



Emparelhamento de VPC

Amazon Virtual Private Cloud



Amazon Virtual Private Cloud: Emparelhamento de VPC

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não são propriedade da Amazon pertencem aos respectivos proprietários, os quais podem ou não ser afiliados, estar conectados ou ser patrocinados pela Amazon.

Table of Contents

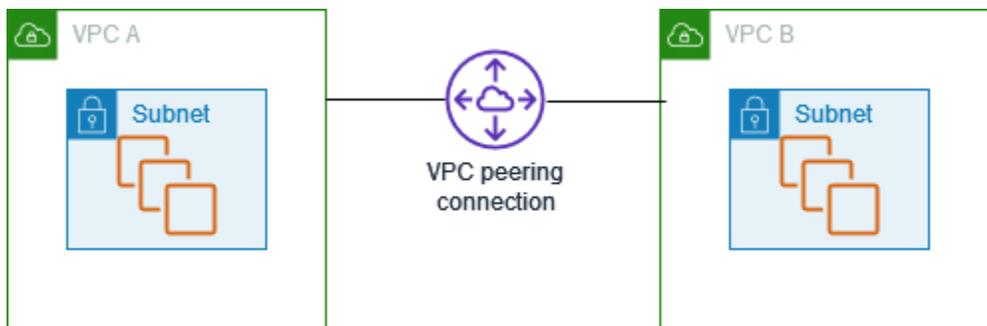
O que é emparelhamento de VPC?	1
Definição de preço para uma conexão de emparelhamento de VPC	2
Conceitos básicos de emparelhamento de VPC	3
Ciclo de vida da conexão de emparelhamento de VPC	3
Várias conexões de emparelhamento de VPC	5
Limitações de emparelhamento de VPC	6
Conexões de emparelhamento da VPC	9
Criar	9
Pré-requisitos	10
Criar com VPCs na mesma conta e região	10
Criar com VPCs na mesma conta e em diferentes regiões	11
Criar com VPCs em contas diferentes e na mesma região	11
Criar com VPCs em contas e regiões diferentes	12
Criar uma conexão de emparelhamento da VPC usando a linha de comando	13
Aceitar	13
Rejeitar	14
Visão	15
Atualizar tabelas de rotas	16
Fazer referência a grupos de segurança de mesmo nível	19
Identificar seus grupos de segurança referenciados	21
Trabalhar com regras de grupo de segurança obsoletas	21
Modificar opções de emparelhamento	23
Habilitar a resolução de DNS para a conexão de emparelhamento da VPC	23
Excluir	25
Solução de problemas	26
Configurações de emparelhamento de VPC	27
Rota para um bloco CIDR da VPC	27
Duas VPCs emparelhadas simultaneamente	27
Uma VPC emparelhada com duas VPCs	29
Três VPCs emparelhadas simultaneamente	33
Várias VPCs emparelhadas	35
Rotear para endereços específicos	45
Duas VPCs que acessam sub-redes específicas em uma VPC	45
Duas VPCs que acessam blocos CIDR específicos em uma VPC	48

Duas VPCs que acessam sub-redes específicas em duas VPCs	49
Instâncias em uma VPC que acessam instâncias específicas em duas VPCs	53
Uma VPC que acessa duas VPCs usando correspondências de prefixo mais longas	54
Configurações de várias VPCs	56
Cenários de emparelhamento de VPC	60
Emparelhar duas ou mais VPCs para fornecer acesso total a recursos	60
Emparelhar com uma VPC para acessar recursos centralizados	61
Gerenciamento de identidade e acesso	62
Criar uma conexão de emparelhamento de VPC	62
Aceitar uma conexão de emparelhamento de VPC	63
Excluir uma conexão de emparelhamento da VPC	65
Trabalhar em uma conta específica	65
Gerenciar conexões de emparelhamento da VPC no console	66
Cotas	68
Histórico do documento	69

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. Qualquer transferência de dados por uma conexão de emparelhamento da VPC que permaneça dentro de uma zona de disponibilidade (mesmo entre contas diferentes) será gratuita. Aplicam-se cobranças pela transferência de dados por meio de conexões de emparelhamento da VPC que cruzem zonas e regiões de disponibilidade. Para obter mais informações, consulte [Definição de preço do Amazon EC2](#).

Conceitos básicos de emparelhamento de VPC

Para estabelecer uma conexão de emparelhamento de VPC, faça o seguinte:

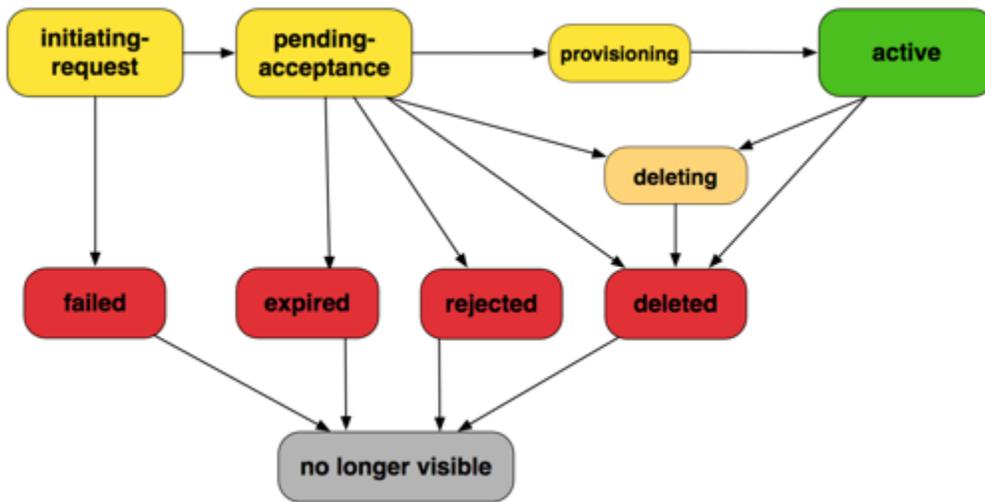
1. O proprietário da VPC solicitante envia um pedido ao proprietário da VPC receptora para criar a conexão de emparelhamento de VPC. O receptor da VPC pode ser de sua propriedade ou de outra conta da AWS e não pode ter um bloco CIDR que se sobreponha ao bloco CIDR da VPC solicitante.
2. O proprietário da VPC receptora aceita a solicitação da conexão de emparelhamento de VPC para aceitá-la.
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 ter mais informações, consulte [Trabalhar com 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

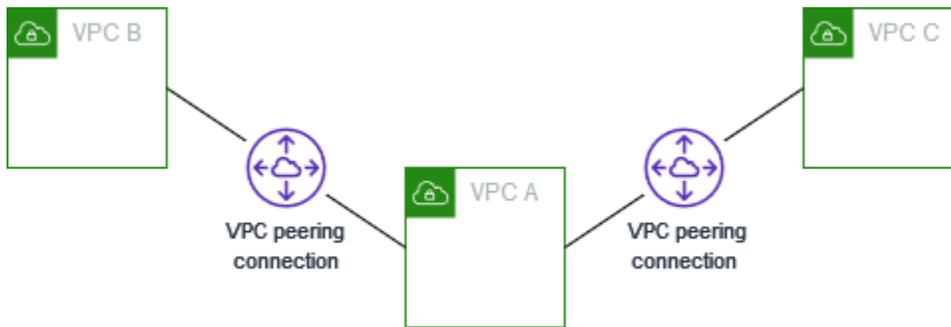
Se um evento em uma região na qual uma VPC reside impedir o fluxo do tráfego, o status da conexão de emparelhamento da VPC permanecerá **Active**.

- **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 de 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 [Exemplos](#) em Gateways de trânsito do Amazon VPC.

Conexões

- Há uma cota para o número de conexões de emparelhamento da VPC ativas e pendentes para cada VPC. Para ter 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 ter 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 ter 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 ter 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

- A unidade de transmissão máxima (MTU) da conexão de emparelhamento da VPC nas regiões é de 1.500 bytes. Não há suporte para jumbo frames (MTUs até 9.001 bytes) para conexões de emparelhamento da VPC entre regiões. Entretanto, eles são compatíveis com conexões de

emparelhamento da VPC na mesma região. 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.

Trabalhar com conexões de emparelhamento da VPC

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 conexão de emparelhamento de VPC](#)
- [Rejeitar uma conexão de emparelhamento de VPC](#)
- [Para visualizar as conexões 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](#)
- [Modificar opções de 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. Você pode solicitar uma conexão de emparelhamento da VPC com outra VPC na sua conta ou com uma VPC em outra conta da AWS. Para uma conexão de emparelhamento da VPC entre regiões na qual as VPCs estão em Regiões diferentes, a solicitação deverá ser feita a partir da Região da VPC solicitante.

Para ativar a solicitação, o proprietário da VPC que receber a solicitação deve aceitá-la. Para uma conexão de emparelhamento da VPC entre Regiões, a solicitação deverá ser aceita na Região da VPC aceitante. Para ter mais informações, consulte [the section called “Aceitar”](#). Para obter mais informações sobre o status de conexões de emparelhamento Pending acceptance, consulte [Ciclo de vida da conexão de emparelhamento de VPC](#).

Tarefas

- [Pré-requisitos](#)
- [Criar com VPCs na mesma conta e região](#)
- [Criar com VPCs na mesma conta e em diferentes regiões](#)

- [Criar com VPCs em contas diferentes e na mesma região](#)
- [Criar com VPCs em contas e regiões diferentes](#)
- [Criar uma conexão de emparelhamento da VPC usando a linha de comando](#)

Pré-requisitos

- Revise as [limitações e regras](#) para 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.

Criar com VPCs na mesma conta e região

Para criar uma conexão de emparelhamento da VPC com VPCs na mesma conta e região

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. Configure as seguintes informações e escolha Criar conexão de emparelhamento quando terminar:
 - Nome: é possível, opcionalmente, nomear sua conexão de emparelhamento da VPC.
 - ID da VPC (solicitante): selecione a VPC na sua conta com a qual deseja criar a conexão de emparelhamento da VPC.
 - Em Selecione uma outra VPC para emparelhar, escolha Minha conta selecione outra de suas VPCs.
 - (Opcional) Para adicionar uma tag, escolha Add new tag (Adicionar nova tag) e insira a chave e o valor da tag.
5. Escolha Ações, Aceitar solicitação.
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 ter mais informações, consulte [Atualizar suas tabelas de rotas para uma conexão de emparelhamento da VPC](#).

Criar com VPCs na mesma conta e em diferentes regiões

Para criar uma conexão de emparelhamento da VPC com VPCs na mesma conta e em diferentes regiões

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. Configure as seguintes informações e escolha Criar conexão de emparelhamento quando terminar:
 - Nome: é possível, opcionalmente, nomear sua conexão de emparelhamento da VPC. Ao fazer isso, é criada uma tag com a chave Name e o valor especificado.
 - ID da VPC (solicitante): selecione a VPC solicitante na sua conta com a qual deseja solicitar a conexão de emparelhamento da VPC.
 - Conta: escolha Minha conta.
 - Região: escolha Outra região, selecione a região da VPC aceitante.
 - ID da VPC (aceitante): selecione a VPC aceitante.
5. No seletor de Regiões, selecione a Região da VPC aceitante.
6. No painel de navegação, escolha Peering Connections (Conexões de emparelhamento). Selecione a conexão de emparelhamento da VPC que você criou e escolha Ações, Aceitar solicitação.
7. Quando a confirmação for solicitada, escolha Aceitar solicitação.
8. 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 ter mais informações, consulte [Atualizar suas tabelas de rotas para uma conexão de emparelhamento da VPC](#).

Criar com VPCs em contas diferentes e na mesma região

Para criar uma conexão de emparelhamento da VPC com VPCs em contas diferentes e na mesma região

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. Configure as informações conforme a seguir e escolha **Criar conexão de emparelhamento** quando terminar:
 - Nome: é possível, opcionalmente, nomear sua conexão de emparelhamento da VPC. Ao fazer isso, é criada uma tag com a chave do Name e um valor que você especificar. Esta tag só é visível para você; o proprietário da VPC de mesmo nível pode criar suas próprias tags para a conexão de emparelhamento de VPC.
 - ID da VPC (solicitante): selecione a VPC na sua conta com a qual criará a conexão de emparelhamento da VPC.
 - Account: escolha **Another account**.
 - ID da conta: digite o ID da Conta da AWS do proprietário da VPC aceitante.
 - ID da VPC (aceitante): insira o ID da VPC com a qual deseja criar a conexão de emparelhamento da VPC.

Criar com VPCs em contas e regiões diferentes

Para solicitar uma conexão de emparelhamento da VPC com VPCs em contas e regiões diferentes

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. Configure as informações conforme a seguir e escolha **Criar conexão de emparelhamento** quando terminar:
 - Nome: é possível, opcionalmente, nomear sua conexão de emparelhamento da VPC. Ao fazer isso, é criada uma tag com a chave do Name e um valor que você especificar. Esta tag só é visível para você; o proprietário da VPC de mesmo nível pode criar suas próprias tags para a conexão de emparelhamento de VPC.
 - ID da VPC (solicitante): selecione a VPC na sua conta com a qual criará a conexão de emparelhamento da VPC.
 - Account: escolha **Another account**.
 - ID da conta: digite o ID da Conta da AWS do proprietário da VPC aceitante.
 - Região: escolha **Outra região**, selecione a região na qual reside a VPC aceitante.

- ID da VPC (aceitante): insira o ID da VPC com a qual deseja criar a conexão de emparelhamento da VPC.

Criar uma conexão de emparelhamento da VPC 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 conexão de emparelhamento de 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](#). Você não pode aceitar uma solicitação de conexão de emparelhamento da VPC que enviou para outra conta da AWS. Se estiver criando uma conexão de emparelhamento da VPC na mesma conta da AWS, você precisará criar e aceitar a solicitação.

Se as VPCs estiverem em regiões diferentes, a solicitação deverá ser aceita na Região da VPC aceitante.

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 [Rejeitar uma conexão de emparelhamento de VPC](#). Você também pode ignorar a solicitação e deixá-la expirar; por padrão, solicitações expiram em 7 dias.

Depois que você aceitar a conexão de emparelhamento da VPC, será preciso adicionar uma entrada às tabelas de rotas para habilitar o tráfego entre as VPCs emparelhadas. Para ter mais informações, consulte [Atualizar suas tabelas de rotas para uma conexão de emparelhamento da VPC](#).

Para aceitar uma conexão de emparelhamento de VPC

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. Selecione a conexão de emparelhamento da VPC pendente (o status é `pending-acceptance`) e 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](#).

 Tip

Se você não conseguir visualizar a conexão pendente de emparelhamento da VPC, confira a Região. A solicitação de emparelhamento entre Regiões deverá ser aceita na Região da VPC aceitante.

5. Quando a confirmação for solicitada, escolha Aceitar solicitação.
6. 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 ter mais informações, consulte [Atualizar suas tabelas de rotas para uma conexão de emparelhamento da VPC](#).

Para aceitar uma conexão de emparelhamento da VPC usando a linha de comando ou uma API

- [accept-vpc-peering-connection](#) (AWS CLI)
- [Approve-EC2VpcPeeringConnection](#) (AWS Tools for Windows PowerShell)
- [AcceptVpcPeeringConnection](#) (API de consulta do Amazon EC2)

Rejeitar uma conexão de emparelhamento de VPC

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](#).

Para rejeitar 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 e escolha Ações, Rejeitar solicitação.
4. Quando a confirmação for solicitada, escolha Rejeitar solicitação.

Para rejeitar uma conexão de emparelhamento da VPC usando a linha de comando ou uma API

- [reject-vpc-peering-connection](#) (AWS CLI)
- [Deny-EC2VpcPeeringConnection](#) (AWS Tools for Windows PowerShell)
- [RejectVpcPeeringConnection](#) (API de consulta do Amazon EC2)

Para visualizar as conexões de emparelhamento da VPC

É possível visualizar todas as conexões de emparelhamento da VPC no console da Amazon VPC. Por padrão, o console exibe todas as conexões de emparelhamento da VPC em estados diferentes, incluindo as que podem ter sido recentemente excluídas ou rejeitadas. Para obter mais informações sobre o ciclo de vida de uma conexão de emparelhamento de VPC, consulte [Ciclo de vida da conexão de emparelhamento de VPC](#).

Para visualizar as conexões 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. Todas as conexões de emparelhamento da VPC estão listadas. Use a barra de pesquisa com filtro para filtrar os resultados.

Para descrever uma conexão de emparelhamento da VPC usando a linha de comando ou uma API

- [describe-vpc-peering-connections](#) (AWS CLI)
- [Get-EC2VpcPeeringConnections](#) (AWS Tools for Windows PowerShell)

- [DescribeVpcPeeringConnections](#) (API de consulta da Amazon EC2)

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	Destino
VPC A	<i>CIDR da VPC A</i>	Local
	<i>CIDR da VPC B</i>	pcx- <i>11112222</i>
VPC B	<i>CIDR da VPC B</i>	Local
	<i>CIDR da VPC A</i>	pcx- <i>11112222</i>

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 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 ter 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 Manual do usuário da Amazon VPC.

Para adicionar ou substituir uma rota usando a linha de comando ou uma API

- [create-route](#) (AWS CLI)
- [New-EC2Route](#) (AWS Tools for Windows PowerShell)
- [CreateRoute](#) (API de consulta do Amazon EC2)
- [replace-route](#) (AWS CLI)
- [Set-EC2Route](#) (AWS Tools for Windows PowerShell)

- [ReplaceRoute](#) (API da consulta do Amazon EC2)

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 security groups de VPC para referenciar security groups na VPC emparelhada. Fazendo isso, você permite que o tráfego flua entre as instâncias associadas com o grupo de segurança referenciado na VPC emparelhada.

Requisitos

- 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 em outra conta da AWS, inclua o número da conta no campo Source (Origem) ou Destination (Destino); 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.
- Para referenciar um security group em uma VPC de mesmo nível, a conexão de emparelhamento precisa estar no estado `active`.
- 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.

Para atualizar regras de um security group usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o grupo de segurança e escolha Ações, Editar regras de entrada para modificar as regras de entrada, ou escolha Ações, Editar regras de saída para modificar as regras de saída.
4. Para adicionar uma regra, escolha Adicionar regra e especifique o tipo, protocolo e intervalo de porta. Em Origem (regra de entrada) ou Destino (regra de saída), insira o ID do grupo de

segurança na VPC de emparelhamento, se ela estiver na mesma região, ou o bloco CIDR da VPC de emparelhamento, se ela estiver em uma região diferente.

 Note

Os security groups em uma VPC de emparelhamento não exibidos automaticamente.

5. Para editar uma regra existente, altere seus valores (por exemplo, a origem ou a descrição).
6. Para excluir uma regra, escolha Excluir, próximo à regra.
7. Escolha Salvar regras.

Para atualizar regras de entrada usando a linha de comando

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

Para atualizar regras de saída usando a linha de comando

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

Por exemplo, para atualizar seu grupo de segurança `sg-aaaa1111` para permitir acesso de entrada por HTTP de `sg-bbbb2222` que está em uma VPC de mesmo nível, você poderá usar o seguinte comando AWS CLI:

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

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)
- [DescribeSecurityGroupReferences](#) (API de consulta do Amazon EC2)

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.

Trabalhar 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.

Para visualizar e excluir regras de security group 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. Escolha Actions (Ações), Manage stale rules (Gerenciar regras obsoletas).
4. Para VPC, escolha a VPC com as regras obsoletas.
5. Selecione a opção Editar.
6. Escolha o botão Delete (Excluir) ao lado da regra que deseja excluir. Selecione Visualizar alterações, Salvar regras.

Para descrever as regras de security group obsoleto usando a linha de comando ou uma API

- [describe-stale-security-groups](#) (AWS CLI)
- [Get-EC2StaleSecurityGroup](#) (AWS Tools for Windows PowerShell)
- [DescribeStaleSecurityGroups](#) (API de consulta do Amazon EC2)

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](#).

Modificar opções de conexão de emparelhamento da VPC

Você pode modificar uma conexão de emparelhamento da VPC para fazer o seguinte:

- Habilite uma VPC para solucionar nomes de hosts DNS de IPv4 público para endereços IPv4 privados quando consultados em instâncias da VPC de mesmo nível. Para ter mais informações, consulte [Habilitar a resolução de DNS para a conexão de emparelhamento da VPC](#).

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

Para habilitar uma VPC para solucionar nomes de hosts DNS de IPv4 público para endereços IPv4 privados quando consultados em instâncias da VPC de mesmo nível, é necessário modificar a conexão de emparelhamento existente.

As duas VPCs devem ser habilitadas para nomes de hosts DNS e resolução DNS.

Não é possível habilitar o suporte de resolução DNS ao criar uma conexão de emparelhamento. É possível habilitar o suporte de resolução DNS para uma conexão de emparelhamento existente que está no estado `active`.

Para habilitar a resolução de DNS para uma conexão de emparelhamento

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 e escolha Ações, Editar configurações de DNS.
4. Para certificar-se de que as consultas da VPC de mesmo nível resolvem endereços IP privados em sua VPC local, escolha a opção para habilitar a resolução DNS para consultas na VPC de mesmo nível. Essa opção é Requester DNS resolution (Resolução DNS do solicitante) ou Acceptor DNS resolution (Resolução DNS do aceitante), dependendo se a VPC é a VPC solicitante ou aceitante.
5. Se a VPC de emparelhamento estiver na mesma Conta da AWS, será possível ativar a resolução de DNS para ambas as VPCs na conexão de emparelhamento.
6. Escolha Salvar alterações.
7. Se a VPC de emparelhamento estiver em uma outra AWS ou em uma região diferente, o proprietário da VPC de emparelhamento deverá fazer login no console da VPC, executar as etapas de 2 a 4 e escolher Salvar alterações.

Para habilitar uma resolução DNS usando a linha de comando ou uma API

- [modify-vpc-peering-connection-options](#) (AWS CLI)
- [Edit-EC2VpcPeeringConnectionOption](#) (AWS Tools for Windows PowerShell)
- [ModifyVpcPeeringConnectionOptions](#) (API de consulta do Amazon EC2)

Você precisa modificar as opções de emparelhamento de VPC do solicitante se você for o solicitante da conexão de emparelhamento de VPC e precisa modificar as opções de emparelhamento de VPC do receptor se você for o receptor da conexão de emparelhamento da VPC. Você pode usar os comandos [describe-vpc-peering-connections](#) ou [Get-EC2VpcPeeringConnections](#) para verificar qual VPC é receptora e qual é solicitante em uma conexão de emparelhamento de VPC. Para conexões de emparelhamento entre Regiões, você precisa usar a Região da VPC solicitante para modificar as opções de emparelhamento da VPC solicitante e a Região da VPC aceitante para modificar as opções de emparelhamento da VPC aceitante.

Neste exemplo, você é o solicitante da conexão de emparelhamento de VPC, portanto, modifique as opções de conexão de emparelhamento usando a AWS CLI, da seguinte forma:

```
aws ec2 modify-vpc-peering-connection-options --vpc-peering-connection-id pcx-aaaabbbb
--requester-peering-connection-options AllowDnsResolutionFromRemoteVpc=true
```

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. Excluimos 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 escolha Excluir.

Para excluir uma conexão de emparelhamento da VPC usando a linha de comando ou uma API

- [delete-vpc-peering-connection](#) (AWS CLI)
- [Remove-EC2VpcPeeringConnection](#) (AWS Tools for Windows PowerShell)
- [DeleteVpcPeeringConnection](#) (API de consulta do Amazon EC2)

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. Para ter mais informações, consulte [Atualizar tabelas de rotas](#).
- Para instâncias do EC2, verifique se os grupos de segurança das instâncias do EC2 permitem tráfego a partir da VPC peer. Para ter mais informações, consulte [Fazer referência a grupos de segurança de mesmo nível](#).
- Para cada recurso de cada VPC, verifique se a ACL de rede de sua sub-rede permite o tráfego proveniente da VPC peer.

Também é possível usar o Analisador de Acessibilidade para identificar o componente com problema de configuração, como tabela de rotas, grupo de segurança ou ACL de rede. Para obter mais informações, consulte o [Guia do Analisador de Acessibilidade](#).

Configurações de emparelhamento de VPC

A documentação a seguir descreve os diferentes tipos de configurações de emparelhamento de VPC.

Configurações

- [Configurações de emparelhamento da VPC com rotas para uma VPC inteira](#)
- [Configurações de emparelhamento de VPCs com rotas específicas](#)

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 emparelhamento de VPC](#). Para obter mais informações sobre como criar e trabalhar com conexões de emparelhamento de VPC, consulte [Trabalhar com conexões de emparelhamento da VPC](#).

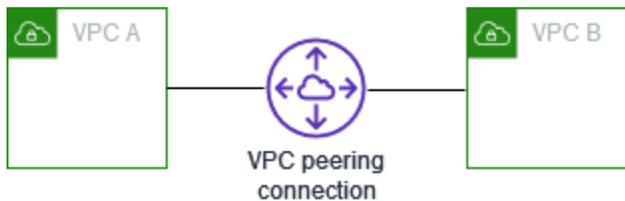
Para obter mais informações sobre como atualizar as tabelas de rotas, consulte [Atualizar suas tabelas de rotas para uma conexão de emparelhamento da VPC](#).

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	<i>CIDR da VPC A</i>	Local
	<i>CIDR da VPC B</i>	pcx-11112222
VPC B	<i>CIDR da VPC B</i>	Local
	<i>CIDR da VPC A</i>	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	<i>CIDR 1 da VPC A</i>	Local
	<i>CIDR 2 da VPC A</i>	Local
	<i>CIDR 1 da VPC B</i>	pcx-11112222
	<i>CIDR 2 da VPC B</i>	pcx-11112222

Tabela de rotas	Destino	Destino
VPC B	<i>CIDR 1 da VPC B</i>	Local
	<i>CIDR 2 da VPC B</i>	Local
	<i>CIDR 1 da VPC A</i>	pcx-11112222
	<i>CIDR 2 da VPC A</i>	pcx-11112222

CIDRs IPv4 e IPv6 da VPC

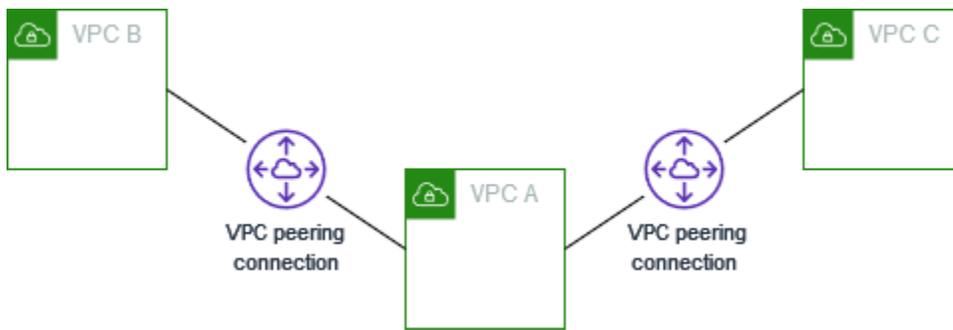
Se a VPC A e a VPC B tiverem vários blocos CIDR IPv6 associados, você poderá atualizar a tabela de rotas para cada VPC com rotas para alguns ou todos os blocos CIDR IPv4 e IPv6 da VPC de mesmo nível.

Tabela de rotas	Destino	Destino
VPC A	<i>CIDR IPv4 da VPC A</i>	Local
	<i>CIDR IPv6 da VPC A</i>	Local
	<i>CIDR IPv4 da VPC B</i>	pcx-11112222
	<i>CIDR IPv6 da VPC B</i>	pcx-11112222
VPC B	<i>CIDR IPv4 da VPC B</i>	Local
	<i>CIDR IPv6 da VPC B</i>	Local
	<i>CIDR IPv4 da VPC A</i>	pcx-11112222
	<i>CIDR IPv6 da VPC A</i>	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.



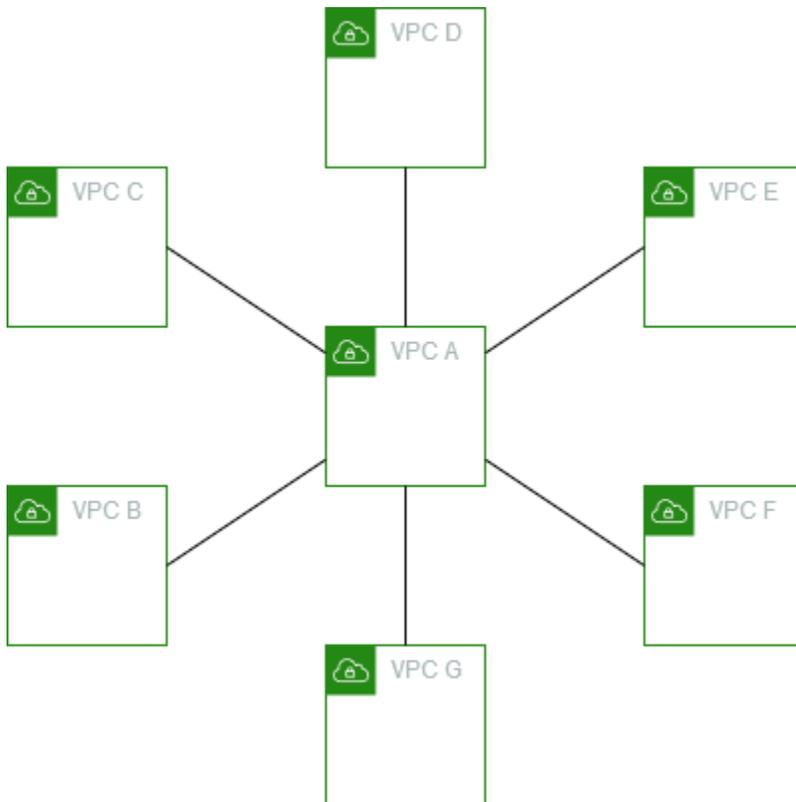
A VPC B e a VPC C não podem enviar tráfego diretamente uma para a outra por meio de uma VPC A, pois o emparelhamento de VPCs não aceita relações de emparelhamento transitivas. É possível criar uma conexão de emparelhamento da VPC entre a VPC B e a VPC C, conforme mostrado em [Três VPCs emparelhadas simultaneamente](#). 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	<i>CIDR da VPC A</i>	Local
	<i>CIDR da VPC B</i>	pcx-12121212
	<i>CIDR da VPC C</i>	pcx-23232323
VPC B	<i>CIDR da VPC B</i>	Local
	<i>CIDR da VPC A</i>	pcx-12121212
VPC C	<i>CIDR da VPC C</i>	Local
	<i>CIDR da VPC A</i>	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	<i>CIDR IPv4 da VPC A</i>	Local
	<i>CIDR IPv6 da VPC A</i>	Local
	<i>CIDR IPv4 da VPC B</i>	pcx-aaaabbbb
	<i>CIDR IPv6 da VPC B</i>	pcx-aaaabbbb
	<i>CIDR IPv4 da VPC C</i>	pcx-aaaacccc
	<i>CIDR IPv6 da VPC C</i>	pcx-aaaacccc

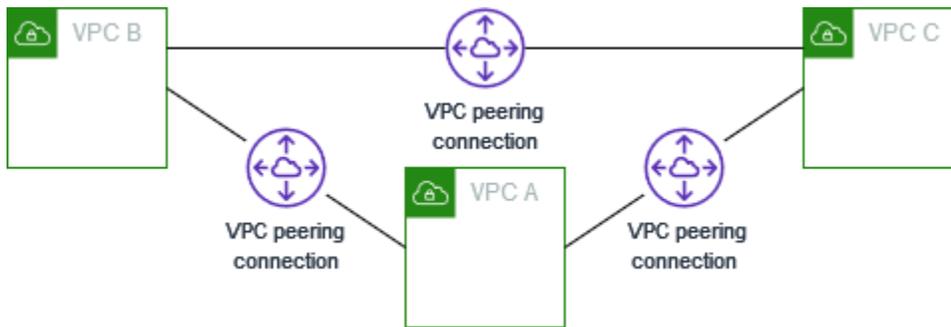
Tabela de rotas	Destino	Destino
	<i>CIDR IPv4 da VPC D</i>	pcx-aaaadddd
	<i>CIDR IPv6 da VPC D</i>	pcx-aaaadddd
	<i>CIDR IPv4 da VPC E</i>	pcx-aaaaeeee
	<i>CIDR IPv6 da VPC E</i>	pcx-aaaaeeee
	<i>CIDR IPv4 da VPC F</i>	pcx-aaaaffff
	<i>CIDR IPv6 da VPC F</i>	pcx-aaaaffff
	<i>CIDR IPv4 da VPC G</i>	pcx-aaaagggg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

Tabela de rotas	Destino	Destino
VPC E	<i>CIDR IPv4 da VPC E</i>	Local
	<i>CIDR IPv6 da VPC E</i>	Local
	<i>CIDR IPv4 da VPC A</i>	pcx-aaaaeeee
	<i>CIDR IPv6 da VPC A</i>	pcx-aaaaeeee
VPC F	<i>CIDR IPv4 da VPC F</i>	Local
	<i>CIDR IPv6 da VPC F</i>	Local
	<i>CIDR IPv4 da VPC A</i>	pcx-aaaaffff
	<i>CIDR IPv6 da VPC A</i>	pcx-aaaaffff
VPC G	<i>CIDR IPv4 da VPC G</i>	Local
	<i>CIDR IPv6 da VPC G</i>	Local
	<i>CIDR IPv4 da VPC A</i>	pcx-aaaagggg
	<i>CIDR IPv6 da VPC A</i>	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	<i>CIDR da VPC A</i>	Local
	<i>CIDR da VPC B</i>	pcx-aaaabbbb
	<i>CIDR da VPC C</i>	pcx-aaaacccc
VPC B	<i>CIDR da VPC B</i>	Local
	<i>CIDR da VPC A</i>	pcx-aaaabbbb
	<i>CIDR da VPC C</i>	pcx-bbbbcccc
VPC C	<i>CIDR da VPC C</i>	Local
	<i>CIDR da VPC A</i>	pcx-aaaacccc
	<i>CIDR da VPC B</i>	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	<i>CIDR IPv4 da VPC A</i>	Local
	<i>CIDR IPv6 da VPC A</i>	Local
	<i>CIDR IPv4 da VPC B</i>	pcx-aaaabbbb
	<i>CIDR IPv6 da VPC B</i>	pcx-aaaabbbb
	<i>CIDR IPv4 da VPC C</i>	pcx-aaaacccc
VPC B	<i>CIDR IPv4 da VPC B</i>	Local
	<i>CIDR IPv6 da VPC B</i>	Local
	<i>CIDR IPv4 da VPC A</i>	pcx-aaaabbbb
	<i>CIDR IPv6 da VPC A</i>	pcx-aaaabbbb
	<i>CIDR IPv4 da VPC C</i>	pcx-bbbbcccc
VPC C	<i>CIDR IPv4 da VPC C</i>	Local
	<i>CIDR IPv4 da VPC A</i>	pcx-aaaacccc
	<i>CIDR IPv4 da VPC B</i>	pcx-bbbbcccc

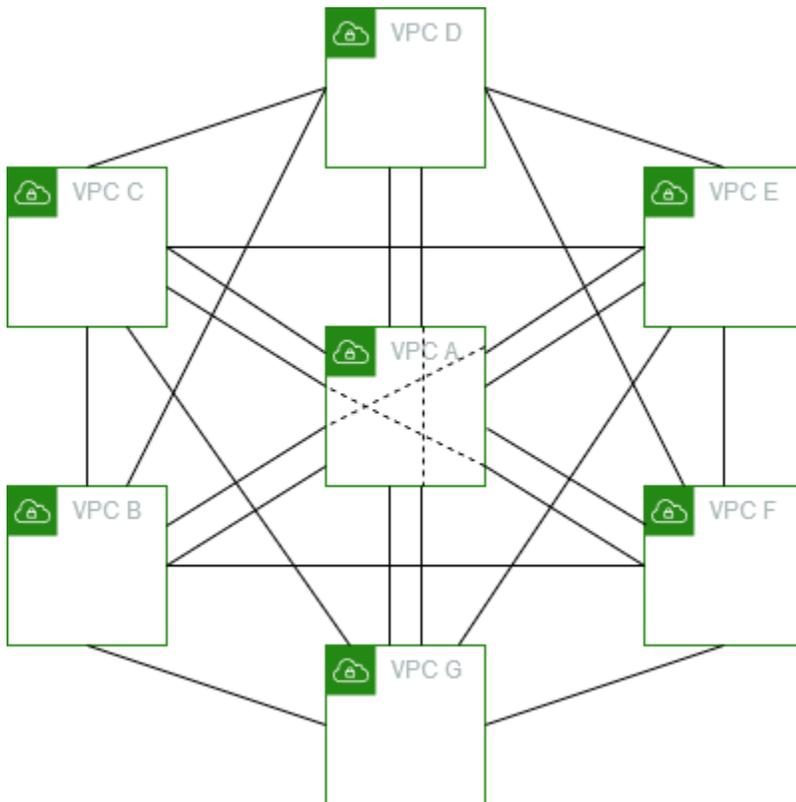
Várias VPCs emparelhadas

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-aaaaeaaa
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	<i>CIDR da VPC A</i>	Local
	<i>CIDR da VPC B</i>	pcx-aaaabbbb
	<i>CIDR da VPC C</i>	pcx-aaaacccc
	<i>CIDR da VPC D</i>	pcx-aaaadddd
	<i>CIDR da VPC E</i>	pcx-aaaaeeee
	<i>CIDR da VPC F</i>	pcx-aaaaffff
	<i>CIDR da VPC G</i>	pcx-aaaagggg
VPC B	<i>CIDR da VPC B</i>	Local
	<i>CIDR da VPC A</i>	pcx-aaaabbbb

Tabela de rotas	Destino	Destino
	<i>CIDR da VPC C</i>	pcx-bbbbcccc
	<i>CIDR da VPC D</i>	pcx-bbbbdddd
	<i>CIDR da VPC E</i>	pcx-bbbbceeee
	<i>CIDR da VPC F</i>	pcx-bbbbffff
	<i>CIDR da VPC G</i>	pcx-bbbbgggg
VPC C	<i>CIDR da VPC C</i>	Local
	<i>CIDR da VPC A</i>	pcx-aaaacccc
	<i>CIDR da VPC B</i>	pcx-bbbbcccc
	<i>CIDR da VPC D</i>	pcx-ccccdddd
	<i>CIDR da VPC E</i>	pcx-cccceeee
	<i>CIDR da VPC F</i>	pcx-ccccffff
	<i>CIDR da VPC G</i>	pcx-ccccgggg
VPC D	<i>CIDR da VPC D</i>	Local
	<i>CIDR da VPC A</i>	pcx-aaaadddd
	<i>CIDR da VPC B</i>	pcx-bbbbdddd
	<i>CIDR da VPC C</i>	pcx-ccccdddd
	<i>CIDR da VPC E</i>	pcx-ddddeeee
	<i>CIDR da VPC F</i>	pcx-ddddffff
	<i>CIDR da VPC G</i>	pcx-ddddgggg
VPC E	<i>CIDR da VPC E</i>	Local

Tabela de rotas	Destino	Destino
	<i>CIDR da VPC A</i>	pcx-aaaaeeee
	<i>CIDR da VPC B</i>	pcx-bbbbeeee
	<i>CIDR da VPC C</i>	pcx-cccceeee
	<i>CIDR da VPC D</i>	pcx-ddddeeee
	<i>CIDR da VPC F</i>	pcx-eeeeffff
	<i>CIDR da VPC G</i>	pcx-eeeegggg
VPC F	<i>CIDR da VPC F</i>	Local
	<i>CIDR da VPC A</i>	pcx-aaaaffff
	<i>CIDR da VPC B</i>	pcx-bbbbffff
	<i>CIDR da VPC C</i>	pcx-ccccffff
	<i>CIDR da VPC D</i>	pcx-ddddffff
	<i>CIDR da VPC E</i>	pcx-eeeeffff
	<i>CIDR da VPC G</i>	pcx-ffffgggg
VPC G	<i>CIDR da VPC G</i>	Local
	<i>CIDR da VPC A</i>	pcx-aaaagggg
	<i>CIDR da VPC B</i>	pcx-bbbbgggg
	<i>CIDR da VPC C</i>	pcx-ccccgggg
	<i>CIDR da VPC D</i>	pcx-ddddgggg
	<i>CIDR da VPC E</i>	pcx-eeeegggg
	<i>CIDR da VPC F</i>	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	<i>CIDR IPv4 da VPC A</i>	Local
	<i>CIDR IPv6 da VPC A</i>	Local
	<i>CIDR IPv4 da VPC B</i>	pcx-aaaabbbb
	<i>CIDR IPv6 da VPC B</i>	pcx-aaaabbbb
	<i>CIDR IPv4 da VPC C</i>	pcx-aaaacccc
	<i>CIDR IPv6 da VPC C</i>	pcx-aaaacccc
	<i>CIDR IPv4 da VPC D</i>	pcx-aaaadddd
	<i>CIDR IPv6 da VPC D</i>	pcx-aaaadddd
	<i>CIDR IPv4 da VPC E</i>	pcx-aaaaeeee
	<i>CIDR IPv6 da VPC E</i>	pcx-aaaaeeee
	<i>CIDR IPv4 da VPC F</i>	pcx-aaaaffff
	<i>CIDR IPv6 da VPC F</i>	pcx-aaaaffff
	<i>CIDR IPv4 da VPC G</i>	pcx-aaaagggg
	<i>CIDR IPv6 da VPC G</i>	pcx-aaaagggg
VPC B	<i>CIDR IPv4 da VPC B</i>	Local
	<i>CIDR IPv6 da VPC B</i>	Local
	<i>CIDR IPv4 da VPC A</i>	pcx-aaaabbbb
	<i>CIDR IPv6 da VPC A</i>	pcx-aaaabbbb
	<i>CIDR IPv4 da VPC C</i>	pcx-bbbbcccc

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

Tabela de rotas	Destino	Destino
	<i>CIDR IPv6 da VPC F</i>	pcx-ccccffff
	<i>CIDR IPv4 da VPC G</i>	pcx-ccccgggg
	<i>CIDR IPv6 da VPC G</i>	pcx-ccccgggg
VPC D	<i>CIDR IPv4 da VPC D</i>	Local
	<i>CIDR IPv6 da VPC D</i>	Local
	<i>CIDR IPv4 da VPC A</i>	pcx-aaaadddd
	<i>CIDR IPv6 da VPC A</i>	pcx-aaaadddd
	<i>CIDR IPv4 da VPC B</i>	pcx-bbbbddd
	<i>CIDR IPv6 da VPC B</i>	pcx-bbbbddd
	<i>CIDR IPv4 da VPC C</i>	pcx-ccccddd
	<i>CIDR IPv6 da VPC C</i>	pcx-ccccddd
	<i>CIDR IPv4 da VPC E</i>	pcx-ddddeeee
	<i>CIDR IPv6 da VPC E</i>	pcx-ddddeeee
	<i>CIDR IPv4 da VPC F</i>	pcx-ddddffff
	<i>CIDR IPv6 da VPC F</i>	pcx-ddddffff
	<i>CIDR IPv4 da VPC G</i>	pcx-ddddgggg
	<i>CIDR IPv6 da VPC G</i>	pcx-ddddgggg
VPC E	<i>CIDR IPv4 da VPC E</i>	Local
	<i>CIDR IPv6 da VPC E</i>	Local
	<i>CIDR IPv4 da VPC A</i>	pcx-aaaaeeee

Tabela de rotas	Destino	Destino
	<i>CIDR IPv6 da VPC A</i>	pcx-aaaaeefe
	<i>CIDR IPv4 da VPC B</i>	pcx-bbbbeefe
	<i>CIDR IPv6 da VPC B</i>	pcx-bbbbeefe
	<i>CIDR IPv4 da VPC C</i>	pcx-cccceefe
	<i>CIDR IPv6 da VPC C</i>	pcx-cccceefe
	<i>CIDR IPv4 da VPC D</i>	pcx-ddddeefe
	<i>CIDR IPv6 da VPC D</i>	pcx-ddddeefe
	<i>CIDR IPv4 da VPC F</i>	pcx-eeeeffff
	<i>CIDR IPv6 da VPC F</i>	pcx-eeeeffff
	<i>CIDR IPv4 da VPC G</i>	pcx-eeeegggg
	<i>CIDR IPv6 da VPC G</i>	pcx-eeeegggg
VPC F	<i>CIDR IPv4 da VPC F</i>	Local
	<i>CIDR IPv6 da VPC F</i>	Local
	<i>CIDR IPv4 da VPC A</i>	pcx-aaaaffff
	<i>CIDR IPv6 da VPC A</i>	pcx-aaaaffff
	<i>CIDR IPv4 da VPC B</i>	pcx-bbbbffff
	<i>CIDR IPv6 da VPC B</i>	pcx-bbbbffff
	<i>CIDR IPv4 da VPC C</i>	pcx-ccccffff
	<i>CIDR IPv6 da VPC C</i>	pcx-ccccffff
	<i>CIDR IPv4 da VPC D</i>	pcx-ddddffff

Tabela de rotas	Destino	Destino
	<i>CIDR IPv6 da VPC D</i>	pcx-ddddffff
	<i>CIDR IPv4 da VPC E</i>	pcx-eeeeffff
	<i>CIDR IPv6 da VPC E</i>	pcx-eeeeffff
	<i>CIDR IPv4 da VPC G</i>	pcx-ffffgggg
	<i>CIDR IPv6 da VPC G</i>	pcx-ffffgggg
VPC G	<i>CIDR IPv4 da VPC G</i>	Local
	<i>CIDR IPv6 da VPC G</i>	Local
	<i>CIDR IPv4 da VPC A</i>	pcx-aaaagggg
	<i>CIDR IPv6 da VPC A</i>	pcx-aaaagggg
	<i>CIDR IPv4 da VPC B</i>	pcx-bbbbgggg
	<i>CIDR IPv6 da VPC B</i>	pcx-bbbbgggg
	<i>CIDR IPv4 da VPC C</i>	pcx-ccccgggg
	<i>CIDR IPv6 da VPC C</i>	pcx-ccccgggg
	<i>CIDR IPv4 da VPC D</i>	pcx-ddddgggg
	<i>CIDR IPv6 da VPC D</i>	pcx-ddddgggg
	<i>CIDR IPv4 da VPC E</i>	pcx-eeeegggg
	<i>CIDR IPv6 da VPC E</i>	pcx-eeeegggg
	<i>CIDR IPv4 da VPC F</i>	pcx-ffffgggg
	<i>CIDR IPv6 da VPC F</i>	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.

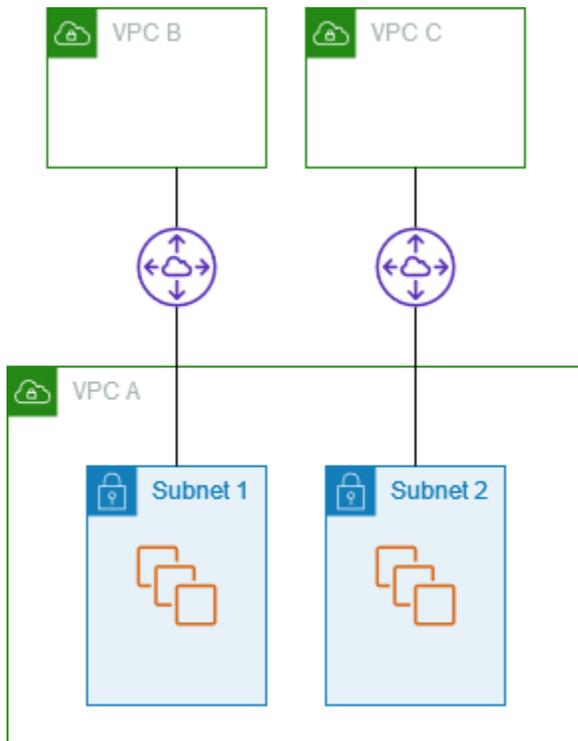
Para exemplos de cenários nos quais você possa precisar de uma configuração de conexão de emparelhamento de VPC específica, consulte [Cenários de emparelhamento de VPC](#). Para obter mais informações sobre como trabalhar com conexões de emparelhamento de VPC, consulte [Trabalhar com conexões de emparelhamento 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	Destino
Sub-rede 1 (VPC A)	<i>CIDR da VPC A</i>	Local
	<i>CIDR da VPC B</i>	<code>pcx-aaaabbbb</code>
Sub-rede 2 (VPC A)	<i>CIDR da VPC A</i>	Local
	<i>CIDR da VPC C</i>	<code>pcx-aaaacccc</code>
VPC B	<i>CIDR da VPC B</i>	Local
	<i>CIDR da sub-rede 1</i>	<code>pcx-aaaabbbb</code>
VPC C	<i>CIDR da VPC C</i>	Local

Tabela de rotas	Destino	Destino
	<i>CIDR da sub-rede 2</i>	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	<i>CIDR IPv4 da VPC A</i>	Local	
	<i>CIDR IPv6 da VPC A</i>	Local	Rota local que é adicionada automaticamente para comunicação IPv6 na VPC.
	<i>CIDR IPv4 da VPC B</i>	pcx-aaaabbbb	
	<i>CIDR IPv6 da VPC B</i>	pcx-aaaabbbb	Rota para o bloco CIDR IPv6 da VPC B.
Sub-rede 2 na VPC A	<i>CIDR IPv4 da VPC A</i>	Local	
	<i>CIDR IPv6 da VPC A</i>	Local	Rota local que é adicionada automaticamente para comunicação IPv6 na VPC.

Tabela de rotas	Destino	Destino	Observações
	<i>CIDR IPv4 da VPC C</i>	pcx-aaaacccc	
VPC B	<i>CIDR IPv4 da VPC B</i>	Local	
	<i>CIDR IPv6 da VPC B</i>	Local	Rota local que é adicionada automaticamente para comunicação IPv6 na VPC.
	<i>CIDR IPv4 da sub-rede 1</i>	pcx-aaaabbbb	
	<i>CIDR IPv4 da sub-rede 2</i>	pcx-aaaabbbb	Rota para o bloco CIDR IPv6 da VPC A.
VPC C	<i>CIDR IPv4 da VPC C</i>	Local	
	<i>CIDR IPv4 da sub-rede 2</i>	pcx-aaaacccc	

Duas VPCs que acessam blocos CIDR específicos em uma VPC

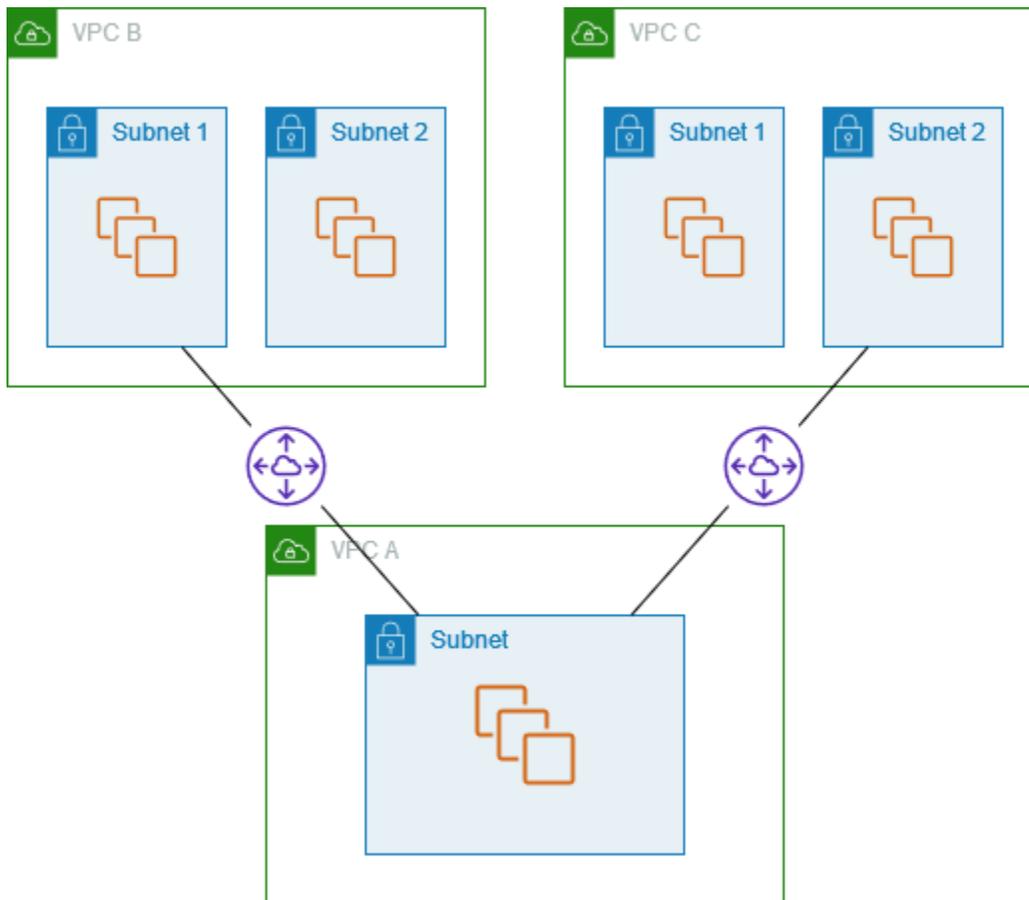
Nessa configuração, há uma VPC central (VPC A), uma conexão de emparelhamento entre a VPC A e a VPC B (pcx-aaaabbbb) e uma conexão de emparelhamento entre a VPC A e a VPC C (pcx-aaaacccc). A VPC A tem um bloco CIDR para cada conexão de emparelhamento.

Tabela de rotas	Destino	Destino
VPC A	<i>CIDR 1 da VPC A</i>	Local
	<i>CIDR 2 da VPC A</i>	Local

Tabela de rotas	Destino	Destino
	<i>CIDR da VPC B</i>	pcx-aaaabbbb
	<i>CIDR da VPC C</i>	pcx-aaaacccc
VPC B	<i>CIDR da VPC B</i>	Local
	<i>CIDR 1 da VPC A</i>	pcx-aaaabbbb
VPC C	<i>CIDR da VPC C</i>	Local
	<i>CIDR 2 da VPC A</i>	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	Destino
VPC A	<i>CIDR da VPC A</i>	Local
	<i>CIDR da sub-rede 1</i>	pcx-aaaabbbb
	<i>CIDR da sub-rede 2</i>	pcx-aaaacccc
Sub-rede 1 (VPC B)	<i>CIDR da VPC B</i>	Local

Tabela de rotas	Destino	Destino
	<i>Sub-rede no CIDR da VPC A</i>	pcx-aaaabbbb
Sub-rede 2 (VPC C)	<i>CIDR da VPC C</i>	Local
	<i>Sub-rede no CIDR da VPC A</i>	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-aaaacccc.

Tabela de rotas	Destino	Destino
Sub-rede 2 (VPC B)	<i>CIDR da VPC B</i>	Local
	<i>Sub-rede no CIDR da VPC A</i>	pcx-aaaabbbb
VPC A	<i>CIDR da VPC A</i>	Local
	<i>CIDR da VPC C</i>	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 B na VPC B e com a sub-rede A na VPC C. Esse cenário é 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.

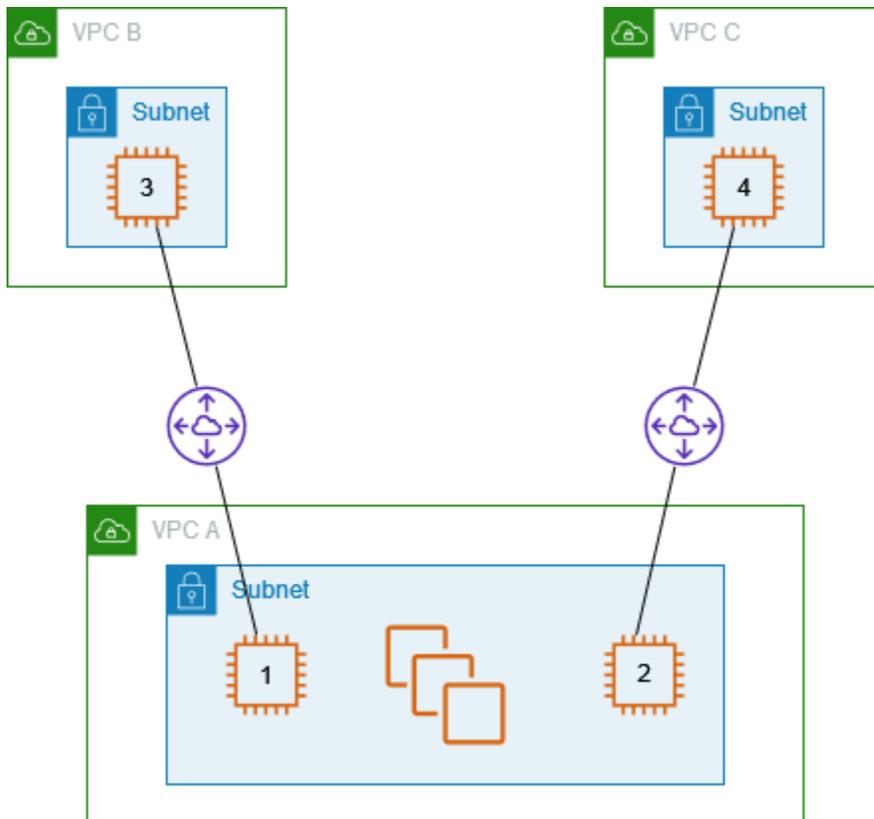
Destination (Destino)	Destino
<i>CIDR da VPC A</i>	Local
<i>CIDR da sub-rede 2</i>	<code>pcx-aaaabbbb</code>
<i>CIDR da sub-rede 1</i>	<code>pcx-aaaacccc</code>

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):

Destination (Destino)	Destino
<i>CIDR da VPC A</i>	Local
<i>Endereço IP específico na sub-rede 2</i>	<code>pcx-aaaabbbb</code>
<i>CIDR da VPC B</i>	<code>pcx-aaaacccc</code>

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.



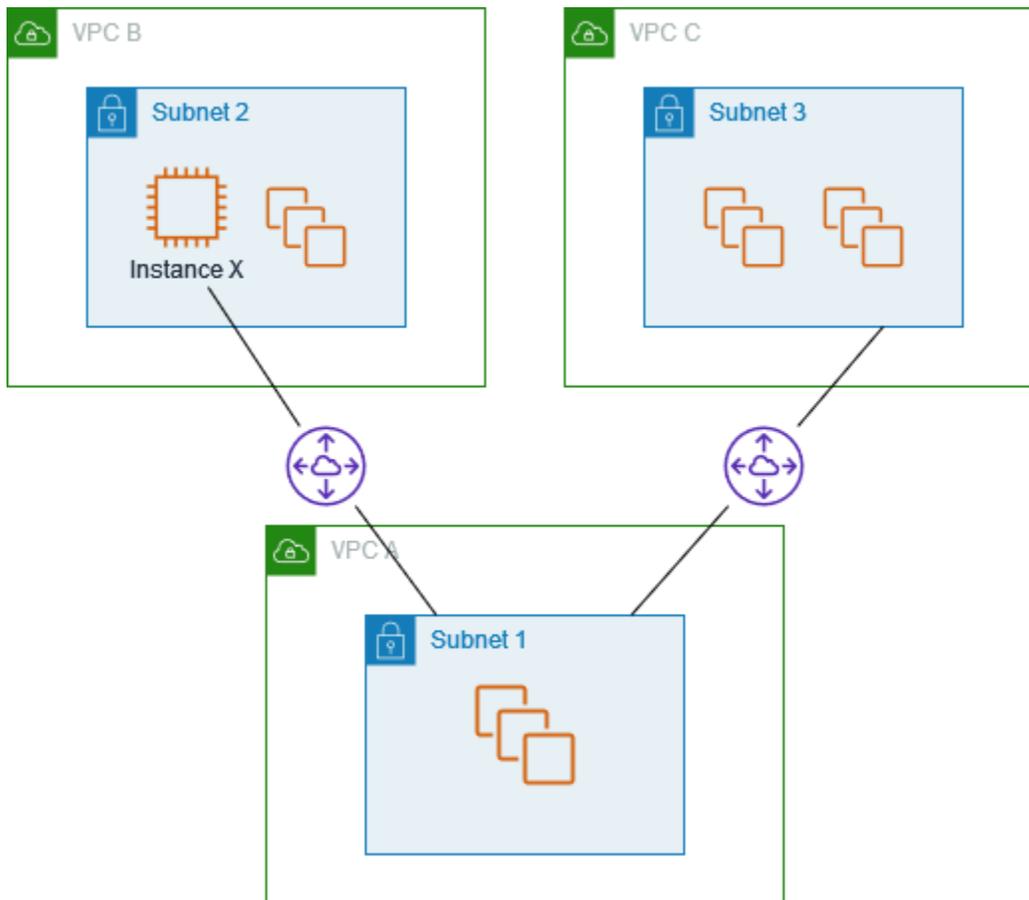
Cada tabela de rota VPC aponta para a conexão de emparelhamento de VPC relevante para acessar um único endereço IP (e, portanto, uma instância específica) na VPC de mesmo nível.

Tabela de rotas	Destino	Destino
VPC A	<i>CIDR da VPC A</i>	Local
	<i>Endereço IP da instância 3</i>	pcx-aaaabbbb

Tabela de rotas	Destino	Destino
	<i>Endereço IP da instância 4</i>	pcx-aaaacccc
VPC B	<i>CIDR da VPC B</i>	Local
	<i>Endereço IP da instância 1</i>	pcx-aaaabbbb
VPC C	<i>CIDR da VPC C</i>	Local
	<i>Endereço IP da instância 2</i>	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	Destino
VPC A	<i>Bloco CIDR da VPC A</i>	Local
	<i>Endereço IP da instância X</i>	<code>pcx-aaaabbbb</code>
	<i>Bloco CIDR da VPC C</i>	<code>pcx-aaaacccc</code>
VPC B	<i>Bloco CIDR da VPC B</i>	Local
	<i>Bloco CIDR da VPC A</i>	<code>pcx-aaaabbbb</code>

Tabela de rotas	Destino	Destino
VPC C	<i>Bloco CIDR da VPC C</i>	Local
	<i>Bloco CIDR da VPC A</i>	pcx-aaaacccc

Important

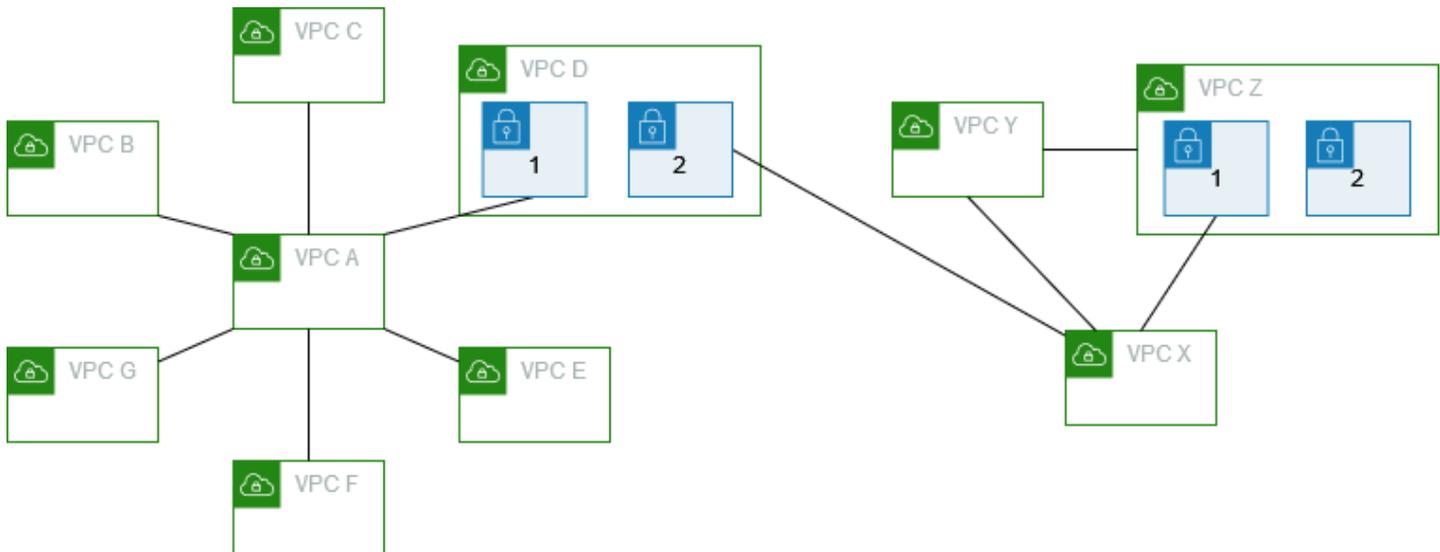
Se uma instância diferente da instância X na VPC B envia tráfego para a VPC A, o tráfego de resposta pode ser roteado para a VPC C em vez de para a VPC B. Para obter mais informações, consulte [Rota para tráfego de resposta](#).

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	Destino
VPC A	<i>CIDR da VPC A</i>	Local
	<i>CIDR da VPC B</i>	pcx-aaaabbbb
	<i>CIDR da VPC C</i>	pcx-aaaacccc
	<i>CIDR da sub-rede 1 na VPC D</i>	pcx-aaaadddd

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

Tabela de rotas	Destino	Destino
	<i>CIDR da sub-rede 1 na VPC Z</i>	pcx-xxxxzzzz
VPC Y	<i>CIDR da VPC Y</i>	Local
	<i>CIDR da VPC X</i>	pcx-xxxxyyyy
	<i>CIDR da VPC Z</i>	pcx-yyyyzzzz
VPC Z	<i>CIDR da VPC Z</i>	Local
	<i>CIDR da VPC Y</i>	pcx-yyyyzzzz
	<i>CIDR da VPC X</i>	pcx-xxxxzzzz

Cenários de emparelhamento de 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 [Trabalhar com 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 [Trabalhar com 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

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.

Nome	Padrão	Ajustável
Conexões emparelhadas de VPC ativas por VPC	50	Sim (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 cotas adicionais da Amazon VPC, consulte [Amazon VPC quotas](#) (Cotas da Amazon VPC) no Amazon VPC User Guide (Guia 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