AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

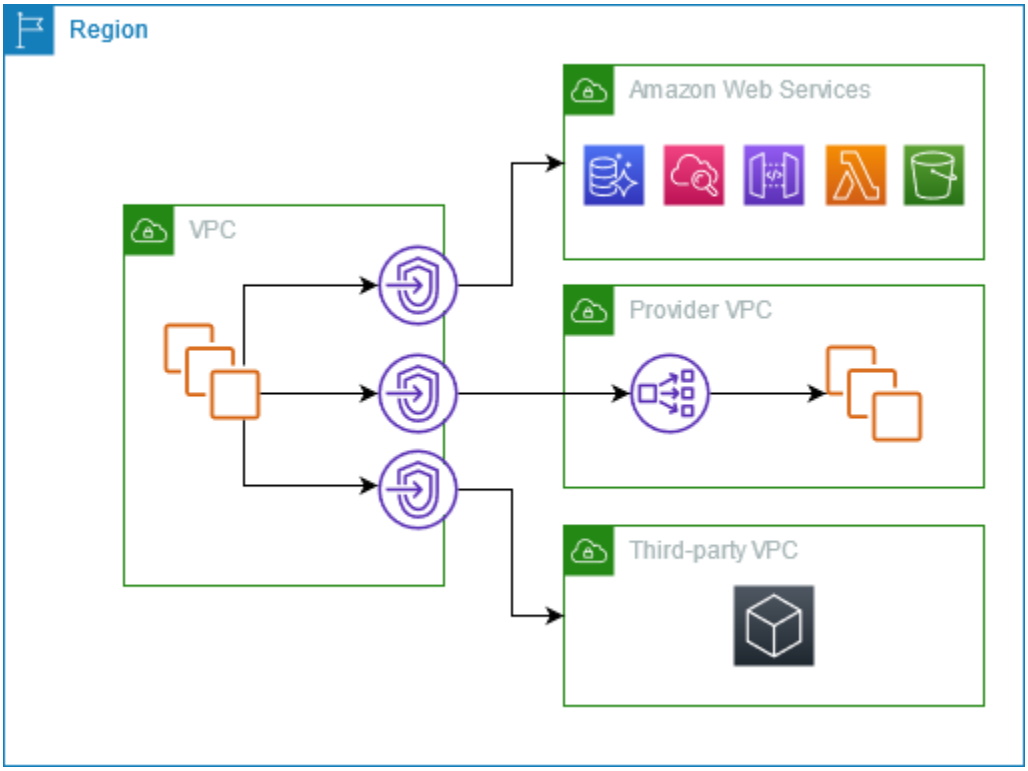
O que AWS PrivateLinké

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

Casos de uso

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

No seguinte diagrama, a VPC à esquerda tem várias instâncias do EC2 em uma sub-rede privada e três endpoints da VPC de interface. O melhor endpoint de VPC se conecta a um. AWS service (Serviço da AWS) O VPC endpoint intermediário se conecta a um serviço hospedado por outro Conta da AWS (um serviço de VPC endpoint). O VPC endpoint inferior se conecta a um AWS Marketplace serviço de parceiro.



Saiba mais

- the section called “Conceitos”
- Acesso 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:

- AWS Management Console— Fornece uma interface web que você pode usar para acessar seus AWS PrivateLink recursos. Abra o console da Amazon VPC e escolha Endpoints ou Endpoint services.
- 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.
- AWS CloudFormation: crie modelos que descrevam seus recursos da AWS . Você usa os modelos para provisionar e gerenciar esses recursos como uma só unidade. Para obter mais informações, consulte os seguintes AWS PrivateLink recursos:
  - AWS::EC2::VPCEndpoint
  - AWS: :EC2: :Notificação de VPC EndpointConnection
  - AWS::EC2::VPCEndpointService
  - AWS: :EC2: :Permissões de VPC EndpointService
  - 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 desenvolver 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.

Definição de preço

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

AWS PrivateLink conceitos

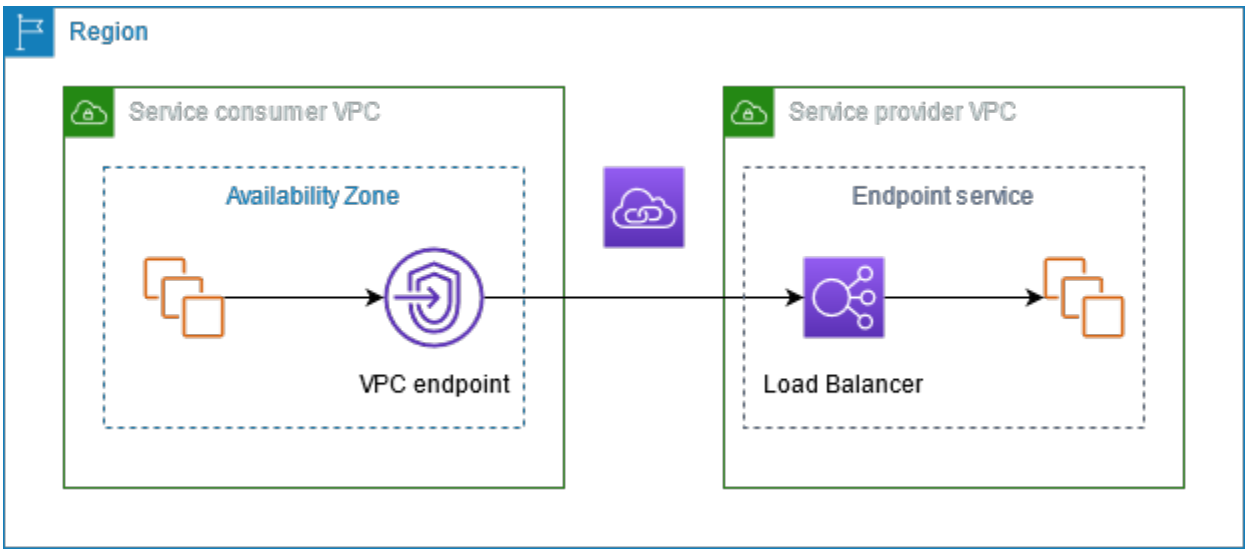
É possível usar a Amazon VPC para definir uma nuvem privada virtual (VPC), que é uma rede virtual isolada logicamente. Você pode lançar AWS recursos em sua VPC. Você pode permitir que os recursos de sua VPC se conectem a recursos fora dessa VPC. Por exemplo, adicione um gateway da internet à VPC para permitir o acesso à Internet ou adicione uma conexão da VPN para permitir o acesso à rede on-premises. Como alternativa, use AWS PrivateLink para permitir que os recursos em sua VPC se conectem a serviços em outras VPCs usando endereços IP privados, como se esses serviços 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 do serviço criam endpoints da VPC de interface para se conectar a serviços de endpoint que são hospedados pelos provedores de serviços.



Provedores 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.

Conceitos

- Serviços de endpoint
- Nomes de serviço
- Estados do serviço

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:

- `Pending`: o serviço de endpoint está sendo criado.
- `Available`: o serviço de endpoint está disponível.
- `Failed`: não foi possível criar o serviço de endpoint.
- `Deleting`: o provedor de serviços excluiu o serviço de endpoint, e a exclusão está em andamento.
- `Deleted`: o serviço de endpoint foi excluído.

Consumidores do serviço

O usuário de um serviço é um consumidor. Os consumidores de serviços podem acessar serviços de endpoint a partir de AWS recursos, como instâncias do EC2, ou de servidores locais.

Conceitos

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

Endpoints da VPC

O consumidor do serviço cria um endpoint da VPC de interface para conectar a VPC a um serviço de endpoint. O consumidor do serviço deve especificar o nome do 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 necessário para o serviço de endpoint.

- `Interface`: crie um endpoint de interface para enviar o 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.

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 ter 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 de endpoint. Para cada sub-rede que você especificar ao criar um endpoint da VPC, criamos uma interface de rede de endpoint na sub-rede.

Se um endpoint da VPC for compatível com IPv4, suas interfaces de rede do endpoint terão endereços IPv4. Se um endpoint da VPC for compatível com IPv6, suas interfaces de rede do 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.

Os endereços IP de uma interface de rede de endpoint não mudarão durante a vida útil de seu endpoint da VPC.

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, o serviço de endpoint recebe uma solicitação de conexão. O provedor de serviços pode aceitar ou rejeitar a solicitação. Se o provedor de serviços aceitar a solicitação, o consumidor do serviço poderá usar o endpoint da VPC depois que ele entrar no estado `Available`.

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.
- `Pending`: o provedor de serviços 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.
- `Available`: o endpoint da VPC está disponível para uso.
- `Rejected`: o provedor de serviços rejeitou a solicitação de conexão. O provedor de serviços também poderá rejeitar uma conexão depois que ela estiver disponível para uso.
- `Expired`: a solicitação de conexão expirou.
- `Failed`: não foi possível disponibilizar o endpoint da VPC.
- `Deleting`: o consumidor do serviço excluiu o endpoint da VPC, e a exclusão está em andamento.
- `Deleted`: o endpoint da VPC foi excluído.

AWS PrivateLink conexões

O tráfego da sua VPC é enviado para um serviço de endpoint usando uma conexão entre o endpoint da VPC e o serviço de endpoint. O tráfego entre um endpoint VPC e um serviço de endpoint permanece dentro da AWS rede, 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.

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

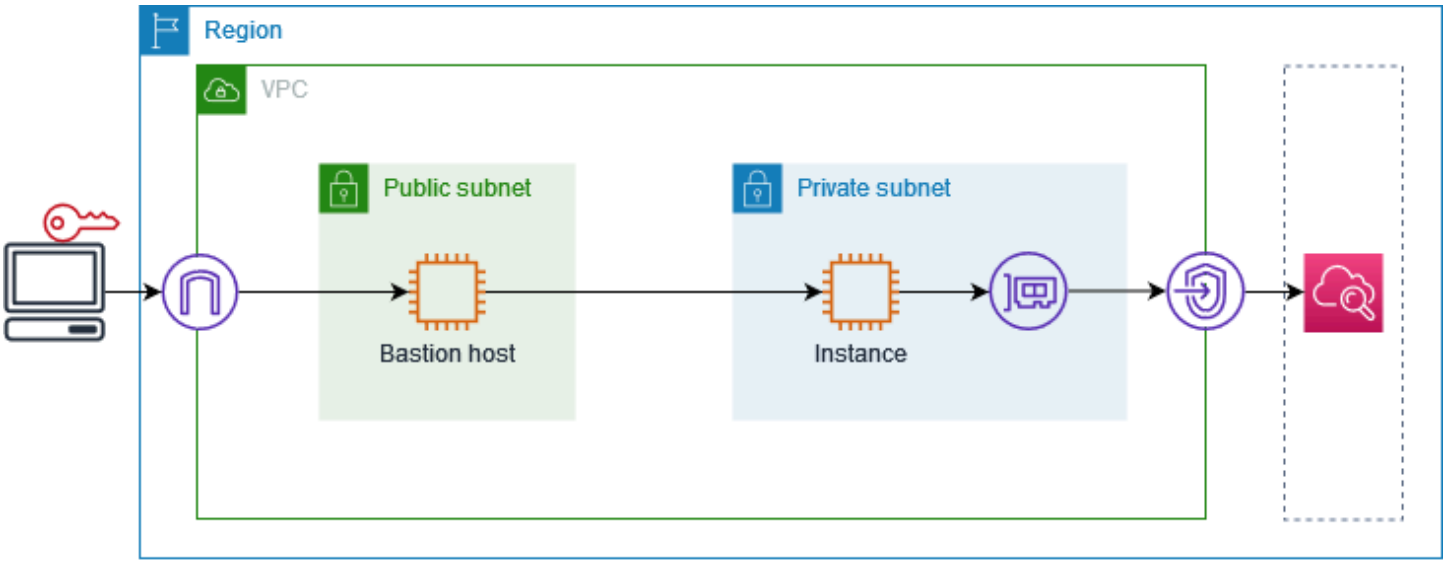
É possível configurar o Amazon Route 53 para encaminhar o tráfego do domínio a um endpoint da VPC. Para obter mais informações, consulte: Routing traffic to a VPC endpoint using your domain name (Encaminhar tráfego a um endpoint da VPC usando seu nome de domínio).

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 host bastion em uma sub-rede pública. Tanto o host bastion quanto a instância devem usar o mesmo par de chaves. Como o arquivo `.pem` da chave privada está no seu computador, e não no host bastion, você usará o encaminhamento de chaves SSH. Em seguida, você poderá conectar à instância desde o host bastion 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 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 do 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 host bastion 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 host bastion e a instância.
- Crie um grupo de segurança para o host bastion 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 host bastion.
- Crie um perfil de instância do IAM e anexe a política de CloudWatchReadOnlyacesso.

Para iniciar o host bastion

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 host bastion.
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. Em Auto-assign public IP (Atribuir IP público automaticamente), selecione Enable (Habilitar).
    d. Em Firewall, escolha Select existing security group (Selecionar grupo de segurança existente) e, em seguida, escolha o grupo de segurança para o host bastion.
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. Em Auto-assign public IP (Atribuir IP público automaticamente), selecione Disable (Desabilitar).

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. Em seu computador, adicione o par de chaves ao agente SSH usando o comando a seguir, em que *key.pem* é o nome do 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 host bastion 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 host bastion.

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

3. Connect à instância desde o host bastion. 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 Service (Serviço), selecione com.amazonaws.***region***.monitoring.
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 seguinte comando na sua 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 host bastion 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 Instances (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.

Acesse Serviços da AWS através de 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.

Definição de preço

Você é cobrado por cada hora em que sua interface VPC endpoint é provisionada em cada zona de disponibilidade. Você também é cobrado por GB de dados processados. Para obter mais informações, consulte Preços do AWS PrivateLink.

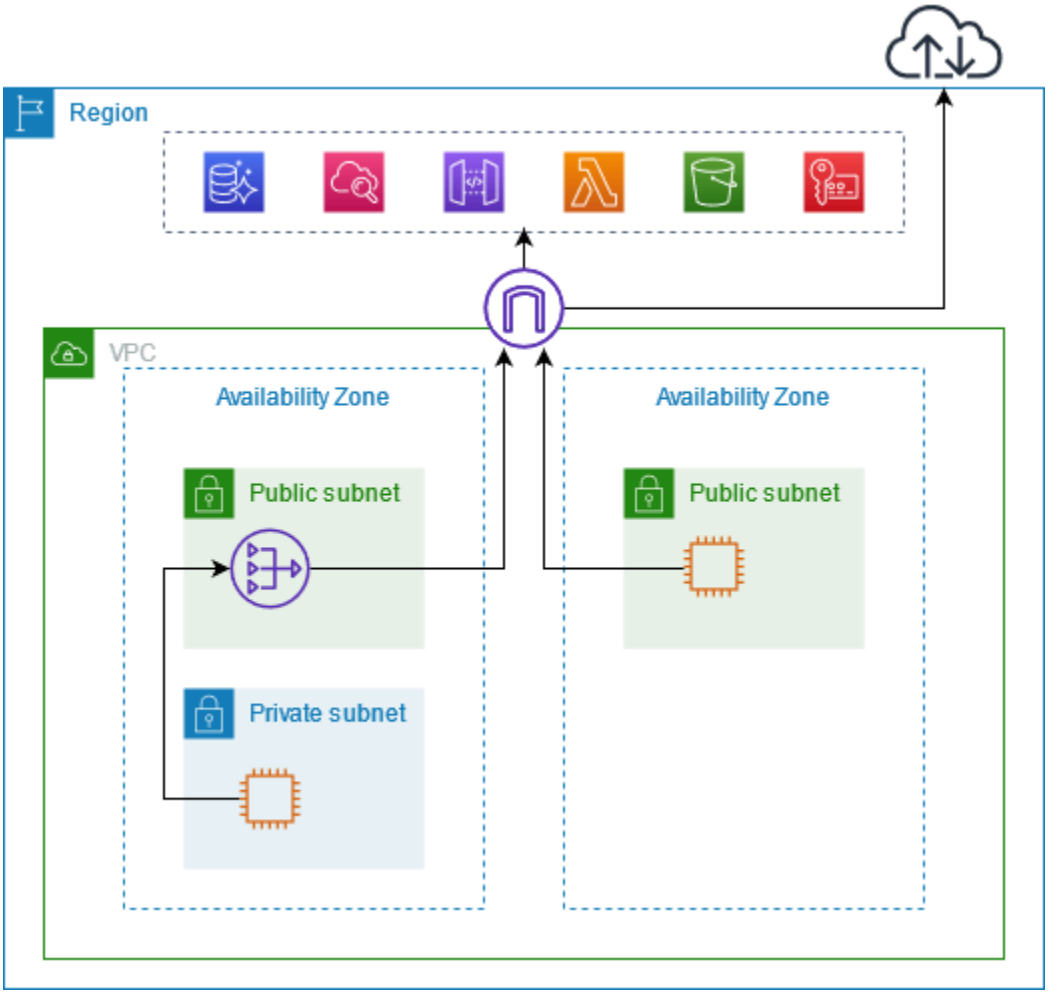
Conteúdo

Visão geral

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.

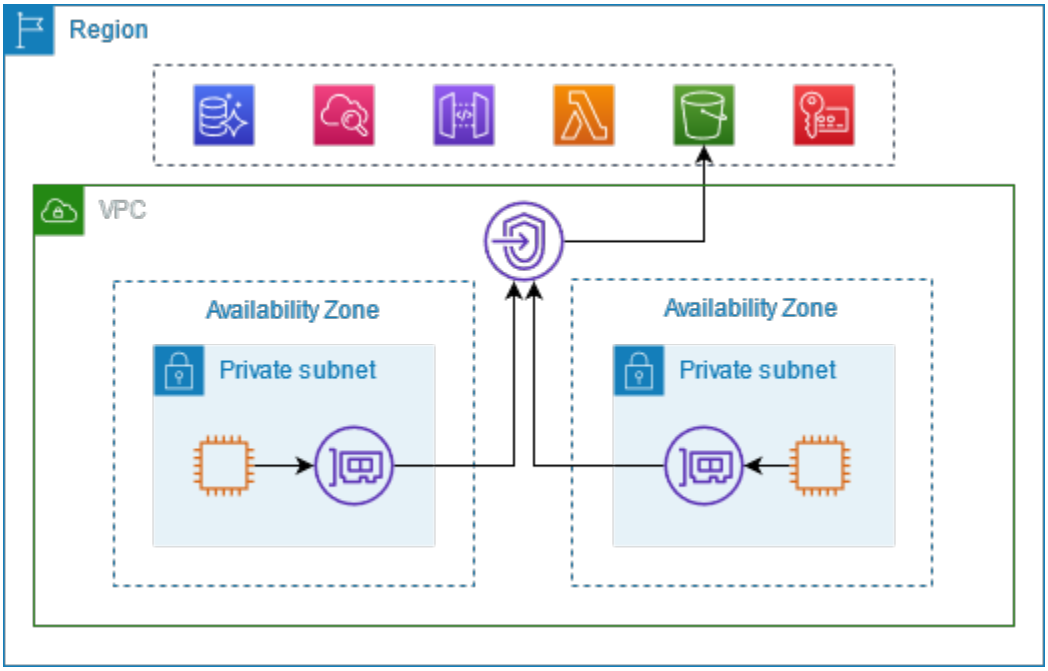
Acesso por meio de endpoints de serviço públicos

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 de 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 ter 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 VPC endpoints 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

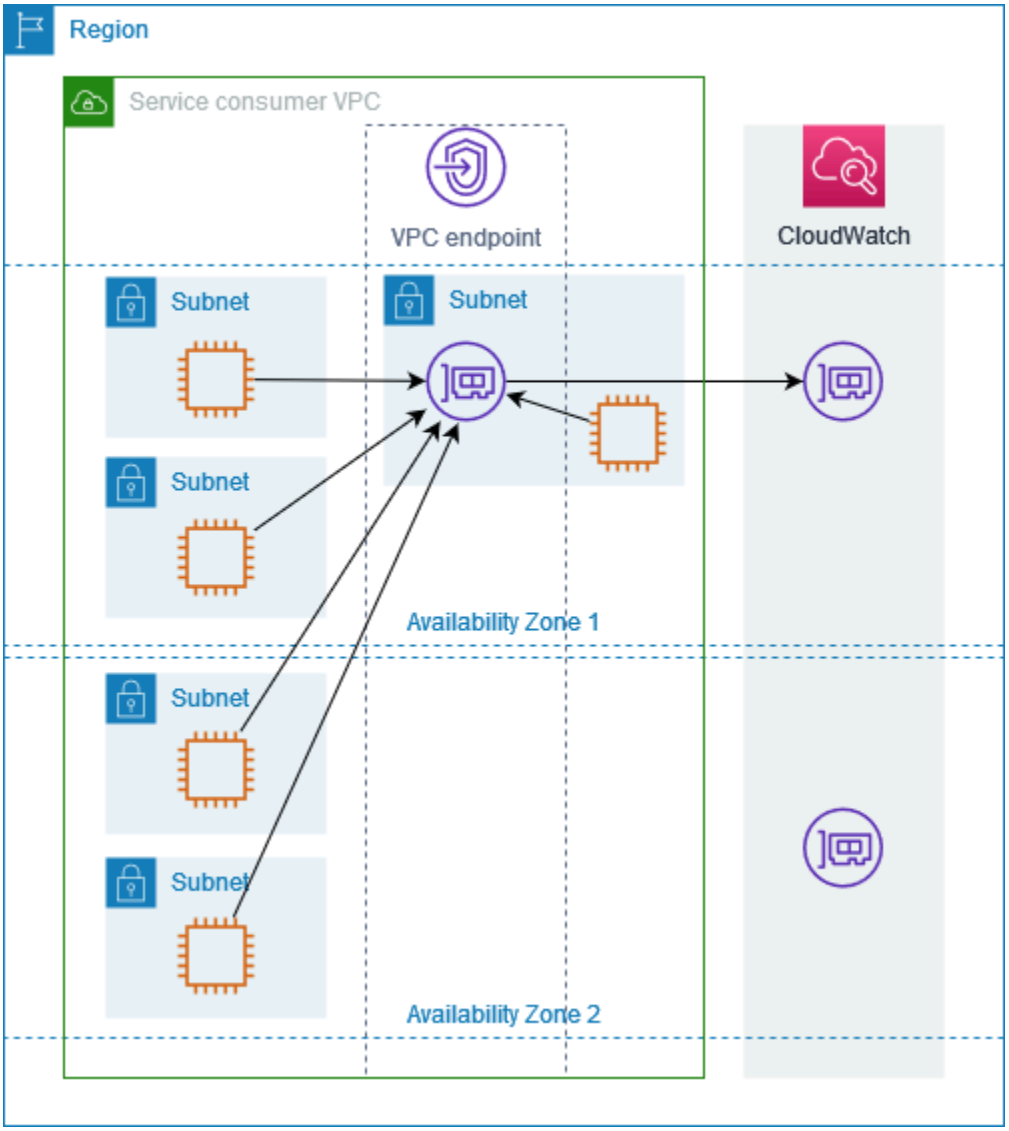
Zonas de disponibilidade e sub-redes

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.

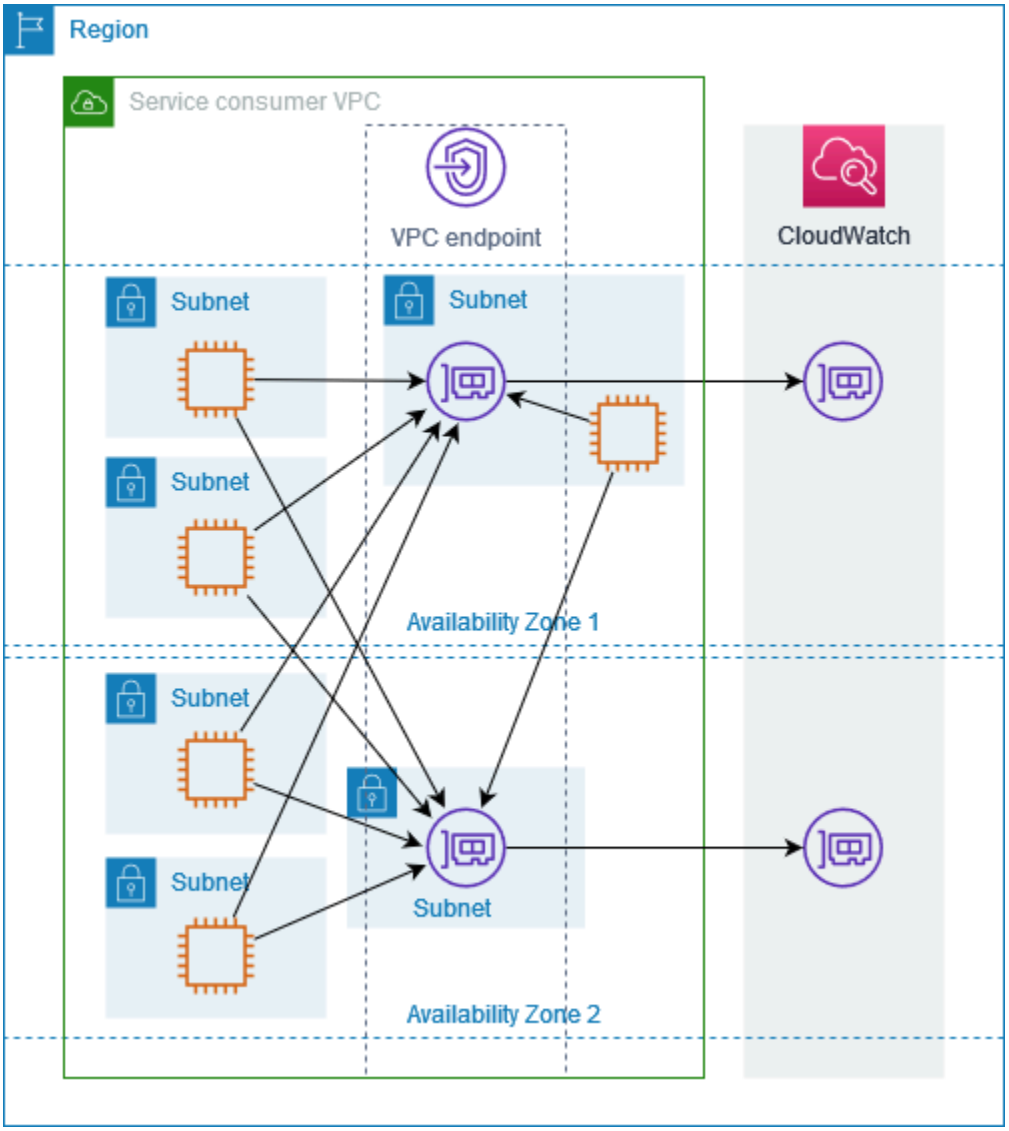
Em um ambiente de produção, para alta disponibilidade e resiliência, recomendamos o seguinte:

- 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.

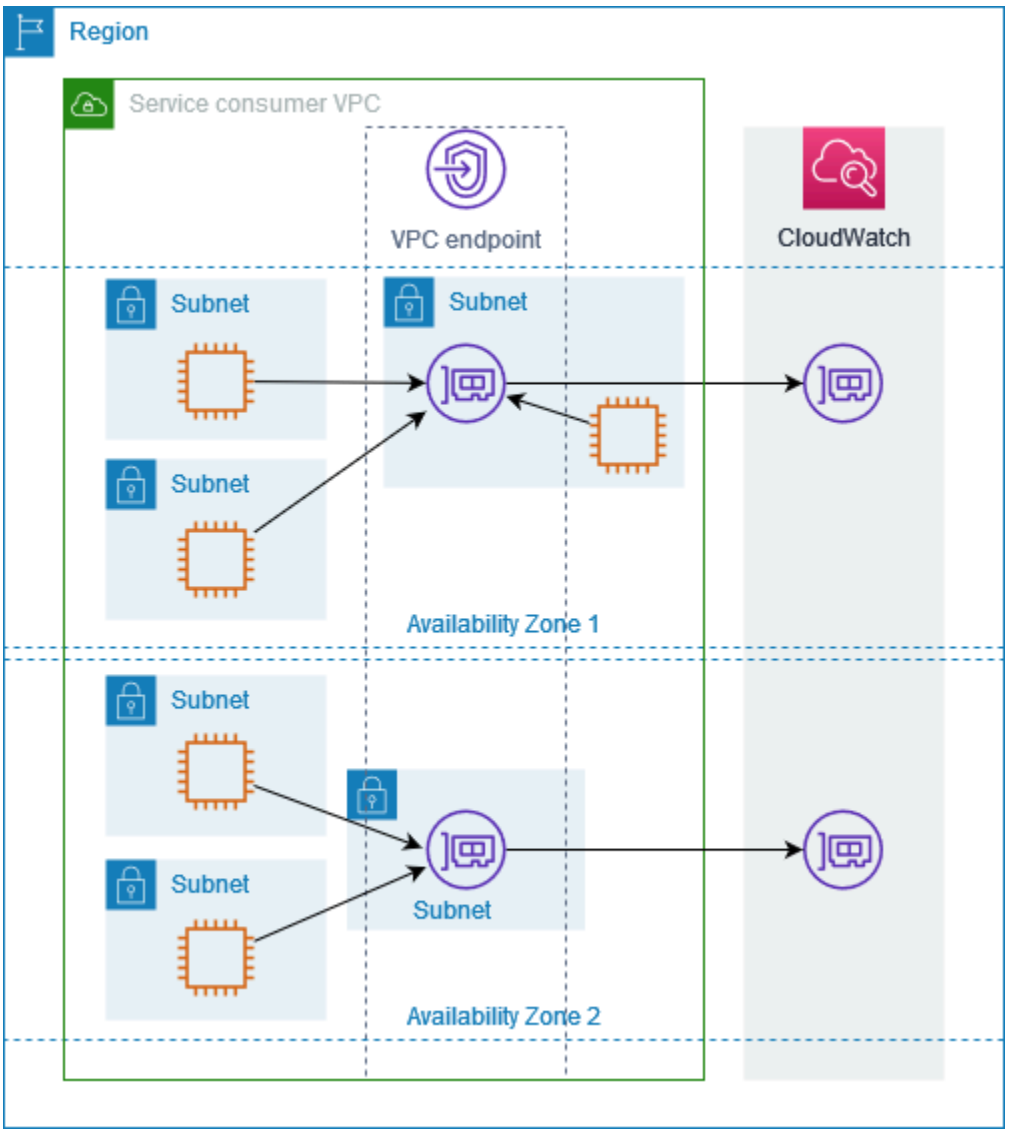
O diagrama a seguir mostra um VPC endpoint para a Amazon CloudWatch com uma interface de rede de endpoint em uma única zona de disponibilidade. Quando qualquer recurso em qualquer sub-rede na VPC acessa a CloudWatch Amazon usando seu endpoint público, resolvemos o tráfego para o endereço IP da interface 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 ter 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.

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 a interface VPC endpoint ou indica que o serviço gerencia o endpoint.

AWS service (Serviço da AWS)	Nome do serviço
Analisador de acesso	com.amazonaws.*region*.access-analyzer
AWS Account Management	com.amazonaws.*region*.account
Amazon API Gateway	com.amazonaws.*region*.execute-api
AWS AppConfig	com.amazonaws.*region*.appconfig
	com.amazonaws.*region*.appconfigdata
AWS App Mesh	com.amazonaws.*region*.appmesh

AWS service (Serviço da AWS)	Nome do serviço
	com.amazonaws.*region*.appmesh-envoy-management
AWS Executor de aplicativos	com.amazonaws.*region*.apprunner
Serviços do AWS App Runner	com.amazonaws.*region*.apprunner.requests
Application Auto Scaling	com.amazonaws.*region*.application-autoscaling
AWS Serviço de migração de aplicativos	com.amazonaws.*region*.mgn
Amazon AppStream 2.0	com.amazonaws.*region*.appstream.api
	com.amazonaws.*region*.appstream.streaming
AWS AppSync	com.amazonaws.*region*.appsync-api
Amazon Athena	com.amazonaws.*region*.athena
AWS Audit Manager	com.amazonaws.*region*.auditmanager
Amazon Aurora	com.amazonaws.*region*.rds
AWS Auto Scaling	com.amazonaws.*region*.autoscaling-plans
AWS B2B Data Interchange	com.amazonaws.*region*.b2bi
AWS Backup	com.amazonaws.*region*.backup
	com.amazonaws.*region*.backup-gateway
AWS Batch	com.amazonaws.*region*.batch
Amazon Bedrock	com.amazonaws.*região*.bedrock
	com.amazonaws. *região* .*bedrock-agent*
	com.amazonaws.*region*.bedrock-agent-runtime
	com.amazonaws.*região*.bedrock-runtime

AWS service (Serviço da AWS)	Nome do serviço
AWS Billing Conductor	com.amazonaws.*region*.billingconductor
Amazon Braket	com.amazonaws.*region*.braket
AWS Clean Rooms	com.amazonaws.*region*.cleanrooms
AWS Salas limpas ML	com.amazonaws. *região .cleanrooms-ml*
AWS Cloud Control API	com.amazonaws.*região*.cloudcontrolapi
	com.amazonaws.*região*.cloudcontrolapi-fips
Amazon Cloud Directory	com.amazonaws.*region*.clouddirectory
AWS CloudFormation	com.amazonaws.*region*.cloudformation
AWS CloudHSM	com.amazonaws.*region*.cloudhsmv2
AWS Cloud Map	com.amazonaws.*região*.servicediscovery
	com.amazonaws.*região*.servicediscovery-fips
	com.amazonaws.*região*.data-servicediscovery
	com.amazonaws.*região*.data-servicediscovery-fips
AWS CloudTrail	com.amazonaws.*region*.cloudtrail
Amazon CloudWatch	com.amazonaws.*region*.evidently
	com.amazonaws.*region*.evidently-dataplane
	com.amazonaws.*region*.monitoring
	com.amazonaws.*region*.rum
	com.amazonaws.*region*.rum-dataplane
	com.amazonaws.*region*.synthetics

AWS service (Serviço da AWS)	Nome do serviço
CloudWatch Registros da Amazon	com.amazonaws.*region*.logs
Monitor CloudWatch de rede Amazon	com.amazonaws. *região.networkmonitor*
AWS CodeArtifact	com.amazonaws.*region*.codeartifact.api
	com.amazonaws.*region*.codeartifact.repositories
AWS CodeBuild	com.amazonaws.*region*.codebuild
	com.amazonaws.*region*.codebuild-fips
AWS CodeCommit	com.amazonaws.*region*.codecommit
	com.amazonaws.*region*.codecommit-fips
	com.amazonaws.*region*.git-codecommit
	com.amazonaws.*region*.git-codecommit-fips
Conexões de código da AWS	com.amazonaws. *região .codeconnections.api*
	com.amazonaws.*region*.codestar-connections.api
AWS CodeDeploy	com.amazonaws.*region*.codedeploy
	com.amazonaws.*region*.codedeploy-commands-secure
Amazon CodeGuru Profiler	com.amazonaws.*region*.codeguru-profiler
CodeGuru Revisor da Amazon	com.amazonaws.*region*.codeguru-reviewer
AWS CodePipeline	com.amazonaws.*region*.codepipeline
Amazon CodeWhisperer	com.amazonaws.*region*.codewhisperer
Amazon Comprehend	com.amazonaws.*region*.comprehend
Amazon Comprehend Medical	com.amazonaws.*region*.comprehendmedical

AWS service (Serviço da AWS)	Nome do serviço
AWS Config	com.amazonaws.*region*.config
Amazon Connect	com.amazonaws.*region*.app-integrations
	com.amazonaws.*region*.cases
	com.amazonaws.*region*.connect-campaigns
	com.amazonaws.*region*.profile
	com.amazonaws.*region*.voiceid
	com.amazonaws.*region*.wisdom
AWS Connector Service	com.amazonaws.*region*.awsconnector
Catálogo de controle da AWS	com.amazonaws. *região. catálogo* de controle
AWS Data Exchange	com.amazonaws.*region*.dataexchange
Amazon Data Firehose	com.amazonaws.*region*.kinesis-firehose
AWS Database Migration Service	com.amazonaws.*region*.dms
	com.amazonaws.*region*.dms-fips
AWS DataSync	com.amazonaws.*region*.datasync
Amazon DataZone	com.amazonaws.*região*.datazone
AWS Deadline Cloud	com.amazonaws. *região .deadline.management*
	com.amazonaws. *região .deadline.scheduling*
DevOpsGuru da Amazon	com.amazonaws.*region*.devops-guru
AWS Directory Service	com.amazonaws.*region*.ds
Amazon DynamoDB	com.amazonaws. *região .dynamodb*

AWS service (Serviço da AWS)	Nome do serviço
APIs diretas do Amazon EBS	com.amazonaws.*region*.ebs
Amazon EC2	com.amazonaws.*region*.ec2
Amazon EC2 Auto Scaling	com.amazonaws.*region*.autoscaling
EC2 Image Builder	com.amazonaws.*region*.imagebuilder
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-telemetry
Amazon EKS	com.amazonaws.*region*.eks
	com.amazonaws.*region*.eks-auth
AWS Elastic Beanstalk	com.amazonaws.*region*.elasticbeanstalk
	com.amazonaws.*region*.elasticbeanstalk-health
AWS Elastic Disaster Recovery	com.amazonaws.*region*.drs
Amazon Elastic File System	com.amazonaws.*region*.elasticfilesystem
	com.amazonaws.*region*.elasticfilesystem-fips
Amazon Elastic Inference	com.amazonaws.*region*.elastic-inference.runtime
Elastic Load Balancing	com.amazonaws.*region*.elasticloadbalancing
Amazon ElastiCache	com.amazonaws.*region*.elasticache
	com.amazonaws.*região*.elasticache-fips

AWS service (Serviço da AWS)	Nome do serviço
AWS Elemental MediaConnect	com.amazonaws.*region*.mediaconnect
Amazon EMR	com.amazonaws.*region*.elasticmapreduce
Amazon EMR no EKS	com.amazonaws.*region*.emr-containers
Amazon EMR Serverless	com.amazonaws.*region*.emr-serverless
Amazon EMR WAL	com.amazonaws. *região .emrwal.prod*
AWS Entity Resolution	com.amazonaws.*região*.entityresolution
Amazon EventBridge	com.amazonaws.*region*.events
	com.amazonaws. *região .pipes-data*
AWS Fault Injection Service	com.amazonaws.*region*.fis
Amazon FinSpace	com.amazonaws.*region*.finspace
	com.amazonaws.*region*.finspace-api
Amazon Forecast	com.amazonaws.*region*.forecast
	com.amazonaws.*region*.forecastquery
	com.amazonaws.*region*.forecast-fips
	com.amazonaws.*region*.forecastquery-fips
Amazon Fraud Detector	com.amazonaws.*region*.frauddetector
Amazon FSx	com.amazonaws.*region*.fsx
	com.amazonaws.*region*.fsx-fips
AWS Glue	com.amazonaws.*region*.glue
AWS Glue DataBrew	com.amazonaws.*region*.databrew

AWS service (Serviço da AWS)	Nome do serviço
Amazon Managed Grafana	com.amazonaws.*region*.grafana
	com.amazonaws.*region*.grafana-workspace
AWS Ground Station	com.amazonaws.*region*.groundstation
Amazon GuardDuty	com.amazonaws.*region*.guardduty-data
	com.amazonaws.*region*.guardduty-data-fips
AWS HealthImaging	com.amazonaws. *região .dicom-medical-imaging*
	com.amazonaws.*region*.medical-imaging
	com.amazonaws.*region*.runtime-medical-imaging
AWS HealthLake	com.amazonaws.*region*.healthlake
AWS HealthOmics	com.amazonaws.*region*.analytics-omics
	com.amazonaws.*region*.control-storage-omics
	com.amazonaws.*region*.storage-omics
	com.amazonaws.*region*.tags-omics
	com.amazonaws.*region*.workflows-omics
IAM Identity Center	com.amazonaws.*region*.identitystore
IAM Roles Anywhere	com.amazonaws.*region*.rolesanywhere
Amazon Inspector	com.amazonaws.*region*.inspector2
AWS IoT Core	com.amazonaws.*region*.iot.data
	com.amazonaws.*region*.iot.credentials
	com.amazonaws.*region*.iot.fleethub.api

AWS service (Serviço da AWS)	Nome do serviço
AWS IoT Core Device Advisor	com.amazonaws.*region*.deviceadvisor.iot
AWS IoT Core for LoRaWAN	com.amazonaws.*region*.iotwireless.api
	com.amazonaws.*region*.lorawan.cups
	com.amazonaws.*region*.lorawan.lns
AWS IoT FleetWise	com.amazonaws.*region*.iotfleetwise
AWS IoT Greengrass	com.amazonaws.*region*.greengrass
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 Key Management Service	com.amazonaws.*region*.kms
	com.amazonaws.*region*.kms-fips
Amazon Keyspaces (for Apache Cassandra)	com.amazonaws.*region*.cassandra
	com.amazonaws.*region*.cassandra-fips
Amazon Kinesis Data Streams	com.amazonaws.*region*.kinesis-streams
AWS Lake Formation	com.amazonaws.*region*.lakeformation
AWS Lambda	com.amazonaws.*region*.lambda

AWS service (Serviço da AWS)	Nome do serviço
Amazon Lex	com.amazonaws.*region*.models-v2-lex
	com.amazonaws.*region*.runtime-v2-lex
AWS License Manager	com.amazonaws.*region*.license-manager
	com.amazonaws.*region*.license-manager-fips
	com.amazonaws.*region*.license-manager-user-subscriptions
Amazon Lookout for Equipment	com.amazonaws.*region*.lookoutequipment
Amazon Lookout for Metrics	com.amazonaws.*region*.lookoutmetrics
Amazon Lookout for Vision	com.amazonaws.*region*.lookoutvision
Amazon Macie	com.amazonaws.*region*.macie2
AWS Mainframe Modernization	com.amazonaws.*região*.m2
Amazon Managed Blockchain	com.amazonaws.*region*.managedblockchain-query
	com.amazonaws.*region*.managedblockchain.bitcoin.mainnet
	com.amazonaws.*region*.managedblockchain.bitcoin.testnet
Amazon Managed Service for Prometheus	com.amazonaws.*region*.aps
	com.amazonaws.*region*.aps-workspaces
Amazon Managed Workflows for Apache Airflow	com.amazonaws.*region*.airflow.api
	com.amazonaws.*region*.airflow.env
	com.amazonaws.*region*.airflow.ops

AWS service (Serviço da AWS)	Nome do serviço
AWS Management Console	com.amazonaws.*region*.console
	com.amazonaws.*region*.signin
Amazon MemoryDB para Redis	com.amazonaws.*region*.memory-db
	com.amazonaws.*region*.memorydb-fips
Orquestrador do AWS Migration Hub	com.amazonaws.*region*.migrationhub-orchestrator
AWS Migration Hub Refactor Spaces	com.amazonaws.*region*.refactor-spaces
Migration Hub Strategy Recommendations	com.amazonaws.*region*.migrationhub-strategy
Análise do Amazon Neptune	com.amazonaws.*region*.neptune-graph
Amazon Nimble Studio	com.amazonaws.*region*.nimble
OpenSearch Serviço Amazon	Esses endpoints são gerenciados por serviços
AWS Organizations	com.amazonaws. *região* .organizações
	com.amazonaws. *região .organizations-fips*
AWS Outposts	com.amazonaws. *região. Postos* avançados
AWS Panorama	com.amazonaws.*region*.panorama
AWS Criptografia de pagamento	com.amazonaws.*region*.payment-cryptography.controlplane
	com.amazonaws.*region*.payment-cryptography.dataplane
Amazon Personalize	com.amazonaws.*region*.personalize
	com.amazonaws.*region*.personalize-events

AWS service (Serviço da AWS)	Nome do serviço
	com.amazonaws.*region*.personalize-runtime
Cadeia de Suprimentos AWS	com.amazonaws. *região .scn*
Amazon Pinpoint	com.amazonaws.*region*.pinpoint
	com.amazonaws.*region*.pinpoint-sms-voice-v2
Amazon Polly	com.amazonaws.*region*.polly
AWS 5G privado	com.amazonaws.*region*.private-networks
AWS Private Certificate Authority	com.amazonaws.*region*.acm-pca
	com.amazonaws.*region*.pca-connector-ad
AWS Proton	com.amazonaws.*region*.proton
Amazon Q Business	aws.api. *região.qbusiness*
Amazon QLDB	com.amazonaws.*region*.qldb.session
Amazon QuickSight	com.amazonaws. *site da região.quicksight*
Amazon RDS	com.amazonaws.*region*.rds
API Data do Amazon RDS	com.amazonaws.*region*.rds-data
AWS re:Post Privado	com.amazonaws. *região.repostspace*
Amazon Redshift	com.amazonaws.*region*.redshift
	com.amazonaws.*region*.redshift-fips
API de dados do Amazon Redshift	com.amazonaws.*region*.redshift-data
	com.amazonaws. *região .redshift-data-fips*
Amazon Rekognition	com.amazonaws.*region*.rekognition

AWS service (Serviço da AWS)	Nome do serviço
	com.amazonaws.*region*.rekognition-fips
	com.amazonaws.*region*.streaming-rekognition
	com.amazonaws.*region*.streaming-rekognition-fips
AWS RoboMaker	com.amazonaws.*region*.robomaker
Amazon S3	com.amazonaws.*region*.s3
Pontos de acesso de várias regiões do Amazon S3	com.amazonaws.s3-global.accesspoint
Amazon S3 on Outposts	com.amazonaws.*region*.s3-outposts
Amazon SageMaker	aws.sagemaker.*region*.notebook
	aws.sagemaker.*region*.studio
	com.amazonaws.*region*.sagemaker.api
	com.amazonaws.*region*.sagemaker.featurestore-runtime
	com.amazonaws.*region*.sagemaker.metrics
	com.amazonaws.*region*.sagemaker.runtime
	com.amazonaws.*region*.sagemaker.runtime-fips
AWS Secrets Manager	com.amazonaws.*region*.secretsmanager
AWS Security Hub	com.amazonaws.*region*.securityhub
AWS Security Token Service	com.amazonaws.*region*.sts
Service Catalog	com.amazonaws.*region*.servicecatalog
	com.amazonaws.*region*.servicecatalog-appregistry

AWS service (Serviço da AWS)	Nome do serviço
Amazon SES	com.amazonaws.*region*.email-smtp
AWS SimSpace Weaver	com.amazonaws.*region*.simspaceweaver
AWS Snow Device Management	com.amazonaws.*region*.snow-device-management
Amazon SNS	com.amazonaws.*region*.sns
Amazon SQS	com.amazonaws.*region*.sqs
Amazon SWF	com.amazonaws.*region*.swf
	com.amazonaws.*region*.swf-fips
AWS Step Functions	com.amazonaws.*region*.states
	com.amazonaws.*region*.sync-states
AWS Storage Gateway	com.amazonaws.*region*.storagegateway
AWS Systems Manager	com.amazonaws.*region*.ec2messages
	com.amazonaws.*region*.ssm
	com.amazonaws.*region*.ssm-contacts
	com.amazonaws.*region*.ssm-incidents
	com.amazonaws.*region*.ssmmessages
AWS Construtor de rede Telco	com.amazonaws.*region*.tnb
Amazon Textract	com.amazonaws.*region*.textract
	com.amazonaws.*region*.textract-fips
Amazon Timestream	com.amazonaws.*região*.timestream.ingest-*célula*
	com.amazonaws.*região*.timestream.query-*célula*

AWS service (Serviço da AWS)	Nome do serviço
Amazon Timestream para InfluxDB	com.amazonaws. *região .timestream-influxdb*
Amazon Transcribe	com.amazonaws.*region*.transcribe
	com.amazonaws.*region*.transcribestreaming
Amazon Transcribe Medical	com.amazonaws.*region*.transcribe
	com.amazonaws.*region*.transcribestreaming
AWS Transfer for SFTP	com.amazonaws.*region*.transfer
	com.amazonaws.*region*.transfer.server
Amazon Translate	com.amazonaws.*region*.translate
AWS Trusted Advisor	com.amazonaws.*region*.trustedadvisor
Amazon Verified Permissions	com.amazonaws.*region*.verifiedpermissions
Amazon VPC Lattice	com.amazonaws.*region*.vpc-lattice
Amazon WorkSpaces	com.amazonaws.*region*.workspaces
Amazon WorkSpaces Thin Client	com.amazonaws. *região .thinclient.api*
AWS X-Ray	com.amazonaws.*region*.xray

Visualizar nomes de AWS service (Serviço da AWS) disponíveis

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
```

A seguir está um exemplo de saída:

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.sagemaker.us-east-1.notebook",
    "aws.sagemaker.us-east-1.studio",
    "com.amazonaws.s3-global.accesspoint",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.account",
    ...
]
```

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"
                }
            ],
            "VpcEndpointPolicySupported": true,
            "AcceptanceRequired": false,
            "ManagesVpcEndpoints": false,
            "Tags": [],
            "PrivateDnsNameVerificationState": "verified",
            "SupportedIpAddressTypes": [
                "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.

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.sagemaker.us-east-1.notebook",
    "aws.sagemaker.us-east-1.studio",
    "com.amazonaws.s3-global.accesspoint",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.account",
    ...
]
```

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.

```
[
    "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.cleanrooms",
    "com.amazonaws.us-east-1.cleanrooms-ml",
    "com.amazonaws.us-east-1.cloudtrail",
    "com.amazonaws.us-east-1.codeguru-profiler",
    "com.amazonaws.us-east-1.codeguru-reviewer",
    "com.amazonaws.us-east-1.codepipeline",
    "com.amazonaws.us-east-1.codewhisperer",
    "com.amazonaws.us-east-1.datasync",
    "com.amazonaws.us-east-1.datazone",
    "com.amazonaws.us-east-1.deadline.management",
    "com.amazonaws.us-east-1.deadline.scheduling",
    "com.amazonaws.us-east-1.deviceadvisor.iot",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.elastic-inference.runtime",
    "com.amazonaws.us-east-1.email-smtp",
    "com.amazonaws.us-east-1.grafana-workspace",
    "com.amazonaws.us-east-1.iot.credentials",
    "com.amazonaws.us-east-1.iot.data",
    "com.amazonaws.us-east-1.iotwireless.api",
    "com.amazonaws.us-east-1.lorawan.cups",
    "com.amazonaws.us-east-1.lorawan.lns",
    "com.amazonaws.us-east-1.macie2",
    "com.amazonaws.us-east-1.neptune-graph",
    "com.amazonaws.us-east-1.nimble",
    "com.amazonaws.us-east-1.organizations",
    "com.amazonaws.us-east-1.outposts",
    "com.amazonaws.us-east-1.pipes-data",
    "com.amazonaws.us-east-1.redshift-data",
    "com.amazonaws.us-east-1.redshift-data-fips",
    "com.amazonaws.us-east-1.refactor-spaces",
    "com.amazonaws.us-east-1.sagemaker.runtime-fips",
    "com.amazonaws.us-east-1.storagegateway",
    "com.amazonaws.us-east-1.transfer",
```

```
    "com.amazonaws.us-east-1.transfer.server",
    "com.amazonaws.us-east-1.verifiedpermissions"
]
```

Visualizar suporte a IPv6

Você 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
```

A seguir está um exemplo de saída:

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.api.us-east-1.qbusiness",
    "com.amazonaws.us-east-1.athena",
    "com.amazonaws.us-east-1.data-servicediscovery",
    "com.amazonaws.us-east-1.data-servicediscovery-fips",
    "com.amazonaws.us-east-1.eks-auth",
    "com.amazonaws.us-east-1.glue",
    "com.amazonaws.us-east-1.lakeformation",
    "com.amazonaws.us-east-1.quicksight-website",
    "com.amazonaws.us-east-1.s3-outposts",
    "com.amazonaws.us-east-1.servicediscovery",
    "com.amazonaws.us-east-1.servicediscovery-fips",
    "com.amazonaws.us-east-1.timestream-influxdb"
]
```

Acesse e AWS service (Serviço da AWS) use 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 Acesso 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 ter 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 seus recursos estiverem em uma sub-rede com uma ACL de rede, verifique se a ACL de rede permite tráfego entre os recursos em sua VPC e as interfaces de rede do endpoint.
- Há cotas em seus AWS PrivateLink recursos. Para ter 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 Service category (Categoria de serviço), escolha Serviços da AWS.
5. Em Service name (Nome do serviço), selecione o serviço. Para ter mais informações, consulte the section called “Serviços que se integram”.
6. Em VPC, selecione a VPC de onde você acessará o AWS service (Serviço da AWS).
7. 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.
8. Em Subnets (Sub-redes), selecione uma sub-rede por zona de disponibilidade pela qual você acessará o AWS service (Serviço da AWS). Não é possível selecionar várias sub-redes em uma mesma zona de disponibilidade. Para ter mais informações, consulte the section called “Zonas de disponibilidade e sub-redes”.

   Criamos uma interface de rede do endpoint em cada sub-rede que você especificar. 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. Observe que os primeiros quatro 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 suas 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 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.
   - 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 ambos os endereços IPv4 e IPv6 e o serviço aceitar solicitações de ambos IPv4 e IPv6.

10. Em Grupos de segurança, selecione os grupos de segurança para associar às interfaces de rede do endpoint para o endpoint da VPC. Por padrão, associamos o grupo de segurança padrão para a VPC.
11. 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. Essa opção ficará disponível somente se o serviço for compatível com as políticas de endpoint da VPC. Para ter mais informações, consulte Políticas de endpoint.
12. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
13. 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. No entanto, você pode usar os endpoints da VPC em sub-redes que são compartilhadas com você.

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 ter 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 ter 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. Selecione Save (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 VPC endpoints 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 ter 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. 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 e o valor da etiqueta.
6. Para remover uma etiqueta, escolha Remove (Remover) à direita da chave e do valor da etiqueta.
7. Selecione Save (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 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 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.

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

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.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:region:account-id:key/key-id",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:region:account-id:vpc-endpoint/endpoint-id"
        },
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

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 endpoints de interface. Para uma comparação das opções, consulte o seguinte:

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

Definição de preço

Não há cobrança adicional pelo uso de endpoints do gateway.

Conteúdo

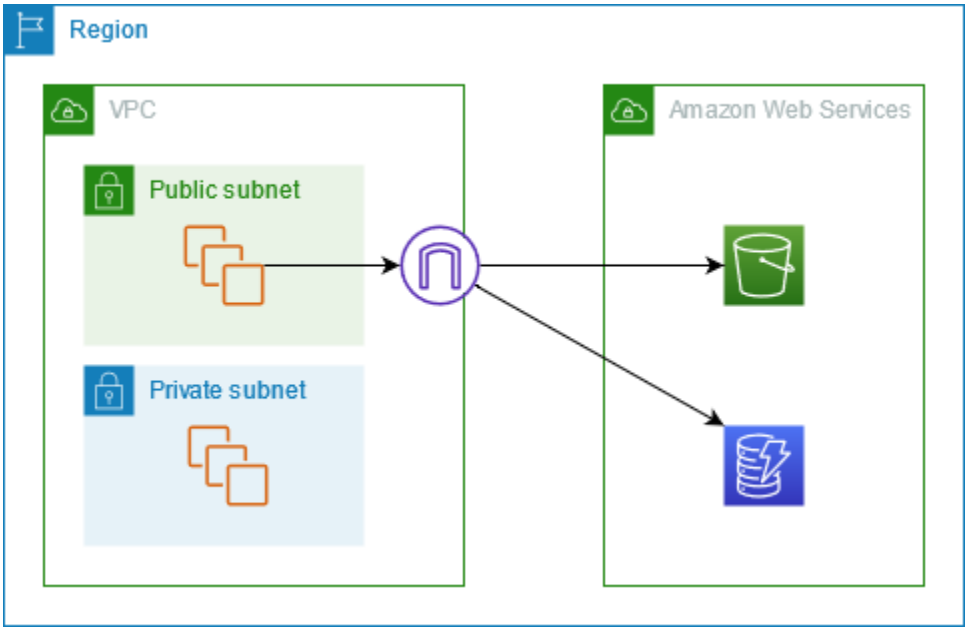
Visão geral

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

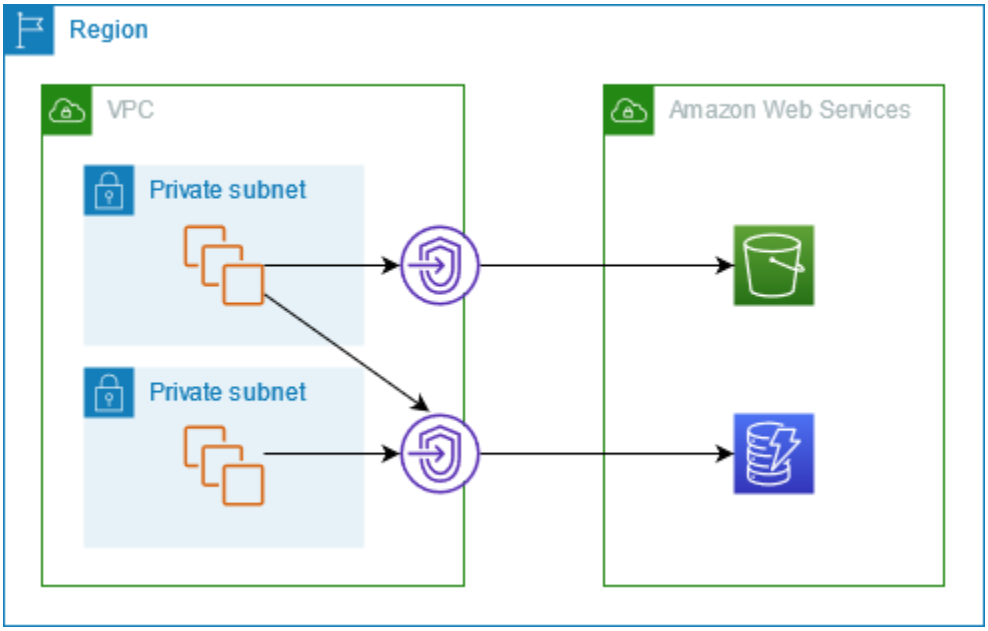
O seguinte diagrama mostra como as instâncias acessam o Amazon S3 e o DynamoDB pelos endpoints de serviço públicos. O tráfego para o Amazon S3 ou o DynamoDB de uma instância em uma sub-rede pública é encaminhado ao gateway da Internet da VPC e depois ao serviço. As

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)	Destino
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 da Internet, a rota de endpoint prevalecerá sobre 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

Destino	Protocolo	Intervalo de portas
service_cidr_block_2	TCP	443
service_cidr_block_3	TCP	443

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

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 endpoints de gateway são compatíveis somente com tráfego IPv4.
- Os endereços IPv4 de origem de instâncias nas sub-redes afetadas, tal como recebidos pelo Amazon S3, mudam de endereços IPv4 públicos para endereços IPv4 privados na 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 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 AWS 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.

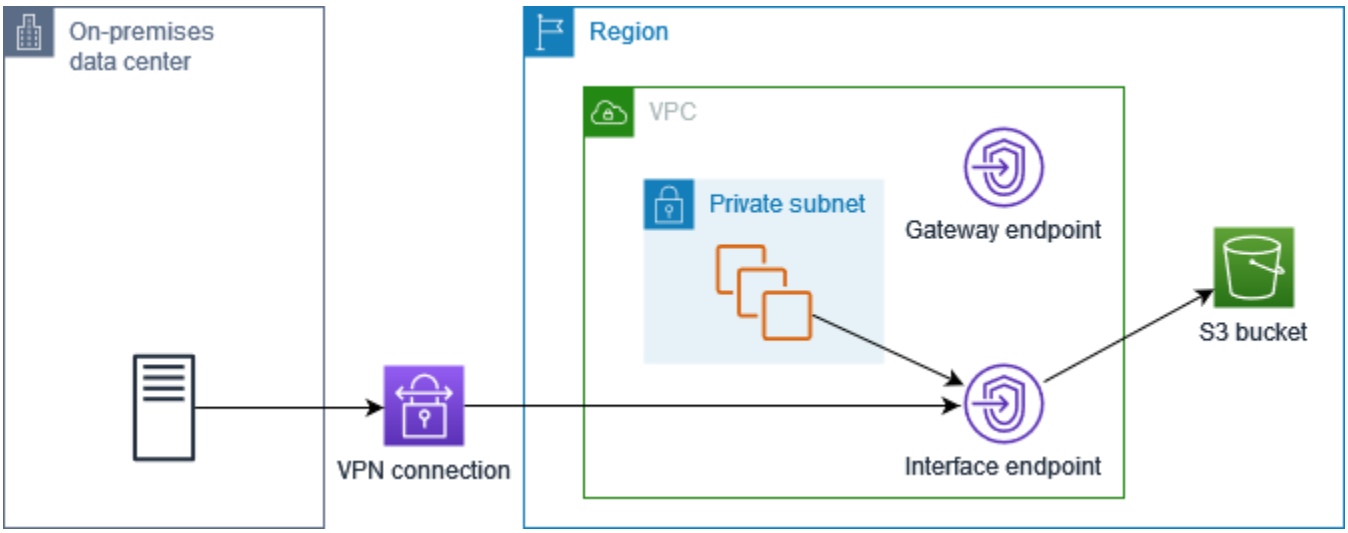
Route 53 Resolver

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.

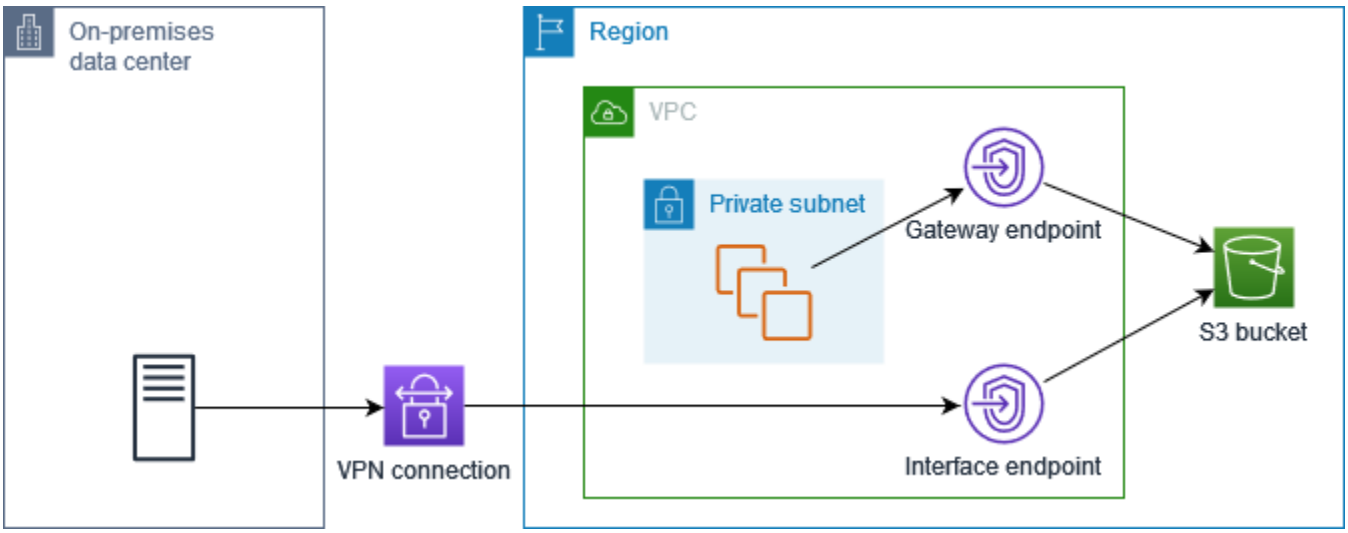
DNS privado

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.



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 Type = Gateway e selecione com.amazonaws. *região* .3.
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 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 AWS Management Console.

```
{
  "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 AWS Management Console.

```
{
  "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 condição aws: VpcSource Ip. 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 AWS Management Console.

```
{
  "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 um determinado 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.

```
{
  "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. A política padrão permite acesso total. Para ter 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. Selecione Save (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.

```
{
  "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.

```
{
  "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.

```
{
  "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 é compatível com endpoints de gateway e endpoints de interface. Com um endpoint de gateway, você pode acessar o DynamoDB de sua VPC, sem precisar de um gateway de internet ou dispositivo NAT para sua VPC e sem custo adicional. 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 VPC endpoints para o DynamoDB no Amazon DynamoDB Developer Guide.

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 AWS 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. *região* .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.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-specific-endpoint",
         "Effect": "Deny",
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:region:account-id: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.

```
{
   "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.

```
{
   "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. A política padrão permite acesso total. Para ter 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. Selecione Save (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.

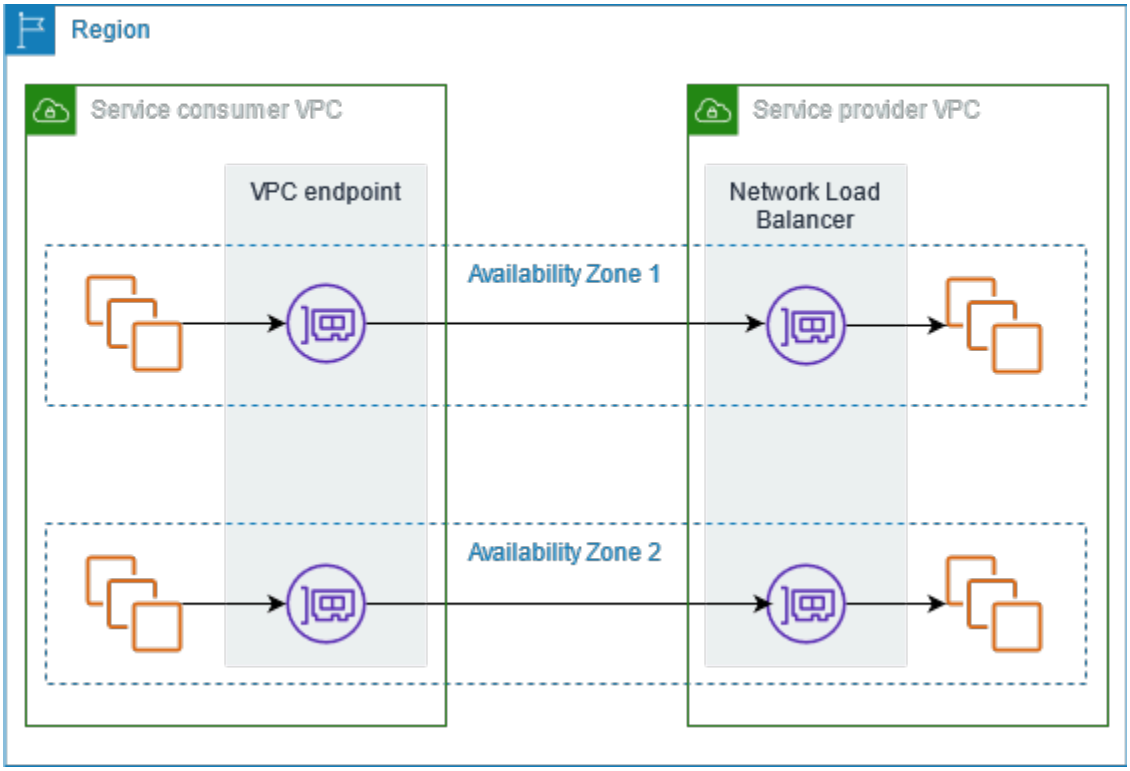
Conteúdo

Visão geral

Você pode descobrir, comprar e provisionar produtos SaaS baseados em. AWS PrivateLink AWS Marketplace Para obter mais informações, consulte AWS Marketplace: - 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 Categoria do serviço, escolha Serviços do AWS Marketplace .
    b. Insira o nome do serviço.
5. Se você se inscreveu em um serviço com a designação AWS Service Ready, faça o seguinte:

   a. Para a categoria Serviço, escolha PrivateLink Ready Partner Services.
   b. Insira o nome do serviço e escolha Verify service (Verificar serviço).
6. Em VPC, selecione a VPC de onde você acessará o produto.
7. Em Subnets (Sub-redes), selecione uma sub-rede por zona de disponibilidade pela qual você acessará o produto.
8. Para Security group (Grupo 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.

Definição de preço

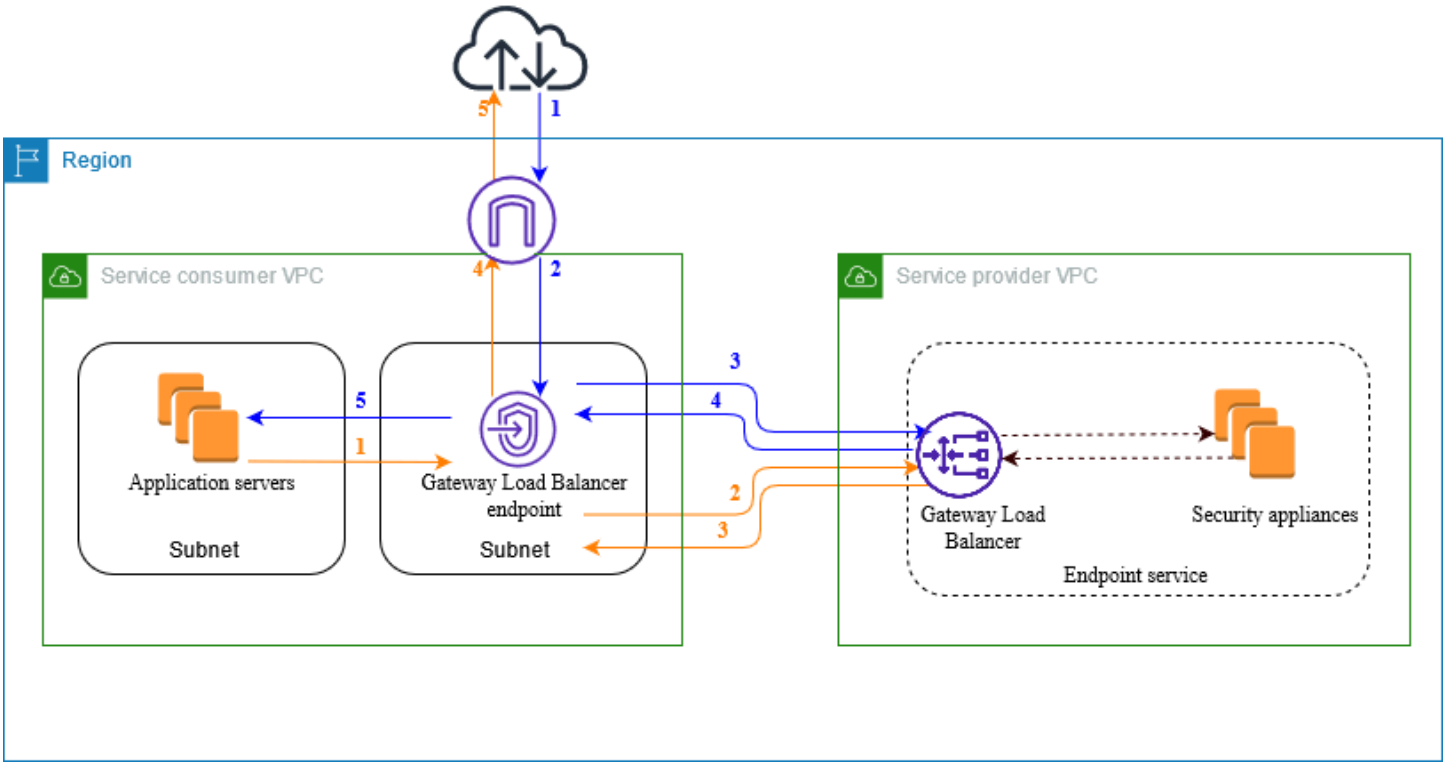
Você é cobrado por cada hora em que seu endpoint do Gateway Load Balancer é provisionado em cada zona de disponibilidade. Você também é cobrado por GB de dados processados. Para obter mais informações, consulte Preços do AWS PrivateLink.

Conteúdo

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

Visão geral

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. Observe que as rotas IPv6 estão incluídas em uma configuração dualstack.

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
CIDR IPv4 da VPC	Local
CIDR IPv6 da VPC	Local
CIDR IPv4 da sub-rede do aplicativo	*vpc-endpoint-id*
CIDR IPv6 da sub-rede do aplicativo	*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
CIDR IPv4 da VPC	Local
CIDR IPv6 da VPC	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
CIDR IPv4 da VPC	Local
CIDR IPv6 da VPC	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 ter 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. Selecione Create (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 ter 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 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 do Gateway Load Balancer. Para ter 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.
- Há cotas em seus AWS PrivateLink recursos. Para ter 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 Service category (Categoria de serviço), escolha Other endpoint services (Outros serviços de endpoint).
5. Em Service name (Nome do serviço), insira o nome do serviço e escolha Verify service (Verificar serviço).
6. Em VPC, selecione a VPC na qual deseja criar o endpoint.
7. Para Subnets (Sub-redes), selecione a sub-rede na qual o endpoint será criado.
8. 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.
   - 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.
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 ter 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. 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 e o valor da etiqueta.
6. Para remover uma etiqueta, escolha Remove (Remover) à direita da chave e do valor da etiqueta.
7. Selecione Save (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 do 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)

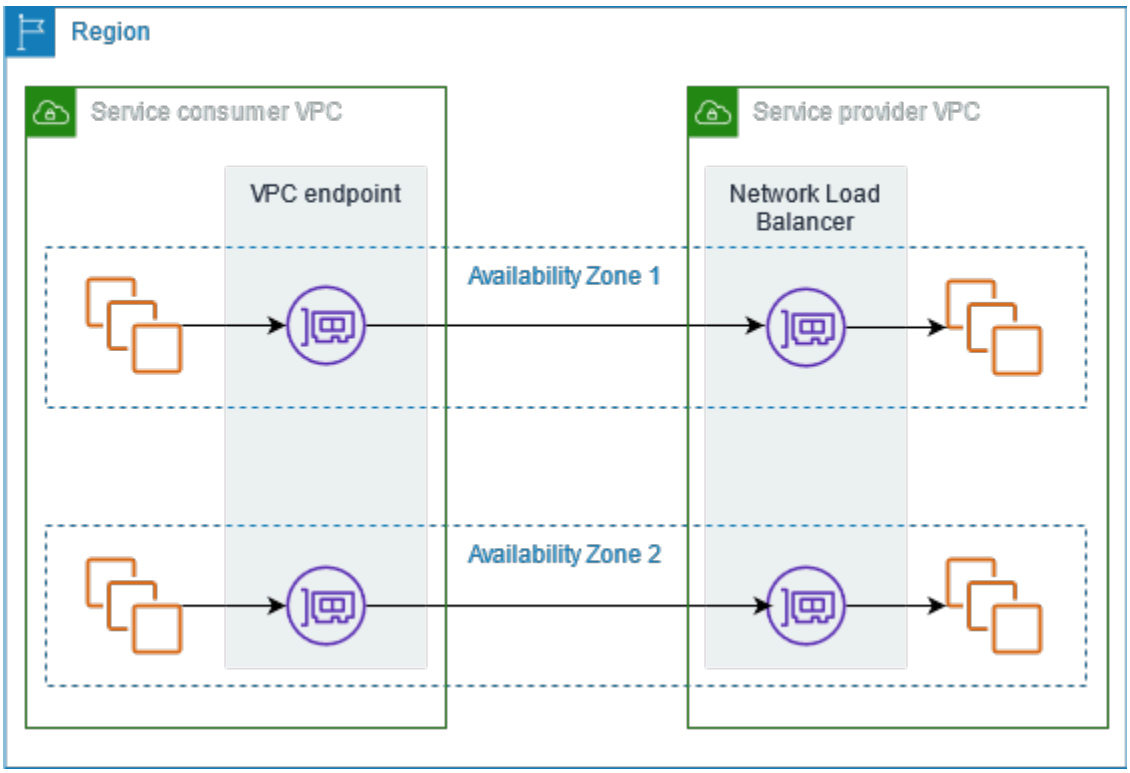
Compartilhe seus serviços por meio de AWS PrivateLink

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

Conteúdo

Visão geral

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.region.vpce.amazonaws.com
```

Os nomes zonais apresentam a seguinte sintaxe:

```
endpoint_id-zone.endpoint_service_id.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 ter mais informações, consulte Gerenciar nomes DNS.

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 back-end 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. É possível acessar o serviço de endpoint de outras regiões usando o emparelhamento da VPC.
- Um serviço de endpoint oferece suporte somente sobre TCP.
- 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.
- 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 ter 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 tráfego de passagem AWS PrivateLink. Para obter mais informações, consulte Grupos de segurança no Guia do usuário para balanceadores de carga de rede.
- 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 carga entre zonas 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. As zonas de disponibilidade incluídas listam as zonas de disponibilidade que estão habilitadas para os balanceadores de carga de rede selecionados. Seu serviço de endpoint estará disponível nessas zonas de disponibilidade.
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. Senão, essas solicitações serão aceitas automaticamente.
7. 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 ter mais informações, consulte Gerenciar nomes DNS.
8. 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.
9. (Opcional) Para adicionar uma tag, escolha Add new tag (Adicionar nova tag) e insira a chave e o valor da tag.
10. Selecione Create (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 ter 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 seguinte procedimento.
- Aceite a solicitação de conexão do endpoint do consumidor do serviço. Para ter 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 Service category (Categoria de serviço), escolha Other endpoint services (Outros serviços de endpoint).
5. Em Service name (Nome do serviço), insira o nome do serviço (por exemplo, `com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`) e escolha Verify service (Verificar serviço).
6. Para VPC, selecione a VPC na qual deseja criar o endpoint.
7. Em Subnets (Sub-redes), selecione as sub-redes (zonas de disponibilidade) pela qual você acessará o serviço de endpoint.
8. 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.
- 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 ambos os endereços IPv4 e IPv6 e o serviço de endpoint aceitar solicitações de ambos IPv4 e IPv6.

9. 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.

10. Para Security group (Grupo de segurança), selecione os grupos de segurança para associar às interfaces de rede do endpoint.
11. 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
- Gerenciar balanceadores de carga
- Associar um nome DNS privado
- 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::*account_id*:root

Função

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

Usuário

arn:aws:iam::*account_id*:user/*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 principals).
4. Para adicionar permissões, escolha Allow principals (Permitir entidades principals). 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 principals).
5. Para remover permissões, selecione a entidade principal e escolha Actions (Ações), Delete (Excluir). Quando a confirmação for solicitada, insira **`delete`** e escolha 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.

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

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 rejeitar uma solicitação que já foi aceita, isso não afetará a conexão entre o endpoint e o serviço.

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)

Gerenciar balanceadores de carga

Você pode gerenciar os balanceadores de carga associados ao seu 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 um Network Load Balancer, também poderá habilitar a zona de disponibilidade para seu serviço de endpoint. Depois de habilitar uma zona de disponibilidade para o serviço de endpoint, os consumidores do serviço podem adicionar uma sub-rede dessa zona de disponibilidade aos seus endpoints VPC de interface.

Para gerenciar os balanceadores de carga do seu 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. Altere a configuração do serviço do endpoint conforme necessário. Por exemplo: .
    - Marque a caixa de seleção de um balanceador de carga para associá-lo ao serviço de endpoint.
    - Desmarque 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.

- Se você habilitou recentemente outra zona de disponibilidade para seu balanceador de carga, ela aparece em Zonas de disponibilidade incluídas. Se você salvar as alterações na próxima etapa, isso ativará o serviço de endpoint para a nova zona de disponibilidade.

6. Selecione Save changes (Salvar alterações)

Para gerenciar os balanceadores de carga do seu 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 ter 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 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. 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. Selecione Save (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. Selecione Save (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. Selecione Save (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. Quando um provedor de serviços usa um nome DNS público existente como nome DNS privado para o serviço de endpoint, os consumidores do serviço não precisam alterar nenhuma aplicação que use

o nome DNS público existente. 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.
- Você não deve criar um registro A para o nome DNS privado, de modo que somente servidores na VPC do consumidor do serviço possam resolver o nome DNS privado.
- Nomes DNS privados não são compatíveis com endpoints do Gateway Load Balancer.
- 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 etiqueta 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.

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 AWS Management Console. 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: L6P0E 45JEVFwOCP RxlTt

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 sua zona hospedada pública. Use os seguintes valores:

- Em Record type (Tipo de registro), escolha TXT.
- Em TTL (seconds) (TTL [segundos]), insira **`1800`**.
- Para Routing policy (Política de roteamento), escolha Simple routing (Roteamento simples).
- Em Record name (Nome do registro), insira o domínio ou subdomínio.
- Para Value/Route traffic to (Valor/encaminhar tráfego para), insira o valor de verificação de domínio.

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.

Provedor de DNS/hospedagem	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 adicionar registros TXT/SPF/DKIM/DMARC ao 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 nslookup comando, que está disponível para Windows e Linux.

Você consultará os servidores DNS que atendem ao seu domínio porque esses servidores contêm a maioria das up-to-date informações do seu domínio. 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 corretamente publicado usando o seguinte comando, em que *name_server* é um dos servidores de nomes que você localizou 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.

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

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.

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

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 escolha 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)

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 você a solicitar as permissões corretas ao seu 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. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM.

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

Autenticando com identidades

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

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação Multifator no AWS IAM Identity Center Guia do Usuário. Usar a autenticação multifator (MFA) na AWS no Guia do Usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a

conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, 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 de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o . AWS IAM Identity Center Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no AWS IAM Identity Center Manual do Usuário do.

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos depender de credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne Chaves de Acesso Regularmente para Casos de Uso que exijam Credenciais de Longo Prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um nome de grupo IAMAdmins e atribuir a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a um aplicativo, mas uma função pode ser assumida por qualquer pessoa que precisar dela. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando Criar um Usuário do IAM (Ao Invés de uma Função) no Guia do Usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte Usando Funções do IAM no Guia do Usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criando um Perfil para um Provedor de Identidades Terceirizado no Guia do Usuário do IAM. Se você usa o IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no AWS IAM Identity Center Manual do Usuário.
- Permissões de usuários temporárias do IAM: um usuário ou perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: você pode usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) acesse recursos na sua conta de uma conta diferente. As funções são a forma primária de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para aprender a diferença entre funções e políticas baseadas em recurso para acesso entre contas, consulte Como as Funções do IAM Diferem das Políticas Baseadas em Recurso no Guia do Usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute

aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões de chamada da entidade principal, uma função de serviço ou uma função vinculada ao serviço.

- Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
- Função de Serviço: uma função de serviço é uma função do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criando um Perfil para Delegar Permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas a serviço.

- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar uma função do IAM para conceder permissões a aplicativos em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para aprender se deseja usar perfis do IAM, consulte Quando Criar uma Função do IAM (em Vez de um Usuário) no Guia do Usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão Geral das Políticas JSON no Guia do Usuário do IAM.

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.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM às funções e os usuários podem assumir as funções.

As políticas do IAM definem permissões para uma ação, independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em quais condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade também podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são incorporadas diretamente a um único usuário, grupo ou função. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como selecionar entre uma política gerenciada ou uma política em linha, consulte Selecionar entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de função do IAM e as políticas do bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em atributos são políticas em linha que estão localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou funções da conta) têm permissão para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Saiba mais sobre ACLs em Configurações da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade e dos seus limites de permissões. As políticas baseadas em atributo que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de Permissões para Entidades do IAM no Guia do Usuário do IAM.

- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte Como os SCPs Funcionam no AWS Organizations Manual do Usuário do.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para uma função ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, 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.

Recursos do IAM que você pode usar com AWS PrivateLink

Atributo do IAM	AWS PrivateLink apoio
Políticas baseadas em identidade	Sim
Políticas baseadas em atributos	Sim
Ações das políticas	Sim

Atributo do IAM	AWS PrivateLink apoio
atributos 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
Funções vinculadas ao serviço	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.

Políticas baseadas em identidade para AWS PrivateLink

Suporta com políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário IAM, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em quais condições. Saiba como criar uma política baseada em identidade consultando Criando Políticas do IAM no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou função à qual ela está anexada. Para saber mais sobre todos os elementos

que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade para AWS PrivateLink

Para ver exemplos de políticas AWS PrivateLink baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para AWS PrivateLink

Políticas baseadas em recursos dentro AWS PrivateLink

É compatível com políticas baseadas em atributos	Sim

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de função do IAM e as políticas do bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve 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, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em atributo é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em atributo conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Como os perfis do IAM diferem de políticas baseadas em recursos 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 ter mais informações, consulte the section called “Políticas de endpoint”.

Ações políticas para AWS PrivateLink

Oferece suporte a 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 você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

AWS PrivateLink compartilha seu namespace de API com o Amazon EC2. As ações de política AWS PrivateLink usam o seguinte prefixo antes da ação:

```
ec2
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
]
```

Você também pode especificar várias ações usando caracteres-curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Describe`, inclua a seguinte ação:

```
"Action": "ec2:Describe*"
```

Para ver uma lista de AWS PrivateLink ações, consulte AWS PrivateLink ações na Amazon EC2 API Reference. Para obter mais informações, consulte Ações definidas pelo Amazon EC2 na Referência de autorização do serviço.

Recursos políticos para AWS PrivateLink

Oferece suporte a atributos 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 `Resource` de política JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem suporte a um tipo de atributo específico, conhecido como permissões em nível de atributo.

Para ações não compatíveis com permissões no nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Chaves de condição de política para AWS PrivateLink

Suporta 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 principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite especificar condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. Você pode criar expressões condicionais que usem operadores de condição, como “igual a” ou “menor que”, para corresponder a condição da política aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos de Política do IAM: Variáveis e Tags no Guia do Usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. 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:VpceServiceName`
- `ec2:VpceServiceOwner`
- `ec2:VpceServicePrivateDnsName`

Para saber com quais ações e recursos você pode usar a chave de condição, consulte Ações definidas pelo Amazon EC2.

ACLs em AWS PrivateLink

Oferece suporte a ACLs	Não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou funções da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com AWS PrivateLink

Oferece suporte a ABAC (tags em políticas)	Sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir

operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre a tag no elemento de condição de uma política usando as chaves de condição `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para todo tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial.

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar Controle de Acesso Baseado em Atributos (ABAC) no Guia do Usuário do IAM.

Usando credenciais temporárias com AWS PrivateLink

Oferece suporte a credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS “Trabalhe com o IAM” no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para uma Função (Console) no Guia do Usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte Credenciais de segurança temporárias no IAM.

Permissões principais entre serviços para AWS PrivateLink

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou uma função do IAM para realizar ações em AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

Funções de serviço para AWS PrivateLink

Oferece suporte a perfis de serviço	Não

O perfil de serviço é um perfil do IAMhttps://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criando um Perfil para Delegar Permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

Funções vinculadas a serviços para AWS PrivateLink

É 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 o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas a serviço.

Exemplos de políticas baseadas em identidade para AWS PrivateLink

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do AWS PrivateLink . Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder permissões de usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis, e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM 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 a seguir.

```
{
    "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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc/*",
                "arn:aws:ec2:region:account-id:security-group/*",
                "arn:aws:ec2:region:account-id:subnet/*",
                "arn:aws:ec2:region:account-id:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id: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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpointServiceConfiguration",
                "ec2:CreateVpcEndpointServiceConfiguration"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id: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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc/*",
                "arn:aws:ec2:region:account-id:security-group/*",
                "arn:aws:ec2:region:account-id:subnet/*",
                "arn:aws:ec2:region:account-id:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.region.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 ter 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.

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 `Principal` elemento deve ser definido como. * Para especificar um principal, use a chave de `aws:PrincipalArn` condição.

```
"Condition": {
    "StringEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:user/endpointuser"
    }
}
```

Se você especificar o principal no formato a seguir, o acesso será concedido Usuário raiz da conta da AWS somente aos usuários e funções da conta, e não a todos.

```
"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. Selecione Save (Salvar).

Para atualizar uma política de endpoint usando a linha de comando

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

Métricas do CloudWatch para AWS PrivateLink

O AWS PrivateLink publica pontos de dados no Amazon CloudWatch para os seus endpoints de interface, endpoints de balanceador de carga de gateway e serviços de endpoint. O CloudWatch permite recuperar estatísticas sobre esses pontos de dados como um conjunto ordenado de dados de séries temporais, conhecidos 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.

Você pode usar métricas para verificar se o sistema está executando conforme o esperado. Por exemplo, você pode criar um alarme do CloudWatch para monitorar uma métrica específica e iniciar uma ação (como enviar uma notificação para um endereço de e-mail) se a métrica sair 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. Por padrão, o AWS PrivateLink envia métricas ao CloudWatch em intervalos de um minuto, sem custos adicionais.

Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch.

Índice

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	Descrição
`ActiveConnections`	O número de conexões ativas simultâneas. Isso métrica inclui conexões nos estados SYN_SENT e ESTABLISHED.

Métrica	Descrição
	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	Descrição
`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	Descrição
`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	Descrição
`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	Descrição
`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	Descrição
	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	Descrição
`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	Descrição
`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.

Visualizar as métricas do CloudWatch

Você pode examinar essas métricas do CloudWatch usando o console da Amazon VPC, o console do CloudWatch ou a AWS CLI, da seguinte maneira.

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).

Como exibir métricas usando o console do CloudWatch

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Metrics (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

O AWS PrivateLink fornece regras integradas do Contributor Insights para os serviços de endpoint, para ajudar você a determinar quais endpoints são os maiores colaboradores para cada métrica compatível. Para obter mais informações, consulte o tópico sobre o Contributor Insights, no Guia do usuário do Amazon CloudWatch.

O 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 para o Contributor Insights, consulte Definição de preços do Amazon CloudWatch.

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 habilitar as regras integradas para o AWS PrivateLink usando o AWS Management Console ou a AWS CLI.

Para habilitar as regras do Contributor Insights para AWS PrivateLink 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 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 usando 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

É possível desabilitar 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 desabilitar as regras do Contributor Insights para AWS PrivateLink 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 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 desabilitar as regras do Contributor Insights para AWS PrivateLink usando 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 integradas para o AWS PrivateLink usando o AWS Management Console ou a AWS CLI. 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 usando o console

1. Abra o console do CloudWatch 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 Delete (Excluir).

Para excluir as regras do Contributor Insights para AWS PrivateLink usando o AWS CLI

Use o comando delete-insight-rules para excluir a regra.

AWS PrivateLink cotas

As seguintes tabelas listam as cotas, denominadas anteriormente de limites, para os recursos do AWS PrivateLink por região para sua conta. Salvo indicação em contrário, é possível solicitar um aumento para essas cotas. Para obter mais informações, consulte Solicitando um Aumento de Cota no Guia do Usuário do Service Quotas.

Se solicitar um aumento de cota que seja aplicável por recurso, aumentaremos a cota para todos os recursos na Região.

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
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
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 Contribut or Insights para identificar endpoints específicos que são os principais contribuidores das CloudWatch métricas. AWS PrivateLink	18 de agosto de 2022
Suporte a IPv6	Os provedores de serviços podem permitir que o serviço de endpoint aceite solicitaç ões de IPv6, mesmo que os serviços de back-end sejam compatíveis somente com IPv4. Se o serviço de endpoint aceitar solicitações IPv6, os consumidores do serviço	11 de maio de 2022

	poderão habilitar o suporte IPv6 para os endpoints de interface para que possam acessar o serviço de endpoint por IPv6.	
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 utilizand o 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.