or Outbound Rules (Regras de entrada ou Regras de saída)** com base na direção (entrada ou saída) das regras do grupo a serem importadas.
6. Na página da guia **Inbound Rules or Outbound Rules (Regras de entrada ou Regras de saída)**, clique em **Import Rules (Importar regras)**.
7. Na janela **Batch Import-Inbound/Outbound Rules (Importar em massa regras de entrada/saída)** exibida, selecione o arquivo de regras de entrada ou saída do modelo editado e clique em **Import (Importar)**.

Nota：
Se já existirem regras no grupo de segurança para o qual você deseja importar, recomendamos que você exporte essas regras primeiro. Caso contrário, as regras importadas substituirão as existentes.
Se não existir nenhuma regra no grupo de segurança para o qual você deseja importar, recomendamos que você primeiro baixe o arquivo de modelo, faça edições e depois importe.

Exportação de uma regra de grupos de segurança

Last updated：2024-01-24 17:55:51

Cenário de operação

É possível exportar as regras de um grupo de segurança para backup local.

Etapas

1. Faça login no Console do CVM.
2. Na barra lateral esquerda, clique em **Security Group (Grupo de segurança)** para ter acesso à pagina de gerenciamento de grupos de segurança.
3. Na página de gerenciamento de grupos de segurança, selecione **Region (Região)** e localize o grupo cujas regras devem ser exportadas.
4. Clique no ID ou nome do grupo de segurança, para acessar a sua respectiva página de regras.
5. Na página de regras do grupo de segurança, clique na guia **Inbound Rules or Outbound Rules (Regras de entrada ou Regras de saída)** com base na direção (entrada ou saída) das regras do grupo a serem exportadas.
6. Na página da guia **Inbound Rules or Outbound Rules (Regras de entrada ou Regras de saída)**, clique em

no canto superior direito, para baixar e salvar o arquivo de regras do grupo de segurança em um diretório local.

Casos de aplicação de grupos de segurança

Last updated：2024-01-24 17:55:51

Os grupos de segurança são usados para gerenciar se um Cloud Virtual Machine (CVM) fica acessível. É possível configurar regras de entrada e de saída para grupos de segurança para especificar se o seu servidor pode ser acessado ou pode acessar outros recursos de rede.
As regras padrão de entrada e de saída para grupos de segurança são as seguintes:
Para garantir a segurança dos dados, a regra de entrada para um grupo de segurança é uma política de rejeição que nega o acesso remoto de redes externas. Para tornar seu CVM acessível a recursos externos, é necessário permitir a regra de entrada para a porta correspondente.
A regra de saída para um grupo de segurança especifica se o CVM pode acessar recursos de redes externas. Se você selecionar **Open all Ports (Abrir todas as portas)** ou **Open Ports 22, 80, 443, 3389 and ICMP protocol (Abrir as portas 22, 80, 443, 3389 e o protocolo ICMP)**, a regra de saída para o grupo de segurança abre as portas para a internet. Se você selecionar uma regra de grupo de segurança personalizada, a regra de saída bloqueia todas as portas por padrão e é necessário configurar a regra de saída para permitir que a porta correspondente acesse recursos de redes externas.

Casos de uso comuns

Este documento descreve vários casos de uso comuns de grupos de segurança. Se algum dos casos abaixo atender aos seus requisitos, é possível definir seus grupos de segurança de acordo com a configuração recomendada para o caso de uso correspondente.

Cenário 1: conexão remota a um CVM do Linux por SSH

Caso: você criou um CVM do Linux e deseja se conectar a ele remotamente por SSH.
Solução: ao adicionar uma regra de entrada, defina **Type (Tipo)** como **Linux Login (Login no Linux)** e abra a porta TCP 22 para a internet, a fim de permitir o login do Linux por SSH.
É possível abrir todos os endereços IP ou um endereço IP especificado (ou intervalo de endereços IP) para a internet, conforme necessário. Isso permite que você configure os endereços IP de origem que podem acessar os CVMs por SSH de forma remota.

Direção	Tipo	Origem	Porta do protocolo	Política
Entrada	Login no Linux	Todos os endereços IP: 0.0.0.0/0 Endereço IP especificado: um endereço IP ou intervalo de endereços IP especificado	TCP: 22	Permitir

Cenário 2: conexão remota a um CVM do Windows por RDP

Caso: você criou um CVM do Windows e deseja conectar-se a ele remotamente por meio da Conexão de área de trabalho remota (RDP).
Solução: ao adicionar uma regra de entrada, defina **Type (Tipo)** como **Windows Login (Login no Windows)** e abra a porta TCP 3389 para a internet, a fim de habilitar o login remoto no Windows.
É possível abrir todos os endereços IP ou um endereço IP especificado (ou intervalo de endereços IP) para a internet, conforme necessário. Isso habilita que você configure os endereços IP de origem que podem acessar remotamente os CVMs por RDP.

Direção	Tipo	Origem	Porta do protocolo	Política
Entrada	Login no Windows	Todos os endereços IP: 0.0.0.0/0 Endereço IP especificado: um endereço IP ou intervalo de endereços IP especificado	TCP: 3389	Permitir

Cenário 3: execução de ping de um CVM a partir da internet

Caso: você criou um CVM e deseja verificar se a comunicação o CVM e outros CVMs está normal.
Solução: teste a conexão usando o programa de ping. Especificamente, ao adicionar uma regra de entrada, defina o **Type (Tipo)** como **Ping** e abra as portas do protocolo ICMP para a internet, a fim de permitir que outros CVMs acessem esse CVM por meio do ICMP.
É possível abrir todos os endereços IP ou um endereço IP especificado (ou intervalo de endereços IP) para a internet, conforme necessário. Isso permite que você configure os endereços IP de origem que podem acessar esse CVM por meio do ICMP.

Direção	Tipo	Origem	Porta do protocolo	Política
Entrada	Ping	Todos os endereços IP: 0.0.0.0/0 Endereço IP especificado: um endereço IP ou intervalo de endereços IP especificado	ICMP	Permitir

Cenário 4: login remoto em um CVM por meio do Telnet

Caso: você deseja fazer login remotamente em um CVM por meio do Telnet.
Solução: ao adicionar uma regra de entrada, configure a seguinte regra de grupo de segurança:

Direção	Tipo	Origem	Porta do protocolo	Política
Entrada	Personalizado	Todos os endereços IP: 0.0.0.0/0 Endereço IP especificado: um endereço IP ou intervalo de endereços IP especificado	TCP: 23	Permitir

Cenário 5: autorização de acesso a um serviço Web por meio de HTTP ou HTTPS

Caso: você criou um site e deseja permitir que os usuários o acessem por meio de HTTP ou HTTPS.

Solução: ao adicionar uma regra de entrada, configure as regras de grupo de segurança, conforme necessário:

Permitir que todos os endereços IP na internet acessem este site

Direção	Tipo	Origem	Porta do protocolo	Política
Entrada	HTTP (80)	0.0.0.0/0	TCP: 80	Permitir
Entrada	HTTPS (443)	0.0.0.0/0	TCP: 443	Permitir

Permitir que alguns endereços IP na internet acessem este site

Direção	Tipo	Origem	Porta do protocolo	Política
Entrada	HTTP (80)	Endereço IP ou intervalo de endereços IP que tem permissão para acessar seu site	TCP: 80	Permitir
Entrada	HTTPS (443)	Endereço IP ou intervalo de endereços IP que tem permissão para acessar seu site	TCP: 443	Permitir

Cenário 6: permissão para um endereço IP externo acessar uma porta especificada

Caso: você implantou um serviço e deseja que a porta de serviços especificada (como a porta 1101) seja acessível externamente.

Solução: ao adicionar uma regra de entrada, defina o **Type (Tipo)** como **Custom (Personalizado)** e abra a porta TCP 1101 para a internet, a fim de que recursos externos acessem a porta de serviços especificada.

É possível abrir todos os endereços IP ou um endereço IP especificado (ou intervalo de endereços IP) para a internet, conforme necessário. Isso permite que o endereço IP de origem acesse a porta de serviços especificada.

Direção	Tipo	Origem	Porta do protocolo	Política
Entrada	Personalizado	Todos os endereços IP: 0.0.0.0/0 Endereço IP especificado: um endereço IP ou intervalo de endereços IP especificado	TCP: 1101	Permitir

Cenário 7: negação do acesso a uma porta especificada por endereços IP externos

Caso: você implantou um serviço e deseja bloquear o acesso externo a uma porta de serviços especificada (como a porta 1102).

Solução: ao adicionar uma regra de entrada, defina o **Type (Tipo)** como **Custom (Personalizado)**, configure a porta TCP 1102 e defina a **Policy (Política)** como **Reject (Rejeitar)**, a fim de negar o acesso externo à porta de serviços especificada.

Direção	Tipo	Origem	Porta do protocolo	Política
Entrada	Personalizado	Todos os endereços IP: 0.0.0.0/0 Endereço IP especificado: um endereço IP ou intervalo de endereços IP especificado	TCP: 1102	Rejeitar

Cenário 8: permissão para um CVM acessar apenas um endereço IP externo especificado

Caso: você deseja que seu CVM acesse apenas um endereço IP externo especificado.

Solução: adicione duas regras de saída de grupo de segurança, referindo-se às seguintes configurações:

Permitir que a instância do CVM acesse um endereço IP público especificado

Não permitir que a instância do CVM acesse endereços IP públicos por meio de nenhum protocolo

Nota：

A regra que permite o acesso deve ter uma prioridade mais alta do que a regra que nega o acesso.

Direção	Tipo	Origem	Porta do protocolo	Política
Saída	Personalizado	O endereço IP público especificado que pode ser acessado pelo CVM	O protocolo e a porta necessários	Permitir
Saída	Personalizado	0.0.0.0/0	Todos	Rejeitar

Cenário 9: negação para um CVM acessar apenas um endereço IP externo especificado

Caso: você não deseja que seu CVM acesse um endereço IP externo especificado.

Solução: adicione uma regra de grupo de segurança referindo-se à seguinte configuração:

Direção	Tipo	Origem	Porta do protocolo	Política
Saída	Personalizado	O endereço IP público especificado que você não deseja que seja acessado pelo CVM	Todos	Rejeitar

Cenário 10: upload ou download de um arquivo de um CVM por FTP

Caso: você deseja fazer upload ou download de um arquivo de um CVM usando um programa FTP.

Solução: adicione uma regra de grupo de segurança referindo-se à seguinte configuração:

Direção	Tipo	Origem	Porta do protocolo	Política
Entrada	Personalizado	0.0.0.0/0	TCP: 20-21	Permitir

Combinação de vários cenários

Em um cenário real, pode ser útil configurar várias regras de grupo de segurança com base nos requisitos de serviço, por exemplo, configurar regras de entrada ou saída ao mesmo tempo. Um CVM pode estar vinculado a um ou mais grupos de segurança. Quando um CVM está vinculado a vários grupos de segurança, eles são combinados e executados em ordem decrescente de prioridade. É possível ajustar as prioridades dos grupos de segurança a qualquer momento.

Portas comuns do servidor

Last updated：2024-01-24 17:55:51

Veja abaixo as descrições das portas de servidor comuns. Para obter mais informações sobre as portas de aplicativos de serviços para Windows, consulte o documento oficial da Microsoft (Visão geral do serviço e requisitos de porta de rede para Windows).

Número da porta	Serviço	Descrição
21	FTP	Uma porta de servidor FTP aberta para upload e download.
22	SSH	A porta 22 é a porta SSH. É usada para conectar remotamente a servidores do Linux no modo CLI.
25	SMTP	Porta aberta do servidor SMTP para envio de e-mails.
80	HTTP	Esta porta é usada para serviços Web, como IIS, Apache e Nginx, para fornecer acesso externo.
110	POP3	A porta 110 fica aberta para o serviço POP3 (protocolo de e-mail 3).
137, 138, 139	Protocolo NetBIOS	As portas 137 e 138 são portas UDP para transferência de arquivos pelos Meus locais de rede. Porta 139: as conexões da porta 139 tentam acessar o serviço NetBIOS/SMB. Esse protocolo é usado para compartilhamento de arquivos e impressoras no Windows e SAMBA.
143	IMAP	A porta 143 é usada principalmente para o protocolo IMAP v2, um protocolo para receber e-mails semelhante ao POP3.
443	HTTPS	Uma porta de navegação na web. HTTPS é outro tipo de HTTP que fornece criptografia e transmissão por portas seguras.
1433	SQL Server	A porta 1433 é a padrão do SQL Server. O SQL Server usa duas portas: porta 1433 para TCP e porta 1434 para UDP. A porta 1433 é usada para o SQL Server para fornecer serviços externos, enquanto a porta 1434 é usada para responder ao solicitante em relação a qual porta TCP/IP está sendo usada pelo SQL Server.
3306	MySQL	A porta 3306 é a padrão para bancos de dados MySQL e é usada para fornecer serviços externos.
3389	Serviços de área de trabalho	A porta 3389 é a porta para serviço de área de trabalho remota do Windows 2000/2003 Server, por meio da qual você pode se conectar a um servidor remoto usando a ferramenta de conexão de área de trabalho remota.

	remota do Windows Server	
8080	Porta proxy	Semelhante à porta 80, a porta 8080 é usada para o serviço de proxy WWW para navegação na web. A extensão do número de porta ":8080" costuma ser adicionada ao URL quando os usuários acessam um site ou usam um servidor proxy. Além disso, após a instalação do servidor Web Apache Tomcat, a porta de serviços padrão é a 8080.

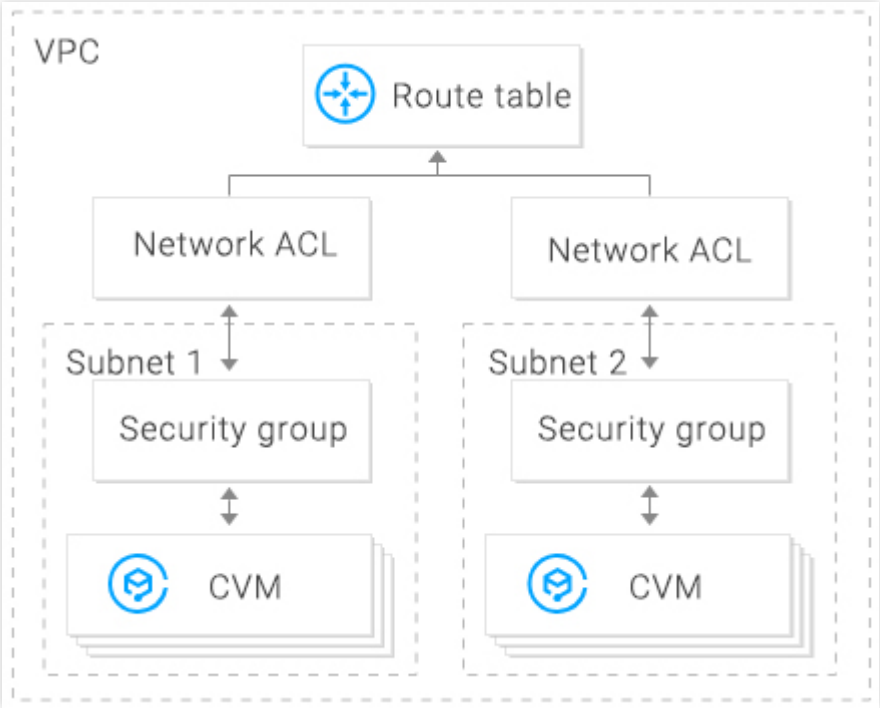
ACL de rede
Visão geral das regras

Last updated：2024-01-24 17:55:51

A lista de controle de acesso (ACL) de rede é uma camada opcional de segurança que limita o tráfego de e para as sub-redes com precisão de protocolo e porta.

Visão geral

Você pode associar uma ACL de rede a várias sub-redes para manter o tráfego e controlar com precisão sua entrada e saída, definindo regras de entrada e saída.
Por exemplo, quando você hospeda um aplicativo da web com várias camadas em uma instância da VPC da Tencent Cloud e cria sub-redes diferentes para serviços de camada da web, camada lógica e camada de dados, é possível usar uma ACL de rede para garantir que as sub-redes da camada da web e da camada de dados não podem acessar umas às outras, mas apenas a sub-rede da camada lógica pode acessar as sub-redes da camada da web e da camada de dados.



Regras de ACL

Quando uma regra de ACL de rede for adicionada ou excluída, a alteração será aplicada automaticamente às sub-redes associadas.
Você pode configurar regras de ACL de rede de entrada e de saída. Cada regra consiste em:
IP de origem/IP de destino: insira o IP de origem para uma regra de entrada ou o IP de destino para uma regra de saída. Formatos aceitos:
IP único: como “192.168.0.1” ou “FF05::B5”
Bloco CIDR: como “192.168.1.0/24” ou “FF05:B5::/60”
Todos os endereços IPv4: “0.0.0.0/0”
Protocol type (Tipo de protocolo): indica os tipos de protocolo que uma regra de ACL permite ou nega, por exemplo, TCP e UDP.
Port (Porta): indica a porta de origem ou destino do tráfego. Formatos aceitos:
Porta única: como “22” ou “80”
Intervalo de portas: como “1-65535” ou “100-20000”
Todas as portas: todas
Policy (Política): indica se deve permitir ou negar a solicitação de acesso.

Regras padrão

Depois de criada, cada ACL de rede tem duas regras padrão que não podem ser modificadas ou excluídas, com a prioridade mais baixa.
Regra de entrada padrão

Tipo de protocolo	Porta	IP de origem	Política	Descrição
Todas	Todas	0.0.0.0/0	Negar	Nega todo o tráfego de entrada.

Regra de saída padrão

Tipo de protocolo	Porta	IP de destino	Política	Descrição
Todas	Todas	0.0.0.0/0	Negar	Nega todo o tráfego de saída.

Prioridades das regras

As regras de uma ACL de rede são priorizadas de cima para baixo. A regra no topo da lista tem a prioridade mais alta e entrará em vigor primeiro, já a regra na parte inferior tem a prioridade mais baixa e entrará em vigor por último.
Se houver um conflito de regras, a regra com a prioridade mais alta prevalecerá por padrão.

Quando o tráfego entrar ou sair de uma sub-rede vinculada a uma ACL de rede, as regras de ACL de rede serão correspondidas sequencialmente de cima para baixo. Se uma regra for correspondida com êxito e entrar em vigor, as regras posteriores não serão correspondidas.

Exemplo de aplicação

Para permitir que todos os endereços IP de origem acessem todas as portas de CVMs em uma sub-rede associada a uma ACL de rede, e negar que o endereço IP de origem HTTP de `192.168.200.11/24` acesse a porta 80, adicione as seguintes duas regras de ACL de rede para tráfego de entrada:

Tipo de protocolo	Porta	IP de origem	Política	Descrição
HTTP	80	192.168.200.11/24	Negar	Nega que este endereço IP de serviços HTTP acesse a porta 80.
Todos	Todas	0.0.0.0/0	Permitir	Permite que todos os endereços IP de origem acessem todas as portas.

Grupos de segurança vs. ACLs de rede

Item	Grupo de segurança	ACL de rede
Limitação de tráfego	Limitação de tráfego no nível de instâncias, como CVM e banco de dados	Limitação de tráfego no nível de sub-redes
Regra	Regras permitir e negar	Regras permitir e negar
Com estado e sem estado	Com estado: o tráfego retornado é permitido automaticamente, sem estar sujeito a nenhuma regra.	Sem estado: o tráfego retornado deve ser explicitamente permitido pelas regras.
Tempo efetivo	As regras são aplicadas a uma instância, como da CVM ou TencentDB, apenas se você especificar um grupo de segurança ao criar a instância ou associar um grupo de segurança à instância após sua criação.	As regras de ACL são aplicadas automaticamente a todas as instâncias, como instâncias da CVM e do TencentDB na sub-rede associada.
Prioridade da regra	Se houver um conflito de regras, a regra com a prioridade mais alta prevalecerá por padrão.	Se houver um conflito de regras, a regra com a prioridade mais alta prevalecerá por padrão.

Limites

Last updated：2024-01-24 17:55:51

Limites de uso

Uma ACL de rede pode ser vinculada a várias sub-redes.
As ACLs de rede não têm estado. Portanto, é necessário definir regras de saída e regras de entrada, respectivamente.
As ACLs de rede não afetam a intercomunicação de rede privada entre as instâncias do CVM nas sub-redes associadas.

Limites de cota

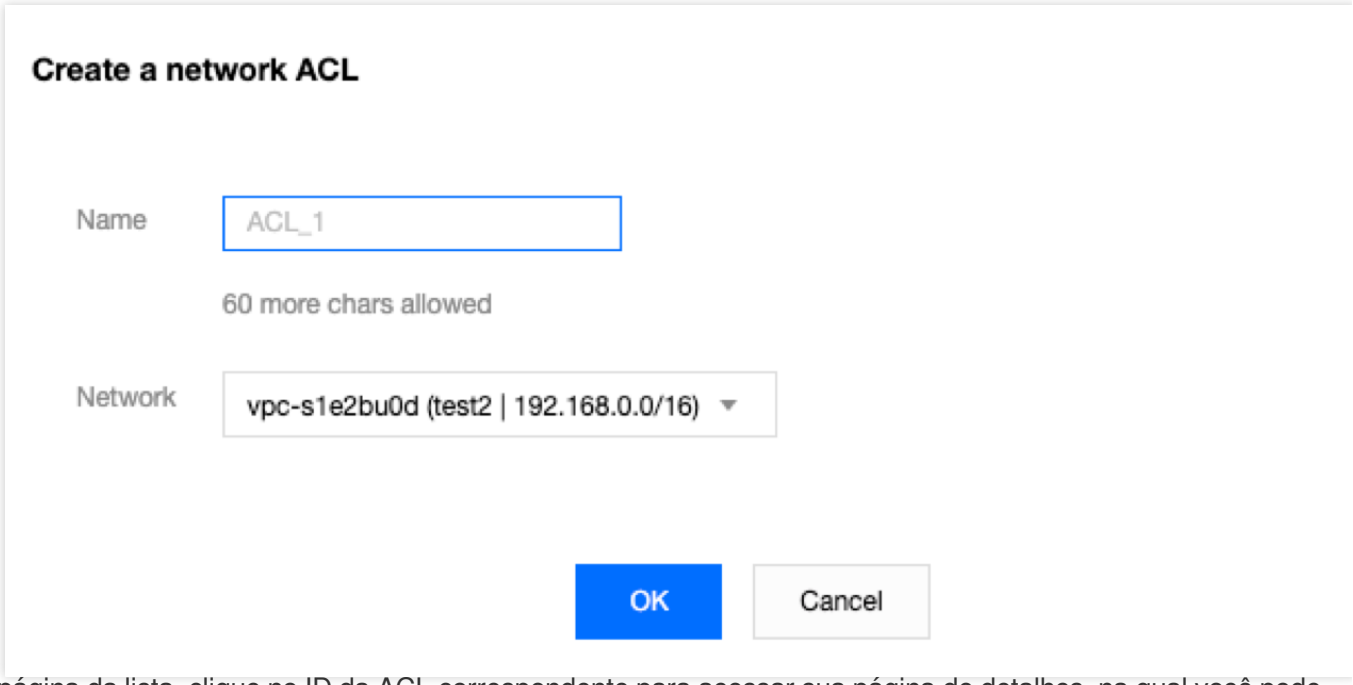
Recurso	Limite
Quantidade de ACLs de rede em cada VPC	50
Quantidade de regras por ACL de rede	Entrada: 20 Saída: 20
Quantidade de ACLs de rede associadas a cada sub-rede	1

Gerenciamento de ACLs de rede

Last updated：2024-01-24 17:55:51

Criação de ACLs de rede

1. Faça login no Console do VPC.
2. Clique em **Security (Segurança)** -> **Network ACL (ACL de rede)** no diretório à esquerda para acessar a página de gerenciamento.
3. Selecione a região e o VPC na parte superior da lista e clique em **+New (+Novo)**.
4. Digite o nome na janela pop-up, selecione o VPC ao qual ela pertence e clique em **OK**.

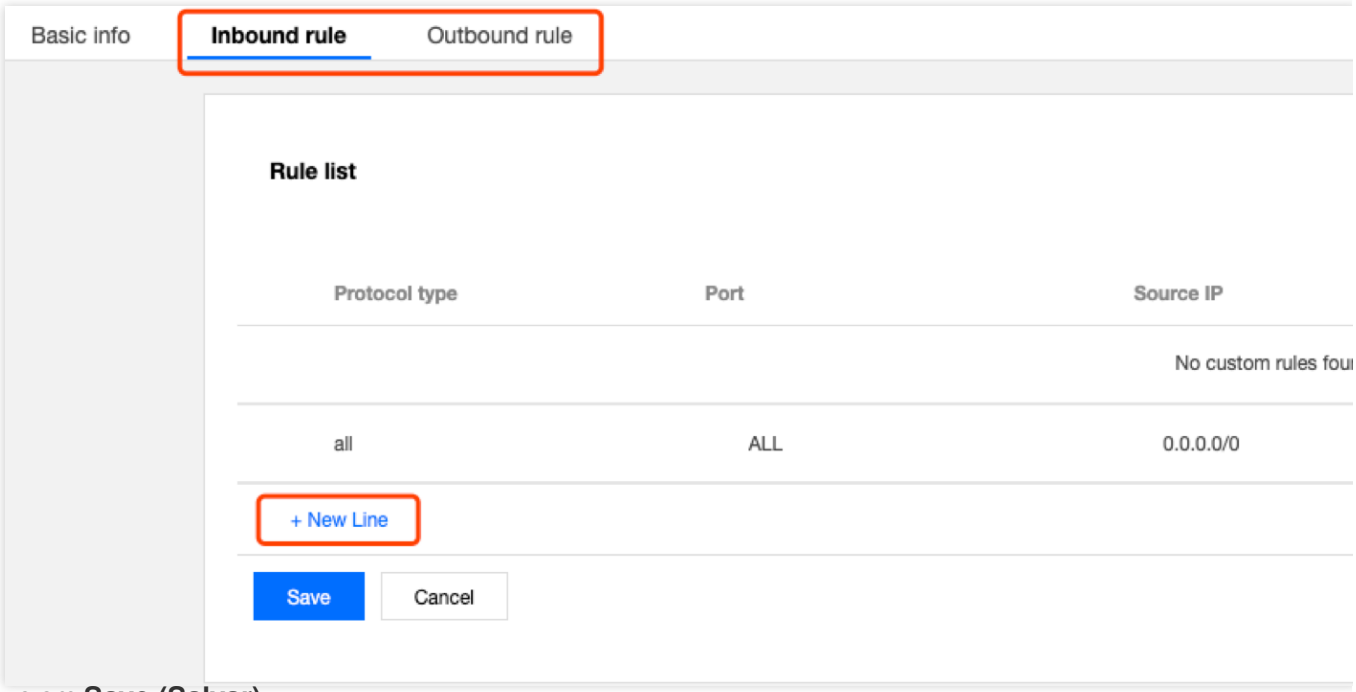


5. Na página da lista, clique no ID da ACL correspondente para acessar sua página de detalhes, na qual você pode adicionar regras de ACL e associá-las a sub-redes.

Adição de regras de ACL de rede

1. Faça login no Console do VPC.
2. Clique em **Security (Segurança)** -> **Network ACL (ACL de rede)** no diretório à esquerda para acessar a página de gerenciamento.
3. Localize na lista a ACL de rede a ser modificada e clique em seu ID para acessar a página de detalhes.
4. Para adicionar uma regra de saída/entrada, clique em **Outbound Rules (Regras de saída)** ou **Inbound Rules (Regras de entrada)** -> **Edit (Editar)** -> **New Line (Nova linha)**, selecione o tipo de protocolo, insira a porta e o

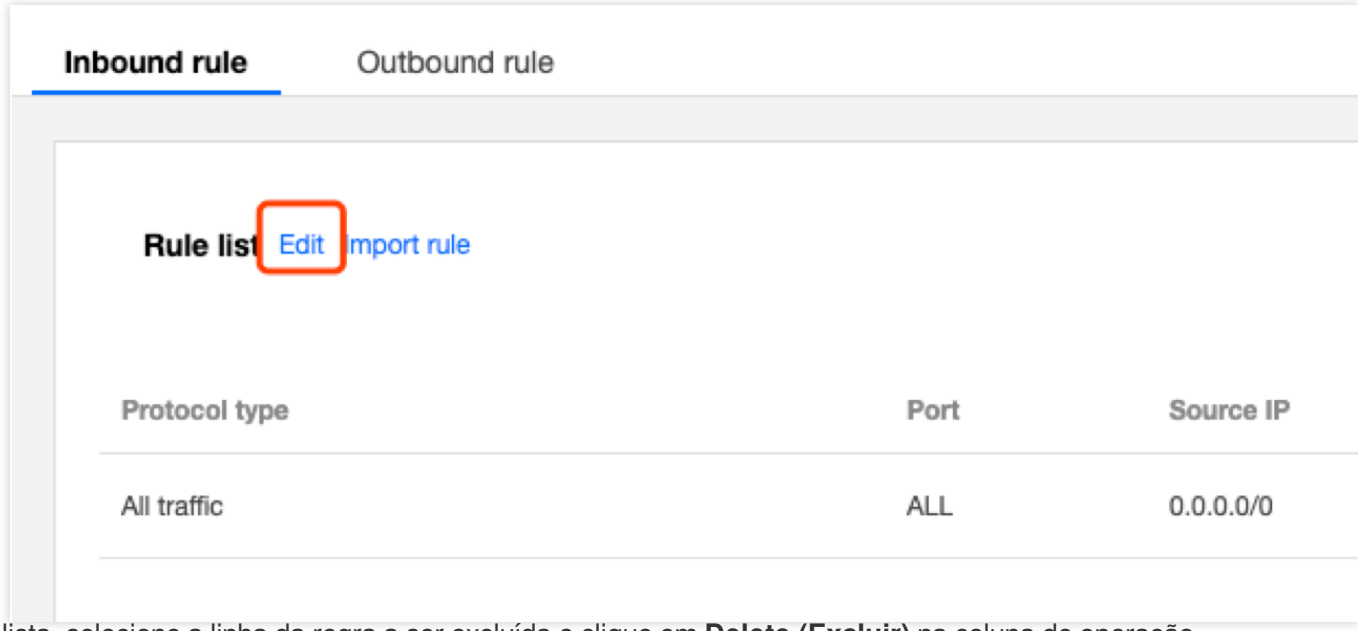
endereço IP de origem e selecione a política.
Protocol type (Tipo de protocolo): indica os tipos de protocolo que uma regra de ACL permite ou rejeita, por exemplo, TCP e UDP.
Port (Porta): indica a porta de origem do tráfego, que pode ser uma única porta ou um segmento de portas, por exemplo, porta 80 ou portas 90 a 100.
Source IP address (Endereço IP de origem): indica o endereço IP de origem ou intervalo de IP de tráfego que aceita o intervalo de IP ou bloco CIDR, por exemplo, `10.20.3.0` ou `10.0.0.2/24`.
Policy (Política): permite ou rejeita a solicitação de acesso.



5. Clique em **Save (Salvar)**.

Exclusão de regras de ACL de rede

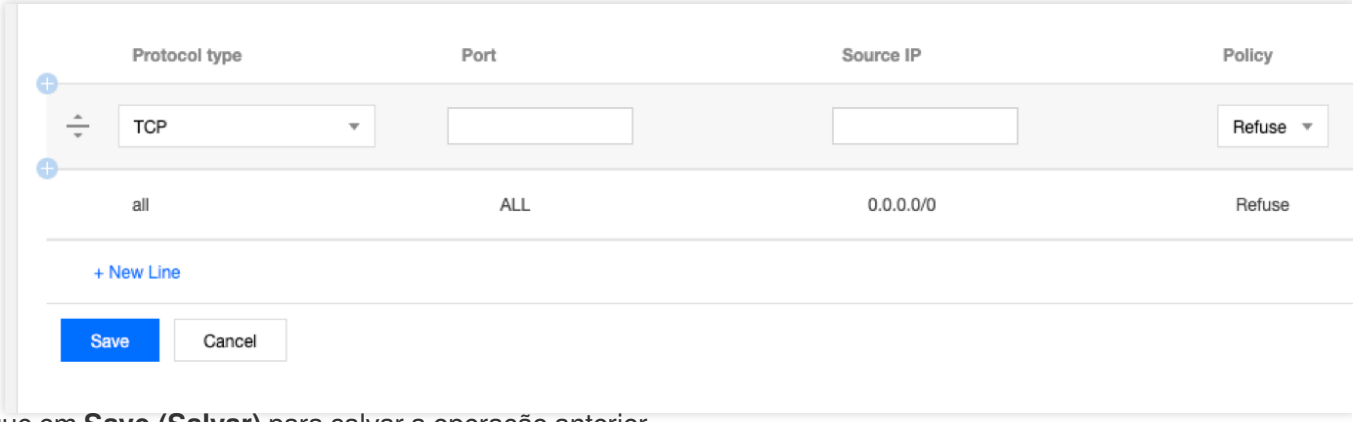
1. Faça login no Console do VPC.
2. Clique em **Security (Segurança)** -> **Network ACL (ACL de rede)** no diretório à esquerda para acessar a página de gerenciamento.
3. Localize na lista a ACL de rede a ser excluída e clique em seu ID para acessar a página **Basic Information (Informações básicas)**.
4. Clique na guia **Inbound Rules (Regras de entrada)** ou na guia **Outbound Rules (Regras de saída)** para acessar a página **Rules List (Lista de regras)**.
5. Clique em **Edit (Editar)**. O processo de exclusão de regras de entrada é igual ao de exclusão de regras de saída. A exclusão de regras de entrada é usada conforme o exemplo aqui.



6. Na lista, selecione a linha da regra a ser excluída e clique em **Delete (Excluir)** na coluna de operação.

Nota:

Esta regra de ACL ficará marcada em cinza. Se você a excluiu acidentalmente, clique em **Recover the deleted rule (Recuperar a regra excluída)** na coluna de operação para restaurar a regra.



7. Clique em **Save (Salvar)** para salvar a operação anterior.

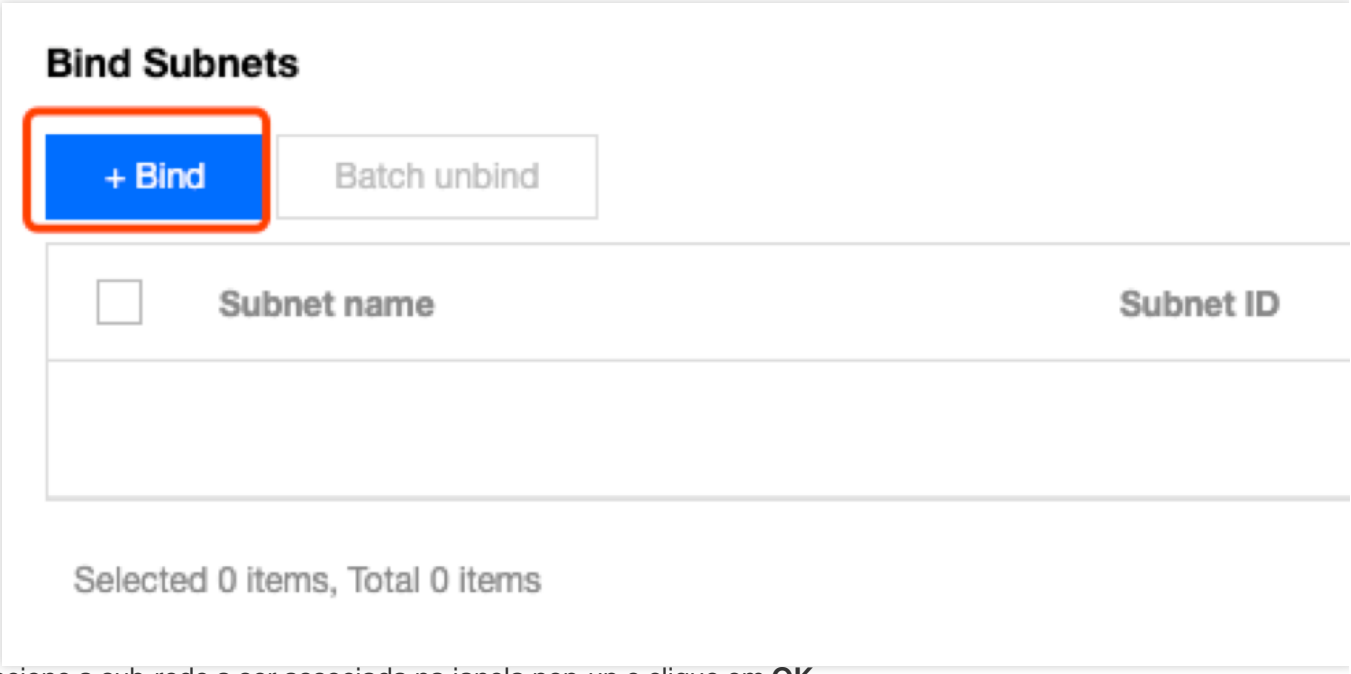
Atenção:

A exclusão ou restauração da regra de ACL só entrará em vigor depois que você salvar a operação.

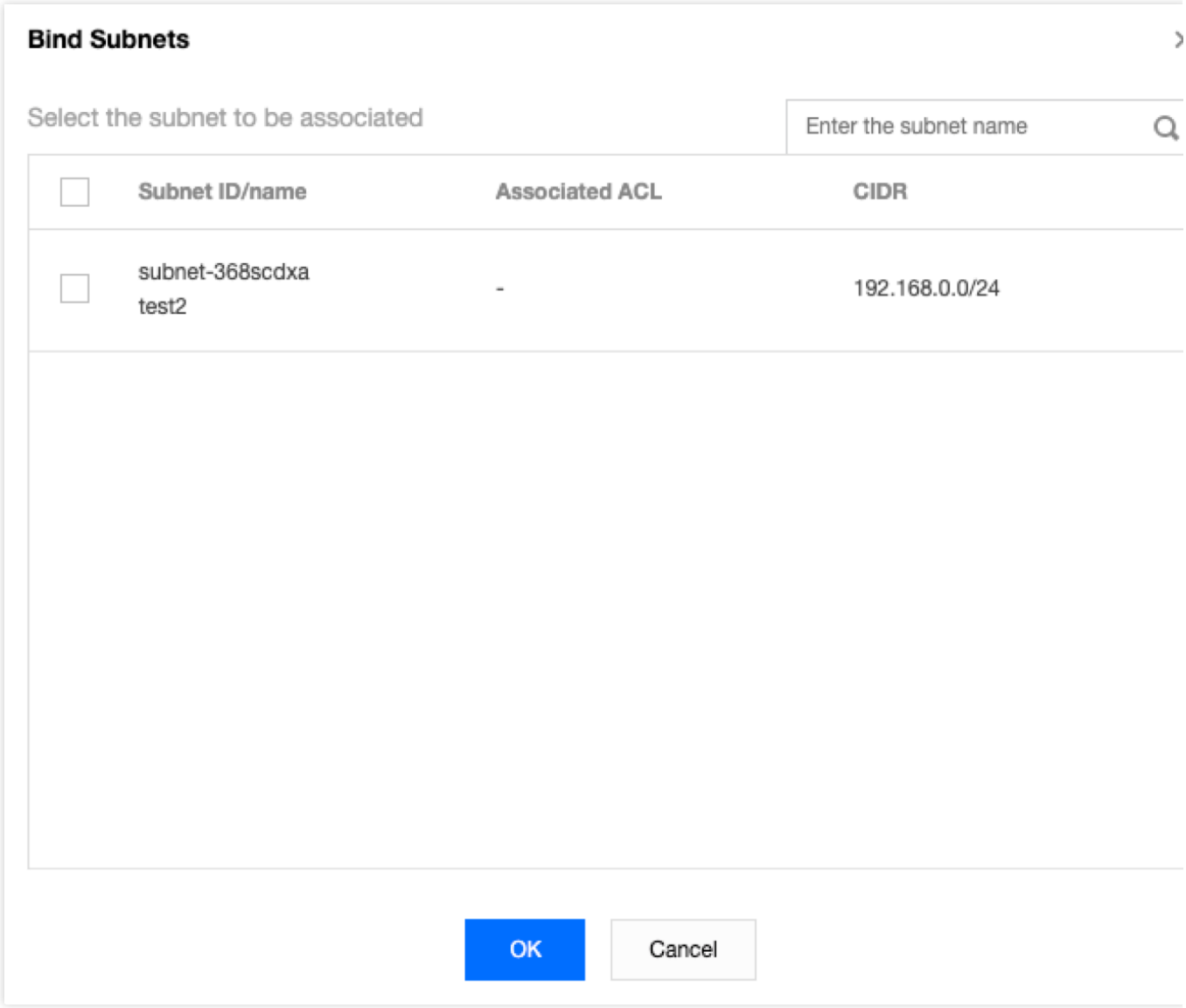
Associação de ACLs de rede a sub-redes

1. Faça login no Console do VPC.
2. Clique em **Security (Segurança)** -> **Network ACL (ACL de rede)** no diretório à esquerda para acessar a página de gerenciamento.
3. Localize na lista a ACL de rede a ser associada e clique em seu ID para acessar a página de detalhes.

4. Na página **Basic Information (Informações básicas)**, clique em **Add Association (Adicionar associação)** no módulo **Associated Subnets (Sub-redes associadas)**.



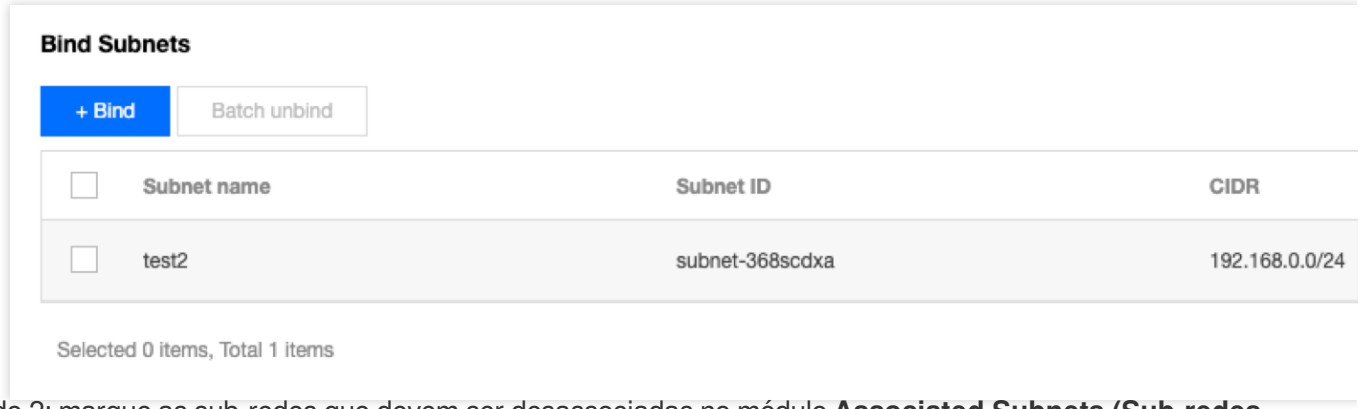
5. Selecione a sub-rede a ser associada na janela pop-up e clique em **OK**.



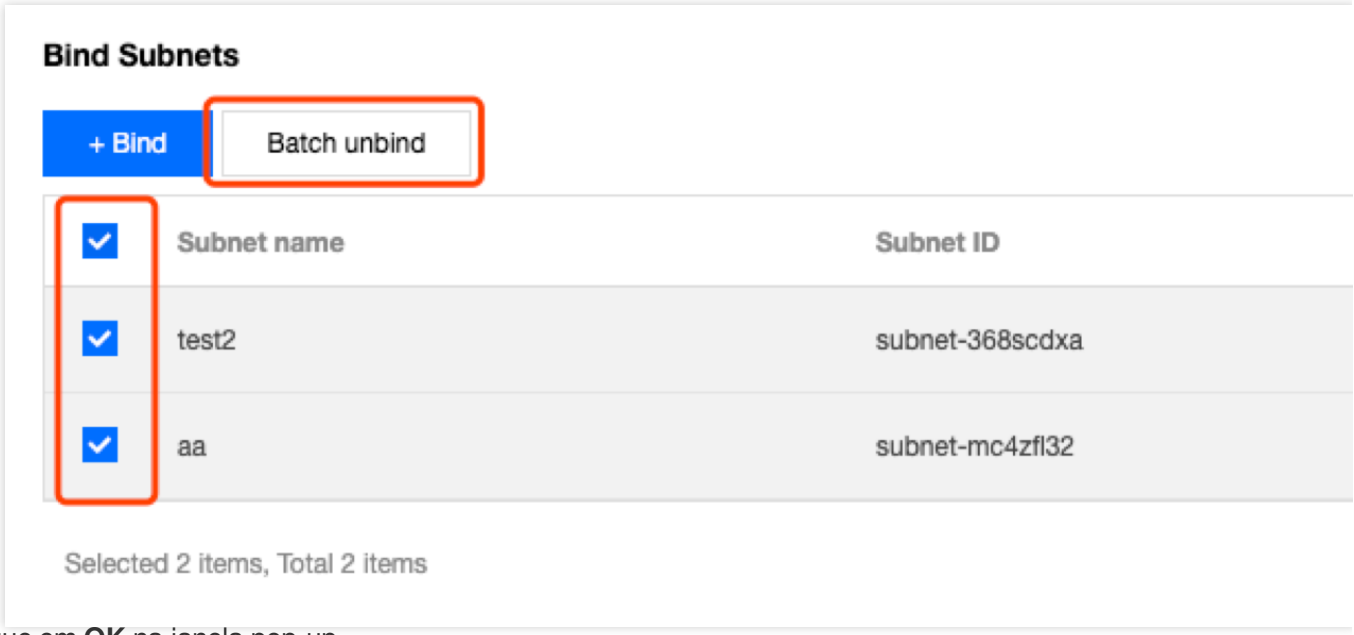
Desassociação de ACLs de rede de sub-redes

1. Faça login no Console do VPC.
2. Clique em **Security (Segurança)** -> **Network ACL (ACL de rede)** no diretório à esquerda para acessar a página de gerenciamento.
3. Localize na lista a ACL de rede a ser desassociada e clique em seu ID para acessar a página de detalhes.
4. Existem diferentes métodos para desassociar ACLs de sub-redes:

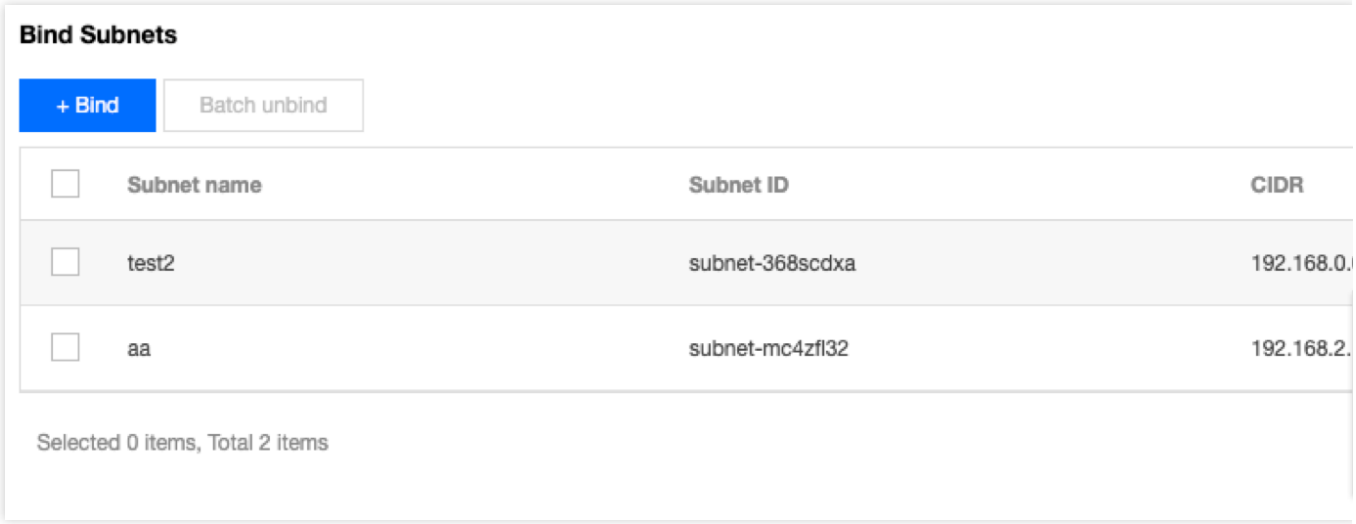
Método 1: localize a sub-rede que deve ser desassociada no módulo **Associated Subnets (Sub-redes associadas)** na página **Basic Information (Informações básicas)** e clique em **Disassociate (Desassociar)**.



Método 2: marque as sub-redes que devem ser desassociadas no módulo **Associated Subnets (Sub-redes associadas)** na página **Basic Information (Informações básicas)** e clique em **Batch Disassociate (Desassociar em lote)**.



5. Clique em **OK** na janela pop-up.

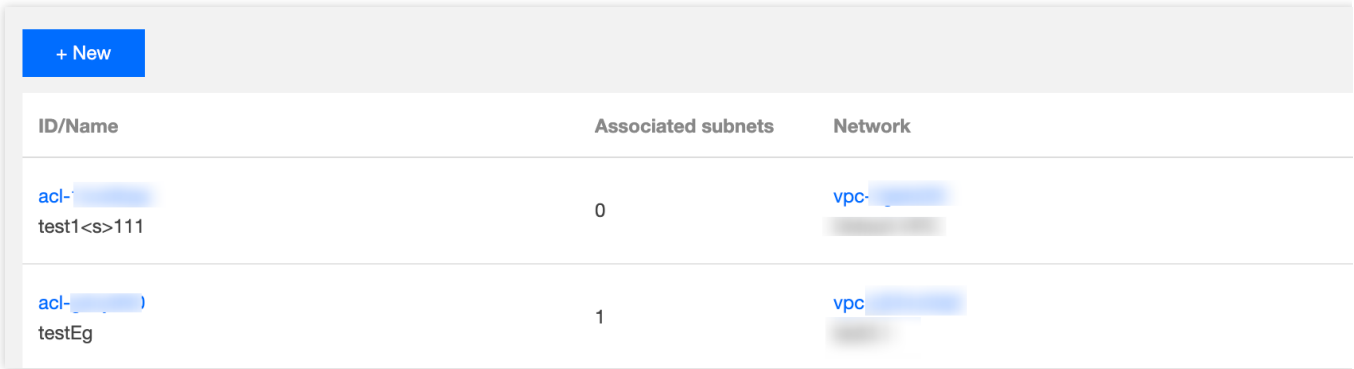


Exclusão de ACLs de rede

1. Faça login no Console do VPC.
2. Clique em **Security (Segurança)** -> **Network ACL (ACL de rede)** no diretório à esquerda para acessar a página de gerenciamento.
3. Selecione a região e o VPC.
4. Na lista, localize a ACL de rede a ser excluída, clique em **Delete (Excluir)** e confirme a exclusão. A ACL de rede e todas as suas regras serão excluídas.

Nota:

Se a opção **Delete (Excluir)** ficar marcada em cinza, como para a ACL de rede `testEg` na figura abaixo, isso indica que a ACL de rede está atualmente associada a uma sub-rede. Você precisará desassociá-la da sub-rede antes de excluí-la.



Modelo de parâmetros
Visão geral

Last updated：2024-01-24 17:55:51

Um modelo de parâmetros é um conjunto de parâmetros de endereço IP ou porta de protocolo. Você pode salvar endereços IP ou portas de protocolo com as mesmas necessidades como um modelo, para que possa importar diretamente o modelo como o IP de origem/destino ou a porta de protocolo ao adicionar regras de grupo de segurança. Os modelos de parâmetros, se usados corretamente, podem aumentar a eficiência no uso de grupos de segurança.

Casos de uso

Os modelos de parâmetros são adequados principalmente para os seguintes cenários:
Gerenciar vários grupos de endereços IP ou de portas de protocolo com os mesmos requisitos.
Gerenciar vários grupos de endereços IP ou de portas de protocolo com necessidades de edição frequentes.

Tipos de modelos de parâmetros

A Tencent Cloud aceita os quatro tipos de modelos de parâmetros a seguir:
Endereço IP: também conhecido como objeto de endereço IP, esse modelo é um conjunto de endereços IP e aceita um único IP, bloco CIDR e intervalo de IP.
Grupo de endereços IP: também conhecido como objeto de grupo de endereços IP, esse modelo é um conjunto de vários objetos de endereço IP.
Porta de protocolo: também conhecido como objeto de porta de protocolo, esse modelo é um conjunto de portas de protocolo e aceita uma única porta, várias portas, intervalo de portas e todas as portas. Ele aceita os protocolos TCP, UDP, ICMP e GRE.
Grupo de portas de protocolo: também conhecido como objeto de grupo de portas de protocolo, esse modelo é um conjunto de objetos de porta de protocolo.

Limites

Last updated：2024-01-24 17:55:51

Limites de uso

Os formatos aceitos pelo modelo de endereço IP são os seguintes:

Endereço IP único: como `10.0.0.1` ;

Endereços IP consecutivos: como `10.0.0.1` - `10.0.0.100` ;

Intervalo de IP: como `10.0.1.0/24` .

Os formatos aceitos pelo modelo de portas são os seguintes:

Porta única: como `TCP:80` ;

Várias portas: como `TCP:80,443` ;

Intervalo de portas: como `TCP:3306-20000;

Todas as portas: como `TCP:ALL` .

Limites de cota

Instância	Limite superior
Objetos de endereços IP (ipm)	1.000 por locatário
Objetos de grupos de endereços IP (ipmg)	1.000 por locatário
Objetos de portas de protocolo (ppm)	1.000 por locatário
Objetos de grupos de portas de protocolo (ppmg)	1.000 por locatário
Membros do endereço IP em um objeto de endereço IP (ipm)	20 por locatário
Membros do objeto de endereço IP (ipm) em um objeto de grupo de endereços IP (ipmg)	20 por locatário
Membros de porta de protocolo em um objeto de grupo de portas de protocolo (ppm)	20 por locatário
Membros de objeto de porta de protocolo (ppm) em um objeto de grupo de portas de protocolo (ppmg)	20 por locatário
Objetos de grupo de endereços IP (ipmg) que podem fazer referência ao mesmo objeto de endereço IP (ipm)	50 por locatário
Objetos de grupo de portas de protocolo (ppmg) que podem fazer referência ao mesmo	50 por locatário

objeto de porta de protocolo (ppm)	

Nota:

Se o modelo de parâmetros for referenciado por um grupo de segurança, os IPs e portas no modelo serão convertidos em várias regras do grupo de segurança (até 2.000).

Gerenciamento do modelo de parâmetros

Last updated：2024-01-24 17:55:51

Este documento descreve como criar e manter modelos de parâmetros (endereços IP, grupo de endereços IP, portas de protocolo e grupo de portas de protocolo) no console, e como usá-los em grupos de segurança.

Criação de modelo de parâmetros

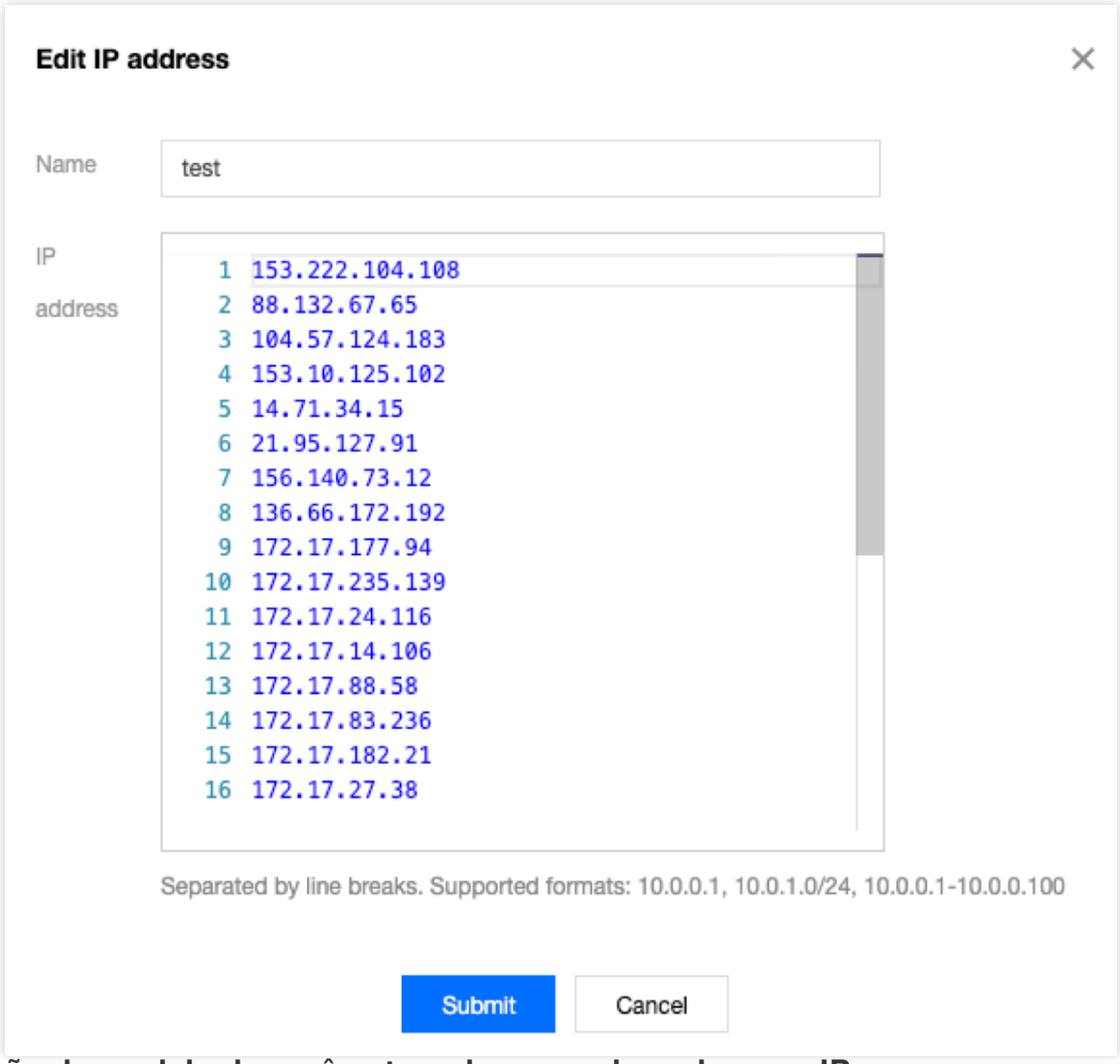
Criação de modelo de parâmetros de endereços IP

Adicione os IPs com as mesmas necessidades ou que são editados com frequência a este objeto de endereço IP.

Instruções

1. Faça login no Console da VPC.
2. Clique em **Security (Segurança)** >**Parameter Template (Modelo de parâmetros)** na barra lateral esquerda, para acessar a página de gerenciamento.
3. Selecione a guia **IP Address (Endereço IP)** e clique em **+New (+Novo)**.
4. Na janela pop-up, insira o nome e os endereços IP, e clique em **Submit (Enviar)**.

Você pode adicionar vários endereços IPv4 nos seguintes intervalos e separá-los por quebras de linha:
Endereço IP único: como `10.0.0.1` ;
Bloco CIDR: como `10.0.1.0/24` ;
Intervalo de IP: como `10.0.0.1` - `10.0.0.100` .

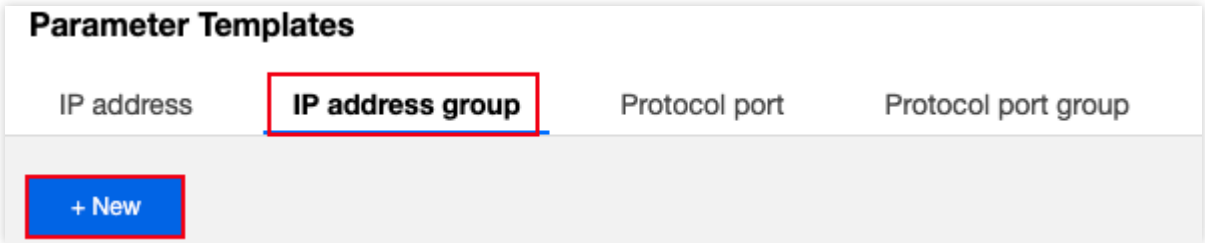


Criação de modelo de parâmetros de grupo de endereços IP

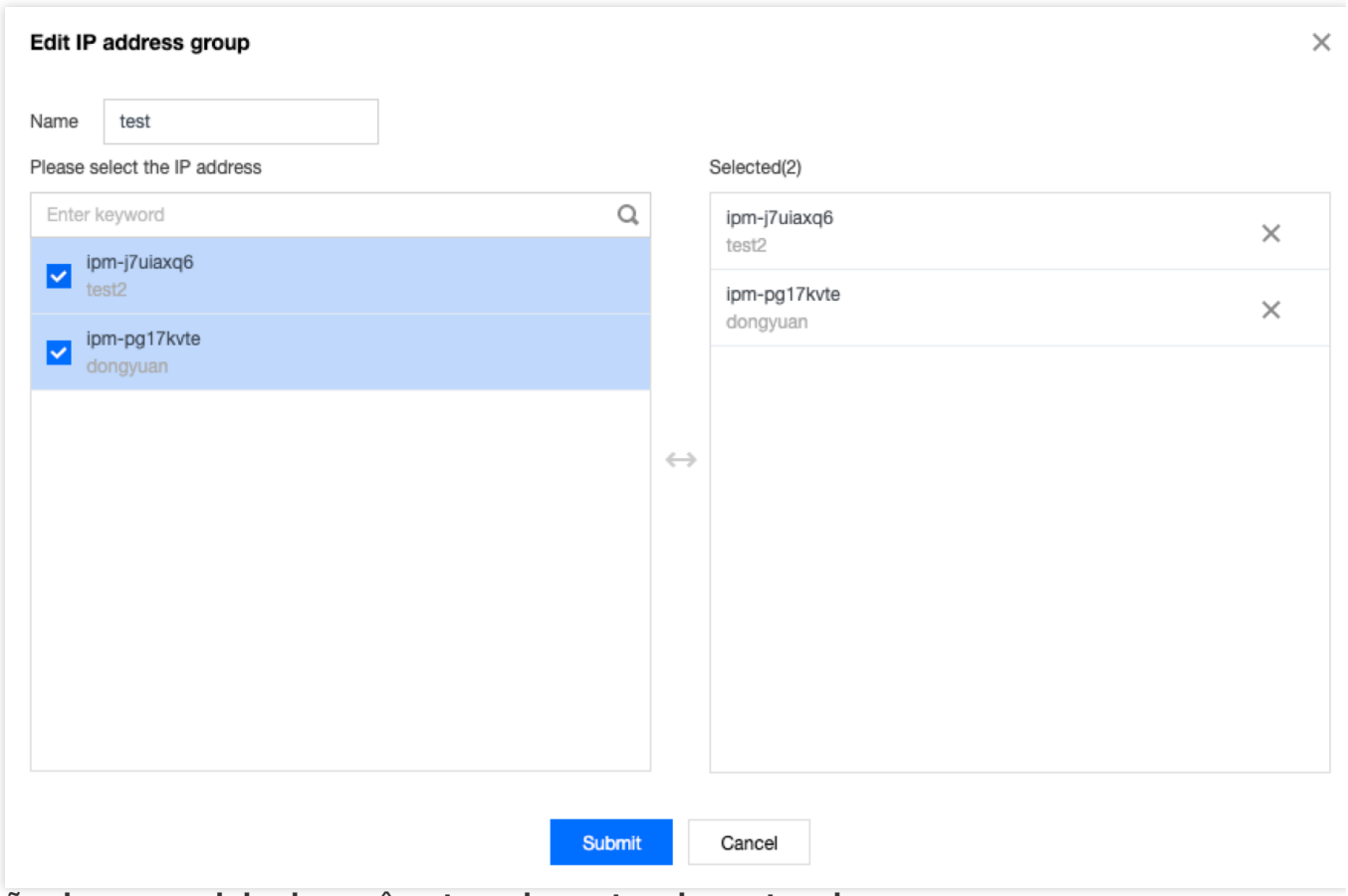
Você pode adicionar vários objetos de endereço IP a um grupo de endereços IP para gerenciamento unificado.

Instruções

1. Selecione a guia **IP Address Group (Grupo de endereços IP)** e clique em **+New (+Novo)**.



2. Na janela pop-up, insira o nome, selecione os objetos de endereço IP a serem adicionados e clique em **Submit (Enviar)**.



Criação de um modelo de parâmetros de portas de protocolo

Você pode adicionar as portas de protocolo com as mesmas necessidades ou que são editadas com frequência a este objeto de porta de protocolo.

Instruções

1. Faça login no Console da VPC.
2. Clique em **Security (Segurança)** >**Parameter Template (Modelo de parâmetros)** na barra lateral esquerda, para acessar a página de gerenciamento.
3. Selecione a guia **Protocol Port (Porta de protocolo)** e clique em **+New (+Novo)**.
4. Na janela pop-up, insira o nome e as portas de protocolo e clique em **Submit (Enviar)**.

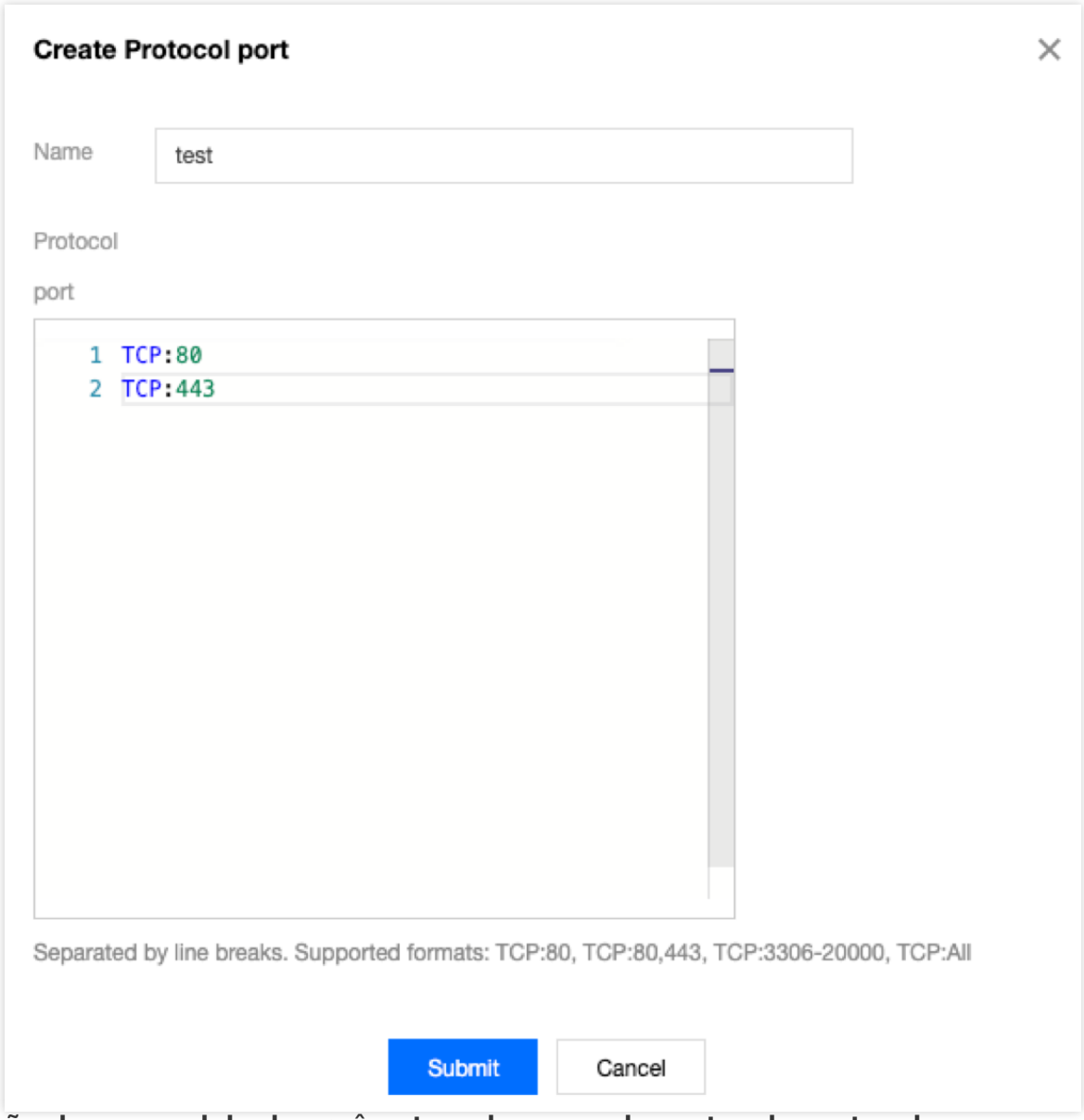
Você pode adicionar várias portas de protocolo nos seguintes intervalos e separá-las com quebras de linha:

Porta única: como `TCP:80` ;

Várias portas: como `TCP:80,443` ;

Intervalo de portas: como `TCP:3306-20000` ;

Todas as portas: como `TCP:ALL` .

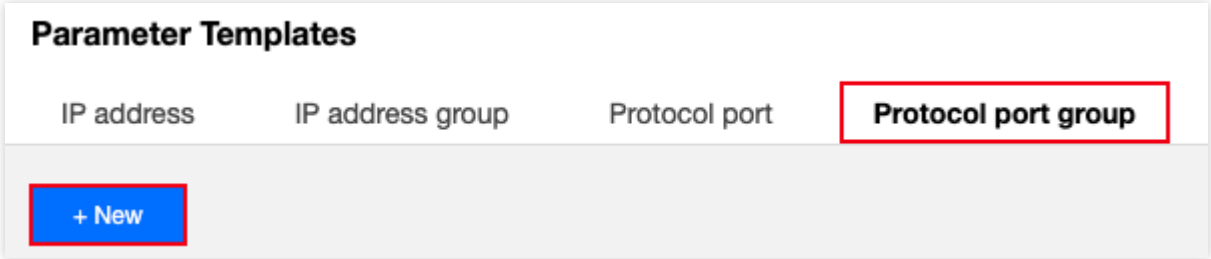


Criação de um modelo de parâmetros de grupo de portas de protocolo

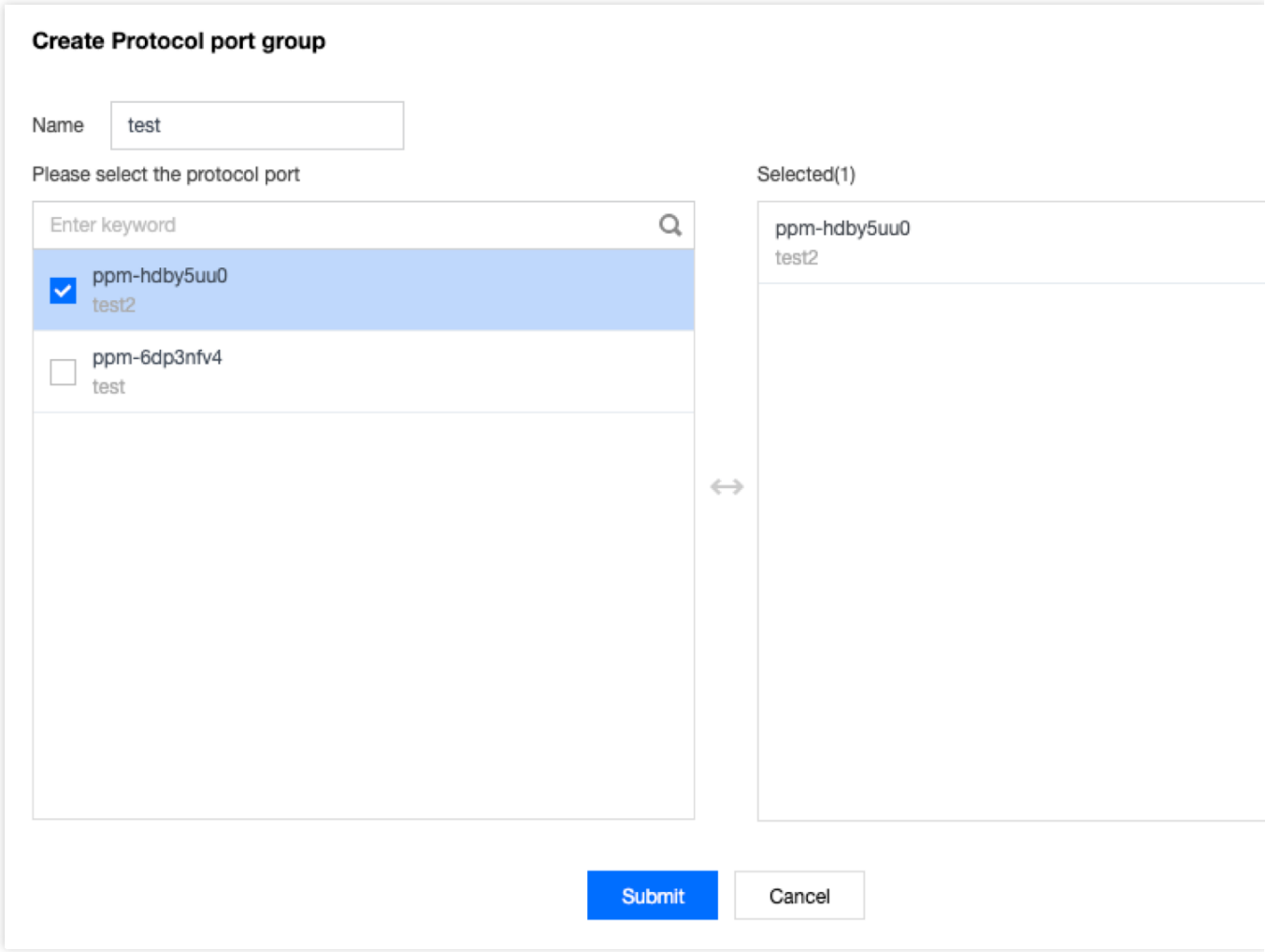
Você pode adicionar vários objetos de porta de protocolo criados a um grupo de portas de protocolo para gerenciamento unificado.

Instruções

1. Selecione a guia **Protocol Port Group (Grupo de portas de protocolo)** e clique em **+New (+Novo)**.



2. Na janela pop-up, insira o nome, selecione o objeto de porta de protocolo a ser adicionado e clique em **Submit (Enviar)**.

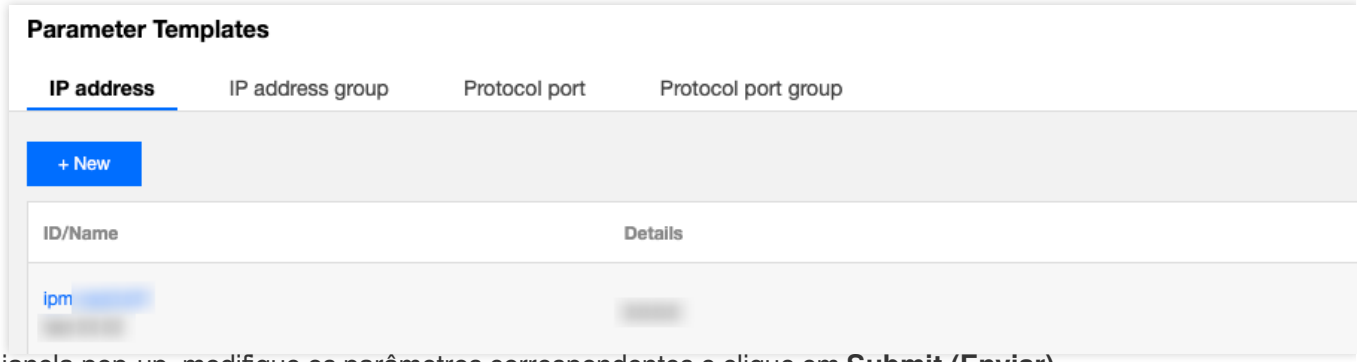


Modificação de modelo de parâmetros

Se você precisar modificar um modelo de parâmetros criado, por exemplo, para adicionar/excluir endereços IP ou portas de protocolo, siga as etapas abaixo.

Instruções

1. Clique no modelo de parâmetros de endereços IP, grupo de endereços IP, portas de protocolo ou grupo de portas de protocolo criado e clique em **Edit (Editar)** à direita. Por exemplo, a figura a seguir mostra como modificar os objetos de endereço IP.



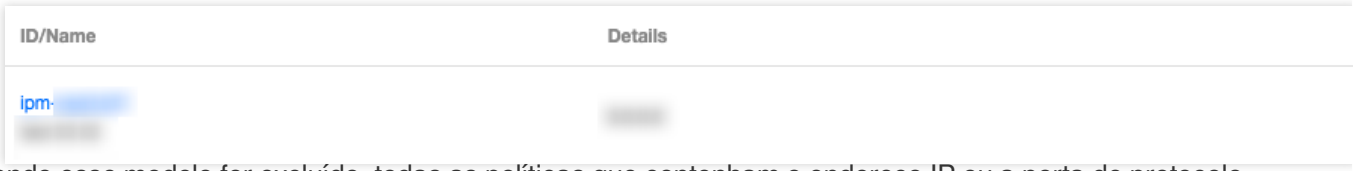
2. Na janela pop-up, modifique os parâmetros correspondentes e clique em **Submit (Enviar)**.

Exclusão de modelo de parâmetros

Se você não usar mais um modelo de parâmetros, poderá excluí-lo. Quando esse modelo é excluído, todas as configurações de política que o contêm no grupo de segurança serão excluídas ao mesmo tempo. Avalie e prossiga com cautela.

Instruções

1. Clique em **Delete (Excluir)** à direita do modelo de parâmetros criado.



2. Quando esse modelo for excluído, todas as políticas que contenham o endereço IP ou a porta de protocolo correspondente também serão excluídas. Depois de confirmar que tudo está correto, clique em **Delete (Excluir)** na janela pop-up **Confirm Deletion (Confirmar exclusão)**.

Importação do modelo de parâmetros para o grupo de segurança

Depois de criar um modelo de parâmetros, você pode importá-lo diretamente ao adicionar regras em um grupo de segurança para adicionar com rapidez origens de IP ou portas de protocolo, o que ajuda a melhorar sua eficiência ao adicionar regras de grupo de segurança.

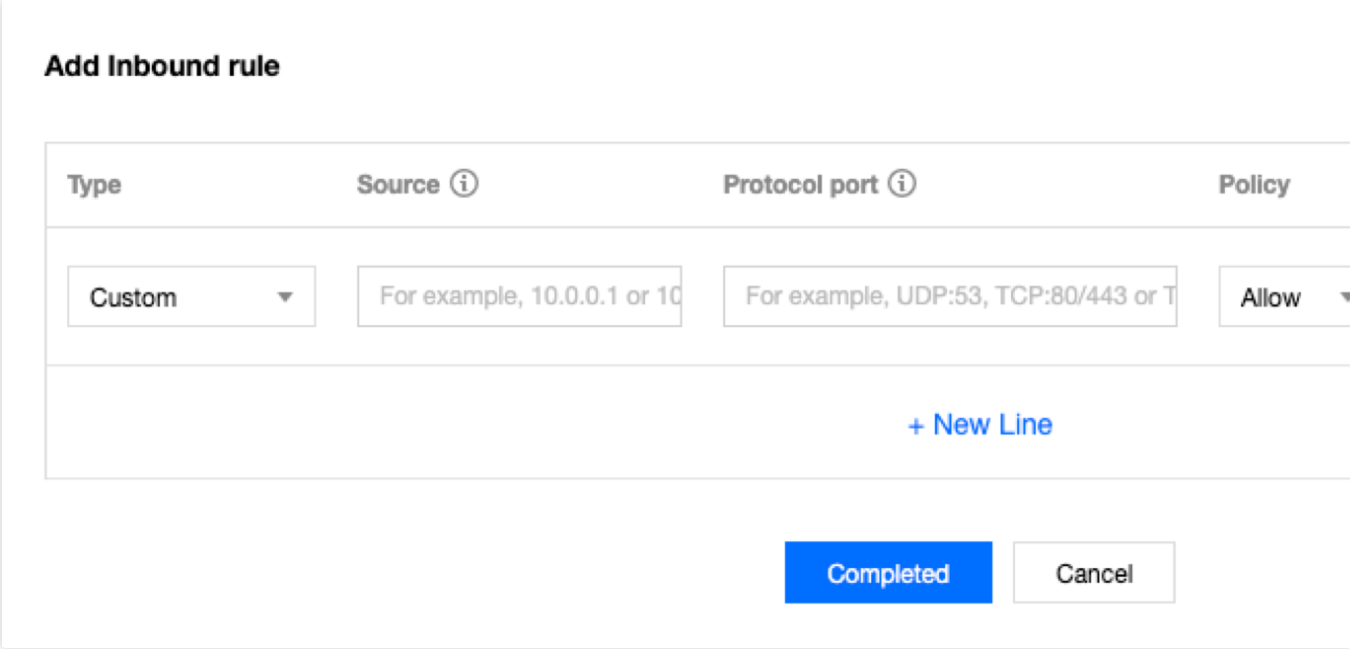
Instruções

1. Faça login no Console da VPC.
2. Clique em **Security (Segurança)** >**Security Group (Grupo de segurança)** na barra lateral esquerda, para acessar a página de gerenciamento.

3. Na lista, localize o grupo de segurança que precisa importar o modelo de parâmetros e clique em seu ID para acessar a página de detalhes.
4. Na guia **Inbound/Outbound Rules (Regras de entrada/saída)**, clique em **Add Rule (Adicionar regra)**.
5. Na janela pop-up, selecione o tipo **Custom (Personalizada)**, selecione o modelo de parâmetros criado em **Source (Origem)** e **Protocol Port (Porta de protocolo)**, e clique em **Complete (Concluir)**. Para mais informações sobre como adicionar regras de entrada/saída, consulte Adição de uma regra de grupo de segurança.

Nota:

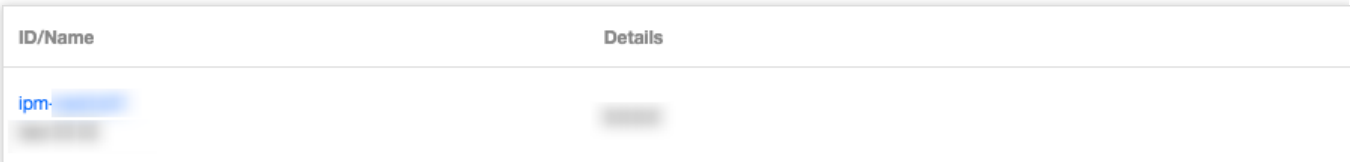
Se você precisar adicionar um novo endereço IP ou porta de protocolo no futuro, basta adicioná-lo ao grupo de endereços IP ou ao grupo de portas de protocolo correspondente, e não há necessidade de modificar as regras do grupo de segurança ou criar outro grupo de segurança.



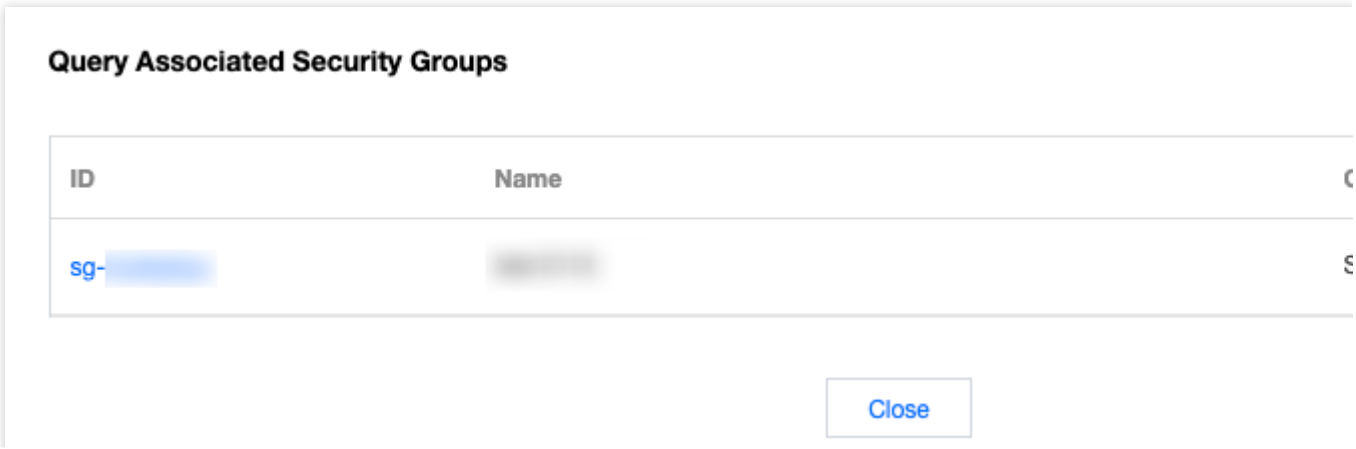
Exibição do grupo de segurança associado

Você pode exibir todas as instâncias dos grupos de segurança que importam um modelo de parâmetros nas etapas a seguir.

1. Clique em **View Association (Exibir associação)** à direita do modelo de parâmetros criado.



2. A lista de grupos de segurança associados exibida mostra todas as instâncias dos grupos de segurança associadas a esse modelo de parâmetros.



Caso de configuração

Last updated：2024-01-24 17:55:51

Casos de uso de modelo de parâmetros

O modelo de parâmetros é uma maneira eficiente, rápida e de fácil manutenção para adicionar regras em grupos de segurança. Por exemplo, quando você precisa adicionar vários intervalos de IP, IPs especificados ou portas de protocolo de vários tipos, é possível definir um modelo de parâmetros. Você também pode usar o modelo de parâmetros posteriormente para manter as origens de IP e as portas de protocolo nas regras de grupo de segurança.
Nota:
Todos os endereços IP e as portas de protocolo neste documento são exemplos. Substitua-os de acordo com as suas condições reais de negócios durante a configuração.

Descrição do exemplo

Suponha que você queira configurar as seguintes regras de grupo de segurança e precise atualizar o intervalo de IP de origem de entrada e a porta de protocolo posteriormente:
Regras de entrada:
Intervalo de IP de origem permitido: 10.0.0.16-10.0.0.30; porta de protocolo: TCP:80,443
Bloco CIDR de origem permitido: 192.168.3.0/24; porta de protocolo: TCP:3600-15000
Regras de saída:
Endereço IP de destino rejeitado: 192.168.10.4; porta de protocolo: TCP:800

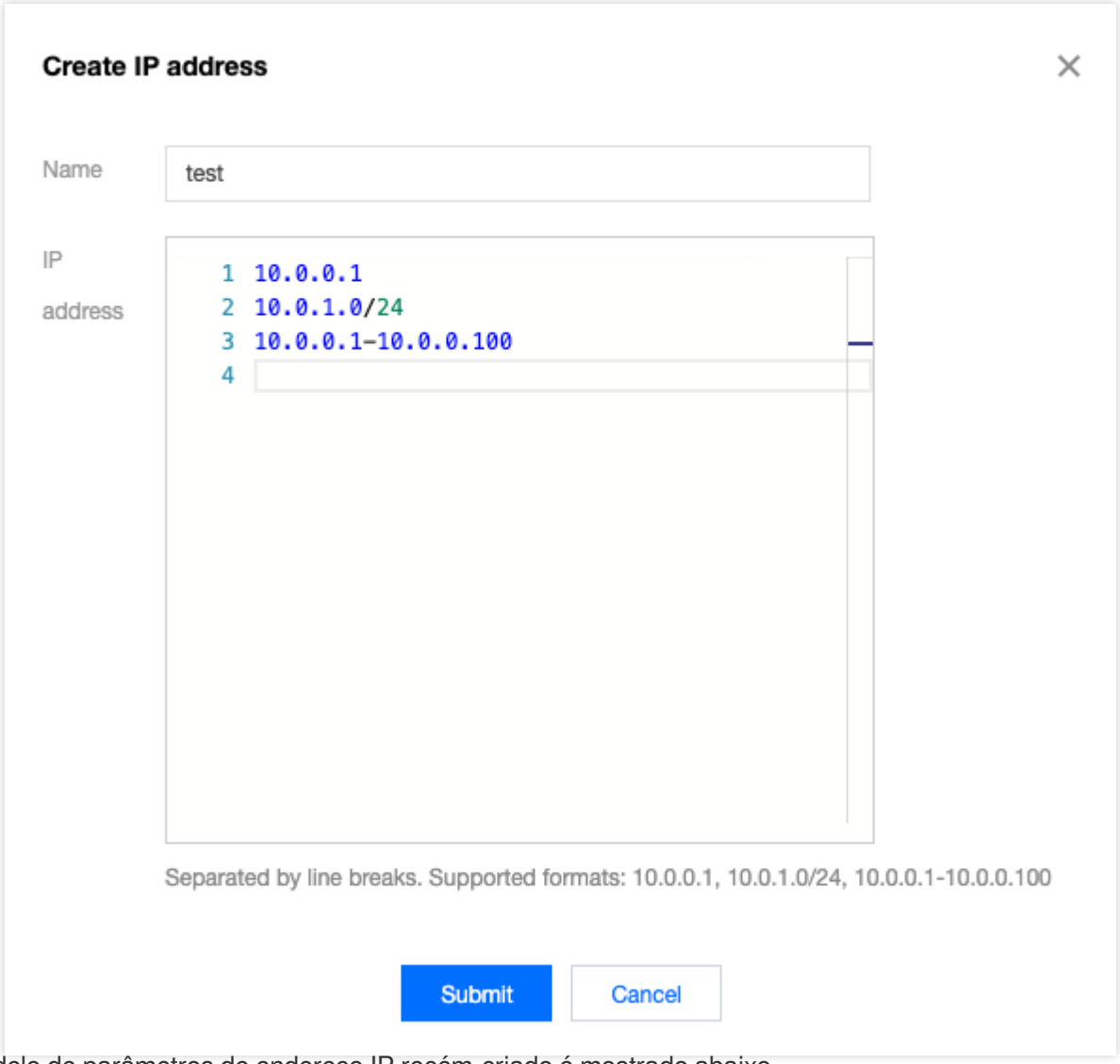
Solução

Como você tem a mesma política de grupo de segurança para vários intervalos de IP e portas de protocolo, e precisa atualizar o intervalo de IP de origem posteriormente, é possível usar um modelo de parâmetros para implementar a adição e manutenção de regras de grupo de segurança.

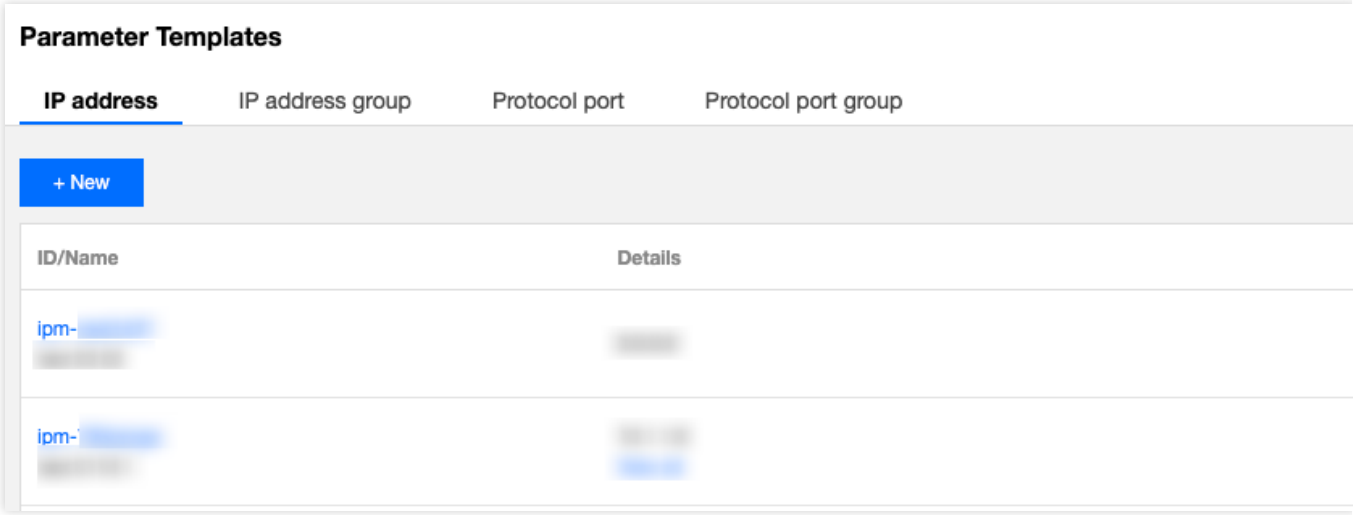
Etapa 1. Criar um modelo de parâmetros

1. Faça login no Console da VPC.
2. Selecione **Security (Segurança)** >**Parameter Template (Modelo de parâmetros)** na barra lateral esquerda, para acessar a página de gerenciamento.
3. Na guia **IP Address (Endereço IP)**, clique em **+ New (+ Novo)** para criar um modelo de parâmetros de endereço IP para adicionar regras de entrada e de saída.

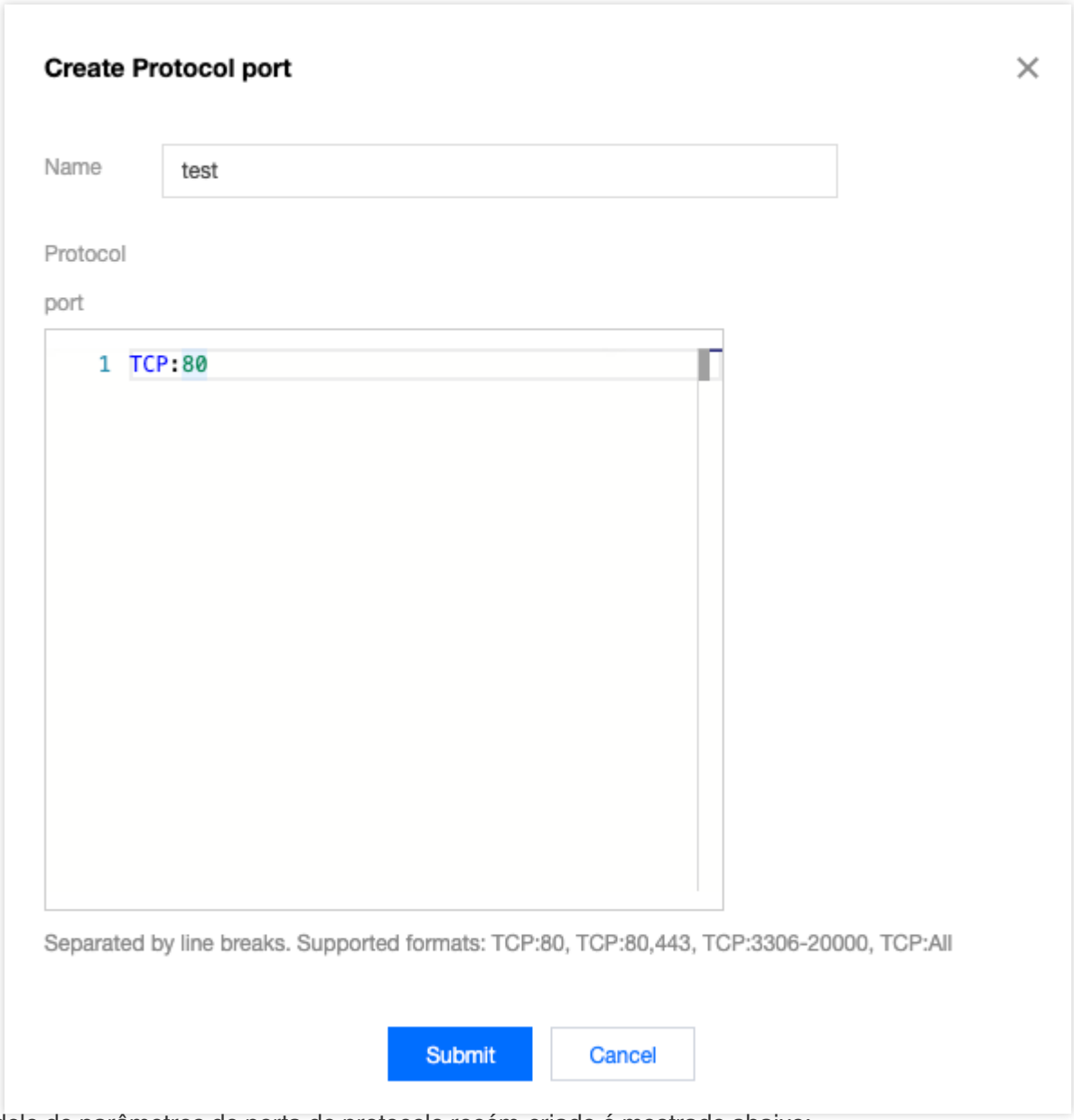
4. Na janela pop-up, insira o intervalo de IP de origem e clique em **Submit (Enviar)**.



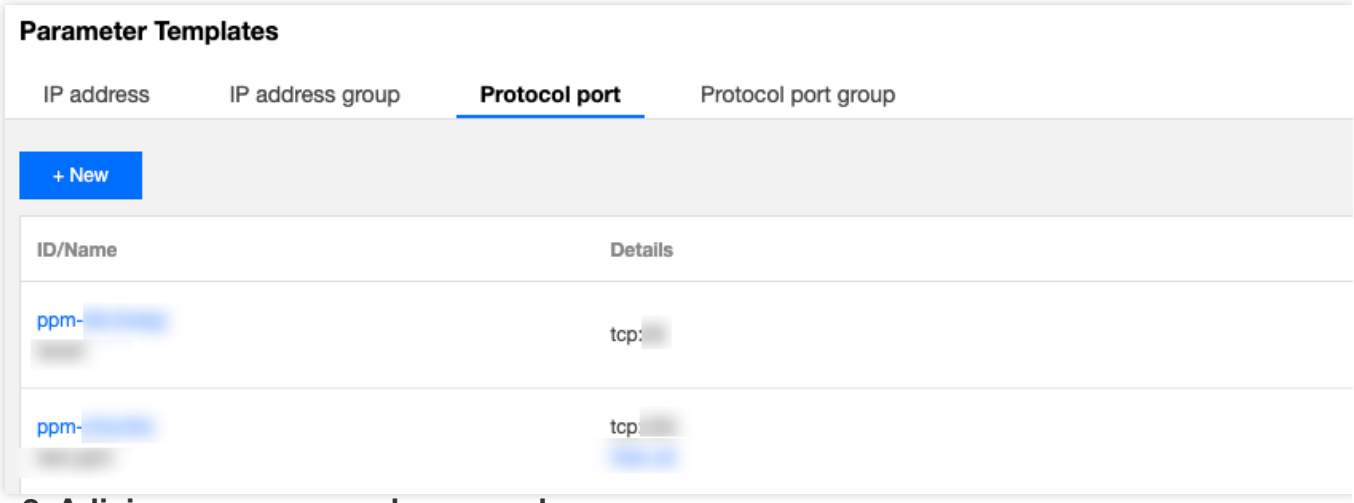
O modelo de parâmetros de endereço IP recém-criado é mostrado abaixo.



5. Na guia **Protocol Port (Porta de protocolo)**, clique em **+ New (+ Novo)** para criar um modelo de parâmetros de porta de protocolo para adicionar regras de entrada e de saída.

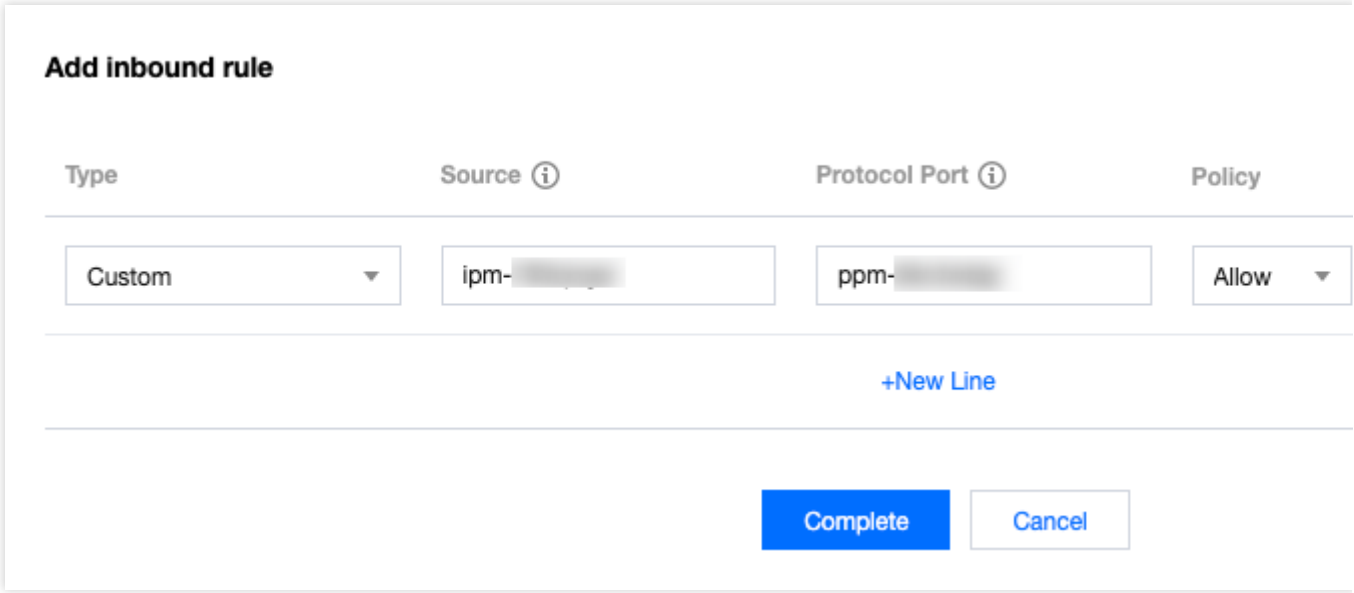


O modelo de parâmetros de porta de protocolo recém-criado é mostrado abaixo:



Etapa 2. Adicionar uma regra de grupo de segurança

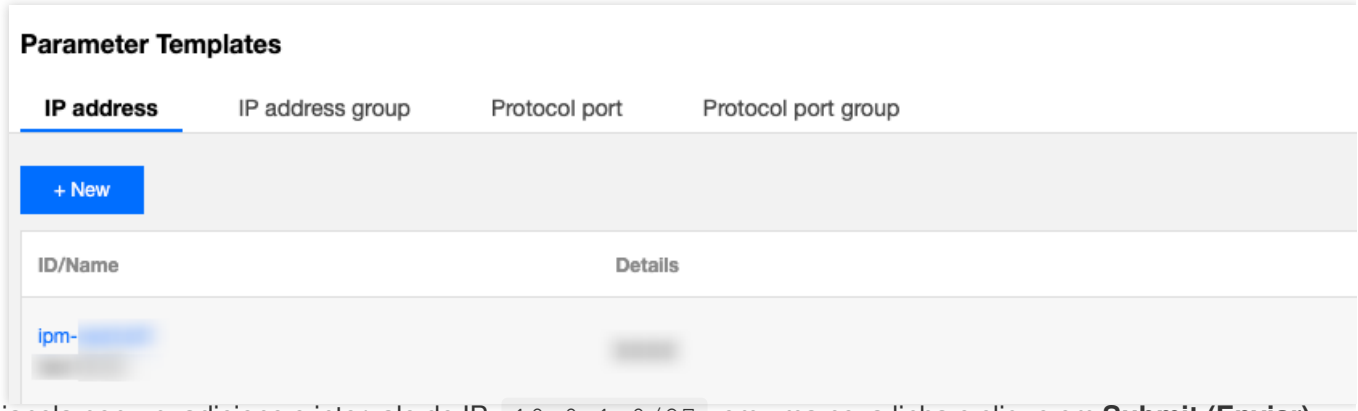
1. Faça login no Console da VPC.
2. Selecione **Security (Segurança)** >**Security Group (Grupo de segurança)** na barra lateral esquerda, para acessar a página de gerenciamento.
3. Na lista, localize o grupo de segurança que precisa importar o modelo de parâmetros e clique em seu ID para acessar a página de detalhes.
4. Na guia **Inbound/Outbound Rules (Regras de entrada/saída)**, clique em **Add Rule (Adicionar regra)**.
5. Na janela pop-up, selecione o tipo “personalizada”, selecione o modelo de parâmetros de endereço IP correspondente da origem/destino, selecione o modelo de parâmetros de porta de protocolo correspondente da porta de protocolo e clique em **Complete (Concluir)**.



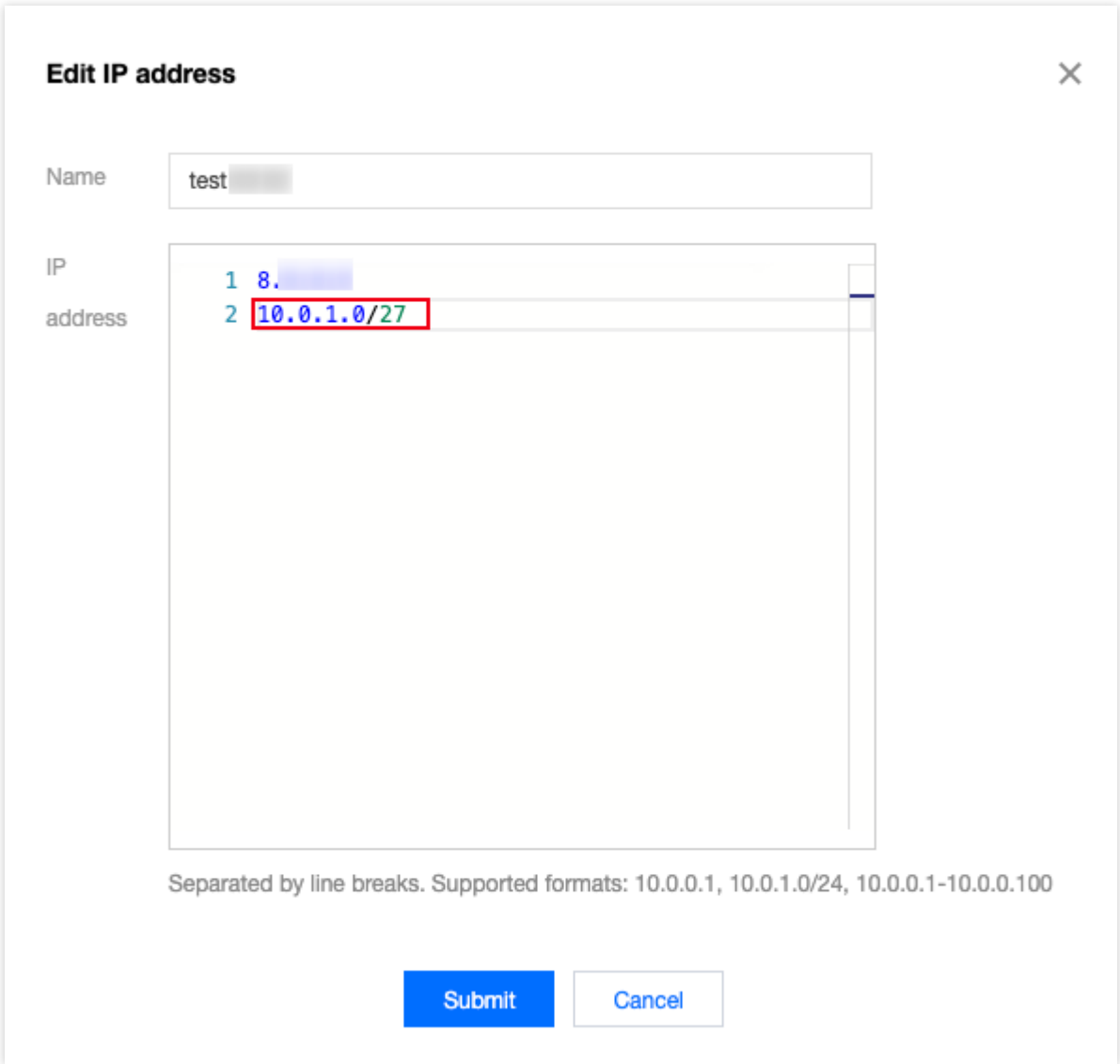
Etapa 3. Atualizar o modelo de parâmetros

Suponha que você precise adicionar uma regra de entrada com a origem de IP sendo o intervalo de IP `10.0.1.0/27` e a porta de protocolo sendo `UDP:58` . Você pode atualizar diretamente os modelos de parâmetros do endereço IP `ipm-0ge3ob8e` e da porta de protocolo `ppm-4ty1ck3i` .

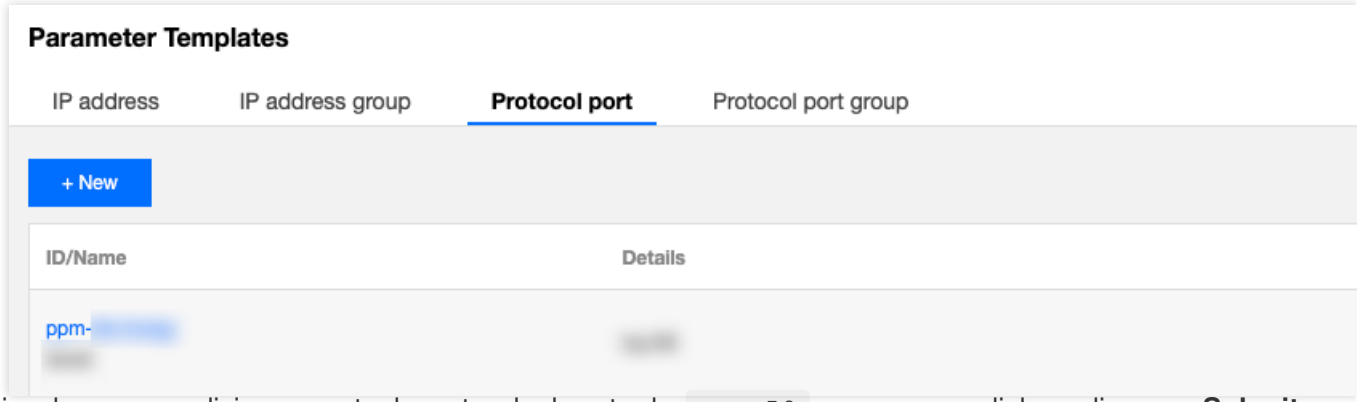
1. Na guia **IP Address (Endereço IP)** do modelo de parâmetros, localize o modelo de parâmetros `ipm-0ge3ob8e` .
2. Clique em **Edit (Editar)** à direita.



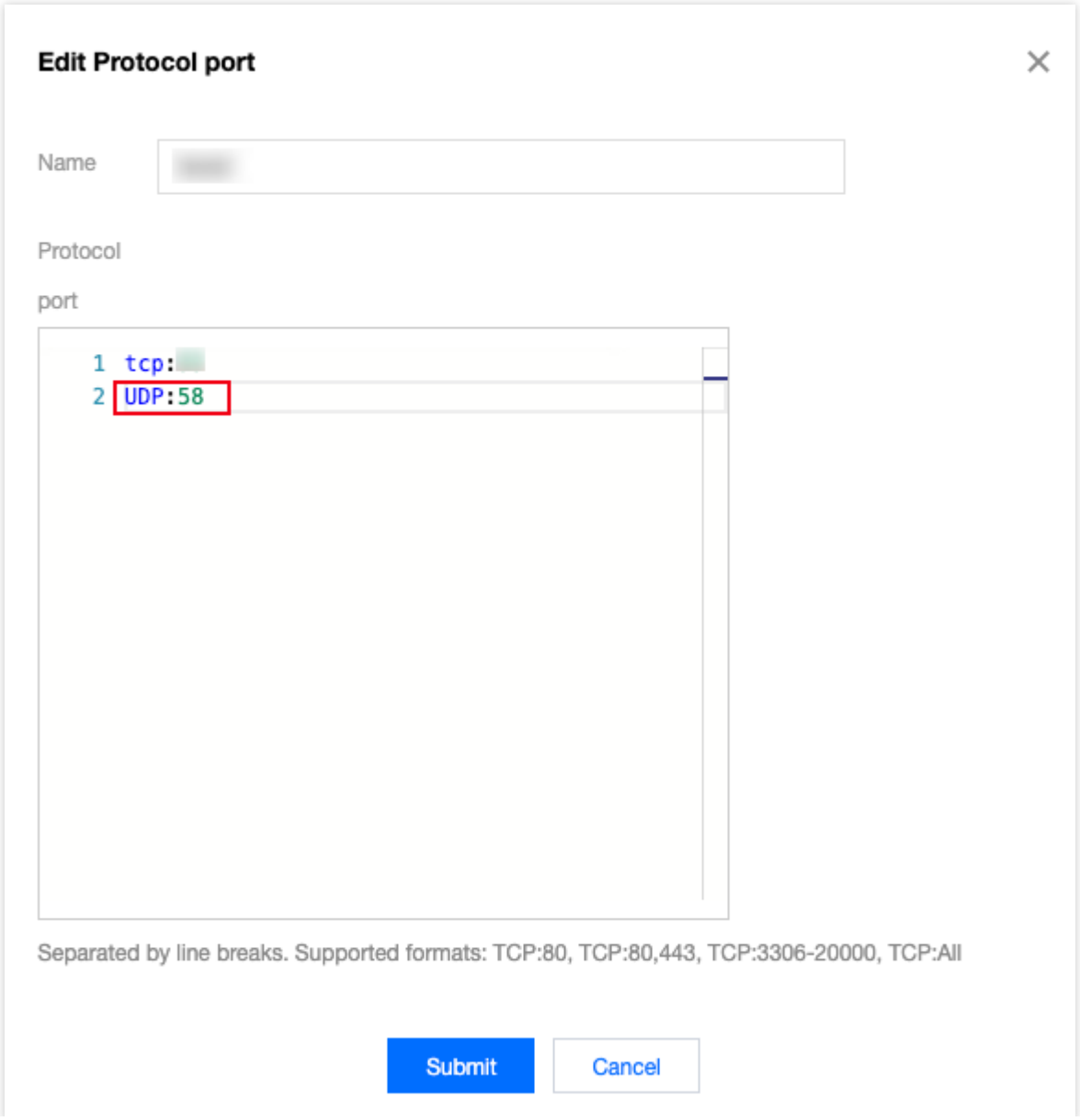
3. Na janela pop-up, adicione o intervalo de IP `10.0.1.0/27` em uma nova linha e clique em **Submit (Enviar)**.



4. Na guia **Protocol Port (Porta de protocolo)** do modelo de parâmetros, localize o modelo de parâmetros `ppm-4ty1ck3i` .
5. Clique em **Edit (Editar)** à direita.



6. Na janela pop-up, adicione a porta de protocolo de entrada `UDP:58` em uma nova linha e clique em **Submit (Enviar)**.</br>



Gerenciamento de acesso
Visão geral do Cloud Access Management

Last updated：2024-01-24 17:55:51

Se você estiver usando vários serviços do Tencent Cloud, como VPC, CVM e TencentDB, que são gerenciados por diferentes usuários que compartilham sua chave de conta do Tencent Cloud, você pode encontrar os seguintes problemas:
Sua chave é compartilhada por vários usuários, o que representa um alto risco de vazamento.
Você não pode limitar as permissões de acesso de outros usuários, o que representa um risco de segurança devido a uma possível operação incorreta.
Para evitar esses problemas, é possível usar subcontas para permitir que usuários diferentes gerenciem serviços diferentes. Por padrão, uma subconta não tem permissão para usar um CVM ou recursos relacionados ao CVM. Portanto, é necessário criar uma política para conceder os recursos ou permissões necessários às subcontas.

Visão geral

O Cloud Access Management (CAM) é um serviço da web fornecido pelo Tencent Cloud para ajudar os clientes a gerenciar as permissões de acesso aos recursos em suas contas do Tencent Cloud de forma segura. É possível usar o CAM para criar, gerenciar e encerrar usuários (ou grupos de usuários), e usar o gerenciamento de identidade e de políticas para controlar os recursos do Tencent Cloud que podem ser usados por cada usuário.
Ao usar o CAM, você pode associar uma política a um usuário ou grupo de usuários. A política pode autorizar ou negar as solicitações dos usuários de usar recursos especificados para concluir tarefas especificadas.
Para obter mais informações básicas sobre as políticas do CAM, consulte Lógica da sintaxe.
Para obter mais informações sobre o uso das políticas do CAM, consulte Políticas.
Se não for necessário gerenciar as permissões de acesso de subcontas para recursos do VPC, pule esta seção. Isso não afetará sua compreensão e uso de outras partes do documento.

Introdução

Uma política do CAM deve autorizar ou negar o uso de uma ou mais operações do VPC. Ao mesmo tempo, ela deve especificar os recursos (que podem ser todos os recursos ou recursos parciais para determinadas operações) que podem ser usados para as operações. A política também pode incluir as condições definidas para os recursos de operação.
Algumas operações de API do VPC aceitam permissões no nível de recursos. Ou seja, ao chamar essas APIs, você não pode especificar alguns recursos para as operações. Em vez disso, você deve especificar todos os recursos para

as operações.

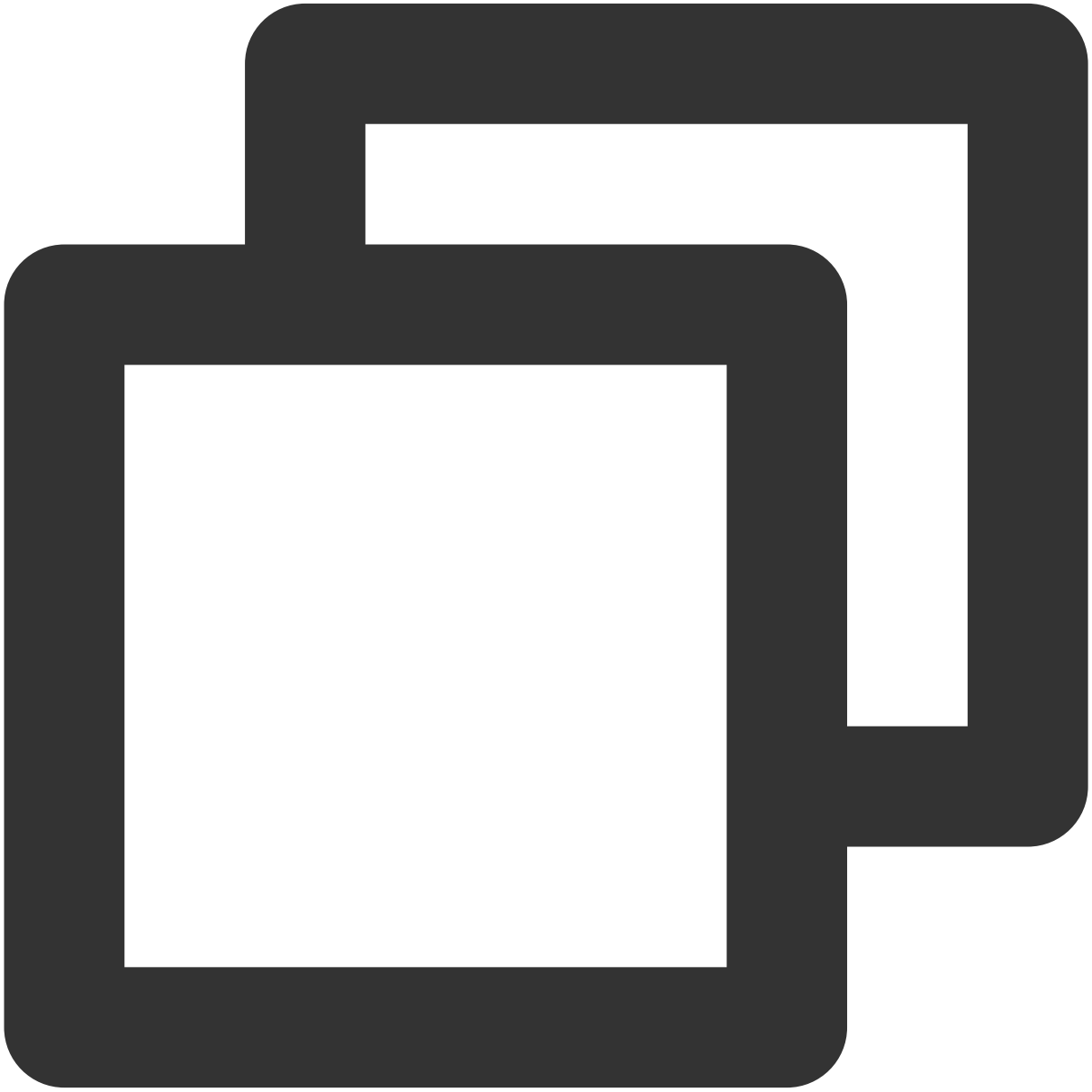
Tarefa	Link
Estrutura básica de uma política	Sintaxe da política
Definir as operações da política	Operações do VPC
Definir os recursos da política	Caminhos dos recursos do VPC
Permissões de nível de recursos compatíveis com o VPC	Permissões de nível de recursos compatíveis com o VPC
Exemplo do console	Exemplo do console

Tipos de recursos autorizáveis

Last updated：2024-01-24 17:55:51

Sintaxe da política

Política do CAM:



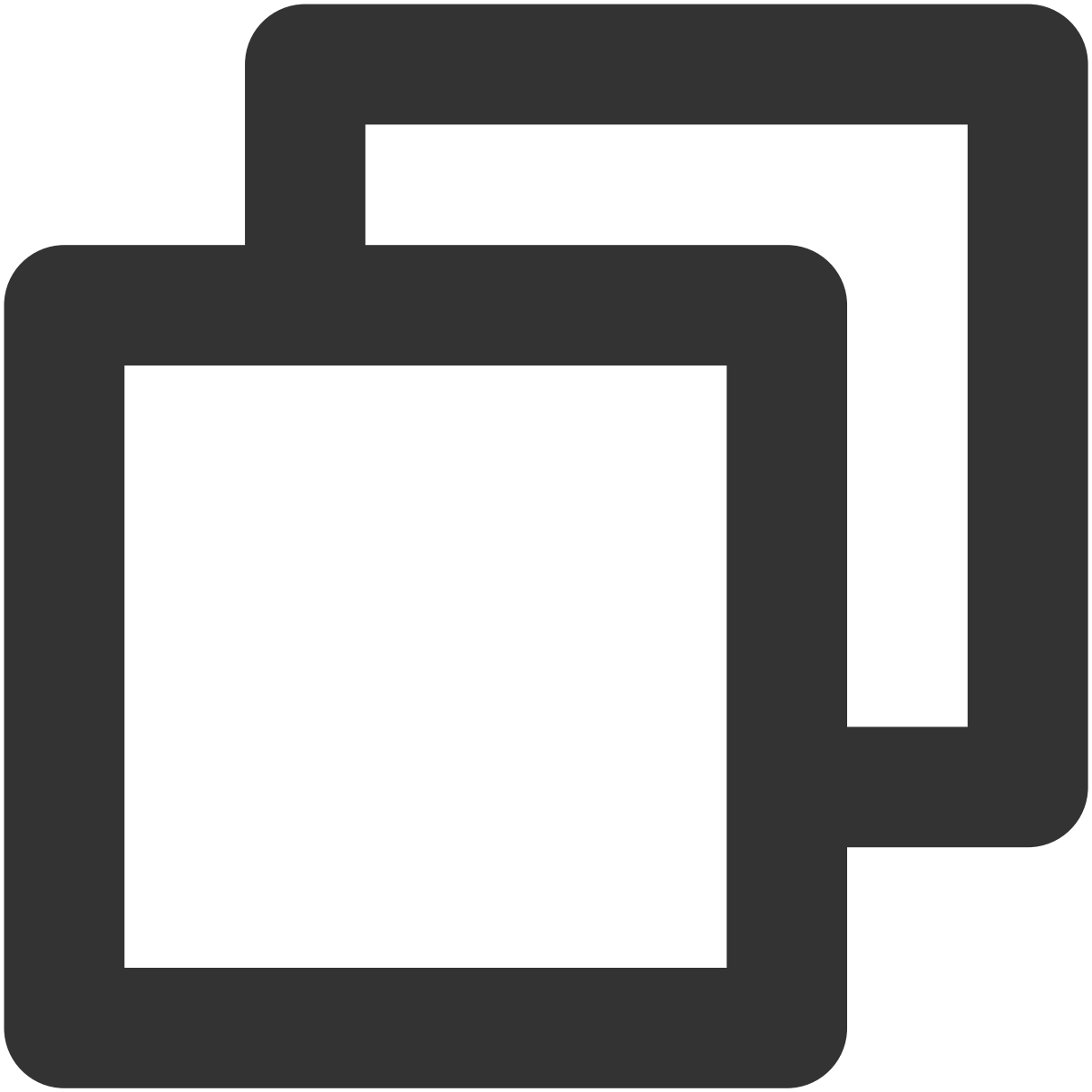
```
{
```

```
        "version":"2.0",
        "statement":
        [
            {
                "effect":"effect",
                "action":["action"],
                "resource":["resource"],
                 "condition": {"key":{"value"}}
            }
        ]
}
```

a **version (versão)** é obrigatória. Atualmente, apenas o valor "2.0" é permitido.
a **statement (instrução)** descreve os detalhes de uma ou mais permissões. Esse elemento contém uma permissão ou conjunto de permissões que é composto por outros elementos, como efeito, ação, recurso e condição. Cada política tem um elemento de instrução.
1.1 **action (ação)** descreve a ação a ser permitida ou negada. Uma ação pode ser uma API (descrita com o prefixo "name") ou um conjunto de funcionalidades (um conjunto de APIs específicas descrito com o prefixo "permid"). Esse elemento é obrigatório.
1.2 **resource (recurso)** descreve os detalhes da autorização. Um recurso é descrito em um formato de seis partes. As definições detalhadas dos recursos variam de acordo com o produto. Para obter mais informações sobre como especificar um recurso, consulte a documentação do produto cujos recursos você está escrevendo uma instrução. Esse elemento é obrigatório.
1.3 A **condition (condição)** descreve a condição para que a política entre em vigor. Uma condição é composta por um operador, uma chave da ação e um valor da ação. Um valor da condição pode conter informações, como a hora e o endereço IP. Alguns serviços permitem que você especifique valores adicionais em uma condição. Esse elemento é opcional.
1.4 O **effect (efeito)** descreve se o resultado produzido pela instrução é "allow (permitir)" ou "deny (negar)". Este elemento é obrigatório.

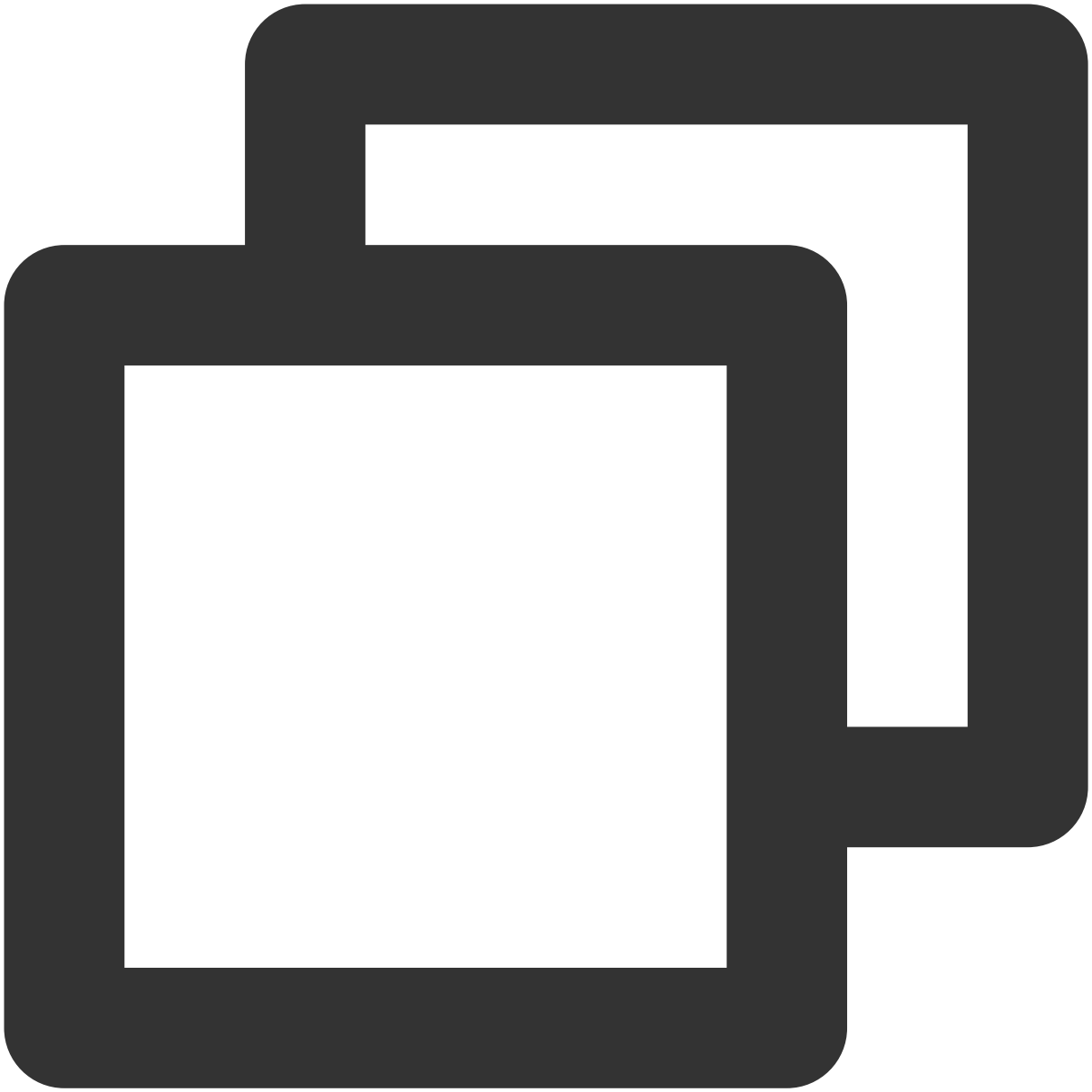
Operações do VPC

Na instrução de uma política do CAM, você pode especificar qualquer ação de API de qualquer serviço que aceite o CAM. Para o VPC, use APIs com o prefixo "name/vpc:", por exemplo, name/vpc:Describe ou name/vpc:CreateRoute. Para especificar várias ações em uma única instrução, separe-as com vírgulas, conforme mostrado abaixo:



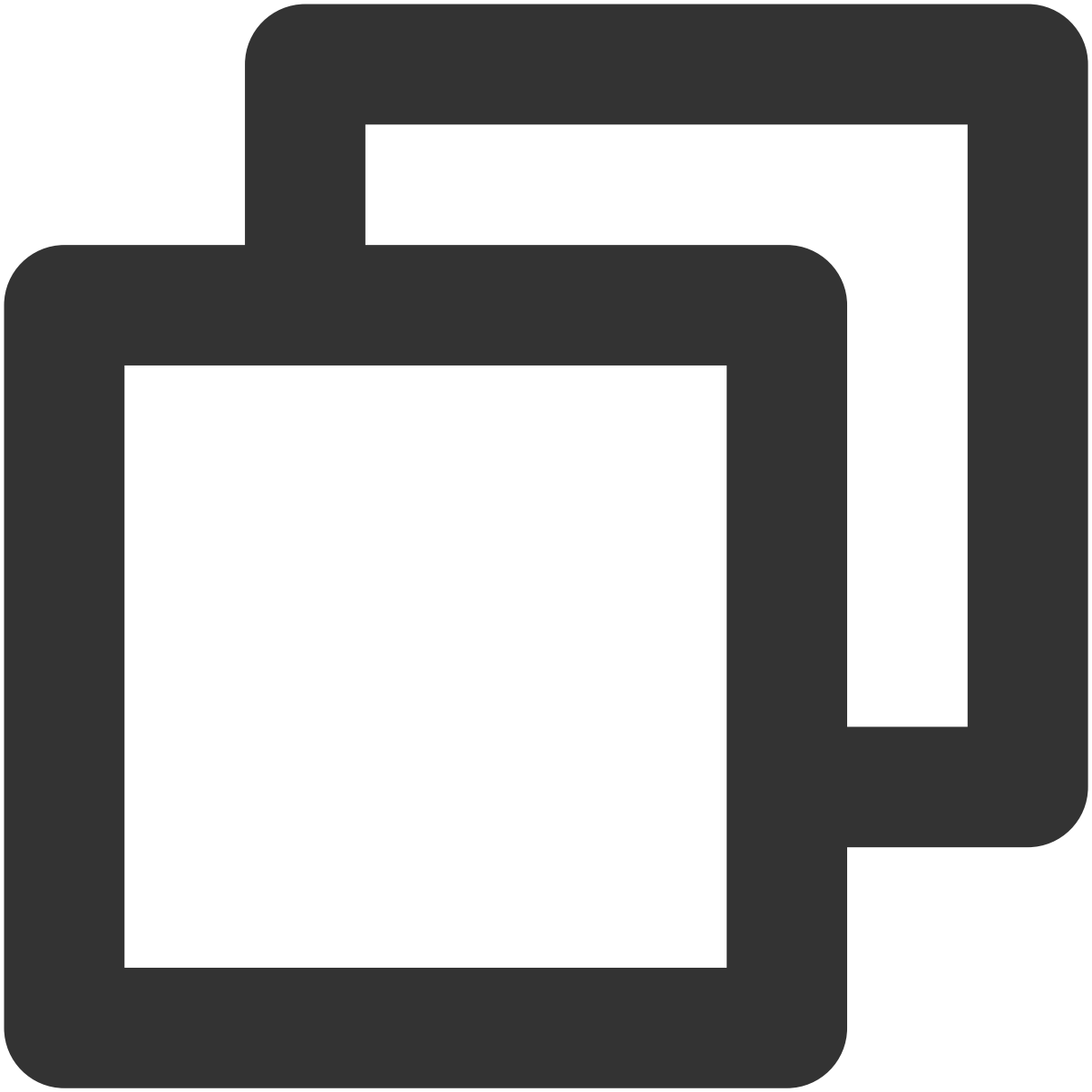
```
"action":["name/vpc:action1","name/vpc:action2"]
```

Você também pode especificar várias ações usando um caractere curinga. Por exemplo, você pode especificar todas as ações cujos nomes começam com "Describe", conforme mostrado abaixo:



```
"action":["name/vpc:Describe*"]
```

Para especificar todas as ações no VPC, use o caractere curinga "*" da seguinte forma:

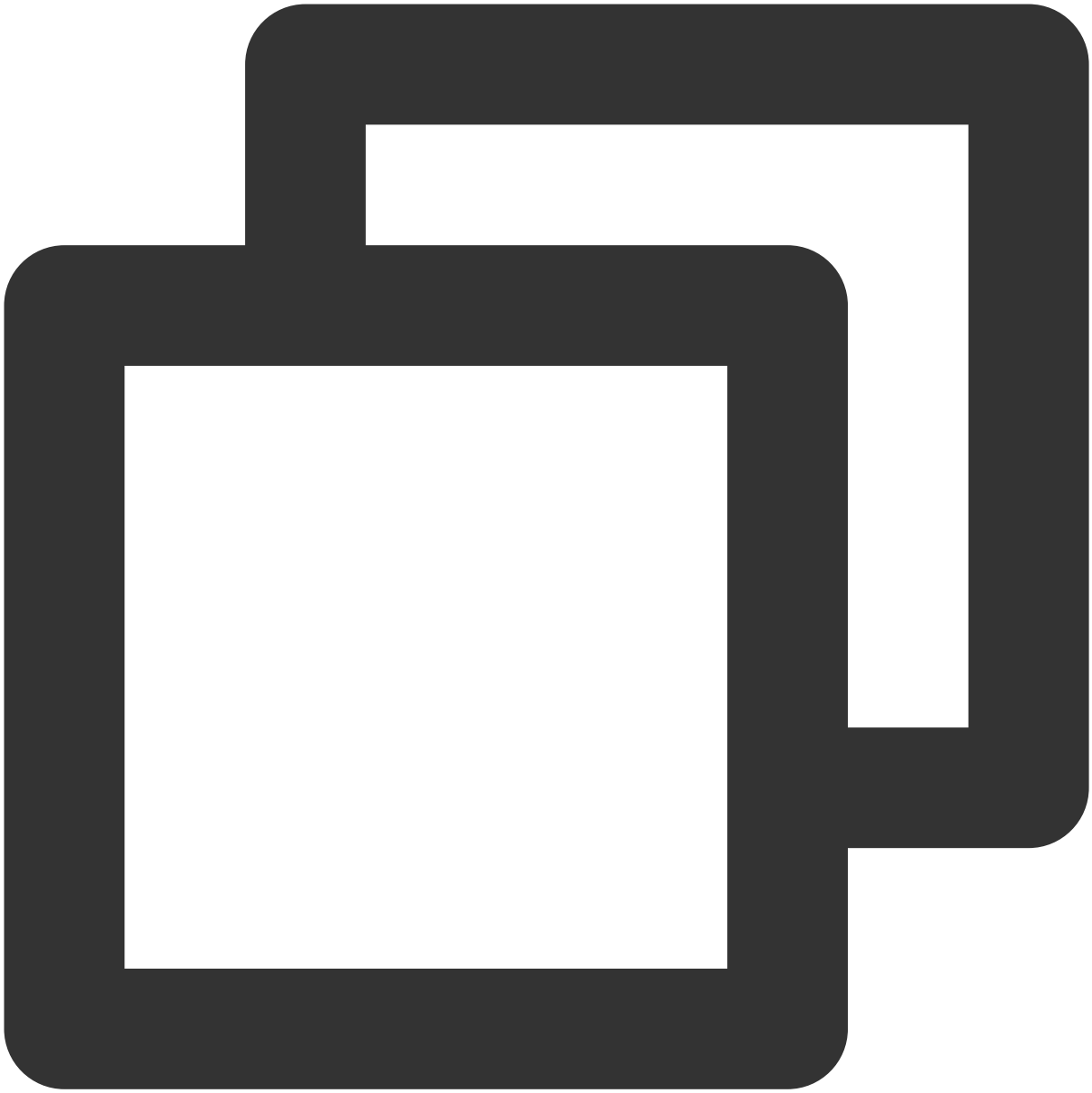


```
"action": ["name/vpc:*"]
```

Caminhos de recursos do VPC

Cada instrução da política do CAM tem seus próprios recursos.

O formato geral de um caminho de recursos é o seguinte:



```
****qcs**:project_id:service_type:region:account:resource**
```

project_id: informações do projeto. Este elemento é usado apenas para permitir a compatibilidade com a lógica do CAM legada e pode ser deixado em branco.

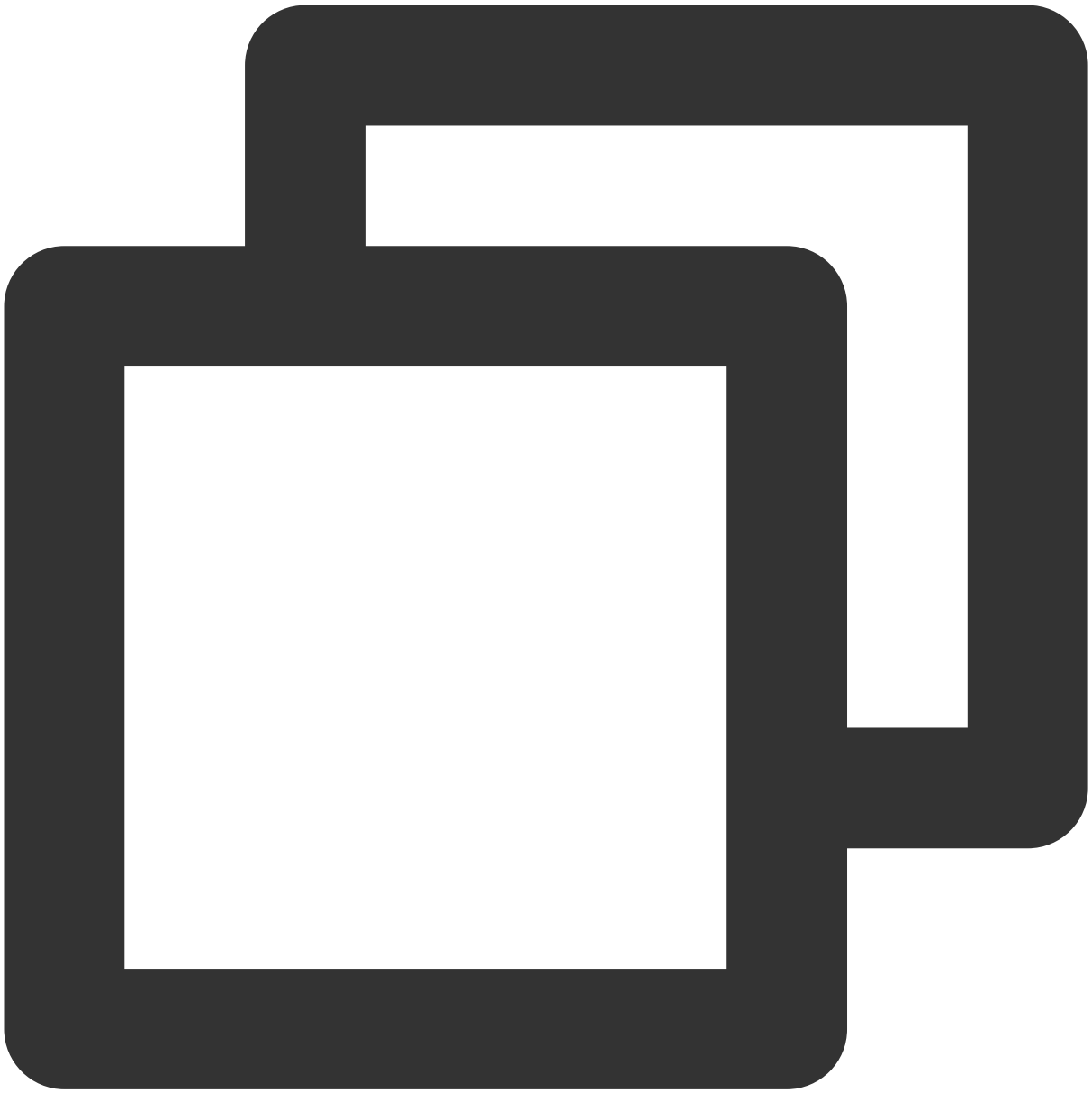
service_type: abreviatura de um produto, como VPC.

region: informações da região, como bj.

account: a conta raiz do proprietário do recurso, como uin/164256472.

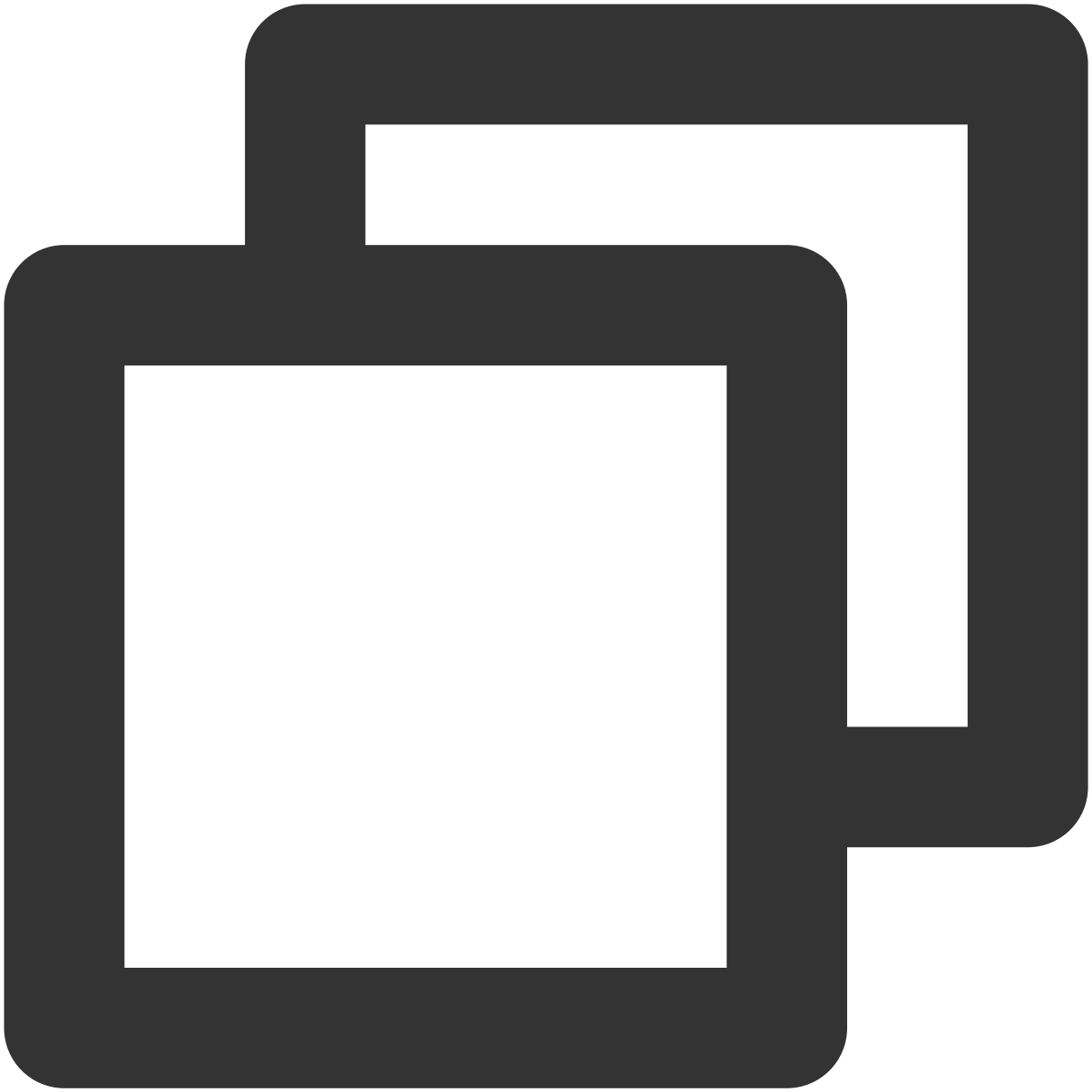
resource: detalhes de recursos de cada produto, como vpc/vpc_id1 ou vpc/*.

Por exemplo, você pode especificar uma instância (vpc-d08sl2zr neste caso) na instrução, conforme mostrado abaixo:



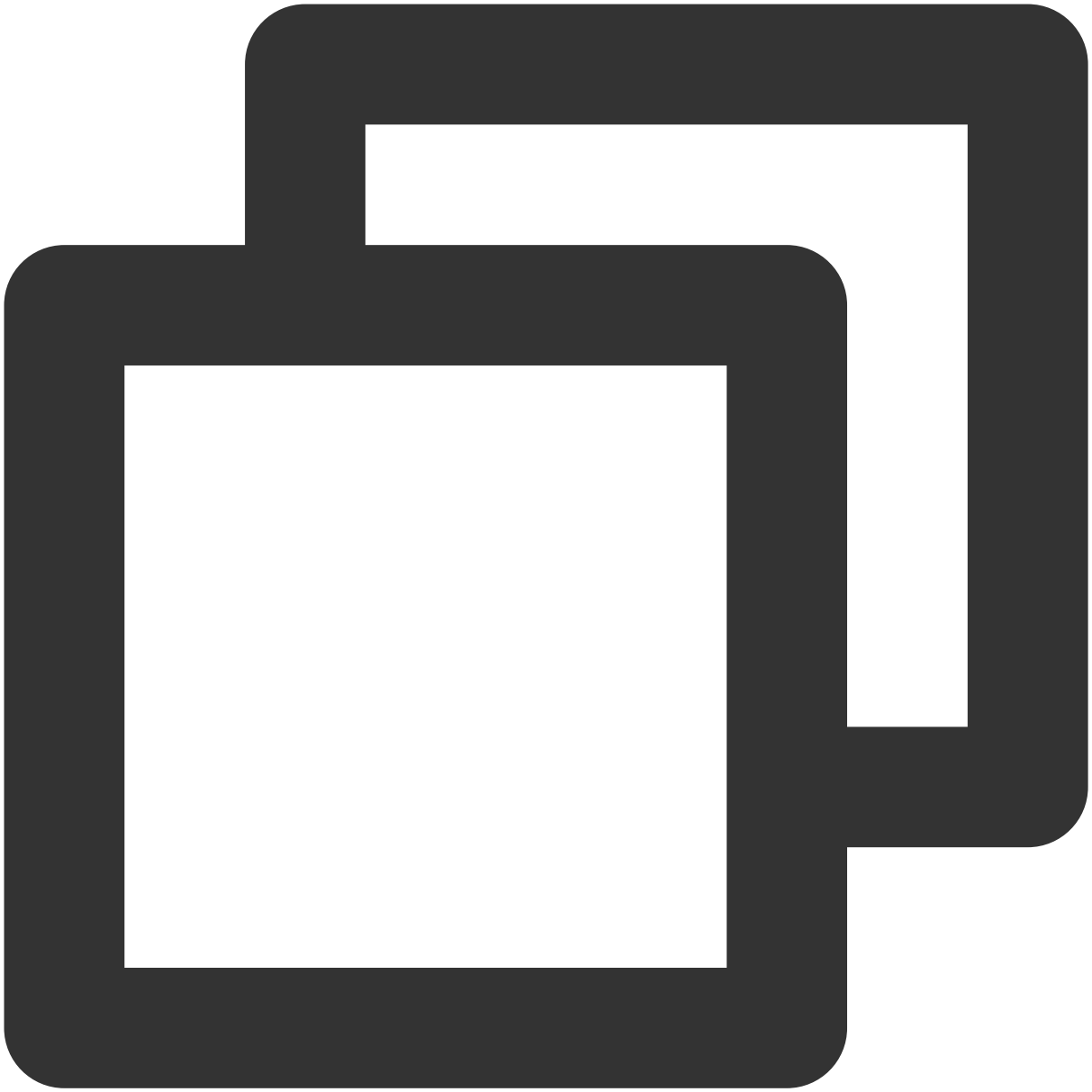
```
"resource":[ "qcs::vpc:bj:uin/164256472:instance/vpc-d08sl2zr"]
```

Você também pode usar o caractere curinga "*" para definir todas as instâncias de uma conta específica, conforme mostrado abaixo:



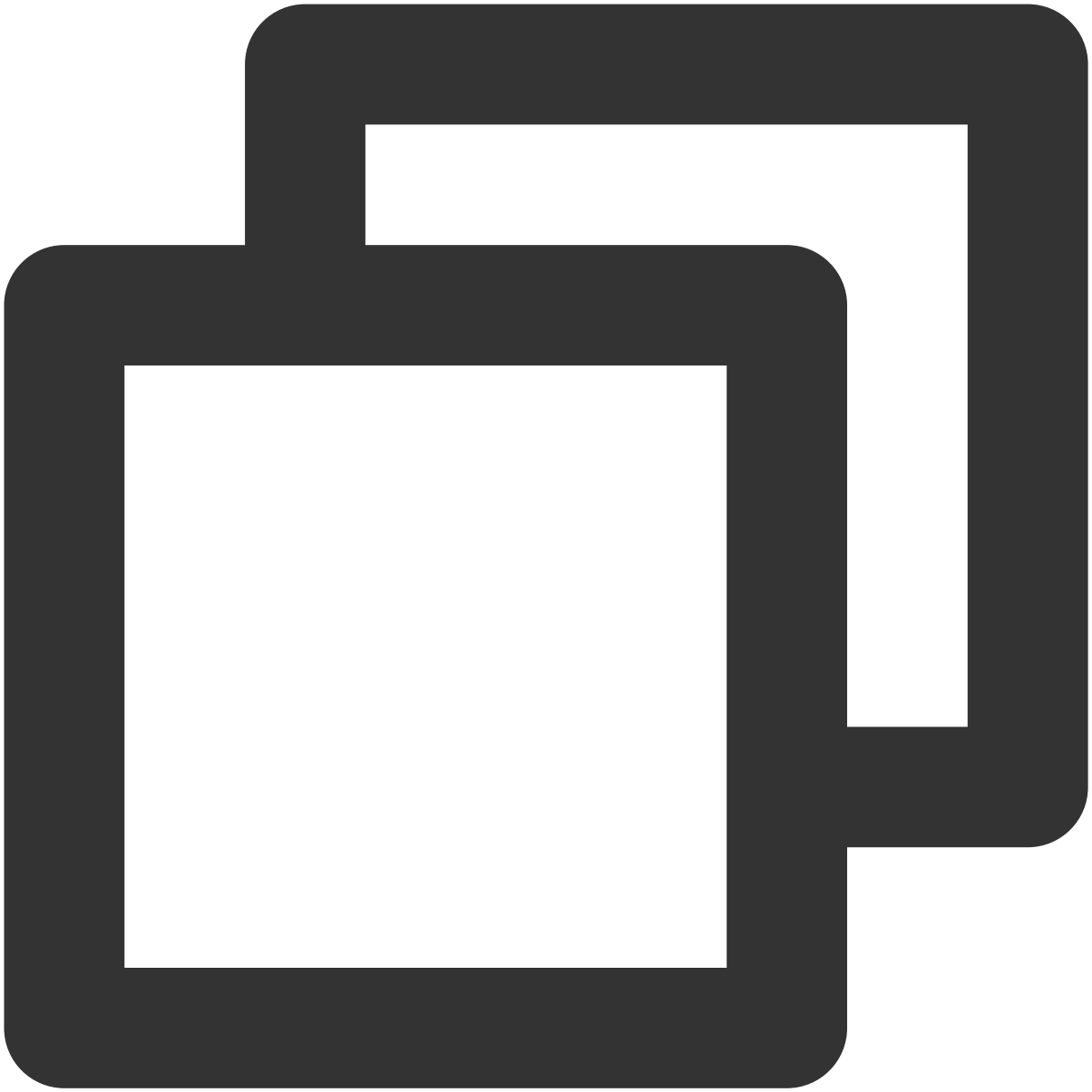
```
"resource":[ "qcs::vpc:bj:uin/164256472:instance/*"]
```

Para especificar todos os recursos ou se alguma ação da API não for compatível com permissões em nível de recurso, você pode usar o caractere curinga "*" no elemento de recurso, conforme mostrado abaixo:



```
"resource": ["*"]
```

Para especificar vários recursos em uma instrução, separe-os com vírgulas. No exemplo a seguir, dois recursos foram especificados:



```
"resource":["resource1","resource2"]
```

A tabela a seguir descreve os recursos que podem ser usados pelo VPC e os métodos correspondentes para descrever esses recursos.

Na tabela abaixo, as palavras prefixadas com "$" são nomes alternativos.

`project` indica o ID do projeto.

`region` indica a região.

`account` indica o ID da conta.

Recurso	Método de descrição de recursos na política de autorização

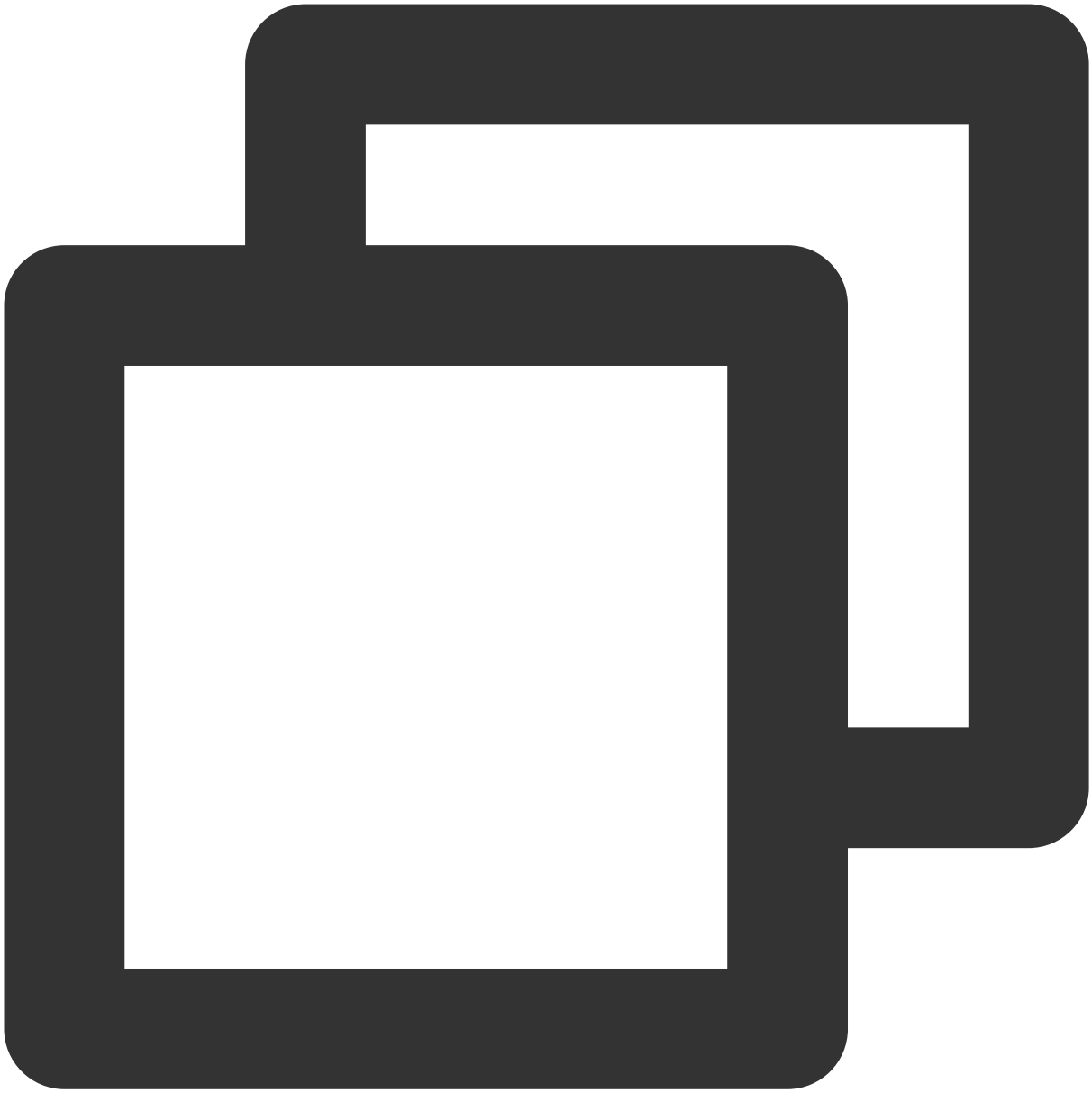
VPC	qcs::vpc:$region:$account:vpc/$vpcId
Sub-rede	qcs::vpc:$region:$account:subnet/$subnetId
Grupo de segurança	qcs::cvm:$region:$account:sg/$sgId
EIP	qcs::cvm:$region:$account:eip/*

Exemplos de políticas de gerenciamento de acesso ao VPC

Last updated：2024-01-24 17:55:51

Política de permissão de leitura e gravação completa do VPC

A seguinte política permite criar e gerenciar instâncias do VPC. É possível associar esta política a um grupo de administradores de rede. O elemento `Action (Ação)` especifica todas as APIs relacionadas ao VPC.

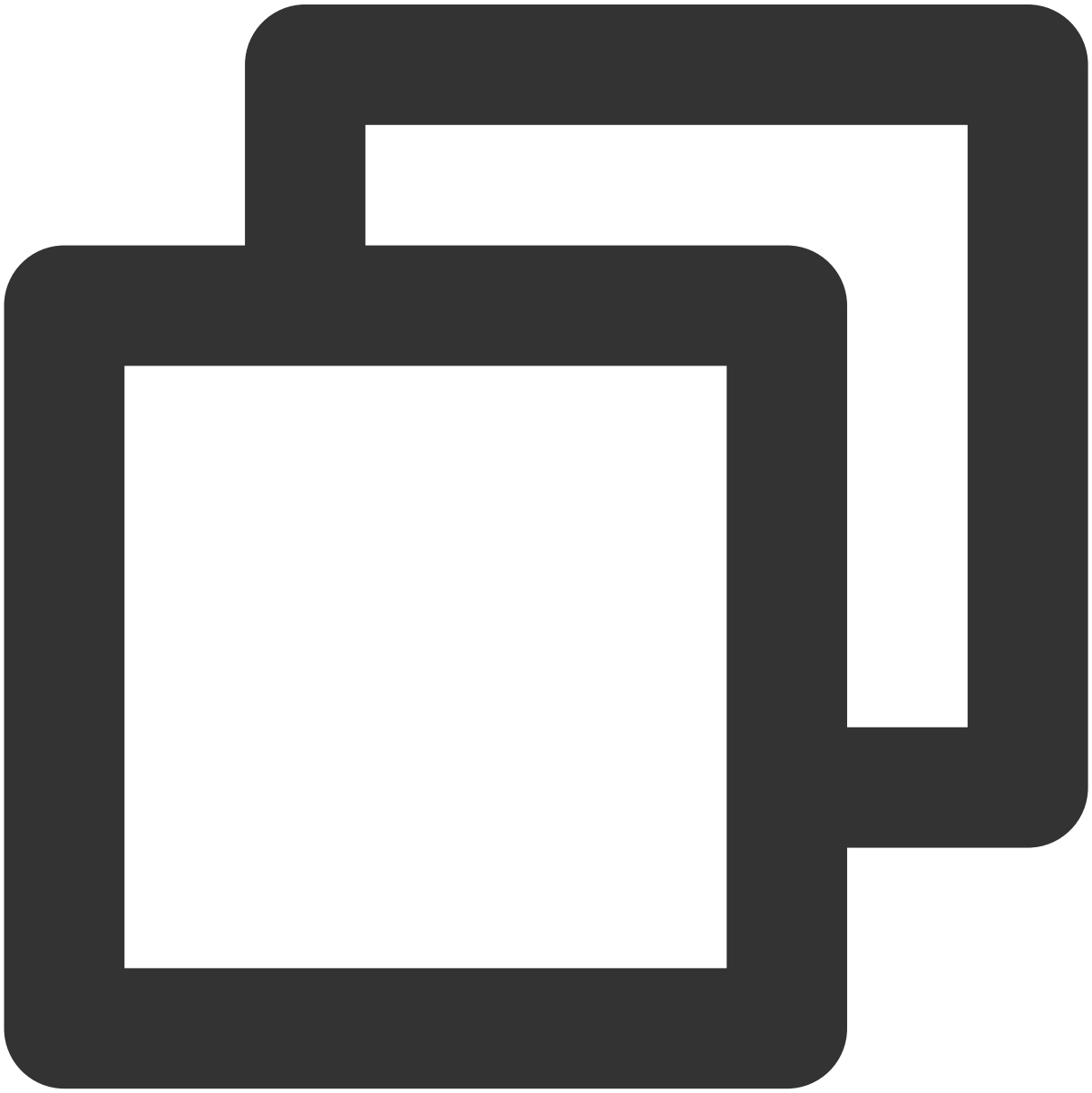


```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "name/vpc:*"
            ],
            "resource": "*",
            "effect": "allow"
        }
    ]
```

```
}
```

Política de permissão de somente leitura do VPC

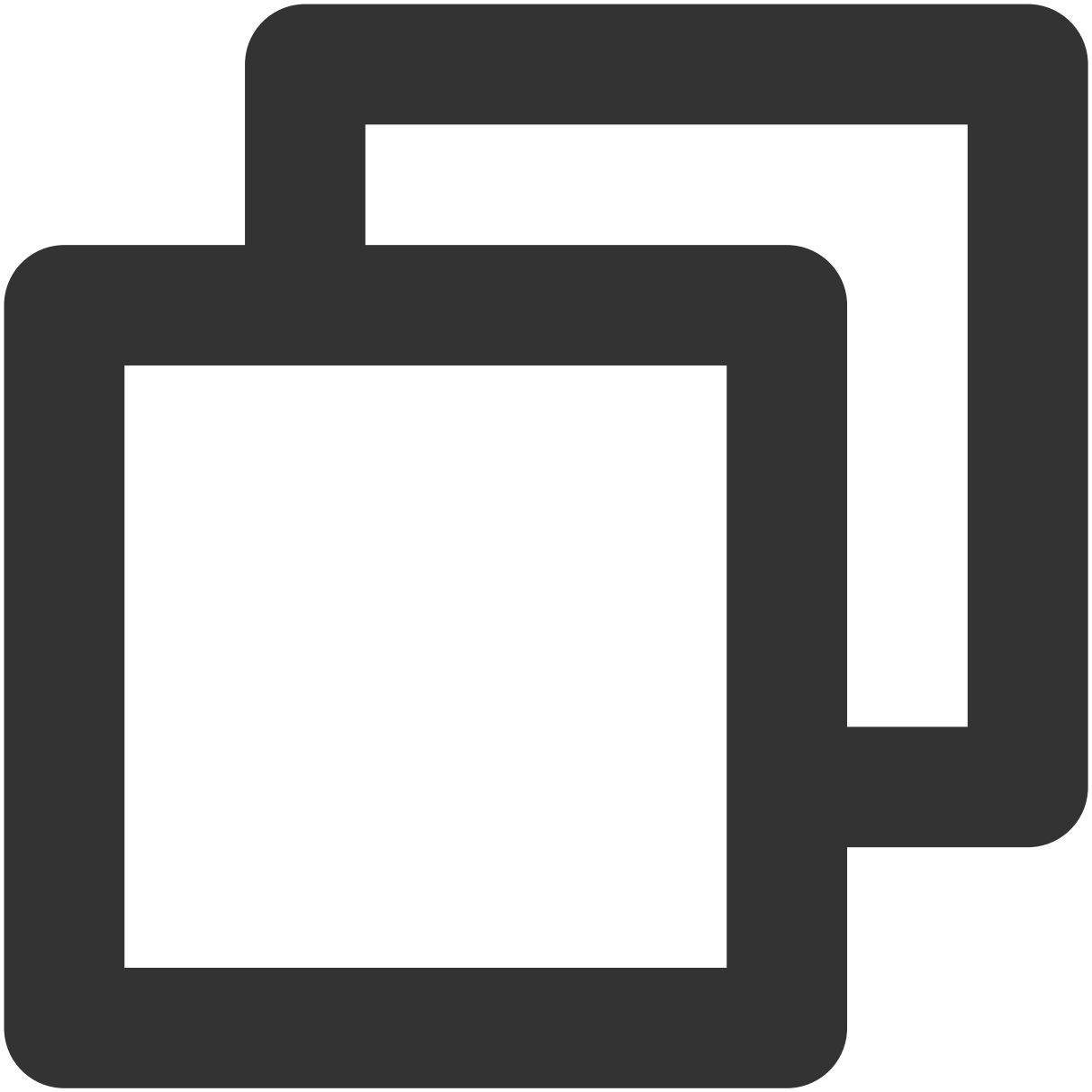
A política a seguir permite que você consulte seu VPC e os recursos relevantes. No entanto, não é possível criar, atualizar ou excluí-los com esta política.
Recomendamos que você conceda a permissão de somente leitura do VPC para os usuários, porque assim eles conseguem visualizar o recurso para operá-lo no console.



```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "name/vpc:Describe*",
                "name/vpc:Inquiry*",
                "name/vpc:Get*"
            ],
            "resource": "*",
            "effect": "allow"
        }
    ]
}
```

Permissão para gerenciar apenas um único VPC por uma subconta

A seguinte política permite que um usuário visualize todas as instâncias do VPC, mas apenas consiga operar o VPC A (por exemplo, o VPC A com um ID de vpc-d08sl2zr) e os recursos de rede no VPC A (como sub-redes e tabelas de rotas, mas excluindo Cloud Virtual Machines (CVMs) e bancos de dados). Em outras palavras, o usuário não tem permissão para gerenciar outras instâncias do VPC.
Esta versão não aceita **permitir que o usuário visualize apenas o VPC A**. Isso será possível em versões futuras.

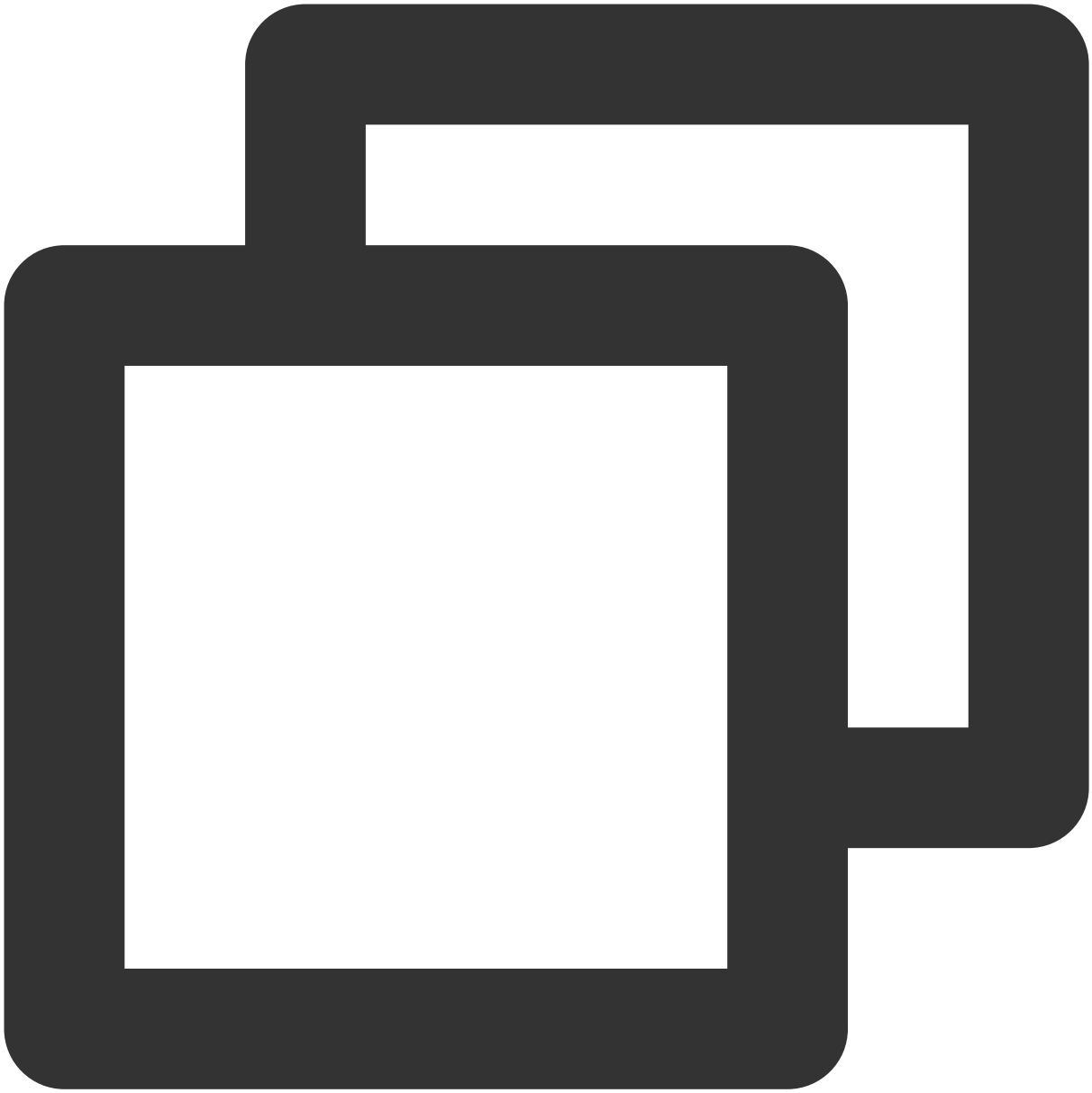


```
{
    "version": "2.0",
    "statement": [
        {
            "action": "name/vpc:*",
            "resource": "*",
            "effect": "allow",
            "condition": {
                "string_equal_if_exist": {  //Julgamento condicional: apenas instân
                    "vpc:vpc": [
                    "vpc-d08sl2zr"
```

```
                    ],
                    "vpc:accepter_vpc": [
                     "vpc-d08sl2zr"
                    ],
                     "vpc:requester_vpc": [
                     "vpc-d08sl2zr"
                    ]
                }
            }
        }
    ]
}
```

Permissão para um usuário gerenciar instâncias do VPC, exceto operar tabelas de rotas

A seguinte política permite que um usuário leia e grave instâncias do VPC e recursos relevantes, mas não permite que o usuário opere tabelas de rotas.

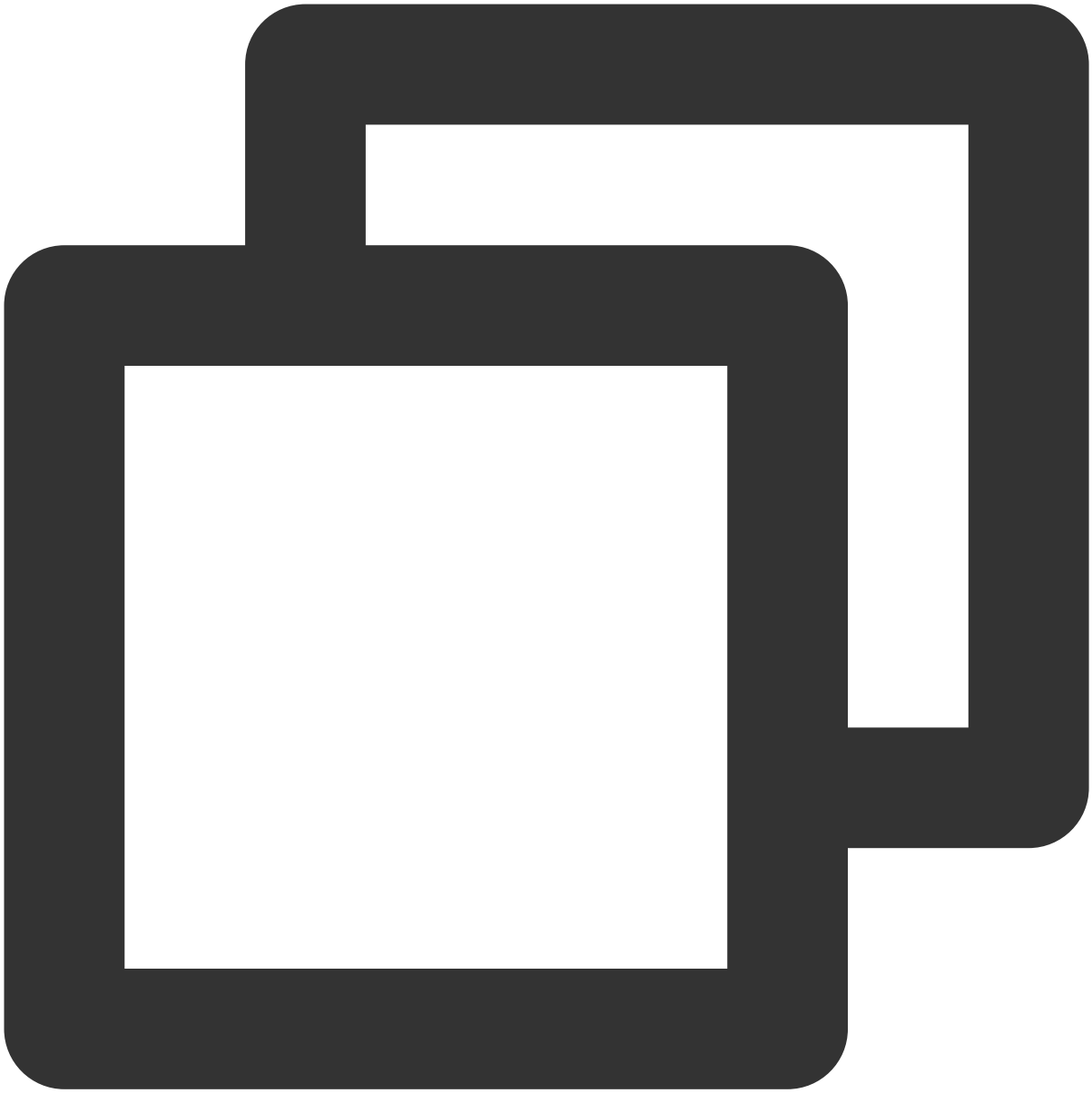


```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "name/vpc:*"
            ],
            "resource": "*",
            "effect": "allow"
        },
        {
```

```
            "action": [
                "name/vpc:AssociateRouteTable",
                "name/vpc:CreateRoute",
                "name/vpc:CreateRouteTable",
                "name/vpc:DeleteRoute",
                "name/vpc:DeleteRouteTable",
                "name/vpc:ModifyRouteTableAttribute"
            ],
            "resource": "*",
            "effect": "deny"
        }
    ]
}
```

Permissão para um usuário gerenciar recursos do VPN

A seguinte política permite que um usuário visualize todos os recursos do VPC, mas permite apenas que o usuário crie, leia, atualize e exclua os recursos do VPN (CRUD).



```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "name/vpc:Describe*",
                "name/vpc:Inquiry*",
                "name/vpc:Get*"
            ],
            "resource": "*",
            "effect": "allow"
```

```
        },
        {
            "action": [
                "name/vpc:*Vpn*",
                "name/vpc:*UserGw*"
            ],
            "resource": "*",
            "effect": "allow"
        }
    ]
}
```

Permissões de nível de recursos compatíveis com as APIs do VPC

Last updated：2024-01-24 17:55:51

You can authorize the following API operations for VPC resources in CAM. Resources supported by specific APIs and the corresponding conditions are as follows:

Nota：

Any VPC API operation that is not listed in the table does not support resource-level permissions. For such an operation, you can still authorize a user to perform it, but you must specify `*` as the resource element in the policy statement.

Operação da API	Recurso
AcceptVpcPeeringConnection	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
—	Recurso Peering Connection qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId
—	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId (the receiver’s vpcId)
AcceptVpcPeeringConnectionEx	Recurso Peering Connection qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId

—	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
AddVpnConnEx	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
—	Recurso VPN Gateway qcs::vpc:$region:$account:vpngw/* qcs::vpc:$region:$account:vpngw/$vpnGwId
—	Recurso gateway do cliente qcs::vpc:$region:$account:cgw/*
—	Recurso túnel VPN qcs::vpc:$region:$account:vpnx/*
AssignPrivateIpAddresses	Recurso ENI qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId
AssociateRouteTable	Recurso sub-rede qcs::vpc:$region:$account:subnet/* qcs::vpc:$region:$account:subnet/$subnetId
—	Recurso tabela de rotas qcs::vpc:$region:$account:rtb/* qcs::vpc:$region:$account:rtb/$routeTableId
AttachClassicLinkVpc	Recurso VPC qcs::vpc:$region:$account:vpc/*

	qcs::vpc:$region:$account:vpc/$vpcId
—	Recurso CVM qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId
AttachNetworkInterface	Recurso ENI qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId
—	Recurso CVM qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId
CreateAndAttachNetworkInterface	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
—	Recurso CVM qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId
—	Recurso ENI qcs::vpc:$region:$account:eni/*
CreateDirectConnectGateway	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
—	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/*
CreateLocalDestinationIPPortTranslationNatRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId

CreateLocalIPTranslationAclRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
CreateLocalIPTranslationNatRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
CreateLocalSourceIPPortTranslationAclRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
CreateLocalSourceIPPortTranslationNatRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
CreatePeerIPTranslationNatRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
CreateNatGateway	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
—	Recurso NAT Gateway qcs::vpc:$region:$account:nat/*
CreateNetworkAcl	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
—	Recurso ACL de rede qcs::vpc:$region:$account:acl/*

CreateNetworkInterface	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
—	Recurso sub-rede qcs::vpc:$region:$account:subnet/* qcs::vpc:$region:$account:subnet/$subnetId
—	Recurso ENI qcs::vpc:$region:$account:eni/*
CreateRoute	Recurso tabela de rotas qcs::vpc:$region:$account:rtb/* qcs::vpc:$region:$account:rtb/$routeTableId
CreateRouteTable	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
—	Recurso tabela de rotas qcs::vpc:$region:$account:rtb/*
CreateSubnet	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
—	Recurso gateway da sub-rede qcs::vpc:$region:$account:subnet/*
CreateSubnetAclRule	Recurso ACL de rede qcs::vpc:$region:$account:acl/* qcs::vpc:$region:$account:acl/$networkAclId
—	Recurso gateway da sub-rede qcs::vpc:$region:$account:subnet/*

CreateVpcPeeringConnection	Recurso VPC (iniciador) qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
—	Recurso Peering Connection qcs::vpc:$region:$account:pcx/*
CreateVpcPeeringConnectionEx	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
—	Recurso Peering Connection qcs::vpc:$region:$account:pcx/*
DeleteDirectConnectGateway	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId
DeleteLocalDestinationIPPortTranslationNatRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId
DeleteLocalIPTranslationAclRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId

DeleteLocalIPTranslationNatRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId
DeleteLocalSourceIPPortTranslationAclRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId
DeletePeerIPTranslationNatRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId
DeleteLocalSourceIPPortTranslationNatRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId
DeleteNatGateway	Recurso NAT Gateway qcs::vpc:$region:$account:nat/* qcs::vpc:$region:$account:nat/$natId
DeleteNetworkAcl	Recurso ACL de rede qcs::vpc:$region:$account:acl/* qcs::vpc:$region:$account:acl/$networkAclId
DeleteNetworkInterface	Recurso ENI qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId
DeleteRoute	Recurso tabela de rotas qcs::vpc:$region:$account:rtb/* qcs::vpc:$region:$account:rtb/$routeTableId

DeleteRouteTable	Recurso tabela de rotas qcs::vpc:$region:$account:rtb/* qcs::vpc:$region:$account:rtb/$routeTableId
DeleteSubnet	Recurso sub-rede qcs::vpc:$region:$account:subnet/* qcs::vpc:$region:$account:subnet/$subnetId
DeleteUserGw	Recurso gateway do cliente qcs::vpc:$region:$account:cgw/* qcs::vpc:$region:$account:cgw/$userGwId
DeleteVpc	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
DeleteVpcPeeringConnection	Recurso Peering Connection qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId
DeleteVpcPeeringConnectionEx	Recurso Peering Connection qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId
DeleteVpnConn	Recurso túnel VPN qcs::vpc:$region:$account:vpnx/*qcs::vpc:$region:$account:v

DetachClassicLinkVpc	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
—	Recurso CVM qcs::cvm:$region:$account:instance/*qcs::cvm:$region:$accou
DetachNetworkInterface	Recurso CVM qcs::cvm:$region:$account:instance/*qcs::cvm:$region:$accou
—	Recurso ENI qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId
DeteleSubnetAclRule	Recurso sub-rede qcs::vpc:$region:$account:subnet/* qcs::vpc:$region:$account:subnet/$subnetId
—	Recurso ACL de rede qcs::vpc:$region:$account:acl/* qcs::vpc:$region:$account:acl/$networkAclId
EipBindNatGateway	Recurso NAT Gateway qcs::vpc:$region:$account:nat/* qcs::vpc:$region:$account:nat/$natId
EipUnBindNatGateway	Recurso NAT Gateway qcs::vpc:$region:$account:nat/* qcs::vpc:$region:$account:nat/$natId
EnableVpcPeeringConnection	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId

—	Recurso Peering Connection qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId
EnableVpcPeeringConnectionEx	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
—	Recurso Peering Connection qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId
MigrateNetworkInterface	Recurso ENI qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId
—	Recurso CVM qcs::cvm:$region:$account:instance/*qcs::cvm:$region:$accou (permission is required before and after the migration)
MigratePrivateIpAddress	Recurso ENI qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId
ModifyDirectConnectGateway	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/*

	qcs::vpc:$region:$account:dcg/$directConnectGatewayId
ModifyLocalDestinationIPPortTranslationNatRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
ModifyLocalIPTranslationAclRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
ModifyLocalIPTranslationNatRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
ModifyLocalSourceIPPortTranslationAclRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
ModifyPeerIPTranslationNatRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
ModifyLocalSourceIPPortTranslationNatRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
ModifyNatGateway	Recurso NAT Gateway qcs::vpc:$region:$account:nat/* qcs::vpc:$region:$account:nat/nat-dc7cdf
ModifyNetworkAcl	Recurso ACL de rede qcs::vpc:$region:$account:acl/* qcs::vpc:$region:$account:acl/$networkAclId
ModifyNetworkAclEntry	Recurso ACL de rede qcs::vpc:$region:$account:acl/* qcs::vpc:$region:$account:acl/$networkAclId

ModifyNetworkInterface	Recurso ENI qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId
ModifyPrivateIpAddress	Recurso ENI qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId
ModifyRouteTableAttribute	Recurso tabela de rotas qcs::vpc:$region:$account:rtb/* qcs::vpc:$region:$account:rtb/$routeTableId
ModifySubnetAttribute	Recurso sub-rede qcs::vpc:$region:$account:subnet/* qcs::vpc:$region:$account:subnet/$subnetId
ModifyUserGw	Recurso gateway do cliente qcs::vpc:$region:$account:cgw/* qcs::vpc:$region:$account:cgw/$userGwId
ModifyVpcAttribute	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
ModifyVpcPeeringConnection	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
—	Recurso Peering Connection qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId

ModifyVpcPeeringConnectionEx	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
—	Recurso Peering Connection qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId
ModifyVpnConnEx	Recurso túnel VPN qcs::vpc:$region:$account:vpnx/* qcs::vpc:$region:$account:vpnx/$vpnConnId
ModifyVpnGw	Recurso VPN Gateway qcs::vpc:$region:$account:vpngw/* qcs::vpc:$region:$account:vpngw/$vpnGwId
RejectVpcPeeringConnection	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
—	Recurso Peering Connection qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId

RejectVpcPeeringConnectionEx	Recurso VPC qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId
—	Recurso Peering Connection qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId
ResetVpnConnSA	Recurso túnel VPN qcs::vpc:$region:$account:vpnx/* qcs::vpc:$region:$account:vpnx/$vpnConnId
SetLocalIPTranslationAclRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
SetLocalSourceIPPortTranslationAclRule	Recurso gateway do Direct Connect qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId
SetSSLVpnDomain	Recurso VPN Gateway qcs::vpc:$region:$account:vpngw/* qcs::vpc:$region:$account:vpngw/$vpnGwId
UnassignPrivateIpAddresses	Recurso ENI

	qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId

Ferramentas de diagnóstico
Sonda de rede

Last updated：2024-01-24 17:55:51

O serviço de sondagem de rede da Tencent Cloud é usado para monitorar a qualidade das conexões de rede da VPC, incluindo a latência, a taxa de perda de pacotes e outras métricas importantes.
Na arquitetura de rede de nuvem híbrida, você cria uma sonda de rede na sub-rede que precisa se comunicar com o IDC para monitorar a taxa de perda de pacotes e a latência da ligação sondada. A configuração permite:
Monitorar a qualidade da conexão
Receber alertas em caso de falhas de conexão

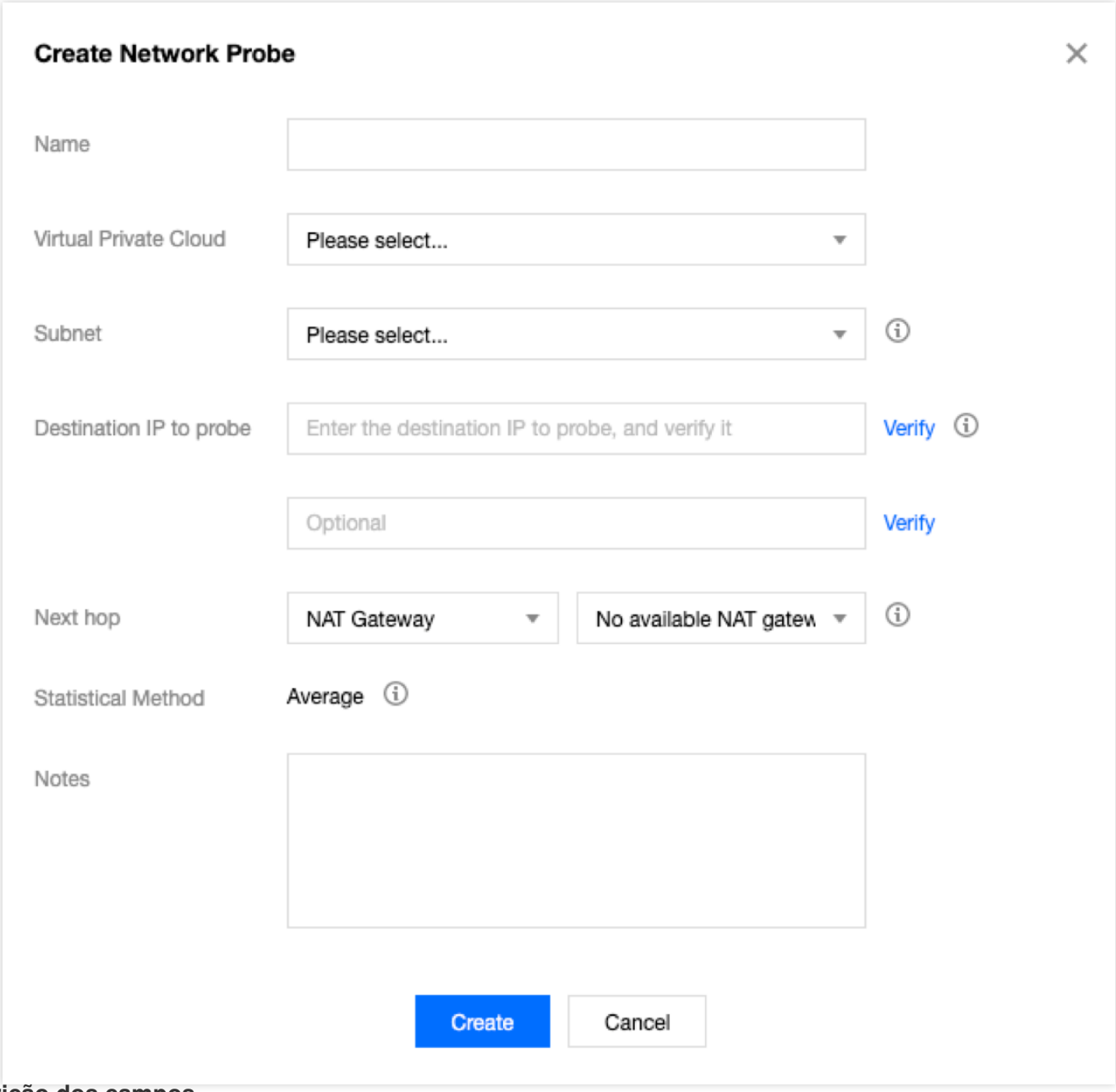
Instruções

O serviço de sondagem de rede adota o método ping com uma frequência de 20 pings por minuto.
São permitidas até 50 sondas para cada VPC.
É possível ter sondas de rede em no máximo 20 sub-redes na mesma VPC.

Criação de uma sonda de rede

1. Faça login no console da VPC.
2. Selecione **Diagnostic Tools (Ferramentas de diagnóstico)** -> **Network Probe (Sonda de rede)** na barra lateral esquerda, para acessar a página de gerenciamento.
3. Clique em **+New (+Novo)** na parte superior da página **Network Probe (Sonda de rede)**.
4. Na janela pop-up **Create Network Probe (Criar sonda de rede)**, preencha os campos relevantes.

Nota:
A rota da sonda de rede é atribuída pelo sistema e não pode ser modificada.
Quando você muda a rota da sub-rede, esta rota padrão será removida da tabela de rotas original associada à sub-rede e adicionada à nova tabela de rotas associada.



Descrição dos campos

Campo	Configuração
Name (Nome)	Nome da sonda de rede.
VPC	A VPC ao qual pertence o IP de origem da sonda.
Subnet (Sub-rede)	A sub-rede à qual pertence o IP de origem da sonda.
Probe Destination IP (IP de destino da sonda)	São aceitos no máximo dois IPs de destino para a sonda de rede. Não se esqueça de ativar a política de firewall ICMP para o servidor de destino da sonda de rede.
Source Next Hop (Próximo salto de origem)	Você pode escolher Specify (Especificar) ou Do Not Specify (Não especificar) o próximo salto.

	Se Do Not Specify (Não especificar)for marcado, nenhum próximo salto será selecionado. **Nota：** Atualmente, a opção Do Not Specify (Não especificar) só está disponível para usuários beta. Para ativá-la, envie um tíquete. Se você especificar o próximo salto, selecione o tipo do próximo salto e as instâncias. Depois, o sistema adiciona automaticamente a rota de 32 bits correspondente à tabela de rotas associada à sub-rede. Atualmente, o tipo do próximo salto aceito inclui NAT Gateway, Peering Connections, gateway do VPN, gateway do Direct Connect, CVM e CCN. **Nota：** Se você especificar o CCN como o próximo salto e os IPs de destino da sonda pertencerem a dois VPCs no CCN, o intervalo de IP com a máscara mais longa será correspondido e entrará em vigor.

5. (Opcional) **Verifique** o **IP de destino da sonda**.

Nota:

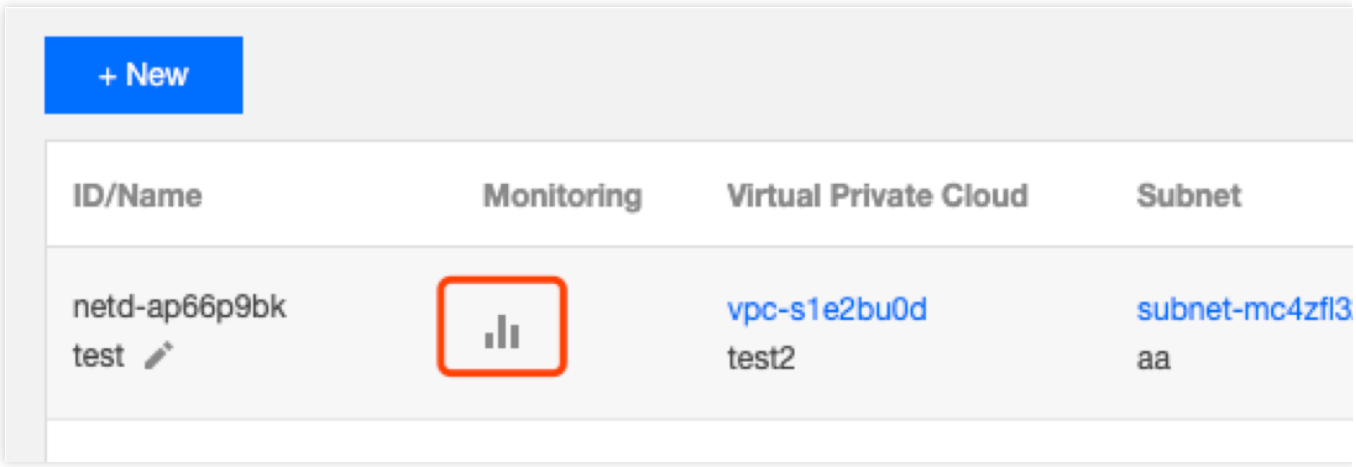
Ignore essa etapa se você não especificar o próximo salto.

Se a conexão obtiver êxito, clique em **OK**.

Se a conexão falhar, verifique se a rota da sub-rede está configurada corretamente e se o dispositivo de sonda habilita a ACL de rede, o grupo de segurança ou outros firewalls, que podem bloquear a conexão. Para mais informações, consulte Gerenciamento de ACLs de rede e Modificação de uma regra de grupo de segurança.

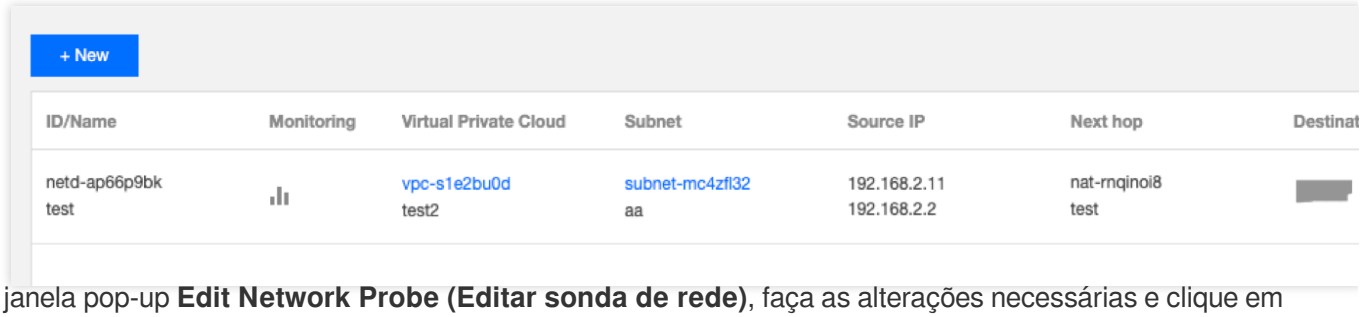
Verificação da latência e perda de pacotes de uma sonda de rede

1. Faça login no console da VPC.
2. Selecione **Diagnostic Tools (Ferramentas de diagnóstico)** -> **Network Probe (Sonda de rede)** na barra lateral esquerda, para acessar a página de gerenciamento.
3. Clique no ícone de monitoramento da instância de sonda de rede em questão para exibir sua latência e taxa de perda de pacotes.



Modificação de uma sonda de rede

1. Faça login no console da VPC.
2. Selecione **Diagnostic Tools (Ferramentas de diagnóstico)** -> **Network Probe (Sonda de rede)** na barra lateral esquerda, para acessar a página de gerenciamento.
3. Na lista, localize a sonda de rede a ser modificada e clique em **Edit (Editar)** na coluna **Operation (Operação)**.



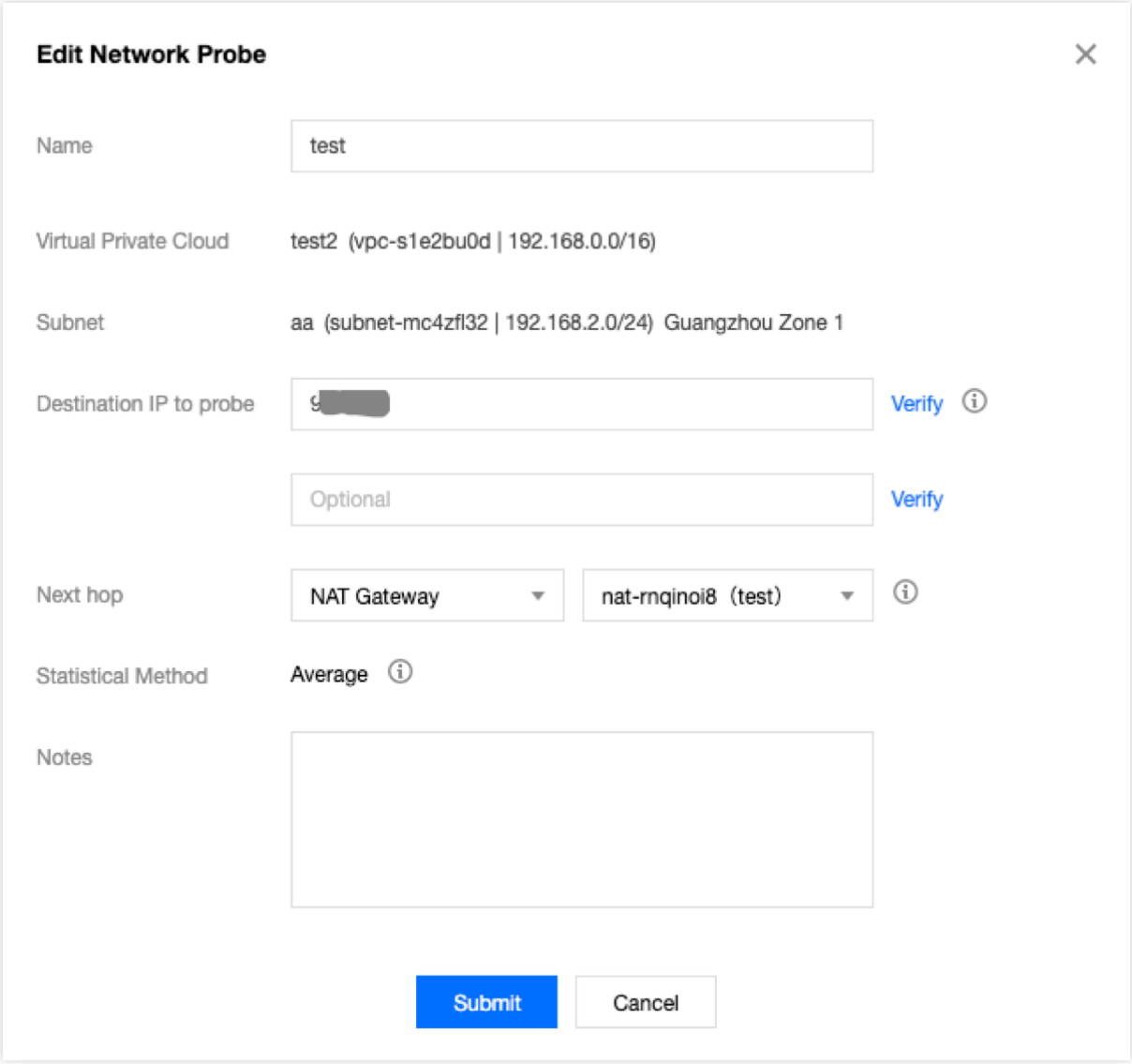
4. Na janela pop-up **Edit Network Probe (Editar sonda de rede)**, faça as alterações necessárias e clique em **Submit (Enviar)** para salvar as alterações.

Nota:

Esse exemplo não tem o próximo salto especificado.

Se nenhum próximo salto for especificado, o nome, o IP de destino da sonda e as observações da sonda de rede podem ser modificados.

Se algum próximo salto for especificado, o nome, o IP de destino da sonda, o próximo salto da origem e as observações da sonda de rede podem ser modificados.

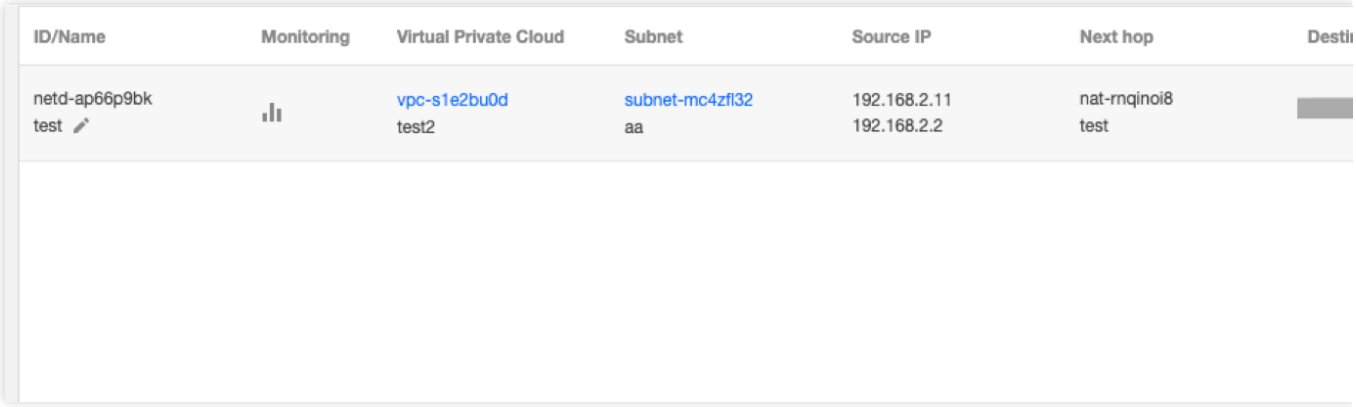


Exclusão de uma sonda de rede

1. Faça login no console da VPC.
2. Selecione **Diagnostic Tools (Ferramentas de diagnóstico)** -> **Network Probe (Sonda de rede)** na barra lateral esquerda, para acessar a página de gerenciamento.
3. Na lista, localize a sonda de rede a ser excluída e clique em **Delete (Excluir)** na coluna **Operation (Operação)**.
4. Clique em **Delete (Excluir)** na janela pop-up para confirmar a exclusão.

Atenção:

A exclusão de uma sonda de rede também exclui todas as políticas de alarme associadas e as rotas configuradas. Verifique se os seus negócios serão afetados antes de continuar.



Configuração de uma política de alarme

Você pode configurar uma política de alarme para o serviço de sondagem de rede, para que possa detectar prontamente qualquer exceção de rota, a fim de ajudar a alternar as rotas rapidamente e a garantir a disponibilidade dos negócios.

1. Faça login no console do CM e acesse a página **Alarm Policy (Política de alarme)**.
2. Clique em **Create (Criar)**.
3. Na janela pop-up **Create Alarm Policy (Criar política de alarme)**, insira o nome da política, selecione **Network Probe (Sonda de rede)** para o tipo de política, configure o objeto de alarme, a condição de disparo do alarme e a política de alarme e clique em **Complete (Concluir)**.

Verificação de portas de instâncias

Last updated：2024-01-24 17:55:51

A funcionalidade de verificação de portas da instância pode ajudar a detectar a acessibilidade da porta de um grupo de segurança associado a instâncias do CVM, localizar falhas e melhorar a experiência do usuário.
Essa funcionalidade aceita detecção de acessibilidade de portas comuns e personalizadas. Confira abaixo as portas comuns.

Regra	Porta	Descrição
Regras de entrada	Protocolo ICMP	Usado para passar mensagens de controle, como o comando ping. ICMP é um protocolo de controle e nenhuma porta está envolvida.
	TCP:20	Usada para permitir uploads e downloads por FTP.
	TCP:21	
	TCP:22	Usada para permitir login SSH no Linux.
	TCP:3389	Usada para permitir login remoto no Windows.
	TCP:443	Usada para fornecer serviço HTTPS de sites.
	TCP:80	Usada para fornecer serviço HTTP de sites.
Regras de saída	TODAS	Usada para permitir todo o tráfego de saída para acesso a redes externas.

Guia de operação

1. Faça login no Console do VPC.
2. Clique em **Diagnostic Tools (Ferramentas de diagnóstico)** > **Port Verification (Verificação de portas)** na barra lateral esquerda, para acessar a página de gerenciamento.
3. Selecione uma região na parte superior da página, localize a instância que deseja verificar na lista e clique em **Quick Check (Verificação rápida)**.
4. Você pode visualizar os detalhes de detecção da porta na janela pop-up. Execute as seguintes operações conforme necessário.
Desmarque a porta que você não deseja detectar.
Insira portas personalizadas para detectar e clique em **Save (Salvar)**.
Protocol (Protocolo): selecione TCP ou UDP.

Port (Porta): insira um número de porta a ser detectado, que não pode ser igual a uma porta comum. Caso contrário, você precisa primeiro desmarcar a porta comum antes de continuar.
Direction (Direção): selecione **Inbound (Entrada)** ou **Outbound (Saída)**.
IP: insira o IP de origem para a direção de entrada e o IP de destino para a direção de saída. Insira **ALL (TODOS)** para todos os endereços IP de origem e destino.
É possível detectar até 15 portas personalizadas.
Se você precisar detectar o tráfego de saída para o IP 10.0.1.12 usando o protocolo TCP por meio da porta 30, insira as seguintes informações na área **Custom port detection (Detecção de porta personalizada)**.
5. Quando concluir a configuração, clique em **Detect (Excluir)**. O resultado será exibido na coluna **Policy (Política)**.
Suponha que você precisa abrir uma porta **Not opened (Não aberta)**, por exemplo **TCP:22**,
Depois, você pode adicionar uma regra de entrada para o grupo de segurança associado à instância no console do grupo de segurança para abrir a porta TCP:22. Você pode selecionar **all (todos)** para **Source (Origem)**, a fim de permitir todos os IPs, ou inserir um IP (intervalo de IP) específico.

Informações relevantes

Para obter informações sobre grupos de segurança, consulte Visão geral de grupos de segurança e Adição de uma regra de grupo de segurança.
Para obter mais informações sobre portas comuns, consulte Portas de servidor comuns.

Logs de fluxo

Last updated：2024-01-24 17:55:51

Os Logs de fluxo (FL) fornecem um serviço de captura de tráfego em tempo real, de fluxo completo e não intrusivo para que você possa armazenar e analisar o tráfego de rede em tempo real. Isso ajuda a realizar solução de problemas, otimização de arquitetura, testes de segurança e auditoria de conformidade.

Procedimentos comuns

Criação de logs de fluxo
Criação de conjuntos de log e tópicos de log
Exclusão de logs de fluxo
Exibição de entradas de log de fluxo

Espelhamento de tráfego
Visão geral

Last updated：2024-01-24 17:55:51

O espelho de tráfego fornece um serviço de coleta de tráfego que filtra e copia o tráfego desejado da interface de rede especificada para instâncias do CVM no mesmo VPC. Essa funcionalidade é aplicável a casos de uso, incluindo auditoria de segurança, monitoramento de risco, solução de problemas e análise empresarial.

Nota:

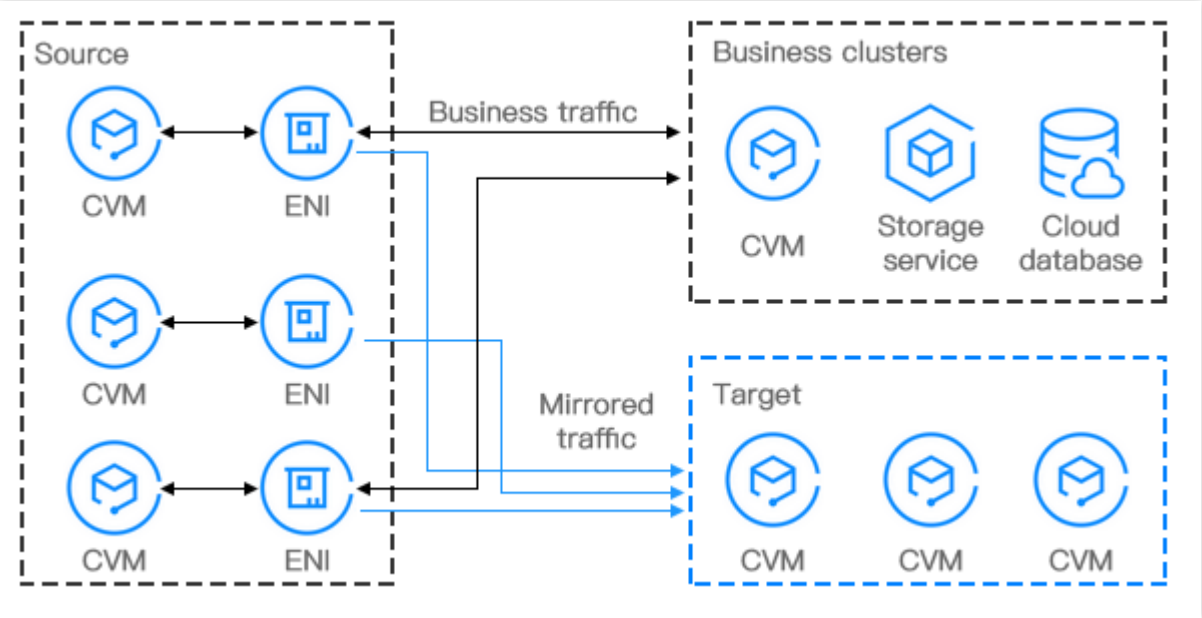
No entanto, o espelho de tráfego consome recursos do CVM como CPU, memória e largura de banda proporcionalmente. Considere como exemplo você espelhar uma interface de rede que tem 1 Gbps de tráfego de entrada e 1 Gbps de tráfego de saída. Nesse caso, a instância precisa lidar com 1 Gbps de tráfego de entrada e 3 Gbps de tráfego de saída (1 Gbps para o tráfego de saída, 1 Gbps para o tráfego de entrada espelhado e 1 Gbps para o tráfego de saída espelhado).

Procedimento

Veja abaixo os principais componentes de um espelho de tráfego, junto com seu fluxo de trabalho.

Source (Origem): o ENI especificado no VPC que aplica as regras de filtro, como rede, intervalo de coleta, tipo de coleta e filtragem de tráfego.

Target (Destino): os IPs de recebimento que obtêm o tráfego coletado.



Casos de uso

Auditoria de segurança

Um sistema em execução pode acarretar tráfego de rede não íntegro ou gerar uma mensagem de erro devido a exceção de software, falha de hardware, vírus de computador ou uso impróprio. Para localizar as causas desses problemas, é possível usar o espelho de tráfego para analisar as mensagens da rede.

Verificação de intrusão

Para garantir a confidencialidade, integridade e disponibilidade dos recursos do sistema de rede, é possível usar o espelho de tráfego para copiar o tráfego para clusters do CVM, para análise em tempo real.

Análise empresarial

Use o espelho de tráfego para apresentar o modo de tráfego da empresa de forma clara e visual.

Limites de serviço

Last updated：2024-01-24 17:55:51

Considere as informações a seguir e mantenha sua empresa intacta ao usar o espelho de tráfego.
Atualmente, o espelho de tráfego está em teste beta. Para solicitá-lo, envie um tíquete. Recomendamos salvar o link do console do Espelho de tráfego, para que você possa fazer login no console sem precisar solicitar novamente.
O espelho de tráfego consome recursos do CVM como CPU, memória e largura de banda proporcionalmente.
O tráfego espelhado é contabilizado para a largura de banda da instância. O impacto depende do volume e do tipo de tráfego. Considere como exemplo você espelhar uma interface de rede que tem 1 Gbps de tráfego de entrada e 1 Gbps de tráfego de saída. Nesse caso, a instância precisa lidar com 1 Gbps de tráfego de entrada e 3 Gbps de tráfego de saída (1 Gbps para o tráfego de saída, 1 Gbps para o tráfego de entrada espelhado e 1 Gbps para o tráfego de saída espelhado).
Os Logs de fluxo não capturam o tráfego espelhado.
Limites em relação a um grupo de segurança:
Origem: o tráfego espelhado não está sujeito às políticas do grupo de segurança.
Destino: o tráfego recebido está sujeito às políticas do grupo de segurança.
O espelho de tráfego não está disponível para:
Protocolo de resolução de endereço
DHCP
Serviço de metadados de instância
NTP
Ativação do Windows
O espelho de tráfego permite a coleta de tráfego de um ENI nos seguintes tipos de CVM:
S1 padrão, S2 padrão, S3 padrão, Memória otimizada M1, Memória otimizada M2, Memória otimizada M3, Alta E/S I1, Alta E/S I2, Alta E/S I3, Computação C2, Computação C3, Computação com rede otimizada CN3 e Big Data D1.

Criação de espelho de tráfego

Last updated：2024-01-24 17:55:51

O Espelho de tráfego fornece um serviço de coleta de tráfego que permite filtrar o tráfego do ENI especificado usando 5 tuplas e outras regras. Depois, é possível copiar o tráfego filtrado para as instâncias da CVM no mesmo VPC. Essa funcionalidade é aplicável a casos de uso que incluem: auditoria de segurança, monitoramento de risco, solução de problemas e análise empresarial. Este documento descreve como criar um espelho de tráfego.

Nota:

Atualmente, a funcionalidade Espelho de tráfego está na versão beta. Se você quiser testá-la, envie um tíquete.

Salve o link do console do Espelho de tráfego para logins posteriores; caso contrário, pode ser necessário solicitar novamente.

Pré-requisitos

Confira se o IP de origem e a ENI de destino estão na mesma VPC, e se o IP de origem tem uma tabela de rotas apontando para a ENI de destino.

Instruções

Etapa 1: criar uma origem de espelho de tráfego

1. Abra o link que você recebeu após enviar um tíquete e faça login no console do Espelho de tráfego. No seletor **Region (Região)** superior, selecione a região na qual o espelho de tráfego será criado.
2. Clique em **+New (+Novo)**.

Nota:

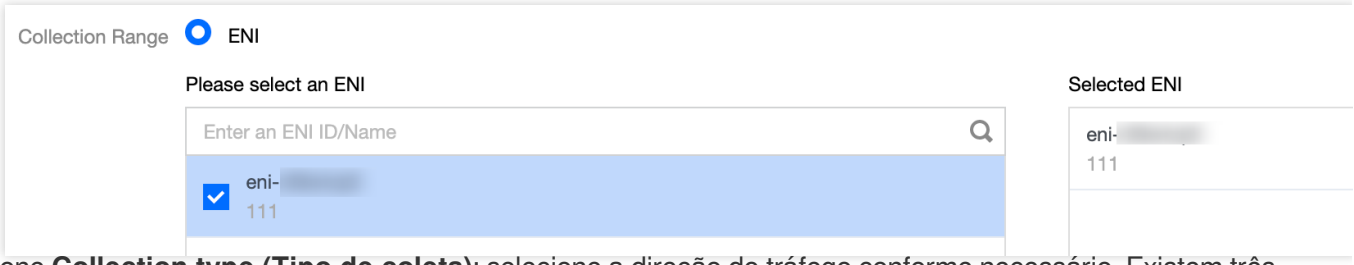
É possível criar até 5 espelhos de tráfego em uma VPC.

3. Na janela pop-up, configure da seguinte maneira:

Insira um nome para o espelho de tráfego (até 60 caracteres).

Selecione **Network (Rede)**.

Selecione **ENI** para **Collection Range (Intervalo de coleta)**. Ou seja, todo o tráfego na VPC será coletado, mas será excluído o tráfego da ENI que está vinculada aos IPs de recebimento. Esta opção requer a seleção de ENIs específicas.

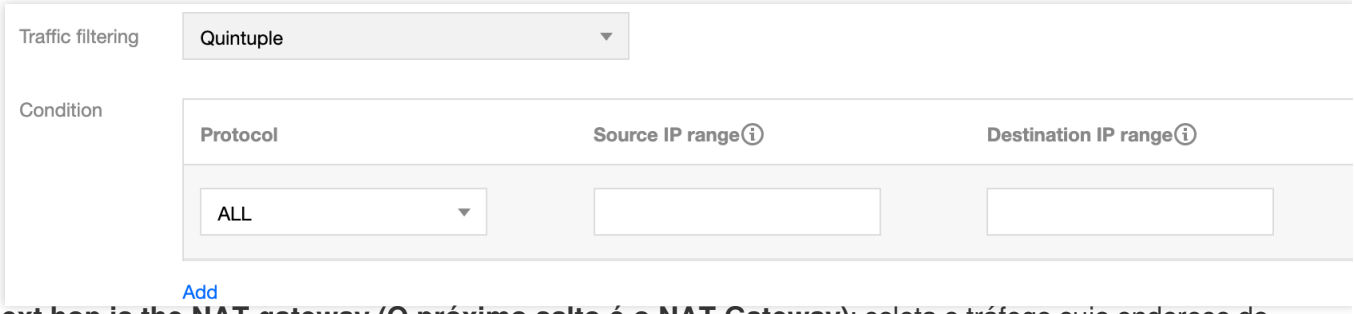


Selecione **Collection type (Tipo de coleta)**: selecione a direção do tráfego conforme necessário. Existem três opções: All traffic (Todo o tráfego), Traffic out (Tráfego de saída) e Traffic in (Tráfego de entrada).

Selecione **Traffic filtering (Filtragem de tráfego)**: selecione um método para filtrar o tráfego desnecessário e manter o espelho pequeno e leve.

N/A: todo o tráfego configurado será coletado.

Quintuple (Quíntuplo): o tráfego que atender às condições de 5 tuplas será coletado. Depois que essa opção for selecionada, especifique o **Protocol (Protocolo)**, o **Source IP range (Intervalo de IP de origem)**, o **Destination IP range (Intervalo de IP de destino)**, a **Source port (Porta de origem)** e a **Destination port (Porta de destino)**. Você pode clicar em **Add (Adicionar)** para criar outra condição de filtro. Apenas o tráfego que atender a todas as condições de filtro será coletado.



The next hop is the NAT gateway (O próximo salto é o NAT Gateway): coleta o tráfego cujo endereço do próximo salto é o NAT Gateway. Após selecionar essa opção, selecione o NAT Gateway correspondente ao lado de **Condition (Condição)**.

4. Quando concluir a configuração, clique em **Next (Avançar)**.

Etapa 2: criar um destino de espelho de tráfego

1. Defina o tráfego de recebimento da seguinte maneira:

Target type (Tipo de destino): selecione a ENI de destino para receber o tráfego.

Nota:

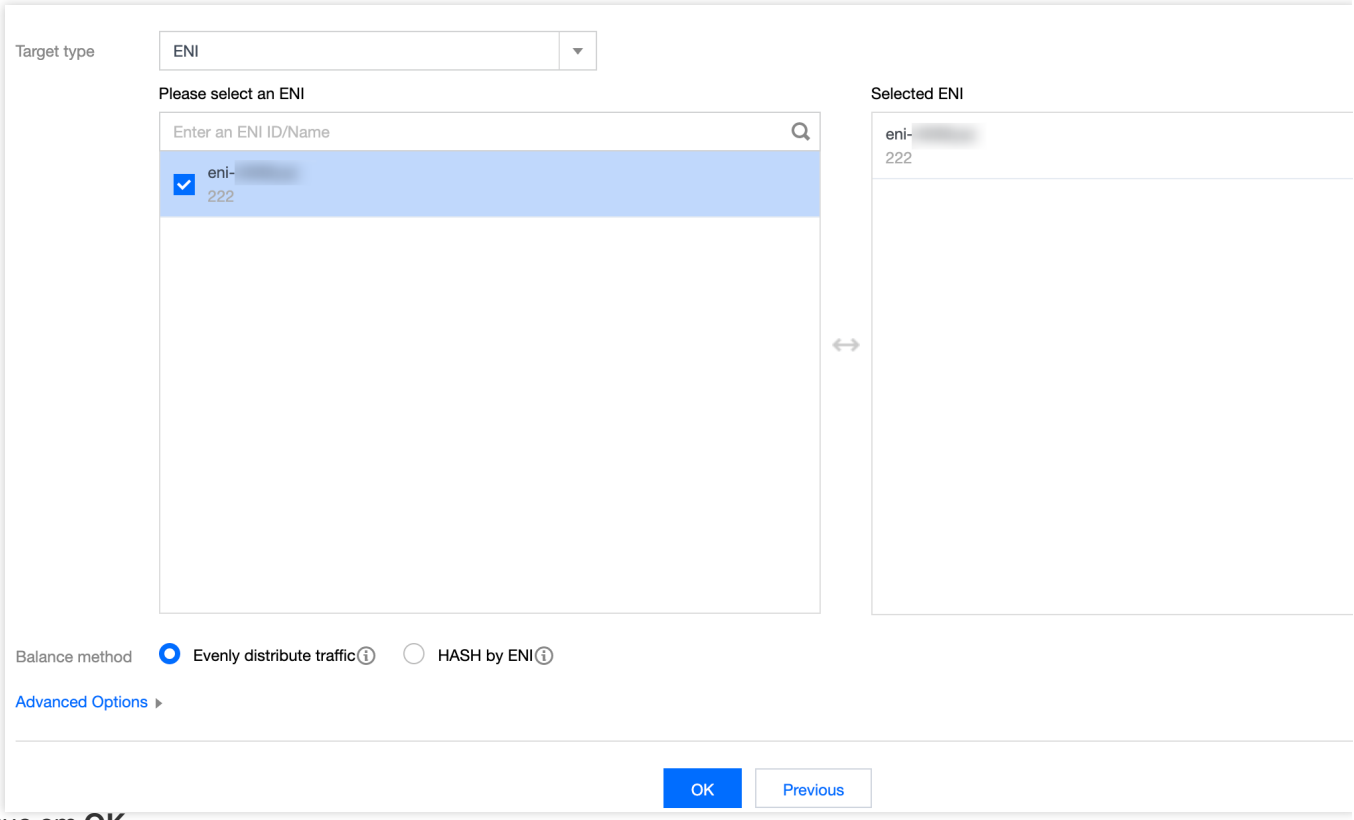
Pelo menos uma ENI de destino precisa ser selecionada.

O tráfego para a ENI de destino de dentro da VPC não é coletado.

Balance method (Método de equilíbrio):

Evenly distribution (Distribuição uniforme): todo o tráfego é distribuído uniformemente entre todas as ENIs de destino.

HASH by ENI (HASH por ENI): o tráfego de uma ENI é sempre encaminhado para uma ENI de destino fixo.



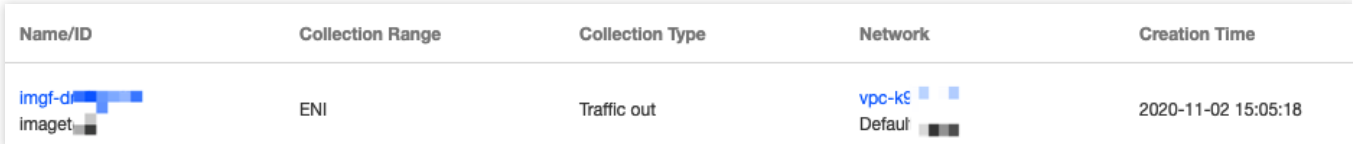
2. Clique em **OK**.

Validação do resultado

Atenção:

Este documento usa como exemplo a criação de um espelho de tráfego que coleta o tráfego de saída da ENI 10.0.0.14, acessando o site www.qq.com.

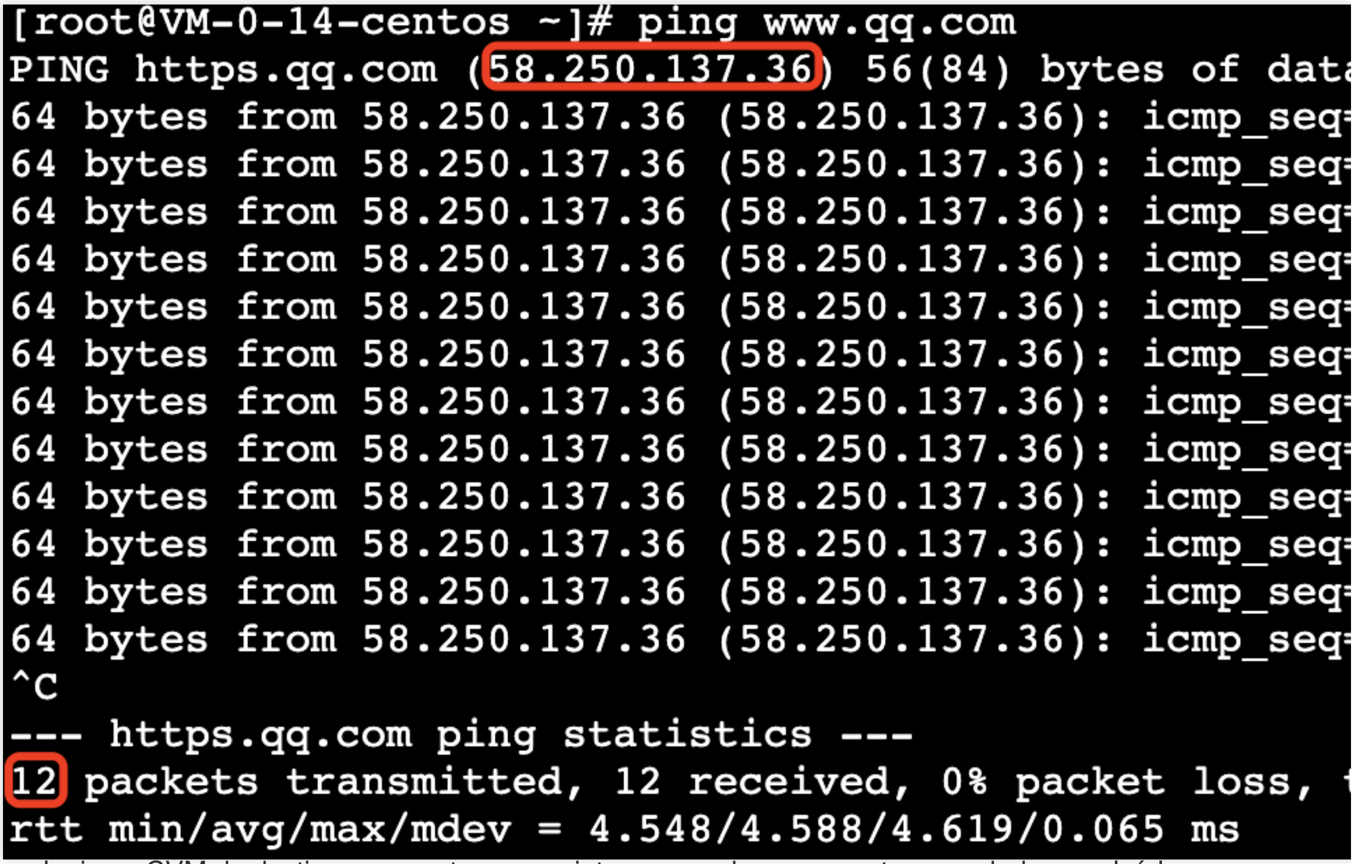
1. Volte para a página **Traffic mirroring (Espelhamento de tráfego)**. Se o espelho de tráfego recém-criado for exibido com **Collect Traffic (Coletar tráfego)** habilitado, significa que ele foi criado com êxito.



2. Execute as etapas a seguir para verificar se o tráfego coletado é espelhado para o IP de recebimento.

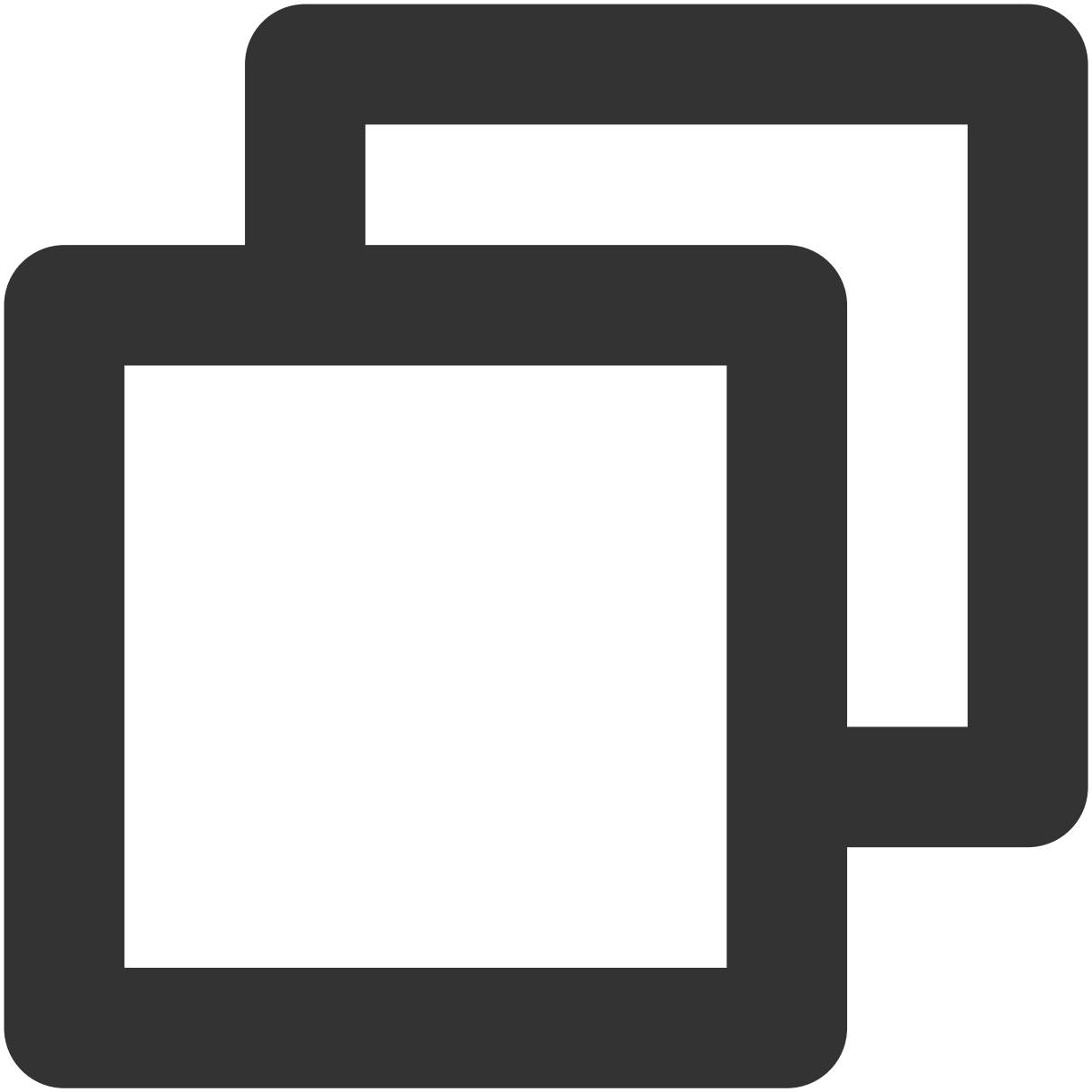
2.1 Gere o tráfego da ENI. Por exemplo, você pode fazer login na CVM de origem e executar o comando ping **public IP**.

Dados de origem:



```
[root@VM-0-14-centos ~]# ping www.qq.com
PING https.qq.com (58.250.137.36) 56(84) bytes of data
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq
64 bytes from 58.250.137.36 (58.250.137.36): icmp_seq
^C
--- https.qq.com ping statistics ---
12 packets transmitted, 12 received, 0% packet loss,
rtt min/avg/max/mdev = 4.548/4.588/4.619/0.065 ms
```

2.2 Faça login na CVM de destino, e execute os seguintes comandos para capturar os dados e salvá-los como um arquivo ".cap" ou ".pcap". Este documento usa o arquivo ".pcap" como exemplo.

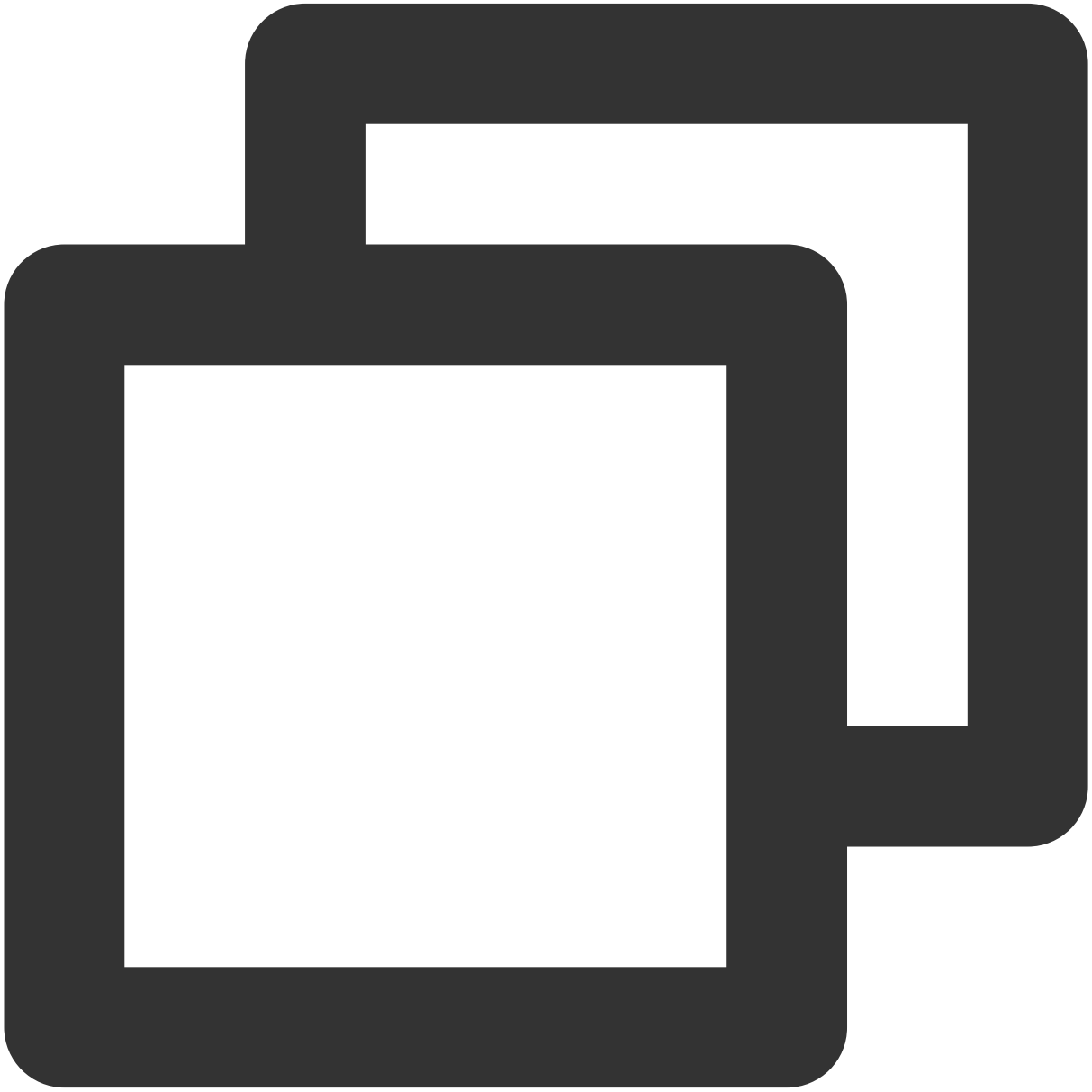


```
tcpdump -i eth0 -w capture-2020-10-27.pcap    #Insira o nome do arquivo real.
```

Pacotes de destino:

```
[root@VM-0-11-centos ~]# tcpdump -i eth0 -w capture-2020-10
tcpdump: listening on eth0, link-type EN10MB (Ethernet), ca
^C721 packets captured
735 packets received by filter
0 packets dropped by kernel
[root@VM-0-11-centos ~]# ls
capture-2020-10-27.pcap
```

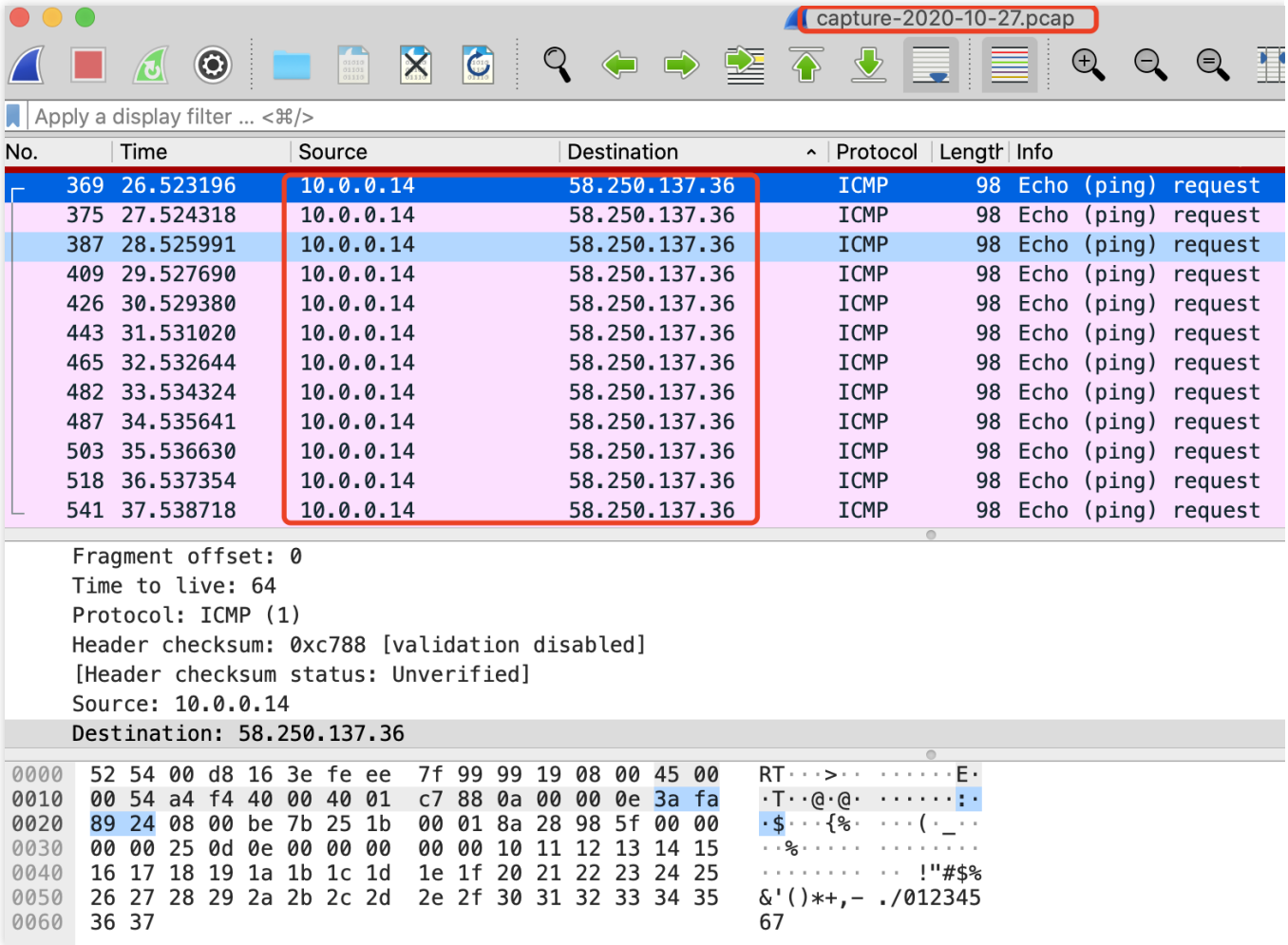
2.3 Use um simulador de terminal (como SecureCRT) para fazer login na CVM de destino e exportar o arquivo salvo na Etapa ii.



```
sz -bye capture-2020-10-27.pcap
```

2.4 Use um analisador de pacotes (como o Wireshark) para obter os dados do arquivo “capture-2020-10-27.pcap” baixado. Neste exemplo, 12 pacotes espelhados da CVM de origem são obtidos da CVM de destino.

Verificação de pacotes:



3. Se um pacote excepcional for obtido, ou se não for possível obter pacotes, envie um tíquete.

Operações posteriores

Ativação ou desativação do espelho de tráfego

Modificação do espelho de tráfego

Adição de uma tag

Exclusão do espelho de tráfego

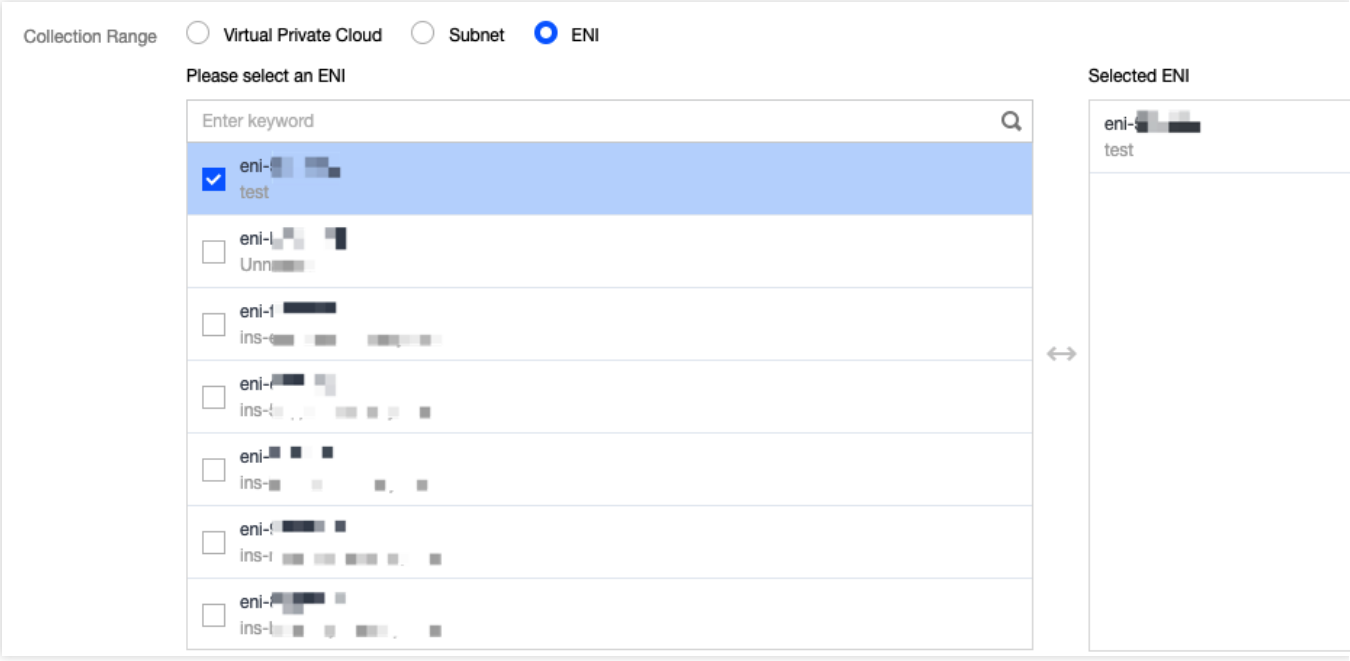
Gerenciamento de um espelho de tráfego

Last updated：2024-01-24 17:55:51

Depois que um espelho de tráfego é criado, é possível ativar, desativar, modificar ou excluí-lo ou adicionar tags no c
onsol
e.

Ativação ou desativação do espelho de tráfego

Uma nova tarefa de espelho de tráfego é ativada por padrão. Para desativá-la e ativá-la novamente, siga as etapas abaixo.
1. Abra o link que você recebeu depois de enviar um tíquete e faça login no console do Espelho de tráfego. No seletor **Region (Região)** superior, selecione a região na qual o espelho de tráfego foi criado.
2. Localize o espelho de tráfego que deseja gerenciar, desative ou ative-o na coluna **Collect Traffic (Coletar tráfego)**.



Modificação do espelho de tráfego

Pa
ra modific

ar um espelho de tráfego existente, siga as etapas abaixo:

1. Abra o link que você recebeu depois de enviar um tíquete e faça login no console do Espelho de tráfego. No seletor **Region (Região)** superior, selecione a região na qual o espelho de tráfego foi criado.

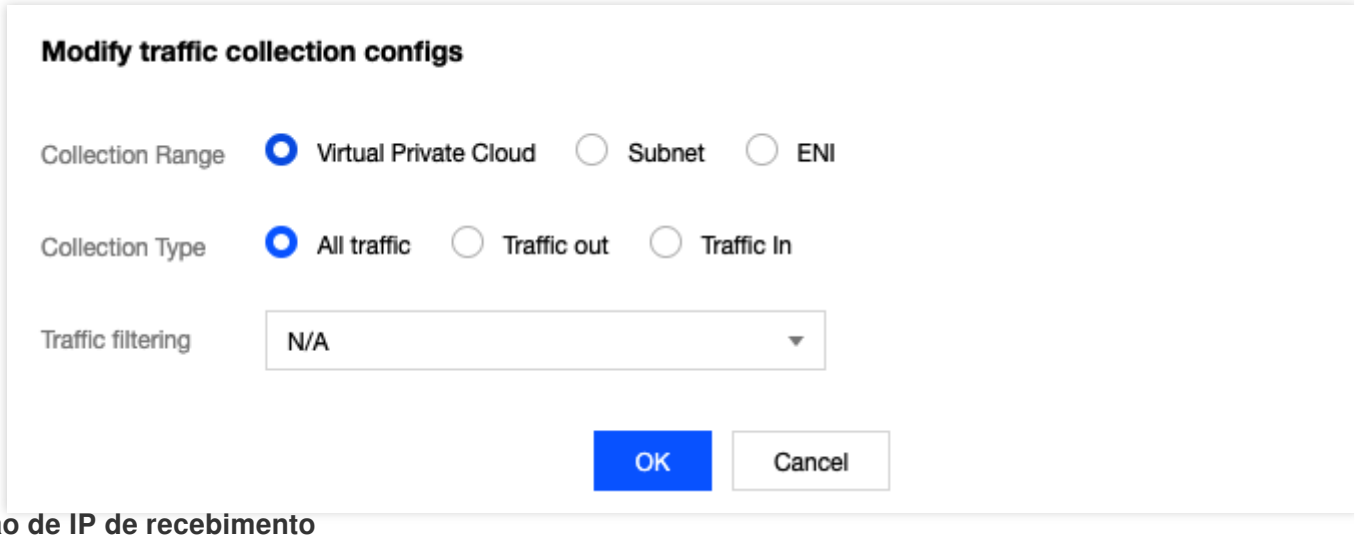
2. Selecione o Nome/ID do espelho de tráfego a ser modificado.

3. Modifique os itens desejados. Este documento usa o **Virtual Private Cloud** para **Collection Range (Intervalo de coleta)** como exemplo.

Edição das configurações de coleta de tráfego

3.1.1 Clique em **Edit (Editar)** no canto superior direito da seção Traffic Collection (Coleta de tráfego).

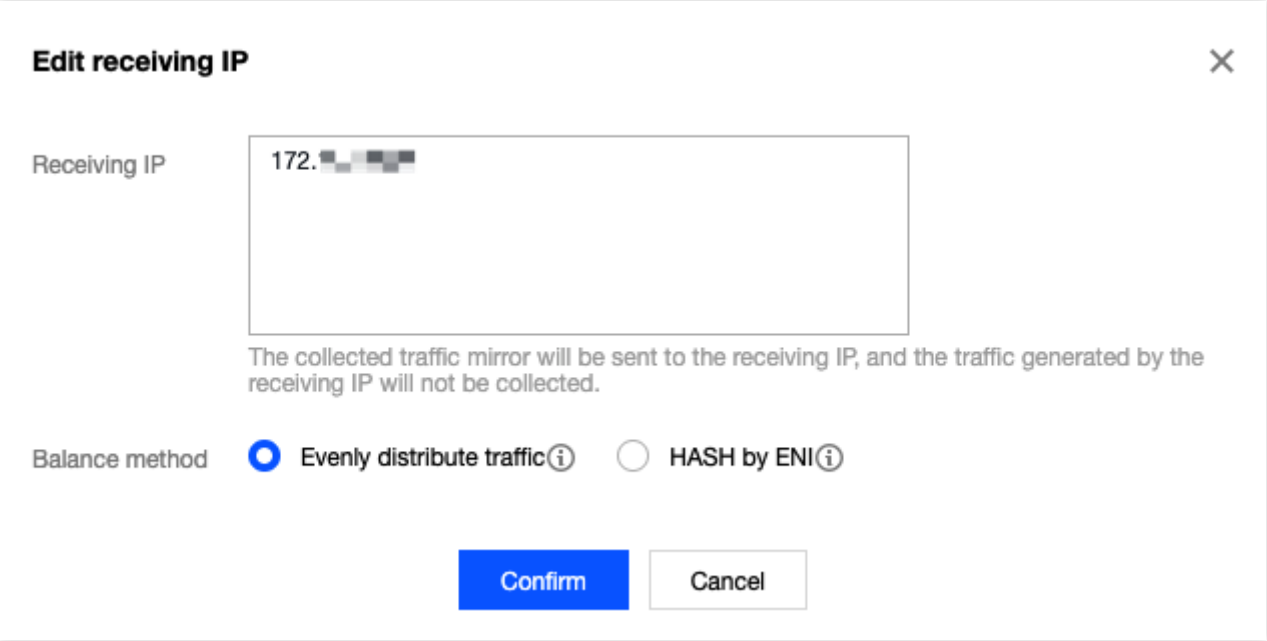
3.1.2 Na janela pop-up, modifique o **Collection Range (Intervalo de coleta)**, o **Collection Type (Tipo de coleta)**, a **Traffic filtering (Filtragem de tráfego)** e outras configurações, conforme necessário, e clique em **OK**.



Edição de IP de recebimento

3.1.1 Clique em **Edit (Editar)** no canto superior direito da seção Receiving IP (IP de recebimento).

3.1.2 Na janela pop-up, modifique o **Receiving IP (IP de recebimento)** e o **Balance method (Método de equilíbrio)**, conforme necessário, e clique em **OK**.



Adição de tags

As ta
gs são
usadas para identificar e organizar os recursos do Tencent Cloud. Cada tag contém uma chave e um valor. Adicionar uma tag ao espelho de tráfego facilita a filtragem e o gerenciamento de recursos de espelho de tráfego.

1. Abra o link que você recebeu depois de enviar um tíquete e faça login no console do Espelho de tráfego. No seletor **Region (Região)** superior, selecione a região na qual o espelho de tráfego foi criado.
2. Localize o espelho de tráfego ao qual deseja adicionar tags e clique em **Edit Tags (Editar tags)** na coluna **Operation (Operação)**.
3. Na caixa de diálogo pop-up, configure da seguinte maneira:

3.1 Para **Tag key (Chave de tag)**, insira o nome da chave ou selecione na lista suspensa.

3.2 Para **Tag value (Valor de tag)**, insira o valor da chave.

Nota:

Uma chave de tag pode ter nenhum ou muitos valores de tag.

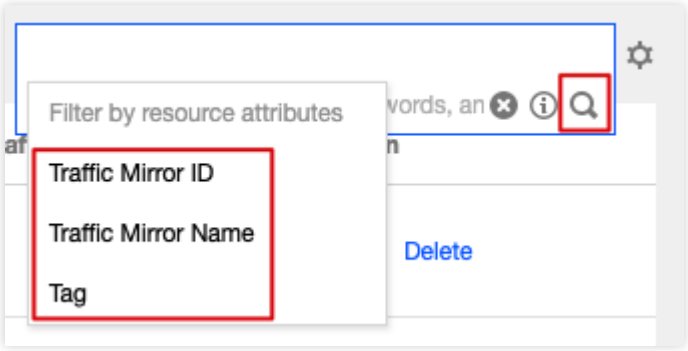
3.3 (Opcional) Clique em **Add (Adicionar)** e configure **Tag key (Chave de tag)** e **Tag value (Valor de tag)**, para adicionar uma tag.

3.4 Quando concluir a configuração, clique em **OK**.

Localização de um espelho de tráfego

1. Clique em


no canto superior direito da página **Traffic mirroring (Espelhamento de tráfego)** e selecione um filtro. Três filtros, conforme mostrado na figura a seguir, estão disponíveis.



2. Insira uma palavra-chave na caixa de edição e clique em


.

Nota:

Separe as pa

lavras-c

have com barras verticais (|).

Exclusão de um espelho de tráfego

1. Abra o link que você recebeu depois de enviar um tíquete e faça login no console do Espelho de tráfego. No seletor **Region (Região)** superior, selecione a região na qual o espelho de tráfego foi criado.
2. Localize o espelho de tráfego a ser excluído, clique em **Delete (Excluir)** na coluna **Operation (Operação)** e confirme a exclusão.

Monitoramento e alarmes

Last updated：2024-01-24 17:48:52

Ao configurar as políticas de alarme, você pode monitorar o status dos recursos em uma VPC, como o NAT Gateway, o gateway do VPN, o gateway do Direct Connect, o EIP etc., para descobrir a execução anormal dos recursos da nuvem a tempo, localizar e resolver os problemas ASSIM QUE POSSÍVEL.

Configuração de uma política de alarme

1. Faça login no Console do Cloud Monitor.
2. Selecione **Alarm Configuration (Configuração de alarmes)** > **Alarm Policy (Política de alarmes)** na barra lateral esquerda, para acessar a página de configuração da política de alarmes.
3. Clique em **Create (Criar)**, insira um nome de política, selecione um recurso de nuvem da VPC a ser configurada para o tipo de política, como **VPC** > **EIP**, e configure as regras de alarme e as notificações de alarme.
4. Clique em **Complete (Concluir)**. Você pode conferir a política de alarme definida na lista de políticas de alarme.

Nota:

Para excluir uma política de alarme, primeiro é necessário desvincular todos os recursos dela.

5. Quando um alarme for acionado, você receberá a notificação de alarme por meio do canal de alarme selecionado (SMS/e-mail/Centro de mensagens etc.).

As configurações de política de alarme para diferentes recursos de nuvem estão detalhadas abaixo:

Direct Connect: Configuração de políticas de alarme

NAT Gateway: Configuração de alarmes

Conexão VPN: Configuração de alarmes

Exibição de informações de monitoramento

Você pode exibir as informações de monitoramento dos recursos de nuvem correspondentes no console da VPC, para ajudar a solucionar as falhas de rede. Consulte:

Direct Connect: Exibição de dados de monitoramento

CCN: Exibição de informações de monitoramento

NAT Gateway: Exibição de informações de monitoramento

Peering Connection: Exibição de dados de monitoramento do tráfego de rede em um Peering Connection entre regiões

Conexão VPN: Exibição de dados de monitoramento