aws

Emparelhamento de VPC

# Amazon Virtual Private Cloud

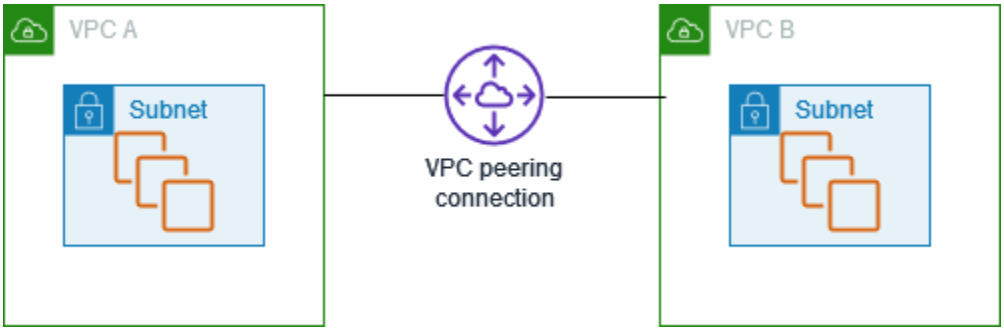
# Amazon Virtual Private Cloud: Emparelhamento de VPC

# Table of Contents

# O que é emparelhamento de VPC?

Uma nuvem privada virtual (VPC) é uma rede virtual dedicada à sua Conta da AWS. Ela é isolada de maneira lógica de outras redes virtuais na Nuvem da AWS. É possível iniciar os recursos da AWS, como instâncias do Amazon EC2, na sua VPC.

Uma conexão de emparelhamento de VPC é uma conexão de rede entre duas VPCs que permite direcionar o tráfego entre elas usando endereços IPv4 ou IPv6 privados. Instâncias em qualquer VPC podem se comunicar umas com as outras como se estivessem na mesma rede. É possível criar uma conexão de emparelhamento de VPC entre suas próprias VPCs ou com uma VPC em outra conta da AWS. As VPCs podem estar em regiões diferentes (também conhecidas como conexão de emparelhamento da VPC entre regiões).




A AWS usa a infraestrutura existente de uma VPC para criar uma conexão de emparelhamento de VPC; não é nem um gateway nem uma conexão VPN, e não depende de uma parte separada do hardware físico. Não há um ponto único de falha de comunicação ou um gargalo de largura de banda.

Uma conexão de emparelhamento de VPC ajuda você a facilitar a transferência de dados. Por exemplo, se houver mais de uma conta da AWS, você poderá emparelhar as VPCs entre essas contas para criar uma rede de compartilhamento de arquivos. Você também pode usar uma conexão de emparelhamento de VPC para permitir que outras VPCs acessem os recursos que você tem em uma de suas VPCs.

Quando você estabelece relações de emparelhamento entre VPCs em diferentes regiões da AWS, os recursos nas VPCs (por exemplo, instâncias do EC2 e funções do Lambda) em diferentes regiões da AWS podem se comunicar entre si usando endereços IP privados, sem usar um gateway, uma conexão VPN ou um dispositivo de rede. O tráfego permanece no espaço do endereço IP privado. Todo o tráfego entre regiões é criptografado sem um único ponto de falha ou gargalo na largura de banda. O tráfego permanece sempre na estrutura global da AWS e nunca atravessa a Internet

pública, o que reduz ameaças, como violações comuns e ataques de DDoS. O emparelhamento de VPCs entre regiões proporciona uma forma simples e econômica de compartilhar recursos entre regiões ou replicar dados para redundância geográfica.

# Definição de preço para uma conexão de emparelhamento de VPC

Não há cobrança para criar uma conexão de emparelhamento da VPC. Todas as transferências de dados por meio de uma conexão de emparelhamento da VPC que permanecem em uma zona de disponibilidade são gratuitas, mesmo que sejam entre contas diferentes. São aplicadas cobranças para as transferências de dados por meio de conexões de emparelhamento da VPC entre zonas de disponibilidade e regiões. Para obter mais informações, consulte Definição de preço do Amazon EC2.

# Como as conexões de emparelhamento da VPC funcionam

As etapas a seguir descrevem o processo de emparelhamento de VPC:

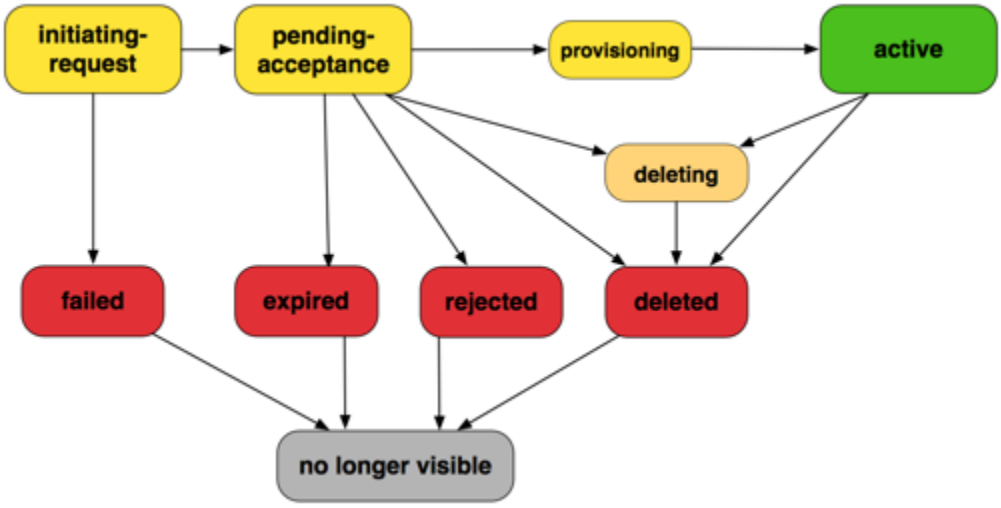
1. O proprietário da VPC solicitante envia um pedido ao proprietário da VPC receptora para criar a conexão de emparelhamento de VPC. O receptor da VPC pode ser de sua propriedade ou de outra conta da AWS e não pode ter um bloco CIDR que se sobreponha ao bloco CIDR da VPC solicitante.
2. O proprietário da VPC aceitante aceita a solicitação da conexão de emparelhamento da VPC para ativar a conexão de emparelhamento da VPC.
3. Para permitir o fluxo de tráfego entre as VPCs usando endereços IP privados, o proprietário de cada VPC na conexão de emparelhamento de VPC deve adicionar manualmente uma rota a uma ou mais tabelas de rotas da VPC que apontam para o intervalo de endereço IP da outra VPC (a VPC de emparelhamento).
4. Se necessário, atualize as regras do grupo de segurança que estão associadas à sua instância do EC2 para garantir que o tráfego de entrada e de saída da VPC emparelhada não fique restrito. Se as duas VPCs estiverem na mesma região, você poderá fazer referência a um grupo de segurança da VPC emparelhada como uma origem ou destino para as regras de entrada ou de saída nas regras do seu grupo de segurança.
5. Com as opções padrão de conexão de emparelhamento da VPC, se as instâncias do EC2 de cada lado de uma conexão de emparelhamento da VPC endereçarem umas as outras usando um nome de host de DNS público, o nome de host será resolvido para o endereço IP público da instância do EC2. Para alterar esse comportamento, habilite a resolução do nome de host DNS para a conexão VPC. Após habilitar a resolução do nome de host de DNS, se as instâncias do EC2 em cada lado do endereço de conexão de emparelhamento da VPC estiverem cada uma usando um nome de host DNS público, o nome do host será resolvido como o endereço IP privado da instância do EC2.

Para obter mais informações, consulte Conexões de emparelhamento da VPC.

## Ciclo de vida da conexão de emparelhamento de VPC

Uma conexão emparelhamento de VPC passa por vários estágios começando pelo momento que solicitação é iniciada. Em cada etapa, pode haver ações que você pode realizar e, no final do seu

ciclo de vida, a conexão de emparelhamento de VPC permanece visível no console da Amazon VPC, na API ou na saída de linha de comando por um período.




- Initiating-request: Foi iniciado um pedido para uma conexão de emparelhamento de VPC. Nesta fase, a conexão de emparelhamento pode falhar ou pode ir para `pending-acceptance`.
- Failed: O pedido da conexão de emparelhamento de VPC falhou. Enquanto estiver nesse estado, ela não pode ser aceita, rejeitada ou excluída. A conexão de emparelhamento de VPC com falha permanece visível para o solicitante por 2 horas.
- Pending-acceptance: A solicitação de conexão de emparelhamento de VPC está aguardando aceitação pelo proprietário da VPC receptora. Durante este estado, o proprietário da VPC solicitante pode excluir a solicitação e o proprietário da VPC receptora pode aceitar ou rejeitar a solicitação. Se nenhuma ação for tomada na solicitação, expira após 7 dias.
- Expired: A solicitação de conexão de emparelhamento de VPC expirou e nenhuma ação pode ser tomada por ela ou pelo proprietário da VPC. A conexão de emparelhamento de VPC falhou e permanece visível para ambos os proprietários da VPC por 2 horas.
- Rejected: O proprietário da VPC receptora rejeitou uma solicitação de conexão de emparelhamento de VPC `pending-acceptance`. Enquanto estiver nesse estado, a solicitação não pode ser aceita. A conexão de emparelhamento de VPC rejeitada permanece visível para o proprietário da VPC solicitante por 2 dias e visível para o proprietário da VPC receptora por 2 horas. Se a solicitação foi criada dentro da mesma conta da AWS, a solicitação rejeitada permanece visível por 2 horas.
- Provisioning: A solicitação de conexão de emparelhamento de VPC foi aceita e em breve estará no estado `active`.

- Active: a conexão de emparelhamento de VPC está ativa e o tráfego pode fluir entre as VPCs (desde que seus grupos de segurança e tabelas de rotas permitam o fluxo de tráfego). Enquanto estiver nesse estado, qualquer um dos proprietários da VPC podem excluir a conexão de emparelhamento de VPC, mas não podem rejeitá-la.

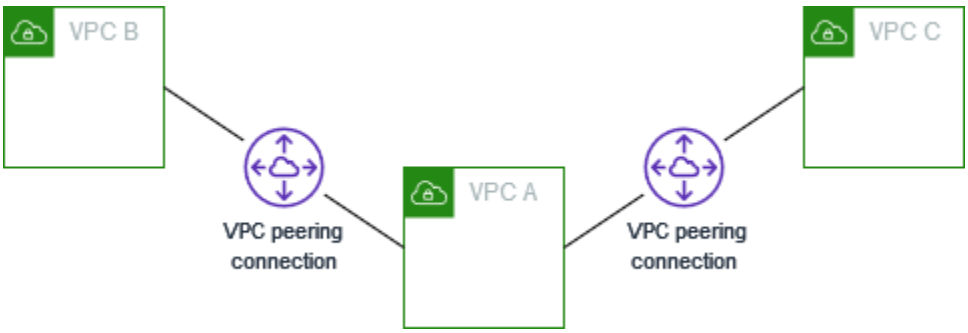
  > **Note**
  >
  > Se um evento em uma região na qual uma VPC reside impedir o fluxo do tráfego, o status da conexão de emparelhamento da VPC permanecerá `Active`.

- Deleting (Exclusão): aplica-se a uma conexão de emparelhamento da VPC entre regiões que está no processo de exclusão. O proprietário de uma VPC enviou uma solicitação para excluir uma conexão de emparelhamento de VPC com o status `active` ou o proprietário da VPC do solicitante enviou uma solicitação para excluir uma solicitação de conexão de emparelhamento de VPC com o status `pending-acceptance`.
- Deleted: Uma conexão de emparelhamento de VPC `active` foi excluída por algum dos proprietários da VPC ou uma solicitação de conexão de emparelhamento de VPC `pending-acceptance` foi excluída pelo proprietário da VPC solicitante. Enquanto estiver nesse estado, a conexão de emparelhamento de VPC não pode ser aceita ou rejeitada. A conexão emparelhamento de VPC permanece visível para a parte que o excluiu por 2 horas e visível para a outra parte por 2 dias. Se a conexão de emparelhamento da VPC foi criada dentro da mesma conta da AWS, a solicitação excluída permanece visível por 2 horas.

## Várias conexões de emparelhamento de VPC

Uma conexão de emparelhamento de VPC é uma relação de um a um entre duas VPCs. Você pode criar várias conexões de emparelhamento de VPC para cada uma das suas VPCs, mas não há suporte para relações de emparelhamentos transitivas. Você não tem nenhum relacionamento de emparelhamento com as VPCs com as quais sua VPC não esteja diretamente emparelhada.

O diagrama a seguir é um exemplo de uma VPC emparelhada com duas VPCs diferentes. Existem duas conexões de emparelhamentos da VPC: VPC A é emparelhada com a VPC B e a VPC C. A VPC B e VPC C não são emparelhadas e você não pode usar a VPC A como ponto de trânsito para emparelhamento entre a VPC B e a VPC C. Se desejar habilitar o roteamento do tráfego entre a VPC B e VPC C, você deve criar uma conexão de emparelhamento de VPC exclusiva entre elas.




# Limitações de emparelhamento de VPC

Considere as seguintes limitações para as conexões de emparelhamento da VPC. Em alguns casos, é possível usar um anexo do gateway de trânsito no lugar da conexão de emparelhamento da VPC. Para obter mais informações, consulte Example transit gateway scenarios no Amazon VPC Transit Gateways.

Conexões

- Há uma cota para o número de conexões de emparelhamento da VPC ativas e pendentes para cada VPC. Para obter mais informações, consulte Cotas.
- Não pode haver mais de uma conexão de emparelhamento da VPC entre duas VPCs ao mesmo tempo.
- Todas as tags que você criar para sua conexão de emparelhamento da VPC só serão aplicadas na conta ou na região em que você as criar.
- Não é possível se conectar ou consultar o servidor DNS da Amazon em uma VPC emparelhada.
- Se o bloco CIDR IPv4 de uma VPC em uma conexão de emparelhamento da VPC ficar fora dos intervalos de endereço IPv4 privados especificados por RFC 1918, os nomes de host DNS privados para a VPC não podem ser resolvidos para endereços IP privados. Para resolver os nomes de host DNS privados para endereços IP privados, você pode habilitar o suporte de resolução DNS para a conexão de emparelhamento da VPC. Para obter mais informações, consulte Habilitar a resolução de DNS para a conexão de emparelhamento da VPC.
- Você pode habilitar recursos em ambos os lados de uma conexão de emparelhamento da VPC para se comunicar por IPv6. Você deve associar um bloco CIDR IPv6 a cada VPC, habilitar as instâncias nas VPCs para comunicação por IPv6 e rotear o tráfego IPv6 destinado à VPC de mesmo nível para a conexão de emparelhamento da VPC.
- O encaminhamento do caminho inverso Unicast não é compatível em conexões de emparelhamento de VPC. Para obter mais informações, consulte Rota para tráfego de resposta.

### Blocos CIDR sobrepostos

- Não é possível criar uma conexão de emparelhamento de VPC entre VPCs que tenham blocos CIDR IPv4 ou IPv6 coincidentes ou sobrepostos.
- Se houver vários blocos CIDR IPv4, você não poderá criar uma conexão de emparelhamento da VPC se alguns dos blocos CIDR estiverem sobrepostos, mesmo que pretenda usar apenas os blocos CIDR que não estão sobrepostos ou apenas os blocos CIDR IPv6.

### Emparelhamento transitivo

- O emparelhamento de VPC não oferece suporte a relações de emparelhamento transitivas. Por exemplo, se houver conexões de emparelhamento da VPC entre a VPC e a VPC B e entre a VPC A e a VPC C, você não poderá rotear o tráfego da VPC B para a VPC C por meio da VPC A. Para rotear o tráfego entre a VPC B e a VPC C, você deverá criar uma conexão de emparelhamento da VPC entre elas. Para obter mais informações, consulte Três VPCs emparelhadas simultaneamente.

### Roteamento de ponta a ponta por um gateway ou conexão privada

- Se a VPC A tiver um gateway de internet, os recursos na VPC B não poderão usar o gateway da Internet da VPC A para acessar a Internet.
- Da mesma forma, se a VPC A tiver um dispositivo NAT que forneça acesso a sub-redes na VPC A, os recursos na VPC B não poderão usar o dispositivo NAT na VPC A para acessar a internet.
- Se a VPC A tiver uma conexão VPN com uma rede corporativa, os recursos na VPC B não poderão usar a conexão VPN para se comunicarem com a rede corporativa.
- Se a VPC A tiver uma conexão AWS Direct Connect com uma rede corporativa, os recursos na VPC B não poderão usar a conexão AWS Direct Connect para se comunicarem com a rede corporativa.
- Se a VPC A tiver um endpoint do gateway que forneça conectividade ao Amazon S3 com sub-redes privadas na VPC A, os recursos na VPC B não poderão usar o endpoint do gateway para acessar o Amazon S3.

### Conexões de emparelhamento da VPC entre regiões

- Para quadros jumbo, a Unidade Máxima de Transmissão (MTU) entre as conexões de emparelhamento da VPC na mesma região é de 9.001 bytes. O MTU para conexões de

emparelhamento da VPC entre regiões é de 8.500 bytes. Para obter mais informações sobre jumbo frames, consulte Jumbo frames (9001 MTU) no Guia do usuário do Amazon EC2.

- Você deve habilitar o suporte para a resolução de DNS para a conexão de emparelhamento de VPC a fim de resolver os nomes de host DNS privados da VPC emparelhada para endereços IP privados, mesmo que o CIDR IPv4 para a VPC caia em intervalos de endereços IPv4 privados especificados pela RFC 1918.

VPCs e sub-redes compartilhadas

- Somente proprietários de VPCs podem trabalhar com (descrição, criação, aceitação, rejeição, modificação ou exclusão) conexões de emparelhamento. Os participantes não podem trabalhar com conexões de emparelhamento. Para obter mais informações, consulte Compartilhar sua VPC com outras contas no Guia do usuário da Amazon VPC.

# Conexões de emparelhamento da VPC

O emparelhamento de VPC permite que você conecte duas VPCs na mesma região ou em regiões diferentes da AWS. Isso permite que as instâncias de uma VPC se comuniquem com as instâncias da outra VPC como se estivessem na mesma rede.

O emparelhamento de VPC cria uma rota de rede direta entre as duas VPCs usando endereços IPv4 ou IPv6 privados. O tráfego enviado entre as VPCs conectadas não atravessa a Internet, uma conexão de VPN nem uma conexão do AWS Direct Connect. Isso torna o emparelhamento de VPC uma forma segura de compartilhar recursos, como bancos de dados ou servidores web, cruzando as fronteiras da VPC.

Para estabelecer uma conexão de emparelhamento da VPC, você cria uma solicitação de conexão de emparelhamento em uma VPC e o proprietário da outra VPC a aceita. Após a conexão ser estabelecida, você poderá atualizar as tabelas de rotas para rotear tráfego entre as VPCs. Isso permite que as instâncias em uma VPC acessem os recursos na outra VPC.

O emparelhamento de VPC é uma ferramenta importante para criar arquiteturas com várias VPCs e compartilhar recursos cruzando as fronteiras organizacionais da AWS. Ele fornece uma maneira simples e de baixa latência de conectar VPCs sem a complexidade de configurar uma VPN ou outro serviço de rede.

Use os procedimentos a seguir para criar e trabalhar com conexões de emparelhamento da VPC.

Tarefas

- Criar uma conexão de emparelhamento de VPC
- Aceitar uma solicitação de conexão de emparelhamento da VPC
- Atualizar suas tabelas de rotas para uma conexão de emparelhamento da VPC
- Atualizar seus grupos de segurança para fazer referência a grupos de segurança de mesmo nível
- Habilitar a resolução de DNS para a conexão de emparelhamento da VPC
- Excluir uma conexão de emparelhamento da VPC
- Solucionar problemas com a conexão de emparelhamento da VPC

# Criar uma conexão de emparelhamento de VPC

Para criar uma conexão de emparelhamento de VPC, crie uma solicitação para fazer emparelhamento com outra VPC. Para ativar a solicitação, o proprietário da VPC que receber a solicitação deve aceitá-la. Os seguintes tipos de conexão de emparelhamento são compatíveis:

- Entre VPCs nas mesmas conta e região
- Entre VPCs nas mesmas conta, mas em regiões diferentes
- Entre VPCs em contas diferentes, mas na mesma região
- Entre VPCs em contas e regiões diferentes

Para uma conexão de emparelhamento da VPC entre regiões, a solicitação deve ser feita a partir da região da VPC solicitante e a solicitação deve ser aceita na região da VPC aceitante. Para obter mais informações, consulte the section called “Aceitar ou rejeitar”.

Tarefas

- Pré-requisitos
- Como criar uma conexão de emparelhamento usando o console
- Criar uma conexão de emparelhamento usando a linha de comando

## Pré-requisitos

- Revise as limitações das conexões de emparelhamento da VPC.
- Certifique-se de que as VPCs não tenham blocos CIDR IPv4 sobrepostos. Se houver sobreposição, o status da conexão de emparelhamento da VPC imediatamente se tornará `failed`. Essa limitação se aplica, mesmo se as VPCs tiverem blocos CIDR IPv6 únicos.

## Como criar uma conexão de emparelhamento usando o console

Use o procedimento a seguir para criar uma conexão de emparelhamento da VPC.

Para criar uma conexão de emparelhamento usando o console

1. Abra o console da Amazon VPC, em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Peering Connections (Conexões de emparelhamento).

3. Selecione Create Peering Connection (Criar conexão de emparelhamento).
4. (Opcional) Em Nome, especifique um nome para a conexão de emparelhamento da VPC. Fazer isso cria uma tag com a chave Name e o valor especificado.
5. Para ID da VPC (Solicitante), selecione uma VPC na conta atual.
6. Em Selecionar outra VPC para emparelhar, faça o seguinte:
   a. Em Conta, para emparelhar com uma VPC em outra conta, escolha Outra conta e insira o ID da conta. Caso contrário, mantenha Minha conta.
   b. Em Região, para emparelhar com uma VPC em outra região, escolha Outra região e escolha a região. Caso contrário, mantenha Esta região.
   c. Para ID da VPC (aceitante), selecione uma VPC da conta e da região especificadas.
7. (Opcional) Para adicionar uma etiqueta, escolha Add new tag (Adicionar nova etiqueta) e insira a chave e o valor da etiqueta.
8. Selecione Create Peering Connection (Criar conexão de emparelhamento).
9. O proprietário da conta aceitante deverá aceitar a conexão de emparelhamento. Para obter mais informações, consulte the section called “Aceitar ou rejeitar”.
10. Atualize as tabelas de rotas de ambas as VPCs para permitir a comunicação entre elas. Para obter mais informações, consulte the section called “Atualizar tabelas de rotas”.

### Criar uma conexão de emparelhamento usando a linha de comando

É possível criar uma conexão de emparelhamento da VPC usando os seguintes comandos:

- create-vpc-peering-connection (AWS CLI)
- New-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

## Aceitar uma solicitação de conexão de emparelhamento da VPC

Uma conexão de emparelhamento da VPC que está no estado `pending-acceptance` deve ser aceita pelo proprietário da VPC receptora para ser ativada. Para obter mais informações sobre o status de conexões de emparelhamento `Deleted`, consulte Ciclo de vida da conexão de emparelhamento de VPC. Não é possível aceitar uma solicitação de conexão de emparelhamento da VPC que enviou para outra conta da AWS. Para criar uma conexão de emparelhamento da VPC entre VPCs na mesma conta da AWS, você deverá criar e aceitar a solicitação.

Você pode rejeitar qualquer solicitação de conexão de emparelhamento da VPC recebida que esteja no estado `pending-acceptance`. Você deve aceitar somente conexões de emparelhamento da VPC de Contas da AWS que conheça e nas quais confie, podendo rejeitar quaisquer solicitações indesejadas. Para obter mais informações sobre o status de conexões de emparelhamento `Rejected`, consulte Ciclo de vida da conexão de emparelhamento de VPC.

> **Important**
>
> Não aceite conexões de emparelhamento da VPC de contas da AWS desconhecidas. Um usuário mal intencionado pode ter enviado uma solicitação de emparelhamento da VPC para você para obter acesso não autorizado à sua VPC. Isso é conhecido como peer phishing (phishing de emparelhamento). Você pode seguramente rejeitar solicitações de conexão de emparelhamento da VPC indesejadas sem qualquer risco de o solicitante obter acesso a quaisquer informações sobre sua conta da AWS ou da sua VPC. Para obter mais informações, consulte Aceitar uma solicitação de conexão de emparelhamento da VPC. Você também pode ignorar a solicitação e deixá-la expirar; por padrão, solicitações expiram em 7 dias.

Para aceitar ou rejeitar uma conexão de emparelhamento usando o console

1. Abra o console da Amazon VPC, em https://console.aws.amazon.com/vpc/.
2. Use o seletor de Regiões para escolher a Região da VPC aceitante.
3. No painel de navegação, escolha Peering Connections (Conexões de emparelhamento).
4. Para rejeitar uma conexão de emparelhamento, selecione a conexão de emparelhamento da VPC e escolha Ações, Rejeitar solicitação. Quando a confirmação for solicitada, escolha Rejeitar solicitação.
5. Para aceitar a conexão de emparelhamento, selecione a conexão de emparelhamento da VPC pendente (o status é `pending-acceptance`) e depois escolha Ações, Aceitar solicitação. Para obter mais informações sobre os status do ciclo de vida das conexões de emparelhamento, consulte Ciclo de vida da conexão de emparelhamento de VPC.

   Se não houver uma conexão de emparelhamento da VPC pendente, verifique se você selecionou a região da VPC aceitante.
6. Quando a confirmação for solicitada, escolha Aceitar solicitação.
7. Escolha Modificar minhas tabelas de rotas agora para adicionar uma rota à tabela de rotas da VPC para que você possa enviar e receber tráfego pela conexão de emparelhamento.

Para obter mais informações, consulte Atualizar suas tabelas de rotas para uma conexão de emparelhamento da VPC.

Para aceitar uma conexão de emparelhamento usando a linha de comando

- accept-vpc-peering-connection (AWS CLI)
- Approve-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

Para rejeitar uma conexão de emparelhamento usando a linha de comando

- reject-vpc-peering-connection (AWS CLI)
- Deny-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

## Atualizar suas tabelas de rotas para uma conexão de emparelhamento da VPC

Para habilitar o tráfego IPv4 privado entre instâncias em VPCs com emparelhamento, é necessário adicionar uma rota às tabelas de rotas associadas às sub-redes de ambas as instâncias. O destino da rota é o bloco CIDR (ou parte do bloco CIDR) da VPC de mesmo nível e o destino é o ID da conexão de emparelhamento da VPC. Para obter mais informações, consulte Configurar tabelas de rotas, no Guia do usuário da Amazon VPC.

O exemplo a seguir mostra tabelas de rotas que permitem a comunicação entre instâncias em duas VPCs com emparelhamento, VPC A e VPC B. Cada tabela tem uma rota local e uma rota que envia tráfego da VPC peer à conexão de emparelhamento da VPC.

| Tabela de rotas | Destino | Alvo |
|---|---|---|
| VPC A | *CIDR da VPC A* | Local |
| | *CIDR da VPC B* | pcx-*11112222* |
| VPC B | *CIDR da VPC B* | Local |
| | *CIDR da VPC A* | pcx-*11112222* |

Da mesma forma, se as VPCs na conexão de emparelhamento da VPC tiverem blocos CIDR IPv6 associados, você poderá adicionar rotas que permitem a comunicação com a VPC de mesmo nível por IPv6.

Para obter mais informações sobre configurações de tabela de rotas compatíveis com conexões de emparelhamento de VPC, consulte Configurações comuns de conexões de emparelhamento de VPC.

Considerações

- Se você tiver uma VPC emparelhada com várias VPCs que possuem blocos CIDR IPv4 correspondentes ou sobrepostos, verifique se as tabelas de rotas estão configuradas, para evitar o envio de tráfego de resposta da sua VPC para a VPC incorreta. Atualmente, a AWS não oferece suporte ao encaminhamento invertido unicast em conexões de emparelhamento da VPC que verificam o IP de origem de pacotes, e encaminham pacotes de resposta de volta à origem. Para obter mais informações, consulte Rota para tráfego de resposta.
- Sua conta tem uma cota para o número de entradas que são adicionadas por tabela de rotas. Se o número de conexões de emparelhamento da VPC na sua VPC exceder a cota de entradas da tabela de rotas para uma única tabela de rotas, use várias sub-redes que estejam associadas a uma tabela de rotas personalizada.
- Você pode adicionar uma rota a uma conexão de emparelhamento da VPC que esteja no estado `pending-acceptance`. Entretanto, a rota tem o estado `blackhole` e não surtirá efeito até que a conexão de emparelhamento da VPC esteja no estado `active`.

Para adicionar uma rota IPv4 para uma conexão de emparelhamento de VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route tables.
3. Marque a caixa de seleção próxima à tabela de rotas associada à sub-rede na qual a instância reside.

   Se você não tiver uma tabela de rotas explicitamente associada a essa sub-rede, a tabela de rotas principal da VPC será implicitamente associada à sub-rede.
4. Selecione Actions (Ações), Edit routes (Editar rotas).
5. Escolha Add route (Adicionar rota).
6. Para Destination, digite o intervalo de endereço IPv4 para o qual o tráfego de rede na conexão de emparelhamento da VPC deve ser direcionado. Você pode especificar todo o bloco CIDR

IPv4 da VPC de mesmo nível, um intervalo específico ou um endereço IPv4 individual, como o endereço IP da instância com a qual deve ser comunicar. Por exemplo, se o bloco CIDR da VPC de mesmo nível for `10.0.0.0/16`, você poderá especificar uma parte `10.0.0.0/24` ou um endereço IP específico `10.0.0.7/32`.

7. Em Destino, selecione a conexão de emparelhamento da VPC.
8. Escolha Salvar alterações.

O proprietário da VPC peer também deve executar essas etapas para adicionar uma rota para direcionar o tráfego de volta para a sua VPC por meio da conexão de emparelhamento da VPC.

Se você tiver recursos em diferentes regiões da AWS que usam endereços IPv6, poderá criar uma conexão de emparelhamento entre regiões. Em seguida, você pode adicionar uma rota IPv6 para comunicação entre os recursos.

Para adicionar uma rota IPv6 para uma conexão de emparelhamento de VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route tables.
3. Marque a caixa de seleção próxima à tabela de rotas associada à sub-rede na qual a instância reside.

> **Note**
>
> Se você não tiver uma tabela de rotas associada a essa sub-rede, selecione a tabela de rotas principal para a VPC como sub-rede e use essa tabela de rotas como padrão.

4. Selecione Actions (Ações), Edit routes (Editar rotas).
5. Escolha Add route (Adicionar rota).
6. Para Destination, digite o intervalo de endereço IPv6 para a VPC de mesmo nível. Você pode especificar todo o bloco CIDR IPv6 da VPC de mesmo nível, um intervalo específico ou um endereço IPv6 individual. Por exemplo, se o bloco CIDR da VPC de mesmo nível for `2001:db8:1234:1a00::/56`, você poderá especificar uma parte `2001:db8:1234:1a00::/64` ou um endereço IP específico `2001:db8:1234:1a00::123/128`.
7. Em Destino, selecione a conexão de emparelhamento da VPC.
8. Escolha Salvar alterações.

Para obter mais informações, consulte Tabelas de rotas no Guia do usuário da Amazon VPC.

Como adicionar ou substituir uma rota usando a linha de comando

- create-route e replace-route (AWS CLI)
- New-EC2Route e Set-EC2Route (AWS Tools for Windows PowerShell)

## Atualizar seus grupos de segurança para fazer referência a grupos de segurança de mesmo nível

Você pode atualizar as regras de entrada e saída dos grupos de segurança da VPC para referenciar grupos de segurança para VPCs emparelhadas. Fazendo isso, você permite que o tráfego flua entre as instâncias associadas com o grupo de segurança referenciado na VPC emparelhada.

> **Note**
>
> Os grupos de segurança em uma VPC de emparelhamento não estão exibidos no console para serem selecionados.

Requisitos

- Para referenciar um security group em uma VPC de mesmo nível, a conexão de emparelhamento precisa estar no estado `active`.
- A VPC emparelhada pode ser uma VPC na sua conta ou uma VPC em outra conta da AWS. Para fazer referência a um grupo de segurança que está em outra conta da AWS, mas na mesma região, inclua o número da conta com a ID do grupo de segurança. Por exemplo, `.123456789012/sg-1a2b3c4d`
- Não é possível referenciar o grupo de segurança de uma VPC de emparelhamento que esteja em uma região diferente. Em vez disso, use o bloco CIDR da VPC de emparelhamento.
- Se você configurar rotas para encaminhar o tráfego entre duas instâncias em sub-redes diferentes por meio de um dispositivo middlebox, deverá garantir que os grupos de segurança de ambas as instâncias permitam o fluxo de tráfego entre as instâncias. O grupo de segurança para cada instância deve fazer referência ao endereço IP privado da outra instância ou ao intervalo CIDR da sub-rede que contém a outra instância, como a origem. Se você fizer referência ao grupo de segurança da outra instância como a origem, isso não permitirá que o tráfego flua entre as instâncias.

Atualizar as regras do grupo de segurança usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Security groups (Grupos de segurança).
3. Selecione o grupo de segurança e siga um destes procedimentos:
   - Para modificar as regras de entrada, escolha Ações, Editar regras de entrada.
   - Para modificar as regras de saída, escolha Ações, Editar regras de saída.
4. Para adicionar uma regra, selecione Adicionar regra e especifique o tipo, protocolo e intervalo de porta. Para Origem (regra de entrada) ou Destino (regra de saída), siga um destes procedimentos:
   - Para uma VPC de emparelhamento na mesma conta e região, insira o ID do grupo de segurança.
   - Para uma VPC de emparelhamento em uma conta diferente, mas na mesma região, insira o ID da conta e o ID do grupo de segurança, separados por uma barra (por exemplo, `123456789012/sg-1a2b3c4d`).
   - Para uma VPC de emparelhamento em uma região diferente, insira o bloco CIDR da VPC de emparelhamento.
5. Para editar uma regra existente, altere seus valores (por exemplo, a origem ou a descrição).
6. Para excluir uma regra, selecione Excluir, próximo à regra.
7. Selecione Salvar rules.

Como atualizar regras de entrada usando a linha de comando

- authorize-security-group-ingress e revoke-security-group-ingress (AWS CLI)
- Grant-EC2SecurityGroupIngress e Revoke-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)

Por exemplo, para atualizar o grupo de segurança `sg-aaaa1111` para permitir acesso de entrada por HTTP de `sg-bbbb2222` que está em uma VPC de emparelhamento, use o comando a seguir. Se a VPC de emparelhamento estiver na mesma região, mas em uma conta diferente, adicione `--group-owner` *`aws-account-id`*.

```
aws ec2 authorize-security-group-ingress --group-id sg-aaaa1111 --protocol tcp --
port 80 --source-group sg-bbbb2222
```

Para atualizar regras de saída usando a linha de comando

- authorize-security-group-egress e revoke-security-group-egress (AWS CLI)
- Grant-EC2SecurityGroupEgress e Revoke-EC2SecurityGroupEgress (AWS Tools for Windows PowerShell)

Depois de atualizar as regras do grupo de segurança, use o comando describe-security-groups, para visualizar o grupo de segurança mencionado nas suas regras de grupo de segurança.

## Identificar seus grupos de segurança referenciados

Para determinar se o security group está sendo referenciado nas regras de um security group em uma VPC de mesmo nível, use um dos comandos a seguir para um ou mais security groups da sua conta.

- describe-security-group-references (AWS CLI)
- Get-EC2SecurityGroupReference (AWS Tools for Windows PowerShell)

No seguinte exemplo, a resposta indica que o security group `sg-bbbb2222` está sendo referenciado por um security group na VPC `vpc-aaaaaaaa`:

```
aws ec2 describe-security-group-references --group-id sg-bbbb2222
```

```
{
  "SecurityGroupsReferenceSet": [
    {
      "ReferencingVpcId": "vpc-aaaaaaaa",
      "GroupId": "sg-bbbb2222",
      "VpcPeeringConnectionId": "pcx-b04deed9"
    }
  ]
}
```

Se a conexão de emparelhamento da VPC for excluída ou se o proprietário da VPC de mesmo nível excluir o security group de referência, a regra do security group ficará obsoleta.

# Visualizar e excluir com regras de grupo de segurança obsoletas

Uma regra de grupo de segurança obsoleta é uma regra que referencia um grupo de segurança excluído na mesma VPC ou em em no par de uma VPC, ou que referencia um grupo de segurança em que a conexão de emparelhamento da VPC foi excluída. Quando uma regra de grupo de segurança se torna obsoleta, ela não é automaticamente removida do seu grupo de segurança; é necessário removê-la manualmente. Se uma regra de grupo de segurança estiver obsoleta porque a conexão de emparelhamento da VPC foi excluída, ela não será mais marcada como obsoleta se você criar uma nova conexão de emparelhamento de VPC com as mesmas VPCs.

É possível visualizar e excluir as regras de grupo de segurança obsoletas para uma VPC usando o console da Amazon VPC.

Como visualizar e excluir regras do grupo de segurança obsoletas

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Security groups (Grupos de segurança).
3. Selecione Ações, Gerenciar regras obsoletas.
4. Em VPC, escolha a VPC com as regras obsoletas.
5. Selecione Editar.
6. Selecione o botão Excluir ao lado da regra que deseja excluir. Selecione Visualizar alterações, Salvar regras.

Como descrever as regras desatualizadas do seu grupo de segurança usando a linha de comando

- describe-stale-security-groups (AWS CLI)
- Get-EC2StaleSecurityGroup (AWS Tools for Windows PowerShell)

No exemplo a seguir, a VPC A (`vpc-aaaaaaaa`) e a VPC B foram emparelhadas e a conexão de emparelhamento de VPC foi excluída. Seu security group `sg-aaaa1111` na VPC A referencia `sg-bbbb2222` na VPC B. Quando você executar o comando `describe-stale-security-groups` para a sua VPC, a resposta indicará que o security group `sg-aaaa1111` possui uma regra SSH obsoleta que referencia `sg-bbbb2222`.

```
aws ec2 describe-stale-security-groups --vpc-id vpc-aaaaaaaa
```

```
{
    "StaleSecurityGroupSet": [
        {
            "VpcId": "vpc-aaaaaaaa",
            "StaleIpPermissionsEgress": [],
            "GroupName": "Access1",
            "StaleIpPermissions": [
                {
                    "ToPort": 22,
                    "FromPort": 22,
                    "UserIdGroupPairs": [
                        {
                            "VpcId": "vpc-bbbbbbbb",
                            "PeeringStatus": "deleted",
                            "UserId": "123456789101",
                            "GroupName": "Prod1",
                            "VpcPeeringConnectionId": "pcx-b04deed9",
                            "GroupId": "sg-bbbb2222"
                        }
                    ],
                    "IpProtocol": "tcp"
                }
            ],
            "GroupId": "sg-aaaa1111",
            "Description": "Reference remote SG"
        }
    ]
}
```

Depois de identificar as regras de grupo de segurança obsoleto, você pode excluí-las usando os comandos revoke-security-group-ingress ou revoke-security-group-egress.

# Habilitar a resolução de DNS para a conexão de emparelhamento da VPC

As configurações de DNS para uma conexão de emparelhamento da VPC determinam como os nomes de host DNS públicos são resolvidos para solicitações que atravessam a conexão de emparelhamento da VPC. Se uma instância do EC2 em um lado de uma conexão de emparelhamento da VPC enviar uma solicitação para uma instância do EC2 do outro lado usando o

nome de host DNS IPv4 público da instância, o nome de host DNS será resolvido conforme mostrado a seguir.

Resolução de DNS desabilitada (padrão)

O nome de host DNS IPv4 público é resolvido no endereço IPv4 público da instância.

Resolução de DNS habilitada

O nome de host DNS IPv4 público é resolvido no endereço IPv4 privado da instância.

Requisitos

- As duas VPCs devem ser habilitadas para nomes de hosts DNS e resolução DNS. Para ter mais informações, consulte Atributos de DNS para sua VPC no Guia do usuário da Amazon VPC.
- A conexão de emparelhamento deve estar no estado `active`. Não é possível habilitar o suporte de resolução de DNS ao criar uma conexão de emparelhamento.
- O proprietário da VPC solicitante deve modificar as opções de emparelhamento da VPC solicitante, e o proprietário da VPC aceitante deve modificar as opções de emparelhamento da VPC aceitante. Se as VPCs estiverem na mesma conta e na mesma região, você poderá habilitar a resolução de DNS para as VPCs solicitante e aceitante ao mesmo tempo.

Para habilitar a resolução de DNS para uma conexão de emparelhamento usando o console

1. Abra o console da Amazon VPC, em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Peering Connections (Conexões de emparelhamento).
3. Selecione a conexão de emparelhamento da VPC.
4. Escolha Ações, Editar configurações de DNS.
5. Para habilitar a resolução de DNS para solicitações da VPC solicitante, selecione Resolução de DNS da solicitante, Permitir que a VPC aceitante resolva o DNS da VPC solicitante.
6. Para garantir a resolução de DNS para solicitações da VPC aceitante, selecione Resolução de DNS da aceitante, Permitir que a VPC solicitante resolva o DNS da VPC aceitante.
7. Escolha Salvar alterações.

Como habilitar a resolução de DNS usando a linha de comando

- modify-vpc-peering-connection-options (AWS CLI)

- Edit-EC2VpcPeeringConnectionOption (AWS Tools for Windows PowerShell)

Para descrever opções de conexão de emparelhamento da VPC usando a linha de comando

- describe-vpc-peering-connections (AWS CLI)
- Get-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

## Excluir uma conexão de emparelhamento da VPC

Qualquer proprietário de uma VPC em uma conexão de emparelhamento pode excluir a conexão de VPC a qualquer momento. Você também pode excluir uma conexão de emparelhamento da VPC que solicitou que ainda esteja no estado `pending-acceptance`.

Quando a conexão de emparelhamento da VPC estiver no estado `rejected` não será possível excluí-la. Excluímos a conexão automaticamente para você.

Excluir uma VPC no console da Amazon VPC que é parte de uma conexão de emparelhamento da VPC também exclui a conexão de emparelhamento de VPC. Se você solicitou uma conexão de emparelhamento da VPC com uma VPC em outra conta e excluiu sua VPC antes da outra parte ter aceitado a solicitação, a conexão de emparelhamento de VPC também será excluída. Você não pode excluir uma VPC para a qual possui uma `pending-acceptance` solicitação de VPC em outra conta. Você precisa, primeiro, rejeitar a solicitação de conexão de emparelhamento de VPC.

Quando você exclui uma conexão de emparelhamento, o status é definido como `Deleting` e, em seguida, como `Deleted`. Depois de excluir uma conexão, ela não poderá ser aceita, rejeitada ou editada. Para obter mais informações sobre por quanto tempo a conexão de emparelhamento permanece visível, consulte Ciclo de vida da conexão de emparelhamento de VPC.

Para excluir uma conexão de emparelhamento de VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Peering Connections (Conexões de emparelhamento).
3. Selecione a conexão de emparelhamento da VPC.
4. Escolha Actions (Ações), Delete peering connection (Excluir conexão de emparelhamento).
5. Quando a confirmação for solicitada, insira **`delete`** e selecione Excluir.

Como excluir uma conexão de emparelhamento da VPC usando a linha de comando

- delete-vpc-peering-connection (AWS CLI)
- Remove-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

## Solucionar problemas com a conexão de emparelhamento da VPC

Se estiver com problemas para se conectar a um recurso em uma VPC a partir de um recurso em uma VPC peer, siga este procedimento:

- Para cada recurso em cada VPC, observe se a tabela de rotas de sua sub-rede contém uma rota que envia o tráfego destinado à VPC peer para a conexão de emparelhamento da VPC. Isso garante que o tráfego de rede possa fluir adequadamente entre as duas VPCs. Para obter mais informações, consulte Atualizar tabelas de rotas.
- Para instâncias do EC2, certifique-se de que os grupos de segurança das instâncias do EC2 permitam tráfego de saída da VPC emparelhada. As regras de grupo de segurança controlam qual tráfego tem permissão para acessar as instâncias do EC2. Para obter mais informações, consulte Fazer referência a grupos de segurança de mesmo nível.
- Verifique se as ACLs de rede para as sub-redes que contêm seus recursos permitem o tráfego necessário vindo da VPC emparelhada. As ACLs de rede são uma camada adicional de segurança que filtra o tráfego no nível da sub-rede.

Se você ainda estiver tendo problemas, use o Analisador de Acessibilidade. O Analisador de Acessibilidade pode ajudar a identificar o componente específico, seja a tabela de rotas, o grupo de segurança ou a ACL de rede, que está causando o problema de conectividade entre as duas VPCs. Para obter mais informações, consulte o Guia do Analisador de Acessabilidade.

Verificar cuidadosamente as configurações da rede VPC é fundamental para diagnosticar e resolver os problemas de conexão de emparelhamento da VPC que você possa encontrar.

# Configurações comuns de conexões de emparelhamento de VPC

Esta seção descreve dois tipos comuns de configurações de emparelhamento de VPC que você pode implementar:

- Configurações de emparelhamento de VPC com rotas para uma VPC inteira: nessa configuração, você cria uma rota na tabela de rotas de cada VPC que envia todo o tráfego destinado à VPC emparelhada para a conexão de emparelhamento da VPC. Isso permite que qualquer recurso em uma VPC se comunique com qualquer recurso na VPC emparelhada, simplificando o gerenciamento. Porém, isso também significa que todo o tráfego entre as VPCs fluirá pela conexão de emparelhamento, o que pode se tornar um gargalo se o volume de tráfego for grande.
- Configurações de emparelhamento de VPC com rotas específicas: como alternativa, você pode criar rotas mais granulares na tabela de rotas de cada VPC que enviem tráfego apenas para determinadas sub-redes ou recursos na VPC emparelhada. Isso permite limitar o tráfego que flui pela conexão de emparelhamento apenas ao necessário, o que pode ser mais eficiente. Porém, isso também requer mais manutenção, pois você precisará atualizar as tabelas de rotas sempre que adicionar novos recursos na VPC emparelhada que precisem se comunicar.

A melhor estratégia depende de fatores como o tamanho e a complexidade da arquitetura da VPC, do volume de tráfego esperado entre as VPCs e das necessidades organizacionais em relação à segurança e ao acesso a recursos. Muitas empresas usam uma estratégia híbrida, com rotas amplas para padrões de tráfego comuns e rotas específicas para casos de uso mais sensíveis ou com intenso consumo de largura de banda.

Configurações



# Configurações de emparelhamento da VPC com rotas para uma VPC inteira

Você pode configurar conexões de emparelhamento de VPC para que suas tabelas de rota tenham acesso ao bloco CIDR da VPC de emparelhamento. Para obter mais informações sobre cenários

em que você possa precisar de uma configuração de conexão de emparelhamento de VPC específica, consulte Cenários de conexão de emparelhamento da VPC. Para obter mais informações sobre como criar e trabalhar com conexões de emparelhamento de VPC, consulte Conexões de emparelhamento da VPC.

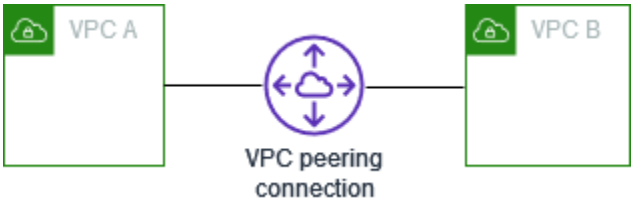
Para obter mais informações sobre como atualizar as tabelas de rotas, consulte Atualizar suas tabelas de rotas para uma conexão de emparelhamento da VPC.

Configurações

- Duas VPCs emparelhadas simultaneamente
- Uma VPC emparelhada com duas VPCs
- Três VPCs emparelhadas simultaneamente
- Várias VPCs emparelhadas

## Duas VPCs emparelhadas simultaneamente

Nesta configuração, há uma conexão de emparelhamento para a VPC A e a VPC B (`pcx-11112222`). As VPCs estão na mesma Conta da AWS, e seus blocos CIDR não se sobrepõem.




Você pode usar essa configuração quando tiver duas VPCs que requerem acesso aos recursos uma da outra. Por exemplo, você configurou a VPC A para seus registros de contabilidade e a VPC B para seus registros financeiros, e cada VPC deve poder acessar os recursos da outra sem restrições.

CIDR de VPC única

Atualize a tabela de rotas para cada VPC com uma rota que envie o tráfego do bloco CIDR da VPC de mesmo nível para a conexão de emparelhamento da VPC.

| Tabela de rotas | Destino | Destino |
| --- | --- | --- |
| VPC A | *CIDR da VPC A* | Local |

| Tabela de rotas | Destino | Destino |
|---|---|---|
| | *CIDR da VPC B* | pcx-11112222 |
| VPC B | *CIDR da VPC B* | Local |
| | *CIDR da VPC A* | pcx-11112222 |

Vários CIDRs IPv4 da VPC

Se a VPC A e a VPC B tiverem vários blocos CIDR IPv4 associados, você poderá atualizar a tabela de rotas para cada VPC com rotas para alguns ou todos os blocos CIDR IPv4 da VPC de mesmo nível.

| Tabela de rotas | Destino | Destino |
|---|---|---|
| VPC A | *CIDR 1 da VPC A* | Local |
| | *CIDR 2 da VPC A* | Local |
| | *CIDR 1 da VPC B* | pcx-11112222 |
| | *CIDR 2 da VPC B* | pcx-11112222 |
| VPC B | *CIDR 1 da VPC B* | Local |
| | *CIDR 2 da VPC B* | Local |
| | *CIDR 1 da VPC A* | pcx-11112222 |
| | *CIDR 2 da VPC A* | pcx-11112222 |

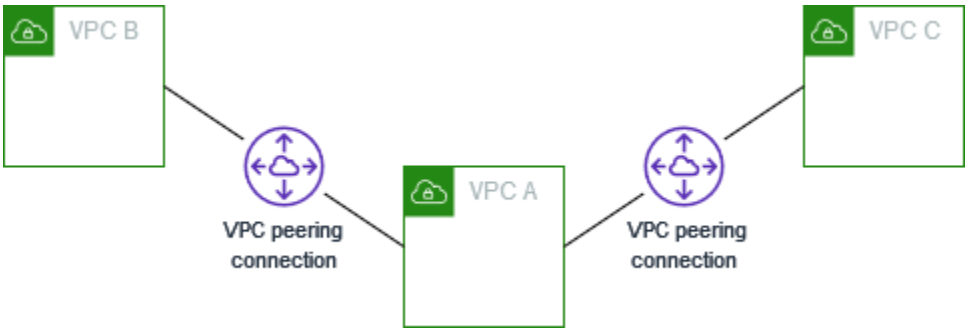
CIDRs IPv4 e IPv6 da VPC

Se a VPC A e a VPC B tiverem vários blocos CIDR IPv6 associados, você poderá atualizar a tabela de rotas para cada VPC com rotas para alguns ou todos os blocos CIDR IPv4 e IPv6 da VPC de mesmo nível.

| Tabela de rotas | Destino | Destino |
|---|---|---|
| VPC A | *CIDR IPv4 da VPC A* | Local |
| | *CIDR IPv6 da VPC A* | Local |
| | *CIDR IPv4 da VPC B* | pcx-11112222 |
| | *CIDR IPv6 da VPC B* | pcx-11112222 |
| VPC B | *CIDR IPv4 da VPC B* | Local |
| | *CIDR IPv6 da VPC B* | Local |
| | *CIDR IPv4 da VPC A* | pcx-11112222 |
| | *CIDR IPv6 da VPC A* | pcx-11112222 |

## Uma VPC emparelhada com duas VPCs

Nessa configuração, há uma VPC central (VPC A), uma conexão de emparelhamento entre a VPC A e a VPC B (`pcx-12121212`) e uma conexão de emparelhamento entre a VPC A e a VPC C (`pcx-23232323`). As três VPCs estão na mesma Conta da AWS, e seus blocos CIDR não se sobrepõem.



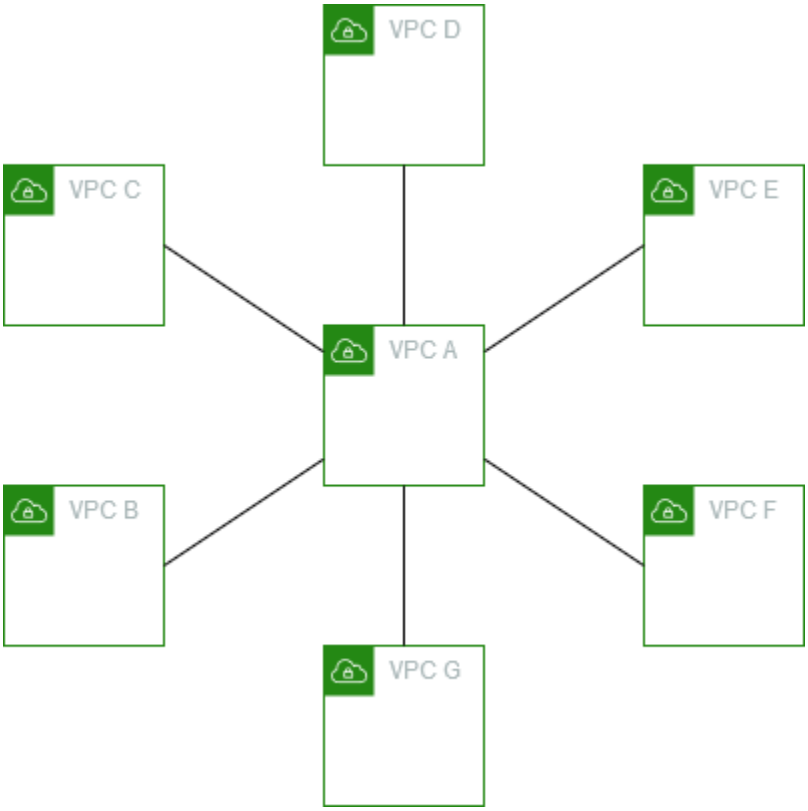

A VPC B e a VPC C não podem enviar tráfego diretamente uma para a outra por meio de uma VPC A, pois o emparelhamento de VPCs não aceita relações de emparelhamento transitivas. É possível criar uma conexão de emparelhamento da VPC entre a VPC B e a VPC C, conforme mostrado em Três VPCs emparelhadas simultaneamente. Para obter mais informações sobre cenários de emparelhamento incompatíveis, consulte the section called “Limitações de emparelhamento de VPC”.

Você pode usar esta configuração quando tiver recursos em uma VPC central, como um repositório de serviços que outras VPCs precisam acessar. As outras VPCs não precisam acessar os recursos umas das outras, só precisam acessar recursos da VPC central.

Atualize a tabela de rotas para cada VPC da seguinte forma para implementar essa configuração usando um bloco CIDR para cada VPC.

| Tabela de rotas | Destino | Destino |
|---|---|---|
| VPC A | *CIDR da VPC A* | Local |
| | *CIDR da VPC B* | pcx-12121212 |
| | *CIDR da VPC C* | pcx-23232323 |
| VPC B | *CIDR da VPC B* | Local |
| | *CIDR da VPC A* | pcx-12121212 |
| VPC C | *CIDR da VPC C* | Local |
| | *CIDR da VPC A* | pcx-23232323 |

Você pode estender essa configuração a VPCs adicionais. Por exemplo, a VPC A é emparelhada com a VPC B por meio da VPC G usando CIDRs IPv4 e IPv6, mas as outras VPCs não são emparelhadas umas com as outras. Nesse diagrama, as linhas representam conexões de emparelhamento da VPC.




Atualize a tabela de rotas da seguinte forma.

| Tabela de rotas | Destino | Destino |
|---|---|---|
| VPC A | *CIDR IPv4 da VPC A* | Local |
| | *CIDR IPv6 da VPC A* | Local |
| | *CIDR IPv4 da VPC B* | pcx-aaaabbbb |
| | *CIDR IPv6 da VPC B* | pcx-aaaabbbb |
| | *CIDR IPv4 da VPC C* | pcx-aaaacccc |
| | *CIDR IPv6 da VPC C* | pcx-aaaacccc |
| | *CIDR IPv4 da VPC D* | pcx-aaaadddd |
| | *CIDR IPv6 da VPC D* | pcx-aaaadddd |
| | *CIDR IPv4 da VPC E* | pcx-aaaaeeee |

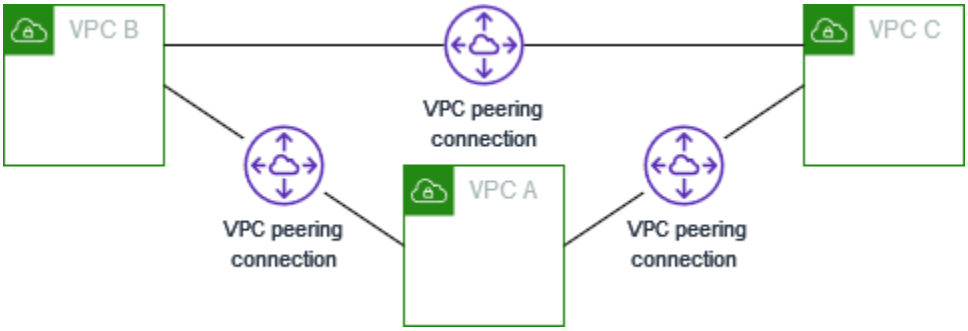
| Tabela de rotas | Destino | Destino |
|---|---|---|
| | *CIDR IPv6 da VPC E* | pcx-aaaaeeee |
| | *CIDR IPv4 da VPC F* | pcx-aaaaffff |
| | *CIDR IPv6 da VPC F* | pcx-aaaaffff |
| | *CIDR IPv4 da VPC G* | pcx-aaaagggg |
| | *CIDR IPv6 da VPC G* | pcx-aaaagggg |
| VPC B | *CIDR IPv4 da VPC B* | Local |
| | *CIDR IPv6 da VPC B* | Local |
| | *CIDR IPv4 da VPC A* | pcx-aaaabbbb |
| | *CIDR IPv6 da VPC A* | pcx-aaaabbbb |
| VPC C | *CIDR IPv4 da VPC C* | Local |
| | *CIDR IPv6 da VPC C* | Local |
| | *CIDR IPv4 da VPC A* | pcx-aaaacccc |
| | *CIDR IPv6 da VPC A* | pcx-aaaacccc |
| VPC D | *CIDR IPv4 da VPC D* | Local |
| | *CIDR IPv6 da VPC D* | Local |
| | *CIDR IPv4 da VPC A* | pcx-aaaadddd |
| | *CIDR IPv6 da VPC A* | pcx-aaaadddd |
| VPC E | *CIDR IPv4 da VPC E* | Local |
| | *CIDR IPv6 da VPC E* | Local |
| | *CIDR IPv4 da VPC A* | pcx-aaaaeeee |

| Tabela de rotas | Destino | Destino |
|---|---|---|
| | *CIDR IPv6 da VPC A* | pcx-aaaaeeee |
| VPC F | *CIDR IPv4 da VPC F* | Local |
| | *CIDR IPv6 da VPC F* | Local |
| | *CIDR IPv4 da VPC A* | pcx-aaaaffff |
| | *CIDR IPv6 da VPC A* | pcx-aaaaffff |
| VPC G | *CIDR IPv4 da VPC G* | Local |
| | *CIDR IPv6 da VPC G* | Local |
| | *CIDR IPv4 da VPC A* | pcx-aaaagggg |
| | *CIDR IPv6 da VPC A* | pcx-aaaagggg |

## Três VPCs emparelhadas simultaneamente

Nesta configuração, há três VPCs na mesma Conta da AWS com blocos CIDR que não se sobrepõem. As VPCs estão emparelhadas em uma malha completa da seguinte forma:

- A VPC A está emparelhada com a VPC B pela conexão de emparelhamento de VPC `pcx-aaaabbbb`
- A VPC A está emparelhada com a VPC C pela conexão de emparelhamento de VPC `pcx-aaaacccc`
- A VPC B está emparelhada com a VPC C pela conexão de emparelhamento de VPC `pcx-bbbbcccc`




É possível usar essa configuração quando há VPCs separadas que precisam compartilhar recursos entre si sem restrições. Por exemplo, como um sistema de compartilhamento de arquivos.

Atualize a tabela de rotas para cada VPC da seguinte forma para implementar essa configuração.

| Tabela de rotas | Destino | Destino |
|---|---|---|
| VPC A | *CIDR da VPC A* | Local |
| | *CIDR da VPC B* | pcx-aaaabbbb |
| | *CIDR da VPC C* | pcx-aaaacccc |
| VPC B | *CIDR da VPC B* | Local |
| | *CIDR da VPC A* | pcx-aaaabbbb |
| | *CIDR da VPC C* | pcx-bbbbcccc |
| VPC C | *CIDR da VPC C* | Local |
| | *CIDR da VPC A* | pcx-aaaacccc |
| | *CIDR da VPC B* | pcx-bbbbcccc |

Se a VPC A e a VPC B tiverem blocos CIDR IPv4 e IPv6 e a VPC C não tiver um bloco CIDR IPv6, atualize as tabelas de rotas da seguinte forma. Os recursos da VPC A e da VPC B podem se comunicar usando IPv6 pela conexão de emparelhamento da VPC. Entretanto, a VPC C não pode se comunicar com a VPC A ou a VPC B usando IPv6.

| Tabelas de rotas | Destination (Destino) | Destino |
|---|---|---|
| VPC A | *CIDR IPv4 da VPC A* | Local |
| | *CIDR IPv6 da VPC A* | Local |
| | *CIDR IPv4 da VPC B* | pcx-aaaabbbb |
| | *CIDR IPv6 da VPC B* | pcx-aaaabbbb |
| | *CIDR IPv4 da VPC C* | pcx-aaaacccc |
| VPC B | *CIDR IPv4 da VPC B* | Local |
| | *CIDR IPv6 da VPC B* | Local |
| | *CIDR IPv4 da VPC A* | pcx-aaaabbbb |
| | *CIDR IPv6 da VPC A* | pcx-aaaabbbb |
| | *CIDR IPv4 da VPC C* | pcx-bbbbcccc |
| VPC C | *CIDR IPv4 da VPC C* | Local |
| | *CIDR IPv4 da VPC A* | pcx-aaaacccc |
| | *CIDR IPv4 da VPC B* | pcx-bbbbcccc |

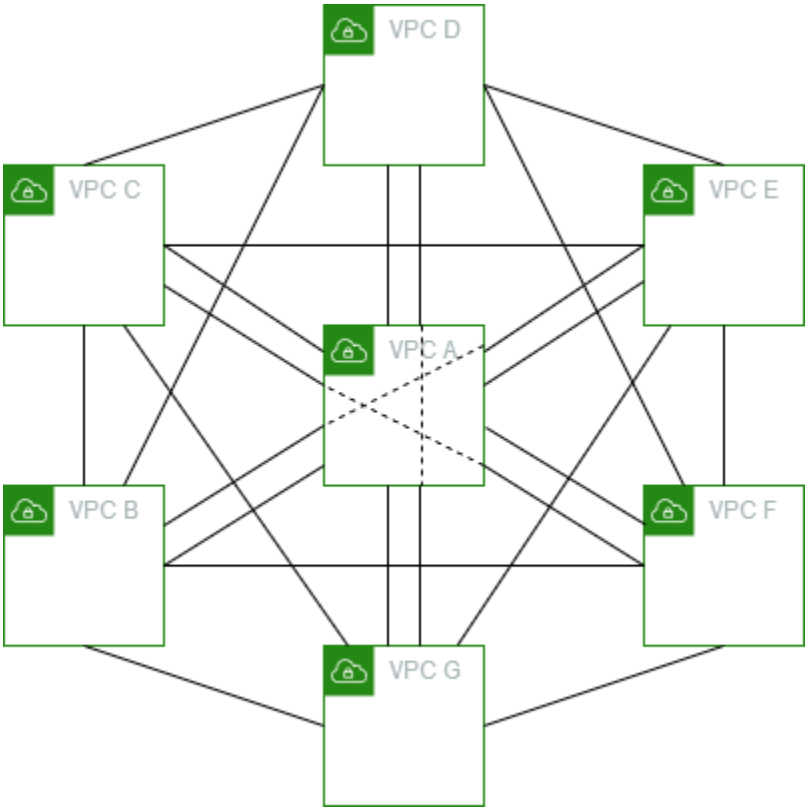
## Várias VPCs emparelhadas

Nessa configuração, há sete VPCs emparelhadas em uma configuração de malha completa. As VPCs estão na mesma Conta da AWS, e seus blocos CIDR não se sobrepõem.

| VPC | VPC | Conexão de emparelhamento de VPC |
|---|---|---|
| A | B | pcx-aaaabbbb |
| A | C | pcx-aaaacccc |
| A | D | pcx-aaaadddd |

| VPC | VPC | Conexão de emparelhamento de VPC |
|---|---|---|
| A | E | pcx-aaaaeeee |
| A | F | pcx-aaaaffff |
| A | G | pcx-aaaagggg |
| B | C | pcx-bbbbcccc |
| B | D | pcx-bbbbdddd |
| B | E | pcx-bbbbeeee |
| B | F | pcx-bbbbffff |
| B | G | pcx-bbbbgggg |
| C | D | pcx-ccccdddd |
| C | E | pcx-cccceeee |
| C | F | pcx-ccccffff |
| C | G | pcx-ccccgggg |
| D | E | pcx-ddddeeee |
| D | F | pcx-ddddffff |
| D | G | pcx-ddddgggg |
| E | F | pcx-eeeeffff |
| E | G | pcx-eeeegggg |
| F | G | pcx-ffffgggg |

Essa configuração de malha completa poderá ser usada quando houver várias VPCs que devem poder acessar recursos entre si sem restrição. Por exemplo, como uma rede de compartilhamento de arquivos. Nesse diagrama, as linhas representam conexões de emparelhamento da VPC.




Atualize a tabela de rotas para cada VPC da seguinte forma para implementar essa configuração.

| Tabela de rotas | Destino | Destino |
|---|---|---|
| VPC A | *CIDR da VPC A* | Local |
| | *CIDR da VPC B* | pcx-aaaabbbb |
| | *CIDR da VPC C* | pcx-aaaacccc |
| | *CIDR da VPC D* | pcx-aaaadddd |
| | *CIDR da VPC E* | pcx-aaaaeeee |
| | *CIDR da VPC F* | pcx-aaaaffff |
| | *CIDR da VPC G* | pcx-aaaagggg |
| VPC B | *CIDR da VPC B* | Local |
| | *CIDR da VPC A* | pcx-aaaabbbb |

| Tabela de rotas | Destino | Destino |
|---|---|---|
| | *CIDR da VPC C* | pcx-bbbbcccc |
| | *CIDR da VPC D* | pcx-bbbbdddd |
| | *CIDR da VPC E* | pcx-bbbbeeee |
| | *CIDR da VPC F* | pcx-bbbbffff |
| | *CIDR da VPC G* | pcx-bbbbgggg |
| VPC C | *CIDR da VPC C* | Local |
| | *CIDR da VPC A* | pcx-aaaacccc |
| | *CIDR da VPC B* | pcx-bbbbcccc |
| | *CIDR da VPC D* | pcx-ccccdddd |
| | *CIDR da VPC E* | pcx-cccceeee |
| | *CIDR da VPC F* | pcx-ccccffff |
| | *CIDR da VPC G* | pcx-ccccgggg |
| VPC D | *CIDR da VPC D* | Local |
| | *CIDR da VPC A* | pcx-aaaadddd |
| | *CIDR da VPC B* | pcx-bbbbdddd |
| | *CIDR da VPC C* | pcx-ccccdddd |
| | *CIDR da VPC E* | pcx-ddddeeee |
| | *CIDR da VPC F* | pcx-ddddffff |
| | *CIDR da VPC G* | pcx-ddddgggg |
| VPC E | *CIDR da VPC E* | Local |

| Tabela de rotas | Destino | Destino |
|---|---|---|
| | *CIDR da VPC A* | pcx-aaaaeeee |
| | *CIDR da VPC B* | pcx-bbbbeeee |
| | *CIDR da VPC C* | pcx-cccceeee |
| | *CIDR da VPC D* | pcx-ddddeeee |
| | *CIDR da VPC F* | pcx-eeeeffff |
| | *CIDR da VPC G* | pcx-eeeegggg |
| VPC F | *CIDR da VPC F* | Local |
| | *CIDR da VPC A* | pcx-aaaaffff |
| | *CIDR da VPC B* | pcx-bbbbffff |
| | *CIDR da VPC C* | pcx-ccccffff |
| | *CIDR da VPC D* | pcx-ddddffff |
| | *CIDR da VPC E* | pcx-eeeeffff |
| | *CIDR da VPC G* | pcx-ffffgggg |
| VPC G | *CIDR da VPC G* | Local |
| | *CIDR da VPC A* | pcx-aaaagggg |
| | *CIDR da VPC B* | pcx-bbbbgggg |
| | *CIDR da VPC C* | pcx-ccccgggg |
| | *CIDR da VPC D* | pcx-ddddgggg |
| | *CIDR da VPC E* | pcx-eeeegggg |
| | *CIDR da VPC F* | pcx-ffffgggg |

Se todas as VPCs tiverem blocos CIDR IPv6 associados, atualize as tabelas de rotas da seguinte forma.

| Tabela de rotas | Destino | Destino |
|---|---|---|
| VPC A | *CIDR IPv4 da VPC A* | Local |
| | *CIDR IPv6 da VPC A* | Local |
| | *CIDR IPv4 da VPC B* | pcx-aaaabbbb |
| | *CIDR IPv6 da VPC B* | pcx-aaaabbbb |
| | *CIDR IPv4 da VPC C* | pcx-aaaacccc |
| | *CIDR IPv6 da VPC C* | pcx-aaaacccc |
| | *CIDR IPv4 da VPC D* | pcx-aaaadddd |
| | *CIDR IPv6 da VPC D* | pcx-aaaadddd |
| | *CIDR IPv4 da VPC E* | pcx-aaaaeeee |
| | *CIDR IPv6 da VPC E* | pcx-aaaaeeee |
| | *CIDR IPv4 da VPC F* | pcx-aaaaffff |
| | *CIDR IPv6 da VPC F* | pcx-aaaaffff |
| | *CIDR IPv4 da VPC G* | pcx-aaaagggg |
| | *CIDR IPv6 da VPC G* | pcx-aaaagggg |
| VPC B | *CIDR IPv4 da VPC B* | Local |
| | *CIDR IPv6 da VPC B* | Local |
| | *CIDR IPv4 da VPC A* | pcx-aaaabbbb |
| | *CIDR IPv6 da VPC A* | pcx-aaaabbbb |
| | *CIDR IPv4 da VPC C* | pcx-bbbbcccc |

| Tabela de rotas | Destino | Destino |
|---|---|---|
| | *CIDR IPv6 da VPC C* | pcx-bbbbcccc |
| | *CIDR IPv4 da VPC D* | pcx-bbbbdddd |
| | *CIDR IPv6 da VPC D* | pcx-bbbbdddd |
| | *CIDR IPv4 da VPC E* | pcx-bbbbeeee |
| | *CIDR IPv6 da VPC E* | pcx-bbbbeeee |
| | *CIDR IPv4 da VPC F* | pcx-bbbbffff |
| | *CIDR IPv6 da VPC F* | pcx-bbbbffff |
| | *CIDR IPv4 da VPC G* | pcx-bbbbgggg |
| | *CIDR IPv6 da VPC G* | pcx-bbbbgggg |
| VPC C | *CIDR IPv4 da VPC C* | Local |
| | *CIDR IPv6 da VPC C* | Local |
| | *CIDR IPv4 da VPC A* | pcx-aaaacccc |
| | *CIDR IPv6 da VPC A* | pcx-aaaacccc |
| | *CIDR IPv4 da VPC B* | pcx-bbbbcccc |
| | *CIDR IPv6 da VPC B* | pcx-bbbbcccc |
| | *CIDR IPv4 da VPC D* | pcx-ccccdddd |
| | *CIDR IPv6 da VPC D* | pcx-ccccdddd |
| | *CIDR IPv4 da VPC E* | pcx-cccceeee |
| | *CIDR IPv6 da VPC E* | pcx-cccceeee |
| | *CIDR IPv4 da VPC F* | pcx-ccccffff |

| Tabela de rotas | Destino | Destino |
|---|---|---|
| | *CIDR IPv6 da VPC F* | pcx-ccccffff |
| | *CIDR IPv4 da VPC G* | pcx-ccccgggg |
| | *CIDR IPv6 da VPC G* | pcx-ccccgggg |
| VPC D | *CIDR IPv4 da VPC D* | Local |
| | *CIDR IPv6 da VPC D* | Local |
| | *CIDR IPv4 da VPC A* | pcx-aaaadddd |
| | *CIDR IPv6 da VPC A* | pcx-aaaadddd |
| | *CIDR IPv4 da VPC B* | pcx-bbbbdddd |
| | *CIDR IPv6 da VPC B* | pcx-bbbbdddd |
| | *CIDR IPv4 da VPC C* | pcx-ccccdddd |
| | *CIDR IPv6 da VPC C* | pcx-ccccdddd |
| | *CIDR IPv4 da VPC E* | pcx-ddddeeee |
| | *CIDR IPv6 da VPC E* | pcx-ddddeeee |
| | *CIDR IPv4 da VPC F* | pcx-ddddffff |
| | *CIDR IPv6 da VPC F* | pcx-ddddffff |
| | *CIDR IPv4 da VPC G* | pcx-ddddgggg |
| | *CIDR IPv6 da VPC G* | pcx-ddddgggg |
| VPC E | *CIDR IPv4 da VPC E* | Local |
| | *CIDR IPv6 da VPC E* | Local |
| | *CIDR IPv4 da VPC A* | pcx-aaaaeeee |

| Tabela de rotas | Destino | Destino |
|---|---|---|
| | *CIDR IPv6 da VPC A* | pcx-aaaaeeee |
| | *CIDR IPv4 da VPC B* | pcx-bbbbeeee |
| | *CIDR IPv6 da VPC B* | pcx-bbbbeeee |
| | *CIDR IPv4 da VPC C* | pcx-cccceeee |
| | *CIDR IPv6 da VPC C* | pcx-cccceeee |
| | *CIDR IPv4 da VPC D* | pcx-ddddeeee |
| | *CIDR IPv6 da VPC D* | pcx-ddddeeee |
| | *CIDR IPv4 da VPC F* | pcx-eeeeffff |
| | *CIDR IPv6 da VPC F* | pcx-eeeeffff |
| | *CIDR IPv4 da VPC G* | pcx-eeeegggg |
| | *CIDR IPv6 da VPC G* | pcx-eeeegggg |
| VPC F | *CIDR IPv4 da VPC F* | Local |
| | *CIDR IPv6 da VPC F* | Local |
| | *CIDR IPv4 da VPC A* | pcx-aaaaffff |
| | *CIDR IPv6 da VPC A* | pcx-aaaaffff |
| | *CIDR IPv4 da VPC B* | pcx-bbbbffff |
| | *CIDR IPv6 da VPC B* | pcx-bbbbffff |
| | *CIDR IPv4 da VPC C* | pcx-ccccffff |
| | *CIDR IPv6 da VPC C* | pcx-ccccffff |
| | *CIDR IPv4 da VPC D* | pcx-ddddffff |

| Tabela de rotas | Destino | Destino |
|---|---|---|
| | *CIDR IPv6 da VPC D* | pcx-ddddffff |
| | *CIDR IPv4 da VPC E* | pcx-eeeeffff |
| | *CIDR IPv6 da VPC E* | pcx-eeeeffff |
| | *CIDR IPv4 da VPC G* | pcx-ffffgggg |
| | *CIDR IPv6 da VPC G* | pcx-ffffgggg |
| VPC G | *CIDR IPv4 da VPC G* | Local |
| | *CIDR IPv6 da VPC G* | Local |
| | *CIDR IPv4 da VPC A* | pcx-aaaagggg |
| | *CIDR IPv6 da VPC A* | pcx-aaaagggg |
| | *CIDR IPv4 da VPC B* | pcx-bbbbgggg |
| | *CIDR IPv6 da VPC B* | pcx-bbbbgggg |
| | *CIDR IPv4 da VPC C* | pcx-ccccgggg |
| | *CIDR IPv6 da VPC C* | pcx-ccccgggg |
| | *CIDR IPv4 da VPC D* | pcx-ddddgggg |
| | *CIDR IPv6 da VPC D* | pcx-ddddgggg |
| | *CIDR IPv4 da VPC E* | pcx-eeeegggg |
| | *CIDR IPv6 da VPC E* | pcx-eeeegggg |
| | *CIDR IPv4 da VPC F* | pcx-ffffgggg |
| | *CIDR IPv6 da VPC F* | pcx-ffffgggg |

# Configurações de emparelhamento de VPCs com rotas específicas

É possível configurar tabelas de rotas para uma conexão de emparelhamento de VPC para restringir o acesso a um bloco CIDR da sub-rede, a um bloco CIDR específico (se a VPC tiver vários blocos CIDR) ou a um recurso específico em uma VPC emparelhada. Nestes exemplos, uma VPC central é emparelhada a pelo menos duas VPCs com blocos CIDR sobrepostos.

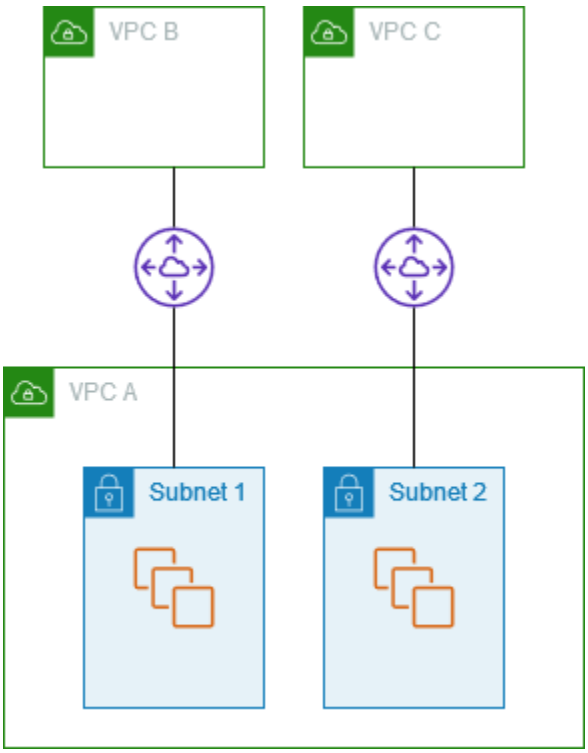
Para exemplos de cenários nos quais você possa precisar de uma configuração de conexão de emparelhamento de VPC específica, consulte Cenários de conexão de emparelhamento da VPC. Para obter mais informações sobre como trabalhar com conexões de emparelhamento de VPC, consulte Conexões de emparelhamento da VPC. Para obter mais informações sobre como atualizar as tabelas de rotas, consulte Atualizar suas tabelas de rotas para uma conexão de emparelhamento da VPC.

Configurações

- Duas VPCs que acessam sub-redes específicas em uma VPC
- Duas VPCs que acessam blocos CIDR específicos em uma VPC
- Duas VPCs que acessam sub-redes específicas em duas VPCs
- Instâncias em uma VPC que acessam instâncias específicas em duas VPCs
- Uma VPC que acessa duas VPCs usando correspondências de prefixo mais longas
- Configurações de várias VPCs

## Duas VPCs que acessam sub-redes específicas em uma VPC

Nesta configuração, há uma VPC central com duas sub-redes (VPC A), uma conexão de emparelhamento entre a VPC A e a VPC B (`pcx-aaaabbbb`) e uma conexão de emparelhamento entre a VPC A e a VPC C (`pcx-aaaacccc`). Cada VPC exige acesso aos recursos em apenas uma das sub-redes na VPC A.




A tabela de rotas da sub-rede 1 usa a conexão de emparelhamento da VPC `pcx-aaaabbbb` para acessar todo o bloco CIDR da VPC B. A tabela de rotas da VPC B usa `pcx-aaaabbbb` para acessar o bloco CIDR da sub-rede 1 na VPC A. A tabela de rotas da sub-rede 2 aponta para a conexão de emparelhamento da VPC `pcx-aaaacccc` para acessar todo o bloco CIDR da VPC C. A tabela de rotas da VPC C usa `pcx-aaaacccc` para acessar o bloco CIDR da sub-rede 2 na VPC A.

| Tabela de rotas | Destino | Alvo |
|---|---|---|
| Sub-rede 1 (VPC A) | *CIDR da VPC A* | Local |
| | *CIDR da VPC B* | pcx-aaaabbbb |
| Sub-rede 2 (VPC A) | *CIDR da VPC A* | Local |
| | *CIDR da VPC C* | pcx-aaaacccc |
| VPC B | *CIDR da VPC B* | Local |
| | *CIDR da sub-rede 1* | pcx-aaaabbbb |
| VPC C | *CIDR da VPC C* | Local |

| Tabela de rotas | Destino | Alvo |
| --- | --- | --- |
| | *CIDR da sub-rede 2* | pcx-aaaacccc |

Você pode estender essa configuração para vários blocos CIDR. Suponha que a VPC A e a VPC B tenham blocos CIDR IPv4 e IPv6 e que a sub-rede 1 tenha um bloco CIDR IPv6 associado. Você pode habilitar a VPC B para se comunicar com a sub-rede 1 na VPC A por meio do IPv6 usando a conexão de emparelhamento da VPC. Para isso, adicione uma rota à tabela de rotas para a VPC A com um destino do bloco CIDR IPv6 para VPC B e uma rota à tabela de rotas para a VPC B com um destino do CIDR IPv6 da sub-rede 1 na VPC A.

| Tabela de rotas | Destino | Destino | Observações |
| --- | --- | --- | --- |
| Sub-rede 1 na VPC A | *CIDR IPv4 da VPC A* | Local | |
| | *CIDR IPv6 da VPC A* | Local | Rota local que é adicionada automaticamente para comunicação IPv6 na VPC. |
| | *CIDR IPv4 da VPC B* | pcx-aaaabbbb | |
| | *CIDR IPv6 da VPC B* | pcx-aaaabbbb | Rota para o bloco CIDR IPv6 da VPC B. |
| Sub-rede 2 na VPC A | *CIDR IPv4 da VPC A* | Local | |
| | *CIDR IPv6 da VPC A* | Local | Rota local que é adicionada automaticamente para comunicação IPv6 na VPC. |

| Tabela de rotas | Destino | Destino | Observações |
|---|---|---|---|
| | *CIDR IPv4 da VPC C* | pcx-aaaacccc | |
| VPC B | *CIDR IPv4 da VPC B* | Local | |
| | *CIDR IPv6 da VPC B* | Local | Rota local que é adicionada automatic amente para comunicação IPv6 na VPC. |
| | *CIDR IPv4 da sub-rede 1* | pcx-aaaabbbb | |
| | *CIDR IPv6 da sub-rede 1* | pcx-aaaabbbb | Rota para o bloco CIDR IPv6 da VPC A. |
| VPC C | *CIDR IPv4 da VPC C* | Local | |
| | *CIDR IPv4 da sub-rede 2* | pcx-aaaacccc | |

## Duas VPCs que acessam blocos CIDR específicos em uma VPC

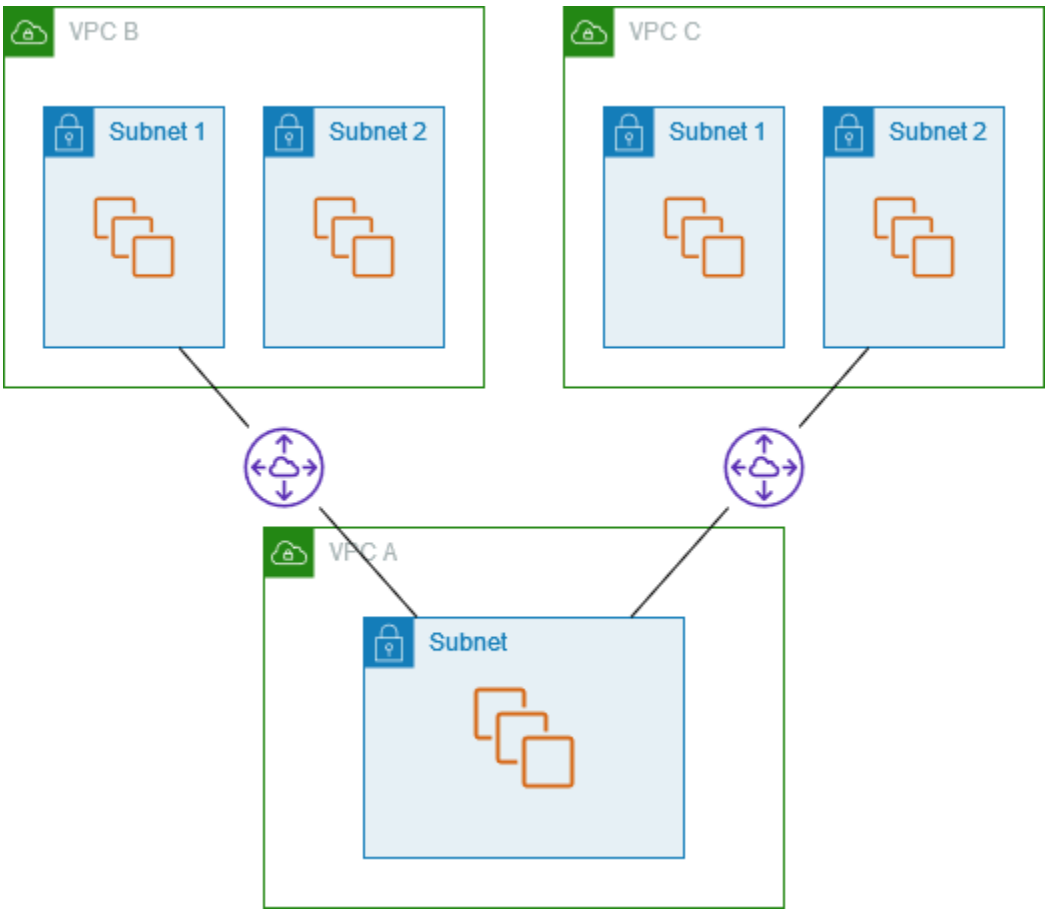
Nessa configuração, há uma VPC central (VPC A), uma conexão de emparelhamento entre a VPC A e a VPC B (`pcx-aaaabbbb`) e uma conexão de emparelhamento entre a VPC A e a VPC C (`pcx-aaaacccc`). A VPC A tem um bloco CIDR para cada conexão de emparelhamento.

| Tabela de rotas | Destino | Alvo |
|---|---|---|
| VPC A | *CIDR 1 da VPC A* | Local |
| | *CIDR 2 da VPC A* | Local |

| Tabela de rotas | Destino | Alvo |
| --- | --- | --- |
| | *CIDR da VPC B* | pcx-aaaabbbb |
| | *CIDR da VPC C* | pcx-aaaacccc |
| VPC B | *CIDR da VPC B* | Local |
| | *CIDR 1 da VPC A* | pcx-aaaabbbb |
| VPC C | *CIDR da VPC C* | Local |
| | *CIDR 2 da VPC A* | pcx-aaaacccc |

## Duas VPCs que acessam sub-redes específicas em duas VPCs

Nesta configuração, há uma VPC central (VPC A) com uma sub-rede, uma conexão de emparelhamento entre a VPC A e a VPC B (`pcx-aaaabbbb`) e uma conexão de emparelhamento entre a VPC A e a VPC C (`pcx-aaaacccc`). VPC B e VPC C possuem duas sub-redes cada. A conexão de emparelhamento entre VPC A e VPC B usa somente uma das sub-redes de VPC B. A conexão de emparelhamento entre VPC A e VPC C usa somente uma das sub-redes da VPC C.




Use essa configuração quando houver uma VPC central que tenha um único conjunto de recursos, como os serviços do Active Directory, que precisa ser acessado por outras VPCs. A VPC central não requer acesso total às VPCs com as quais foi emparelhada.

A tabela de rotas da VPC A usa as conexões de emparelhamento para acessar somente sub-redes específicas nas VPCs emparelhadas. A tabela de rotas da sub-rede 1 usa a conexão de emparelhamento com a VPC A para acessar a sub-rede na VPC A. A tabela de rotas da sub-rede 2 usa a conexão de emparelhamento com a VPC A para acessar a sub-rede na VPC A.

| Tabela de rotas | Destino | Alvo |
|---|---|---|
| VPC A | *CIDR da VPC A* | Local |
| | *CIDR da sub-rede 1* | pcx-aaaabbbb |
| | *CIDR da sub-rede 2* | pcx-aaaacccc |
| Sub-rede 1 (VPC B) | *CIDR da VPC B* | Local |

| Tabela de rotas | Destino | Alvo |
|---|---|---|
| | *Sub-rede no CIDR da VPC A* | pcx-aaaabbbb |
| Sub-rede 2 (VPC C) | *CIDR da VPC C* | Local |
| | *Sub-rede no CIDR da VPC A* | pcx-aaaacccc |

## Rota para tráfego de resposta

Se você tiver uma VPC emparelhada com várias VPCs que possuem blocos CIDR correspondentes ou sobrepostos, verifique se as tabelas de rotas estão configuradas, para evitar o envio de tráfego de resposta da sua VPC para a VPC incorreta. A AWS não oferece suporte ao encaminhamento invertido unicast em conexões de emparelhamento de VPC que verificam o IP de origem de pacotes e encaminham pacotes de resposta de volta à origem.

Por exemplo, a VPC A é emparelhada com VPC B e VPC C. VPC B e VPC C possuem blocos CIDR correspondentes e suas sub-redes possuem blocos CIDR correspondentes. A tabela de rotas para a sub-rede 2 na VPC B aponta para a conexão de emparelhamento da VPC `pcx-aaaabbbb` para acessar a sub-rede da VPC A. A tabela de rotas da VPC A está configurada para enviar tráfego destinado ao CIDR da VPC para a conexão de emparelhamento `pcx-aaaaccccc`.

| Tabela de rotas | Destino | Alvo |
|---|---|---|
| Sub-rede 2 (VPC B) | *CIDR da VPC B* | Local |
| | *Sub-rede no CIDR da VPC A* | pcx-aaaabbbb |
| VPC A | *CIDR da VPC A* | Local |
| | *CIDR da VPC C* | pcx-aaaacccc |

Suponha que uma instância na sub-rede 2 na VPC B envie tráfego para o servidor do Active Directory na VPC A usando a conexão de emparelhamento da VPC `pcx-aaaabbbb`. A VPC A

envia o tráfego de resposta ao servidor do Active Directory. Entretanto, a tabela de rotas da VPC A está configurada para enviar todo o tráfego dentro do intervalo de CIDR da VPC para a conexão de emparelhamento da VPC `pcx-aaaacccc`. Se a sub-rede 2 na VPC C tiver uma instância com o mesmo endereço IP da instância na sub-rede dois da VPC B, ela receberá o tráfego de resposta da VPC A. A instância na sub-rede 2 na VPC B não receberá resposta à sua solicitação à VPC A.

Para evitar essa situação, você pode adicionar uma rota específica à tabela de rotas da VPC A com o CIDR da sub-rede 2 na VPC B como destino de `pcx-aaaabbbb`. A nova rota é mais específica. Portanto, o tráfego destinado para o CIDR da sub-rede 2 é roteado para a conexão de emparelhamento da VPC `pcx-aaaabbbb`

Como alternativa, no exemplo a seguir, a tabela de rotas da VPC A possui uma rota para cada sub-rede da conexão de emparelhamento da VPC. A VPC A pode se comunicar com a sub-rede 2 na VPC B e com a sub-rede 1 na VPC C. Esse cenário será útil caso você precise adicionar outra conexão de emparelhamento da VPC a outra sub-rede que esteja no intervalo de endereço que a VPC B e a VPC C. Basta adicionar outra rota para essa sub-rede específica.

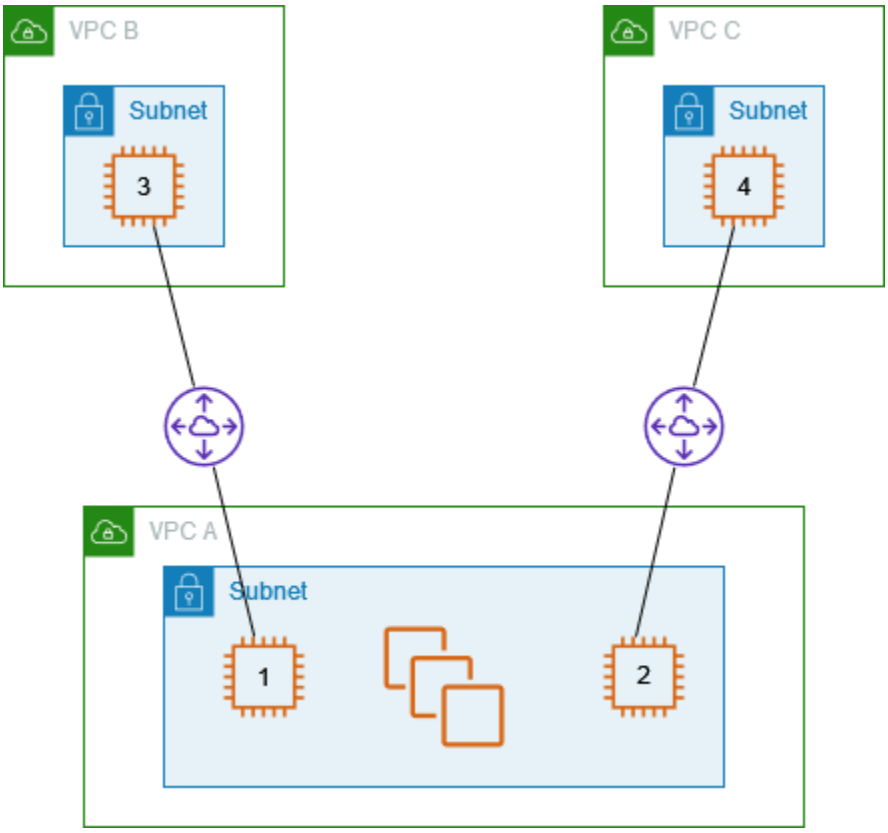
| Destino | Destino |
| --- | --- |
| *CIDR da VPC A* | Local |
| *CIDR da sub-rede 2* | pcx-aaaabbbb |
| *CIDR da sub-rede 1* | pcx-aaaacccc |

Como alternativa, dependendo do caso de uso, você pode criar uma rota para um endereço IP específico na VPC B para garantir que o tráfego volte para o servidor correto (a tabela de rotas usa a correspondência de prefixo mais longa para priorizar as rotas):

| Destino | Destino |
| --- | --- |
| *CIDR da VPC A* | Local |
| *Endereço IP específico na sub-rede 2* | pcx-aaaabbbb |
| *CIDR da VPC B* | pcx-aaaacccc |

# Instâncias em uma VPC que acessam instâncias específicas em duas VPCs

Nesta configuração, há uma VPC central (VPC A) com uma sub-rede, uma conexão de emparelhamento entre a VPC A e a VPC B (`pcx-aaaabbbb`) e uma conexão de emparelhamento entre a VPC A e a VPC C (`pcx-aaaacccc`). VPC A tem uma sub-rede com uma instância para cada conexão de emparelhamento. Você pode usar essa configuração para limitar o tráfego de emparelhamento a instâncias específicas.



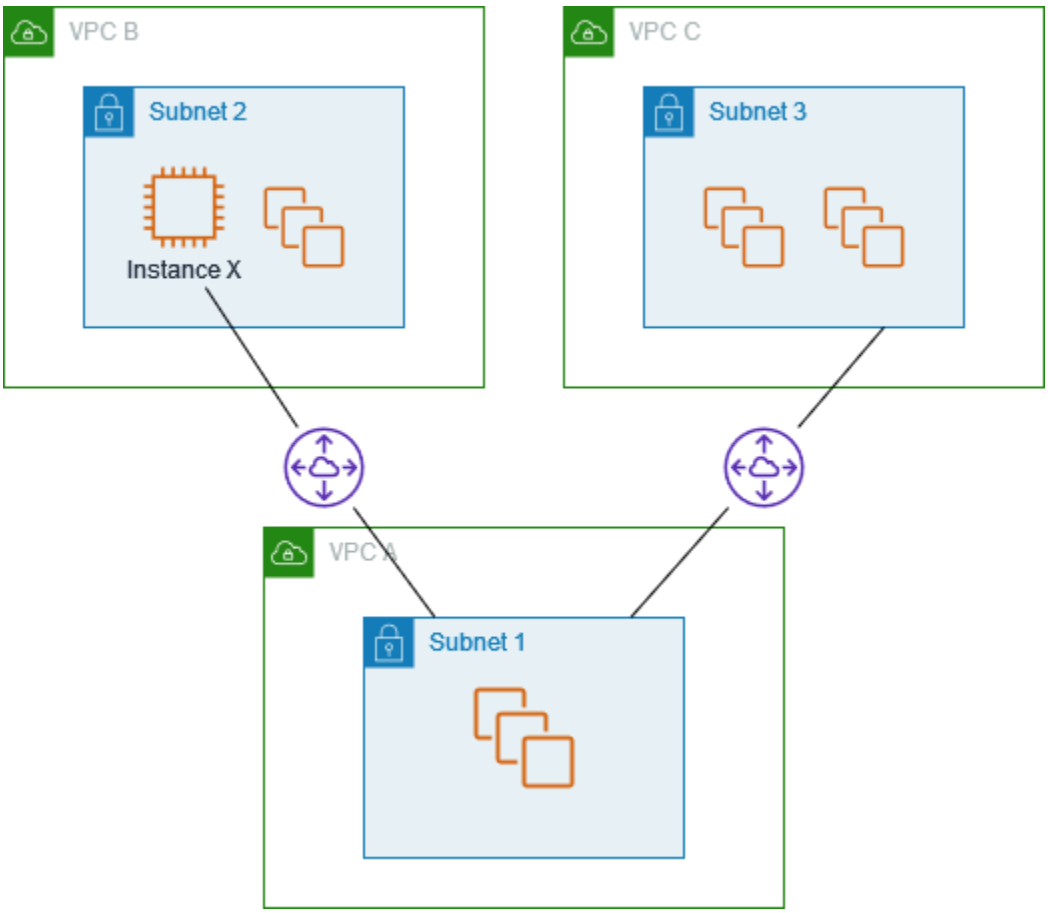

Cada tabela de rota VPC aponta para a conexão de emparelhamento de VPC relevante para acessar um único endereço IP (e, portanto, uma instância específica) na VPC de mesmo nível.

| Tabela de rotas | Destino | Alvo |
| --- | --- | --- |
| VPC A | *CIDR da VPC A* | Local |
| | *Endereço IP da instância 3* | pcx-aaaabbbb |

| Tabela de rotas | Destino | Alvo |
| --- | --- | --- |
| | *Endereço IP da instância 4* | pcx-aaaacccc |
| VPC B | *CIDR da VPC B* | Local |
| | *Endereço IP da instância 1* | pcx-aaaabbbb |
| VPC C | *CIDR da VPC C* | Local |
| | *Endereço IP da instância 2* | pcx-aaaacccc |

## Uma VPC que acessa duas VPCs usando correspondências de prefixo mais longas

Nesta configuração, há uma VPC central (VPC A) com uma sub-rede, uma conexão de emparelhamento entre a VPC A e a VPC B (`pcx-aaaabbbb`) e uma conexão de emparelhamento entre a VPC A e a VPC C (`pcx-aaaacccc`). A VPC B e VPC C possuem blocos CIDR correspondentes. Você utiliza a conexão de emparelhamento da VPC `pcx-aaaabbbb` para rotear o tráfego entre a VPC A e a instância específica na VPC B. Qualquer outro tráfego destinado ao intervalo de endereços CIDR compartilhado por VPC B e VPC C é roteado para a VPC C por meio de `pcx-aaaacccc`.




As tabelas de rotas VPC usam a correspondência de prefixo mais longa para selecionar a rota mais específica em toda a conexão de emparelhamento de VPC desejada. Qualquer outro tráfego é roteado através da próxima rota correspondente. Neste caso, através da conexão de emparelhamento de VPC `pcx-aaaacccc`.

| Tabela de rotas | Destino | Alvo |
|---|---|---|
| VPC A | *Bloco CIDR da VPC A* | Local |
| | *Endereço IP da instância X* | pcx-aaaabbbb |
| | *Bloco CIDR da VPC C* | pcx-aaaacccc |
| VPC B | *Bloco CIDR da VPC B* | Local |
| | *Bloco CIDR da VPC A* | pcx-aaaabbbb |

| Tabela de rotas | Destino | Alvo |
| --- | --- | --- |
| VPC C | *Bloco CIDR da VPC C* | Local |
| | *Bloco CIDR da VPC A* | pcx-aaaacccc |

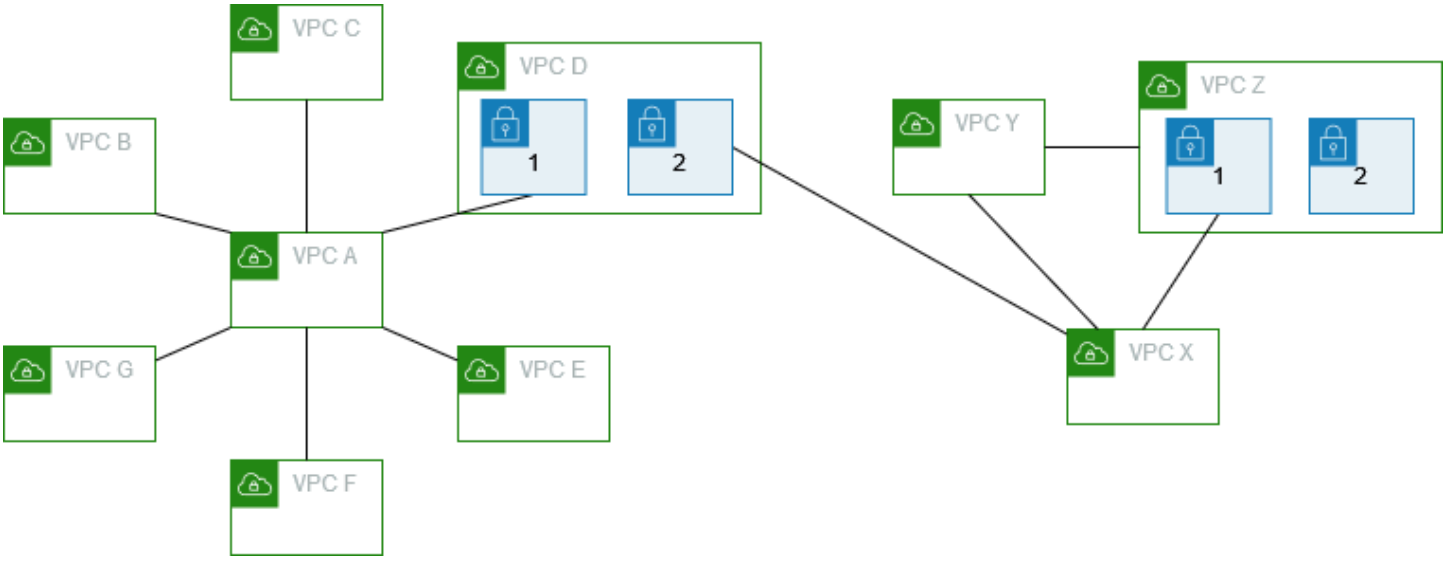
> **Important**
>
> Se uma instância diferente da instância X na VPC B envia tráfego para a VPC A, o tráfego de resposta pode ser roteado para a VPC C em vez de para a VPC B. Para obter mais informações, consulte Rota para tráfego de resposta.

## Configurações de várias VPCs

Nesta configuração, uma VPC central (VPC A) é emparelhada com várias VPCs em uma configuração spoke. Você também possui três VPCs (VPCs X, Y e Z) emparelhadas em uma configuração de malha completa.

A VPC D também possui uma conexão de emparelhamento da VPC com a VPC X (`pcx-ddddxxxx`). A VPC A e VPC X possuem blocos CIDR sobrepostos. Isso significa que o tráfego de emparelhamento entre a VPC A e a VPC D é limitado a uma sub-rede específica (sub-rede 1) na VPC D. Isso garante que, se a VPC D receber uma solicitação da VPC A ou da VPC X, ela enviará o tráfego de resposta à VPC correta. A AWS não oferece suporte ao encaminhamento do caminho inverso unicast em conexões de emparelhamento da VPC, que verifica o IP de origem de pacotes e roteia pacotes de resposta de volta à origem. Para ter mais informações, consulte Rota para tráfego de resposta.

Da mesma forma, a VPC D e a VPC Z possuem blocos CIDR sobrepostos. O tráfego entre a VPC D e a VPC X é limitado à sub-rede 2 na VPC D e o tráfego de emparelhamento entre a VPC X e a VPC Z está limitado à sub-rede 1 na VPC Z. Isso garante que, se a VPC X receber tráfego de emparelhamento da VPC D ou VPC Z, ela enviará o tráfego de resposta de volta à VPC correta.




As tabelas de rotas das VPCs B, C, E, F e G apontam para as conexões de emparelhamento relevantes para acessar o bloco CIDR completo para a VPC A. A tabela de rotas da VPC A aponta para as conexões de emparelhamento relevantes para as VPCs B, C, E, F e G para acessar seus blocos CIDR completos. Para a conexão de emparelhamento `pcx-aaaadddd`, a tabela de rotas da VPC A roteia o tráfego apenas para a sub-rede 1 na VPC D e a tabela de rotas da sub-rede 1 na VPCDC aponta para o bloco CIDR completo da VPC A.

A tabela de rotas da VPC Y aponta para as conexões de emparelhamento relevantes para acessar os blocos CIDR completos da VPC X e da VPC Z. A tabela de rotas da VPC Z aponta para a conexão de emparelhamento relevante para acessar o bloco CIDR completo da VPC Y. A tabela de rotas da sub-rede 1 na VPC Z aponta para a conexão de emparelhamento relevante para acessar o bloco CIDR completo da VPC Y. A tabela de rotas da VPC X aponta para a conexão de emparelhamento relevante para acessar a sub-rede 2 na VPC D e a sub-rede 1 na VPC Z.

| Tabela de rotas | Destino | Alvo |
|---|---|---|
| VPC A | *CIDR da VPC A* | Local |
| | *CIDR da VPC B* | pcx-aaaabbbb |
| | *CIDR da VPC C* | pcx-aaaacccc |
| | *CIDR da sub-rede 1 na VPC D* | pcx-aaaadddd |

| Tabela de rotas | Destino | Alvo |
|---|---|---|
| | *CIDR da VPC E* | pcx-aaaaeeee |
| | *CIDR da VPC F* | pcx-aaaaffff |
| | *CIDR da VPC G* | pcx-aaaagggg |
| VPC B | *CIDR da VPC B* | Local |
| | *CIDR da VPC A* | pcx-aaaabbbb |
| VPC C | *CIDR da VPC C* | Local |
| | *CIDR da VPC A* | pcx-aaaacccc |
| Sub-rede 1 na VPC D | *CIDR da VPC D* | Local |
| | *CIDR da VPC A* | pcx-aaaadddd |
| Sub-rede 2 na VPC D | *CIDR da VPC D* | Local |
| | *CIDR da VPC X* | pcx-ddddxxxx |
| VPC E | *CIDR da VPC E* | Local |
| | *CIDR da VPC A* | pcx-aaaaeeee |
| VPC F | *CIDR da VPC F* | Local |
| | *CIDR da VPC A* | pcx-aaaaffff |
| VPC G | *CIDR da VPC G* | Local |
| | *CIDR da VPC A* | pcx-aaaagggg |
| VPC X | *CIDR da VPC X* | Local |
| | *CIDR da sub-rede 2 na VPC D* | pcx-ddddxxxx |
| | *CIDR da VPC Y* | pcx-xxxxyyyy |

| Tabela de rotas | Destino | Alvo |
| --- | --- | --- |
| | *CIDR da sub-rede 1 na VPC Z* | pcx-xxxxzzzz |
| VPC Y | *CIDR da VPC Y* | Local |
| | *CIDR da VPC X* | pcx-xxxxyyyy |
| | *CIDR da VPC Z* | pcx-yyyyzzzz |
| VPC Z | *CIDR da VPC Z* | Local |
| | *CIDR da VPC Y* | pcx-yyyyzzzz |
| | *CIDR da VPC X* | pcx-xxxxzzzz |

# Cenários de conexão de emparelhamento da VPC

Inúmeros motivos podem exigir que você configure uma conexão de emparelhamento da VPC entre VPCs ou entre uma VPC que você possui e uma VPC em uma conta da AWS diferente. Os cenários a seguir podem ajudar você a determinar qual configuração melhor se adequa aos requisitos da rede.

Cenários

- Emparelhar duas ou mais VPCs para fornecer acesso total a recursos
- Emparelhar com uma VPC para acessar recursos centralizados

## Emparelhar duas ou mais VPCs para fornecer acesso total a recursos

Neste cenário, você possui duas ou mais VPCs que deseja emparelhar para permitir um compartilhamento total de recursos entre todas as VPCs. Veja os seguintes exemplos:

- Sua empresa possui uma VPC para o departamento financeiro e outra VPC para o departamento de contabilidade. O departamento financeiro exige acesso a todos os recursos do departamento de contabilidade e o departamento de contabilidade exige acesso a todos os recursos do departamento financeiro.
- Sua empresa possui vários departamentos de TI, cada um com sua própria VPC. Algumas VPCs estão localizadas na mesma conta da AWS e outras em uma conta da AWS diferente. Você deseja emparelhar todas as VPCs para que os departamentos de TI tenham acesso total aos recursos uns dos outros.

Para obter mais informações sobre como definir a configuração da conexão de emparelhamento de VPC e das tabelas de rotas para esse cenário, consulte a documentação a seguir:

- Duas VPCs emparelhadas simultaneamente
- Três VPCs emparelhadas simultaneamente
- Várias VPCs emparelhadas

Para obter mais informações sobre como criar e trabalhar com conexões de emparelhamento de VPC no console da Amazon VPC, consulte Conexões de emparelhamento da VPC.

## Emparelhar com uma VPC para acessar recursos centralizados

Neste cenário, você possui uma VPC central que contém recursos que deseja compartilhar com outras VPCs. Sua VPC central pode exigir acesso total ou parcial às VPCs de mesmo nível e, similarmente, as VPCs de mesmo nível podem exigir acesso total ou parcial à VPC central. Veja os seguintes exemplos:

- O departamento de TI da sua empresa possui uma VPC para compartilhamento de arquivos. Você quer emparelhar outras VPCs com a VPC central entretanto, não quer que as outras VPCs enviem tráfego entre si.
- Sua empresa possui uma VPC que você deseja compartilhar com seus clientes. Cada cliente pode criar uma conexão de emparelhamento de VPC com sua VPC, entretanto, seus clientes não podem rotear o tráfego para outras VPCs que estejam emparelhadas com a sua, nem conhecem as rotas de outros clientes.
- Você possui uma VPC central que é usada para serviços do Active Directory. Instâncias específicas em VPCs de mesmo nível enviam solicitações para os servidores do Active Directory e exigem acesso total à VPC central. A VPC central não exige acesso total às VPCs de mesmo nível; ela só precisa rotear o tráfego de resposta para as instâncias específicas.

Para obter mais informações sobre como criar e trabalhar com conexões de emparelhamento de VPC no console da Amazon VPC, consulte Conexões de emparelhamento da VPC.

# Identity and Access Management para emparelhamento de VPC

Por padrão, usuários não podem criar ou modificar conexões de emparelhamento de VPC. Para conceder acesso a recursos de emparelhamento da VPC, anexe uma política do IAM a uma identidade do IAM, como um perfil.

Exemplos

- Exemplo: criar uma conexão de emparelhamento da VPC
- Exemplo: aceitar uma conexão de emparelhamento da VPC
- Exemplo: excluir uma conexão de emparelhamento da VPC
- Exemplo: trabalhar em uma conta específica
- Exemplo: gerenciar conexões de emparelhamento da VPC usando o console

Para obter uma lista de ações da Amazon VPC, dos recursos compatíveis e das chaves de condição para cada ação, consulte Ações, recursos e chaves de condição do Amazon EC2 na Referência de autorização do serviço.

## Exemplo: criar uma conexão de emparelhamento da VPC

A política a seguir permite que usuários criem solicitações de conexão de emparelhamento da VPC usando VPCs marcadas com `Purpose=Peering`. A primeira instrução aplica uma chave de condição (`ec2:ResourceTag`) ao recurso da VPC. Observe que o recurso de VPC para a ação `CreateVpcPeeringConnection` é sempre a VPC solicitante.

A segunda instrução concede permissão aos usuários para criar os recursos de conexão de emparelhamento da VPC e usar o curinga * no lugar de um ID de recurso específico.

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id:vpc/*",
      "Condition": {
```

```
        "StringEquals": {
          "ec2:ResourceTag/Purpose": "Peering"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id:vpc-peering-connection/*"
    }
  ]
}
```

A política a seguir permite que os usuários da conta da AWS especificada criem conexões de emparelhamento da VPC usando qualquer VPC na região indicada, mas somente se a VPC que aceitará as conexões de emparelhamento for uma VPC específica em uma conta específica.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id-1:vpc/*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id-1:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:AccepterVpc": "arn:aws:ec2:region:account-id-2:vpc/vpc-id"
        }
      }
    }
  ]
}
```

## Exemplo: aceitar uma conexão de emparelhamento da VPC

A política a seguir permite que usuários aceitem solicitações de conexão de emparelhamento da VPC de uma conta específica da AWS. Isso ajuda a evitar que usuários aceitem solicitações

de conexão de emparelhamento de VPC de contas desconhecidas. A instrução usa a chave de condição `ec2:RequesterVpc` para reforçar isso.

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id-1:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:RequesterVpc": "arn:aws:ec2:region:account-id-2:vpc/*"
        }
      }
    }
  ]
}
```

A política a seguir concede permissões aos usuários para aceitarem solicitações de emparelhamento da VPC se a VPC tiver a tag `Purpose=Peering`.

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect": "Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id:vpc/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Purpose": "Peering"
        }
      }
    }
  ]
}
```

# Exemplo: excluir uma conexão de emparelhamento da VPC

A política a seguir permite que usuários da conta indicada excluam qualquer conexão de emparelhamento da VPC, exceto as que usam a VPC especificada, que está na mesma conta. A política especifica as chaves de condição `ec2:AccepterVpc` e `ec2:RequesterVpc`, já que a VPC pode ter sido a VPC solicitante ou a VPC de mesmo nível na solicitação de conexão de emparelhamento da VPC original.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
      "Action": "ec2:DeleteVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id:vpc-peering-connection/*",
      "Condition": {
        "ArnNotEquals": {
          "ec2:AccepterVpc": "arn:aws:ec2:region:account-id:vpc/vpc-id",
          "ec2:RequesterVpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
        }
      }
    }
  ]
}
```

# Exemplo: trabalhar em uma conta específica

A política a seguir permite que os usuários trabalhem com conexões de emparelhamento da VPC em uma conta específica. Os usuários podem visualizar, criar, aceitar, rejeitar e excluir conexões de emparelhamento da VPC, desde que todas estejam na conta da AWS.

A primeira instrução permite que os usuários visualizem todas as conexões de emparelhamento da VPC. O elemento `Resource` exige um * curinga neste caso, pois esta ação de API (`DescribeVpcPeeringConnections`), atualmente, não é compatível com permissões em nível de recurso.

A segunda instrução permite que os usuários criem conexões de emparelhamento da VPC e, para que possam fazê-lo, proporciona acesso a todas as VPCs na conta especificada.

A terceira instrução usa um curinga * como parte do elemento `Action` para permitir todas as ações de conexão de emparelhamento da VPC. As chaves de condição garantem que todas as ações só possam ser executadas em conexões de emparelhamento da VPC em VPCs que façam parte da conta. Por exemplo, um usuário não pode excluir uma conexão de emparelhamento da VPC se a VPC receptora ou solicitante estiver em uma conta diferente. Um usuário não pode criar uma conexão de emparelhamento da VPC com uma VPC em uma conta diferente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeVpcPeeringConnections",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": ["ec2:CreateVpcPeeringConnection","ec2:AcceptVpcPeeringConnection"],
      "Resource": "arn:aws:ec2:*:account-id:vpc/*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:*VpcPeeringConnection",
      "Resource": "arn:aws:ec2:*:account-id:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:AccepterVpc": "arn:aws:ec2:*:account-id:vpc/*",
          "ec2:RequesterVpc": "arn:aws:ec2:*:account-id:vpc/*"
        }
      }
    }
  ]
}
```

## Exemplo: gerenciar conexões de emparelhamento da VPC usando o console

Para visualizar conexões de emparelhamento de VPC no console da Amazon VPC, os usuários precisam ter permissão para usar a ação `ec2:DescribeVpcPeeringConnections`. Para usar a página Create Peering Connection (Criar conexão de emparelhamento), os usuários precisam ter

permissão para usar a ação `ec2:DescribeVpcs`. Isso concede a eles permissão para visualizar e selecionar uma VPC. Você pode aplicar permissões em nível de recurso para todas as ações `ec2:*PeeringConnection`, exceto `ec2:DescribeVpcPeeringConnections`.

A política a seguir permite que os usuários visualizem as conexões de emparelhamento da VPC e usem a caixa de diálogo Create VPC Peering Connection (Criar conexão de emparelhamento da VPC) para criar uma conexão de emparelhamento da VPC usando somente uma VPC solicitante específica. Se usuários tentarem criar uma conexão de emparelhamento de VPC com uma VPC solicitante, haverá falha na solicitação.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
      "Action": [
        "ec2:DescribeVpcPeeringConnections", "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": [
        "arn:aws:ec2:*:*:vpc/vpc-id",
        "arn:aws:ec2:*:*:vpc-peering-connection/*"
      ]
    }
  ]
}
```

# Cotas de conexão de emparelhamento da VPC para uma conta

O emparelhamento de VPC permite que você conecte duas VPCs. Isso permite que os recursos de uma VPC se comuniquem com os recursos da outra VPC como se estivessem na mesma rede. O emparelhamento de VPC é um atributo útil para conectar suas VPCs, seja na mesma região ou em regiões diferentes da AWS. Esta seção descreve as cotas que você deve observar ao trabalhar com conexões de emparelhamento de VPC.

As seguintes tabelas indicam as cotas, denominadas anteriormente limites, para conexões de emparelhamento da VPC para sua conta da AWS. Salvo indicação em contrário, é possível solicitar um aumento para essas cotas.

Se você descobrir que seus requisitos atuais de conexão de emparelhamento da VPC excedem as cotas padrão, recomendamos que envie uma solicitação de aumento de limite do serviço. Analisaremos seu caso de uso e trabalharemos com você para ajustar as cotas adequadamente, garantindo que seu ambiente de VPC possa atender às crescentes necessidades de sua empresa.

| Nome | Padrão | Ajustável |
| --- | --- | --- |
| Conexões emparelhadas de VPC ativas por VPC | 50 | Sim<br>(até 125) |
| Solicitações de conexão de emparelhamento da VPC pendentes | 25 | Sim |
| Tempo de expiração para uma solicitação de conexão de emparelhamento da VPC não aceita | 1 semana (168 horas) | Não |

Para obter mais informações sobre as regras de uso das conexões de emparelhamento da VPC, consulte Limitações de emparelhamento de VPC. Para obter mais informações sobre as cotas da Amazon VPC, consulte Cotas da Amazon VPC no Manual do usuário da Amazon VPC.

# Histórico do documento do Guia de emparelhamento da Amazon VPC

A tabela a seguir descreve as versões da documentação do Guia de emparelhamento da Amazon VPC.

| Alteração | Descrição | Data |
| --- | --- | --- |
| Tag na criação | É possível adicionar tags ao criar uma conexão de emparelhamento da VPC e uma tabela de rotas. | 20 de julho de 2020 |
| Emparelhamento entre regiões | A resolução do nome de host DNS é compatível com conexões de emparelhamento da VPC entre regiões na região Ásia-Pacífico (Hong Kong). | 26 de agosto de 2019 |
| Emparelhamento entre regiões | É possível criar uma conexão de emparelhamento da VPC entre VPCs em diferentes regiões da AWS. | 29 de novembro de 2017 |
| Suporte de resolução de DNS para emparelhamento de VPC | Você pode habilitar uma VPC local para que determine nomes de host DNS públicos para endereços IP privados quando em consultas provenientes de instâncias na VPC emparelhada. | 28 de julho de 2016 |
| Regras de grupo de segurança obsoletas | Você pode identificar se seu grupo de segurança está sendo referido nas regras de um grupo de segurança em | 12 de maio de 2016 |

| | | |
|---|---|---|
| | uma VPC emparelhada e pode identificar regras de grupo de segurança obsoletas. | |
| Uso de ClassicLink em uma conexão de emparelhamento de VPC | Você pode modificar sua conexão de emparelhamento da VPC para permitir que instâncias locais vinculados ao EC2-Classic comuniquem-se com instâncias em uma VPC emparelhada ou vice-versa. | 26 de abril de 2016 |
| Emparelhamento de VPC | É possível criar uma conexão de emparelhamento da VPC entre duas VPCs, o que permite que as instâncias em ambas as VPCs comuniquem-se entre si usando endereços IP privados. | 24 de março de 2014 |