AWS PrivateLink

Amazon Virtual Private Cloud

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Virtual Private Cloud: AWS PrivateLink

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens de marcas 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 os 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

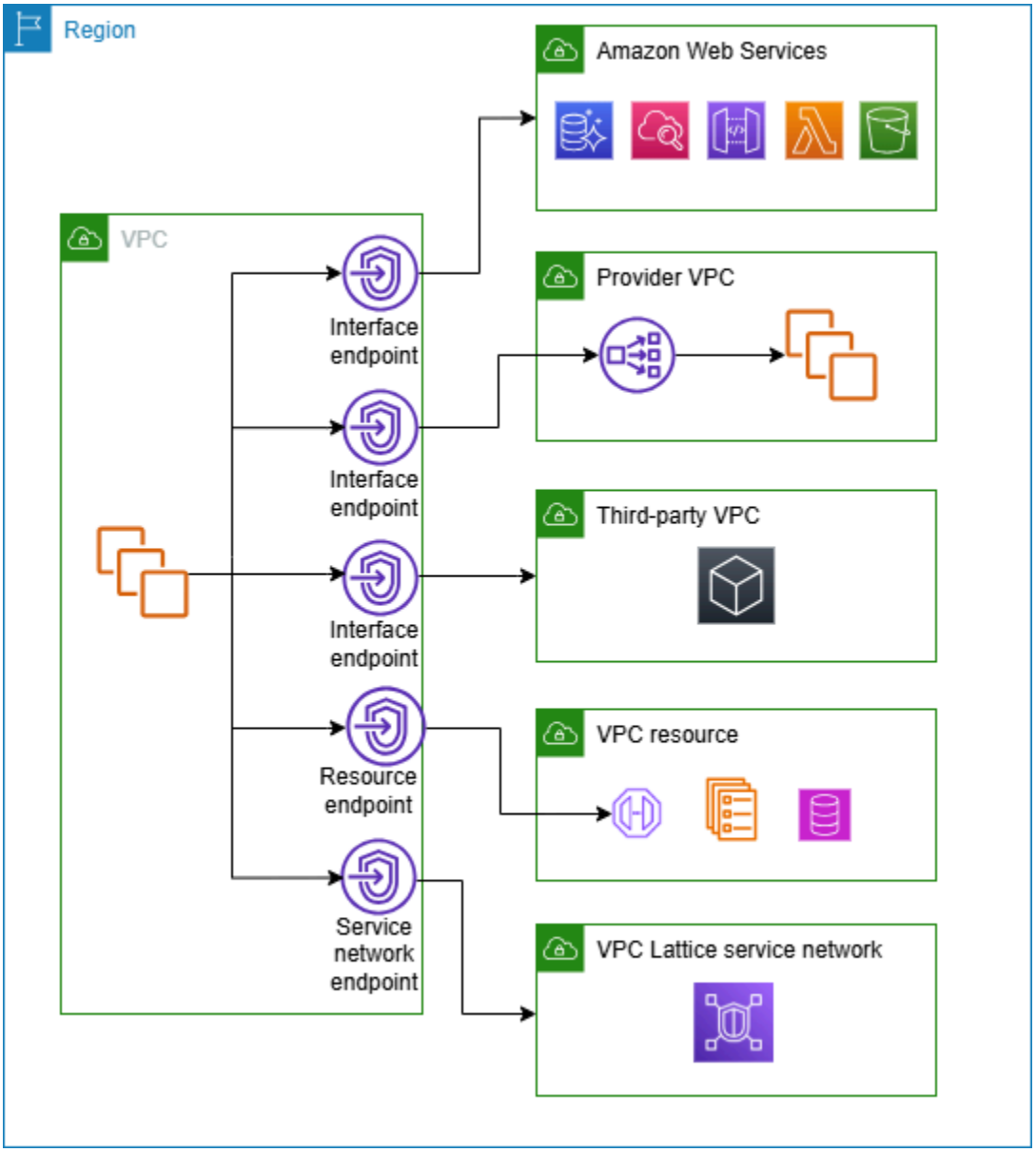
O que é AWS PrivateLink?

AWS PrivateLink é uma tecnologia altamente disponível e escalável que você pode usar para conectar de forma privada sua VPC a serviços e recursos como se estivessem em sua VPC. Você não precisa usar um gateway de internet, dispositivo NAT, endereço IP público, conexão ou Direct Connect AWS Site-to-Site VPN conexão para permitir a comunicação com o serviço ou recurso a partir de suas sub-redes privadas. Assim, você controla os endpoints de API, os sites, os serviços e os recursos específicos que sua VPC pode alcançar.

Casos de uso

Você pode criar endpoints de VPC para conectar clientes em sua VPC a serviços e recursos que se integram com o. AWS PrivateLink Você pode criar seu próprio serviço de VPC endpoint e disponibilizá-lo para outros clientes. AWS Para obter mais informações, consulte the section called “Conceitos”.

No diagrama a seguir, a VPC da esquerda tem várias instâncias do Amazon EC2 em uma sub-rede privada e cinco endpoints da VPC: três endpoints da VCP de interface e um endpoint da VPC de rede de serviço. O primeiro endpoint da VPC de interface se conecta a um serviço da AWS . O segundo endpoint da VPC de interface se conecta a um serviço hospedado por outra conta da AWS (um serviço de endpoint da VPC). O terceiro endpoint da VPC de interface se conecta a um serviço de parceiro do AWS Marketplace. O endpoint da VPC de recurso se conecta a um banco de dados. O endpoint da VPC de rede de serviço se conecta a uma rede de serviço.



Saiba mais

- Conceitos
- Acessar Serviços da AWS
- Acessar produtos SaaS
- Acessar dispositivos virtuais
- Compartilhar serviços

Trabalhar com VPC endpoints

Você pode criar, acessar e gerenciar VPC endpoints de qualquer um das seguintes formas:

- Console de gerenciamento da AWS— Fornece uma interface web que você pode usar para acessar seus AWS PrivateLink recursos. Abra o console da Amazon VPC e escolha Endpoints ou serviços de Endpoint.
- AWS Command Line Interface (AWS CLI) — Fornece comandos para um amplo conjunto de Serviços da AWS, incluindo AWS PrivateLink. Para obter mais informações sobre comandos para AWS PrivateLink, consulte ec2 na Referência de AWS CLI comandos.
- CloudFormation: crie modelos que descrevam seus recursos da AWS . Você usa os modelos para provisionar e gerenciar esses recursos como uma só unidade. Para mais informações, consulte os seguintes recursos do AWS PrivateLink :
  - AWS::EC2::VPCEndpoint
  - AWS: :EC2:: VPCEndpointConnectionNotification
  - AWS: :EC2:: VPCEndpointService
  - AWS: :EC2:: VPCEndpointServicePermissions
  - AWS::ElasticLoadBalancingV2: LoadBalancer
- AWS SDKs — forneça APIs específicas para cada idioma. Os SDKs cuidam de muitos dos detalhes da conexão, como calcular assinaturas, lidar com tentativas de solicitação e lidar com erros. Para obter mais informações, consulte Ferramentas para criar na AWS.
- API de consulta: fornece ações de API de baixo nível que são chamadas usando solicitações HTTPS. Usar a API de consulta é a maneira mais direta de acessar a Amazon VPC. No entanto, ela exige que o aplicativo trate detalhes de baixo nível, como gerar o hash para assinar a solicitação e tratar erros. Para obter mais informações, consulte Ações de AWS PrivateLink na Referência de API do Amazon EC2.

Preços

Para obter informações sobre preços de endpoints da VPC, consulte Definição de preço do AWS PrivateLink.

AWS PrivateLink conceitos

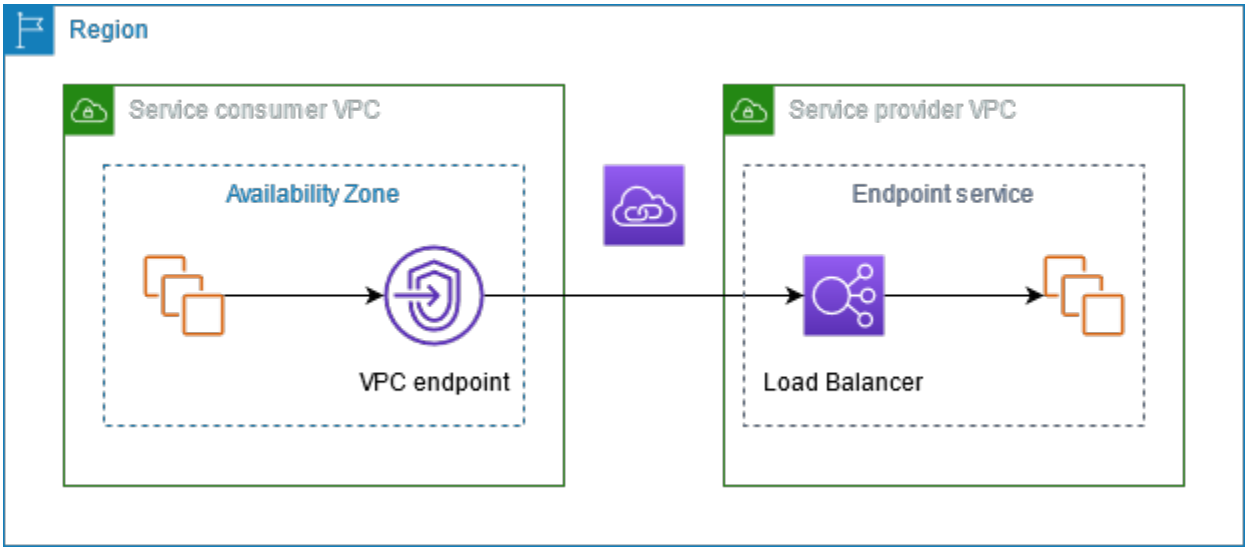
É possível usar a Amazon VPC para definir uma nuvem privada virtual (VPC), que é uma rede virtual isolada logicamente. Você pode permitir que os clientes em sua VPC se conectem a destinos fora dela. Por exemplo, adicione um gateway da internet à VPC para permitir o acesso à internet ou adicione uma conexão de VPN para permitir o acesso à rede on-premises. Como alternativa, use AWS PrivateLink para permitir que os clientes em sua VPC se conectem a serviços e recursos em outras VPCs usando endereços IP privados, como se esses serviços e recursos estivessem hospedados diretamente em sua VPC.

Veja a seguir conceitos importantes que você deve entender ao começar a usar o AWS PrivateLink.

Conteúdo

Diagrama de arquitetura

O diagrama a seguir fornece uma visão geral de alto nível de como AWS PrivateLink funciona. Os consumidores criam endpoints da VPC para se conectarem a serviços e recursos de endpoint hospedados por provedores.



Provedores

Entenda os conceitos relacionados a um provedor.

Provedor de serviço

O proprietário de um serviço é o provedor de serviços. Os provedores de serviços incluem AWS AWS parceiros e outros Contas da AWS. Os provedores de serviços podem hospedar seus serviços usando AWS recursos, como instâncias do EC2, ou usando servidores locais.

Provedor de recurso

O proprietário de um recurso, por exemplo, um banco de dados ou uma instância do Amazon EC2, é o provedor do recurso. Os provedores de recursos incluem AWS serviços, AWS parceiros e outras AWS contas. Os provedores de recursos podem hospedar os recursos em VPCs ou redes on-premises.

Conceitos

- Serviços de endpoint
- Nomes de serviço
- Estados do serviço
- Configuração de recursos
- Gateway de recursos

Serviços de endpoint

Um provedor de serviços cria um serviço de endpoint para disponibilizar seu serviço em uma região. Um provedor de serviços deve especificar um balanceador de carga ao criar um serviço de endpoint. O balanceador de carga recebe solicitações de consumidores do serviço e as encaminha ao serviço.

Por padrão, o serviço de endpoint não está disponível aos consumidores do serviço. Você deve adicionar permissões que permitam que AWS entidades específicas se conectem ao seu serviço de endpoint.

Nomes de serviço

Cada serviço de endpoint é identificado por um nome de serviço. O consumidor do serviço deve especificar o nome do serviço ao criar um endpoint da VPC. Os consumidores de serviços podem

consultar os nomes dos serviços Serviços da AWS. Os provedores de serviços devem compartilhar os nomes de seus serviços com os consumidores.

Estados do serviço

Estes são estados possíveis para um serviço de endpoint:

- Pendente: o serviço de endpoint está sendo criado.
- Disponível: o serviço de endpoint está disponível.
- Com falha: não foi possível criar o serviço de endpoint.
- Excluindo: o provedor do serviço excluiu o serviço de endpoint e a exclusão está em andamento.
- Excluído: o serviço de endpoint foi excluído.

Configuração de recursos

O provedor do recurso cria uma configuração de recurso para compartilhar um recurso. Uma configuração de recurso é um objeto lógico que representa um único recurso, como um banco de dados, ou um grupo de recursos. Um recurso pode ser um endereço IP, um destino de nome de domínio ou um banco de dados do Amazon Relational Database Service (Amazon RDS).

Ao compartilhar com outras contas, o provedor de recursos deve compartilhar o recurso por meio de um compartilhamento de recursos AWS Resource Access Manager(AWS RAM) para permitir que AWS diretores específicos na outra conta se conectem ao recurso por meio de um endpoint VPC de recursos.

As configurações de recursos podem ser associadas a uma rede de serviço à qual as entidades principais se conectam por um endpoint da VPC de rede de serviço.

Gateway de recursos

Um gateway de recursos é um ponto de entrada de uma VPC da qual um recurso está sendo compartilhado. O provedor cria um gateway de recursos para compartilhar recursos da VPC.

Consumidores de serviços ou recursos

O usuário de um serviço ou recurso é um consumidor. Os consumidores podem acessar serviços e recursos de endpoint de suas VPCs ou redes on-premises.

Conceitos

- Endpoints da VPC
- Interfaces de rede de endpoint
- Políticas de endpoint
- Estados do endpoint

Endpoints da VPC

O consumidor cria um endpoint da VPC para conectar sua VPC a um serviço ou recurso de endpoint. O consumidor deve especificar o serviço, o recurso ou a rede de serviço de endpoint ao criar um endpoint da VPC. Há vários tipos de endpoints da VPC. Você deve criar o tipo de endpoint da VPC de que precisa.

- `Interface`: crie um endpoint de interface para enviar tráfego TCP para um serviço de endpoint. O tráfego destinado ao serviço de endpoint é resolvido usando DNS.
- `GatewayLoadBalancer`: crie um endpoint do Gateway Load Balancer para enviar tráfego a uma frota de dispositivos virtuais usando endereços IP privados. Encaminhe o tráfego da VPC ao endpoint do Gateway Load Balancer usando tabelas de rotas. O Gateway Load Balancer distribui o tráfego aos dispositivos virtuais e pode ser escalado conforme a demanda.
- `Resource`: crie um endpoint de recurso para acessar um recurso que foi compartilhado com você e que reside em outra VPC. Um endpoint de recurso permite que você acesse, privadamente e em segurança, recursos como um banco de dados, uma instância do Amazon EC2, um endpoint de aplicação, um destino de nome de domínio ou um endereço IP que pode estar em uma sub-rede privada em outra VPC ou no local. Os endpoints de recursos não exigem um balanceador de carga e permitem que você acesse o recurso diretamente.
- `Service network`: crie um endpoint de rede de serviço para acessar uma rede de serviço que criou ou que foi compartilhada com você. Você pode usar um único endpoint de rede de serviço para acessar, privadamente e em segurança, vários recursos e serviços associados a uma rede de serviço.

Há outro tipo de endpoint da VPC, o `Gateway`, que cria um endpoint de gateway para enviar tráfego ao Amazon S3 ou ao DynamoDB. Os endpoints de gateway não são usados AWS PrivateLink, ao contrário dos outros tipos de endpoints de VPC. Para obter mais informações, consulte the section called “Endpoints de gateway”.

Interfaces de rede de endpoint

Uma interface de rede de endpoint é uma interface de rede gerenciada pelo solicitante que serve como ponto de entrada para o tráfego destinado a um serviço, um recurso ou uma rede de serviço de endpoint. Para cada sub-rede que você especifica ao criar um endpoint da VPC, nós criamos uma interface de rede de endpoint na sub-rede.

Se um endpoint da VPC for compatível com IPv4, suas interfaces de rede de endpoint terão endereços IPv4. Se um endpoint da VPC for compatível com IPv6, suas interfaces de rede de endpoint terão endereços IPv6. Não é possível acessar o endereço IPv6 de uma interface de rede de endpoint pela Internet. Ao descrever um endpoint de interface de rede com um endereço IPv6, observe que `denyAllIgwTraffic` está habilitado.

Políticas de endpoint

Uma política de endpoint da VPC é uma política de recursos do IAM que você anexa a um endpoint da VPC. Ele determina quais entidades principais poderão usar o endpoint da VPC para acessar o serviço de endpoint. A política padrão de endpoint da VPC permite todas as ações realizadas por todas as entidades principais em todos os recursos sobre o endpoint da VPC.

Estados do endpoint

Quando você cria um endpoint da VPC de interface, o serviço de endpoint recebe uma solicitação de conexão. O provedor de serviços pode aceitar ou rejeitar a solicitação. Se o provedor do serviço aceitar a solicitação, o consumidor do serviço poderá usar o endpoint da VPC quando ele entrar no estado Disponível.

Estes são os estados possíveis para um endpoint da VPC:

- PendingAcceptance - A solicitação de conexão está pendente. Esse será o estado inicial se as solicitações forem aceitas manualmente.
- Pendente: o provedor do serviço aceitou a solicitação de conexão. Esse será o estado inicial se as solicitações forem aceitas automaticamente. O endpoint da VPC retornará a esse estado se o consumidor do serviço modificar o endpoint da VPC.
- Disponível: o endpoint da VPC está disponível para uso.
- Rejeitado: o provedor do serviço rejeitou a solicitação de conexão. O provedor de serviços também poderá rejeitar uma conexão depois que ela estiver disponível para uso.
- Expirado: a solicitação de conexão expirou.

- Com falha: não foi possível disponibilizar o endpoint da VPC.
- Excluindo: o consumidor do serviço excluiu o endpoint da VPC, e a exclusão está em andamento.
- Excluído: o endpoint da VPC foi excluído.

A AWS PrivateLink API retorna os estados possíveis usando camel case.

AWS PrivateLink conexões

O tráfego de sua VPC é enviado para um serviço ou recurso de endpoint usando uma conexão entre o endpoint da VPC e o serviço ou recuso de endpoint. O tráfego entre um endpoint da VPC e um serviço ou recurso de endpoint permanece na rede da AWS sem atravessar a internet pública.

Um provedor de serviços adiciona permissões para que os consumidores possam acessar o serviço de endpoint. O consumidor do serviço inicia a conexão e o provedor aceita ou rejeita as solicitações de conexão. O proprietário de um recurso ou proprietário da rede de serviços compartilha uma configuração de recursos ou uma rede de serviços com os consumidores AWS Resource Access Manager para que os consumidores possam acessar a rede de recursos ou serviços.

Com endpoints da VPC de interface, os consumidores podem usar políticas de endpoint para controlar quais entidades principais do IAM podem usar um endpoint da VPC para acessar o serviço ou recurso de endpoint.

Zonas hospedadas privadas

Uma zona hospedada é um contêiner para registros DNS que define como encaminhar o tráfego a um domínio ou subdomínio. Com uma zona hospedada pública, os registros especificam a forma como você quer encaminhar o tráfego na Internet. Com uma zona hospedada privada, os registros especificam como encaminhar o tráfego nas VPCs.

É possível configurar o Amazon Route 53 para encaminhar o tráfego do domínio a um endpoint da VPC. Para obter mais informações, consulte: Routing traffic to a VPC endpoint using your domain name (Encaminhar tráfego a um endpoint da VPC usando seu nome de domínio).

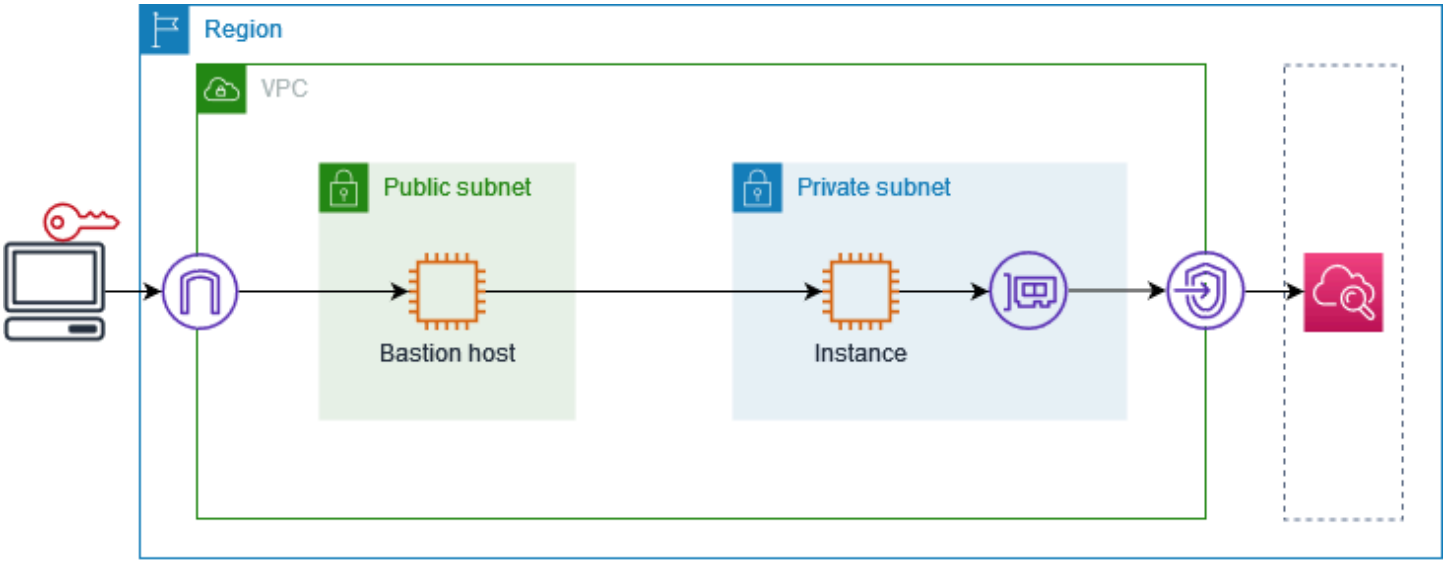
Você pode usar o Route 53 para configurar o DNS de horizonte dividido, onde você usa o mesmo nome de domínio para um site público e um serviço de endpoint desenvolvido por. AWS PrivateLink As solicitações de DNS para o nome de host público da VPC do consumidor são direcionadas aos endereços IP privados das interfaces de rede do endpoint, mas as solicitações de fora da VPC continuam sendo resolvidas para os endpoints públicos. Para obter mais informações,

consulte Mecanismos DNS para encaminhar tráfego e habilitar failover para implantações de AWS PrivateLink.

Comece com AWS PrivateLink

Este tutorial demonstra como enviar uma solicitação de uma instância do EC2 em uma sub-rede privada para a Amazon usando. CloudWatch AWS PrivateLink

O diagrama a seguir fornece uma visão geral desse cenário. Para se conectar do seu computador à instância na sub-rede privada, primeiro é necessário conectar a um bastion host em uma sub-rede pública. Tanto o bastion host quanto a instância devem usar o mesmo par de chaves. Como o arquivo `.pem` da chave privada está no seu computador, e não no bastion host, você usará o encaminhamento de chaves SSH. Em seguida, você poderá conectar à instância desde o bastion host sem especificar o arquivo `.pem` no comando ssh. Depois de configurar um VPC endpoint para CloudWatch, o tráfego da instância destinada CloudWatch é resolvido para a interface de rede do endpoint e, em seguida, enviado para o uso CloudWatch do VPC endpoint.



Para fins de teste, é possível usar uma única zona de disponibilidade. Em um ambiente de produção, recomendamos usar pelo menos duas zonas de disponibilidade para garantir baixa latência e alta disponibilidade.

Tarefas

- Etapa 1: criar uma VPC com sub-redes
- Etapa 2: iniciar as instâncias
- Etapa 3: testar o CloudWatch acesso
- Etapa 4: criar um VPC endpoint para acessar CloudWatch
- Etapa 5: testar o endpoint da VPC

Etapa 1: criar uma VPC com sub-redes

Use o procedimento a seguir para criar uma VPC com uma sub-rede pública e uma sub-rede privada.

Como criar a VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. Escolha Criar VPC.
3. Em Resources to create (Recursos a serem criados), escolha VPC and more (VPC e mais).
4. Em Name tag auto-generation (Geração automática de tags de nome), insira um nome para a VPC.
5. Para configurar as sub-redes, faça o seguinte:
   a. Em Number of Availability Zones (Número de zonas de disponibilidade), escolha 1 ou 2 dependendo das suas necessidades.
   b. Em Number of public subnets (Número de sub-redes públicas), verifique se você tem uma sub-rede pública por zona de disponibilidade.
   c. Em Number of private subnets (Número de sub-redes privadas), verifique se você tem uma sub-rede privada por zona de disponibilidade.
6. Escolha Criar VPC.

Etapa 2: iniciar as instâncias

Usando a VPC criada na etapa anterior, inicie o bastion host na sub-rede pública e a instância na sub-rede privada.

Pré-requisitos

- Crie um par de chaves usando o formato .pem. É necessário escolher esse par de chaves ao iniciar o bastion host e a instância.
- Crie um grupo de segurança para o bastion host que permita o tráfego SSH de entrada do bloco CIDR para seu computador.
- Crie um grupo de segurança para a instância que permita o tráfego SSH de entrada do grupo de segurança para o bastion host.

- Crie um perfil de instância do IAM e anexe a CloudWatchReadOnlyAccesspolítica.

Para iniciar o bastion host

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Iniciar instância.
3. Em Name (Nome), insira um nome para o bastion host.
4. Mantenha os valores padrão de imagem e tipo de instância.
5. Em Key pair (Par de chaves), selecione seu par de chaves.
6. Em Network settings (Configurações de rede), faça o seguinte:
    a. Em VPC, escolha sua VPC.
    b. Em Subnet (Sub-rede), escolha a sub-rede pública.
    c. Para IP Auto-assign público, escolha Habilitar.
    d. Em Firewall, escolha Select existing security group (Selecionar grupo de segurança existente) e, em seguida, escolha o grupo de segurança para o bastion host.
7. Escolha Iniciar instância.

Para iniciar a instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Iniciar instância.
3. Em Name (Nome), insira um nome para a instância.
4. Mantenha os valores padrão de imagem e tipo de instância.
5. Em Key pair (Par de chaves), selecione seu par de chaves.
6. Em Network settings (Configurações de rede), faça o seguinte:
    a. Em VPC, escolha sua VPC.
    b. Em Subnet (Sub-rede), escolha a sub-rede privada.
    c. Para IP Auto-assign público, escolha Desativar.
    d. Em Firewall, escolha Select existing security group (Selecionar grupo de segurança existente) e, em seguida, escolha o grupo de segurança para a instância.
7. Expanda Advanced details (Detalhes avançados). Em IAM instance profile (Perfil de instância do IAM), escolha o perfil de instância do IAM.

8. Escolha Iniciar instância.

Etapa 3: testar o CloudWatch acesso

Use o procedimento a seguir para confirmar que a instância não pode acessar CloudWatch. Você fará isso usando um AWS CLI comando somente de leitura para. CloudWatch

Para testar o CloudWatch acesso

1. No seu computador, adicione o key pair ao agente SSH usando o comando a seguir, onde *key.pem* está o nome do seu arquivo.pem.

   ```
   ssh-add ./key.pem
   ```

   Se você receber um erro informando que as permissões do seu par de chaves estão muito abertas, execute o comando a seguir e repita o comando anterior.

   ```
   chmod 400 ./key.pem
   ```

2. Conecte ao bastion host do seu computador. É necessário especificar a opção `-A`, o nome de usuário da instância (por exemplo, `ec2-user`) e o endereço IP público do bastion host.

   ```
   ssh -A ec2-user@bastion-public-ip-address
   ```

3. Connect à instância desde o bastion host. Você deve especificar o nome de usuário da instância (por exemplo,`ec2-user`) e o endereço IP privado da instância.

   ```
   ssh ec2-user@instance-private-ip-address
   ```

4. Execute o comando CloudWatch list-metrics na instância da seguinte maneira. Para a opção `--region`, especifique a região em que você a VPC foi criada.

   ```
   aws cloudwatch list-metrics --namespace AWS/EC2 --region us-east-1
   ```

5. Após alguns minutos, o tempo limite do comando é excedido. Isso demonstra que você não pode acessar a CloudWatch partir da instância com a configuração atual da VPC.

   ```
   Connect timeout on endpoint URL: https://monitoring.us-east-1.amazonaws.com/
   ```

6. Permaneça conectado à sua instância Depois de criar o endpoint da VPC, você tentará este comando list-metrics novamente.

Etapa 4: criar um VPC endpoint para acessar CloudWatch

Use o procedimento a seguir para criar um VPC endpoint que se conecta a. CloudWatch

Pré-requisito

Crie um grupo de segurança para o VPC endpoint que permita tráfego para o. CloudWatch Por exemplo, adicione uma regra que permita o tráfego de HTTPS do bloco CIDR da VPC.

Para criar um VPC endpoint para CloudWatch

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Escolha Criar endpoint.
4. Em Name tag (Etiqueta de nome), insira um nome para o endpoint.
5. Em Service category (Categoria de serviço), escolha Serviços da AWS.
6. Em Serviço, selecione com.amazonaws. ***region***.monitoramento.
7. Em VPC, selecione sua VPC.
8. Em Subnets (Sub-redes), selecione a zona de disponibilidade e, em seguida, selecione a sub-rede privada.
9. Em Security group (Grupo de segurança), selecione o grupos de segurança para o endpoint da VPC.
10. Em Policy (Política), selecione Full access (Acesso total) para permitir todas as operações de todas as entidades principais em todos os recursos no endpoint da VPC.
11. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
12. Escolha Criar endpoint. O status inicial é Pending (Pendente). Antes de passar para a próxima etapa, aguarde até que o status se torne Available (Disponível). Isso pode levar alguns minutos.

Etapa 5: testar o endpoint da VPC

Verifique se o VPC endpoint está enviando solicitações da sua instância para o. CloudWatch

Para testar o endpoint da VPC

Execute o comando apresentado a seguir na instância. Para a opção `--region`, especifique a região em que o endpoint da VPC foi criado.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --region us-east-1
```

Se você receber uma resposta, mesmo uma resposta com resultados vazios, estará conectado ao CloudWatch uso AWS PrivateLink.

Se você receber um `UnauthorizedOperation` erro, certifique-se de que a instância tenha uma função do IAM que permita acesso CloudWatch a.

Se a solicitação atingir o tempo limite, verifique o seguinte:

- O grupo de segurança do endpoint permite o tráfego para CloudWatch.
- A opção `--region` especifica a região na qual você criou o endpoint da VPC.

Etapa 6: limpar

Se o bastion host e a instância criados durante este tutorial não forem mais necessários, você poderá encerrá-los.

Para encerrar as instâncias

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instâncias.
3. Selecione ambas as instâncias de teste e escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).
4. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

Caso não precise mais do endpoint da VPC, você poderá excluí-lo.

Para excluir o endpoint da VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint da VPC.

4. Escolha Actions (Ações), Delete VPC endpoints (Excluir endpoints da VPC).
5. Quando a confirmação for solicitada, insira **`delete`** e escolha Excluir.

Acesso Serviços da AWS através AWS PrivateLink

Você acessa e AWS service (Serviço da AWS) usa um endpoint. Os endpoints de serviço padrão são interfaces públicas, então é necessário adicionar um gateway da Internet à VPC para que o tráfego possa ir da VPC para o AWS service (Serviço da AWS). Se essa configuração não funcionar com seus requisitos de segurança de rede, você pode usar AWS PrivateLink para conectar sua VPC Serviços da AWS como se ela estivesse em sua VPC, sem o uso de um gateway de internet.

Você pode acessar de forma privada aqueles Serviços da AWS que se integram com o AWS PrivateLink uso de VPC endpoints. Você pode criar e gerenciar todas as camadas da pilha de aplicações sem usar um gateway da Internet.

Preços

Você é cobrado por cada hora que o endpoint de interface é provisionado em cada zona de disponibilidade. Você também é cobrado por GB de dados processados. Para obter mais informações, consulte AWS PrivateLink Preço.

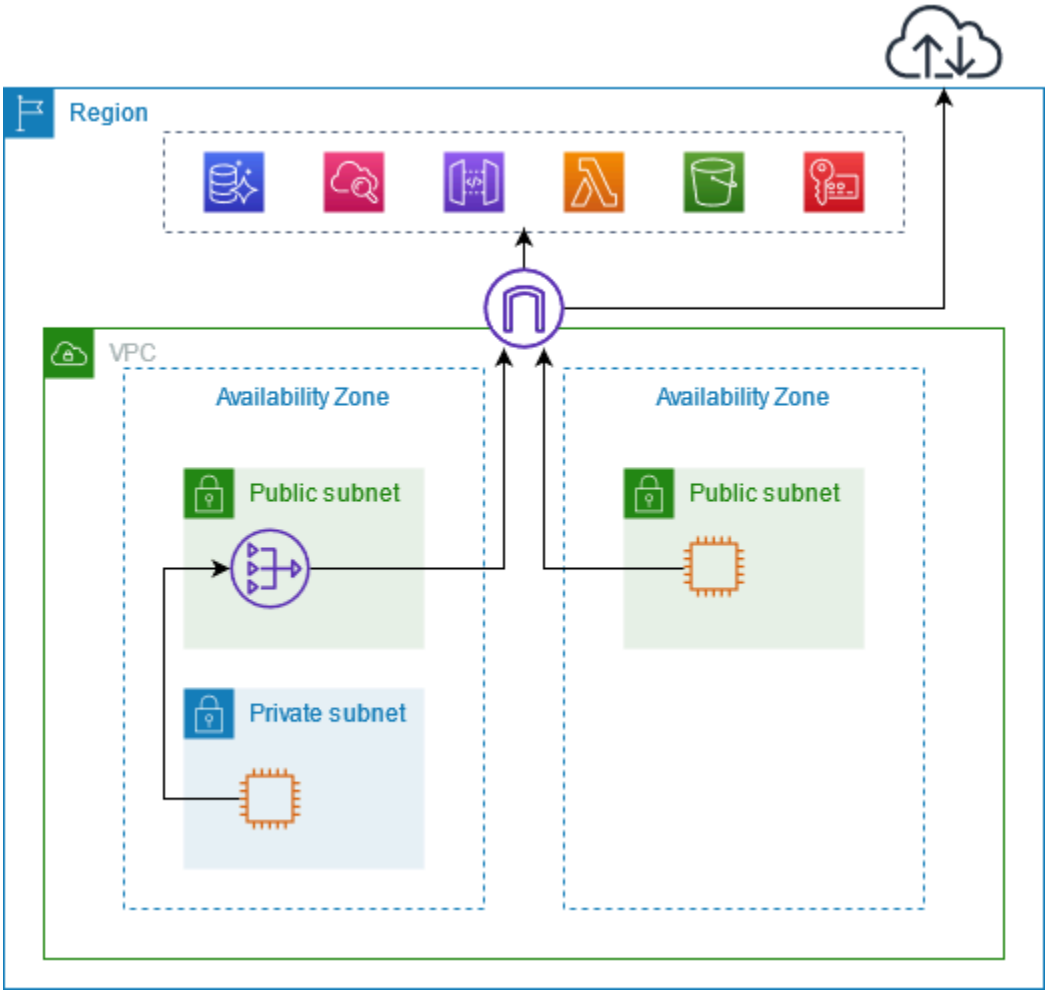
Conteúdo

Visão geral do

Você pode acessar Serviços da AWS por meio de seus endpoints de serviço público ou se conectar a um Serviços da AWS uso AWS PrivateLink compatível. Esta visão geral compara esses métodos.

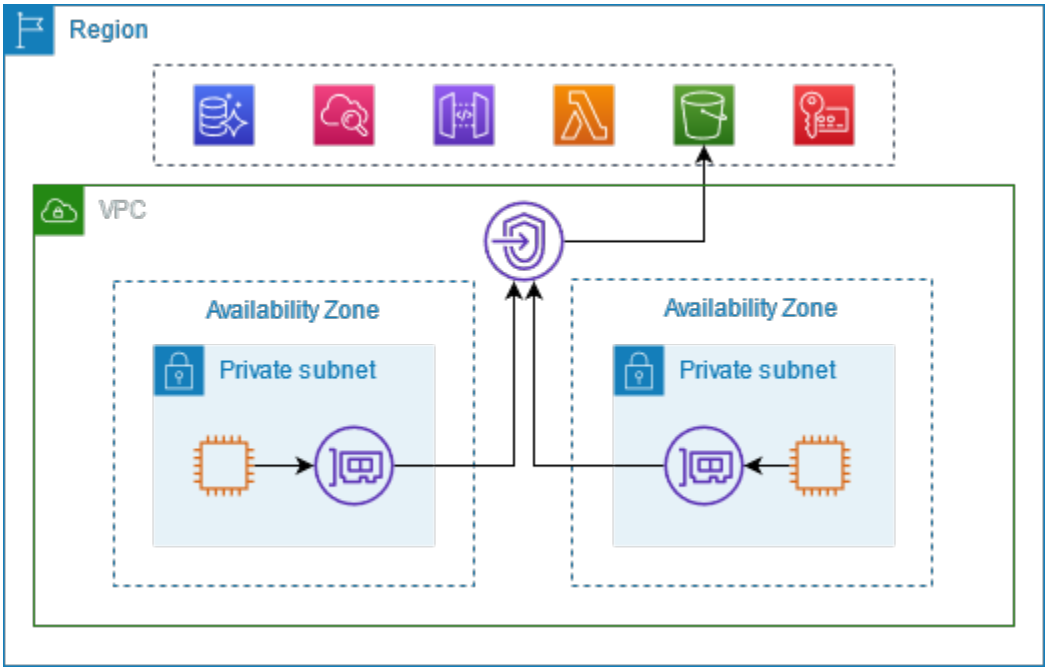
Acesso por meio de endpoints de serviço públicos

O diagrama a seguir mostra como as instâncias acessam Serviços da AWS por meio dos endpoints de serviço público. O tráfego AWS service (Serviço da AWS) de e para uma instância em uma sub-rede pública é roteado para o gateway da Internet da VPC e, em seguida, para o. AWS service (Serviço da AWS) O tráfego para um AWS service (Serviço da AWS) de uma instância em uma sub-rede privada é encaminhado a um gateway NAT, depois ao gateway da Internet da VPC e depois ao AWS service (Serviço da AWS). Enquanto esse tráfego atravessa o gateway da Internet, ele não sai da AWS rede.



Conecte-se por meio de AWS PrivateLink

O diagrama a seguir mostra como as instâncias Serviços da AWS acessam AWS PrivateLink. Primeiro, você cria uma interface VPC endpoint, que estabelece conexões entre as sub-redes em sua VPC e uma interface de rede de uso. AWS service (Serviço da AWS) O tráfego destinado ao AWS service (Serviço da AWS) é resolvido para os endereços IP privados das interfaces de rede do endpoint usando o DNS e, em seguida, enviado para o AWS service (Serviço da AWS) usando a conexão entre o VPC endpoint e o. AWS service (Serviço da AWS)



Serviços da AWS aceite solicitações de conexão automaticamente. O serviço não pode iniciar solicitações para recursos pelo endpoint da VPC.

Nomes de hosts DNS

A maioria Serviços da AWS oferece endpoints regionais públicos, que têm a seguinte sintaxe.

```
protocol://service_code.region_code.amazonaws.com
```

Por exemplo, o endpoint público da Amazon CloudWatch em us-east-2 é o seguinte.

```
https://monitoring.us-east-2.amazonaws.com
```

Com AWS PrivateLink, você envia tráfego para o serviço usando endpoints privados. Quando você cria uma interface de VPC endpoint, criamos nomes DNS regionais e zonais que você pode usar para se comunicar com a VPC. AWS service (Serviço da AWS)

O nome DNS regional para seu endpoint da VPC de interface tem a seguinte sintaxe:

```
endpoint_id.service_id.region.vpce.amazonaws.com
```

Os nomes DNS zonais apresentam a seguinte sintaxe:

```
endpoint_id-az_name.service_id.region.vpce.amazonaws.com
```

Ao criar uma interface VPC endpoint para um AWS service (Serviço da AWS), você pode habilitar o DNS privado. Com o DNS privado, você pode continuar fazendo solicitações a um serviço usando o nome de DNS de seu endpoint público enquanto utiliza a conectividade privada por meio do endpoint da VPC da interface. Para obter mais informações, consulte the section called “Resolução do DNS”.

O seguinte comando describe-vpc-endpoints exibe as entradas DNS para um endpoint da interface.

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-id vpce-099deb00b40f00e22 --query
 VpcEndpoints[*].DnsEntries
```

Veja a seguir um exemplo de saída para um endpoint de interface para a Amazon CloudWatch com nomes DNS privados habilitados. A primeira entrada é o endpoint regional privado. As três entradas seguintes são os endpoints zonais privados. A entrada final é da zona hospedada privada oculta, que resolve solicitações para o endpoint público para os endereços IP privados das interfaces de rede do endpoint.

```
[
    [
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2c.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2a.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
```

```
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2b.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "monitoring.us-east-2.amazonaws.com",
            "HostedZoneId": "Z06320943MMOWYG6MAVL9"
        }
    ]
]
```

Resolução do DNS

Os registros DNS que criamos para o endpoint da VPC de interface são públicos. Logo, esses nomes DNS podem ser resolvidos publicamente. Porém, as solicitações de DNS de fora da VPC ainda retornam os endereços IP privados das interfaces de rede do endpoint. Portanto, esses endereços IP não podem ser usados para acessar o serviço de endpoint, a menos que você tenha acesso à VPC.

DNS privado

Se você habilitar o DNS privado para sua interface VPC endpoint e sua VPC tiver nomes de host DNS e resolução de DNS ativados, criaremos uma zona hospedada privada gerenciada e oculta para você. AWS A zona hospedada contém um conjunto de registros para o nome do DNS padrão do serviço que é resolvido para os endereços IP privados das interfaces de rede do endpoint na VPC. Portanto, se você tiver aplicativos existentes que enviam solicitações para o AWS service (Serviço da AWS) usando um endpoint regional público, essas solicitações agora passam pelas interfaces de rede do endpoint, sem exigir que você faça alterações nesses aplicativos.

Recomendamos que você habilite nomes DNS privados para seus endpoints da VPC para Serviços da AWS. Isso garante que as solicitações que usam os endpoints de serviço público, como solicitações feitas por meio de um AWS SDK, cheguem ao seu VPC endpoint.

A Amazon fornece um servidor de DNS à VPC, o Route 53 Resolver. O Route 53 Resolver resolve automaticamente nomes de domínio de VPC locais e os registra em zonas hospedadas privadas. No entanto, não é possível usar o Route 53 Resolver de fora da sua VPC. Se desejar acessar seu endpoint da VPC por sua rede on-premises, use endpoints do Route 53 Resolver e regras

do Resolver. Para obter mais informações, consulte Integração AWS Transit Gateway com AWS PrivateLink e. Amazon Route 53 Resolver

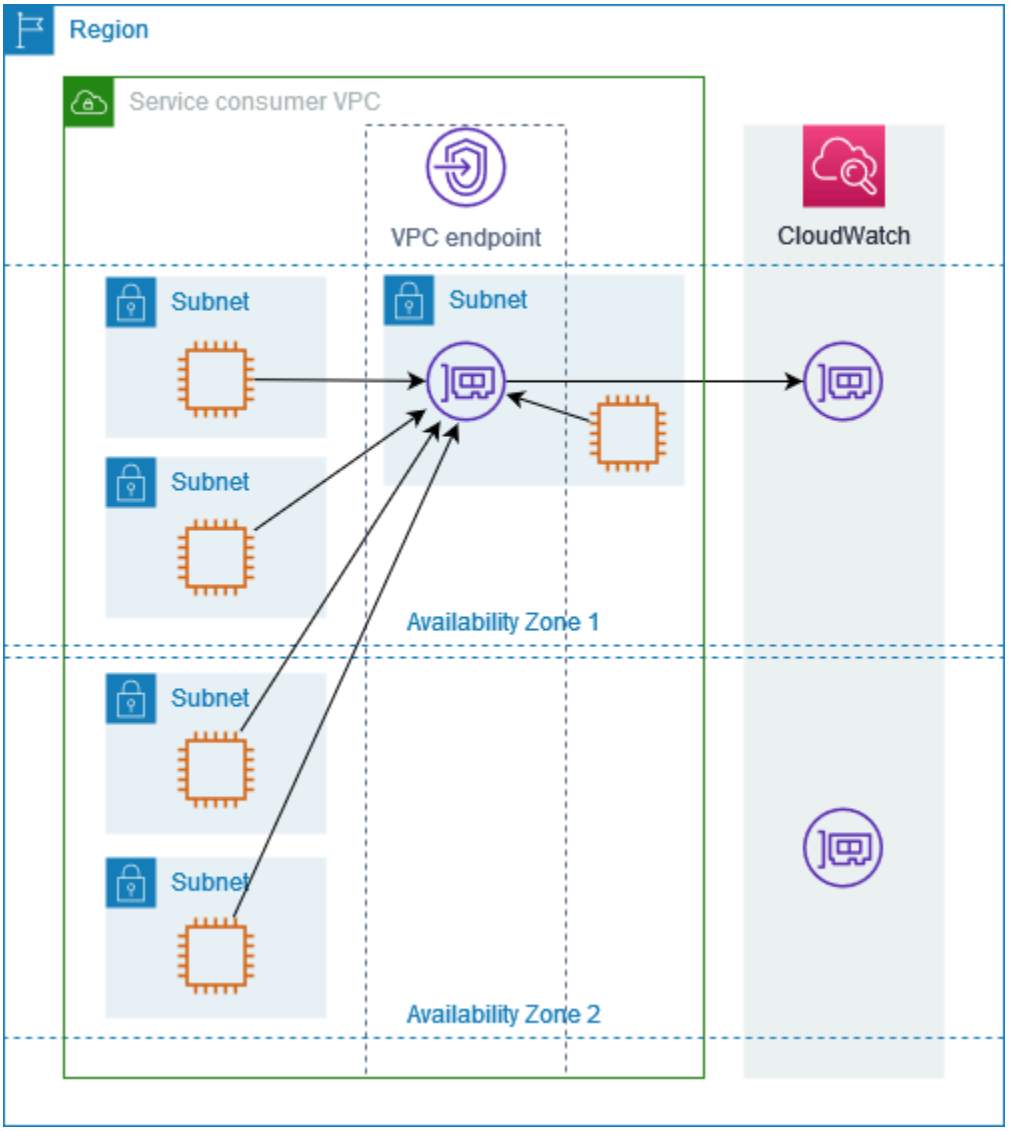
Zonas de disponibilidade e sub-redes

Você pode configurar um endpoint da VPC com uma sub-rede por zona de disponibilidade. Criamos uma interface de rede do endpoint para o endpoint da VPC na sub-rede. Atribuímos endereços IP a cada interface de rede de endpoint a partir de sua sub-rede, com base no tipo de endereço IP do endpoint da VPC. Os endereços IP de uma interface de rede de endpoint não mudarão durante a vida útil de seu endpoint da VPC.

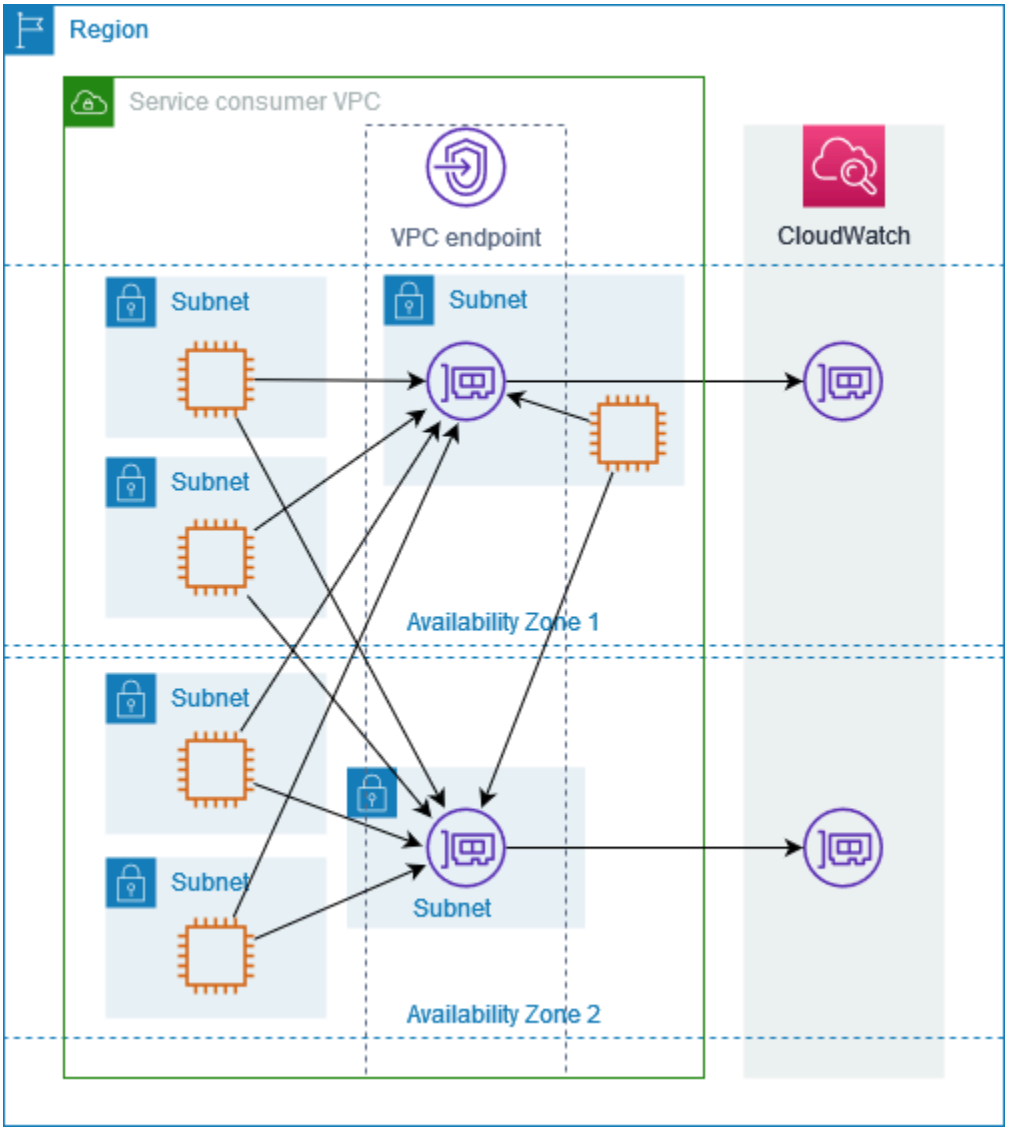
Em um ambiente de produção, para alta disponibilidade e resiliência, recomendamos o seguinte:

- Configure pelo menos duas zonas de disponibilidade por VPC endpoint e implante seus AWS recursos que devem ser acessados AWS service (Serviço da AWS) nessas zonas de disponibilidade.
- Configure nomes DNS privados para o endpoint da VPC.
- Acesse o AWS service (Serviço da AWS) usando seu nome DNS regional, também conhecido como endpoint público.

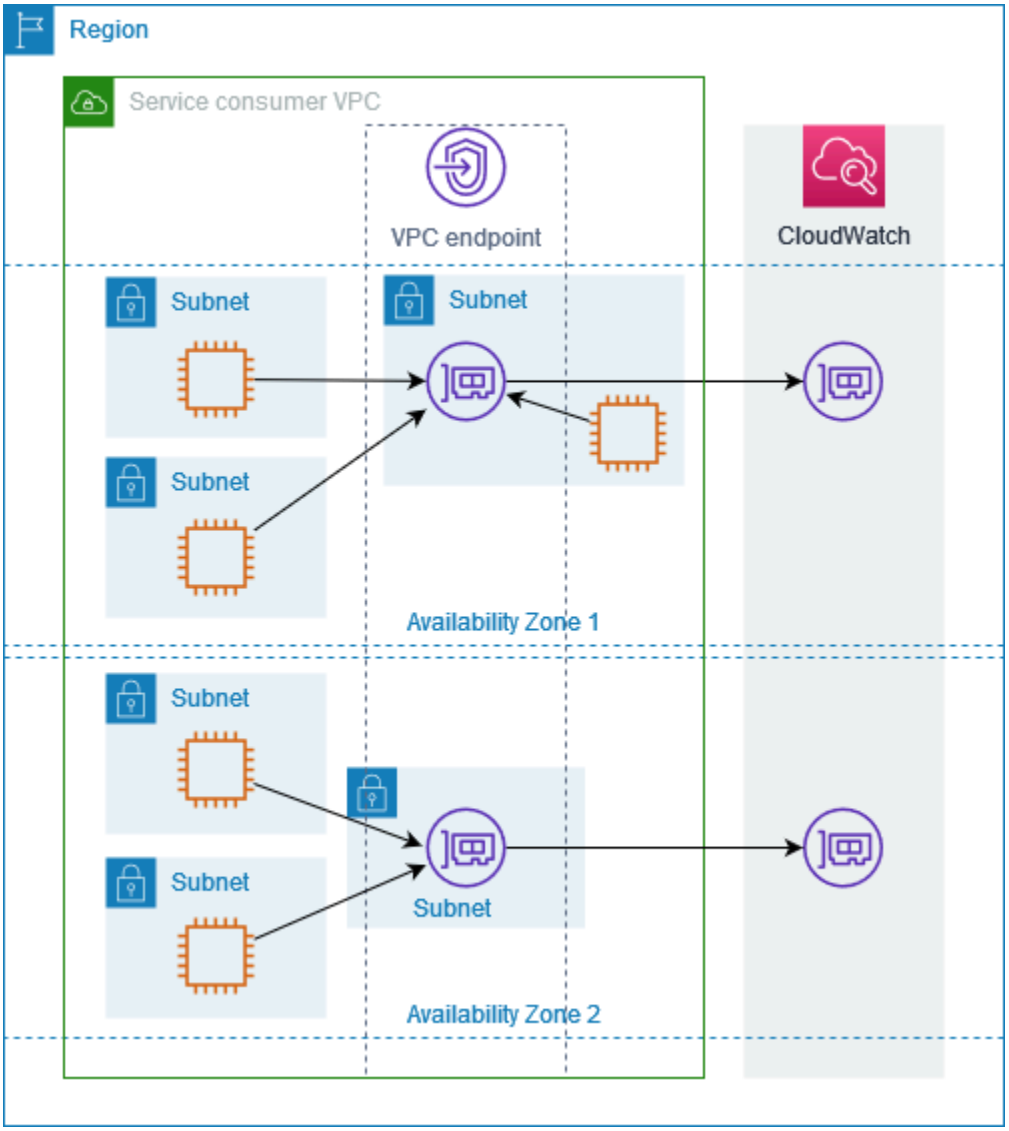
O diagrama a seguir mostra um VPC endpoint para a Amazon CloudWatch com uma interface de rede de endpoint em uma única zona de disponibilidade. Quando qualquer recurso em qualquer sub-rede na VPC acessa a CloudWatch Amazon usando seu endpoint público, resolvemos o tráfego para o endereço IP da interface de rede do endpoint. Isso inclui tráfego de sub-redes em outras zonas de disponibilidade. No entanto, se a Zona de Disponibilidade 1 for prejudicada, os recursos na Zona de Disponibilidade 2 perderão o acesso à Amazon CloudWatch.



O diagrama a seguir mostra um VPC endpoint para a Amazon CloudWatch com interfaces de rede de endpoint em duas zonas de disponibilidade. Quando qualquer recurso em qualquer sub-rede na VPC acessa a CloudWatch Amazon usando seu endpoint público, selecionamos uma interface de rede de endpoint saudável, usando o algoritmo round robin para alternar entre eles. Em seguida, resolvemos o tráfego para o endereço IP da interface de rede do endpoint selecionada.



Se for melhor para seu caso de uso, você poderá enviar tráfego de seus recursos para o AWS service (Serviço da AWS) usando a interface de rede do endpoint na mesma zona de disponibilidade. Para fazer isso, use o endpoint zonal privado ou o endereço IP da interface de rede do endpoint.



Tipos de endereço IP

Serviços da AWS podem oferecer suporte a IPv6 por meio de seus endpoints privados, mesmo que não suportem IPv6 por meio de seus endpoints públicos. Os endpoints que oferecem suporte a IPv6 podem responder a consultas de DNS com registros AAAA.

Requisitos para habilitar IPv6 para um endpoint de interface

- Eles AWS service (Serviço da AWS) devem disponibilizar seus endpoints de serviço via IPv6. Para obter mais informações, consulte the section called “Visualizar suporte a IPv6”.
- O tipo de endereço IP de um endpoint da interface deve ser compatível com as sub-redes do endpoint da interface, conforme descrito aqui:

- IPv4: atribua endereços IPv4 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4.
- IPv6: atribua endereços IPv6 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas forem sub-redes IPv6 apenas.
- Dualstack: atribua endereços IPv4 e IPv6 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4 e IPv6.

Se um endpoint da VPC de interface for compatível com IPv4, as interfaces de rede do endpoint terão endereços IPv4. Se um endpoint da VPC de interface for compatível com IPv6, as interfaces de rede do endpoint terão endereços IPv6. Não é possível acessar o endereço IPv6 de uma interface de rede de endpoint pela Internet. Se você descrever uma interface de rede de endpoint com um endereço IPv6, observe que `denyAllIgwTraffic` está habilitado.

Tipo de IP de registro DNS

Dependendo do seu tipo de endereço IP, quando você chama um VPC endpoint, o AWS serviço pode retornar registros A, registros AAAA ou registros A e AAAA. Você pode personalizar quais tipos de registro seu AWS serviço retorna modificando o tipo de IP do registro DNS. A tabela a seguir mostra os tipos de IP de registro DNS compatíveis e os tipos de registro retornados:

Tipo de IP de registro DNS	Tipos de registros retornado
IPv4	A
IPv6	AAAA
Pilha dupla	A e AAAA

Por padrão, o tipo de registro DNS é igual ao tipo de endereço IP. Você pode escolher outro tipo de IP de registro DNS, mas deve usar um tipo de endereço IP compatível para o serviço de endpoint. A tabela a seguir mostra o tipo de IP de registro DNS compatível com cada tipo de endereço IP para endpoints de interface:

Tipo de endereço IP	Tipos de IP de registro DNS compatíveis
IPv4	IPv4
IPv6	IPv6
Pilha dupla	Pilha dupla*, IPv4, IPv6, definido pelo serviço

* Representa o tipo de IP de registro DNS padrão.

Um tipo IP de registro DNS definido pelo serviço retorna registros DNS com base no endpoint de serviço que você chama. Se você usar um tipo de IP de registro DNS definido pelo serviço, certifique-se de que o serviço possa lidar com chamadas variáveis de endpoints de serviço. Para ver os registros DNS compatíveis com seu endpoint de interface, consulte os nomes DNS do seu VPC endpoint no, ou use. Console de gerenciamento da AWSDescribeVpcEndpoints

O comportamento do tipo de IP de registro DNS é diferente nos endpoints de gateway. Para obter mais informações, consulte DNS record IP type for gateway endpoints.

Serviços da AWS que se integram com AWS PrivateLink

O seguinte Serviços da AWS se integra com AWS PrivateLink. É possível criar um endpoint da VPC para estabelecer conexão privada com esses serviços, como se eles estivessem sendo executados em sua própria VPC.

Escolha o link na AWS service (Serviço da AWS)coluna para ver a documentação dos serviços que se integram com AWS PrivateLink o. A coluna Nome do serviço contém o nome do serviço que você especifica ao criar o endpoint da VPC da interface ou indica que o serviço gerencia o endpoint.

AWS service (Serviço da AWS)	Nome do serviço
AWS Gerenciamento de contas	com.amazonaws. *region*.conta
Amazon API Gateway	com.amazonaws. *region*.execute-api
	com.amazonaws. *region*.api gateway
AWS AppConfig	com.amazonaws. *region*.appconfig

AWS service (Serviço da AWS)	Nome do serviço
AWS App Mesh	com.amazonaws. *region*.appconfig-fips
	com.amazonaws. *region*.appconfigdata
	com.amazonaws. *region*.appconfigdata-fips
	com.amazonaws. *region*.appmesh
	com.amazonaws. *region*.appmesh-envoy-management
AWS Executor de aplicativos	com.amazonaws. *region*.app runner
Serviços do AWS App Runner	com.amazonaws. *region*.apprunner.requests
Application Auto Scaling	com.amazonaws. *region*.escalonamento automático de aplicativos
AWS Application Discovery Service	com.amazonaws. *region*.descoberta
	com.amazonaws. *region*.descoberta do arsenal
AWS Serviço de migração de aplicativos	com.amazonaws. *region*.mg
WorkSpaces Aplicativos da Amazon	com.amazonaws. *region*.appstream.api
	com.amazonaws. *region*.appstream.streaming
AWS AppSync	com.amazonaws. *region*.appsync-api
Amazon Athena	com.amazonaws. *region*.atena
AWS Audit Manager	com.amazonaws. *region*.gerente de auditoria
Amazon Aurora	com.amazonaws. *region*.rds
	com.amazonaws. *region*.rds-fips
Amazon Aurora DSQL	com.amazonaws. *region*.dsql

AWS service (Serviço da AWS)	Nome do serviço
AWS Auto Scaling	com.amazonaws. *region*.planos de escalonamento automático
AWS B2B Data Interchange	com.amazonaws. *region*.b2bi
AWS Backup	com.amazonaws. *region*.cópia de segurança
	com.amazonaws. *region*.gateway de backup
AWS Batch	com.amazonaws. *region*.lote
Amazon Bedrock	com.amazonaws. *region*.alicerce
	com.amazonaws. *region*.agente fundamental
	com.amazonaws. *region*.bedrock-agent-runtime
	com.amazonaws. *region*.bedrock-data-automation
	com.amazonaws. *region*.bedrock-data-automation-tips
	com.amazonaws. *region*.bedrock-data-automation-runtime
	com.amazonaws. *region*.bedrock-data-automation-runtime-fips
	com.amazonaws. *region*.bedrock-runtime
Amazon Bedrock AgentCore	com.amazonaws. *region*.bedrock-agentcore-control
	com.amazonaws. *region*.bedrock-agentcore
Gerenciamento de Faturamento e Custos da AWS	com.amazonaws. *region*.faturamento
	com.amazonaws. *region*.nível gratuito
	com.amazonaws. *region*.imposto

AWS service (Serviço da AWS)	Nome do serviço
AWS Billing Conductor	com.amazonaws. *region*. condutor de cobrança
Amazon Braket	com.amazonaws. *region*.suporte
AWS Certificate Manager	com.amazonaws. *region*.acm
	com.amazonaws. *region*.acm-fips
AWS Clean Rooms	com.amazonaws. *region*.salas limpas
	com.amazonaws. *region*.dicas para salas limpas
AWS Clean Rooms ML	com.amazonaws. *region*.salas limpas - ml
AWS API Cloud Control	com.amazonaws. *region*.API de controle de nuvem
	com.amazonaws. *region*.cloudcontrol api-fips
Amazon Cloud Directory	com.amazonaws. *region*diretório.cloud
AWS CloudFormation	com.amazonaws. *region*.formação em nuvem
	com.amazonaws. *region*.cloudformation-fips
Amazon CloudFront	com.amazonaws.cloudfront
AWS CloudHSM	com.amazonaws. *region*.cloudhsmv2
AWS Cloud Map	com.amazonaws. *region*.descoberta de serviços
	com.amazonaws. *region*.servicediscovery-fips
	com.amazonaws. *region*.descoberta de serviços de dados
	com.amazonaws. *region*.data-servicediscovery-fips
AWS CloudTrail	com.amazonaws. *region*.trilha na nuvem
AWS WAN em nuvem	com.amazonaws. *region*.gerenciador de rede

AWS service (Serviço da AWS)	Nome do serviço
Amazon CloudWatch	com.amazonaws. *region*.sinais de aplicação
	com.amazonaws. *region*. insights sobre o aplicativo
	com.amazonaws. *region*. monitor de internet
	com.amazonaws. *region*.monitor de internet - fips
	com.amazonaws. *region*.monitoramento
	com.amazonaws. *region*. monitor de fluxo de rede
	com.amazonaws. *region*. relatórios do monitor de fluxo de rede
	com.amazonaws. *region*. monitor de rede
	com.amazonaws. *region*.observabilityadmin
	com.amazonaws. *region*.rum
	com.amazonaws. *region*.rum-dataplane
	com.amazonaws. *region*.sintéticos
	com.amazonaws. *region*.synthetics-fips
	com.amazonaws. *region*.espuma
CloudWatch Registros da Amazon	com.amazonaws. *region*.registros
AWS CodeArtifact	com.amazonaws. *region*.codeartifact.api
	com.amazonaws. *region*.codeartifact.repositórios
AWS CodeBuild	com.amazonaws. *region*.codebuild
	com.amazonaws. *region*.codebuild-fips
AWS CodeCommit	com.amazonaws. *region*.codecommit

AWS service (Serviço da AWS)	Nome do serviço
	com.amazonaws. *region*.codecommit-fips
	com.amazonaws. *region*.git-codecommit
	com.amazonaws. *region*.git-codecommit-fips
Conexões de código da AWS	com.amazonaws. *region*.codeconnections.api
	com.amazonaws. *region*.codestar-connections.api
AWS CodeDeploy	com.amazonaws. *region*.codedeploy
	com.amazonaws. *region*.codedeploy-commands-secure
	com.amazonaws. *region*.codedeploy-fips
Amazon CodeGuru Profiler	com.amazonaws. *region*.codeguru-profiler
CodeGuru Revisor da Amazon	com.amazonaws. *region*.codeguru-revisor
AWS CodePipeline	com.amazonaws. *region*.codepipeline
Amazon Comprehend	com.amazonaws. *region*.compreender
	com.amazonaws. *region*.compreend-fips
Amazon Comprehend Medical	com.amazonaws. *region*. compreenda a medicina
AWS Compute Optimizer	com.amazonaws. *region*.otimizador de computação
AWS Config	com.amazonaws. *region*.config
	com.amazonaws. *region*.config-fips
Connect Customer	com.amazonaws. *region*integrações de.app
	com.amazonaws. *region*.casos
	com.amazonaws. *region*.conectar

AWS service (Serviço da AWS)	Nome do serviço
	com.amazonaws. *region*.connect-fips
	com.amazonaws. *region*.connect - campanhas
	com.amazonaws. *region*.perfil
	com.amazonaws. *region*.identificação de voz
	com.amazonaws. *region*.sabedoria
AWS Connector Service	com.amazonaws. *region*.conector aws
Catálogo de controle da AWS	com.amazonaws. *region*.catálogo de controle
AWS Cost Explorer	com.amazonaws. *region*.ce
Hub de Otimização de Custos da AWS	com.amazonaws. *region*.hub de otimização de custos
AWS Control Tower	com.amazonaws. *region*. torre de controle
	com.amazonaws. *region*.controltower-fips
AWS Data Exchange	com.amazonaws. *region*. troca de dados
Exportações de dados da AWS	aws.api. *region*.bcm-data-exports
	com.amazonaws. *region*Calculadora de preços de.bcm
Amazon Data Firehose	com.amazonaws. *region*. mangueira de incêndio kinesis
Amazon Data Lifecycle Manager	com.amazonaws. *region*.dlm
	com.amazonaws. *region*.dlm-fips
AWS Database Migration Service	com.amazonaws. *region*.dms
	com.amazonaws. *region*.dms-fips
AWS DataSync	com.amazonaws. *region*.sincronização de dados

AWS service (Serviço da AWS)	Nome do serviço
Amazon DataZone	com.amazonaws. *region*.zona de dados
	com.amazonaws. *region*.datazone-fips
AWS Deadline Cloud	com.amazonaws. *region*.prazos.gerenciamento
	com.amazonaws. *region*.prazo.agendamento
Amazon Detective	com.amazonaws. *region*.detetive
	com.amazonaws. *region*.detective-fips
DevOpsGuru da Amazon	com.amazonaws. *region*.devops-guru
AWS Direct Connect	com.amazonaws. *region*. conexão direta
	com.amazonaws. *region*.directconnect-fips
AWS Directory Service	com.amazonaws. *region*.ds
	com.amazonaws. *region*.ds-dados
	com.amazonaws. *region*.ds-data-fips
Amazon DocumentDB	com.amazonaws. *region*.rds
Amazon DynamoDB	com.amazonaws. *region*.dynamodb
	com.amazonaws. *region*.dynamodb-fips
	com.amazonaws. *region*.dynamodb-streams
APIs diretas do Amazon EBS	com.amazonaws. *region*.ebs
	com.amazonaws. *region*.ebs-fips
Amazon EC2	com.amazonaws. *region*.ec2
	com.amazonaws. *region*.ec2-fips

AWS service (Serviço da AWS)	Nome do serviço
Amazon EC2 Auto Scaling	com.amazonaws. *region*.escalonamento automático
	com.amazonaws. *region*.autoscaling-fips
EC2 Image Builder	com.amazonaws. *region*.construtor de imagens
Amazon ECR	com.amazonaws. *region*.ecr.api
	com.amazonaws. *region*.ecr.dkr
Amazon ECS	com.amazonaws. *region*.ecs
	com.amazonaws. *region*.ecs-agent
	com.amazonaws. *region*.ecs-telemetria
Amazon EKS	com.amazonaws. *region*.eks
	com.amazonaws. *region*.eks-auth
	com.amazonaws. *region*.eks-fips
	com.amazonaws. *region*.eks-proxy
AWS Elastic Beanstalk	com.amazonaws. *region*. pé de feijão elástico
	com.amazonaws. *region*. pedúnculo de feijão elástico - saúde
Recuperação de desastres do AWS Elastic	com.amazonaws. *region*.drs
Amazon Elastic File System	com.amazonaws. *region*.sistema de arquivos elástico
	com.amazonaws. *region*.elasticfilesystem-fips
Elastic Load Balancing	com.amazonaws. *region*. balanceamento de carga elástico

AWS service (Serviço da AWS)	Nome do serviço
Amazon Elastic VMware Service	com.amazonaws. *region*.evs
	com.amazonaws. *region*.evs-fips
Amazon ElastiCache	com.amazonaws. *region*.cache elástico
	com.amazonaws. *region*.elasticache-fips
AWS Elemental MediaConnect	com.amazonaws. *region*.conexão de mídia
AWS Elemental MediaConvert	com.amazonaws. *region*.conversor de mídia
	com.amazonaws. *region*.mediaconvert-fips
Amazon EMR	com.amazonaws. *region*. elasticmapreduce
	com.amazonaws. *region*.elasticmapreduce-fips
Amazon EMR no EKS	com.amazonaws. *region*contêineres.emr
Amazon EMR Sem Servidor	com.amazonaws. *region*.emr-sem servidor
	com.amazonaws. *region*.emr-serverless-services.livy
	com.amazonaws. *region*.emr-serverless.dashboard
Amazon EMR WAL	com.amazonaws. *region*.emerwal.prod
AWS Mensagens sociais para o usuário final	com.amazonaws. *region*.mensagens sociais
	com.amazonaws. *region*.dicas de mensagens sociais
AWS Entity Resolution	com.amazonaws. *region*. resolução da entidade
	com.amazonaws. *region*.entityresolution-fips
Amazon EventBridge	com.amazonaws. *region*.eventos
	com.amazonaws. *region*.events-fips

AWS service (Serviço da AWS)	Nome do serviço
	com.amazonaws. *region*.tubos
	com.amazonaws. *region*.pipes-data
	com.amazonaws. *region*.pipes-fips
	com.amazonaws. *region*.esquemas
Amazon EventBridge Scheduler	com.amazonaws. *region*.agendador
AWS Fault Injection Service	com.amazonaws. *region*.peixe
	com.amazonaws. *region*.fis-fips
Amazon FinSpace	com.amazonaws. *region*.finspace
	com.amazonaws. *region*.finspace-api
AWS Firewall Manager	com.amazonaws. *region*.fms
	com.amazonaws. *region*.fms-fips
Amazon Forecast	com.amazonaws. *region*.previsão
	com.amazonaws. *region*.consulta de previsão
	com.amazonaws. *region*.dicas de previsão
	com.amazonaws. *region*.forecastquery-fips
Amazon Fraud Detector	com.amazonaws. *region*.detector de fraudes
Amazon FSx	com.amazonaws. *region*.fsx
	com.amazonaws. *region*.fsx-fips
GameLift Servidores Amazon	com.amazonaws. *region*.gamelift
Amazon GameLift Streams	com.amazonaws. *region*.gameliftstreams

AWS service (Serviço da AWS)	Nome do serviço
Redes globais da AWS para gateways de trânsito	com.amazonaws. *region*.gerenciador de rede
AWS Glue	com.amazonaws. *region*.cola
	com.amazonaws. *region*.glue.painel
AWS Glue DataBrew	com.amazonaws. *region*.databrew
	com.amazonaws. *region*.databrew-fips
Amazon Managed Grafana	com.amazonaws. *region*.grafana
	com.amazonaws. *region*.grafana-workspace
AWS Ground Station	com.amazonaws. *region*.estação terrestre
	com.amazonaws. *region*.groundstation-fips
Amazon GuardDuty	com.amazonaws. *region*.dever de guarda
	com.amazonaws. *region*.guardduty-data
	com.amazonaws. *region*.guardduty-data-fips
	com.amazonaws. *region*.guardduty-fips
AWS HealthImaging	com.amazonaws. *region*.dicom-medical-imaging
	com.amazonaws. *region*.imagiologia médica
	com.amazonaws. *region*.runtime-medical-imaging
AWS HealthLake	com.amazonaws. *region*.lago de saúde
AWS HealthOmics	com.amazonaws. *region*.analítica-ômica
	com.amazonaws. *region*.analytics-omics-fips
	com.amazonaws. *region*.control-storage-omics

AWS service (Serviço da AWS)	Nome do serviço
	com.amazonaws. *region*.control-storage-omics-fips
	com.amazonaws. *region*.storage-omics
	com.amazonaws. *region*.tags-comics
	com.amazonaws. *region*.tags-omics-fips
	com.amazonaws. *region*.workflows-omics
	com.amazonaws. *region*.workflows-omics-fips
AWS Identity and Access Management (IAM)	com.amazonaws.iam
IAM Access Analyzer	com.amazonaws. *region*.analisador de acesso
	com.amazonaws. *region*.access-analyzer-fips
Centro de Identidade do IAM	com.amazonaws. *region*.loja de identidades
IAM Roles Anywhere	com.amazonaws. *region*.funções em qualquer lugar
	com.amazonaws. *region*.rolesanywhere-fips
Amazon Inspector	com.amazonaws. *region*.inspetor 2
	com.amazonaws. *region*.inspector2-fips
	com.amazonaws. *region*.inspector-scan
	com.amazonaws. *region*.inspector-scan-fips
Amazon Interactive Video Service	com.amazonaws. *region*.ivs.contribute
AWS IoT Core	com.amazonaws. *region*.iot.api
	com.amazonaws. *region*.iot-fips.api
	com.amazonaws. *region*.iot.data

AWS service (Serviço da AWS)	Nome do serviço
	com.amazonaws. *region*.iot.credentials
AWS IoT Device Management tunelamento seguro	com.amazonaws. *region*.iot.tunneling.api
	com.amazonaws. *region*.iot-fips.tunneling.api
	com.amazonaws. *region*.iot.tunneling.data
	com.amazonaws. *region*.iot-fips.tunneling.data
AWS IoT Core Device Advisor	com.amazonaws. *region*.deviceadvisor.iot
Integrações gerenciadas para AWS IoT Device Management	com.amazonaws. *region*.iotmanagedintegrations.api
	com.amazonaws. *region*.integrações gerenciadas por IoT - fips.api
AWS IoT Core for LoRaWAN	com.amazonaws. *region*.iot sem fio.api
	com.amazonaws. *region*.lorawan.cups
	com.amazonaws. *region*.lorawan.lns
AWS IoT FleetWise	com.amazonaws. *region*.iot em termos de frota
AWS IoT Greengrass	com.amazonaws. *region*.erva verde
AWS IoT RoboRunner	com.amazonaws. *region*.iotroborunner
AWS IoT SiteWise	com.amazonaws. *region*.iotsitewise.api
	com.amazonaws. *region*.iotsitewise.data
AWS IoT TwinMaker	com.amazonaws. *region*.iottwinmaker.api
	com.amazonaws. *region*.iottwinmaker.data
Amazon Kendra	com.amazonaws. *region*.kendra
	aws.api. *region*.kendra-ranking

AWS service (Serviço da AWS)	Nome do serviço
AWS Key Management Service	com.amazonaws. *region*.kms
	com.amazonaws. *region*.kms-fips
Amazon Keyspaces (para Apache Cassandra)	com.amazonaws. *region*.cassandra
	com.amazonaws. *region*.cassandra-fips
Amazon Kinesis Data Streams	com.amazonaws. *region*.kinesis-streams
	com.amazonaws. *region*.kinesis-streams-fips
AWS Lake Formation	com.amazonaws. *region*. formação de lago
AWS Lambda	com.amazonaws. *region*.lambda
AWS Launch Wizard	com.amazonaws. *region*.assistente de lançamento
Amazon Lex	com.amazonaws. *region*.models-v2-lex
	com.amazonaws. *region*.runtime-v2-lex
AWS License Manager	com.amazonaws. *region*.gerenciador de licenças
	com.amazonaws. *region*.license-manager-fips
	com.amazonaws. *region*.license-manager-linux-subscriptions
	com.amazonaws. *region*.license-manager-linux-subscriptions-fips
	com.amazonaws. *region*.license-manager-user-subscriptions
	com.amazonaws. *region*.license-manager-user-subscriptions-fips
Amazon Lightsail	com.amazonaws. *region*. vela leve

AWS service (Serviço da AWS)	Nome do serviço
Amazon Location Service	com.amazonaws. *region*.geo.maps
	com.amazonaws. *region*.geo.places
	com.amazonaws. *region*.geo.routes
	com.amazonaws. *region*.geo.geofencing
	com.amazonaws. *region*.geo.tracking
	com.amazonaws. *region*.geo.metadados
Amazon Lookout for Equipment	com.amazonaws. *region*. equipamento de vigia
Amazon Lookout for Vision	com.amazonaws. *region*.lookoutvision
Amazon Macie	com.amazonaws. *region*.macie2
	com.amazonaws. *region*.macie2-fips
AWS Mainframe Modernization	com.amazonaws. *region*.apptest
	com.amazonaws. *region*.m2
Amazon Managed Blockchain	com.amazonaws. *region*.consulta de blockchain gerenciada
	com.amazonaws. *region*.managedblockchain.bitcoin.mainnet
	com.amazonaws. *region*.managedblockchain.bitcoin.testnet
AWS Contrato do Marketplace	com.amazonaws. *region*.agreement-marketplace
AWS Marketplace Discovery	com.amazonaws. *region*.discovery-marketplace
AWS Marketplace Metering Service	com.amazonaws. *region*.metering-marketplace

AWS service (Serviço da AWS)	Nome do serviço
Amazon Managed Service for Prometheus	com.amazonaws. *region*.apps
	com.amazonaws. *region*.aps - espaços de trabalho
Amazon Managed Streaming for Apache Kafka (MSK)	com.amazonaws. *region*.kafka
	com.amazonaws. *region*.kafka-fips
Amazon Managed Workflows for Apache Airflow	com.amazonaws. *region*.airflow.api
	com.amazonaws. *region*.airflow.api-fips
	com.amazonaws. *region*.airflow.env
	com.amazonaws. *region*.airflow.env-fips
	com.amazonaws. *region*.airflow.ops
Amazon Route 53	com.amazonaws.route53
Amazon Route 53 Global Resolver	resolvedor global aws.api.us-east-2.route53
	aws.api.us-east-2.route53 globalresolver-fips
Console de gerenciamento da AWS	com.amazonaws. *region*.console
	com.amazonaws. *region*.login
Amazon MemoryDB	com.amazonaws. *region*.memória-db
	com.amazonaws. *region*.memorydb-fips
Orquestrador do AWS Migration Hub	com.amazonaws. *region*.migrationhub - orquestrador
AWS Migration Hub Refactor Spaces	com.amazonaws. *region*.espaços de refator
Migration Hub Strategy Recommendations	com.amazonaws. *region*.estratégia do hub de migração
Amazon MQ	com.amazonaws. *region*.mq

AWS service (Serviço da AWS)	Nome do serviço
	com.amazonaws. *region*.mq-fips
Amazon Neptune Analytics	com.amazonaws. *region*.gráfico de netuno
	com.amazonaws. *region*.neptune-graph-data
	com.amazonaws. *region*.netune-graph-fips
AWS Network Firewall	com.amazonaws. *region*.firewall de rede
	com.amazonaws. *region*.network-firewall-fips
OpenSearch Serviço Amazon	Esses endpoints são gerenciados por serviços
OpenSearch Ingestão da Amazon	com.amazonaws. *region*.ose
AWS Organizations	com.amazonaws. *region*.organizações
	com.amazonaws. *region*.organizations-fips
AWS Outposts	com.amazonaws. *region*.postos avançados
AWS Panorama	com.amazonaws. *region*.panorama
AWS Criptografia de pagamento	com.amazonaws. *region*.payment-cryptography.plano de controle
	com.amazonaws. *region*.criptografia-de-pagamento. dataplane
AWS PCS	com.amazonaws. *region*.peças
	com.amazonaws. *region*.pcs-fips
Amazon Personalize	com.amazonaws. *region*.personalizar
	com.amazonaws. *region*.personalize eventos

AWS service (Serviço da AWS)	Nome do serviço
	com.amazonaws. *region*.personalize o tempo de execução
Amazon Pinpoint	com.amazonaws. *region*.identificar
	com.amazonaws. *region*.pinpoint-sms-voice-v2
Amazon Polly	com.amazonaws. *region*.polly
	com.amazonaws. *region*.polly-fips
AWS Price List	com.amazonaws. *region*.preços.api
Autoridade de Certificação Privada da AWS	com.amazonaws. *region*.acm-pca
	com.amazonaws. *region*.acm-pca-fips
	com.amazonaws. *region*.pca-connector-ad
	com.amazonaws. *region*.pca-connector-scep
AWS Proton	com.amazonaws. *region*.próton
Amazon Q Business	aws.api. *region*.qbusiness
Amazon Q Developer	com.amazonaws. *region*.codewhisperer
	com.amazonaws. *region*.q
	com.amazonaws. *region*.apps
Amazon Q User Subscriptions	com.amazonaws. *region*.service.subscrições de usuário
Rápido	com.amazonaws. *region*.quicksight - site
Amazon RDS	com.amazonaws. *region*.rds
	com.amazonaws. *region*.rds-fips
API Data do Amazon RDS	com.amazonaws. *region*.rds-data

AWS service (Serviço da AWS)	Nome do serviço
Insights de Performance do Amazon RDS	com.amazonaws. *region*.pi
	com.amazonaws. *region*.pi-fips
AWS re:Post Privado	com.amazonaws. *region*.espaço de repostagem
Lixeira	com.amazonaws. *region*.rbin
	com.amazonaws. *region*.rbin-fips
Amazon Redshift	com.amazonaws. *region*.redshift
	com.amazonaws. *region*.redshift-fips
	com.amazonaws. *region*.redshift - sem servidor
	com.amazonaws. *region*.redshift-serverless-fips
API de dados do Amazon Redshift	com.amazonaws. *region*.redshift - dados
	com.amazonaws. *region*.redshift-data-fips
Amazon Rekognition	com.amazonaws. *region*.reconhecimento
	com.amazonaws. *region*.dicas de reconhecimento
	com.amazonaws. *region*.reconhecimento de streaming
	com.amazonaws. *region*.dicas de reconhecimento de streaming
AWS Resource Access Manager	com.amazonaws. *region*.ram
	com.amazonaws. *region*.ram-fips
Explorador de recursos da AWS	com.amazonaws. *region*.explorador de recursos-2
	com.amazonaws. *region*.resource-explorer-2-fips
AWS Resource Groups	com.amazonaws. *region*.grupos de recursos

AWS service (Serviço da AWS)	Nome do serviço
	com.amazonaws. *region*.resource-groups-fips
AWS Resource Groups Tagging API	com.amazonaws. *region*.marcação
Amazon S3	com.amazonaws. *region*.s3
	com.amazonaws. *region*.tabelas s3
Pontos de acesso do Amazon S3 Multi-Region	com.amazonaws.s3-global.accesspoint
Amazon S3 on Outposts	com.amazonaws. *region*.s3 - postos avançados
SageMaker Inteligência Artificial da Amazon	aws.sagemaker. *region*.experimentos
	aws.sagemaker. *region*.caderno
	aws.sagemaker. *region*.aplicativo parceiro
	aws.sagemaker. *region*.estúdio
	com.amazonaws. *region*.sagemaker-data-science-assistant
	com.amazonaws. *region*.sagemaker.api
	com.amazonaws. *region*.sagemaker.api-fips
	com.amazonaws. *region*.sagemaker.featurestore-runtime
	com.amazonaws. *region*.sagemaker.featurestore-runtime-fips
	com.amazonaws. *region*.sagemaker.metrics
	com.amazonaws. *region*.sagemaker.runtime
	com.amazonaws. *region*.sagemaker.runtime-fips

AWS service (Serviço da AWS)	Nome do serviço
Savings Plans	com.amazonaws.savingsplans
AWS Secrets Manager	com.amazonaws. *region*.gerente de segredos
AWS Agente de segurança	com.amazonaws. *region*. agente de segurança
AWS Security Hub CSPM	com.amazonaws. *region*.hub de segurança
	com.amazonaws. *region*.securityhub-fips
Amazon Security Lake	com.amazonaws. *region*. lago de segurança
	com.amazonaws. *region*.securitylake-fips
AWS Security Token Service	com.amazonaws. *region*.sts
	com.amazonaws. *region*.sts-fips
AWS Serverless Application Repository	com.amazonaws. *region*.repositório sem servidor
Service Catalog	com.amazonaws. *region*.catálogo de serviços
	com.amazonaws. *region*.servicecatalog-registro de aplicativos
Service Quotas	com.amazonaws. *region*.cotas de serviço
Amazon SES	com.amazonaws. *region*.email-smtp
	com.amazonaws. *region*.gerenciador de e-mail
	com.amazonaws. *region*.mail-manager-fips
	com.amazonaws. *region*.mail-manager-smtp.auth.fips
	com.amazonaws. *region*.mail-manager-smtp.open.fips

AWS service (Serviço da AWS)	Nome do serviço
AWS Snowball Edge Device Management	com.amazonaws. *region*.gerenciamento de dispositivos Snow
Amazon SNS	com.amazonaws. *region*.sns
Amazon SQS	com.amazonaws. *region*.sqs
	com.amazonaws. *region*.sqs-fips
Amazon SWF	com.amazonaws. *region*.swf
	com.amazonaws. *region*.swf-fips
AWS Step Functions	com.amazonaws. *region*.estados
	com.amazonaws. *region*.estados de sincronização
AWS Storage Gateway	com.amazonaws. *region*. gateway de armazenamento
Cadeia de Suprimentos AWS	com.amazonaws. *region*.scn
AWS Systems Manager	com.amazonaws. *region*mensagens.ec2
	com.amazonaws. *region*.sms
	com.amazonaws. *region*.ssm-contacts
	com.amazonaws. *region*.ssm-incidentes
	com.amazonaws. *region*.ssm-incidents-fips
	com.amazonaws. *region*.ssm - configuração rápida
	com.amazonaws. *region*.mensagens ssm
AWS Systems Manager para SAP	com.amazonaws. *region*.ssm-sap
	com.amazonaws. *region*.ssm-sap-fips
AWS Construtor de rede Telco	com.amazonaws. *region*.tnb

AWS service (Serviço da AWS)	Nome do serviço
Amazon Textract	com.amazonaws. *region*.extrato
	com.amazonaws. *region*.textract-fips
Amazon Timestream	com.amazonaws. *region*.timestream.ingest- *cell*
	com.amazonaws. *region*.timestream.query- *cell*
Amazon Timestream for InfluxDB	com.amazonaws. *region*.timestream-influxdb
	com.amazonaws. *region*.timestream-influxdb-fips
Amazon Transcribe	com.amazonaws. *region*.transcrever
	com.amazonaws. *region*.transcribe-fips
	com.amazonaws. *region*.transcrever streaming
com.amazonaws. *region*.transcrever dicas de streaming	
Amazon Transcribe Medical	com.amazonaws. *region*.transcrever
	com.amazonaws. *region*.transcrever streaming
AWS Transfer for SFTP	com.amazonaws. *region*.transferência
	com.amazonaws. *region*.transfer.servidor
AWS Transform	com.amazonaws. *region*.transformar
AWS Transform personalizado	com.amazonaws. *region*.transform-custom
Amazon Translate	com.amazonaws. *region*.traduzir
AWS Trusted Advisor	com.amazonaws. *region*. conselheiro confiável
Notificações de Usuários da AWS	com.amazonaws. *region*.notificações
	com.amazonaws. *region*.notificações-contatos

AWS service (Serviço da AWS)	Nome do serviço
Amazon Verified Permissions	com.amazonaws. *region*. permissões verificadas
	com.amazonaws. *region*.permissões verificadas - fips
Amazon VPC Lattice	com.amazonaws. *region*.vpc-lattice
AWS WAFV2	com.amazonaws. *region*.wafv2
	com.amazonaws. *region*.wafv2-fips
AWS Well-Architected Tool	com.amazonaws. *region*. bem arquitetado
Amazon WorkMail	com.amazonaws. *region*.email de trabalho
	com.amazonaws. *region*.fluxo de mensagens de trabalho
Amazon WorkSpaces	com.amazonaws. *region*.espaços de trabalho
WorkSpaces Navegador Amazon Secure	com.amazonaws. *region*.espaços de trabalho na web
	com.amazonaws. *region*.workspaces-web-fips
WorkSpaces streaming	com.amazonaws. *region*.highlander
Amazon WorkSpaces Thin Client	com.amazonaws. *region*.thinclient.api
aws.api. *region*arquivos.s3	
aws.api. *region*.s3files-fips	
AWS X-Ray	com.amazonaws. *region*.raio-x
Amazon Managed Service for Apache Flink	com.amazonaws. *region*.kinesis analytics
	com.amazonaws. *region*.kinesisanalytics-fips

Visualizar disponível AWS service (Serviço da AWS) Nomes

Você pode usar o comando describe-vpc-endpoint-services para visualizar os nomes de serviço que suportam VPC endpoints.

O exemplo a seguir exibe Serviços da AWS os endpoints da interface de suporte na região especificada. A opção `--query` limita a saída para aos nomes dos serviços

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query ServiceNames
```

O seguinte é um exemplo de saída. A saída completa não é mostrada.

```
[
    "api.aws.us-east-1.cassandra-streams",
    "aws.api.us-east-1.bcm-data-exports",
    "aws.api.us-east-1.emr-service-cell01",
    "aws.api.us-east-1.freetier",
    "aws.api.us-east-1.kendra-ranking",
    "aws.api.us-east-1.qbusiness",
    . . .
     "com.amazonaws.us-east-1.xray"
]
```

Visualizar informações sobre um serviço

Com o nome do serviço à disposição, você poderá usar o comando describe-vpc-endpoint-services para visualizar informações detalhadas sobre cada serviço de endpoint.

O exemplo a seguir exibe informações sobre o endpoint da CloudWatch interface Amazon na região especificada.

```
aws ec2 describe-vpc-endpoint-services \
  --service-name "com.amazonaws.us-east-1.monitoring" \
  --region us-east-1
```

O exemplo a seguir mostra uma saída. `VpcEndpointPolicySupported` indica se as políticas de endpoint são aceitas. `SupportedIpAddressTypes` indica quais tipos de endereço IP são compatíveis.

```
{
    "ServiceDetails": [
        {
            "ServiceName": "com.amazonaws.us-east-1.monitoring",
            "ServiceId": "vpce-svc-0fc975f3e7e5beba4",
            "ServiceType": [
                {
                    "ServiceType": "Interface"
                }
            ],
            "AvailabilityZones": [
                "us-east-1a",
                "us-east-1b",
                "us-east-1c",
                "us-east-1d",
                "us-east-1e",
                "us-east-1f"
            ],
            "Owner": "amazon",
            "BaseEndpointDnsNames": [
                "monitoring.us-east-1.vpce.amazonaws.com"
            ],
            "PrivateDnsName": "monitoring.us-east-1.amazonaws.com",
            "PrivateDnsNames": [
                {
                    "PrivateDnsName": "monitoring.us-east-1.amazonaws.com"
                },
                {
                    "PrivateDnsName": "monitoring.us-east-1.api.aws"
                },
                {
                    "PrivateDnsName": "monitoring-fips.us-east-1.amazonaws.com"
                },
                {
                    "PrivateDnsName": "monitoring-fips.us-east-1.api.aws"
                }           ],
            "VpcEndpointPolicySupported": true,
            "AcceptanceRequired": false,
            "ManagesVpcEndpoints": false,
            "Tags": [],
            "PrivateDnsNameVerificationState": "verified",
            "SupportedIpAddressTypes": [
                "ipv6",
```

```
                "ipv4"
            ]
        }
    ],
    "ServiceNames": [
        "com.amazonaws.us-east-1.monitoring"
    ]
}
```

Visualizar suporte a politicas de endpoint

Para verificar se um serviço oferece suporte a políticas de endpoint, chame o comando describe-vpc-endpoint-services e verifique o valor de `VpcEndpointPolicySupported`. Os valores possíveis são `true` e `false`.

O exemplo a seguir verifica se o serviço especificado oferece suporte a políticas de endpoint na região especificada. A opção `--query` limita a saída ao valor de `VpcEndpointPolicySupported`.

```
aws ec2 describe-vpc-endpoint-services \
  --service-name "com.amazonaws.us-east-1.s3" \
  --region us-east-1 \
  --query ServiceDetails[*].VpcEndpointPolicySupported \
  --output text
```

O seguinte é um exemplo de saída.

```
True
```

O exemplo a seguir lista as Serviços da AWS que oferecem suporte às políticas de endpoint na região especificada. A opção `--query` limita a saída para aos nomes dos serviços Para executar este comando usando o prompt de comando do Windows, remova as aspas simples ao redor da string de consulta e altere o caractere de continuação de linha de \ para ^.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query 'ServiceDetails[?VpcEndpointPolicySupported==`true`].ServiceName'
```

O seguinte é um exemplo de saída. A saída completa não é mostrada.

```
[
    "api.aws.us-east-1.cassandra-streams",
    "aws.api.us-east-1.bcm-data-exports",
    "aws.api.us-east-1.emr-service-cell01",
    "aws.api.us-east-1.freetier",
    "aws.api.us-east-1.kendra-ranking",
    . . .
    "com.amazonaws.us-east-1.xray"
]
```

O exemplo a seguir lista as Serviços da AWS que não oferecem suporte às políticas de endpoint na região especificada. A opção `--query` limita a saída para aos nomes dos serviços Para executar este comando usando o prompt de comando do Windows, remova as aspas simples ao redor da string de consulta e altere o caractere de continuação de linha de \ para ^.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query 'ServiceDetails[?VpcEndpointPolicySupported==`false`].ServiceName'
```

O seguinte é um exemplo de saída. A saída completa não é mostrada.

```
[
    "com.amazonaws.us-east-1.appmesh-envoy-management",
    "com.amazonaws.us-east-1.apprunner.requests",
    "com.amazonaws.us-east-1.appstream.api",
    "com.amazonaws.us-east-1.appstream.streaming",
    "com.amazonaws.us-east-1.awsconnector",
    . . .
    "com.amazonaws.us-east-1.transfer.server"
]
```

Visualizar suporte a IPv6

Para ver o suporte IPv6 para AWS serviços, consulte AWS serviços que oferecem suporte a IPv6. Você também pode usar o seguinte comando describe-vpc-endpoint-services para visualizar o Serviços da AWS que você pode acessar por IPv6 na região especificada. A opção `--query` limita a saída para aos nomes dos serviços

```
aws ec2 describe-vpc-endpoint-services \
```

```
  --filters Name=supported-ip-address-types,Values=ipv6 Name=owner,Values=amazon
 Name=service-type,Values=Interface \
  --region us-east-1 \
  --query ServiceNames
```

O seguinte é um exemplo de saída. A saída completa não é mostrada.

```
[
    "api.aws.us-east-1.cassandra-streams",
    "aws.api.us-east-1.bcm-data-exports",
    "aws.api.us-east-1.freetier",
    "aws.api.us-east-1.kendra-ranking",
    "aws.api.us-east-1.qbusiness",
    "aws.api.us-east-1.resource-explorer-2",
    "aws.api.us-east-1.resource-explorer-2-fips",
    "aws.sagemaker.us-east-1.experiments",
    "aws.sagemaker.us-east-1.partner-app",
    "com.amazonaws.iam",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.account",
    . . .
    "com.amazonaws.us-east-1.xray"
]
```

Cross-region habilitado Serviços da AWS

O seguinte Serviços da AWS se integra com várias regiões AWS PrivateLink. Você pode criar um endpoint de interface para se conectar a esses serviços em outra AWS região, de forma privada, como se estivessem sendo executados em sua própria VPC.

Escolha o link na AWS service (Serviço da AWS)coluna para ver a documentação do serviço. A coluna Nome do serviço contém o nome do serviço que você especifica ao criar o endpoint da interface.

AWS service (Serviço da AWS)	Nome do serviço
Amazon S3	com.amazonaws. *region*.s3
AWS Identity and Access Management (IAM)	com.amazonaws.iam

AWS service (Serviço da AWS)	Nome do serviço
Amazon ECR	com.amazonaws. *region*.ecr.api
	com.amazonaws. *region*.ecr.dkr
AWS Key Management Service	com.amazonaws. *region*.kms
	com.amazonaws. *region*.kms-fips
Amazon ECS	com.amazonaws. *region*.ecs
AWS Lambda	com.amazonaws. *region*.lambda
Amazon Data Firehose	com.amazonaws. *region*. mangueira de incêndio kinesis
Amazon Managed Service for Apache Flink	com.amazonaws. *region*.kinesis analytics
	com.amazonaws. *region*.kinesisanalytics-fips
Amazon Route 53	com.amazonaws.route53

Exibir AWS service (Serviço da AWS) nomes disponíveis

Você pode usar o comando describe-vpc-endpoint-services para visualizar serviços habilitados entre regiões.

O exemplo a seguir mostra o Serviços da AWS que um usuário na `us-east-1` região pode acessar pelos endpoints da interface, até a região de serviço especificada (`us-west-2`). A opção `--query` limita a saída para aos nomes dos serviços

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --service-region us-west-2 \
  --query ServiceNames
```

O seguinte é um exemplo de saída. A saída completa não é mostrada.

```
[
```

```
    "com.amazonaws.us-west-2.ecr.api",
    "com.amazonaws.us-west-2.ecr.dkr",
    "com.amazonaws.us-west-2.ecs",
    "com.amazonaws.us-west-2.ecs-fips",
    ...
    "com.amazonaws.us-west-2.s3"
]
```

> **Note**
>
> Você deve usar o DNS regional. O DNS zonal não é suportado ao acessar Serviços da AWS em outra região. Para obter mais informações, consulte Visualizar e atualizar atributos de DNS no Guia do usuário da Amazon VPC.

Permissões e considerações

- Por padrão, as entidades do IAM não têm permissão para acessar uma AWS service (Serviço da AWS) em outra região. Para conceder as permissões necessárias para acesso entre regiões, um administrador do IAM pode criar políticas do IAM que permitam a ação somente `vpce:AllowMultiRegion` de permissão.
- Certifique-se de que sua Política de Controle de Serviços (SCP) não negue ações somente com `vpce:AllowMultiRegion` permissão. Para usar AWS PrivateLink o recurso de conectividade entre regiões, tanto sua política de identidade quanto seu SCP devem permitir essa ação.
- Para controlar as regiões que uma entidade do IAM pode especificar como uma região de serviço ao criar um endpoint da VPC, use a chave de condição `ec2:VpceServiceRegion`.
- Um consumidor de serviço deve fazer a opção por uma região opcional antes de selecioná-la como uma região de serviço para um endpoint. Sempre que possível, recomendamos que os consumidores de serviços acessem um serviço usando a conectividade intrarregional em vez da conectividade entre regiões. Intra-Region a conectividade fornece menor latência e custos mais baixos.
- Você pode usar a nova chave de condição `aws:SourceVpcArn` global do IAM para proteger de quais regiões Contas da AWS e VPCs seus recursos podem ser acessados. Essa chave ajuda a implementar a residência de dados e o controle de acesso baseado na região.
- Para obter alta disponibilidade, crie um endpoint de interface compatível com várias regiões em pelo menos duas zonas de disponibilidade. Nesse caso, provedores e consumidores não precisam usar as mesmas zonas de disponibilidade.

- Com o acesso entre regiões, AWS PrivateLink gerencia o failover entre as zonas de disponibilidade nas regiões de serviço e de consumo. Ele não gerencia o failover inter-regional.
- O acesso entre regiões não é suportado nas seguintes zonas de disponibilidade: `use1-az3` `usw1-az2apne1-az3`,`apne2-az2`,, `apne2-az4` e.
- Você pode usar AWS Fault Injection Service para simular eventos regionais e modelar cenários de falha para endpoints de interface habilitados na região e entre regiões. Para saber mais, consulte a AWS FIS documentação.

Crie um endpoint de interface para um AWS service (Serviço da AWS) em outra região

Para criar um endpoint de interface usando o console, consulte a seção Criar um endpoint VPC.

Na CLI, você pode usar o comando create-vpc-endpoint para criar um VPC endpoint para uma região diferente. AWS service (Serviço da AWS) O exemplo a seguir cria um endpoint de interface para o Amazon S3 a partir de uma `us-west-2` entrada VPC. `us-east-1`

```
aws ec2 create-vpc-endpoint \
  --vpc-id vpc-id \
  --service-name com.amazonaws.us-west-2.s3 \
  --vpc-endpoint-type Interface \
  --subnet-ids subnet-id-1 subnet-id-2 \
  --region us-east-1 \
  --service-region us-west-2
```

Acesse um AWS service (Serviço da AWS) usando uma interface VPC endpoint

Você pode criar uma interface VPC endpoint para se conectar a serviços fornecidos por AWS PrivateLink, incluindo muitos. Serviços da AWS Para obter uma visão geral, consulte the section called “Conceitos” e Acessar Serviços da AWS.

Para cada sub-rede que você especifica em sua VPC, criamos uma interface de rede de endpoint na sub-rede e atribuímos a ela um endereço IP privado do intervalo de endereços da sub-rede. Uma interface de rede do endpoint é uma interface de rede gerenciada pelo solicitante; você pode visualizá-la em sua Conta da AWS, mas não pode gerenciá-la sozinho.

Você é cobrado pelas tarifas de uso por hora e processamento de dados. Para obter mais informações, consulte Preço do endpoint da interface.

Conteúdos

Pré-requisitos

- Implante os recursos que acessarão o AWS service (Serviço da AWS) em sua VPC.
- Para usar DNS privado, é necessário habilitar os nomes de host DNS e a resolução de DNS da VPC. Para mais informações, consulte Visualizar e atualizar atributos DNS para sua VPC no Manual do usuário da Amazon VPC.
- Para habilitar o IPv6 para um endpoint de interface, eles AWS service (Serviço da AWS) devem oferecer suporte ao acesso via IPv6. Para obter mais informações, consulte the section called "Tipos de endereço IP".
- Crie um grupo de segurança para a interface de rede do endpoint que permita o tráfego esperado dos recursos em sua VPC. Por exemplo, para garantir que eles AWS CLI possam enviar solicitações HTTPS para o AWS service (Serviço da AWS), o grupo de segurança deve permitir tráfego HTTPS de entrada.
- Se os recursos estiverem em uma sub-rede com uma ACL de rede, verifique se a ACL de rede permite tráfego entre os recursos na sua VPC e as interfaces de rede do endpoint.
- Há cotas em seus AWS PrivateLink recursos. Para obter mais informações, consulte AWS PrivateLink cotas.

Criar um VPC endpoint

Use o seguinte procedimento para criar um endpoint da VPC de interface que se conecta a um AWS service (Serviço da AWS).

Para criar um endpoint de interface para um AWS service (Serviço da AWS)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.

2. No painel de navegação, escolha Endpoints.
3. Escolha Criar endpoint.
4. Em Tipo, escolha Serviços da AWS .
5. (Opcional) Se estiver criando um endpoint para um AWS service (Serviço da AWS) em outra região, marque a caixa de seleção Habilitar endpoint entre regiões e, em seguida, selecione a região de serviço no menu suspenso.
6. Em Service name (Nome do serviço), selecione o serviço. Para obter mais informações, consulte the section called “Serviços que se integram”.
7. Em VPC, selecione a VPC de onde você acessará o AWS service (Serviço da AWS).
8. Se, na Etapa 5, você selecionou o nome do serviço para o Amazon S3 e deseja configurar o suporte a DNS privado, selecione Configurações adicionais e, em seguida, Habilitar nome de DNS. Quando essa seleção é feita, a opção Habilitar DNS privado somente para endpoint de entrada é selecionada automaticamente. É possível configurar o DNS privado com um endpoint do Resolver de entrada somente para endpoints de interface do Amazon S3. Se você não tiver um endpoint de gateway para o Amazon S3 e selecionar Habilitar DNS privado somente para endpoint de entrada, você receberá um erro ao tentar executar a etapa final desse procedimento.

   Se, na Etapa 5, você selecionou o nome do serviço para qualquer serviço diferente do Amazon S3, a opção Configurações adicionais, Habilitar nome de DNS já está selecionada. Recomendamos que você mantenha o valor padrão. Isso garante que as solicitações que usam os endpoints de serviço público, como solicitações feitas por meio de um AWS SDK, cheguem ao seu VPC endpoint.
9. Em Sub-redes, selecione as sub-redes nas quais serão criadas as interfaces de rede de endpoint. Você só pode selecionar uma sub-rede por zona de disponibilidade. Não é possível selecionar várias sub-redes em uma mesma zona de disponibilidade. Para obter mais informações, consulte the section called “Zonas de disponibilidade e sub-redes”.

   Por padrão, selecionamos endereços IP dos intervalos de endereços IP da sub-rede e os atribuímos às interfaces de rede do endpoint. Para escolher os endereços IP você mesmo, selecione Designar endereços IP. Observe que os quatro primeiros endereços IP e o último endereço IP em um bloco CIDR de sub-rede são reservados para uso interno, portanto, você não pode especificá-los para as interfaces de rede de endpoint.
10. Em IP address type (Tipo de endereço IP), escolha uma das seguintes opções:

- IPv4: atribua endereços IPv4 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4 e o serviço aceitar solicitações de IPv4.
- IPv6: atribua endereços IPv6 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv6 e o serviço aceitar solicitações de IPv6.
- Pilha dupla: atribua endereços IPv4 e IPv6 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de ambos os endereços IPv4 e IPv6 e o serviço aceitar solicitações de ambos IPv4 e IPv6.

11. Em Grupos de segurança, selecione os grupos de segurança para associar às interfaces de rede do endpoint. Por padrão, associamos o grupo de segurança padrão para a VPC.
12. Em Política, para permitir que todas as entidades principais façam todas as operações em todos os recursos pelo endpoint de interface, selecione Acesso total. Para restringir o acesso, selecione Personalizado e insira uma política. Essa opção ficará disponível somente se o serviço for compatível com as políticas de endpoint da VPC. Para obter mais informações, consulte Políticas de endpoint.
13. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
14. Escolha Criar endpoint.

Para criar um endpoint da interface usando a linha de comando

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Sub-redes compartilhadas

Você não pode criar, descrever, modificar ou excluir endpoints da VPC em sub-redes que são compartilhadas com você. Os VPC endpoints gerenciados por um AWS serviço (endpoints VPC gerenciados pelo serviço) podem ser criados pelo serviço em uma sub-rede compartilhada.

ICMP

Os endpoints da interface não respondem às solicitações ping. Em vez disso, você pode usar os comandos nc ou nmap.

Configurar um endpoint da interface

Depois de criar um endpoint da VPC de interface, você poderá atualizar a configuração.

Tarefas

- Adicionar ou remover sub-redes
- Associar grupos de segurança
- Editar a política de endpoints da VPC
- Habilitar nomes DNS privados
- Gerenciar tags

Adicionar ou remover sub-redes

Você pode escolher somente uma sub-rede por zona de disponibilidade para seu endpoint da interface. Se você adicionar uma sub-rede, criaremos uma interface de rede de endpoint na sub-rede e atribuiremos a ela um intervalo de endereço IP da sub-rede. Se você remover uma sub-rede, excluiremos a interface de rede do endpoint. Para obter mais informações, consulte the section called “Zonas de disponibilidade e sub-redes”.

Para alterar as sub-redes usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint da interface.
4. Escolha Actions (Ações), Manage Subnets (Gerenciar sub-redes).
5. Selecione ou desmarque as zonas de disponibilidade conforme necessário. Para cada zona de disponibilidade, selecione uma sub-rede. Por padrão, selecionamos endereços IP dos intervalos de endereços IP da sub-rede e os atribuímos às interfaces de rede do endpoint. Para escolher os endereços IP para uma interface de rede do endpoint, selecione Designar endereços IP e insira um endereço IPv4 do intervalo de endereços da sub-rede. Se o serviço de endpoint for compatível com o IPv6, você também poderá inserir um endereço IPv6 do intervalo de endereços da sub-rede.

   Se você especificar um endereço IP para uma sub-rede que já tem uma interface de rede de endpoint para esse endpoint da VPC, substituiremos a interface de rede do endpoint por uma nova. Esse processo desconecta temporariamente a sub-rede e o endpoint da VPC.

6. Escolha Modify subnets (Modificar sub-redes).

Para alterar as sub-redes usando a linha de comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Associar grupos de segurança

Você pode alterar os grupos de segurança associados às interfaces de rede para o endpoint da interface. As regras do grupo de segurança controlam o tráfego permitido para a interface de rede do endpoint com base nos recursos de sua VPC.

Para alterar os grupos de segurança usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint da interface.
4. Escolha Actions, Manage security groups.
5. Selecione ou desmarque grupos de segurança, conforme necessário.
6. Escolha Modify security groups (Modificar grupos de segurança).

Para alterar os grupos de segurança usando a linha de comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Editar a política de endpoints da VPC

Se o AWS service (Serviço da AWS) suporta políticas de endpoint, você pode editar a política de endpoint para o endpoint. Depois que você atualizar uma política de endpoint, poderá levar alguns minutos para que as alterações sejam aplicadas. Para obter mais informações, consulte Políticas de endpoint.

Para alterar a política de endpoint usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint da interface.
4. Escolha Actions (Ações), Manage policy (Gerenciar política).
5. Escolha Full Access (Acesso total) para permitir acesso total ao serviço ou escolha Custom (Personalizado) e anexe uma política personalizada.
6. Escolha Salvar.

Para alterar a política de endpoint usando a linha de comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Habilitar nomes DNS privados

Recomendamos que você habilite nomes DNS privados para seus endpoints da VPC para Serviços da AWS. Isso garante que as solicitações que usam os endpoints de serviço público, como solicitações feitas por meio de um AWS SDK, cheguem ao seu VPC endpoint.

Para usar nomes DNS privados, é necessário habilitar os nomes de host DNS e a resolução de DNS da VPC. Depois que você habilitar os nomes DNS privados, poderá levar alguns minutos para que os endereços IP privados fiquem disponíveis. Os registros DNS que criamos ao habilitar nomes DNS privados são privados. Portanto, não é possível resolver publicamente o nome DNS privado.

Para alterar a opção de nomes DNS privados usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint da interface.
4. Escolha Actions (Ações), Modify private DNS name (Modificar nome DNS privado).
5. Selecione ou desmarque Enable for this endpoint (Habilitar para este endpoint), conforme necessário.
6. Se o serviço for o Amazon S3, selecionar Habilitar para este endpoint na etapa anterior também selecionará Habilitar DNS privado somente para endpoint de entrada. Se você preferir a

funcionalidade de DNS privado padrão, desmarque a opção Habilitar DNS privado somente para endpoint de entrada. Se você não tiver um endpoint de gateway para o Amazon S3 além de um endpoint de interface para o Amazon S3 e selecionar Habilitar DNS privado somente para endpoint de entrada, você receberá um erro ao salvar as alterações na próxima etapa. Para obter mais informações, consulte the section called “DNS privado”.

7. Escolha Salvar alterações.

Para alterar a opção de nomes DNS privados usando a linha de comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Gerenciar tags

Você pode marcar o endpoint da interface para ajudar a identificá-lo ou categorizá-lo de acordo com as necessidades da organização.

Para gerenciar etiquetas usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint da interface.
4. Selecione Ações, Gerenciar tags.
5. Para cada etiqueta a ser adicionada, escolha Add new tag (Adicionar nova etiqueta) e insira a chave e o valor da etiqueta.
6. Para remover uma etiqueta, escolha Remove (Remover) à direita da chave e do valor da etiqueta.
7. Escolha Salvar.

Para gerenciar etiquetas usando a linha de comando

- create-tags and delete-tags (AWS CLI)
- New-EC2Tage Remove-EC2Tag(Ferramentas para Windows PowerShell)

Receber alertas para eventos de endpoint da interface

Você pode criar uma notificação para receber alertas de eventos específicos relacionados ao endpoint da interface. Por exemplo, é possível receber um e-mail quando uma solicitação de conexão é aceita ou rejeitada.

Tarefas

- Criação de uma notificação do SNS
- Adição de uma política de acesso
- Adição de uma política de chave

Criação de uma notificação do SNS

Use o procedimento a seguir para criar um tópico do Amazon SNS para as notificações e se inscrever nele.

Para criar uma notificação para um endpoint da interface usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint da interface.
4. Na guia Notifications (Notificações), selecione Create notification (Criar notificação).
5. Em ARN da notificação, escolha o nome do recurso da Amazon (ARN) do tópico do SNS que você criou.
6. Para assinar um evento, selecione-o em Events (Eventos).
   - Connect (Conectar): o consumidor do serviço criou o endpoint da interface. Isso envia uma solicitação de conexão ao provedor de serviços.
   - Accept (Aceitar): o provedor de serviços aceitou a solicitação de conexão.
   - Reject (Rejeitar): o provedor de serviços rejeitou a solicitação de conexão.
   - Delete (Excluir): o consumidor do serviço excluiu o endpoint da interface.
7. Escolha Create Notification (Criar notificação).

Para criar uma notificação para um endpoint da interface usando a linha de comando

- create-vpc-endpoint-connection-notification (AWS CLI)
- New-EC2VpcEndpointConnectionNotification(Ferramentas para Windows PowerShell)

Adição de uma política de acesso

Adicione uma política de acesso ao tópico do Amazon SNS que permita AWS PrivateLink publicar notificações em seu nome, como as seguintes. Para obter mais informações, consulte: Como edito a política de acesso do meu tópico do Amazon SNS? Use as chaves de condição globais `aws:SourceArn` e `aws:SourceAccount` para se proteger contra o problema confused deputy.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpce.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:us-east-1:111111111111:topic-name",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint/endpoint-id"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                }
            }
        }
    ]
}
```

Adição de uma política de chave

Se você estiver usando tópicos de SNS criptografados, a política de recursos da chave KMS deve ser confiável AWS PrivateLink para chamar as operações AWS KMS da API. Veja a seguir um exemplo de política de chave.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpce.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-east-1:111111111111:key/key-id",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint/endpoint-id"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                }
            }
        }
    ]
}
```

Excluir um endpoint de interface

Quando não precisar mais de um endpoint da VPC, você poderá excluí-lo. Excluir um endpoint de interface também exclui as interfaces de rede do endpoint.

Para excluir um endpoint da interface usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint da interface.
4. Escolha Actions (Ações), Delete VPC endpoints (Excluir endpoints da VPC).
5. Quando a confirmação for solicitada, insira **`delete`**.
6. Escolha Excluir.

Para excluir um endpoint da interface usando a linha de comando

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Endpoints de gateway

Os endpoints da VPC de gateway fornecem conectividade confiável para o Amazon S3 e o DynamoDB sem a necessidade de um gateway da Internet ou um dispositivo NAT para sua VPC. Os endpoints de gateway não usam AWS PrivateLink, ao contrário de outros tipos de endpoints de VPC.

O Amazon S3 e o DynamoDB oferecem suporte a endpoints de gateway e de interface. Para conferir uma comparação entre as opções, veja:

- Tipos de VPC endpoints para o Amazon S3
- Tipos de endpoint da Amazon VPC para o Amazon DynamoDB

Preços

Não há cobrança adicional pelo uso de endpoints do gateway.

Conteúdo

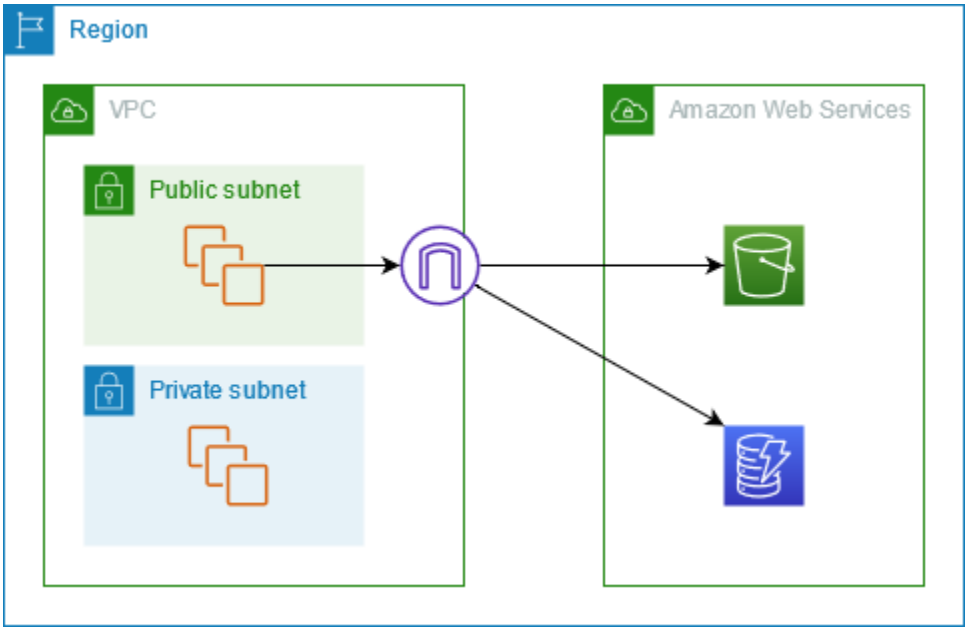
- Tipo de IP de registro DNS
- Endpoints de gateway para o Amazon S3
- Endpoints de gateway para o Amazon DynamoDB

Visão geral do

É possível acessar o Amazon S3 e o DynamoDB por meio de endpoints de serviço públicos ou endpoints de gateway. Esta visão geral compara esses métodos.

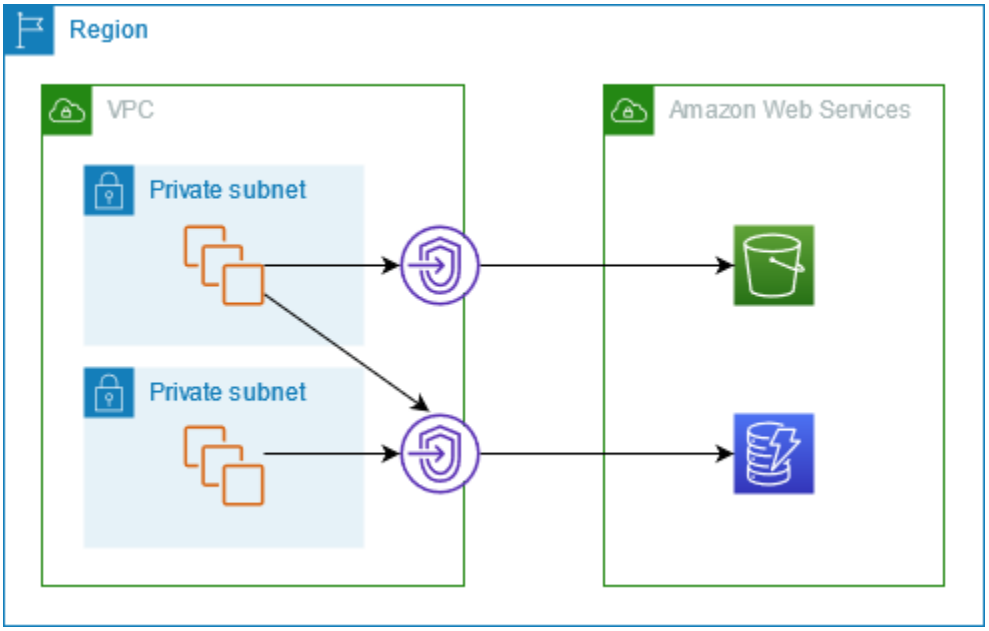
Acessar por meio de um gateway da Internet

O seguinte diagrama mostra como as instâncias acessam o Amazon S3 e o DynamoDB pelos endpoints de serviço públicos. O tráfego para o Amazon S3 ou o DynamoDB de uma instância em uma sub-rede pública é encaminhado ao gateway da Internet da VPC e depois ao serviço. As instâncias de uma sub-rede privada não podem enviar tráfego ao Amazon S3 ou ao DynamoDB porque, por definição, as sub-redes privadas não têm rotas para um gateway da Internet. Para habilitar que instâncias na sub-rede privada enviem tráfego ao Amazon S3 ou ao DynamoDB, você deve adicionar um dispositivo NAT à sub-rede pública e rotear o tráfego na sub-rede privada para o dispositivo NAT. Embora o tráfego para o Amazon S3 ou o DynamoDB passe pelo gateway da Internet, ele não sai da rede. AWS



Acessar por meio de um endpoint de gateway

O seguinte diagrama mostra como as instâncias acessam o Amazon S3 e o DynamoDB por um endpoint de gateway. O tráfego da VPC para o Amazon S3 ou o DynamoDB é encaminhado ao endpoint de gateway. Cada tabela de rotas de sub-rede deve ter uma rota que envie o tráfego destinado ao serviço para o endpoint de gateway usando a lista de prefixos do serviço. Para obter mais informações, consulte listaS de prefixos gerenciados da AWS no Guia do usuário da Amazon VPC.



Roteamento

Ao criar um endpoint de gateway, selecione as tabelas de rota da VPC para as sub-redes que você habilitar. A seguinte rota será adicionada automaticamente a cada tabela de rotas que você selecionar. O destino é uma lista de prefixos para o serviço de propriedade AWS e o destino é o endpoint do gateway.

Destination (Destino)	Alvo
prefix_list_id	*gateway_endpoint_id*

Considerações

- É possível revisar as rotas de endpoint que adicionamos à tabela de rotas, mas não é possível modificá-las nem excluí-las. Para adicionar uma rota de endpoint a uma tabela de rotas, associe-a

ao endpoint de gateway. Excluímos a rota do endpoint quando você desassocia a tabela de rotas do endpoint de gateway ou quando exclui o endpoint de gateway.

- Todas as instâncias das sub-redes associadas a uma tabela de rotas associada a um endpoint de gateway usarão esse endpoint automaticamente para acessar o serviço. As instâncias em sub-redes que não estão associadas a essas tabelas de rotas usarão o endpoint de serviço público, não o endpoint de gateway.
- A tabela de rotas pode ter uma rota de endpoint para o Amazon S3 e uma rota de endpoint para o DynamoDB. É possível ter rotas de endpoint para o mesmo serviço (Amazon S3 ou DynamoDB) em várias tabelas de rotas. É possível ter várias rotas de endpoint para o mesmo serviço (Amazon S3 ou DynamoDB) em uma única tabela de rotas.
- Para determinar como encaminhar o tráfego, usamos a rota mais específica que corresponde ao tráfego (correspondência de prefixo mais longa). Para tabelas de rotas com uma rota de endpoint, isso significa que:
  - Se houver uma rota que envie todo o tráfego da Internet (0.0.0. 0/0) para um gateway de internet, a rota do endpoint tem precedência para o tráfego destinado ao serviço (Amazon S3 ou DynamoDB) na região atual. O tráfego destinado a um diferente AWS service (Serviço da AWS) usa o gateway da Internet.
  - O tráfego destinado ao serviço (Amazon S3 ou DynamoDB) em uma região diferente vai para o gateway da Internet porque as listas de prefixos são específicas de uma região.
  - Se houver uma rota que especifique o intervalo exato de endereços IP para o serviço (Amazon S3 ou DynamoDB) na mesma região, essa rota prevalecerá sobre a rota do endpoint.

Segurança

Quando as instâncias acessam o Amazon S3 ou o DynamoDB por um endpoint de gateway, elas acessam o serviço usando um endpoint público. Os grupos de segurança dessas instâncias devem permitir o tráfego no serviço. Veja a seguir um exemplo de uma regra de saída. Ela faz referência ao ID da lista de prefixos do serviço.

Destino	Protocolo	Intervalo de portas
prefix_list_id	TCP	443

As ACLs de rede para as sub-redes dessas instâncias também devem permitir o tráfego no serviço. Veja a seguir um exemplo de uma regra de saída. Você não pode referenciar as listas de prefixos

nas regras de ACL de rede, mas pode obter os intervalos de endereços IP do serviço na lista de prefixos.

Destino	Protocolo	Intervalo de portas
service_cidr_block_1	TCP	443
service_cidr_block_2	TCP	443
service_cidr_block_3	TCP	443

Tipo de endereço IP

O tipo de endereço IP determina qual lista de prefixos é associada à tabela de rotas.

Requisitos para habilitar IPv6 para um endpoint de gateway

- O tipo de endereço IP de um endpoint de gateway deve ser compatível com as sub-redes do endpoint de gateway, como descrito aqui:
  - IPv4: adicione a lista de prefixos IPv4 do serviço à tabela de rotas.
  - IPv6: adicione a lista de prefixos IPv6 do serviço à tabela de rotas. Só haverá suporte para esta opção se todas as sub-redes selecionadas forem sub-redes IPv6 apenas.
  - Pilha dupla: adicione a lista de prefixos IPv4 do serviço à tabela de rotas e adicione a lista de prefixos IPv6 do serviço à tabela de rotas. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4 e IPv6.

Tipo de IP de registro DNS

Por padrão, um endpoint de gateway retorna registros DNS com base no endpoint de serviço que você chama. Se você criar seu endpoint de gateway usando o endpoint de serviço IPv4, como, por exemplo, o Amazon `s3.us-east-2.amazonaws.com` S3 retornará registros A para seus clientes, e todas as sub-redes em sua tabela de rotas usarão IPv4.

Por outro lado, se você criar seu endpoint de gateway usando o endpoint de serviço dualstack, como, por exemplo, o Amazon `s3.dualstack.us-east-2.amazonaws.com` S3 retornará os registros A e AAAA para seus clientes, e as sub-redes em sua tabela de rotas usarão IPv4 e IPv6.

> **Note**
>
> Para buckets de diretório ou S3 Express One Zone, os endpoints do gateway para o plano de dados seriam `s3express-use2-az1.us-east-2.amazonaws.com` e respectivamente. `s3express-use2-az1.dualstack.us-east-2.amazonaws.com`

O tipo de IP do registro DNS afeta a forma como o tráfego é roteado para seus clientes. Se você criar um endpoint de gateway usando o endpoint de serviço IPv4 e depois chamar o endpoint de serviço dualstack, o tráfego que usa registros AAAA não será roteado pelo endpoint do gateway. O tráfego será descartado ou roteado por um IPv6-compatible caminho, se houver um. Se você usa um tipo de IP de registro DNS definido pelo serviço, certifique-se de que seu serviço possa lidar com chamadas variáveis de vários endpoints de serviço.

Em vez da configuração padrão do tipo IP do registro DNS definido pelo serviço, você pode personalizar o tipo IP do registro DNS para escolher quais registros serão retornados para um endpoint específico. A tabela a seguir mostra os tipos de IP de registro DNS compatíveis e os tipos de registro retornados:

Tipo de IP de registro DNS	Tipos de registros retornado
IPv4	A
IPv6	AAAA
Pilha dupla	A e AAAA
definido pelo serviço	Os registros dependem do ponto final do serviço

Para escolher um tipo de IP de registro DNS, você deve usar um tipo de endereço IP compatível para o serviço de endpoint. A tabela a seguir mostra o tipo de IP de registro DNS suportado para cada tipo de endereço IP para endpoints de gateway:

Tipo de endereço IP	Tipos de IP de registro DNS compatíveis
IPv4	IPv4, definido pelo serviço*

Tipo de endereço IP	Tipos de IP de registro DNS compatíveis
IPv6	IPv6, definido pelo serviço*
Pilha dupla	IPv4, IPv6, Pilha dupla, definido pelo serviço*

* Representa o tipo de IP de registro DNS padrão.

> **Note**
>
> Para usar tipos de IP de registro DNS diferentes dos definidos pelo serviço para seu endpoint do Gateway, você deve permitir `enableDnsSupport` e atribuir atributos `enableDnsHostnames` nas configurações de VPC.

Você não pode alterar o tipo de IP do registro DNS para um endpoint do gateway DynamoDB. O DynamoDB só é compatível com o tipo IP de registro DNS definido pelo serviço.

O comportamento do tipo de IP de registro DNS é diferente nos endpoints de interface. Para obter mais informações, consulte DNS record IP type for interface endpoints.

Endpoints de gateway para o Amazon S3

É possível acessar o Amazon S3 de sua VPC usando endpoints da VPC de gateway. Depois de criar o endpoint de gateway, é possível adicioná-lo como um destino na tabela de rotas para o tráfego destinado da VPC ao Amazon S3.

Não há cobrança adicional pelo uso de endpoints do gateway.

O Amazon S3 oferece suporte a endpoints de gateway e de interface. Com um endpoint de gateway, é possível acessar o Amazon S3 utilizando a sua VPC sem precisar de um gateway de Internet ou um dispositivo de NAT para a sua VPC, e tudo isso sem custos adicionais. No entanto, os endpoints de gateway não permitem acesso de redes locais, de VPCs emparelhadas em outras AWS regiões ou por meio de um gateway de trânsito. Para esses cenários, você deve usar um endpoint de interface, o qual está disponível por um custo adicional. Para obter mais informações, consulte Tipos de endpoints da VPC para o Amazon S3 no Guia do usuário da Amazon VPC.

Conteúdo

- DNS privado
- Criar um endpoint do gateway
- Controlar acesso usando políticas de bucket
- Associar tabela de rotas
- Editar a política de endpoints da VPC
- Excluir um endpoint de gateway

Considerações

- Um endpoint de gateway só estará disponível na região em que você o criou. Crie o endpoint de gateway na mesma região que os buckets do S3.
- Se você estiver usando os servidores DNS da Amazon, será necessário habilitar os nomes de host DNS e a resolução de DNS para sua VPC. Se você estiver usando seu próprio servidor DNS, certifique-se de que as solicitações para o Amazon S3 sejam resolvidas corretamente para os endereços IP mantidos pela AWS.
- As regras de saída do grupo de segurança para as instâncias que acessam o Amazon S3 pelo endpoint de gateway devem permitir o tráfego no Amazon S3. Você pode referenciar o ID da lista de prefixos do Amazon S3 nas regras do grupo de segurança.
- A ACL da rede para a sub-rede das instâncias que acessam o Amazon S3 pelo endpoint de gateway deve permitir o tráfego no Amazon S3. Você não pode referenciar as listas de prefixos nas regras de ACL da rede, mas pode obter os intervalos de endereços IP para o Amazon S3 da lista de prefixos para o Amazon S3.
- Verifique se você está usando um AWS service (Serviço da AWS) que exija acesso a um bucket do S3. Por exemplo, um serviço pode requerer acesso a buckets que contêm arquivos de log ou pode requerer que você baixe drivers ou agentes para suas instâncias do EC2. Nesse caso, certifique-se de que sua política de endpoint permita que o recurso AWS service (Serviço da AWS) ou acesse esses buckets usando a `s3:GetObject` ação.
- Você não pode usar a condição `aws:SourceIp` em uma política de identidade ou uma política de bucket para solicitações ao Amazon S3 que atravessam um endpoint da VPC. Em vez disso, use a condição `aws:VpcSourceIp`. Como alternativa, você pode usar tabelas de rotas para controlar quais instâncias do EC2 podem acessar o Amazon S3 por meio do endpoint da VPC.
- Os endereços IPv4 ou IPv6 de origem das instâncias em suas sub-redes afetadas, conforme recebidos pelo Amazon S3, mudam de endereços públicos para endereços privados em sua VPC. Um endpoint troca as rotas de rede e desconecta as conexões TCP abertas. As conexões

anteriores que usavam endereços públicos não são retomadas. É recomendável não ter nenhuma tarefa essencial em execução ao criar ou modificar um endpoint; ou que você faça um teste para verificar se seu software consegue reconectar-se automaticamente ao Amazon S3 após a interrupção da conexão.

- Não é possível estender conexões de endpoint para fora de uma VPC. Recursos do outro lado de uma conexão VPN, conexão de emparelhamento de VPC, gateway de trânsito ou Direct Connect conexão em sua VPC não podem usar um endpoint de gateway para se comunicar com o Amazon S3.
- Sua conta tem uma cota padrão de 20 endpoints de gateway por região, o que é ajustável. Há também um limite de 255 endpoints de gateway por VPC.

DNS privado

É possível configurar o DNS privado para otimizar os custos ao criar um endpoint de gateway e um endpoint de interface para o Amazon S3.

Route 53 Resolver

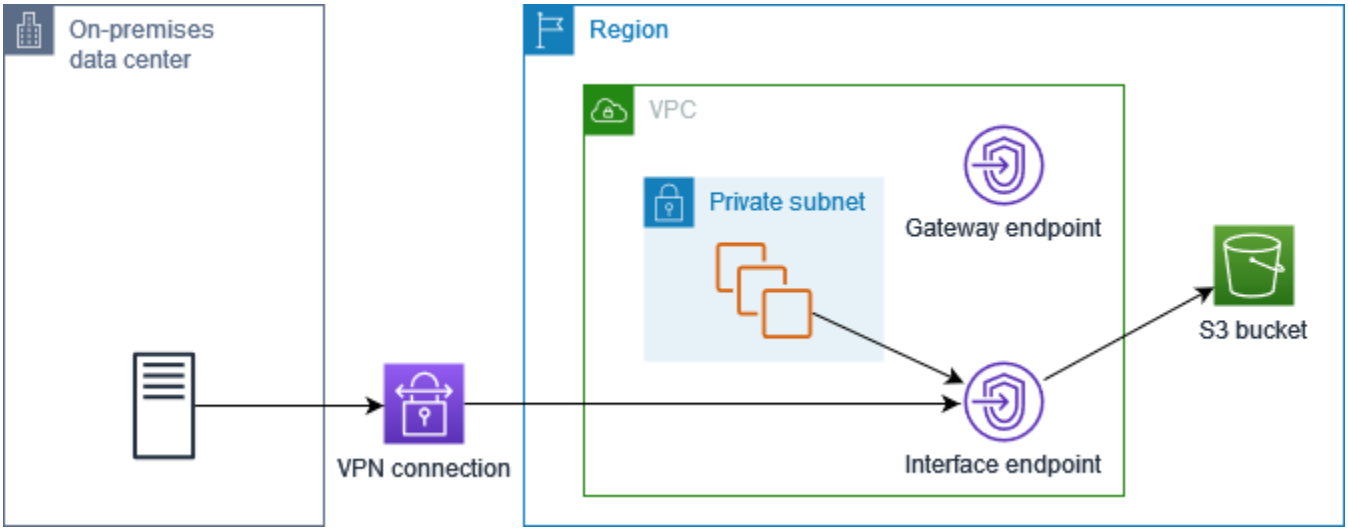
A Amazon fornece um servidor de DNS à VPC, o Route 53 Resolver. O Route 53 Resolver resolve automaticamente nomes de domínio de VPC locais e os registra em zonas hospedadas privadas. No entanto, não é possível usar o Route 53 Resolver de fora da sua VPC. O Route 53 fornece endpoints e regras de Resolver para que você possa usar o Route 53 Resolver por fora da VPC. Um endpoint do Resolver de entrada encaminha consultas de DNS da rede on-premises para o Route 53 Resolver. Um endpoint do Resolver de saída encaminha consultas de DNS do Route 53 Resolver para a rede on-premises.

Quando você configura o endpoint da interface para o Amazon S3 para usar DNS privado somente para o endpoint do Resolver de entrada, criamos um endpoint do Resolver de entrada. O endpoint do Resolver de entrada resolve consultas de DNS para o Amazon S3 dos endereços IP on-premises para os endereços IP privados do endpoint da interface. Também adicionamos registros ALIAS do Route 53 Resolver à zona hospedada pública do Amazon S3 para que as consultas de DNS da sua VPC sejam resolvidas para os endereços IP públicos do Amazon S3, que roteia o tráfego para o endpoint do gateway.

DNS privado

Se você configurar o DNS privado para seu endpoint da interface para o Amazon S3, mas não configurar o DNS privado somente para o endpoint do Resolver de entrada, as solicitações da sua

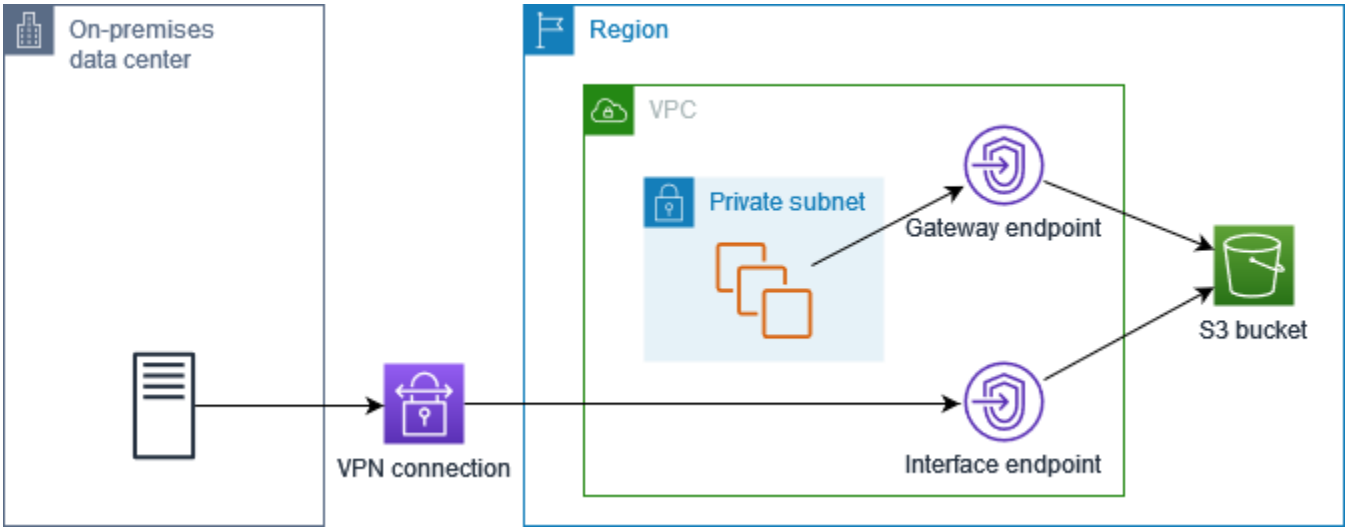
on-premises e da sua VPC usarão o endpoint da interface para acessar o Amazon S3. Portanto, você paga para usar o endpoint da interface para tráfego da VPC, em vez de usar o endpoint do gateway sem custo adicional.



DNS privado somente para o endpoint do Resolver de entrada

Se você configurar o DNS privado somente para o endpoint do Resolver de entrada, as solicitações da sua rede on-premises usarão o endpoint da interface para acessar o Amazon S3 e as solicitações da sua VPC usarão o endpoint do gateway para acessar o Amazon S3. Portanto, você otimiza seus custos, pois paga para usar o endpoint da interface somente para tráfego que não pode usar o endpoint do gateway.

Para configurar isso, o tipo IP do registro DNS do endpoint do gateway deve corresponder ao endpoint da interface ou ser. `service-defined` AWS PrivateLink não suporta nenhuma outra combinação. Para obter mais informações, consulte the section called “Tipo de IP de registro DNS”.



Configurar o DNS privado

É possível configurar o DNS privado para um endpoint de interface para o Amazon S3 ao criá-lo ou depois de criá-lo. Para obter mais informações, consulte the section called “Criar um VPC endpoint” (configurar durante a criação) ou the section called “Habilitar nomes DNS privados” (configurar após a criação).

Criar um endpoint do gateway

Use o seguinte procedimento para criar um endpoint de gateway que se conecte ao Amazon S3.

Para criar um endpoint do gateway usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Escolha Criar endpoint.
4. Em Service category (Categoria de serviço), escolha Serviços da AWS.
5. Para Serviços, adicione o filtro Tipo = Gateway.

   Se seus dados do Amazon S3 estiverem armazenados em buckets de uso geral, selecione com.amazonaws. *region*.s3.

   Se seus dados do Amazon S3 estiverem armazenados em buckets de diretório, selecione com.amazonaws. *region*.s3 express.
6. Em VPC, selecione a VPC na qual deseja criar o endpoint.
7. Em IP address type (Tipo de endereço IP), escolha uma das seguintes opções:

   - IPv4: atribua endereços IPv4 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4 e o serviço aceitar solicitações de IPv4.
   - IPv6: atribua endereços IPv6 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv6 e o serviço aceitar solicitações de IPv6.
   - Pilha dupla: atribua endereços IPv4 e IPv6 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de ambos os endereços IPv4 e IPv6 e o serviço aceitar solicitações de ambos IPv4 e IPv6.

8. Em Route tables (Tabelas de rotas), selecione as tabelas de rotas a serem usadas pelo endpoint. Adicionamos automaticamente uma rota que aponta o tráfego destinado ao serviço para a interface de rede do endpoint.
9. Em Policy (Política), selecione Full access (Acesso total) para permitir todas as operações de todas as entidades principais em todos os recursos no endpoint da VPC. Ou então selecione Custom (Personalizar) para anexar uma política de endpoint da VPC que controle as permissões das entidades principais para realizar ações em recursos sobre o endpoint da VPC.
10. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
11. Escolha Criar endpoint.

Para criar um endpoint de gateway usando a linha de comando

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Controlar acesso usando políticas de bucket

Você pode usar políticas de bucket para controlar o acesso a buckets de endpoints específicos, VPCs, intervalos de endereços IP e. Contas da AWS Estes exemplos supõem que também exista uma declaração de política que permita o acesso necessário para os seus casos de uso.

Example Exemplo: restringir o acesso a um endpoint específico

Você pode criar uma política de bucket que restrinja o acesso a um endpoint da VPC específico usando a chave de condição aws:sourceVpce. A seguinte política negará acesso ao bucket especificado usando as ações especificadas, a menos que o endpoint de gateway especificado seja usado. Observe que essa política bloqueia o acesso ao bucket especificado usando as ações especificadas por meio do Console de gerenciamento da AWS.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPCE",
      "Effect": "Deny",
```

```
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
                   "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

Example Exemplo: restringir o acesso a uma VPC específica

Você pode criar uma política de bucket que restrinja o acesso a VPCs específicas usando a chave de condição aws:sourceVpc. Isso será útil se houver vários endpoints configurados na mesma VPC. A seguinte política nega acesso ao bucket especificado usando as ações especificadas, a menos que a solicitação venha da VPC especificada. Observe que essa política bloqueia o acesso ao bucket especificado usando as ações especificadas por meio do Console de gerenciamento da AWS.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPC",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::example_bucket",
                   "arn:aws:s3:::example_bucket/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpc": "vpc-111bbb22"
        }
      }
    }
  ]
```

```
}
```

Example Exemplo: restringir o acesso a um intervalo de endereços IP específico

Você pode criar uma política que restrinja o acesso a intervalos específicos de endereços IP usando a chave de VpcSourceIp condição aws:. A seguinte política nega acesso ao bucket especificado usando as ações especificadas, a menos que a solicitação venha do endereço IP especificado. Observe que essa política bloqueia o acesso ao bucket especificado usando as ações especificadas por meio do Console de gerenciamento da AWS.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPC-CIDR",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
                   "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "NotIpAddress": {
          "aws:VpcSourceIp": "172.31.0.0/16"
        }
      }
    }
  ]
}
```

Example Exemplo: restringir o acesso a buckets em uma área específica Conta da AWS

Você pode criar uma política de bucket que restrinja o acesso a buckets do S3 em uma Conta da AWS específica usando a chave de condição `s3:ResourceAccount`. A seguinte política nega acesso aos buckets do S3 usando as ações especificadas, a menos que sejam de propriedade da Conta da AWS especificada.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-bucket-in-specific-account",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:GetObject", "s3:PutObject", "s3:DeleteObject"],
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "StringNotEquals": {
          "s3:ResourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

Associar tabela de rotas

Você pode alterar tabelas de rotas associadas ao endpoint de gateway. Quando você associa uma tabela de rotas, adicionamos automaticamente uma rota que aponta o tráfego destinado ao serviço para a interface de rede do endpoint. Quando você desassocia uma tabela de rotas, removemos automaticamente a rota do endpoint da tabela de rotas.

Para associar tabelas de rotas usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint de gateway.
4. Escolha Actions, Manage route tables.
5. Selecione ou cancele a seleção das tabelas de rotas, conforme necessário.
6. Escolha Modify route tables (Modificar tabelas de rotas).

Para associar tabelas de rotas usando a linha de comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Editar a política de endpoints da VPC

É possível editar a política de endpoint para um endpoint de gateway, que controla o acesso ao Amazon S3 da VPC até o endpoint. Depois que você atualizar uma política de endpoint, poderá levar alguns minutos para que as alterações sejam aplicadas. A política padrão permite acesso total. Para obter mais informações, consulte Políticas de endpoint.

Para alterar a política de endpoint usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint de gateway.
4. Escolha Actions (Ações), Manage policy (Gerenciar política).
5. Escolha Full Access (Acesso total) para permitir acesso total ao serviço ou escolha Custom (Personalizado) e anexe uma política personalizada.
6. Escolha Salvar.

Veja a seguir exemplos de políticas de endpoint para acessar o Amazon S3.

Example Exemplo: restringir acesso a um bucket específico

Você pode criar uma política que restrinja o acesso a somente alguns buckets do S3. Isso é útil se você tiver outros Serviços da AWS em sua VPC que usam buckets S3.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-bucket",
      "Effect": "Allow",
```

```
      "Principal": "*",
      "Action": [
         "s3:ListBucket",
         "s3:GetObject",
         "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::bucket_name",
        "arn:aws:s3:::bucket_name/*"
      ]
    }
  ]
}
```

Example Exemplo: restringir acesso a um perfil do IAM específico

Você pode criar uma política que restrinja o acesso a perfil do IAM específico. É necessário usar `aws:PrincipalArn` para conceder acesso a uma entidade principal.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-IAM-role",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/role_name"
        }
      }
    }
  ]
}
```

Example Exemplo: restringir o acesso a usuários em uma conta específica

Você pode criar uma política que restrinja o acesso a uma conta específica.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-callers-from-specific-account",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      }
    }
  ]
}
```

Excluir um endpoint de gateway

Quando não precisar mais de um endpoint de gateway, você poderá excluí-lo. Quando você exclui um endpoint de gateway, removemos a rota do endpoint das tabelas de rotas da sub-rede.

Não é possível excluir um endpoint de gateway quando o DNS privado está habilitado.

Para excluir um endpoint de gateway do cliente usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint de gateway.
4. Escolha Actions (Ações), Delete VPC endpoints (Excluir endpoints da VPC).
5. Quando a confirmação for solicitada, insira **delete**.
6. Escolha Excluir.

Para excluir um endpoint de gateway do cliente usando a linha de comando

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Endpoints de gateway para o Amazon DynamoDB

É possível acessar o Amazon DynamoDB de sua VPC usando endpoints da VPC de gateway. Depois de criar o endpoint de gateway, é possível adicioná-lo como um destino na tabela de rotas para o tráfego destinado da VPC ao DynamoDB.

Não há cobrança adicional pelo uso de endpoints do gateway.

O DynamoDB oferece suporte a endpoints de gateway e de interface. Com um endpoint de gateway, é possível acessar o DynamoDB utilizando a sua VPC sem precisar de um gateway de Internet ou um dispositivo de NAT para a sua VPC, e tudo isso sem custos adicionais. No entanto, os endpoints de gateway não permitem acesso de redes locais, de VPCs emparelhadas em outras AWS regiões ou por meio de um gateway de trânsito. Para esses cenários, você deve usar um endpoint de interface, o qual está disponível por um custo adicional. Para obter mais informações, consulte Tipos de endpoints da VPC para o Amazon S3 no Guia do desenvolvedor do Amazon DynamoDB.

Conteúdo

Considerações

- Um endpoint de gateway só estará disponível na região em que você o criou. Crie o endpoint de gateway na mesma região que as tabelas do DynamoDB.
- Se você estiver usando os servidores DNS da Amazon, será necessário habilitar os nomes de host DNS e a resolução de DNS para sua VPC. Se você estiver usando seu próprio servidor DNS,

certifique-se de que as solicitações para o DynamoDB sejam resolvidas corretamente para os endereços IP mantidos pela AWS.

- As regras de saída dos grupos de segurança para instâncias que acessam o DynamoDB pelo endpoint de gateway devem permitir o tráfego no DynamoDB. Você pode referenciar o ID da lista de prefixos do DynamoDB nas regras do grupo de segurança.
- A ACL da rede para a sub-rede das instâncias que acessam o DynamoDB pelo endpoint de gateway deve permitir o tráfego no DynamoDB. Você não pode referenciar as listas de prefixos nas regras de ACL da rede, mas pode obter os intervalos de endereços IP para o DynamoDB da lista de prefixos do DynamoDB.
- Se você usa AWS CloudTrail para registrar as operações do DynamoDB, os arquivos de log contêm os endereços IP privados das instâncias do EC2 na VPC do consumidor de serviços e o ID do endpoint do gateway para todas as solicitações realizadas por meio do endpoint.
- Os endpoints de gateway são compatíveis somente com tráfego IPv4.
- Os endereços IPv4 de origem de instâncias nas sub-redes afetadas são alterados de endereços IPv4 públicos para endereços IPv4 privados em sua VPC. Um endpoint troca as rotas de rede e desconecta as conexões TCP abertas. As conexões anteriores que usavam endereços IPv4 públicos não são retomadas. É recomendável que não haja nenhuma tarefa essencial em execução ao criar ou modificar um endpoint de gateway. Como alternativa, faça um teste para garantir que o software possa se reconectar automaticamente ao DynamoDB, caso a conexão seja interrompida.
- Não é possível estender conexões de endpoint para fora de uma VPC. Recursos do outro lado de uma conexão VPN, conexão de emparelhamento de VPC, gateway de trânsito ou Direct Connect conexão em sua VPC não podem usar um endpoint de gateway para se comunicar com o DynamoDB.
- Sua conta tem uma cota padrão de 20 endpoints de gateway por região, o que é ajustável. Há também um limite de 255 endpoints de gateway por VPC.

Criar um endpoint do gateway

Use o seguinte procedimento para criar um endpoint de gateway que se conecta ao DynamoDB.

Para criar um endpoint do gateway usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.

3. Escolha Criar endpoint.
4. Em Service category (Categoria de serviço), escolha Serviços da AWS.
5. Para Serviços, adicione o filtro Type = Gateway e selecione com.amazonaws.*region*.dynamodb.
6. Em VPC, selecione a VPC na qual deseja criar o endpoint.
7. Em Route tables (Tabelas de rotas), selecione as tabelas de rotas a serem usadas pelo endpoint. Adicionamos automaticamente uma rota que aponta o tráfego destinado ao serviço para a interface de rede do endpoint.
8. Em Policy (Política), selecione Full access (Acesso total) para permitir todas as operações de todas as entidades principais em todos os recursos no endpoint da VPC. Ou então selecione Custom (Personalizar) para anexar uma política de endpoint da VPC que controle as permissões das entidades principais para realizar ações em recursos sobre o endpoint da VPC.
9. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
10. Escolha Criar endpoint.

Para criar um endpoint de gateway usando a linha de comando

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Controlar o acesso usando políticas do IAM

É possível criar políticas do IAM para controlar quais entidades principais do IAM poderão acessar as tabelas do DynamoDB usando um endpoint da VPC específico.

Example Exemplo: restringir o acesso a um endpoint específico

Você pode criar uma política que restrinja o acesso a um endpoint da VPC específico usando a chave de condição aws:sourceVpce. A seguinte política nega o acesso às tabelas do DynamoDB na conta, a menos que se utilize o endpoint da VPC especificado. Este exemplo supõe que também exista uma declaração de política que permite o acesso necessário para os seus casos de uso.

JSON

```
{
```

```
   "Version":"2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-specific-endpoint",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:us-east-1:111111111111:table/*",
         "Condition": {
            "StringNotEquals" : {
               "aws:sourceVpce": "vpce-11aa22bb"
            }
         }
      }
   ]
}
```

Example Exemplo: permitir acesso de um perfil do IAM específico

Você pode criar uma política que permita acesso usando um perfil do IAM específico. A seguinte política concede acesso ao perfil do IAM especificado.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-specific-IAM-role",
         "Effect": "Allow",
         "Principal": "*",
         "Action": "*",
         "Resource": "*",
         "Condition": {
            "ArnEquals": {
               "aws:PrincipalArn": "arn:aws:iam::111122223333:role/role_name"
            }
         }
      }
   ]
}
```

Example Exemplo: permite o acesso de uma conta específica

Você pode criar uma política que permita o acesso de apenas uma conta específica. A seguinte política concede acesso aos usuários na conta especificada.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-account",
         "Effect": "Allow",
         "Principal": "*",
         "Action": "*",
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "aws:PrincipalAccount": "111122223333"
            }
         }
      }
   ]
}
```

Associar tabela de rotas

Você pode alterar tabelas de rotas associadas ao endpoint de gateway. Quando você associa uma tabela de rotas, adicionamos automaticamente uma rota que aponta o tráfego destinado ao serviço para a interface de rede do endpoint. Quando você desassocia uma tabela de rotas, removemos automaticamente a rota do endpoint da tabela de rotas.

Para associar tabelas de rotas usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint de gateway.
4. Escolha Actions, Manage route tables.
5. Selecione ou cancele a seleção das tabelas de rotas, conforme necessário.

6. Escolha Modify route tables (Modificar tabelas de rotas).

Para associar tabelas de rotas usando a linha de comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Editar a política de endpoints da VPC

É possível editar a política de endpoint para um endpoint de gateway, que controla o acesso ao DynamoDB da VPC até o endpoint. Depois que você atualizar uma política de endpoint, poderá levar alguns minutos para que as alterações sejam aplicadas. A política padrão permite acesso total. Para obter mais informações, consulte Políticas de endpoint.

Para alterar a política de endpoint usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint de gateway.
4. Escolha Actions (Ações), Manage policy (Gerenciar política).
5. Escolha Full Access (Acesso total) para permitir acesso total ao serviço ou escolha Custom (Personalizado) e anexe uma política personalizada.
6. Escolha Salvar.

Para modificar um endpoint de gateway usando a linha de comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Veja a seguir exemplos de políticas de endpoint para acessar o DynamoDB.

Example Exemplo: permitir acesso somente leitura

Você pode criar uma política que restrinja o acesso para somente leitura. A seguinte política concede permissão para listar e descrever tabelas do DynamoDB.

```
{
```

```
  "Statement": [
    {
      "Sid": "ReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "dynamodb:DescribeTable",
        "dynamodb:ListTables"
      ],
      "Resource": "*"
    }
  ]
}
```

Example Exemplo: restrição de acesso a uma tabela específica

Você pode criar uma política que restrinja o acesso a uma tabela específica do DynamoDB. A seguinte política permite acesso à tabela do DynamoDB especificada.

```
{
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-table",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "dynamodb:Batch*",
        "dynamodb:Delete*",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Update*"
      ],
      "Resource": "arn:aws:dynamodb:region:123456789012:table/table_name"
    }
  ]
}
```

Excluir um endpoint de gateway

Quando não precisar mais de um endpoint de gateway, você poderá excluí-lo. Quando você exclui um endpoint de gateway, removemos a rota do endpoint das tabelas de rotas da sub-rede.

Para excluir um endpoint de gateway do cliente usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint de gateway.
4. Escolha Actions (Ações), Delete VPC endpoints (Excluir endpoints da VPC).
5. Quando a confirmação for solicitada, insira **`delete`**.
6. Escolha Excluir.

Para excluir um endpoint de gateway do cliente usando a linha de comando

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Acesse produtos SaaS por meio de AWS PrivateLink

Usando AWS PrivateLink, você pode acessar produtos SaaS de forma privada, como se estivessem sendo executados em sua própria VPC.

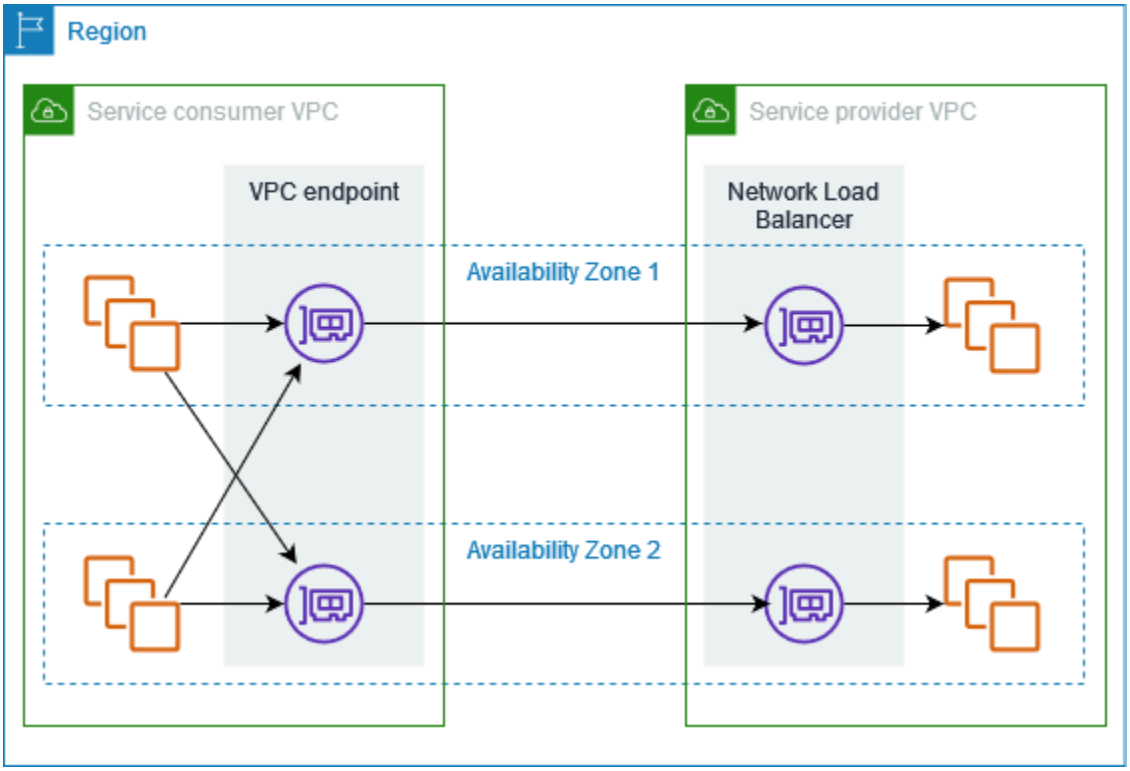
Conteúdo

Visão geral do

Você pode descobrir, comprar e provisionar produtos SaaS baseados em. AWS PrivateLink AWS Marketplace Para obter mais informações, consulte Acesse aplicativos SaaS de forma segura e privada usando. AWS PrivateLink

Você também pode encontrar produtos SaaS desenvolvidos pela AWS PrivateLink Partners. AWS Para obter mais informações, consulte Parceiros do AWS PrivateLink.

O seguinte diagrama mostra como usar endpoints da VPC para se conectar a produtos SaaS. O provedor de serviços cria um serviço de endpoint e concede aos clientes acesso ao serviço de endpoint. Como consumidor do serviço, crie um endpoint da VPC de interface que estabelece conexões entre uma ou mais sub-redes da VPC e o serviço de endpoint.



Como criar um endpoint de interface

Use o seguinte procedimento para criar um endpoint da VPC de interface que se conecta ao produto SaaS.

Requisito

Assine o serviço.

Para criar um endpoint de interface para um serviço de parceiro

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Escolha Criar endpoint.
4. Se você comprou o serviço em AWS Marketplace, faça o seguinte:
   a. Em Tipo, escolha Serviços da AWS Marketplace .
   b. Selecione o serviço.
5. Se você assinou um serviço com a designação AWS Service Ready, faça o seguinte:

   a. Em Tipo, escolha PrivateLink Ready partner services.
   b. Insira o nome do serviço e escolha Verificar serviço.
6. Em VPC, selecione a VPC de onde você acessará o produto.
7. Em Sub-redes, selecione as sub-redes nas quais serão criadas as interfaces de rede de endpoint.
8. Em Grupos de segurança, selecione os grupos de segurança para associar às interfaces de rede do endpoint. As regras do grupo de segurança deverão permitir o tráfego entre os recursos na VPC e as interfaces de rede do endpoint.
9. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
10. Escolha Criar endpoint.

Para configurar um endpoint da interface

Para obter mais informações sobre como configurar o agente para usar o endpoint da interface, consulte the section called “Configurar um endpoint da interface”.

Acesse dispositivos virtuais por meio de AWS PrivateLink

Você pode usar um Gateway Load Balancer para distribuir tráfego para uma frota de dispositivos virtuais de rede. Os dispositivos podem ser usados para inspeção de segurança, conformidade, controles de políticas e outros serviços de rede. Especifique o Gateway Load Balancer ao criar um serviço de endpoint da VPC. Outras entidades principais da AWS acessam o serviço de endpoint criando um endpoint do Gateway Load Balancer.

Preços

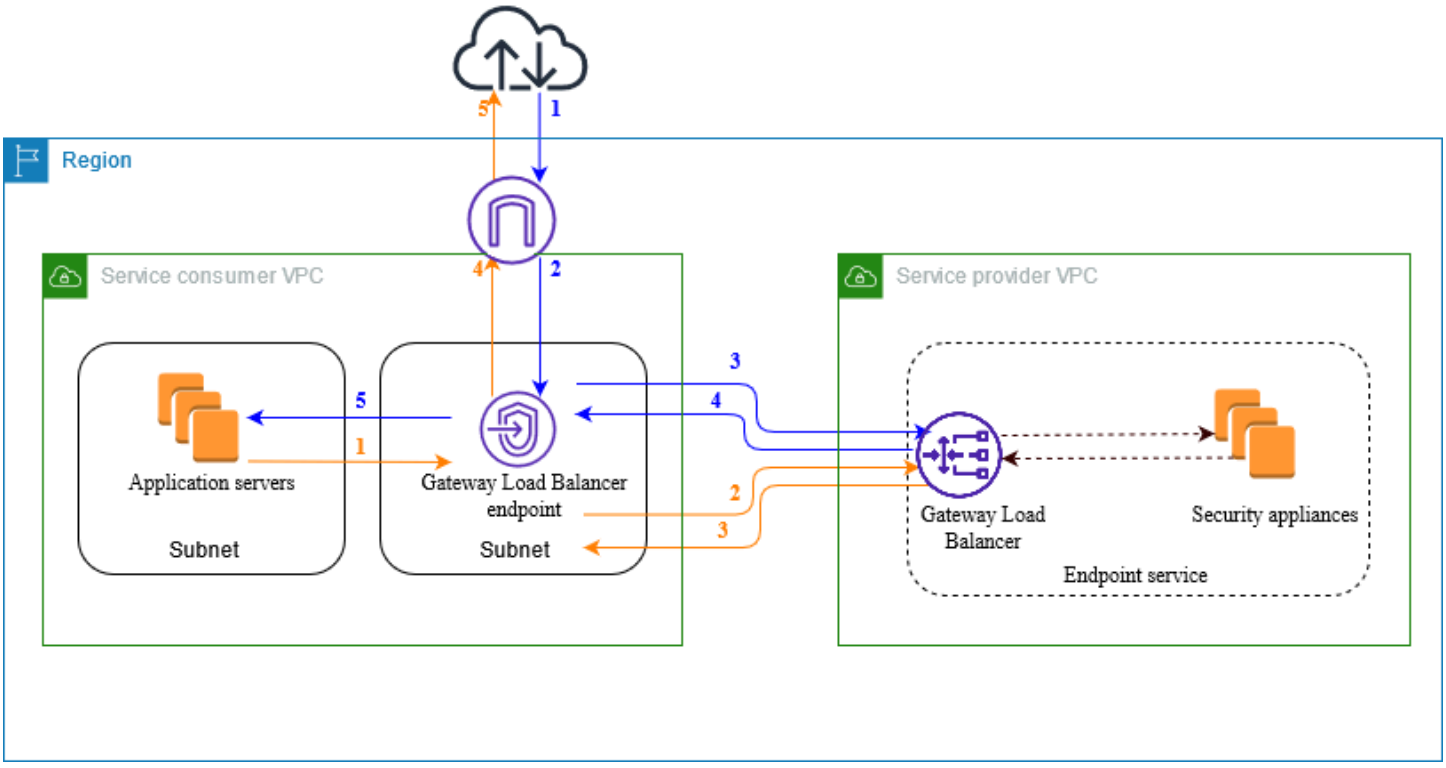
Você é cobrado por cada hora que seu endpoint do Gateway Load Balancer é provisionado em cada zona de disponibilidade. Você também é cobrado por GB de dados processados. Para obter mais informações, consulte AWS PrivateLink Preço.

Conteúdo

Para obter mais informações, consulte Balanceadores de carga de gateway.

Visão geral do

O diagrama a seguir mostra como os servidores de aplicativos acessam os dispositivos de segurança por meio de AWS PrivateLink. Os servidores de aplicações são executados em uma sub-rede da VPC do consumidor do serviço. Crie um endpoint do Gateway Load Balancer em outra sub-rede da mesma VPC. Todo o tráfego que entra na VPC do consumidor do serviço pelo gateway da Internet é encaminhado primeiro ao endpoint do Gateway Load Balancer para inspeção antes de ser encaminhado à sub-rede de destino. Da mesma forma, todo o tráfego que sai dos servidores da aplicação é encaminhado primeiro ao endpoint do Gateway Load Balancer para inspeção antes de ser encaminhado ao gateway da Internet.



Tráfego da Internet para os servidores de aplicações (setas azuis):

1. O tráfego entra na VPC do consumidor do serviço pelo gateway da Internet.
2. O tráfego é enviado ao endpoint do Gateway Load Balancer com base na configuração da tabela de rotas.
3. O tráfego é enviado ao Gateway Load Balancer para inspeção pelo dispositivo de segurança.
4. O tráfego é reencaminhado ao endpoint do Gateway Load Balancer após a inspeção.
5. O tráfego é enviado aos servidores de aplicações com base na configuração da tabela de rotas.

Tráfego dos servidores de aplicações para a Internet (setas laranja):

1. O tráfego é enviado ao endpoint do Gateway Load Balancer com base na configuração da tabela de rotas.
2. O tráfego é enviado ao Gateway Load Balancer para inspeção pelo dispositivo de segurança.
3. O tráfego é reencaminhado ao endpoint do Gateway Load Balancer após a inspeção.
4. O tráfego é enviado ao gateway da Internet com base na configuração da tabela de rotas.
5. O tráfego é reencaminhado à Internet.

Tipos de endereço IP

Os provedores de serviços podem disponibilizar os endpoints para consumidores de serviços por IPv4, IPv6 ou ambos, mesmo que os dispositivos de segurança ofereçam suporte apenas a IPv4. Se você habilitar o suporte dualstack, os consumidores existentes poderão continuar usando o IPv4 para acessar seu serviço, e os novos consumidores poderão optar por usar o IPv6 para acessar o serviço.

Se um endpoint de Gateway Load Balancer for compatível com IPv4, as interfaces de rede do endpoint terão endereços IPv4. Se um endpoint de Gateway Load Balancer for compatível com IPv6, as interfaces de rede do endpoint terão endereços IPv6. Não é possível acessar o endereço IPv6 de uma interface de rede de endpoint pela Internet. Se você descrever uma interface de rede de endpoint com um endereço IPv6, observe que `denyAllIgwTraffic` está habilitado.

Requisitos para habilitar IPv6 para um serviço de endpoint

- A VPC e as sub-redes do serviço de endpoint devem conter blocos CIDR IPv6 associados.
- Os Gateway Load Balancers do serviço de endpoint devem usar o tipo de endereço IP dualstack. Os dispositivos de segurança não precisam ser compatíveis com tráfego IPv6.

Requisitos para habilitar o IPv6 para um endpoint do Gateway Load Balancer

- O serviço de endpoint deve ter um tipo de endereço IP que inclua suporte a IPv6.
- O tipo de endereço IP de um Gateway Load Balancer deve ser compatível com as sub-redes do endpoint do Gateway Load Balancer, conforme descrito aqui:
  - IPv4: atribua endereços IPv4 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4.
  - IPv6: atribua endereços IPv6 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas forem sub-redes IPv6 apenas.
  - Dualstack: atribua endereços IPv4 e IPv6 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4 e IPv6.
- As tabelas de rotas para as sub-redes na VPC do consumidor de serviços devem rotear o tráfego IPv6 e as ACLs de rede para essas sub-redes devem permitir tráfego IPv6.

Roteamento

Para encaminhar o tráfego ao serviço de endpoint, especifique o endpoint do Gateway Load Balancer como destino nas tabelas de rotas usando o ID. No diagrama acima, adicione rotas às tabelas de rotas da seguinte forma. Ao usar um endpoint do Gateway Load Balancer como destino, não é possível especificar uma lista de prefixos como destino. Nessas tabelas, as rotas IPv6 estão incluídas para uma configuração de pilha dupla.

Tabela de rotas para o gateway da Internet

A tabela de rotas deve conter uma rota que envie o tráfego destinado aos servidores de aplicações ao endpoint do Gateway Load Balancer.

Destination (Destino)	Destino
VPC IPv4 CIDR	Local
VPC IPv6 CIDR	Local
Application subnet IPv4 CIDR	*vpc-endpoint-id*
Application subnet IPv6 CIDR	*vpc-endpoint-id*

Tabela de rotas para a sub-rede com os servidores de aplicações

A tabela de rotas deve conter uma rota que envie todo o tráfego dos servidores de aplicações ao endpoint do Gateway Load Balancer.

Destination (Destino)	Destino
VPC IPv4 CIDR	Local
VPC IPv6 CIDR	Local
0.0.0. 0/0	*vpc-endpoint-id*
::/0	*vpc-endpoint-id*

Tabela de rotas para a sub-rede com o endpoint do Gateway Load Balancer

Essa tabela de rotas deverá enviar o tráfego que é retornado da inspeção ao destino final. Para o tráfego proveniente da Internet, a rota local enviará o tráfego aos servidores de aplicações. Para o tráfego proveniente dos servidores de aplicações, adicione uma rota que envie todo o tráfego ao gateway da Internet.

Destination (Destino)	Destino
VPC IPv4 CIDR	Local
VPC IPv6 CIDR	Local
0.0.0. 0/0	*internet-gateway-id*
::/0	*internet-gateway-id*

Criar um sistema de inspeção como serviço de endpoint do Gateway Load Balancer

Você pode criar seu próprio serviço desenvolvido por AWS PrivateLink, conhecido como serviço de endpoint. Você é o provedor de serviços, e AWS os principais que criam conexões com seu serviço são os consumidores do serviço.

Os serviços de endpoint necessitam de um Network Load Balancer ou de um Gateway Load Balancer. Neste caso, você criará um serviço de endpoint usando um Gateway Load Balancer. Para obter mais informações sobre como criar um serviço de endpoint usando um Network Load Balancer, consulte Criar um serviço de endpoint.

Conteúdo

Considerações

- O serviço de endpoint está disponível na região em que você o criou.

- Ao recuperarem informações sobre um serviço de endpoint, os clientes podem ver somente as zonas de disponibilidade que têm em comum com o provedor de serviços. Quando o provedor de serviços e o consumidor do serviço estão em contas diferentes, um nome de zona de disponibilidade, como `us-east-1a`, pode ser mapeado para uma zona de disponibilidade física diferente em cada Conta da AWS. Você pode usar IDs de zonas de disponibilidade para identificar de forma consistente as zonas de disponibilidade do serviço. Para obter mais informações, consulte AZ IDs no Guia do usuário do Amazon EC2.
- Há cotas em seus AWS PrivateLink recursos. Para obter mais informações, consulte AWS PrivateLink cotas.

Pré-requisitos

- Crie uma VPC do provedor de serviços com pelo menos duas sub-redes na zona de disponibilidade na qual o serviço deverá ser disponibilizado. Uma sub-rede é destinada às instâncias do dispositivo de segurança, e a outra é destinada ao Gateway Load Balancer.
- Crie um Gateway Load Balancer na VPC do provedor de serviços. Se você planeja habilitar o suporte a IPv6 em seu serviço de endpoint, é necessário habilitar o suporte a dualstack em seu Gateway Load Balancer. Para obter mais informações, consulte Conceitos básicos do Gateway Load Balancers.
- Inicie os dispositivos de segurança na VPC do provedor de serviços e registre-os em um grupo de destino do balanceador de carga.

Criar o serviço de endpoint

Use o seguinte procedimento para criar um serviço de endpoint usando um Gateway Load Balancer.

Para criar um serviço de endpoint usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).
3. Escolha Create endpoint service (Criar serviço de endpoint).
4. Em Load balancer type (Tipo de load balancer), escolha Gateway.
5. Em Available load balancers (Balanceadores de carga disponíveis), selecione seu Gateway Load Balancer.

6. Em Require acceptance for endpoint (Exigir aceitação para o endpoint), selecione Acceptance required (Aceitação obrigatória) para exigir que as solicitações de conexão ao serviço de endpoint sejam aceitas manualmente. Caso contrário, elas serão aceitas automaticamente.
7. Em Supported IP address types (Tipos de endereço IP compatíveis), siga um destes procedimentos:
   - Selecionar IPv4: habilite o serviço de endpoint para aceitar solicitações IPv4.
   - Selecionar IPv6: habilite o serviço de endpoint para aceitar solicitações IPv6.
   - Selecionar IPv4 e IPv6: habilite o serviço de endpoint para aceitar solicitações IPv4 e IPv6.
8. (Opcional) Para adicionar uma tag, escolha Add new tag (Adicionar nova tag) e insira a chave e o valor da tag.
9. Escolha Criar.

Para criar um serviço de endpoint usando a linha de comando

- create-vpc-endpoint-service-configuration (AWS CLI)
- New-EC2VpcEndpointServiceConfiguration(Ferramentas para Windows PowerShell)

Disponibilizar o serviço de endpoint

Os provedores de serviços devem fazer o seguinte para disponibilizar seus serviços aos consumidores.

- Adicione permissões para que cada consumidor do serviço se conecte ao serviço de endpoint. Para obter mais informações, consulte the section called “Gerenciar permissões”.
- Forneça ao consumidor do serviço o nome do serviço e as zonas de disponibilidade compatíveis para que ele possa criar um endpoint da interface para se conectar ao serviço. Para obter mais informações, consulte o procedimento abaixo.
- Aceite a solicitação de conexão do endpoint do consumidor do serviço. Para obter mais informações, consulte the section called “Aceitar ou rejeitar solicitações de conexão”.

AWS os principais podem se conectar ao seu serviço de endpoint de forma privada criando um endpoint Gateway Load Balancer. Para obter mais informações, consulte Criar um endpoint do Gateway Load Balancer.

Acesse um sistema de inspeção usando um endpoint do Gateway Load Balancer

Você pode criar um endpoint do Gateway Load Balancer para se conectar aos serviços de endpoint do AWS PrivateLink.

Para cada sub-rede que você especifica em sua VPC, criamos uma interface de rede de endpoint na sub-rede e atribuímos a ela um endereço IP privado do intervalo de endereços da sub-rede. Uma interface de rede de endpoint é uma interface de rede gerenciada pelo solicitante; você pode visualizá-la no seu Conta da AWS, mas não pode gerenciá-la sozinho.

Você é cobrado pelas tarifas de uso por hora e processamento de dados. Para obter mais informações, consulte Preços de endpoint do balanceador de carga de gateway.

Conteúdo

Considerações

- É possível escolher apenas uma zona de disponibilidade na VPC do consumidor do serviço. Não será possível alterar essa sub-rede mais tarde. Para usar um endpoint do Gateway Load Balancer em uma sub-rede diferente, é necessário criar um novo endpoint do Gateway Load Balancer.
- Você pode criar um único endpoint do Gateway Load Balancer por zona de disponibilidade por serviço, mas é necessário selecionar a zona de disponibilidade compatível com o Gateway Load Balancer. Quando o provedor de serviços e o consumidor do serviço estão em contas diferentes, um nome de zona de disponibilidade, como `us-east-1a`, pode ser mapeado para uma zona de disponibilidade física diferente em cada Conta da AWS. Você pode usar IDs de zonas de disponibilidade para identificar de forma consistente as zonas de disponibilidade do serviço. Para obter mais informações, consulte AZ IDs no Guia do usuário do Amazon EC2.

- Antes de usar o serviço de endpoint, o provedor de serviços deverá aceitar as solicitações de conexão. O serviço não pode iniciar solicitações para recursos em sua VPC pelo endpoint da VPC. O endpoint retorna apenas respostas ao tráfego que foi iniciado por recursos em sua VPC.
- Cada endpoint do balanceador de carga do gateway é compatível com uma largura de banda de até 10 Gbps por zona de disponibilidade e pode aumentar a escala verticalmente para até 100 Gbps de modo automático.
- Se um serviço de endpoint estiver associado a vários Gateway Load Balancers, um endpoint do Gateway Load Balancer estabelecerá uma conexão com somente um balanceador de carga por zona de disponibilidade.
- Para manter o tráfego na mesma zona de disponibilidade, recomendamos criar um endpoint do Gateway Load Balancer em cada zona de disponibilidade para a qual você enviará tráfego.
- Não há suporte para a preservação de IP do cliente do Network Load Balancer quando o tráfego é encaminhado por meio de um endpoint do Gateway Load Balancer, mesmo que o destino esteja na mesma VPC que o Network Load Balancer.
- Se os servidores de aplicações e o endpoint do Gateway Load Balancer estiverem na mesma sub-rede, as regras de NACL serão avaliadas para o tráfego dos servidores de aplicações ao endpoint do Gateway Load Balancer.
- Se você usar um Gateway Load Balancer com um gateway de internet somente de saída, o tráfego IPv6 será descartado. Em vez disso, use um gateway de internet e regras de firewall de entrada.
- Há cotas em seus AWS PrivateLink recursos. Para obter mais informações, consulte AWS PrivateLink cotas.

Pré-requisitos

- Crie uma VPC do consumidor do serviço com pelo menos duas sub-redes na zona de disponibilidade na qual você acessará o serviço. Uma sub-rede é destinada aos servidores da aplicação, e a outra é destinada ao endpoint do Gateway Load Balancer.
- Para verificar quais zonas de disponibilidade são compatíveis com o serviço de endpoint, descreva o serviço de endpoint usando o console ou o comando describe-vpc-endpoint-services.
- Se os recursos estiverem em uma sub-rede com uma ACL de rede, verifique se a ACL de rede permite tráfego entre as interfaces de rede do endpoint e os recursos na VPC.

Criar o endpoint

Use o seguinte procedimento para criar um endpoint do Gateway Load Balancer que se conecte ao serviço de endpoint do sistema de inspeção.

Para criar um endpoint do Gateway Load Balancer usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Escolha Criar endpoint.
4. Em Tipo, escolha Serviços de endpoint que usam NLBs e GWLBs.
5. Em Service name (Nome do serviço), insira o nome do serviço e escolha Verify service (Verificar serviço).
6. Em VPC, selecione a VPC da qual você acessará o serviço de endpoint.
7. Em Sub-redes, selecione uma única sub-rede na qual será criada uma interface de rede de endpoint.
8. Em IP address type (Tipo de endereço IP), escolha uma das seguintes opções:
   - IPv4: atribua endereços IPv4 à interface de rede de endpoint. Essa opção será compatível somente se a sub-rede selecionada tiver um intervalo de endereços IPv4.
   - IPv6: atribua endereços IPv6 à interface de rede de endpoint. Essa opção será compatível somente se a sub-rede selecionada for uma sub-rede somente IPv6.
   - Pilha dupla: atribua endereços IPv4 e IPv6 à interface de rede de endpoint. Essa opção será compatível somente se a sub-rede selecionada tiver intervalos de endereços IPv4 e IPv6.
9. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
10. Escolha Criar endpoint. O status inicial é `pending acceptance`.

Para criar um endpoint do Gateway Load Balancer usando a linha de comando

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Configurar o roteamento

Use o seguinte procedimento para configurar as seguintes tabelas de rotas para a VPC do consumidor do serviço. Isso permite que os dispositivos de segurança realizem a inspeção de segurança do tráfego de entrada destinado aos servidores de aplicações. Para obter mais informações, consulte the section called “Roteamento”.

Para configurar o encaminhamento usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route Tables.
3. Selecione a tabela de rotas do gateway da Internet e faça o seguinte:
   a. Selecione Actions (Ações), Edit routes (Editar rotas).
   b. Se você oferece suporte a IPv4, escolha Add route (Adicionar rota). Em Destination (Destino), insira o bloco CIDR IPv4 da sub-rede para os servidores de aplicações. Em Target (Destino), selecione o endpoint da VPC.
   c. Se você oferece suporte a IPv6, escolha Add route (Adicionar rota). Em Destination (Destino), insira o bloco CIDR IPv6 da sub-rede para os servidores de aplicações. Em Target (Destino), selecione o endpoint da VPC.
   d. Escolha Salvar alterações.
4. Selecione a tabela de rotas para a sub-rede com os servidores de aplicações e faça o seguinte:
   a. Selecione Actions (Ações), Edit routes (Editar rotas).
   b. Se você oferece suporte a IPv4, escolha Add route (Adicionar rota). Em Destination, insira **`0.0.0.0/0`**. Em Target (Destino), selecione o endpoint da VPC.
   c. Se você oferece suporte a IPv6, escolha Add route (Adicionar rota). Em Destination, insira **`::/0`**. Em Target (Destino), selecione o endpoint da VPC.
   d. Escolha Salvar alterações.
5. Selecione a tabela de rotas para a sub-rede com o endpoint do Gateway Load Balancer e faça o seguinte:
   a. Selecione Actions (Ações), Edit routes (Editar rotas).
   b. Se você oferece suporte a IPv4, escolha Add route (Adicionar rota). Em Destination, insira **`0.0.0.0/0`**. Em Target (Destino), selecione o gateway da Internet.

c. Se você oferece suporte a IPv6, escolha Add route (Adicionar rota). Em Destination, insira **::/0**. Em Target (Destino), selecione o gateway da Internet.

d. Escolha Salvar alterações.

Para configurar o encaminhamento usando a linha de comando

- create-route (AWS CLI)
- New-EC2Route(Ferramentas para Windows PowerShell)

Gerenciar tags

Você pode marcar o endpoint do Gateway Load Balancer para ajudar a identificá-lo ou categorizá-lo de acordo com as necessidades da organização.

Para gerenciar etiquetas usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint da interface.
4. Selecione Ações, Gerenciar tags.
5. Para cada etiqueta a ser adicionada, escolha Add new tag (Adicionar nova etiqueta) e insira a chave e o valor da etiqueta.
6. Para remover uma etiqueta, escolha Remove (Remover) à direita da chave e do valor da etiqueta.
7. Escolha Salvar.

Para gerenciar etiquetas usando a linha de comando

- create-tags and delete-tags (AWS CLI)
- New-EC2Tage Remove-EC2Tag(Ferramentas para Windows PowerShell)

Excluir um endpoint do Gateway Load Balancer

Quando não precisar mais de um endpoint, você poderá excluí-lo. A exclusão de um endpoint do Gateway Load Balancer também exclui as interfaces de rede de endpoint. Não será possível excluir

um endpoint do Gateway Load Balancer se houver rotas nas tabelas de rotas que apontem para o endpoint.

Para excluir um endpoint do Gateway Load Balancer

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints e selecione o seu endpoint.
3. Escolha Actions, Delete Endpoint.
4. Na tela de confirmação, escolha Yes, Delete.

Para excluir um endpoint do Gateway Load Balancer

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint (AWS Tools for Windows PowerShell)

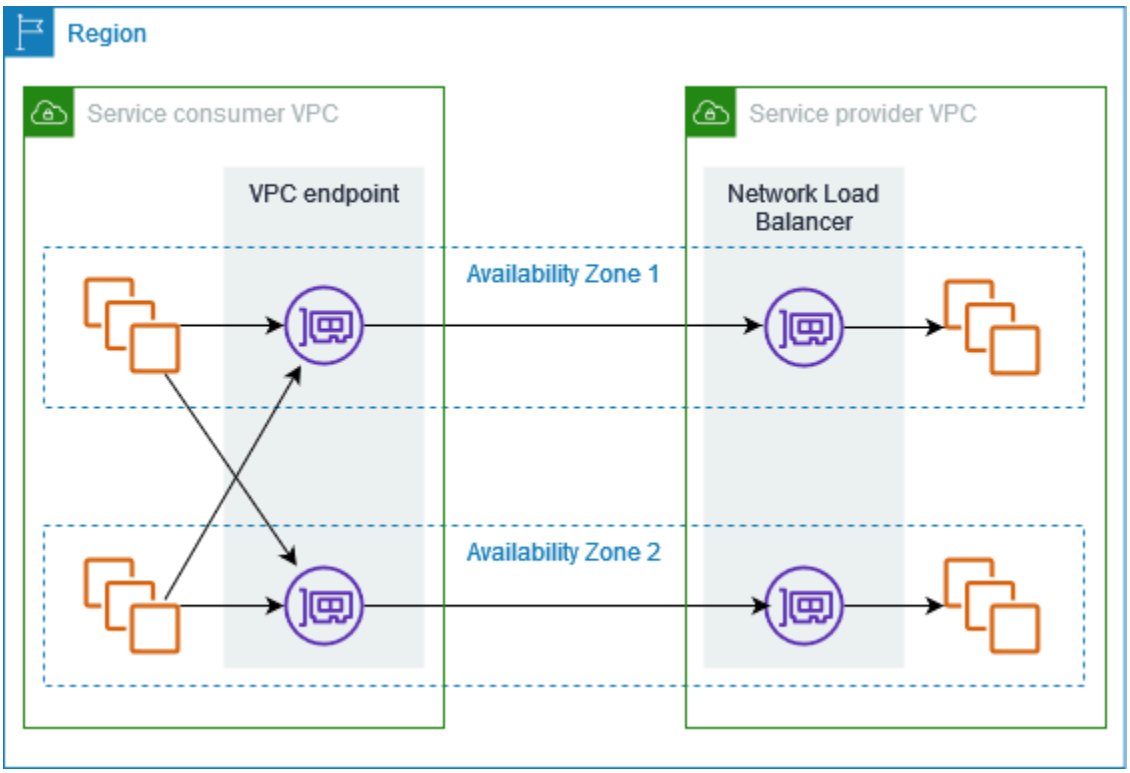
Compartilhe seus serviços por meio de AWS PrivateLink

Você pode hospedar seu próprio serviço AWS PrivateLink motorizado, conhecido como serviço de endpoint, e compartilhá-lo com outros AWS clientes.

Conteúdo

Visão geral do

O diagrama a seguir mostra como você compartilha seu serviço hospedado AWS com outros AWS clientes e como esses clientes se conectam ao seu serviço. Como provedor de serviços, crie um Network Load Balancer em sua VPC como o front-end do serviço. Em seguida, selecione esse balanceador de carga ao criar a configuração do serviço de endpoint da VPC. Conceda permissão a entidades principais da AWS específicas para que elas possam se conectar ao serviço. Como consumidor do serviço, o cliente cria um endpoint da VPC de interface, que estabelece conexões entre as sub-redes que ele selecionou da VPC e o serviço de endpoint. O balanceador de carga recebe solicitações do consumidor do serviço e as encaminha aos destinos que hospedam o serviço.



Para garantir baixa latência e alta disponibilidade, recomenda-se disponibilizar o serviço em pelo menos duas zonas de disponibilidade.

Nomes de hosts DNS

Quando um provedor de serviços cria um serviço de endpoint VPC, AWS gera um nome de host DNS específico do endpoint para o serviço. Esses nomes apresentam a seguinte sintaxe:

```
endpoint_service_id.region.vpce.amazonaws.com
```

Veja a seguir um exemplo de nome de host de DNS para um serviço de endpoint da VPC na região us-east-2:

```
vpce-svc-071afff70666e61e0.us-east-2.vpce.amazonaws.com
```

Quando um consumidor do serviço cria um endpoint da VPC de interface, criamos nomes DNS regionais e zonais que o consumidor do serviço pode usar para se comunicar com o serviço de endpoint. Os nomes regionais apresentam a seguinte sintaxe:

```
endpoint_id.endpoint_service_id.service_region.vpce.amazonaws.com
```

Os nomes zonais apresentam a seguinte sintaxe:

```
endpoint_id-endpoint_zone.endpoint_service_id.service_region.vpce.amazonaws.com
```

DNS privado

Um provedor de serviços também pode associar um nome DNS privado ao serviço de endpoint para que os consumidores possam continuar acessando o serviço com o nome DNS existente. Se um provedor de serviços tiver associado um nome de DNS privado ao serviço de endpoint, os consumidores do serviço poderão habilitar nomes de DNS privados para seus endpoints de interface. Se um provedor de serviços não habilitar o DNS privado, talvez os consumidores do serviço precisem atualizar suas aplicações para usar o nome de DNS público para o serviço de endpoint da VPC. Para obter mais informações, consulte Gerenciar nomes DNS.

Zonas de disponibilidade e sub-redes

O serviço de endpoint está disponível nas zonas de disponibilidade que você habilita para o Network Load Balancer. Para garantir alta disponibilidade e resiliência, recomendamos que você habilite o balanceador de carga em pelo menos duas zonas de disponibilidade, implante instâncias do EC2 em todas as zonas habilitadas e registre essas instâncias no grupo de destino do balanceador de carga.

Você pode habilitar o balanceamento de carga entre zonas como alternativa a hospedar o serviço de endpoint em várias zonas de disponibilidade. Porém, os consumidores perderão o acesso ao serviço de endpoint em ambas as zonas se houver falha na zona que hospeda o serviço. Considere também que, quando você habilita o balanceamento de carga entre zonas para um Network Load Balancer, as tarifas de transferência de dados do EC2 se aplicam.

O consumidor pode criar endpoints da VPC de interface nas zonas de disponibilidade em que o serviço de endpoint está disponível. Criaremos uma interface de rede de endpoint em cada sub-rede que o cliente configurar para o endpoint da VPC. Atribuímos endereços IP a cada interface de rede de endpoint a partir de sua sub-rede, com base no tipo de endereço IP do endpoint da VPC. Quando uma solicitação usa o endpoint regional para o serviço de endpoint da VPC, selecionamos uma interface de rede de endpoint íntegra utilizando o algoritmo round robin para alternar entre as interfaces de rede em diferentes zonas de disponibilidade. Em seguida, resolvemos o tráfego para o endereço IP da interface de rede do endpoint selecionada.

O consumidor poderá usar os endpoints zonais para o endpoint da VPC se for melhor para seu caso de uso manter o tráfego na mesma zona de disponibilidade.

Cross-Region acesso

Um provedor de serviço pode hospedar um serviço em uma região e disponibilizá-lo em um conjunto de regiões compatíveis. O consumidor de um serviço seleciona uma região de serviço ao criar um endpoint.

Permissões

- Por padrão, as entidades do IAM não têm permissão para disponibilizar um serviço de endpoint em várias regiões nem para acessar um serviço de endpoint inter-regional. Para conceder as permissões necessárias para acesso inter-regional, um administrador do IAM pode criar políticas do IAM que permitam a ação de permissão somente `vpce:AllowMultiRegion`.
- Para controlar as regiões que uma entidade do IAM pode especificar como uma região compatível ao criar um serviço de endpoint, use a chave de condição `ec2:VpceSupportedRegion`.
- Para controlar as regiões que uma entidade do IAM pode especificar como uma região de serviço ao criar um endpoint da VPC, use a chave de condição `ec2:VpceServiceRegion`.

Considerações

- Um provedor de serviço deve fazer a opção por uma região opcional antes de adicioná-la como uma região compatível para um serviço de endpoint.
- O serviço de endpoint deve ser acessado da região em que está hospedado. Você não pode remover a região hospedeira do conjunto de regiões compatíveis. Para garantir redundância, é possível implantar o serviço de endpoint em várias regiões e habilitar o acesso inter-regional para cada serviço de endpoint.
- Um consumidor de serviço deve fazer a opção por uma região opcional antes de selecioná-la como uma região de serviço para um endpoint. Sempre que possível, recomendamos que os consumidores de serviços acessem um serviço usando a conectividade intrarregional em vez da conectividade entre regiões. Intra-Region a conectividade fornece menor latência e custos mais baixos.
- Se um provedor de serviço remover uma região do conjunto de regiões compatíveis, os consumidores do serviço não poderão selecionar essa região como a região de serviço ao criar novos endpoints. Observe que isso não afeta o acesso ao serviço de endpoint a partir de endpoints existentes que usam essa região como a região de serviço.

- Para alta disponibilidade, os provedores devem usar pelo menos duas zonas de disponibilidade. Cross-Region o acesso não exige que provedores e consumidores usem as mesmas zonas de disponibilidade.
- Cross-Region o acesso não é suportado nas seguintes zonas de disponibilidade: `use1-az3` `usw1-az2apne1-az3`,`apne2-az2`,, `apne2-az4` e.
- Com o acesso entre regiões, AWS PrivateLink gerencia o failover entre as zonas de disponibilidade. Ele não gerencia o failover inter-regional.
- Cross-Region o acesso não é suportado para balanceadores de carga de rede com um valor personalizado configurado para o tempo limite de inatividade do TCP.
- Cross-Region o acesso não é suportado com a fragmentação UDP.
- Cross-Region o acesso só é suportado para serviços por meio dos quais você compartilha AWS PrivateLink.

Tipos de endereço IP

Os provedores de serviços podem disponibilizar os endpoints para consumidores de serviços por IPv4, IPv6 ou ambos, mesmo que os servidores de backend ofereçam suporte apenas ao IPv4. Se você habilitar o suporte dualstack, os consumidores existentes poderão continuar usando o IPv4 para acessar seu serviço, e os novos consumidores poderão optar por usar o IPv6 para acessar o serviço.

Se um endpoint da VPC de interface for compatível com IPv4, as interfaces de rede do endpoint terão endereços IPv4. Se um endpoint da VPC de interface for compatível com IPv6, as interfaces de rede do endpoint terão endereços IPv6. Não é possível acessar o endereço IPv6 de uma interface de rede de endpoint pela Internet. Se você descrever uma interface de rede de endpoint com um endereço IPv6, observe que `denyAllIgwTraffic` está habilitado.

Requisitos para habilitar IPv6 para um serviço de endpoint

- A VPC e as sub-redes do serviço de endpoint devem conter blocos CIDR IPv6 associados.
- Todos os Network Load Balancers do serviço de endpoint devem usar o tipo de endereço IP dualstack. Os destinos não precisam ser compatíveis com tráfego IPv6. Se o serviço processar endereços IP de origem do cabeçalho do protocolo proxy versão 2, deverá processar endereços IPv6.

Requisitos para habilitar IPv6 para um endpoint de interface

- O serviço de endpoint precisa ser compatível com solicitações IPv6.
- O tipo de endereço IP de um endpoint da interface deve ser compatível com as sub-redes do endpoint da interface, conforme descrito aqui:
  - IPv4: atribua endereços IPv4 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4.
  - IPv6: atribua endereços IPv6 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas forem sub-redes IPv6 apenas.
  - Dualstack: atribua endereços IPv4 e IPv6 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4 e IPv6.

Tipo de endereço IP do registro DNS para um endpoint da interface

O tipo de endereço IP do registro DNS compatível com um endpoint da interface determina os registros DNS que criamos. O tipo de endereço IP do registro DNS de um endpoint de interface deve ser compatível com o tipo de endereço IP do endpoint da interface, conforme descrito aqui:

- IPv4: crie registros A para nomes DNS privados, regionais e zonais. O tipo de endereço IP deve ser IPv4 ou Dualstack.
- IPv6: crie registros AAAA para nomes DNS privados, regionais e zonais. O tipo de endereço IP deve ser IPv6 ou Dualstack.
- Dualstack: crie registros A e AAAA para nomes DNS privados, regionais e zonais. O tipo de endereço IP deve ser Dualstack.

Crie um serviço desenvolvido por AWS PrivateLink

Você pode criar seu próprio serviço desenvolvido por AWS PrivateLink, conhecido como serviço de endpoint. Você é o provedor de serviços, e as entidades principais da AWS que criam conexões ao serviço são os consumidores do serviço.

Os serviços de endpoint necessitam de um Network Load Balancer ou de um Gateway Load Balancer. O balanceador de carga recebe solicitações de consumidores do serviço e as encaminha ao serviço. Neste caso, você criará um serviço de endpoint usando um Network Load Balancer.

Para obter mais informações sobre como criar um serviço de endpoint usando um Gateway Load Balancer, consulte Acessar dispositivos virtuais.

Conteúdo

Considerações

- O serviço de endpoint está disponível na região em que você o criou. Os consumidores poderão acessar seu serviço de outras regiões se você habilitar o acesso inter-regional ou se usarem emparelhamento de VPC ou um gateway de trânsito.
- Ao recuperarem informações sobre um serviço de endpoint, os clientes podem ver somente as zonas de disponibilidade que têm em comum com o provedor de serviços. Quando o provedor de serviços e o consumidor do serviço estão em contas diferentes, um nome de zona de disponibilidade, como `us-east-1a`, pode ser mapeado para uma zona de disponibilidade física diferente em cada Conta da AWS. Você pode usar IDs de zonas de disponibilidade para identificar de forma consistente as zonas de disponibilidade do serviço. Para obter mais informações, consulte AZ IDs no Guia do usuário do Amazon EC2.
- Quando os consumidores do serviço enviarem tráfego a um serviço por meio de um endpoint da interface, os endereços IP de origem fornecidos para a aplicação serão os endereços IP privados dos nós do balanceador de carga, e não os endereços IP dos consumidores do serviço. Se habilitar o protocolo proxy no balanceador de carga, você poderá obter os endereços dos consumidores do serviço e os IDs dos endpoints da interface no cabeçalho do protocolo proxy. Para mais informações, consulte Protocolo proxy no Guia do usuário de Network Load Balancers.
- Um Network Load Balancer pode ser associado a um único serviço de endpoint, mas um serviço de endpoint pode ser associado a vários Network Load Balancers.
- Se um serviço de endpoint for associado a vários Network Load Balancers, cada interface de rede de endpoint estará associado a um balanceador de carga. Quando a primeira conexão de uma interface de rede de endpoint é iniciada, selecionamos aleatoriamente um Network Load Balancer na mesma zona de disponibilidade da interface de rede do endpoint. Todas as solicitações de conexão subsequentes dessa interface de rede de endpoint usam o balanceador

de carga selecionado. Recomendamos que você use a mesma configuração de receptor e grupo de destino para todos os balanceadores de carga de um serviço de endpoint, para que os consumidores possam usar o serviço de endpoint com sucesso, independentemente do balanceador de carga escolhido.

- Há cotas em seus AWS PrivateLink recursos. Para obter mais informações, consulte AWS PrivateLink cotas.

Pré-requisitos

- Crie uma VPC do serviço de endpoint com pelo menos uma sub-rede em cada zona de disponibilidade em que o serviço deverá ser disponibilizado.
- Para permitir que os consumidores do serviço criem endpoints da VPC de interface IPv6 para o serviço de endpoint, a VPC e as sub-redes devem ter blocos CIDR IPv6 associados.
- Crie um Network Load Balancer na VPC. Selecione uma sub-rede em cada zona de disponibilidade em que o serviço deverá estar disponível para os consumidores do serviço. Para obter baixa latência e tolerância a falhas, recomenda-se disponibilizar o serviço em pelo menos duas zonas de disponibilidade na região.
- Se o Network Load Balancer tiver um grupo de segurança, ele deverá permitir o tráfego de entrada dos endereços IP dos clientes. Como alternativa, você pode desativar a avaliação das regras do grupo de segurança de entrada para o tráfego de passagem AWS PrivateLink. Para mais informações, consulte Grupos de segurança no Manual do usuário de Network Load Balancers.
- Para permitir que o serviço de endpoint aceite solicitações IPv6, os Network Load Balancers devem usar o tipo de endereço IP dualstack. Os destinos não precisam ser compatíveis com tráfego IPv6. Para mais informações, consulte IP address type (Tipo de endereço IP) no Manual do usuário de Network Load Balancers.

  Se você processar endereços IP de origem do cabeçalho do protocolo proxy versão 2, verifique se é possível processar endereços IPv6.
- Inicie instâncias em cada zona de disponibilidade em que o serviço deverá estar disponível e registre-as em um grupo de destino do balanceador de carga. Se você não executar instâncias em todas as zonas de disponibilidade habilitadas, poderá habilitar o balanceamento de carga entre zonas para oferecer suporte aos consumidores de serviços que usam nomes de host DNS zonais para acessar o serviço. Aplicam-se cobranças de transferência de dados regionais quando o balanceamento de carga entre zonas está habilitado. Para obter mais informações, consulte balanceamento de Cross-zone carga no Guia do usuário para balanceadores de carga de rede.

Criar um serviço de endpoint

Use o seguinte procedimento para criar um serviço de endpoint usando um Network Load Balancer.

Para criar um serviço de endpoint usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).
3. Escolha Create endpoint service (Criar serviço de endpoint).
4. Em Load balancer type (Tipo de balanceador de carga), escolha Network (Rede).
5. Em Available load balancers (Balanceadores de carga disponíveis), selecione os balanceadores de carga de rede para associar ao serviço de endpoint. Para ver as zonas de disponibilidade que estão habilitadas para o balanceador de carga selecionado, consulte Details of selected load balancers, Included Availability Zones. Seu serviço de endpoint estará disponível nessas zonas de disponibilidade.
6. (Opcional) Para disponibilizar o serviço de endpoint em regiões diferentes daquele em que ele está hospedado, selecione-as em Regiões do serviço. Para obter mais informações, consulte the section called “Cross-Region acesso”.
7. Em Require acceptance for endpoint (Exigir aceitação para o endpoint), selecione Acceptance required (Aceitação obrigatória) para exigir que as solicitações de conexão ao serviço de endpoint sejam aceitas manualmente. Senão, essas solicitações serão aceitas automaticamente.
8. Em Enable private DNS name (Habilitar nome DNS privado), selecione Associate a private DNS name with the service (Associar um nome DNS privado ao serviço) para associar um nome DNS privado que os consumidores podem usar para acessar seu serviço e insira o nome DNS privado. Caso contrário, os consumidores do serviço podem usar o nome DNS específico do endpoint fornecido por. AWS Antes que os consumidores do serviço possam usar o nome DNS, o provedor de serviços deve verificar se eles são proprietários do domínio. Para obter mais informações, consulte Gerenciar nomes DNS.
9. Em Supported IP address types (Tipos de endereço IP compatíveis), siga um destes procedimentos:

   - Selecionar IPv4: habilite o serviço de endpoint para aceitar solicitações IPv4.
   - Selecionar IPv6: habilite o serviço de endpoint para aceitar solicitações IPv6.
   - Selecionar IPv4 e IPv6: habilite o serviço de endpoint para aceitar solicitações IPv4 e IPv6.

10. (Opcional) Para adicionar uma tag, escolha Add new tag (Adicionar nova tag) e insira a chave e o valor da tag.
11. Escolha Criar.

Para criar um serviço de endpoint usando a linha de comando

- create-vpc-endpoint-service-configuration (AWS CLI)
- New-EC2VpcEndpointServiceConfiguration(Ferramentas para Windows PowerShell)

Disponibilizar o serviço de endpoint aos consumidores do serviço

AWS os diretores podem se conectar ao seu serviço de endpoint de forma privada criando uma interface VPC endpoint. Os provedores de serviços devem fazer o seguinte para disponibilizar seus serviços aos consumidores.

- Adicione permissões para que cada consumidor do serviço se conecte ao serviço de endpoint. Para obter mais informações, consulte the section called “Gerenciar permissões”.
- Forneça ao consumidor do serviço o nome do serviço e as zonas de disponibilidade compatíveis para que ele possa criar um endpoint da interface para se conectar ao serviço. Para obter mais informações, consulte the section called “Conectar-se a um serviço de endpoint como consumidor do serviço”.
- Aceite a solicitação de conexão do endpoint do consumidor do serviço. Para obter mais informações, consulte the section called “Aceitar ou rejeitar solicitações de conexão”.

Conectar-se a um serviço de endpoint como consumidor do serviço

Um consumidor do serviço usa o seguinte procedimento para criar um endpoint da interface para se conectar ao serviço de endpoint.

Para criar um endpoint da interface usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Escolha Criar endpoint.
4. Em Tipo, escolha Serviços de endpoint que usam NLBs e GWLBs.

5. Em Nome do serviço, insira o nome do serviço (por exemplo, `com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`) e escolha Verificar serviço.
6. (Opcional) Para se conectar a um serviço de endpoint que esteja disponível em uma região diferente da região do endpoint, selecione Região do serviço, Habilitar endpoint inter-regional e depois selecione a região. Para obter mais informações, consulte the section called “Cross-Region acesso”.
7. Em VPC, selecione a VPC da qual você acessará o serviço de endpoint.
8. Em Sub-redes, selecione as sub-redes nas quais serão criadas as interfaces de rede de endpoint.
9. Em IP address type (Tipo de endereço IP), escolha uma das seguintes opções:
   - IPv4: atribua endereços IPv4 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4 e o serviço de endpoint aceitar solicitações de IPv4.
   - IPv6: atribua endereços IPv6 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv6 e o serviço de endpoint aceitar solicitações de IPv6.
   - Pilha dupla: atribua endereços IPv4 e IPv6 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de ambos os endereços IPv4 e IPv6 e o serviço de endpoint aceitar solicitações de ambos IPv4 e IPv6.
10. Em DNS record IP type (Tipo de IP de registro DNS), escolha uma das seguintes opções:
    - IPv4: crie registros A para nomes DNS privados, regionais e zonais. O tipo de endereço IP deve ser IPv4 ou Dualstack.
    - IPv6: crie registros AAAA para nomes DNS privados, regionais e zonais. O tipo de endereço IP deve ser IPv6 ou Dualstack.
    - Dualstack: crie registros A e AAAA para nomes DNS privados, regionais e zonais. O tipo de endereço IP deve ser Dualstack.
    - Serviço definido: crie registros A para os nomes DNS privados, regionais e zonais e registros AAAA para os nomes DNS regionais e zonais. O tipo de endereço IP deve ser Dualstack.
11. Para Security group (Grupo de segurança), selecione os grupos de segurança para associar às interfaces de rede do endpoint.
12. Escolha Criar endpoint.

Para criar um endpoint da interface usando a linha de comando

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Configurar um serviço de endpoint

Depois de criar um serviço de endpoint, você pode atualizar a configuração.

Tarefas

- Gerenciar permissões
- Aceitar ou rejeitar solicitações de conexão
- Manage load balancers (Gerenciar balanceadores de carga)
- Associar um nome DNS privado
- Modificar as regiões compatíveis
- Modificar os tipos de endereço IP compatíveis
- Gerenciar tags

Gerenciar permissões

A combinação de permissões e configurações de aceitação ajuda você a controlar quais consumidores de serviços (AWS diretores) podem acessar seu serviço de endpoint. Por exemplo, é possível conceder permissões a entidades principais específicas em que você confia e aceitar automaticamente todas as solicitações de conexão ou conceder permissões a um grupo maior de entidades principais e aceitar manualmente as solicitações de conexão específicas em que você confia.

Por padrão, o serviço de endpoint não está disponível aos consumidores do serviço. Você deve adicionar permissões que permitam que AWS diretores específicos criem uma interface VPC endpoint para se conectar ao seu serviço de endpoint. Para adicionar permissões para um AWS diretor, você precisa do Amazon Resource Name (ARN). A lista a seguir inclui os ARNs de exemplo das entidades principais da AWS aceitas.

ARNs para diretores AWS

Conta da AWS (inclui todos os diretores na conta)

arn:aws:iam: ::root *account_id*

Perfil

arn:aws:iam: ::role/ *account_id role_name*

Usuário

arn:aws:iam: ::usuário/ *account_id user_name*

Todos os diretores ao todo Contas da AWS

*

Considerações

- Se você conceder permissão a todos para acessar o serviço de endpoint e configurar o serviço de endpoint para aceitar todas as solicitações, seu balanceador de carga será público, mesmo que não tenha um endereço IP público.
- Se você remover as permissões, isso não afetará as conexões existentes entre o endpoint e o serviço que foram aceitas anteriormente.

Para gerenciar as permissões para o serviço de endpoint usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).
3. Selecione o serviço de endpoint e escolha a guia Allow principals (Permitir entidades principais).
4. Para adicionar permissões, escolha Allow principals (Permitir entidades principais). Em Principals to add, (Entidades principais a serem adicionadas), insira o ARN da entidade principal. Para adicionar outra entidade principal, escolha Add principal (Adicionar principal). Quando terminar de adicionar as entidades principais, escolha Allow principals (Permitir entidades principais).
5. Para remover permissões, selecione a entidade principal e escolha Actions (Ações), Delete (Excluir). Quando a confirmação for solicitada, insira **`delete`** e selecione Excluir.

Para adicionar permissões para o serviço de endpoint usando a linha de comando

- modify-vpc-endpoint-service-permissions (AWS CLI)
- Edit-EC2EndpointServicePermission(Ferramentas para Windows PowerShell)

Aceitar ou rejeitar solicitações de conexão

A combinação de permissões e configurações de aceitação ajuda você a controlar quais consumidores de serviços (AWS diretores) podem acessar seu serviço de endpoint. Por exemplo, é possível conceder permissões a entidades principais específicas em que você confia e aceitar automaticamente todas as solicitações de conexão ou conceder permissões a um grupo maior de entidades principais e aceitar manualmente as solicitações de conexão específicas em que você confia.

É possível configurar o serviço de endpoint para aceitar solicitações de conexão automaticamente. Senão, será necessário aceitá-los ou rejeitá-los manualmente. Se você não aceitar uma solicitação de conexão, o consumidor do serviço não poderá acessar o serviço de endpoint.

Se você conceder permissão a todos para acessar o serviço de endpoint e configurar o serviço de endpoint para aceitar todas as solicitações, seu balanceador de carga será público, mesmo que não tenha um endereço IP público.

É possível receber uma notificação quando uma solicitação de conexão é aceita ou rejeitada. Para obter mais informações, consulte the section called “Receber alertas para eventos de serviço de endpoint”.

Para modificar a configuração de aceitação usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).
3. Selecione o serviço de endpoint.
4. Escolha Actions, Modify endpoint acceptance setting.
5. Selecionar ou desmarcar Acceptance required (Aceitação obrigatória).
6. Selecione Save changes (Salvar alterações)

Para modificar a configuração de aceitação usando a linha de comando

- modify-vpc-endpoint-service-configuration (AWS CLI)
- Edit-EC2VpcEndpointServiceConfiguration(Ferramentas para Windows PowerShell)

Para aceitar ou rejeitar uma solicitação de conexão usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).
3. Selecione o serviço de endpoint.
4. Na guia Endpoint connections (Conexões de endpoint), selecione a conexão de endpoint.
5. Para aceitar a solicitação de conexão, escolha Actions (Ações), Accept endpoint connection request (Aceitar solicitação de conexão de endpoint). Quando a confirmação for solicitada, insira **`accept`** e escolha Accept (Aceitar).
6. Para rejeitar a solicitação de conexão, escolha Actions (Ações),Reject endpoint connection request (Rejeitar solicitação de conexão de endpoint). Quando a confirmação for solicitada, insira **`reject`** e escolha Reject (Rejeitar).

Para aceitar ou rejeitar uma solicitação de conexão usando a linha de comando

- accept-vpc-endpoint-connections ou reject-vpc-endpoint-connections (AWS CLI)
- Approve-EC2EndpointConnectionou Deny-EC2EndpointConnection(Ferramentas para Windows PowerShell)

Manage load balancers (Gerenciar balanceadores de carga)

É possível gerenciar os balanceadores de carga associados ao serviço de endpoint. Não será possível dissociar um balanceador de carga se houver endpoints conectados ao serviço de endpoint.

Se você habilitar outra zona de disponibilidade para os balanceadores de carga, a zona de disponibilidade aparecerá na guia Balanceadores de carga na página Serviços de endpoint. Porém, ela não estará habilitada para o serviço de endpoint nem listada na guia Detalhes do serviço de endpoint no Console de gerenciamento da AWS. Você precisará habilitar o serviço de endpoint para a nova zona de disponibilidade.

Pode levar alguns minutos para que a zona de disponibilidade do balanceador de carga esteja pronta para o serviço de endpoint. Se você estiver usando uma automação, recomendamos que adicione uma espera ao processo de automação antes de habilitar o serviço de endpoint para a nova zona de disponibilidade.

Para gerenciar os balanceadores de carga para o serviço de endpoint usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).
3. Selecione o serviço de endpoint.
4. Escolha Actions (Ações), Associate or disassociate load balancers (Associar ou desassociar balanceadores de carga).
5. Alterar a configuração do serviço do endpoint conforme necessário. Por exemplo:
   - Marque a caixa de seleção para um balanceador de carga e associe-o ao serviço de endpoint.
   - Limpe a caixa de seleção de um balanceador de carga para desassociá-lo do serviço de endpoint. Você deve manter pelo menos um balanceador de carga selecionado.
6. Selecione Save changes (Salvar alterações)

   O serviço de endpoint será habilitado para todas as novas zonas de disponibilidade adicionadas ao balanceador de carga. A nova zona de disponibilidade está listada na guia Balanceadores de carga e na guia Detalhes do serviço de endpoint.

Depois de habilitar uma zona de disponibilidade para o serviço de endpoint, os consumidores do serviço podem adicionar uma sub-rede nessa zona de disponibilidade aos endpoint de VPC da interface.

Para gerenciar os balanceadores de carga para o serviço de endpoint usando a linha de comando

- modify-vpc-endpoint-service-configuration (AWS CLI)
- Edit-EC2VpcEndpointServiceConfiguration(Ferramentas para Windows PowerShell)

Para habilitar o serviço de endpoint em uma zona de disponibilidade que foi habilitada recentemente para o balanceador de carga, basta chamar o comando com o ID do serviço de endpoint.

Associar um nome DNS privado

É possível associar um nome DNS privado ao serviço de endpoint. Após associar um nome de DNS privado, você deverá atualizar a entrada para o domínio no servidor de DNS. Antes que os consumidores do serviço possam usar o nome DNS, o provedor de serviços deve verificar se eles são proprietários do domínio. Para obter mais informações, consulte Gerenciar nomes DNS.

Para modificar um nome de DNS privado do serviço de endpoint usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).
3. Selecione o serviço de endpoint.
4. Escolha Actions (Ações), Modify private DNS name (Modificar nome DNS privado).
5. Selecione Associate a private DNS name with the service (Associar um nome DNS privado ao serviço) e insira o nome DNS privado.
   - Os nomes de domínio devem usar letras minúsculas.
   - Você pode usar curingas em nomes de domínio (por exemplo, **`*.myexampleservice.com`**).
6. Escolha Salvar alterações.
7. O nome DNS privado está pronto para ser usado pelos consumidores do serviço quando o status de verificação é verified (verificado). Se o status da verificação for alterado, as novas solicitações de conexão serão negadas, mas as conexões existentes não serão afetadas.

Para modificar um nome de DNS privado do serviço de endpoint usando a linha de comando

- modify-vpc-endpoint-service-configuration (AWS CLI)
- Edit-EC2VpcEndpointServiceConfiguration(Ferramentas para Windows PowerShell)

Para iniciar o processo de verificação de domínio usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).
3. Selecione o serviço de endpoint.
4. Escolha Actions (Ações), Verify domain ownership for private DNS name (Verificar a propriedade do domínio para o nome DNS privado).

5. Quando a confirmação for solicitada, insira **`verify`** e escolha Verify (Verificar).

Para iniciar o processo de verificação de domínio usando a linha de comando

- start-vpc-endpoint-service-private-dns-verification (AWS CLI)
- Start-EC2VpcEndpointServicePrivateDnsVerification(Ferramentas para Windows PowerShell)

Modificar as regiões compatíveis

Você pode modificar o conjunto de regiões compatíveis com o serviço de endpoint. Antes de adicionar uma região opcional, você precisa optar por ela. Você não pode remover a região que hospeda o serviço de endpoint.

Depois que você remove uma região, os consumidores do serviço não podem criar novos endpoints que a especifiquem como a região do serviço. A remoção de uma região não afeta os endpoints existentes que a especificam como a região do serviço. Ao remover uma região, recomendamos que você rejeite todas as conexões de endpoint existentes dessa região.

Para modificar as regiões compatíveis com o serviço de endpoint

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).
3. Selecione o serviço de endpoint.
4. Escolha Ações, Modificar regiões compatíveis.
5. Selecione e desmarque as regiões conforme necessário.
6. Escolha Salvar alterações.

Modificar os tipos de endereço IP compatíveis

Você pode alterar os tipos de endereço IP que são compatíveis com seu serviço de endpoint.

Consideração

Para permitir que o serviço de endpoint aceite solicitações IPv6, os Network Load Balancers devem usar o tipo de endereço IP dualstack. Os destinos não precisam ser compatíveis com tráfego IPv6. Para mais informações, consulte IP address type (Tipo de endereço IP) no Manual do usuário de Network Load Balancers.

Para modificar os tipos de endereço IP compatíveis usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).
3. Selecione o serviço de endpoint da VPC.
4. Escolha Actions (Ações), Modify supported IP address types (Modificar os tipos de endereço IP compatíveis).
5. Em Supported IP address types (Tipos de endereço IP compatíveis), siga um destes procedimentos:
   - Selecionar IPv4: habilite o serviço de endpoint para aceitar solicitações IPv4.
   - Selecionar IPv6: habilite o serviço de endpoint para aceitar solicitações IPv6.
   - Selecionar IPv4 e IPv6: habilite o serviço de endpoint para aceitar solicitações IPv4 e IPv6.
6. Escolha Salvar alterações.

Para modificar os tipos de endereço IP compatíveis usando a linha de comando

- modify-vpc-endpoint-service-configuration (AWS CLI)
- Edit-EC2VpcEndpointServiceConfiguration(Ferramentas para Windows PowerShell)

Gerenciar tags

Você pode marcar os recursos para ajudar a identificá-los ou categorizá-los de acordo com as necessidades da organização.

Para gerenciar as tags para o serviço de endpoint usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).
3. Selecione o serviço de endpoint da VPC.
4. Selecione Ações, Gerenciar tags.
5. Para cada etiqueta a ser adicionada, escolha Add new tag (Adicionar nova etiqueta) e insira a chave da etiqueta e o valor da etiqueta.
6. Para remover uma etiqueta, escolha Remove (Remover) à direita da chave e do valor da etiqueta.

7. Escolha Salvar.

Para gerenciar as tags para as conexões de endpoint usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).
3. Selecione o serviço de endpoint da VPC e, em seguida, escolha a guia Endpoint connections (Conexões d endpoint).
4. Selecione a conexão de endpoint e depois escolha Actions (Ações), Manage tags (Gerenciar tags).
5. Para cada etiqueta a ser adicionada, escolha Add new tag (Adicionar nova etiqueta) e insira a chave da etiqueta e o valor da etiqueta.
6. Para remover uma etiqueta, escolha Remove (Remover) à direita da chave e do valor da etiqueta.
7. Escolha Salvar.

Para gerenciar as tags para as permissões do serviço de endpoint usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).
3. Selecione o serviço de endpoint da VPC e depois escolha a guia Allow principals (Permitir entidades principals).
4. Selecione a entidade principal e depois escolha Actions (Ações), Manage tags (Gerenciar tags).
5. Para cada etiqueta a ser adicionada, escolha Add new tag (Adicionar nova etiqueta) e insira a chave da etiqueta e o valor da etiqueta.
6. Para remover uma etiqueta, escolha Remove (Remover) à direita da chave e do valor da etiqueta.
7. Escolha Salvar.

Para adicionar e remover etiquetas usando a linha de comando

- create-tags and delete-tags (AWS CLI)
- New-EC2Tage Remove-EC2Tag(Ferramentas para Windows PowerShell)

Nomes DNS gerenciados para serviços de endpoint da VPC

Os provedores de serviços podem configurar nomes DNS privados para serviços de endpoint. Suponha que um provedor de serviço disponibilize seu serviço por um endpoint público como um serviço de endpoint. Se o provedor de serviço usar o nome DNS do endpoint público como o nome DNS privado do serviço de endpoint, os consumidores do serviço poderão acessar o endpoint público ou o serviço de endpoint usando a mesma aplicação cliente, sem modificação. Se uma solicitação vier da VPC do consumidor do serviço, os servidores DNS privados resolverão o nome DNS para os endereços IP das interfaces de rede de endpoint. Caso contrário, os servidores DNS públicos resolverão o nome DNS para o endpoint público.

Para configurar um nome de DNS privado para o serviço de endpoint, você deve executar uma verificação de propriedade do domínio para comprovar que o domínio é seu.

Considerações

- O serviço de endpoint pode ter somente um nome de DNS privado.
- Quando o consumidor cria um endpoint de interface para se conectar ao serviço, nós criamos uma zona hospedada privada e a associamos à VPC do consumidor do serviço. Criamos um registro CNAME na zona hospedada privada que mapeia o nome DNS privado do serviço de endpoint para o nome DNS regional do endpoint da VPC. Quando um consumidor envia uma solicitação para o nome DNS público do serviço, os servidores DNS privados resolvem a solicitação para os endereços IP das interfaces de rede de endpoint.
- Para verificar um domínio, é necessário ter um nome de host público ou um provedor DNS público.
- Você pode verificar o domínio de um subdomínio. Por exemplo, você pode verificar example.com, em vez de a.example.com. Cada rótulo DNS pode ter até 63 caracteres e o nome de domínio inteiro não deve exceder um comprimento total de 255 caracteres.

  Se adicionar um subdomínio adicional, será necessário verificar o subdomínio ou o domínio. Por exemplo, digamos que você tinha a.example.com, e verificou example.com. Agora você adiciona b.example.com como um nome de DNS privado. O example.com ou b.example.com deve ser verificado antes que os consumidores do serviço possam usar o nome.
- Nomes DNS privados não são compatíveis com endpoints do Gateway Load Balancer.

Verificação da propriedade do domínio

Seu domínio está associado a um conjunto de registros de serviços de nomes de domínio (DNS) que você pode gerenciar por meio do seu provedor de DNS. Um registro TXT é um tipo de registro DNS que fornece informações adicionais sobre seu domínio. Consiste em um nome e um valor. Como parte do processo de verificação, é necessário adicionar um registro TXT ao servidor DNS de seu domínio público.

A verificação de propriedade de domínio estará concluída quando detectarmos a existência do registro TXT nas configurações de DNS do domínio.

Após adicionar um registro, você pode verificar o status do processo de verificação de domínio usando o console da Amazon VPC. No painel de navegação, escolha Endpoint Services (Serviços do endpoint). Selecione o serviço de endpoint e verifique o valor de Domain verification status (Status da verificação do domínio) na guia Details (Detalhes). Se a verificação do domínio estiver pendente, aguarde mais alguns minutos e atualize a tela. Se necessário, você pode iniciar o processo de verificação manualmente. Escolha Actions (Ações), Verify domain ownership for private DNS name (Verificar a propriedade do domínio para o nome DNS privado).

O nome DNS privado está pronto para ser usado pelos consumidores do serviço quando o status de verificação é verified (verificado). Se o status da verificação for alterado, as novas solicitações de conexão serão negadas, mas as conexões existentes não serão afetadas.

Se o status da verificação for failed (com falha), consulte the section called “Solucionar problemas de verificação de domínio”.

Obtenha o nome e o valor

Fornecemos o nome e o valor que você utiliza no registro TXT. Por exemplo, as informações estão disponíveis no Console de gerenciamento da AWS. Selecione o serviço de endpoint e consulte Domain verification name (Nome de verificação de domínio) e Domain verification value (Valor de verificação de domínio) na guia Details (Detalhes) do serviço de endpoint. Você também pode usar o seguinte AWS CLI comando describe-vpc-endpoint-service-configurations para recuperar informações sobre a configuração do nome DNS privado para o serviço de endpoint especificado.

```
aws ec2 describe-vpc-endpoint-service-configurations \
    --service-ids vpce-svc-071afff70666e61e0 \
    --query ServiceConfigurations[*].PrivateDnsNameConfiguration
```

O seguinte é um exemplo de saída. Você usará `Value` e `Name` ao criar o registro TXT.

```
[
    {
        "State": "pendingVerification",
        "Type": "TXT",
        "Value": "vpce:l6p0ERxlTt45jevFwOCp",
        "Name": "_6e86v84tqgqubxbwii1m"
    }
]
```

Por exemplo, suponhamos que o nome de domínio seja example.com e que `Value` e `Name` sejam os mostrados no exemplo de saída anterior. A seguinte tabela é um exemplo das configurações de registro TXT.

Nome	Tipo	Valor
_6e86v84tqgqubxbwi i1m.example.com	TXT	vpce: l6p0 ERxlTt45jevFwOCp

Sugerimos usar `Name` como subdomínio de registro porque o nome do domínio base pode já estar em uso. Porém, se o provedor de DNS não permitir que nomes de registro de DNS contenham sublinhados, você pode omitir “_6e86v84tqgqubxbwii1m” e simplesmente usar “example.com” no registro TXT.

Depois de verificarmos “_6e86v84tqgqubxbwii1m.example.com”, os consumidores do serviço podem usar “example.com” ou um subdomínio (por exemplo, “service.example.com” ou “my.service.example.com”).

Adicionar um registro TXT ao servidor DNS do seu domínio

O procedimento para adicionar registros TXT ao servidor DNS do seu domínio depende de quem fornece seu serviço de DNS. O provedor de DNS pode ser o Amazon Route 53 ou outro registrador de nomes de domínio.

Amazon Route 53

Crie um registro para a zona hospedada pública utilizando uma política de roteamento simples. Use os seguintes valores:

- Em Record name (Nome do registro), insira o domínio ou subdomínio.
- Em Record type (Tipo de registro), escolha TXT.
- Para Value/Route tráfego para, insira o valor de verificação do domínio.
- Em TTL (seconds) (TTL [segundos]), insira **`1800`**.

Para obter mais informações, consulte Criar registros usando o console no Guia do desenvolvedor do Amazon Route 53.

Procedimento geral

Acesse o site do provedor de DNS e faça login em sua conta. Localize a página para atualizar os registros DNS de seu domínio. Adicione um registro TXT com o nome e o valor que fornecemos. Pode levar até 48 horas para as atualizações de registros de DNS serem efetivadas, mas a efetivação geralmente ocorre muito antes.

Para obter instruções mais específicas, consulte a documentação de seu provedor de DNS. A seguinte tabela fornece links para a documentação de vários provedores de DNS comuns. Essa lista não pretende ser abrangente nem é uma recomendação dos produtos ou serviços fornecidos por essas empresas.

DNS/Hosting provedor	Link da documentação
GoDaddy	Adicionar um registro TXT
Dreamhost	Adicionar registros DNS personalizados
Cloudflare	Gerenciar registros DNS
HostGator	Gerencie registros DNS com HostGator/eNom
Namecheap	Como faço para adicionar TXT/SPF/DKIM/DMARC registros ao meu domínio?
Names.co.uk	Alterar configurações de DNS do domínio
Wix	Adicionar ou atualizar registros TXT na sua conta do Wix

Verificar se o registro TXT foi publicado

Você pode conferir se o registro TXT de verificação de propriedade do domínio de nome DNS privado está publicado corretamente no servidor DNS realizando as seguintes etapas. Você executará o comando nslookup, que está disponível para Windows e Linux.

Você consultará os servidores de DNS que atendam seu domínio, pois esses servidores contêm as informações mais atualizadas dele. As informações do domínio podem levar algum tempo para serem propagadas para outros servidores de DNS.

Para examinar se o registro TXT foi publicado no servidor DNS

1. Localize os servidores de nome de seu domínio usando o seguinte comando.

   ```
   nslookup -type=NS example.com
   ```

   A saída indicará os servidores de nome que atendem seu domínio. Você poderá consultar um desses servidores na próxima etapa.

2. Verifique se o registro TXT foi publicado corretamente usando o comando a seguir, onde *name_server* está um dos servidores de nomes que você encontrou na etapa anterior.

   ```
   nslookup -type=TXT  _6e86v84tqgqubxbwii1m.example.com name_server
   ```

3. Na saída da etapa anterior, verifique se a string após `text =` corresponde ao valor TXT.

   Em nosso exemplo, se o registro tiver sido publicado corretamente, a saída conterá o seguinte:

   ```
   _6e86v84tqgqubxbwii1m.example.com text = "vpce:l6p0ERxlTt45jevFwOCp"
   ```

Solucionar problemas de verificação de domínio

Se o processo de verificação de domínio falhar, as seguintes informações poderão ajudar você a solucionar problemas.

- Verifique se o provedor de DNS permite sublinhados em nomes de registro TXT. Se o provedor de DNS não permitir sublinhados, você poderá omitir o nome de verificação do domínio (por exemplo, “_6e86v84tqgqubxbwii1m”) do registro TXT.

- Verifique se o provedor de DNS acrescentou o nome de domínio ao final do registro TXT. Alguns provedores de DNS anexam automaticamente o nome do seu domínio ao nome de atributo do registro TXT. Para evitar essa duplicação do nome do domínio, adicione um ponto ao final do nome do domínio ao criar o registro TXT. Isso informa ao seu provedor de DNS que não é necessário anexar o nome do domínio ao registro TXT.
- Verifique se o provedor de DNS modificou o valor do registro DNS para usar apenas letras minúsculas. Verificamos o domínio somente quando há um registro de verificação com um valor de atributo que corresponda exatamente ao valor que fornecemos. Se o provedor de DNS alterou os valores do registro TXT para usar apenas letras minúsculas, entre em contato com o provedor para obter assistência.
- Talvez seja necessário verificar o domínio mais de uma vez porque você está oferecendo suporte a várias regiões ou a várias Contas da AWS. Se o provedor de DNS não permitir que você tenha mais de um registro TXT com o mesmo nome de atributo, verifique se o provedor de DNS permite atribuir vários valores de atributo ao mesmo registro TXT. Por exemplo, se o DNS for gerenciado pelo Amazon Route 53, será possível usar o seguinte procedimento.

  1. No console do Route 53, selecione o registro TXT que você criou ao verificar o domínio na primeira região.
  2. Em Value (Valor), vá até o final do valor de atributo existente e pressione Enter.
  3. Acrescente o valor do atributo para a Região adicional e, em seguida, salve o conjunto de registros.

  Se o provedor de DNS não permitir que você atribua vários valores ao mesmo registro TXT, verifique o domínio uma vez com o valor no nome do atributo do registro TXT e outra vez sem o valor no nome do atributo. Porém, só é possível verificar o mesmo domínio duas vezes.

Receber alertas para eventos de serviço de endpoint

Você pode criar uma notificação para receber alertas de eventos específicos relacionados ao serviço de endpoint. Por exemplo, é possível receber um e-mail quando uma solicitação de conexão é aceita ou rejeitada.

Tarefas

- Criação de uma notificação do SNS
- Adição de uma política de acesso
- Adição de uma política de chave

Criação de uma notificação do SNS

Use o procedimento a seguir para criar um tópico do Amazon SNS para as notificações e se inscrever nele.

Para criar uma notificação para um serviço de endpoint da interface usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).
3. Selecione o serviço de endpoint.
4. Na guia Notifications (Notificações), selecione Create notification (Criar notificação).
5. Em Notification ARN (ARN da notificação), escolha o ARN para o tópico do SNS que você criou.
6. Para assinar um evento, selecione-o em Events (Eventos).
   - Connect (Conectar): o consumidor do serviço criou o endpoint da interface. Isso envia uma solicitação de conexão ao provedor de serviços.
   - Accept (Aceitar): o provedor de serviços aceitou a solicitação de conexão.
   - Reject (Rejeitar): o provedor de serviços rejeitou a solicitação de conexão.
   - Delete (Excluir): o consumidor do serviço excluiu o endpoint da interface.
7. Escolha Create Notification (Criar notificação).

Para criar uma notificação para um serviço de endpoint da interface usando a linha de comando

- create-vpc-endpoint-connection-notification (AWS CLI)
- New-EC2VpcEndpointConnectionNotification(Ferramentas para Windows PowerShell)

Adição de uma política de acesso

Adicione uma política de acesso ao tópico do SNS que AWS PrivateLink permita publicar notificações em seu nome, como as seguintes. Para obter mais informações, consulte: Como edito a política de acesso do meu tópico do Amazon SNS? Use as chaves de condição globais `aws:SourceArn` e `aws:SourceAccount` para se proteger contra o problema confused deputy.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpce.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:us-east-1:111111111111:topic-name",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint-service/service-id"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                }
            }
        }
    ]
}
```

Adição de uma política de chave

Se você estiver usando tópicos de SNS criptografados, a política de recursos da chave KMS deve ser confiável AWS PrivateLink para chamar as operações AWS KMS da API. Veja a seguir um exemplo de política de chave.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpce.amazonaws.com"
```

```
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-east-1:111111111111:key/key-id",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint-service/service-id"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                }
            }
        }
    ]
}
```

Excluir um serviço de endpoint

Quando não precisar mais de um serviço de endpoint, você poderá excluí-lo. Você não poderá excluir um serviço de endpoint se houver algum endpoint conectado ao serviço de endpoint que esteja no estado `available` ou `pending-acceptance`.

Exluir um serviço de endpoint não exclui o balanceador de carga associado e não afeta os servidores de aplicações registrados nos grupos de destino do balanceador de carga.

Para excluir um serviço de endpoint usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).
3. Selecione o serviço de endpoint.
4. Escolha Actions (Ações), Delete endpoint services (Excluir serviços de endpoint).
5. Quando a confirmação for solicitada, insira **`delete`** e selecione Excluir.

Para excluir um serviço de endpoint usando a linha de comando

- delete-vpc-endpoint-service-configurations (AWS CLI)

- Remove-EC2EndpointServiceConfiguration(Ferramentas para Windows PowerShell)

Acesse recursos de VPC por meio de AWS PrivateLink

Você pode acessar um recurso de VPC em outra VPC usando um endpoint da VPC de recurso (endpoint de recurso). Um endpoint de recurso permite que você acesse privadamente e em segurança recursos de VCP, como um banco de dados, uma instância do Amazon EC2, um endpoint de aplicação, um destino de nome de domínio ou um endereço IP, que podem estar em uma sub-rede privada em outra VPC ou em um ambiente on-premises. Sem endpoints de recursos, você precisa adicionar um gateway de internet à sua VPC ou acessar o recurso usando AWS PrivateLink um endpoint de interface e um Network Load Balancer. Os endpoints de recurso não exigem um balanceador de carga, portanto, permitem que você acesse a VPC diretamente. Um recurso de VPC é representado por uma configuração de recurso. Uma configuração de recurso é associada a um gateway de recursos.

Preços

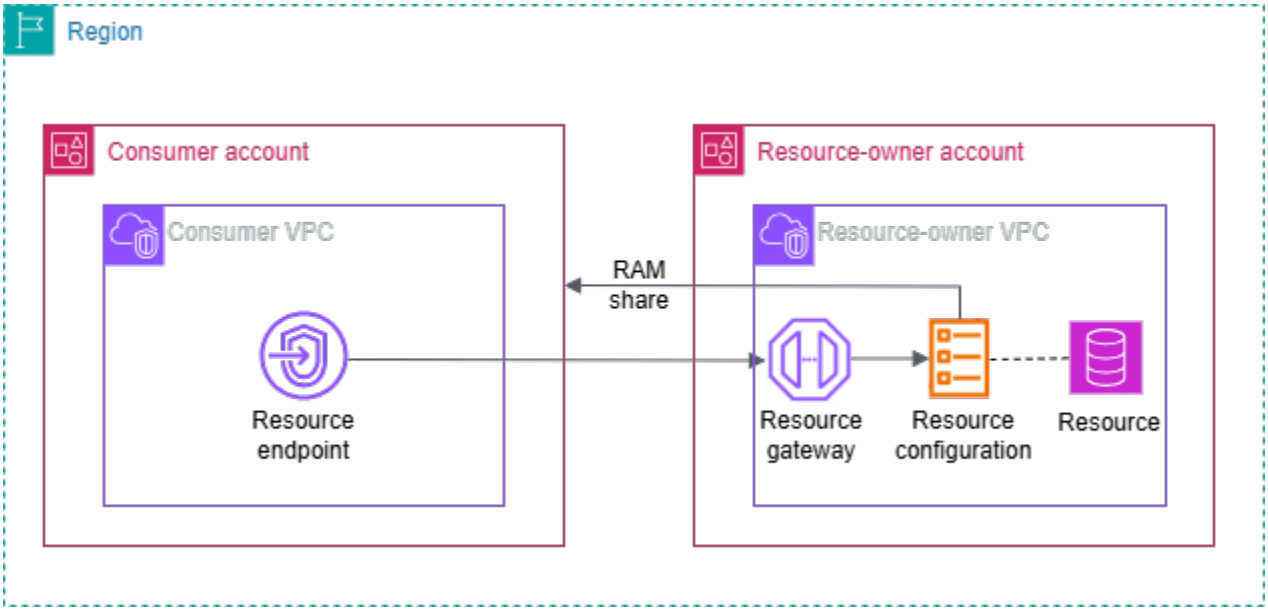
Quando acessa recursos usando endpoints de recurso, a cobrança é feita por cada hora que o endpoint da VPC de recurso é provisionado. Você também é cobrado por GB de dados processados quando acessa os recursos. Para obter mais informações, consulte Preços do AWS PrivateLink. Quando você habilita o acesso aos recursos usando configurações de recursos e gateways de recursos, a cobrança é feita por GB de dados processados por gateways de recursos. Para obter mais informações, consulte Preços do Amazon VPC Lattice.

Conteúdo

Visão geral do

Você pode acessar os recursos da sua conta ou os que foram compartilhados com você de outra conta. Para acessar um recuso, você cria um endpoint da VPC de recurso, que estabelece conexões entre as sub-redes de sua VPC e o recurso usando interfaces de rede. O tráfego destinado ao recurso é resolvido para os endereços IP privados das interfaces de rede de endpoint de recurso usando o DNS. Em seguida, o tráfego é enviado ao recurso usando a conexão entre o endpoint da VPC e o recurso pelo gateway de recursos.

A imagem a seguir mostra um endpoint de recurso em uma conta de consumidor acessando um recurso que pertence a uma conta diferente e é compartilhado por meio AWS RAM de:



Considerações

- Tráfego TCP é compatível. Tráfego UDP não é compatível.
- As conexões de rede devem ser iniciadas da VPC que contém o endpoint do recurso, não da VPC que tem o recurso. A VPC do recurso não pode iniciar conexões de rede com a VPC de endpoint.
- Os únicos ARN-based recursos compatíveis são os recursos do Amazon RDS.
- Pelo menos uma zona de disponibilidade do endpoint da VPC e o gateway de recursos precisam se sobrepor.

Nomes de hosts DNS

Com AWS PrivateLink, você envia tráfego para recursos usando endpoints privados. Quando você cria um endpoint da VPC de recurso, criamos nomes DNS regionais (denominados nomes DNS padrão) que podem ser usados para comunicação com o recurso de sua VPC e da rede on-premises. Recomendamos o uso do DNS em vez de IPs de endpoint para conexão com seus recursos. O nome DNS padrão para o endpoint da VPC de recurso tem a seguinte sintaxe:

```
endpoint_id.rcfgId.randomHash.vpc-lattice-rsc.region.on.aws
```

Quando você cria um endpoint da VPC de recurso para configurações de recursos selecionadas que usam ARNs, você pode habilitar o DNS privado. Com o DNS privado, você pode continuar fazendo solicitações ao recurso usando o nome DNS provisionado para o recurso pelo AWS serviço, enquanto aproveita a conectividade privada por meio do endpoint VPC do recurso. Para obter mais informações, consulte the section called “Resolução do DNS”.

O seguinte comando describe-vpc-endpoint-associations exibe as entradas DNS para um endpoint de recurso.

```
aws ec2 describe-vpc-endpoint-associations --vpc-endpoint-id vpce-123456789abcdefgh --
query 'VpcEndpointAssociations[*].*'
```

O exemplo a seguir é a saída de um endpoint de recurso para um banco de dados do Amazon RDS com nomes DNS privados habilitados. O primeiro nome DNS é o nome DNS padrão. A segunda entrada vem da zona hospedada privada oculta, que resolve as solicitações ao endpoint público para os endereços IP privados das interfaces de rede de endpoint.

```
[
    [
        "vpce-rsc-asc-abcd1234abcd",
        "vpce-123456789abcdefgh",
        "Accessible",
        {
            "DnsName": "vpce-1234567890abcdefg-
snra-1234567890abcdefg.rcfg-abcdefgh123456789.4232ccc.vpc-lattice-rsc.us-
east-1.on.aws",
            "HostedZoneId": "ABCDEFGH123456789000"
        },
        {
```

```
            "DnsName": "database-5-test.cluster-ro-example.us-
east-1.rds.amazonaws.com",
            "HostedZoneId": "A1B2CD3E4F5G6H8I91234"
        },
        "arn:aws:vpc-lattice:us-east-1:111122223333:resourceconfiguration/
rcfg-1234567890abcdefg",
        "arn:aws:vpc-lattice:us-east-1:111122223333:resourceconfiguration/
rcfg-1234567890xyz"
    ]
]
```

Resolução do DNS

Os registros DNS que criamos para o endpoint da VPC de recurso são públicos. Logo, esses nomes DNS podem ser resolvidos publicamente. Porém, as solicitações ao DNS de fora da VPC continuam a retornar os endereços IP privados das interfaces de rede do endpoint de recurso. Você pode usar esses nomes DNS para acessar o recurso da rede on-premises, desde que tenha acesso à VPC em que o endpoint de recurso se encontra, por VPN ou Direct Connect.

DNS privado

Se você habilitar o DNS privado para seu endpoint VPC de recursos para selecionar configurações de recursos que usam ARNs, e sua VPC tiver nomes de host DNS e resolução de DNS ativados, criaremos zonas hospedadas privadas AWS ocultas e gerenciadas para configurações de recursos com um nome DNS personalizado. A zona hospedada contém um conjunto de registros para o nome DNS padrão do recurso que é resolvido para os endereços IP privados das interfaces de rede do endpoint de recurso em sua VPC.

A Amazon fornece um servidor de DNS à VPC, o Route 53 Resolver. O Route 53 Resolver resolve automaticamente nomes de domínio de VPC locais e os registra em zonas hospedadas privadas. No entanto, não é possível usar o Route 53 Resolver de fora da sua VPC. Se desejar acessar o endpoint da VPC da sua rede on-premises, você poderá usar o nome DNS personalizado ou os endpoints do Route 53 Resolver e as regras do Resolver. Para obter mais informações, consulte Integração AWS Transit Gateway com AWS PrivateLink e. Amazon Route 53 Resolver

Zonas de disponibilidade e sub-redes

Você pode configurar um endpoint da VPC com uma sub-rede por zona de disponibilidade. Criamos uma interface de rede do endpoint para o endpoint da VPC na sub-rede. Atribuímos endereços IP

a cada interface de rede de endpoint a partir de sua sub-rede, com base no tipo de endereço IP do endpoint da VPC. Em um ambiente de produção, para garantir alta disponibilidade e resiliência, recomendamos configurar pelo menos duas zonas de disponibilidade para cada endpoint da VPC.

Tipos de endereço IP

Os endpoints de recurso são compatíveis com endereços IPv4, IPv6 ou pilha dupla. Os endpoints que oferecem suporte a IPv6 podem responder a consultas de DNS com registros AAAA. O tipo de endereço IP de um endpoint de recurso deve ser compatível com as sub-redes do endpoint de recurso, como descrito aqui:

- IPv4: atribua endereços IPv4 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4.
- IPv6: atribua endereços IPv6 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas forem sub-redes IPv6 apenas.
- Dualstack: atribua endereços IPv4 e IPv6 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4 e IPv6.

Se um endpoint da VPC de recurso for compatível com IPv4, as interfaces de rede de endpoint terão endereços IPv4. Se um endpoint da VPC de recurso for compatível com IPv6, as interfaces de rede de endpoint terão endereços IPv6. Não é possível acessar o endereço IPv6 de uma interface de rede de endpoint pela Internet. Se você descrever uma interface de rede de endpoint com um endereço IPv6, observe que `denyAllIgwTraffic` está habilitado.

Acessar um recurso por um endpoint da VPC de recurso

Você pode acessar um recurso da VPC, como nome de domínio, endereço IP ou banco de dados do Amazon RDS usando um endpoint de recurso. Um endpoint de recurso fornece acesso privado a um recurso. Ao criar o endpoint de recurso, você especifica uma configuração de recurso do tipo único, grupo ou ARN. Um endpoint de recurso pode ser associado apenas a uma configuração de recurso. A configuração de recurso pode representar um único recurso ou um grupo de recursos.

Pré-requisitos

Para criar um endpoint de recurso, você deve atender aos pré-requisitos a seguir.

- Deve ter uma configuração de recurso que criou ou que outra conta criou e compartilhou com você usando o AWS RAM.
- Se uma configuração de recurso for compartilhada com você de outra conta, será necessário revisar e aceitar o compartilhamento de recursos que contém a configuração de recurso. Para obter mais informações, consulte Aceitar e rejeitar convites no Guia do usuário do AWS RAM .

O VPC Lattice não cria um endpoint de recursos se o seguinte for verdadeiro:

- O gateway de recursos está na mesma VPC do endpoint de recursos.
- Para alvos de nomes de domínio
  - A resolução de DNS é definida como IN_VPC no gateway de recursos.
  - O nome de domínio personalizado ou domínio de grupo é o mesmo domínio ou um domínio de nível superior do destino do nome de domínio.

Criar um endpoint de recurso de VPC

Use o procedimento a seguir para criar um endpoint de recurso de VCP. Depois de criar um endpoint de recurso, você somente poderá modificar seus grupos de segurança ou tags.

Para criar um endpoint de recurso de VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Escolha Criar endpoint.
4. Você pode especificar um nome para facilitar a localização e o gerenciamento do endpoint.
5. Em Tipo de recurso, escolha Recursos.
6. Em Configurações de recursos, selecione a configuração de recurso.
7. Em Configurações de rede, selecione a VPC da qual você acessará o recurso.
8. Se você quiser configurar o suporte de DNS privado para configurações de recursos, selecione Configurações adicionais, Ativar nome DNS. Para usar esse atributo, certifique-se de que os atributos Habilitar hostnames DNS e Habilitar compatibilidade com DNS sejam habilitados para sua VPC. Para obter mais informações, consulte the section called “Nomes de domínio personalizados para consumidores de recursos”.
9. Em Sub-redes, selecione uma sub-rede na qual será criada a interface de rede de endpoint.

Em um ambiente de produção, para garantir alta disponibilidade e resiliência, recomendamos configurar pelo menos duas zonas de disponibilidade para cada endpoint da VPC.

10. Em Grupos de segurança, selecione um grupo de segurança.

    Se você não especificar um grupo de segurança, associaremos o grupo de segurança padrão para a VPC.

11. Escolha Criar endpoint.

Para criar um endpoint de recurso usando a linha de comando

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Gerenciar endpoints de recurso

Depois de criar um endpoint de recurso, você pode gerenciar seus grupos de segurança ou tags.

Tarefas

- Excluir um endpoint
- Atualizar um endpoint

Excluir um endpoint

Quando não precisar mais de um endpoint da VPC, você poderá excluí-lo.

Para excluir um endpoint usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint.
4. Escolha Actions (Ações), Delete VPC endpoints (Excluir endpoints da VPC).
5. Quando a confirmação for solicitada, insira **`delete`**.
6. Escolha Excluir.

Para excluir um endpoint usando a linha de comando

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Atualizar um endpoint

Você pode atualizar um endpoint da VPC.

Para atualizar um endpoint usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint.
4. Escolha Ações e a opção apropriada.
5. Siga as etapas do console para enviar a atualização.

Para atualizar um endpoint usando a linha de comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Configuração de recurso para recursos de VPC

Uma configuração de recurso representa um recurso ou um grupo de recursos que você deseja tornar acessível aos clientes em outras VPCs e contas. Definindo uma configuração de recurso, você pode permitir conectividade de rede privada, segura e unidirecional de clientes em outras VPCs e contas com os recursos de sua VPC. Uma configuração de recursos é associada a um gateway de recursos pelo qual recebe tráfego.

Conteúdo

- Nomes de domínio personalizados para proprietários de redes de serviços
- Definição de recurso
- Protocolo
- Intervalo de portas
- Acesso a recursos da
- Associação com tipo de rede de serviço
- Tipos de redes de serviço
- Compartilhando configurações de recursos por meio de AWS RAM
- Monitoramento
- Create a resource configuration in VPC Lattice
- Manage associations for a VPC Lattice resource configuration

Tipos de configurações de recursos

Um configuração de recurso pode ser de vários tipos. Os diferentes tipos ajudam a representar diferentes tipos de recursos. Os tipos são:

- Configuração de recurso único: um endereço IP ou um nome de domínio. Ela pode ser compartilhada de modo independente.
- Configuração de recurso de grupo: um conjunto de configurações de recursos secundárias. Ela pode ser compartilhada de modo independente.
- Configuração de recurso secundária: um membro de uma configuração de recurso de grupo. Representa um endereço IP ou um nome de domínio. Ela não pode ser compartilhada de modo independente, só pode ser compartilhada como parte de um grupo. Pode ser adicionada e removida de um grupo facilmente. Quando adicionada, pode ser acessada automaticamente por quem pode acessar o grupo.
- Configuração do recurso ARN: representa um tipo de recurso suportado que é provisionado por um serviço. AWS Por exemplo, um banco de dados do Amazon RDS. As configurações de recursos secundárias são gerenciadas automaticamente pela AWS.

Gateway de recursos

Uma configuração de recurso é associada a um gateway de recursos. Um gateway de recursos é um conjunto de ENIs que serve como ponto de entrada na VPC em que o recurso se encontra.

Várias configurações de recursos podem ser associadas ao mesmo gateway de recursos. Quando clientes em outras VPCs ou contas acessam um recurso em sua VPC, o recurso vê o tráfego vindo localmente do gateway de recursos nessa VPC.

Nomes de domínio personalizados para provedores de recursos

Os provedores de recursos podem anexar um nome de domínio personalizado a uma configuração de recursos, como`example.com`, por exemplo, qual recurso os consumidores podem usar para acessar a configuração do recurso. O nome de domínio personalizado pode pertencer e ser verificado pelo provedor de recursos, ou pode ser de um terceiro ou de um AWS domínio. Os provedores de recursos podem usar configurações de recursos para compartilhar clusters de cache e clusters, TLS-based aplicativos ou outros recursos do Kafka. AWS

As considerações a seguir se aplicam aos fornecedores de configurações de recursos:

- Uma configuração de recurso só pode ter um domínio personalizado.
- O nome de domínio personalizado de uma configuração de recurso não pode ser alterado.
- O nome de domínio personalizado é visível para todos os consumidores de configuração de recursos.
- Você pode verificar seu nome de domínio personalizado usando o processo de verificação de nome de domínio no VPC Lattice. Para obter mais informações, consultehttps://docs.aws.amazon.com/vpc-lattice/latest/ug/create-and-verify.html.
- Para configurações de recursos do tipo grupo e filho, você deve primeiro especificar um domínio de grupo na configuração de recursos do grupo. Depois, as configurações de recursos secundários podem ter domínios personalizados que são subdomínios do domínio do grupo. Se o grupo não tiver um domínio de grupo, você poderá usar qualquer nome de domínio personalizado para o filho, mas o VPC Lattice não provisionará nenhuma zona hospedada para os nomes de domínio secundário na VPC do consumidor do recurso.

Nomes de domínio personalizados para consumidores de recursos

Quando os consumidores de recursos habilitam a conectividade com uma configuração de recurso que tem um nome de domínio personalizado, eles podem permitir que o VPC Lattice gerencie uma zona hospedada privada do Route 53 em sua VPC. Os consumidores de recursos têm opções granulares para quais domínios desejam permitir que o VPC Lattice gerencie zonas hospedadas privadas.

Os consumidores de recursos podem definir o `private-dns-enabled` parâmetro ao habilitar a conectividade às configurações de recursos por meio de um endpoint de recursos, de um endpoint de rede de serviços ou de uma associação VPC de rede de serviços. Junto com o `private-dns-enabled` parâmetro, os consumidores podem usar as opções de DNS para especificar para quais domínios desejam que o VPC Lattice gerencie zonas hospedadas privadas. Os consumidores podem escolher entre as seguintes preferências de DNS privado:

`ALL_DOMAINS`

O VPC Lattice provisiona zonas hospedadas privadas para todos os nomes de domínio personalizados.

`VERIFIED_DOMAINS_ONLY`

O VPC Lattice provisiona uma zona hospedada privada somente se o nome de domínio personalizado tiver sido verificado pelo provedor.

`VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS`

O VPC Lattice provisiona zonas hospedadas privadas para todos os nomes de domínio personalizados verificados e outros nomes de domínio especificados pelo consumidor do recurso. O consumidor do recurso especifica os nomes de domínio no `private DNS specified domains` parâmetro.

`SPECIFIED_DOMAINS_ONLY`

O VPC Lattice provisiona uma zona hospedada privada para nomes de domínio especificados pelo consumidor do recurso. O consumidor do recurso especifica os nomes de domínio no `private DNS specified domains` parâmetro.

Quando você ativa o DNS privado, o VPC Lattice cria uma zona hospedada privada em sua VPC para o nome de domínio personalizado associado à configuração do recurso. Por padrão, a preferência de DNS privado é definida como. `VERIFIED_DOMAINS_ONLY` Isso significa que as zonas hospedadas privadas são criadas somente se o nome de domínio personalizado tiver sido verificado pelo provedor de recursos. Se você definir sua preferência de DNS privado como `ALL_DOMAINS` ou`SPECIFIED_DOMAINS_ONLY`, em seguida, o VPC Lattice cria zonas hospedadas privadas, independentemente do status de verificação do nome de domínio personalizado. Quando uma zona hospedada privada é criada para um determinado domínio, todo o tráfego da sua VPC para esse domínio é roteado pela VPC Lattice. Recomendamos que você use as `SPECIFIED_DOMAINS_ONLY`

preferênciasALL_DOMAINS,VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS, ou somente quando quiser que o tráfego para esses nomes de domínio personalizados passe pelo VPC Lattice.

Recomendamos que os consumidores de recursos definam suas preferências de DNS privado comoVERIFIED_DOMAINS_ONLY. Isso permite que os consumidores aumentem seu perímetro de segurança, permitindo apenas que a VPC Lattice provisione zonas hospedadas privadas para domínios verificados na conta do consumidor do recurso.

Para selecionar domínios nos domínios específicos do DNS privado, os consumidores de recursos podem inserir um nome de domínio totalmente qualificado, como, `my.example.com` ou usar um caractere curinga, como. `*.example.com`

As considerações a seguir se aplicam aos consumidores de configurações de recursos:

- O parâmetro DNS privado habilitado não pode ser alterado.
- O DNS privado deve estar habilitado em uma associação de recursos de rede de serviços para que uma hospedagem privada seja criada em uma VPC. Para uma configuração de recursos, o status habilitado para DNS privado da associação de recursos de rede de serviços substitui o status habilitado para DNS privado do endpoint da rede de serviços ou da associação VPC da rede de serviços.

Para configurações de recursos que são destinos de nome de domínio, uma entrada de zona hospedada privada não é criada se o seguinte for verdadeiro:

- O gateway de recursos está na mesma VPC que a associação VPC da rede de serviços VPC da endpoint/service rede VPC.
- A resolução de DNS é definida como IN_VPC no gateway de recursos.
- O nome de domínio personalizado ou domínio de grupo é o mesmo domínio ou um domínio de nível superior do destino do nome de domínio.

Para configurações de recursos do tipo ARN, o VPC Lattice não cria uma entrada de zona hospedada privada se o seguinte for verdadeiro:

- O gateway de recursos está na mesma VPC que a associação VPC da rede de serviços VPC da endpoint/service rede VPC.

Nomes de domínio personalizados para proprietários de redes de serviços

A propriedade habilitada para DNS privado da associação de recursos da rede de serviços substitui a propriedade habilitada para DNS privado do endpoint da rede de serviços e a associação VPC da rede de serviços.

Se o proprietário de uma rede de serviços criar uma associação de recursos de rede de serviços e não habilitar o DNS privado, o VPC Lattice não provisionará zonas hospedadas privadas para essa configuração de recursos em nenhuma VPC à qual a rede de serviços esteja conectada, mesmo que o DNS privado esteja habilitado no endpoint da rede de serviços ou nas associações VPC da rede de serviços.

Para configurações de recursos do tipo ARN, o sinalizador de DNS privado é verdadeiro e imutável. Portanto, o VPC Lattice provisiona zonas hospedadas privadas para tipos de recursos ARN, independentemente da configuração da propriedade DNS privada do endpoint da rede de serviços e da associação VPC da rede de serviços, exceto quando o gateway de recursos também está na mesma VPC. Em outras palavras, quando uma VPC é consumidora e provedora de uma configuração de recursos do tipo ARN, a VPC Lattice ignora a criação de zonas hospedadas privadas nessa VPC.

Definição de recurso

Na configuração do recurso, identifique o recurso de uma das seguintes maneiras:

- Por um nome de recurso da Amazon (ARN): os tipos de recursos compatíveis que são provisionados por AWS serviços podem ser identificados por seu ARN. Somente os bancos de dados do Amazon RDS são compatíveis. Você não pode criar uma configuração de recurso para um cluster acessível publicamente.
- Por um alvo de nome de domínio: você pode usar qualquer nome de domínio. Se você usa um servidor DNS privado ou seu domínio está em uma zona hospedada privada do Route53, o gateway de recursos deve ter a resolução DNS definida como IN_VPC. Se o nome de domínio apontar para um IP fora de sua VPC, você deverá ter um gateway NAT em sua VPC.
- Por um IP-address: Para IPv4, especifique um IP privado dos seguintes intervalos: 10.0.0. 0/8, 10.64.0. 0/10, 172.16.0. 0/12, 192.168.0. 0/16. Para IPv6, especifique um IP da VPC. IPs públicos não são compatíveis.

Protocolo

Quando você cria uma configuração de recurso, pode definir os protocolos com que o recurso será compatível. Atualmente, apenas o protocolo TCP é compatível.

Intervalo de portas

Quando você cria uma configuração de recurso, pode definir as portas em que aceitará solicitações. O acesso de cliente em outras portas não será permitido.

Acesso a recursos da

Os consumidores podem acessar as configurações de recursos diretamente de sua VPC usando um endpoint da VPC ou por uma rede de serviço. Como consumidor, você pode habilitar o acesso de sua VPC a uma configuração de recurso que esteja em sua conta ou que tenha sido compartilhada com você de outra conta pelo AWS RAM.

- Acessar uma configuração de recurso diretamente

  Você pode criar um AWS PrivateLink VPC endpoint do tipo resource (endpoint de recurso) na sua VPC para acessar uma configuração de recursos de forma privada a partir da sua VPC. Para obter mais informações sobre como criar um endpoint de recurso, consulte Accessing VPC resources no AWS PrivateLink User Guide.
- Acessar uma configuração de recurso por uma rede de serviço

  Você pode associar uma configuração de recurso a uma rede de serviço e conectar sua VPC à rede de serviço. Você pode conectar sua VPC à rede de serviços por meio de uma associação ou usando um endpoint VPC de AWS PrivateLink rede de serviços.

  Para obter mais informações sobre associações de rede de serviço, consulte Manage the associations for a VPC Lattice service network.

  Para obter mais informações sobre endpoints da VPC de rede de serviço, consulte Access service networks no AWS PrivateLink User Guide.

Quando DNS privado está habilitado para a VPC, você não pode criar um endpoint de recurso e um endpoint de rede de serviço para a mesma configuração de recurso.

Associação com tipo de rede de serviço

Quando você compartilha uma configuração de recursos com uma conta de consumidor, por exemplo,, Account-B por meio de AWS RAM, Account-B pode acessar a configuração do recurso diretamente por meio de um endpoint VPC de recursos ou por meio de uma rede de serviços.

Para acessar uma configuração de recursos por meio de uma rede de serviços, Account-B seria necessário associar a configuração do recurso a uma rede de serviços. As redes de serviço podem ser compartilhadas entre contas. Assim, Account-B podem compartilhar sua rede de serviços (à qual a configuração do recurso está associada) Account-C, tornando seu recurso acessível a partir de Account-C.

Para evitar esse compartilhamento transitivo, você pode especificar que a configuração de recurso não pode ser adicionada a redes de serviço que possam ser compartilhadas entre contas. Se você especificar isso, Account-B não será possível adicionar sua configuração de recursos às redes de serviços que são compartilhadas ou podem ser compartilhadas com outra conta no futuro.

Tipos de redes de serviço

Quando você compartilha uma configuração de recurso com outra conta, por exemplo Account-B, por meio de AWS RAM, Account-B pode acessar o recurso de uma das três maneiras:

- Usando um endpoint da VPC do tipo recurso (endpoint da VPC de recurso).
- Usando um endpoint da VPC do tipo rede de serviço (endpoint da VPC de rede de serviço).
- Usando uma associação de VPC de rede de serviço.

  Quando você usa uma associação de serviço-rede, cada recurso recebe um IP por sub-rede do 129.224.0. 0/17 bloco, que é AWS próprio e não roteável. Isso é além da lista de prefixos gerenciados que o VPC Lattice usa para rotear o tráfego para serviços pela rede do VPC Lattice. Esses dois IPs são atualizados para a tabela de rotas de sua VPC.

Para o endpoint VPC da rede de serviços e a associação VPC da rede de serviços, a configuração do recurso teria que ser colocada em uma rede de serviços em. Account-B As redes de serviço podem ser compartilhadas entre contas. Assim, Account-B podem compartilhar sua rede de serviços (que contém a configuração do recurso) com Account-C, tornando seu recurso acessível a partir de Account-C. Para evitar esse compartilhamento transitivo, você pode impedir que sua configuração de recursos seja adicionada às redes de serviços que podem ser compartilhadas entre contas. Se

você não permitir isso, Account-B não poderá adicionar sua configuração de recursos a uma rede de serviços compartilhada ou que possa ser compartilhada com outra conta.

Compartilhando configurações de recursos por meio de AWS RAM

As configurações de recursos são integradas com o. AWS Resource Access Manager Você também pode compartilhar a configuração de recurso com outra conta pelo AWS RAM. Quando você compartilha uma configuração de recurso com uma AWS conta, os clientes dessa conta podem acessar o recurso de forma privada. Você pode compartilhar uma configuração de recurso usando um compartilhamento de recurso no AWS RAM.

Use o AWS RAM console para ver os compartilhamentos de recursos aos quais você foi adicionado, os recursos compartilhados que você pode acessar e as AWS contas que compartilharam recursos com você. Para obter mais informações, consulte Resources shared with you no AWS RAM User Guide.

Para acessar um recurso de outra VPC na mesma conta da configuração do recurso, você não precisa compartilhar a configuração do recurso por meio de. AWS RAM

Monitoramento

Você pode habilitar logs de monitoramento na configuração de recurso. Você pode escolher um destino para enviar os logs.

Create a resource configuration in VPC Lattice

Crie uma configuração de recursos.

Console de gerenciamento da AWS

Para criar uma configuração de recurso usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, em PrivateLink e Lattice, escolha Configurações de recursos.
3. Escolha Criar configuração de recurso.
4. Insira um nome que seja exclusivo em sua AWS conta. Não é possível alterar esse nome depois que a configuração de recurso é criada.
5. Em Tipo de configuração, escolha Recurso, para um recurso único ou secundário, ou Grupo de recursos para um grupo de recursos secundários.

6. Escolha um gateway de recursos criado anteriormente ou crie um agora.
7. (Opcional) Para inserir um nome de domínio personalizado, faça o seguinte:
   - Se você tiver uma configuração de recurso do tipo single, poderá inserir um nome de domínio personalizado. Os consumidores de recursos podem usar esse nome de domínio para acessar suas configurações de recursos.
   - Se você tiver uma configuração de recursos do tipo grupo e filho, deverá primeiro especificar um domínio de grupo na configuração de recursos do grupo. Em seguida, as configurações de recursos secundários podem ter domínios personalizados que são subdomínios do domínio do grupo.
8. (Opcional) Insira a ID de verificação.

   Forneça um ID de verificação se quiser que seu nome de domínio seja verificado. Isso permite que os consumidores de recursos saibam que você é o proprietário do nome de domínio.
9. Escolha o identificador do recurso que você deseja que essa configuração de recurso represente.
10. Escolha os intervalos de portas pelas quais você deseja compartilhar o recurso.
11. Em Configurações de associação, especifique se essa configuração de recurso pode ser associada a redes de serviço compartilháveis.
12. Em Compartilhar configuração de recurso, escolha os compartilhamentos de recurso que identificam as entidades principais que podem acessar esse recurso.
13. (Opcional) Em Monitorar, habilite Logs de acesso ao recurso e o destino de entrega se quiser monitorar solicitações e respostas enviadas e recebidas da configuração de recurso.
14. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
15. Escolha Criar configuração de recurso.

AWS CLI

O comando create-resource-configuration a seguir cria uma única configuração de recurso e a associa ao nome de domínio personalizado. `example.com`

```
aws vpc-lattice create-resource-configuration \
    --name my-resource-config \
    --type SINGLE \
```

```
    --resource-gateway-identifier rgw-0bba03f3d56060135 \
    --resource-configuration-definition 'ipResource={ipAddress=10.0.14.85}' \
    --custom-domain-name example.com \
    --verification-id dv-aaaa0000000111111
```

O comando create-resource-configuration a seguir cria uma configuração de recursos de grupo e a associa ao nome de domínio personalizado. `example.com`

```
aws vpc-lattice-custom-dns create-resource-configuration \
  --name my-custom-dns-resource-config-group \
  --type GROUP \
  --resource-gateway-identifier rgw-0bba03f3d56060135 \
  --domain-verification-identifier dv-aaaa0000000111111
```

O comando create-resource-configuration a seguir cria uma configuração de recurso secundário e a associa ao nome de domínio personalizado. `child.example.com`

```
aws vpc-lattice-custom-dns create-resource-configuration \
  --name my-custom-dns-resource-config-child \
  --type CHILD \
  --resource-configuration-definition 'dnsResource={domainName=my-alb-123456789.us-
west-2.elb.amazonaws.com,ipAddressType=IPV4}' \
  --resource-configuration-group-identifier rcfg-07129f3acded87626 \
  --custom-domain-name child.example.com
```

Manage associations for a VPC Lattice resource configuration

As contas de consumidores com as quais você compartilha uma configuração de recurso e os clientes em sua conta podem acessar a configuração de recurso diretamente usando um endpoint da VPC de recurso ou por um endpoint de rede de serviço. Como resultado, a configuração de recurso terá associações de endpoints e associações de redes de serviço.

Gerenciar associações de recursos de rede de serviços

Crie ou exclua uma associação de rede de serviço.

> **Note**
>
> Se você receber uma mensagem de acesso negado ao criar a associação entre a rede de serviços e a configuração do recurso, verifique a versão da AWS RAM política e certifique-se de que seja a versão 2. Para obter mais informações, consulte o guia AWS RAM do usuário.

Para gerenciar associações de rede de serviço usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, em PrivateLink e Lattice, escolha Configurações de recursos.
3. Escolha o nome da configuração de recurso para abrir sua página de detalhes.
4. Selecione a guia Associações de rede de serviço.
5. Escolha Criar associações.
6. Selecione uma rede de serviços nas Redes de serviços VPC Lattice. Para criar uma rede de serviços, escolha Criar uma rede VPC Lattice.
7. (Opcional) Para adicionar uma tag, expanda Tags de associação de serviço, escolha Adicionar nova tag e insira uma chave de tag e um valor de tag.
8. (Opcional) Para habilitar nomes DNS privados para essa associação de recursos de rede de serviços, escolha habilitar nome DNS privado. Para obter mais informações, consulte the section called “Nomes de domínio personalizados para proprietários de redes de serviços”.
9. Escolha Salvar alterações.
10. Para excluir uma associação, marque a caixa de seleção da associação e escolha Ações, Excluir. Quando a confirmação for solicitada, insira **`confirm`** e selecione Excluir.

Para criar uma associação de rede de serviços usando o AWS CLI

Use o comando create-service-network-resource-association.

Para excluir uma associação de rede de serviços usando o AWS CLI

Use o comando delete-service-network-resource-association.

Gerencie associações de endpoints de VPC de recursos

Contas de consumidores com acesso à sua configuração de recursos ou clientes em sua conta podem acessar a configuração de recursos usando um endpoint VPC de recursos. Se a configuração

do seu recurso tiver um nome de domínio personalizado, você poderá usar habilitar o DNS privado para permitir que o VPC Lattice provisione zonas hospedadas privadas para seu endpoint de recursos ou endpoint de rede de serviços. Com isso, os clientes podem curvar diretamente o nome do domínio para acessar a configuração do recurso. Para obter mais informações, consulte the section called “Nomes de domínio personalizados para consumidores de recursos”.

Console de gerenciamento da AWS

1. Para criar uma nova associação de endpoint, acesse PrivateLink e Lattice no painel de navegação esquerdo e escolha Endpoints.
2. Escolha Criar endpoints.
3. Selecione a configuração do recurso que você deseja conectar à sua VPC.
4. Selecione a VPC, as sub-redes e os grupos de segurança.
5. (Opcional) Para ativar o DNS privado e configurar as opções de DNS, selecione Habilitar nome DNS.
6. (Opcional) Para marcar o endpoint da VPC, escolha Adicionar nova tag e insira uma chave de tag e um valor de tag.
7. Escolha Criar endpoint.

AWS CLI

O comando create-vpc-endpoint a seguir cria um VPC endpoint que usa DNS privado. As preferências de DNS privado são definidas como `VERIFIED_AND_SELECTED` e os domínios selecionados são e. `example.com` `example.org` O VPC Lattice só provisiona zonas hospedadas privadas para quaisquer domínios verificados ou ou. `example.com` `example.org`

```
aws ec2 create-vpc-endpoint \
  --vpc-endpoint-type Resource \
  --vpc-id vpc-111122223333aabbc \
  --subnet-ids subnet-0011aabbcc2233445 \
  --resource-configuration-arn arn:aws:vpc-lattice:us-
west-2:111122223333:resourceconfiguration/rcfg-07129f3acded87625 \
  --private-dns-enabled \
  --private-dns-preferences VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS \
  --private-domains-set example.com, example.org
```

Para criar uma associação de VPC endpoint usando o AWS CLI

Use o comando create-vpc-endpoint.

Para excluir uma associação de VPC endpoint usando o AWS CLI

Use o comando delete-vpc-endpoint.

Gateway de recursos no VPC Lattice

Um gateway de recursos é um ponto de entrada para a VPC em que um recurso reside. Ele abrange várias zonas de disponibilidade.

Uma VPC deverá ter um gateway de recursos se você planejar tornar os recursos dentro da VPC acessíveis de outras VPCs ou contas. Cada recurso que você compartilha está associado a um gateway de recursos. Quando clientes em outras VPCs ou contas acessam um recurso em sua VPC, o recurso vê o tráfego vindo localmente do gateway de recursos nessa VPC. O IP de origem do tráfego é o endereço IP do gateway de recursos. Você pode atribuir vários endereços IP a um gateway de recursos para permitir mais conexões de rede com o recurso. Vários recursos podem ser associadas ao mesmo gateway de recursos.

Um gateway de recursos não fornece recursos de balanceamento de carga.

Conteúdo

Considerações

As considerações a seguir se aplicam aos gateways de recursos:

- Para que o recurso seja acessível de todas as zonas de disponibilidade, você deve criar os gateways de recursos para abranger o maior número possível de zonas de disponibilidade.

- Pelo menos uma zona de disponibilidade do endpoint da VPC e o gateway de recursos precisam se sobrepor.
- Uma VPC pode ter no máximo 100 gateways de recursos. Para obter mais informações, consulte Quotas for VPC Lattice.
- Você não pode criar um gateway de recursos em uma sub-rede compartilhada.

Grupos de segurança

Você pode anexar grupos de segurança a um gateway de recursos. As regras de grupo de segurança para gateways de recursos controlam o tráfego de saída do gateway de recursos para os recursos.

Regras de saída recomendadas para o fluxo de tráfego de um gateway de recursos para um recurso do banco de dados

Para que o tráfego flua de um gateway de recursos para um recurso, você deve criar regras de saída para os protocolos de receptor e intervalos de portas aceitos pelo recurso.

Destino	Protocolo	Intervalo de portas	Comment
CIDR range for resource	TCP	3306	Permite o tráfego do gateway de recursos para os bancos de dados.

Tipos de endereço IP

Um gateway de recursos pode ter endereços IPv4, IPv6 ou de pilha dupla. O tipo de endereço IP de um gateway de recursos deve ser compatível com as sub-redes do gateway de recursos e com o tipo de endereço IP do recurso, como descrito aqui:

- IPv4: atribua endereços IPv4 às interfaces de rede do gateway. Essa opção será compatível somente se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4 e o recurso também tiver um endereço IPv4.
- IPv6: atribua endereços IPv6 às interfaces de rede do gateway. Essa opção será compatível somente se todas as sub-redes selecionadas forem apenas IPV6 e o recurso também tiver um endereço IPv6.

- Pilha dupla: atribua endereços IPv4 e IPv6 às interfaces de rede do gateway. Essa opção será compatível somente se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4 e IPv6, e o recurso tiver um endereço IPv4 ou IPv6.

O tipo de endereço IP do gateway de recursos independe do tipo de endereço IP do cliente ou do endpoint da VPC pelo qual o recurso é acessado.

Endereços IPv4 por ENI

Se o tipo de endereço IP do gateway de recursos for IPv4 ou pilha dupla, você poderá configurar o número de endereços IPv4 atribuídos a cada ENI do gateway de recursos. Ao criar um gateway de recursos, você escolhe de 1 a 62 endereços IPv4. Depois que você define o número de endereços IPv4, o valor não pode ser alterado.

Os endereços IPv4 são usados para traduzir os endereços de rede e determinam o número máximo de conexões IPv4 simultâneas com um recurso. Por padrão, 16 endereços IPv4 por ENI são atribuídos aos gateways de recursos. Esse é um número adequado de IPs para estabelecer conexões com seus recursos de backend.

Se tipo de endereço do gateway de recursos for IPv6, o gateway de recursos receberá automaticamente um CIDR /80 por ENI. Esse valor não pode ser alterado.

Resolução de DNS do Resource Config

É possível especificar como um gateway de recursos realiza a resolução de DNS para configurações de recursos que sejam destinos de nomes de domínio. Esta propriedade é imutável. É possível escolher:

- PÚBLICO (padrão) - Os nomes de domínio são resolvidos usando resolvedores de DNS públicos.
- IN_VPC - Os nomes de domínio são resolvidos usando o servidor DNS configurado no conjunto de opções DHCP da VPC na qual o gateway de recursos está. Escolha esse modo se utilizar um servidor DNS privado ou se os destinos de nomes de domínio estiverem em uma zona hospedada privada do Route 53.

Caso a resolução de DNS seja IN_VPC, não é possível anexar configurações de recursos definidas por ARN ao gateway de recursos. Você não pode definir a resolução de DNS como IN_VPC se o gateway de recursos usar sub-redes. IPv6-only

Create a resource gateway in VPC Lattice

Use o console para criar um gateway de recursos.

Para criar um gateway de recursos usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, em PrivateLink e Lattice, escolha Resource gateways.
3. Escolha Criar um gateway de recursos.
4. Insira um nome que seja exclusivo em sua AWS conta.
5. Escolha o tipo de endereço IP do gateway de recursos.
6. Em Tipo de endereço IP, escolha o tipo de endereço IP do gateway de recursos.
    - Se você selecionou IPv4 ou Pilha dupla como o tipo de endereço IP, poderá inserir o número de endereços IPv4 por ENI para o gateway de recursos.

      O padrão são 16 endereços IPv4 por ENI. Esse é um número adequado de IPs para estabelecer conexões com seus recursos de backend.
7. Escolha a VPC na qual o recurso se encontra.
8. Para grupos de segurança, escolha até cinco grupos de segurança para controlar o tráfego de entrada da VPC para a rede de serviços.
9. Em Resource Config DNS Resolution, escolha como você deseja que o DNS seja resolvido para destinos de nome de domínio.
    - Se você estiver usando um servidor DNS privado ou se seus destinos de nome de domínio estiverem em uma zona hospedada privada do Route53, defina como IN_VPC
10. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
11. Escolha Criar um gateway de recursos.

Para criar um gateway de recursos usando o AWS CLI

Use o comando create-resource-gateway.

Delete a resource gateway in VPC Lattice

Use o console para excluir um gateway de recursos.

Para excluir um gateway de recursos usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, em PrivateLink e Lattice, escolha Resource gateways.
3. Marque a caixa de seleção do gateway de recursos que você deseja excluir e escolha Ações, Excluir. Quando a confirmação for solicitada, insira **`confirm`** e selecione Excluir.

Para excluir um gateway de recursos usando o AWS CLI

Use o comando delete-resource-gateway.

Acesse redes de serviços por meio de AWS PrivateLink

Você pode se conectar privadamente a uma rede de serviço de sua VPC usando um endpoint da VPC de rede de serviço (endpoint de rede de serviço). Um endpoint de rede de serviço permite acessar, privadamente e em segurança, os recursos e serviços associados a uma rede de serviço. Dessa maneira, você pode acessar privadamente vários recursos e serviços por um único endpoint da VPC.

Uma rede de serviço é um conjunto lógico de configurações de recursos e de serviços do VPC Lattice. Usando um endpoint de rede de serviço, você pode conectar uma rede de serviço à sua VPC e acessar privadamente esses recursos e serviços da VPC ou on-premises. O endpoint de rede de serviço permite que você se conecte a uma rede de serviço. Para se conectar de sua VPC a várias redes de serviço, você pode criar vários endpoints de rede de serviço, cada um apontando para uma rede de serviço diferente.

As redes de serviços são integradas com AWS Resource Access Manager (AWS RAM). Você pode compartilhar a rede de serviço com outra conta pelo AWS RAM. Quando você compartilha uma rede de serviços com outra AWS conta, essa conta pode criar um endpoint de rede de serviços para se conectar à rede de serviços. Você pode compartilhar uma rede de serviço usando um compartilhamento de recursos no AWS RAM.

Use o AWS RAM console para visualizar os compartilhamentos de recursos aos quais você foi adicionado, as redes de serviços compartilhados que você pode acessar e as AWS contas que compartilharam os recursos com você. Para obter mais informações, consulte Resources shared with you no AWS RAM User Guide.

Preços

A cobrança é feita por hora pelas configurações de recursos associadas à rede de serviço. A cobrança é feita também por GB de dados processados quando você acessa os recursos pelo endpoint da VPC de rede de serviço. Não há cobrança por hora pelo endpoint da VPC de rede de serviço em si. Para obter mais informações, consulte Preços do Amazon VPC Lattice.

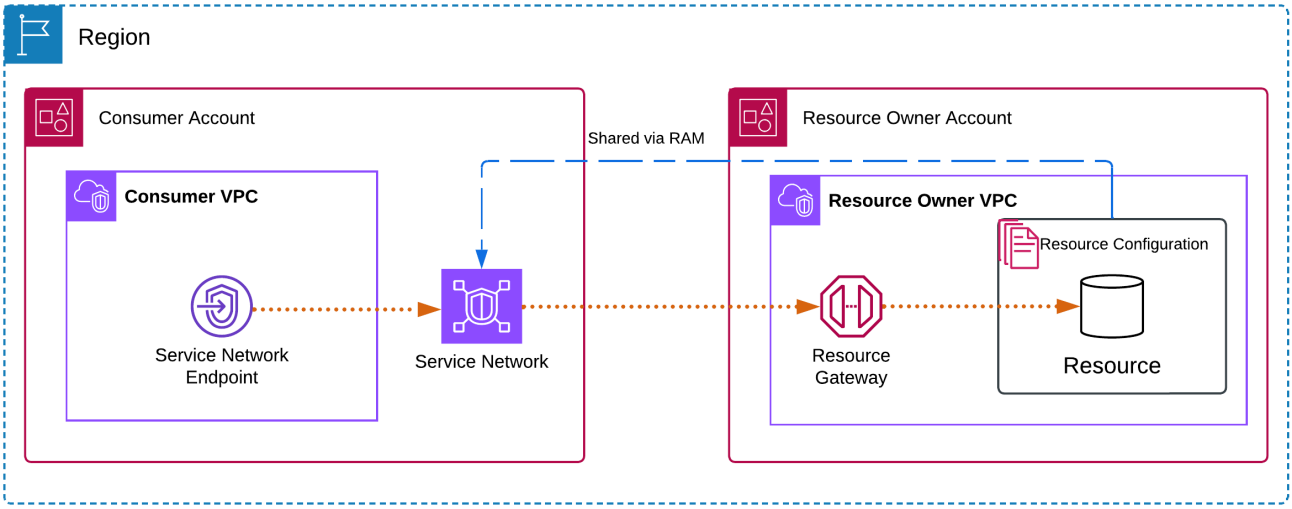
Conteúdo

- DNS privado
- Zonas de disponibilidade e sub-redes
- Tipos de endereço IP
- Acessar uma rede de serviço por um endpoint de rede de serviço
- Gerenciar endpoints de rede de serviço

Visão geral do

É possível criar sua própria rede de serviço ou uma rede de serviço pode ser compartilhada com você por outra conta. De qualquer das duas maneiras, você pode criar um endpoint de rede de serviço para se conectar a ele de sua VPC. Para obter mais informações sobre como criar uma rede de serviço e associar a ela configurações de recursos, consulte o Amazon VPC Lattice User Guide.

O diagrama a seguir mostra como um endpoint de rede de serviço na sua VPC acessa uma rede de serviço.



As conexões de rede podem ser iniciadas apenas pela VPC que tem o endpoint de rede de serviço para os recursos e serviços na rede de serviço. A VPC com os recursos e serviços não pode iniciar conexões de rede com a VPC de endpoint.

Nomes de hosts DNS

Com AWS PrivateLink, você envia tráfego para redes de serviços usando endpoints privados. Quando você cria um endpoint da VPC de rede de serviço, nós criamos nomes DNS regionais

(denominados nomes DNS padrão) para cada recurso e serviço que podem ser usados para comunicação com o recurso e o serviço de sua VPC e on-premises. Os endereços IP associados ao endpoint podem mudar. Recomendamos o uso do DNS em vez de IPs de endpoint para conexão com as redes de serviço.

O nome DNS padrão para um recurso na rede de serviço tem a seguinte sintaxe:

```
endpointId-snraId.rcfgId.randomHash.vpc-lattice-rsc.region.on.aws
```

O nome DNS padrão para um serviço do Lattice na rede de serviço tem a seguinte sintaxe:

```
endpointId-snsaId.randomHash.vpc-lattice-svcs.region.on.aws
```

Se você estiver usando o Console de gerenciamento da AWS, você pode encontrar o nome DNS na guia Associações. Se você estiver usando o AWS CLI, use o comando describe-vpc-endpoint-associations.

Você só pode habilitar o DNS privado quando sua rede de serviços tem uma configuração de ARN-type recursos para um serviço de banco de dados do Amazon RDS. Com o DNS privado, você pode continuar fazendo solicitações ao recurso usando o nome DNS provisionado para o recurso pelo AWS serviço, enquanto aproveita a conectividade privada por meio do endpoint VPC da rede de serviços. Para obter mais informações, consulte the section called “Resolução do DNS”.

Resolução do DNS

Quando você cria um endpoint de rede de serviço, nós criamos nomes DNS para cada configuração de recurso e serviço do Lattice associado à rede de serviço. Esses registros DNS são públicos. Logo, esses nomes DNS podem ser resolvidos publicamente. Porém, as solicitações ao DNS de fora da VPC continuam a retornar os endereços IP privados das interfaces de rede do endpoint de rede de serviço. Você pode usar esses nomes DNS para acessar o recurso e os serviços da rede on-premises, desde que tenha acesso à VPC em que o endpoint de rede de serviço se encontra, por VPN ou Direct Connect.

DNS privado

Se você habilitar o DNS privado para seu endpoint VPC de rede de serviços e sua VPC tiver nomes de host DNS e resolução de DNS ativados, criaremos zonas hospedadas privadas AWS ocultas e gerenciadas para as configurações de recursos que têm nomes DNS personalizados. A zona

hospedada contém um conjunto de registros para o nome DNS padrão do recurso que é resolvido para os endereços IP privados das interfaces de rede do endpoint em sua rede de serviço.

A Amazon fornece um servidor de DNS à VPC, o Route 53 Resolver. O Route 53 Resolver resolve automaticamente nomes de domínio de VPC locais e os registra em zonas hospedadas privadas. No entanto, não é possível usar o Route 53 Resolver de fora da sua VPC. Se desejar acessar o endpoint da VPC da sua rede on-premises, você poderá usar os nomes DNS padrão ou os endpoints do Route 53 Resolver e as regras do Resolver. Para obter mais informações, consulte Integração AWS Transit Gateway com AWS PrivateLink e. Amazon Route 53 Resolver

Zonas de disponibilidade e sub-redes

Você pode configurar seu endpoint de rede de serviços com uma sub-rede por zona de disponibilidade. Criamos uma interface de rede elástica para o VPC endpoint em cada sub-rede que você especificar. Atribuímos endereços IP a cada interface de rede elástica a partir de sua sub-rede da seguinte forma:

- Serviços VPC Lattice (camada 7) — Atribuímos um bloco /28 (16 endereços IPv4 contíguos) por zona de disponibilidade para todos os serviços VPC Lattice associados à rede de serviços. Esse bloco /28 é alocado quando o endpoint da rede de serviços é criado, mesmo que não haja serviços atualmente na rede de serviços. O bloco /28 deve consistir em 16 endereços IPv4 contíguos e não ocupados e não pode se sobrepor aos cinco endereços AWS reservados (primeiros quatro e último IP). Certifique-se de que haja espaço de endereço contíguo livre suficiente disponível. Para IPv6, também atribuímos um bloco /80 por zona de disponibilidade para serviços VPC Lattice.
- Recursos de rede VPC (camada 4/TCP) — atribuímos um endereço IPv4 por configuração de recurso por zona de disponibilidade. O espaço de endereço contíguo não é necessário para os recursos do VPC Lattice. Alocamos até 63 endereços IP por interface de rede elástica. Quando configurações de recursos adicionais excedem esse limite, criamos outra interface de rede elástica na mesma sub-rede. Para IPv6, atribuímos um bloco /80 na primeira interface de rede elástica criada para recursos; nenhuma interface de rede elástica adicional é criada ao usar IPv6. Quando você remove uma configuração de recurso da rede de serviços, liberamos o endereço IP associado. Quando todos os endereços IPv4 em uma interface de rede elástica são liberados, removemos a interface de rede elástica.

Em um ambiente de produção, para alta disponibilidade e resiliência, recomendamos que você configure pelo menos duas zonas de disponibilidade para cada endpoint da rede de serviços e garanta que cada sub-rede tenha endereços IPv4 disponíveis suficientes.

Tipos de endereço IP

Service-network os endpoints podem oferecer suporte a endereços IPv4, IPv6 ou de pilha dupla. Os endpoints que oferecem suporte a IPv6 podem responder a consultas de DNS com registros AAAA. O tipo de endereço IP de um endpoint de rede de serviço deve ser compatível com as sub-redes de endpoint de recurso, como descrito aqui:

- IPv4: atribua endereços IPv4 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4.
- IPv6: atribua endereços IPv6 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas forem sub-redes IPv6 apenas.
- Dualstack: atribua endereços IPv4 e IPv6 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4 e IPv6.

Se um endpoint da VPC de rede de serviço for compatível com IPv4, as interfaces de rede de endpoint terão endereços IPv4. Se um endpoint da VPC de rede de serviço for compatível com IPv6, as interfaces de rede de endpoint terão endereços IPv6. Não é possível acessar o endereço IPv6 de uma interface de rede de endpoint pela Internet. Se você descrever uma interface de rede de endpoint com um endereço IPv6, observe que `denyAllIgwTraffic` está habilitado.

Acessar uma rede de serviço por um endpoint de rede de serviço

Você pode acessar uma rede de serviço usando um endpoint de rede de serviço. Um endpoint de rede de serviço fornece acesso privado às configurações de recursos e serviços na rede de serviço.

Pré-requisitos

Para criar um endpoint de rede de serviço, você deve atender aos pré-requisitos a seguir.

- Você deve ter uma rede de serviço que foi criada por você ou compartilhada com você de outra conta pelo AWS RAM.
- Se uma rede de serviço for compartilhada com você de outra conta, será necessário revisar e aceitar o compartilhamento de recursos que contém a rede de serviço. Para obter mais informações, consulte Aceitar e rejeitar convites no Guia do usuário do AWS RAM .
- Para serviços VPC Lattice associados à rede de serviços, o endpoint da rede de serviços exige um bloco /28 contíguo (16 endereços IPv4) por zona de disponibilidade. Esse bloco /28 é alocado

quando o endpoint é criado, mesmo que nenhum serviço esteja atualmente na rede de serviços. O bloco /28 deve consistir em 16 endereços IPv4 contíguos e não ocupados e não pode se sobrepor aos cinco endereços AWS reservados (os primeiros quatro e o último IP na sub-rede). Para IPv6, um bloco /80 por zona de disponibilidade é alocado para serviços VPC Lattice. Verifique se há espaço de endereço contíguo livre suficiente disponível em cada sub-rede selecionada.

- Para recursos do VPC Lattice (Layer 4/TCP) associados à rede de serviços, é necessário um endereço IPv4 por configuração de recurso por zona de disponibilidade. Não é necessário espaço de endereço contíguo. Até 63 endereços IP podem ser alocados por interface de rede elástica. Quando configurações adicionais de recursos excedem esse limite, uma interface de rede elástica adicional é criada na mesma sub-rede. Para IPv6, um bloco /80 é atribuído na primeira interface de rede elástica criada para recursos; nenhuma interface de rede elástica adicional é criada ao usar IPv6.

Se você precisar evitar o consumo de endereços IP CIDR da VPC ou prever um grande número de configurações de recursos associadas à rede de serviços, considere usar uma associação VPC da rede de serviços. Para obter mais informações, consulte Manage VPC endpoint associations no Amazon VPC Lattice User Guide.

Criação de um endpoint de rede de serviço

Crie um endpoint de rede de serviço para acessar a rede de serviço que foi compartilhada com você. Depois de criar um endpoint de rede de serviço, você somente poderá modificar seus grupos de segurança ou tags.

Para criar um endpoint de rede de serviço

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, em PrivateLink e Lattice, escolha Endpoints.
3. Escolha Criar endpoint.
4. Você pode especificar um nome para facilitar a localização e o gerenciamento do endpoint.
5. Em Tipo, escolha Redes de serviço.
6. Em Redes de serviços, selecione a rede de serviço.
7. Em Configurações de rede, selecione sua VPC da qual você acessará a rede de serviço.
8. Se você quiser configurar o suporte a DNS privado, selecione Configurações adicionais, Ativar nome DNS privado. Para usar esse atributo, certifique-se de que os atributos Habilitar hostnames DNS e Habilitar compatibilidade com DNS sejam habilitados para sua VPC.

9. Em Sub-redes, selecione uma sub-rede na qual será criada a interface de rede de endpoint.

   Em um ambiente de produção, para garantir alta disponibilidade e resiliência, recomendamos configurar pelo menos duas zonas de disponibilidade para cada endpoint da VPC.

10. Em Grupos de segurança, selecione um grupo de segurança.

    Se você não especificar um grupo de segurança, associaremos o grupo de segurança padrão para a VPC.

11. Escolha Criar endpoint.

Para criar um endpoint de rede de serviço usando a linha de comando

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Gerenciar endpoints de rede de serviço

Depois de criar um endpoint de rede de serviço, você poderá atualizar apenas seus grupos de segurança ou tags.

Tarefas

- Excluir um endpoint
- Atualizar um endpoint de rede de serviço

Excluir um endpoint

Quando não precisar mais de um endpoint da VPC, você poderá excluí-lo.

Para excluir um endpoint usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint de rede de serviço.
4. Escolha Actions (Ações), Delete VPC endpoints (Excluir endpoints da VPC).
5. Quando a confirmação for solicitada, insira **`delete`**.

6. Escolha Excluir.

Para excluir um endpoint usando a linha de comando

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Atualizar um endpoint de rede de serviço

Você pode atualizar um endpoint da VPC.

Para atualizar um endpoint usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint.
4. Escolha Ações e a opção apropriada.
5. Siga as etapas do console para enviar a atualização.

Para atualizar um endpoint usando a linha de comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

Gerenciamento de identidade e acesso para AWS PrivateLink

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar AWS PrivateLink os recursos. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Conteúdo

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz AWS PrivateLink.

Usuário do serviço — Se você usar o AWS PrivateLink serviço para realizar seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais AWS PrivateLink recursos para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar a solicitar as permissões corretas ao administrador.

Administrador de serviços — Se você é responsável pelos AWS PrivateLink recursos da sua empresa, provavelmente tem acesso total AWS PrivateLink a. É seu trabalho determinar quais AWS PrivateLink recursos e recursos seus usuários do serviço devem acessar. Envie as solicitações ao administrador do IAM para alterar as permissões dos usuários de serviço. Revise as informações nesta página para compreender os conceitos básicos do IAM.

Administrador do IAM: se você for um administrador do IAM, talvez queira saber detalhes sobre como pode gravar políticas para gerenciar o acesso ao AWS PrivateLink.

Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado como usuário do IAM ou assumindo uma função do IAM. Usuário raiz da conta da AWS

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como Centro de Identidade do AWS IAM (IAM Identity Center), autenticação de login único ou credenciais. Google/Facebook Para ter mais informações sobre como fazer login, consulte Como fazer login em sua Conta da AWS no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para ter mais informações, consulte AWS Signature Version 4 para solicitações de API no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente recomendável não usar o usuário-raiz em tarefas diárias. Consulte as tarefas que exigem credenciais de usuário-raiz em Tarefas que exigem credenciais de usuário-raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários humanos usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório corporativo, provedor de identidade da web ou Directory Service que acessa Serviços da AWS usando credenciais de uma fonte de identidade. As identidades federadas assumem funções que oferecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos Centro de Identidade do AWS IAM. Para saber mais, consulte O que é o IAM Identity Center? no Guia do usuário do Centro de Identidade do AWS IAM .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte Exigir que usuários humanos usem a federação com um provedor de identidade para acessar AWS usando credenciais temporárias no Guia do usuário do IAM.

Um grupo do IAM especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para ter mais informações, consulte Casos de uso de usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Uma perfil do IAM é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função mudando de um usuário para uma função do IAM (console) ou chamando uma operação de AWS API AWS CLI ou. Para saber mais, consulte Métodos para assumir um perfil no Manual do usuário do IAM.

Os perfis do IAM são úteis para acesso de usuário federado, permissões de usuário do IAM temporárias, acesso entre contas, acesso entre serviços e aplicações em execução no Amazon EC2. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para ter mais informações sobre documentos de política JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Por meio de políticas, os administradores especificam quem tem acesso a que, definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona aos perfis, os quais os usuários podem então assumir. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

Identity-based políticas

Identity-based políticas são documentos de políticas de permissões JSON que você anexa a uma identidade (usuário, grupo ou função). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Identity-based as políticas podem ser políticas em linha (incorporadas diretamente em uma única identidade) ou políticas gerenciadas (políticas autônomas anexadas a várias identidades). Para saber como escolher entre uma política gerenciada e políticas em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Resource-based políticas

Resource-based políticas são documentos de política JSON que você anexa a um recurso. Entre os exemplos estão políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. É necessário especificar uma entidade principal em uma política baseada em recursos.

Resource-based políticas são políticas embutidas que estão localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para saber mais sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de Controle de Serviços (SCPs): as SCPs especificam o número máximo de permissões para uma organização ou uma unidade organizacional no AWS Organizations. Para saber mais, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .
- Políticas de controle de recursos (RCPs): definem o número máximo de permissões disponíveis para recursos em suas contas. Consulte mais informações em Resource control policies (RCPs) no Guia do usuário do AWS Organizations .

- Políticas de sessão: políticas avançadas transmitidas como um parâmetro durante a criação de uma sessão temporária para um perfil ou um usuário federado. Para saber mais, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como AWS PrivateLink funciona com o IAM

Antes de usar o IAM para gerenciar o acesso AWS PrivateLink, saiba com quais recursos do IAM estão disponíveis para uso AWS PrivateLink.

Recurso do IAM	AWS PrivateLink apoio
Identity-based políticas	Sim
Resource-based políticas	Sim
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC (tags em políticas)	Sim
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não

Recurso do IAM	AWS PrivateLink apoio
Service-linked funções	Não

Para ter uma visão de alto nível de como AWS PrivateLink e outros Serviços da AWS funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Identity-based políticas para AWS PrivateLink

Compatível com políticas baseadas em identidade: sim

Identity-based políticas são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como um usuário do IAM, um grupo de usuários ou uma função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais atributos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Identity-based exemplos de políticas para AWS PrivateLink

Para ver exemplos de políticas AWS PrivateLink baseadas em identidade, consulte. Identity-based exemplos de políticas para AWS PrivateLink

Resource-based políticas dentro AWS PrivateLink

Compatível com políticas baseadas em recursos: sim

Resource-based políticas são documentos de política JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. É necessário especificar uma

entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, é possível especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

AWS PrivateLink O serviço oferece suporte a um tipo de política baseada em recursos, conhecida como política de endpoint. Uma política de endpoint controla quais entidades principais da AWS poderão usar o endpoint para acessar o serviço de endpoint. Para obter mais informações, consulte the section called “Políticas de endpoint”.

Ações políticas para AWS PrivateLink

Compatível com ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. Incluem ações em uma política para conceder permissões para executar a operação associada.

Ações no namespace do ec2

Algumas ações do AWS PrivateLink fazem parte da API do Amazon EC2. Essas ações de política usam o prefixo `ec2`. Para obter mais informações, consulte Ações de AWS PrivateLink na Referência de API do Amazon EC2.

Ações no namespace do vpce

AWS PrivateLink também fornece a ação `AllowMultiRegion` somente de permissões. Essa ação de política usa o prefixo `vpce`.

Recursos políticos para AWS PrivateLink

Compatível com recursos de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Para ações que não oferecem compatibilidade com permissões em nível de recurso, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Chaves de condição de política para AWS PrivateLink

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` especifica quando as instruções são executadas com base em critérios definidos. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

As seguintes chaves de condição são específicas para AWS PrivateLink:

- `ec2:VpceMultiRegion`
- `ec2:VpceServiceName`
- `ec2:VpceServiceOwner`
- `ec2:VpceServicePrivateDnsName`
- `ec2:VpceServiceRegion`
- `ec2:VpceSupportedRegion`

Para obter mais informações, consulte Condition keys for Amazon EC2.

ACLs em AWS PrivateLink

Compatível com ACLs: não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com AWS PrivateLink

Compatível com ABAC (tags em políticas): sim

Attribute-based controle de acesso (ABAC) é uma estratégia de autorização que define permissões com base em atributos chamados de tags. Você pode anexar tags a entidades e AWS recursos do IAM e, em seguida, criar políticas ABAC para permitir operações quando a tag do diretor corresponder à tag no recurso.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para saber mais sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso por atributo (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com AWS PrivateLink

Compatível com credenciais temporárias: sim

As credenciais temporárias fornecem acesso de curto prazo aos AWS recursos e são criadas automaticamente quando você usa a federação ou troca de funções. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para ter mais informações, consulte Credenciais de segurança temporárias no IAM e Serviços da Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Cross-service permissões principais para AWS PrivateLink

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

As sessões de acesso direto (FAS) usam as permissões do principal chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) de fazer solicitações aos serviços posteriores. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Funções de serviço para AWS PrivateLink

Compatível com perfis de serviço: não

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para saber mais, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

Service-linked funções para AWS PrivateLink

Compatível com perfis vinculados ao serviço: Não

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir a função de realizar uma ação em seu nome. Service-linked as funções aparecem no seu Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

Identity-based exemplos de políticas para AWS PrivateLink

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do AWS PrivateLink . Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos por AWS PrivateLink, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para o Amazon EC2 na Referência de autorização de serviço.

Exemplos

- Controlar o uso dos VPC endpoints
- Controlar a criação de VPC endpoints com base no proprietário do serviço
- Controlar os nomes de DNS privados que podem ser especificados para serviços do VPC endpoint
- Controlar os nomes de serviço que podem ser especificados para serviços do VPC endpoint

Controlar o uso dos VPC endpoints

Por padrão, os usuários do não têm permissão para trabalhar com endpoints. Você pode criar uma política baseada em identidade que conceda aos usuários permissão para criar, modificar, descrever e excluir endpoints. Veja um exemplo do a seguir:

JSON

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect": "Allow",
            "Action":"ec2:*VpcEndpoint*",
            "Resource":"*"
        }
    ]
}
```

Para obter informações sobre como controlar o acesso a serviços que usam VPC endpoints, consulte the section called “Políticas de endpoint”.

Controlar a criação de VPC endpoints com base no proprietário do serviço

É possível usar a chave de condição `ec2:VpceServiceOwner` para controlar qual endpoint da VPC pode ser criado com base em quem é o proprietário do serviço (`amazon`, `aws-marketplace` ou o ID da conta). O seguinte exemplo concede permissão para criar endpoints da VPC com o proprietário do serviço especificado. Para usar o exemplo, substitua a região, o ID da conta e o proprietário do serviço.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
```

```
                "arn:aws:ec2:us-east-1:111111111111:vpc/*",
                "arn:aws:ec2:us-east-1:111111111111:security-group/*",
                "arn:aws:ec2:us-east-1:111111111111:subnet/*",
                "arn:aws:ec2:us-east-1:111111111111:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceOwner": [
                        "amazon"
                    ]
                }
            }
        }
    ]
}
```

Controlar os nomes de DNS privados que podem ser especificados para serviços do VPC endpoint

É possível usar a chave de condição `ec2:VpceServicePrivateDnsName` para controlar qual serviço do endpoint da VPC pode ser modificado ou criado com base no nome de DNS privado associado ao serviço do endpoint da VPC. O seguinte exemplo concede permissão para criar um serviço do endpoint da VPC com o nome de DNS privado especificado. Para usar o exemplo, substitua a região, o ID da conta e o nome de DNS privado.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:ModifyVpcEndpointServiceConfiguration",
                "ec2:CreateVpcEndpointServiceConfiguration"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint-service/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServicePrivateDnsName": [
                        "example.com"
                    ]
                }
            }
        }
    ]
}
```

Controlar os nomes de serviço que podem ser especificados para serviços do VPC endpoint

É possível usar a chave de condição `ec2:VpceServiceName` para controlar qual VPC endpoint pode ser criado com base no nome do serviço do VPC endpoint. O seguinte exemplo concede permissão para criar um endpoint da VPC com o nome do serviço especificado. Para usar o exemplo, substitua a região, o ID da conta e o nome do serviço.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc/*",
                "arn:aws:ec2:us-east-1:111111111111:security-group/*",
                "arn:aws:ec2:us-east-1:111111111111:subnet/*",
                "arn:aws:ec2:us-east-1:111111111111:route-table/*"
            ]
        },
```

```
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.111111111111.s3"
                    ]
                }
            }
        }
    ]
}
```

Controlar o acesso a endpoints da usando políticas de endpoint

Uma política de endpoint é uma política baseada em recursos que você anexa a um endpoint VPC para controlar quais AWS diretores podem usar o endpoint para acessar um. AWS service (Serviço da AWS)

Uma política de endpoint não substitui políticas baseadas em identidade nem políticas baseadas em recursos. Por exemplo, se você estiver usando um endpoint da interface para se conectar ao Amazon S3, também poderá usar políticas de bucket do Amazon S3 para controlar o acesso a buckets de endpoints específicos ou de VPCs específicas.

Conteúdo

Considerações

- Uma política de endpoint é um documento de política JSON que usa a linguagem de política do IAM. A política deve conter um elemento Principal. O tamanho de uma política de endpoint não pode exceder 20.480 caracteres, incluindo espaços em branco.
- Ao criar uma interface ou um endpoint de gateway para um AWS service (Serviço da AWS), você pode anexar uma única política de endpoint ao endpoint. Você pode atualizar a política de endpoint a qualquer momento. Se você não anexar uma política de endpoint, anexaremos a política de endpoint padrão.
- Nem todas Serviços da AWS oferecem suporte a políticas de endpoint. Se um AWS service (Serviço da AWS) não oferecer suporte às políticas de endpoint, permitimos acesso total a qualquer endpoint do serviço. Para obter mais informações, consulte the section called “Visualizar suporte a politicas de endpoint”.
- Quando você cria um endpoint da VPC para um serviço de endpoint diferente de um AWS service (Serviço da AWS), nós permitimos acesso total ao endpoint.
- Não é permitido usar caracteres curinga (* ou?) ou operadores de condições numéricas com chaves de contexto globais que fazem referência a identificadores gerados pelo sistema (por exemplo, `aws:PrincipalAccount` ou `aws:SourceVpc`).
- Ao usar um operador de condição de cadeia de caracteres, você deve usar pelo menos seis caracteres consecutivos antes ou depois de cada caractere curinga.
- Quando você especifica um ARN em um elemento de recurso ou condição, a parte da conta do ARN pode incluir um ID de conta ou um caractere curinga, mas não ambos.
- Depois que você atualizar uma política de endpoint, poderá levar alguns minutos para que as alterações sejam aplicadas.

Política de endpoint padrão

A política de endpoint padrão concede acesso total ao endpoint.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*"
```

```
        }
    ]
}
```

Políticas para endpoints de interface

Por exemplo, políticas de endpoint para Serviços da AWS, consultethe section called “Serviços que se integram”. A primeira coluna da tabela contém links para a AWS PrivateLink documentação de cada uma AWS service (Serviço da AWS). Se um AWS service (Serviço da AWS) oferece suporte a políticas de endpoint, sua documentação inclui exemplos de políticas de endpoint.

Entidades principais de endpoints de gateway

Com endpoints de gateway, o elemento `Principal` deve ser definido como `*`. Para especificar uma entidade principal, use a chave de condição `aws:PrincipalArn`.

```
"Condition": {
    "StringEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:user/endpointuser"
    }
}
```

Se você especificar a entidade principal no formato abaixo, o acesso será concedido somente ao Usuário raiz da conta da AWS , e não a todos os usuários e perfis da conta.

```
"AWS": "account_id"
```

Veja abaixo alguns exemplos de políticas do endpoint para endpoints de gateway:

- Endpoints para o Amazon S3
- Endpoints para o DynamoDB

Atualizar uma política de endpoint da VPC

Use o seguinte procedimento para atualizar uma política de endpoint para um AWS service (Serviço da AWS). Depois que você atualizar uma política de endpoint, poderá levar alguns minutos para que as alterações sejam aplicadas.

Para atualizar uma política de endpoint usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint da VPC.
4. Escolha Actions (Ações), Manage policy (Gerenciar política).
5. Escolha Full Access (Acesso total) para permitir acesso total ao serviço ou escolha Custom (Personalizado) e anexe uma política personalizada.
6. Escolha Salvar.

Para atualizar uma política de endpoint usando a linha de comando

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Ferramentas para Windows PowerShell)

AWS políticas gerenciadas para AWS PrivateLink

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) for lançada ou novas operações de API forem disponibilizadas para serviços existentes.

Para saber mais, consulte AWS Políticas gerenciadas pela no Guia do usuário do IAM.

AWS PrivateLink atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas AWS PrivateLink desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página Histórico do AWS PrivateLink documento.

Alteração	Descrição	Data
AWS PrivateLink começou a rastrear as alterações	AWS PrivateLink começou a rastrear as mudanças em suas políticas AWS gerenciadas.	1.º de março de 2021

CloudWatch métricas para AWS PrivateLink

AWS PrivateLink publica pontos de dados na Amazon CloudWatch para seus endpoints de interface, endpoints do Gateway Load Balancer e serviços de endpoint. CloudWatch permite que você recupere estatísticas sobre esses pontos de dados como um conjunto ordenado de dados de séries temporais, conhecido como métricas. Considere uma métrica como uma variável a ser monitorada, e os pontos de dados como os valores dessa variável ao longo do tempo. Cada ponto de dados tem um time stamp associado e uma unidade de medida opcional.

É possível usar métricas para verificar se o sistema está executando conforme o esperado. Por exemplo, você pode criar um CloudWatch alarme para monitorar uma métrica específica e iniciar uma ação (como enviar uma notificação para um endereço de e-mail) se a métrica estiver fora do que você considera um intervalo aceitável.

Métricas são publicadas para todos os endpoints de interface, endpoints de balanceador de carga de gateway e serviços de endpoint. Elas não são publicadas para endpoints de gateway nem para consumidores de serviço de endpoint que usam acesso inter-regional. Por padrão, AWS PrivateLink envia métricas para CloudWatch em intervalos de um minuto, sem custo adicional.

Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

Conteúdo

Métricas e dimensões de endpoints

O namespace `AWS/PrivateLinkEndpoints` inclui as seguintes métricas para endpoints de interface e endpoints de balanceador de carga de gateway.

Métrica	Description
`ActiveConnections`	O número de conexões ativas simultâneas. Isso métrica inclui conexões nos estados SYN_SENT e ESTABLISHED.

Métrica	Description
	Reporting criteria (Critérios de relatório): o endpoint recebeu tráfego durante o período de um minuto. Estatísticas: as estatísticas mais úteis são `Average`, `Maximum` e `Minimum`. Dimensões • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`
`BytesProcessed`	O número de bytes que foram trocados entre os endpoints e os serviços de endpoint, agregados em ambas as direções. Este é o número de bytes cobrados do proprietário do endpoint. A fatura discrimina esse valor em GB. Reporting criteria (Critérios de relatório): o endpoint recebeu tráfego durante o período de um minuto. Statistics (Estatísticas): as estatísticas mais úteis são `Average`, `Sum`, `Maximum` e `Minimum`. Dimensões • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Métrica	Description
`NewConnections`	O número de novas conexões estabelecidas por meio do endpoint. Reporting criteria (Critérios de relatório): o endpoint recebeu tráfego durante o período de um minuto. Statistics (Estatísticas): as estatísticas mais úteis são `Average`, `Sum`, `Maximum` e `Minimum`. Dimensões • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`
`PacketsDropped`	O número de pacotes descartados pelo endpoint. Essa métrica pode não capturar todos os descartes de pacotes. Um aumento nos valores pode indicar que o serviço de endpoint ou o endpoint não está íntegro. Reporting criteria (Critérios de relatório): o endpoint recebeu tráfego durante o período de um minuto. Estatísticas: as estatísticas mais úteis são `Average`, `Sum` e `Maximum`. Dimensões • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Métrica	Description
`RstPacketsReceived`	O número de pacotes RST recebidos pelo endpoint. Um aumento nos valores pode indicar que o serviço de endpoint não está íntegro. Reporting criteria (Critérios de relatório): o endpoint recebeu tráfego durante o período de um minuto. Estatísticas: as estatísticas mais úteis são `Average`, `Sum` e `Maximum`. Dimensões • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Para filtrar essas métricas, use as seguintes dimensões.

Dimensão	Description
`Endpoint Type`	Filtra os dados das métricas por tipo de endpoint (`Interface` | `GatewayLoadBalancer`).
`Service Name`	Filtra os dados das métricas por nome do serviço.
`Subnet Id`	Filtra os dados das métricas por sub-rede.
`VPC Endpoint Id`	Filtra os dados das métricas por endpoint da VPC.
`VPC Id`	Filtra os dados das métricas por VPC.

Métricas e dimensões de serviços de endpoint

O namespace `AWS/PrivateLinkServices` inclui as seguintes métricas para serviços de endpoint.

Métrica	Description
`ActiveConnections`	O número máximo de conexões ativas provenientes de clientes com destinos através dos endpoints. Um aumento nos valores pode indicar a necessidade de adicionar destinos ao balanceador de carga. Reporting criteria (Critérios de relatório): um endpoint que está conectado ao serviço de endpoint enviou tráfego durante o período de um minuto. Estatísticas: as estatísticas mais úteis são `Average` e `Maximum`. Dimensões • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`
`BytesProcessed`	O número de bytes que foram trocados os serviços de endpoints e endpoints, em ambas as direções. Reporting criteria (Critérios de relatório): um endpoint que está conectado ao serviço de endpoint enviou tráfego durante o período de um minuto. Estatísticas: as estatísticas mais úteis são `Average`, `Sum` e `Maximum`. Dimensões • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`
`EndpointsCount`	O número de endpoints que estão conectados ao serviço de endpoint.

Métrica	Description
	Reporting criteria (Critérios de relatório): existe um valor diferente de zero durante o período de cinco minutos. Estatísticas: as estatísticas mais úteis são `Average` e `Maximum`. Dimensões • `Service Id`
`NewConnections`	O número máximo de novas conexões estabelecidas de clientes com destinos através dos endpoints. Um aumento nos valores pode indicar a necessidade de adicionar destinos ao balanceador de carga. Reporting criteria (Critérios de relatório): um endpoint que está conectado ao serviço de endpoint enviou tráfego durante o período de um minuto. Estatísticas: as estatísticas mais úteis são `Average`, `Sum` e `Maximum`. Dimensões • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`

Métrica	Description
`RstPacketsSent`	O número de pacotes RST que foram enviados a endpoints pelo serviço de endpoint. Um aumento nos valores pode indicar que existem destinos não íntegros. Reporting criteria (Critérios de relatório): um endpoint que está conectado ao serviço de endpoint enviou tráfego durante o período de um minuto. Estatísticas: as estatísticas mais úteis são `Average`, `Sum` e `Maximum`. Dimensões • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`

Para filtrar essas métricas, use as seguintes dimensões.

Dimensão	Description
`Az`	Filtra os dados de métrica por zona de disponibilidade.
`Load Balancer Arn`	Filtra os dados da métrica por load balancer.
`Service Id`	Filtra os dados das métricas por serviço de endpoint.
`VPC Endpoint Id`	Filtra os dados das métricas por endpoint da VPC.

Veja as CloudWatch métricas

Você pode visualizar essas CloudWatch métricas usando o console da Amazon VPC, o CloudWatch console ou o AWS CLI seguinte.

Para visualizar métricas usando o console da Amazon VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints. Selecione o endpoint e escolha a guia Monitoring (Monitoramento).
3. No painel de navegação, escolha Endpoint Services (Serviços do endpoint). Selecione o serviço de endpoint e escolha a guia Monitoring (Monitoramento).

Para visualizar métricas usando o CloudWatch console

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Métricas.
3. Selecione o namespace AWS/PrivateLinkEndpoints.
4. Selecione o namespace AWS/PrivateLinkServices.

Para visualizar métricas usando o AWS CLI

Use o seguinte comando list-metrics para listar as métricas disponíveis para endpoints de interface e endpoints de balanceador de rede de gateway:

```
aws cloudwatch list-metrics --namespace AWS/PrivateLinkEndpoints
```

Use o comando list-metrics para listar as métricas disponíveis para serviços de endpoint:

```
aws cloudwatch list-metrics --namespace AWS/PrivateLinkServices
```

Usar regras integradas do Contributor Insights

AWS PrivateLink fornece regras integradas do Contributor Insights para seus serviços de endpoint para ajudá-lo a descobrir quais endpoints são os maiores contribuintes para cada métrica suportada. Para obter mais informações, consulte Contributor Insights no Guia do CloudWatch usuário da Amazon.

AWS PrivateLink fornece as seguintes regras:

- `VpcEndpointService-ActiveConnectionsByEndpointId-v1` – Classifica endpoints pelo número de conexões ativas.

- `VpcEndpointService-BytesByEndpointId-v1` – Classifica endpoints pelo número de bytes processados.
- `VpcEndpointService-NewConnectionsByEndpointId-v1` – Classifica endpoints pelo número de novas conexões.
- `VpcEndpointService-RstPacketsByEndpointId-v1` –Classifica endpoints pelo número de pacotes RST que foram enviados a endpoints.

Para usar uma regra integrada, é necessário habilitá-la. Depois que você habilita uma regra, ela começa a coletar dados do colaborador. Para obter informações sobre as cobranças do Contributor Insights, consulte Amazon CloudWatch Pricing.

É necessário ter as seguintes permissões para usar o Contributor Insights:

- `cloudwatch:DeleteInsightRules`: para excluir as regras do Contributor Insights.
- `cloudwatch:DisableInsightRules`: para desabilitar regras do Contributor Insights.
- `cloudwatch:GetInsightRuleReport`: para obter os dados.
- `cloudwatch:ListManagedInsightRules`: para listar as regras do Contributor Insights.
- `cloudwatch:PutManagedInsightRules`: para habilitar as regras do Contributor Insights.

Tarefas

- Habilitar as regras do Contributor Insights
- Desabilitar as regras do Contributor Insights
- Excluir as regras do Contributor Insights

Habilitar as regras do Contributor Insights

Use os procedimentos a seguir para ativar as regras internas para AWS PrivateLink usar o Console de gerenciamento da AWS ou AWS CLI o.

Para habilitar as regras do Contributor Insights para AWS PrivateLink usar o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).
3. Selecione o serviço de endpoint.

4. Na guia Contributor Insights, escolha Enable (Habilitar).
5. (Opcional) Por padrão, todas as regras são habilitadas. Para habilitar somente regras específicas, selecione as regras que não devem ser habilitadas e, em seguida, escolha Actions (Ações), Disable rule (Desabilitar regra). Quando a confirmação for solicitada, escolha Disable (Desabilitar).

Para habilitar as regras do Contributor Insights para AWS PrivateLink usar o AWS CLI

1. Use o comando list-managed-insight-rules, como a seguir, para enumerar as regras disponíveis. Na opção `--resource-arn`, especifique o ARN do serviço de endpoint.

```
aws cloudwatch list-managed-insight-rules --resource-arn
 arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-svc-0123456789EXAMPLE
```

2. Na saída do comando `list-managed-insight-rules`, copie o nome do modelo do campo `TemplateName`. A seguir, temos um exemplo desse campo.

```
"TemplateName": "VpcEndpointService-NewConnectionsByEndpointId-v1"
```

3. Use o comando put-managed-insight-rules, como a seguir, para habilitar a regra. Você deve especificar o nome do modelo e o ARN do serviço de endpoint.

```
aws cloudwatch put-managed-insight-rules --managed-rules
 TemplateName=VpcEndpointService-NewConnectionsByEndpointId-
v1,ResourceARN=arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-
svc-0123456789EXAMPLE
```

Desabilitar as regras do Contributor Insights

Você pode desativar as regras integradas do AWS PrivateLink a qualquer momento. Depois que você desabilitar uma regra, ela interromperá a coleta de dados do colaborador, mas os dados existentes do colaborador serão mantidos até que eles completem 15 dias. Após desabilitar uma regra, você poderá habilitá-la novamente para retomar a coleta de dados.

Para desativar as regras do Contributor Insights para AWS PrivateLink usar o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).

3. Selecione o serviço de endpoint.
4. Na guia Contributor Insights, escolha Disable all (Desabilitar todas) para desabilitar todas as regras. Como alternativa, expanda o painel Rules (Regras), selecione as regras a serem desabilitadas e escolha Actions (Ações), Disable rule(Desabilitar regra)
5. Quando a confirmação for solicitada, escolha Disable (Desabilitar).

Para desativar as regras do Contributor Insights para AWS PrivateLink usar o AWS CLI

Usar o comando disable-insight-rules para desabilitar uma regra.

Excluir as regras do Contributor Insights

Use os procedimentos a seguir para excluir as regras internas para AWS PrivateLink usar o Console de gerenciamento da AWS ou AWS CLI o. Depois que você exclui uma regra, ela interrompe a coleta de dados do colaborador e excluímos os dados existentes do colaborador.

Para excluir as regras do Contributor Insights para AWS PrivateLink usar o console

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Insights, Contributor Insights.
3. Expanda o painel Rules (Regras) e selecione as regras.
4. Escolha Actions (Ações), Delete rule (Excluir regra).
5. Quando a confirmação for solicitada, escolha Excluir.

Para excluir as regras do Contributor Insights para AWS PrivateLink usar o AWS CLI

Use o comando delete-insight-rules para excluir a regra.

AWS PrivateLink cotas

Sua AWS conta tem cotas padrão, anteriormente chamadas de limites, para cada AWS serviço. Salvo indicação em contrário, cada cota é Region-specific. Você pode solicitar o aumento de algumas cotas, porém, algumas delas não podem ser aumentadas. Se solicitar um aumento de cota que seja aplicável por recurso, aumentaremos a cota para todos os recursos na Região.

Para solicitar um aumento da cota, consulte Requesting a quota increase no Guia do usuário do Service Quotas.

Controle de utilização de solicitações

As ações de API para AWS PrivateLink fazem parte da API do Amazon EC2. O Amazon EC2 limita suas solicitações de API no mesmo nível. Conta da AWS Para obter mais informações, consulte Limitação de solicitações no Guia do desenvolvedor do Amazon ECS. Além disso, as solicitações de API também são limitadas no nível da organização para ajudar no desempenho do. AWS PrivateLink Se você estiver usando AWS Organizations e receber um código de `RequestLimitExceeded` erro enquanto ainda estiver dentro dos limites da API no nível da conta, consulte Como identificar AWS contas que fazem um grande número de chamadas de API. Se precisar de ajuda, entre em contato com a equipe da sua conta ou abra um caso de suporte técnico usando o serviço VPC e a categoria Endpoints da VPC. Certifique-se de anexar uma imagem do código de erro `RequestLimitExceeded`.

Cotas de endpoint da VPC

Sua AWS conta tem as seguintes cotas relacionadas aos VPC endpoints.

Nome	Padrão	Ajustável	Comentários
Endpoints do Gateway Load Balancer e da interface por VPC	50	Sim	Essa é uma cota combinada para endpoints de interface e endpoints do Gateway Load Balancer
VPC endpoints do gateway por Região	20	Sim	É possível criar até 255 endpoints de gateway por VPC
Endpoints da VPC de recurso por VPC	200	Sim	

Nome	Padrão	Ajustável	Comentários
Endpoints da VPC de rede de serviço por VPC	50	Sim	
Caracteres por política de endpoint da VPC	20.480	Não	O tamanho máximo de uma política de um endpoint da VPC, incluindo espaços em branco

As seguintes observações se aplicam ao tráfego que passa por um endpoint da VPC:

- Por padrão, cada endpoint da VPC é compatível com uma largura de banda de até 10 Gbps por zona de disponibilidade e pode aumentar a escala verticalmente para até 100 Gbps de modo automático. A largura de banda máxima para um endpoint da VPC ao distribuir a carga em todas as zonas de disponibilidade é o número de zonas de disponibilidade multiplicado por 100 Gbps. Se a sua aplicação precisar de throughput mais alta, entre em contato com o suporte da AWS .
- A MTU de uma conexão de rede é o tamanho, em bytes, do maior pacote permissível que pode ser passado por um endpoint da VPC. Quanto maior a MTU, mais dados podem ser passados em um único pacote. Um endpoint de VPC é compatível com uma MTU de 8500 bytes. Pacotes com um tamanho maior que 8500 bytes que chegam ao endpoint da VPC são descartados.
- Não há suporte ao Path MTU Discovery (PMTUD). Os endpoints da VPC não geram a seguinte mensagem ICMP: `Destination Unreachable: Fragmentation needed and Don't Fragment was Set` (Tipo 3, Código 4).
- Os endpoints da VPC impõem o ajuste do Maximum Segment Size (MSS – Tamanho máximo de segmento) para todos os pacotes. Para obter mais informações, consulte RFC879.

Histórico do documento para AWS PrivateLink

A tabela a seguir descreve as versões do AWS PrivateLink.

Alteração	Descrição	Data
Acessar recursos e redes de serviços	AWS PrivateLink suporta o acesso a recursos e redes de serviços em todos os limites da VPC e da conta.	1.º de dezembro de 2024
Cross-Region access	Um provedor de serviços pode hospedar um serviço em uma região e disponibilizá-lo em um conjunto de AWS regiões. Um consumidor de serviço seleciona as regiões de serviço ao criar um endpoint.	26 de novembro de 2024
Endereços IP designados	Especifique os endereços IP para as interfaces de rede do endpoint quando você criar ou modificar o endpoint da VPC.	17 de agosto de 2023
Suporte a IPv6	É possível configurar seus serviços de endpoint do Gateway Load Balancer e os endpoints do Gateway Load Balancer para oferecer suporte a endereços IPv4 e IPv6 ou somente endereços IPv6.	12 de dezembro de 2022
Contributor Insights	Você pode usar as regras integradas do Contributor Insights para identificar	18 de agosto de 2022

	endpoints específicos que são os principais contribuidores das CloudWatch métricas. AWS PrivateLink	
Suporte a IPv6	Os provedores de serviços podem permitir que o serviço de endpoint aceite solicitaç ões de IPv6, mesmo que os serviços de backend sejam compatíveis somente com IPv4. Se o serviço de endpoint aceitar solicitações IPv6, os consumidores do serviço poderão habilitar o suporte IPv6 para os endpoints de interface para que possam acessar o serviço de endpoint por IPv6.	11 de maio de 2022
CloudWatch métricas	AWS PrivateLink publica CloudWatch métricas para seus endpoints de interface , endpoints do Gateway Load Balancer e serviços de endpoint.	27 de janeiro de 2022
Endpoints do Gateway Load Balancer	Você pode criar um endpoint do Gateway Load Balancer na VPC para rotear o tráfego para um serviço do VPC endpoint que você configurou usando o Gateway Load Balancer.	10 de novembro de 2020

Políticas de VPC endpoint	Você pode anexar uma política do IAM a um endpoint da VPC de interface de um serviço da AWS para controlar o acesso a esse serviço.	23 de março de 2020
Chaves de condição para VPC endpoints e serviços de endpoint	É possível usar chaves de condição do EC2 para controlar o acesso a endpoints da VPC e serviços de endpoint.	6 de março de 2020
Marcar endpoints da VPC e serviços de endpoint na criação	É possível adicionar etiquetas ao criar endpoints da VPC ou serviços de endpoint.	5 de fevereiro de 2020
Nomes DNS privados	Você pode acessar serviços AWS PrivateLink baseados de dentro da sua VPC usando nomes DNS privados.	6 de janeiro de 2020
Serviços do VPC endpoint	Você pode criar seus próprios serviços de endpoint e permitir que outras Contas da AWS e usuários se conectem ao seu serviço por meio de um endpoint da VPC de interface . É possível oferecer serviços de endpoint para assinatura no AWS Marketplace.	28 de novembro de 2017
Interface de endpoints VPC para Serviços da AWS	Você pode criar um endpoint de interface para se conectar a Serviços da AWS essa integração AWS PrivateLi nk sem usar um gateway de internet ou dispositivo NAT.	8 de novembro de 2017

VPC endpoints para o DynamoDB	É possível criar um endpoint da VPC de gateway para acessar o Amazon DynamoDB utilizando a sua VPC sem usar um gateway de Internet ou um dispositivo de NAT.	16 de agosto de 2017
Endpoints da VPC para o Amazon S3	É possível criar um endpoint da VPC de gateway para acessar o Amazon S3 utilizando a sua VPC sem usar um gateway de Internet ou um dispositivo de NAT.	11 de maio de 2015

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.