AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

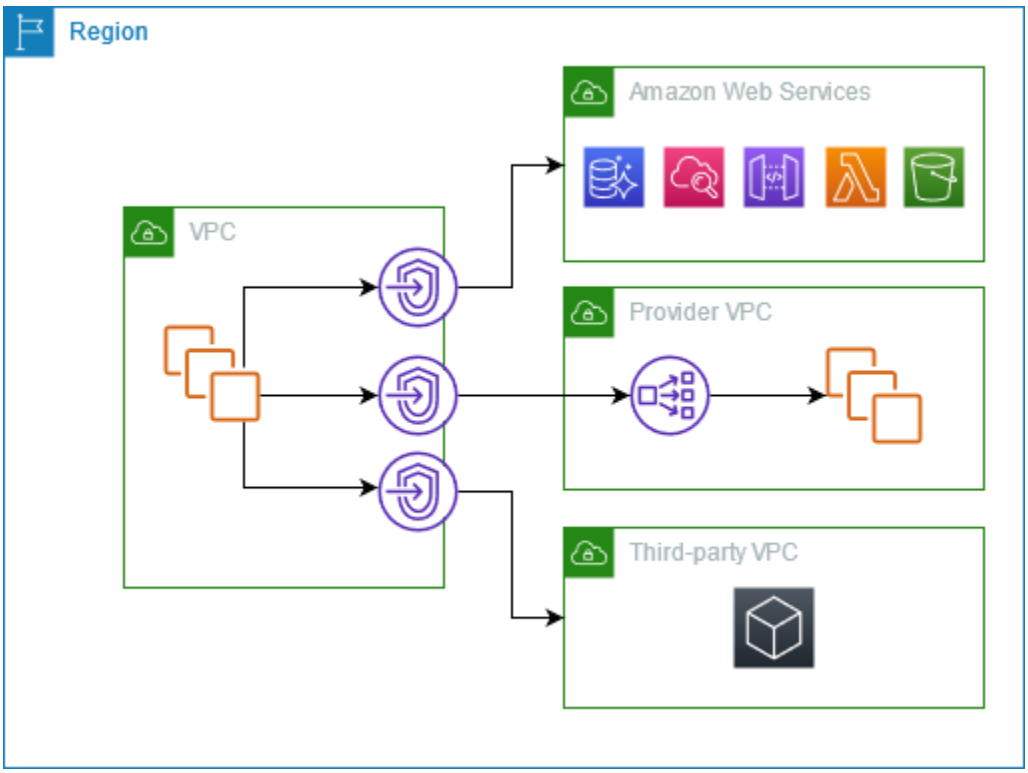
とは AWS PrivateLink

AWS PrivateLink は可用性が高くスケーラブルなテクノロジーで、 を のサービスとリソースVPC にプライベートに接続するために、 内にあるかのように使用できますVPC。プライベートサブネットからサービスまたは AWS Site-to-Site VPN リソースとの通信を許可するために、インターネットゲートウェイ、NATデバイス、パブリック IP アドレス、 AWS Direct Connect 接続、または接続を使用する必要はありません。したがって、 から到達可能な特定のAPIエンドポイント、サイト、サービス、リソースを制御しますVPC。

ユースケース

VPC エンドポイントを作成して、 内のクライアントVPCを と統合する のサービスやリソースに接続できます AWS PrivateLink。独自のVPCエンドポイントサービスを作成し、他の AWS お客様が利用できるようにします。詳細については、「the section called “概念”」を参照してください。

次の図VPCでは、左側の にプライベートサブネットに複数の Amazon EC2インスタンスがあり、3 つのインターフェイスVPCエンドポイント、リソースVPCエンドポイント、サービスネットワークVPCエンドポイントの 5 つのVPCエンドポイントがあります。最初のインターフェイスVPCエンドポイントは AWS サービスに接続します。2 番目のインターフェイスVPCエンドポイントは、別の AWS アカウント (VPCエンドポイントサービス) によってホストされるサービスに接続します。3 番目のインターフェイスVPCエンドポイントは AWS Marketplace パートナーサービスに接続します。リソースVPCエンドポイントはデータベースに接続します。サービスネットワークVPCエンドポイントは、サービスネットワークに接続します。



詳細

- the section called “概念”
- アクセス AWS のサービス
- SaaS 製品にアクセスする
- 仮想アプライアンスにアクセスする
- サービスを共有する

VPC エンドポイントの使用

VPC エンドポイントは、次のいずれかを使用して作成、アクセス、管理できます。

- AWS Management Console — AWS PrivateLink リソースへのアクセスに使用できるウェブインターフェイスを提供します。Amazon VPCコンソールを開き、エンドポイントまたはエンドポイントサービスを選択します。
- AWS Command Line Interface （ AWS CLI ） - AWS のサービスを含む幅広い のセットのコマンドを提供します AWS PrivateLink。のコマンドの詳細については AWS PrivateLink、「 コマンドリファレンス」の「ec2」を参照してください。 AWS CLI

- AWS CloudFormation - AWS リソースを説明するテンプレートを作成します。テンプレートを使用すると、これらのリソースを単一のユニットとして提供および管理できます。詳細については、以下の AWS PrivateLink リソースを参照してください。
  - AWS::EC2::VPCEndpoint
  - AWS::EC2::VPCEndpointConnectionNotification
  - AWS::EC2::VPCEndpointService
  - AWS::EC2::VPCEndpointServicePermissions
  - AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS SDKs — 言語固有の を提供しますAPIs。は、署名の計算、リクエストの再試行処理、エラー処理など、接続の詳細の多くSDKsを処理します。詳細については、「AWSでの構築ツール」を参照してください。
- クエリ API — HTTPSリクエストを使用して呼び出す低レベルのAPIアクションを提供します。クエリの使用はAPI、Amazon にアクセスする最も直接的な方法ですVPC。ただし、この方法では、リクエストに署名するハッシュの生成やエラー処理など、低レベルの詳細な作業をアプリケーションで処理する必要があります。詳細については、「Amazon EC2APIリファレンス」の「 AWS PrivateLink アクション」を参照してください。

料金

VPC エンドポイントの料金については、AWS PrivateLink 「 の料金」を参照してください。

AWS PrivateLink の概念

Amazon を使用して、論理的に分離された仮想ネットワークである仮想プライベートクラウド (VPC) VPCを定義できます。内のクライアントが、その 以外の送信先VPCに接続することを許可できますVPC。例えば、インターネットゲートウェイを に追加VPCしてインターネットへのアクセスを許可するか、VPN接続を追加してオンプレミスネットワークへのアクセスを許可します。または、 AWS PrivateLink を使用して、 内のクライアントがプライベート IP アドレスVPCsを使用して他の のサービスとリソースVPCに接続できるようにします。これは、それらのサービスおよびリソースが で直接ホストされている場合と同様ですVPC。

AWS PrivateLinkの使用を開始する際に理解しておくべき重要な概念を次に示します。

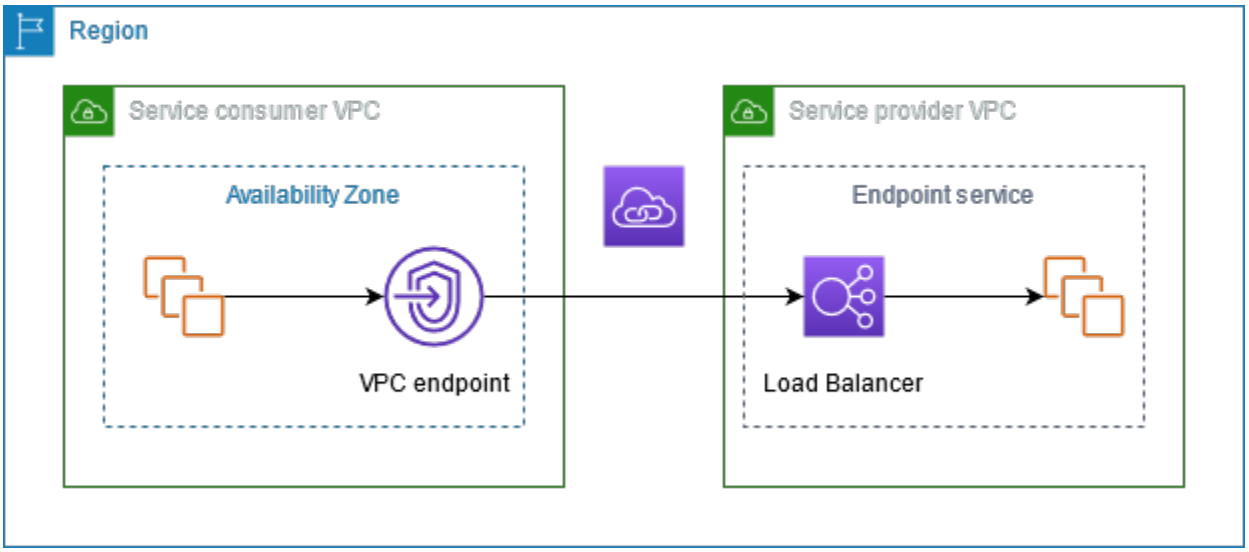
内容

- アーキテクチャ図

- プロバイダー
- サービスまたはリソースコンシューマー
- AWS PrivateLink 接続
- プライベートホストゾーン

アーキテクチャ図

次の図は、 AWS PrivateLink の仕組みの概要を示しています。コンシューマーは、プロバイダーがホストするVPCエンドポイントサービスとリソースに接続するためのエンドポイントを作成します。



プロバイダー

プロバイダーに関連する概念を理解します。

サービスプロバイダー

サービスの所有者はサービスプロバイダーです。サービスプロバイダーには AWS、 AWS 、パートナー、その他が含まれます AWS アカウント。サービスプロバイダーは、 EC2 インスタンスなどの AWS リソースまたはオンプレミスサーバーを使用してサービスをホストできます。

リソースプロバイダー

データベース、ノードのクラスター、インスタンスなどのリソースの所有者は、リソースプロバイダーです。リソースプロバイダーには、 AWS サービス、 AWS パートナー、およびその他の AWS

アカウントが含まれます。リソースプロバイダーは、 VPCsまたはオンプレミスでリソースをホストできます。

概念

- エンドポイントサービス
- サービス名
- サービスの状態
- リソース設定
- リソースゲートウェイ

エンドポイントサービス

サービスプロバイダーは、エンドポイントサービスを作成して、あるリージョンでそのサービスを利用できるようにします。サービスプロバイダーは、エンドポイントサービスを作成するときにロードバランサーを指定する必要があります。ロードバランサーは、サービスコンシューマーからリクエストを受け取ってサービスにルーティングします。

デフォルトでは、サービスコンシューマーはエンドポイントサービスを使用できません。特定の AWS プリンシパルがエンドポイントサービスに接続できるようにするアクセス許可を追加する必要があります。

サービス名

各エンドポイントサービスはサービス名で識別されます。サービスコンシューマーは、VPCエンドポイントの作成時にサービスの名前を指定する必要があります。サービスコンシューマーは、サービス名をクエリできます AWS のサービス。サービスプロバイダーは、自社のサービスの名前をサービスコンシューマーと共有する必要があります。

サービスの状態

エンドポイントサービスの可能な状態は次のとおりです。

- `Pending` - エンドポイントサービスを作成しています。
- `Available` - エンドポイントサービスが使用可能です。
- `Failed` - エンドポイントサービスを作成できませんでした。
- `Deleting` - サービスプロバイダーがエンドポイントサービスを削除し、その処理が進行中です。

- `Deleted` - エンドポイントサービスが削除されました。

リソース設定

リソースプロバイダーは、リソースを共有するためのリソース設定を作成します。リソース設定は、データベースなどの単一のリソース、またはノードのクラスターなどのリソースのグループを表す論理オブジェクトです。リソースには、IP アドレス、ドメイン名ターゲット、または Amazon RDS データベースを使用できます。

他のアカウントと共有する場合、リソースプロバイダーはリソース共有を介して AWS RAM リソースを共有し、他のアカウントの特定の AWS プリンシパルがリソースVPCエンドポイントを介してリソースに接続できるようにする必要があります。

リソース設定は、プリンシパルがサービスネットワークVPCエンドポイントを介して に接続するサービスネットワークに関連付けることができます。

リソースゲートウェイ

リソースゲートウェイは、リソースを共有している VPC への進入ポイントです。プロバイダーは、からリソースを共有するためのリソースゲートウェイを作成しますVPC。

サービスまたはリソースコンシューマー

サービスまたはリソースのユーザーはコンシューマーです。コンシューマーは、 VPCsまたはオンプレミスからエンドポイントサービスとリソースにアクセスできます。

概念

- VPC のエンドポイント
- エンドポイントのネットワークインターフェイス
- エンドポイントポリシー
- エンドポイントの状態

VPC のエンドポイント

コンシューマーは、VPCエンドポイントを作成して、 をVPCエンドポイントサービスまたはリソースに接続します。コンシューマーは、エンドポイントの作成時にVPCエンドポイントサービス、リソース、またはサービスネットワークを指定する必要があります。VPC エンドポイントには複数のタイプがあります。必要なVPCエンドポイントのタイプを作成する必要があります。

- `Interface` - エンドポイントサービスに TCPまたは UDPトラフィックを送信するインターフェイスエンドポイントを作成します。エンドポイントサービス宛てのトラフィックは、 を使用して解決されますDNS。
- `GatewayLoadBalancer` - Gateway Load Balancer エンドポイントを作成し、プライベート IP アドレスを使用してトラフィックを仮想アプライアンスのフリートに送信します。ルートテーブルを使用して、 から Gateway Load Balancer エンドポイントVPCにトラフィックをルーティングします。Gateway Load Balancer は、トラフィックを仮想アプライアンスに分散し、需要に応じてスケールできます。
- `Resource` - 共有され、別の にあるリソースにアクセスするためのリソースエンドポイントを作成しますVPC。リソースエンドポイントを使用すると、データベース、ノードのクラスター、インスタンス、アプリケーションエンドポイント、ドメイン名ターゲット、または別の VPC またはオンプレミス環境のプライベートサブネットにある IP アドレスなどのリソースに、プライベートかつ安全にアクセスできます。リソースエンドポイントはロードバランサーを必要とせず、リソースに直接アクセスできます。
- `Service network` - サービスネットワークエンドポイントを作成して、作成または共有したサービスネットワークにアクセスします。単一のサービスネットワークエンドポイントを使用して、サービスネットワークに関連付けられている複数のリソースとサービスにプライベートかつ安全にアクセスできます。

別のタイプのVPCエンドポイント がありGateway、Amazon S3 または DynamoDB にトラフィックを送信するゲートウェイエンドポイントを作成します。ゲートウェイエンドポイントは、他のタイプのVPCエンドポイントとは異なり AWS PrivateLink、 を使用しません。詳細については、「the section called “ゲートウェイエンドポイント”」を参照してください。

エンドポイントのネットワークインターフェイス

エンドポイントネットワークインターフェイスは、エンドポイントサービス、リソース、またはサービスネットワークを宛先とするトラフィックのエントリポイントとして機能するリクエスタマネージドネットワークインターフェイスです。VPC エンドポイントの作成時に指定したサブネットごとに、サブネットにエンドポイントネットワークインターフェイスが作成されます。

VPC エンドポイントが をサポートしている場合IPv4、そのエンドポイントネットワークインターフェイスには IPv4 アドレスがあります。VPC エンドポイントが をサポートしている場合IPv6、そのエンドポイントネットワークインターフェイスには IPv6 アドレスがあります。エンドポイントネットワークインターフェイスのIPv6アドレスにインターネットからアクセスできません。IPv6 アドレスを使用してエンドポイントネットワークインターフェイスを記述するときは、`denyAllIgwTraffic` が有効になっていることに注意してください。

エンドポイントポリシー

VPC エンドポイントポリシーは、VPCエンドポイントにアタッチする IAMリソースポリシーです。エンドポイントを使用してVPCエンドポイントサービスにアクセスできるプリンシパルを決定します。デフォルトのVPCエンドポイントポリシーでは、VPCエンドポイント上のすべてのリソースに対するすべてのプリンシパルによるすべてのアクションが許可されます。

エンドポイントの状態

インターフェイスVPCエンドポイントを作成すると、エンドポイントサービスは接続リクエストを受け取ります。サービスプロバイダーは、リクエストを受け入れるか、または拒否できます。サービスプロバイダーがリクエストを受け入れると、サービスコンシューマーは `Available`状態になった後にVPCエンドポイントを使用できます。

VPC エンドポイントに考えられる状態は次のとおりです。

- `PendingAcceptance` - 接続リクエストが保留中です。これは、リクエストが手動で受け入れられた場合の初期状態です。
- `Pending` - サービスプロバイダーが接続リクエストを受け入れました。これは、リクエストが自動で受け入れられた場合の初期状態です。サービスコンシューマーがVPCエンドポイントを変更すると、VPCエンドポイントはこの状態に戻ります。
- `Available` - VPCエンドポイントを使用できます。
- `Rejected` - サービスプロバイダーが接続リクエストを拒否しました。サービスプロバイダーは、接続が使用可能になった後にその接続を拒否することもできます。
- `Expired` - 接続リクエストの有効期限が切れました。
- `Failed` - VPCエンドポイントを使用できませんでした。
- `Deleting` - サービスコンシューマーがVPCエンドポイントを削除し、削除が進行中です。
- `Deleted` - VPCエンドポイントが削除されます。

AWS PrivateLink 接続

からのトラフィックVPCは、エンドポイントとエンドポイントサービスまたはリソース間の接続を使用してVPCエンドポイントサービスまたはリソースに送信されます。VPC エンドポイントとエンドポイントサービスまたはリソース間のトラフィックは、パブリックインターネットを経由することなく、ネットワーク内に AWS 留まります。

サービスプロバイダーは、サービスコンシューマーがエンドポイントサービスにアクセスできるように許可を追加します。サービスコンシューマーが接続を開始すると、サービスプロバイダーは接続リクエストを承諾または拒否します。リソース所有者またはサービスネットワーク所有者は、 を介してリソース設定またはサービスネットワークをコンシューマーと共有 AWS Resource Access Manager し、コンシューマーがリソースまたはサービスネットワークにアクセスできるようにします。

インターフェイスVPCエンドポイントを使用すると、コンシューマーはエンドポイントポリシーを使用して、エンドポイントを使用してVPCエンドポイントサービスまたはリソースにアクセスできるIAMプリンシパルを制御できます。

プライベートホストゾーン

ホストゾーンは、ドメインまたはサブドメインのトラフィックをルーティングする方法を定義するDNSレコードのコンテナです。パブリックホストゾーンでは、インターネット上でトラフィックをルーティングする方法をレコードで指定します。プライベートホストゾーンでは、レコードは でトラフィックをルーティングする方法を指定しますVPCs。

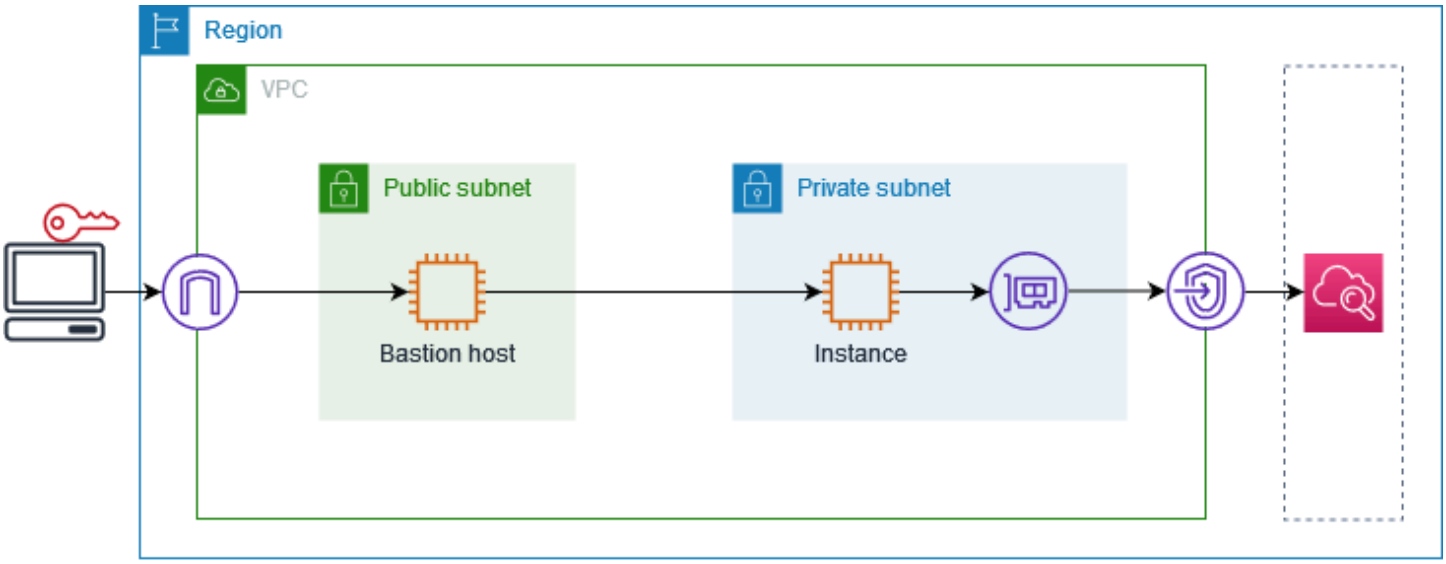
ドメイントラフィックをVPCエンドポイントにルーティングするように Amazon Route 53 を設定できます。詳細については、「ドメイン名を使用したVPCエンドポイントへのトラフィックのルーティング」を参照してください。

Route 53 を使用して分割期間 を設定できます。この場合DNS、パブリックウェブサイトと を使用するエンドポイントサービスの両方に同じドメイン名を使用します AWS PrivateLink。コンシューマーからのパブリックホスト名の DNS リクエストはエンドポイントネットワークインターフェイスのプライベート IP アドレスにVPC解決されますが、 の外部からの リクエストVPCは引き続きパブリックエンドポイントに解決されます。詳細については、DNS「トラフィックのルーティングとデプロイのフェイルオーバーの有効化のメカニズム AWS PrivateLink」を参照してください。

の使用を開始する AWS PrivateLink

このチュートリアルでは、 CloudWatch を使用してプライベートサブネットのEC2インスタンスから Amazon にリクエストを送信する方法を示します AWS PrivateLink。

次の図は、このシナリオの概要を示しています。コンピュータからプライベートサブネットのインスタンスに接続するには、まずパブリックサブネットの踏み台ホストに接続します。踏み台ホストとインスタンスの両方で同じキーペアを使用する必要があります。プライベートキーの.pemファイルは踏み台ホストではなくコンピュータにあるため、SSHキー転送を使用します。これで、ssh コマンドで .pem ファイルを指定しなくても、踏み台ホストからインスタンスに接続できます。のVPCエンドポイントを設定すると CloudWatch、送信先のインスタンスからのトラフィック CloudWatch はエンドポイントネットワークインターフェイスに解決され、VPCエンドポイント CloudWatch を使用して に送信されます。



テスト目的で、1 つのアベイラビリティーゾーンを使用できます。本番環境では、低レイテンシーと高可用性を得るために少なくとも 2 つのアベイラビリティーゾーンを使用することをお勧めします。

タスク

- ステップ 1: サブネットVPCを使用して を作成する
- ステップ 2: インスタンスを起動する
- ステップ 3: CloudWatch アクセスをテストする
- ステップ 4: アクセスするVPCエンドポイントを作成する CloudWatch

- ステップ 5: VPCエンドポイントをテストする
- ステップ 6: クリーンアップする

ステップ 1: サブネットVPCを使用して を作成する

次の手順を使用して、パブリックサブネットとプライベートサブネットVPCを持つ を作成します。

VPC を作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. [作成]VPC を選択します。
3. 作成するリソースで、 VPC などを選択します。
4. 名前タグの自動生成には、 の名前を入力しますVPC。
5. サブネットを設定するには、次の操作を行います。
   a. [アベイラビリティーゾーンの数] で、ニーズに応じて [1] または [2] を選択します。
   b. [パブリックサブネットの数] で、アベイラビリティーゾーンごとに 1 つのパブリックサブネットがあることを確認します。
   c. [Number of private subnets] (プライベートサブネットの数) で、アベイラビリティーゾーンごとに 1 つのプライベートサブネットがあることを確認します。
6. [作成]VPC を選択します。

ステップ 2: インスタンスを起動する

前のステップでVPC作成した を使用して、パブリックサブネットで踏み台ホストを起動し、プライベートサブネットでインスタンスを起動します。

前提条件

- .pem 形式を使用してキーペアを作成します。踏み台ホストとインスタンスの両方を起動するときに、このキーペアを選択する必要があります。
- コンピュータの CIDRブロックからのインバウンドSSHトラフィックを許可する踏み台ホストのセキュリティグループを作成します。
- 踏み台ホストのセキュリティグループからのインバウンドSSHトラフィックを許可するインスタンスのセキュリティグループを作成します。

- IAM インスタンスプロファイルを作成し、CloudWatchReadOnlyAccessポリシーをアタッチします。

踏み台ホストを起動するには

1. で Amazon EC2コンソールを開きますhttps://console.aws.amazon.com/ec2/。
2. Launch instance (インスタンスの起動) を選択します。
3. [Name] (名前) に、踏み台ホストの名前を入力します。
4. デフォルトのイメージおよびインスタンスタイプを維持します。
5. [Key pair] (キーペア) で、キーペアを選択します。
6. [Network settings] (ネットワーク設定) で、次の操作を行います。
   a. でVPC、 を選択しますVPC。
   b. [Subnet] (サブネット) で、パブリックサブネットを選択します。
   c. [Auto-assign public IP] (パブリック IP の自動割り当て) で、[Enable] (有効化) を選択します。
   d. [Firewall] (ファイアウォール) で [Select existing security group] (既存のセキュリティグループの選択) を選択してから、踏み台ホストのセキュリティグループを選択します。
7. Launch instance (インスタンスの起動) を選択します。

インスタンスを起動するには

1. で Amazon EC2コンソールを開きますhttps://console.aws.amazon.com/ec2/。
2. Launch instance (インスタンスの起動) を選択します。
3. [Name] (名前) に、インスタンスの名前を入力します。
4. デフォルトのイメージおよびインスタンスタイプを維持します。
5. [Key pair] (キーペア) で、キーペアを選択します。
6. [Network settings] (ネットワーク設定) で、次の操作を行います。
   a. でVPC、 を選択しますVPC。
   b. [Subnet] (サブネット) で、プライベートサブネットを選択します。
   c. [Auto-assign public IP] (パブリック IP の自動割り当て) で、[Disable] (無効化) を選択します。

d. [Firewall] (ファイアウォール) で [Select existing security group] (既存のセキュリティグループの選択) を選択してから、インスタンスのセキュリティグループを選択します。

7. [Advanced Details] (高度な詳細) を展開します。IAM インスタンスプロファイルで、IAMインスタンスプロファイルを選択します。
8. Launch instance (インスタンスの起動) を選択します。

ステップ 3: CloudWatch アクセスをテストする

インスタンスがアクセスできないことを確認するには、次の手順に従います CloudWatch。これを行うには、読み取り専用 AWS CLI コマンドを使用します CloudWatch。

CloudWatch アクセスをテストするには

1. コンピュータから、次のコマンドを使用してキーペアをSSHエージェントに追加します。ここで、 *key.pem*は .pem ファイルの名前です。

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

キーペアのアクセス許可が開放しすぎているいうエラーが表示された場合は、次のコマンドを実行してから、前のコマンドを再試行してください。

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

2. コンピュータから踏み台ホストに接続します。-A オプション、インスタンスユーザー名 (例: ec2-user)、および踏み台ホストのパブリック IP アドレスを指定する必要があります。

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

3. 踏み台ホストからインスタンスに接続します。インスタンスユーザー名 (例: ec2-user) とインスタンスのプライベート IP アドレスを指定する必要があります。

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

4. 次のようにインスタンスで CloudWatch list-metrics コマンドを実行します。--region オプションで、 を作成したリージョンを指定しますVPC。

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

5. 数分後、コマンドはタイムアウトします。これは、現在のVPC設定のインスタンス CloudWatch から にアクセスできないことを示しています。

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

6. インスタンスへの接続を維持します。VPC エンドポイントを作成したら、このlist-metricsコマンドを再試行します。

ステップ 4: アクセスするVPCエンドポイントを作成する CloudWatch

接続先のVPCエンドポイントを作成するには、次の手順に従います CloudWatch。

前提条件

トラフィックを許可するVPCエンドポイントのセキュリティグループを作成します CloudWatch。たとえば、 VPCCIDRブロックからのHTTPSトラフィックを許可するルールを追加します。

のVPCエンドポイントを作成するには CloudWatch

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. [エンドポイントの作成] を選択します。
4. [Name tag] (名前タグ) に、エンドポイントの名前を入力します。
5. [Service category] (サービスカテゴリ) で、AWS のサービス を選択します。
6. サービス で、com.amazonaws***region***.monitoring を選択します。
7. でVPC、 を選択しますVPC。
8. [Subnets] (サブネット) で、アベイラビリティーゾーンを選択してから、プライベートサブネットを選択します。
9. セキュリティグループで、VPCエンドポイントのセキュリティグループを選択します。
10. ポリシー では、フルアクセス を選択して、VPCエンドポイント上のすべてのリソースに対するすべてのプリンシパルによるすべてのオペレーションを許可します。
11. (オプション) タグを追加するには、[新しいタグを追加] を選択し、そのタグのキーと値を入力します。

12. [エンドポイントの作成] を選択します。初期ステータスは、Pending です。次のステップに進む前に、ステータスが Available になるまで待機します。これは数分かかることがあります。

ステップ 5: VPCエンドポイントをテストする

VPC エンドポイントがインスタンスから にリクエストを送信していることを確認します CloudWatch。

VPC エンドポイントをテストするには

インスタンスで次の コマンドを実行します。`--region` オプションで、VPCエンドポイントを作成したリージョンを指定します。

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

レスポンスが表示された場合は、空のレスポンスであっても、 CloudWatch を使用して に接続されます AWS PrivateLink。

`UnauthorizedOperation` エラーが発生した場合は、インスタンスにアクセスを許可する IAMロールがあることを確認してください CloudWatch。

リクエストがタイムアウトした場合は、次の点を確認してください。

- エンドポイントのセキュリティグループは、 へのトラフィックを許可します CloudWatch。
- `--region` オプションは、VPCエンドポイントを作成したリージョンを指定します。

ステップ 6: クリーンアップする

このチュートリアルで作成した踏み台ホストとインスタンスが不要になった場合は、終了させることができます。

インスタンスを終了するには

1. で Amazon EC2コンソールを開きますhttps://console.aws.amazon.com/ec2/。
2. ナビゲーションペインで、[インスタンス] を選択します。
3. 両方のテストインスタンスを選択し、[インスタンスの状態]、[インスタンスの終了] の順に選択します。
4. 確認を求めるメッセージが表示されたら、[終了] を選択します。

VPC エンドポイントが不要になった場合は、削除できます。

VPC エンドポイントを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. VPC エンドポイントを選択します。
4. アクション、VPCエンドポイントの削除を選択します。
5. 確認を求められたら、**delete**と入力し、[削除] を選択します。

AWS のサービス を介したアクセス AWS PrivateLink

エンドポイント AWS のサービス を使用して にアクセスします。デフォルトのサービスエンドポイントはパブリックインターフェイスであるため、トラフィックが から VPCに到達VPCできるように、インターネットゲートウェイを に追加する必要があります AWS のサービス。この設定がネットワークセキュリティ要件に対応していない場合は、 AWS PrivateLink を使用して、インターネットゲートウェイを使用せずにVPC、 内にあるVPC AWS のサービス かのように に接続できます。

VPC エンドポイント AWS PrivateLink を使用して、 と統合 AWS のサービス する にプライベートにアクセスできます。インターネットゲートウェイを使用せずに、アプリケーションスタックのすべてのレイヤーを構築および管理できます。

料金

インターフェイスVPCエンドポイントが各アベイラビリティーゾーンでプロビジョニングされる 1 時間ごとに課金されます。また、処理されたデータの GB ごとに課金されます。詳細については、「AWS PrivateLink 料金」を参照してください。

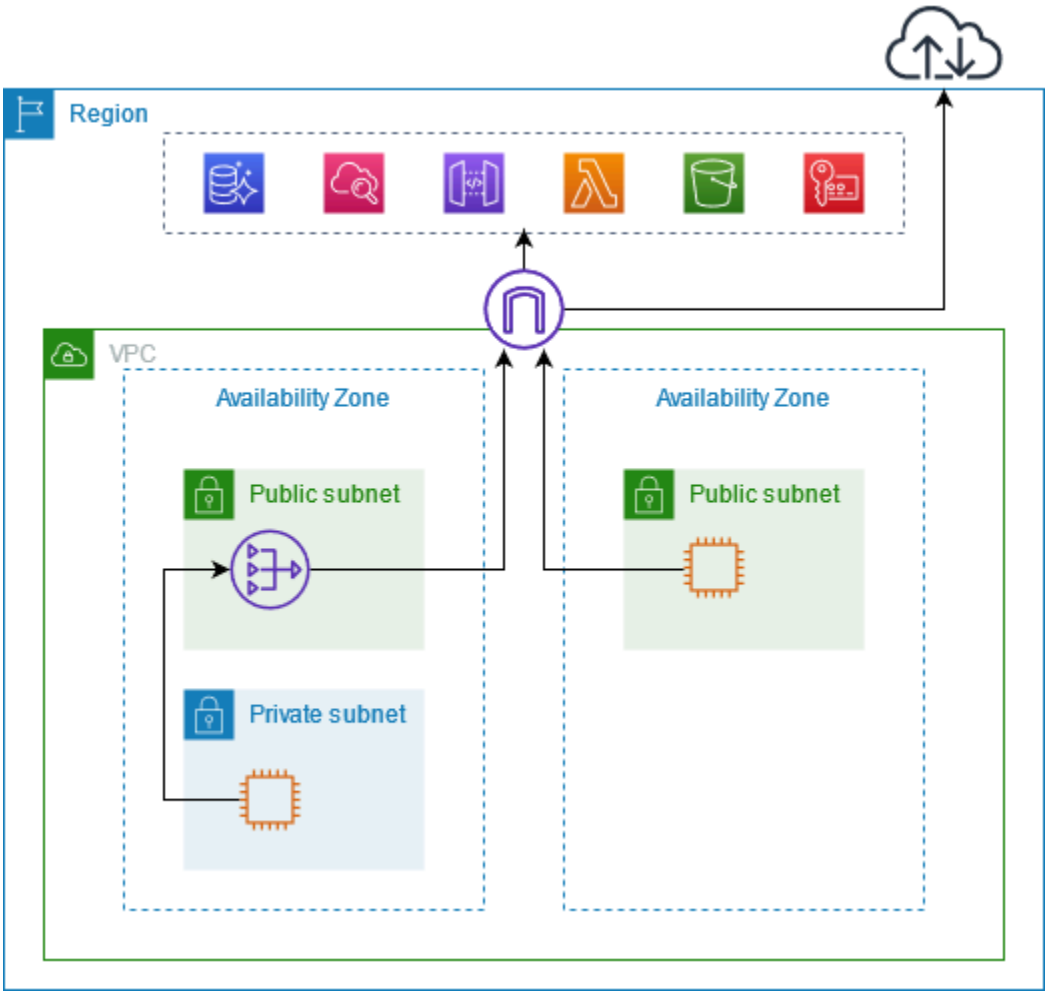
内容

概要

パブリックサービスエンドポイント AWS のサービス から にアクセスするか、 AWS のサービス を使用してサポートされている に接続できます AWS PrivateLink。この概要では、これらの方法を比較します。

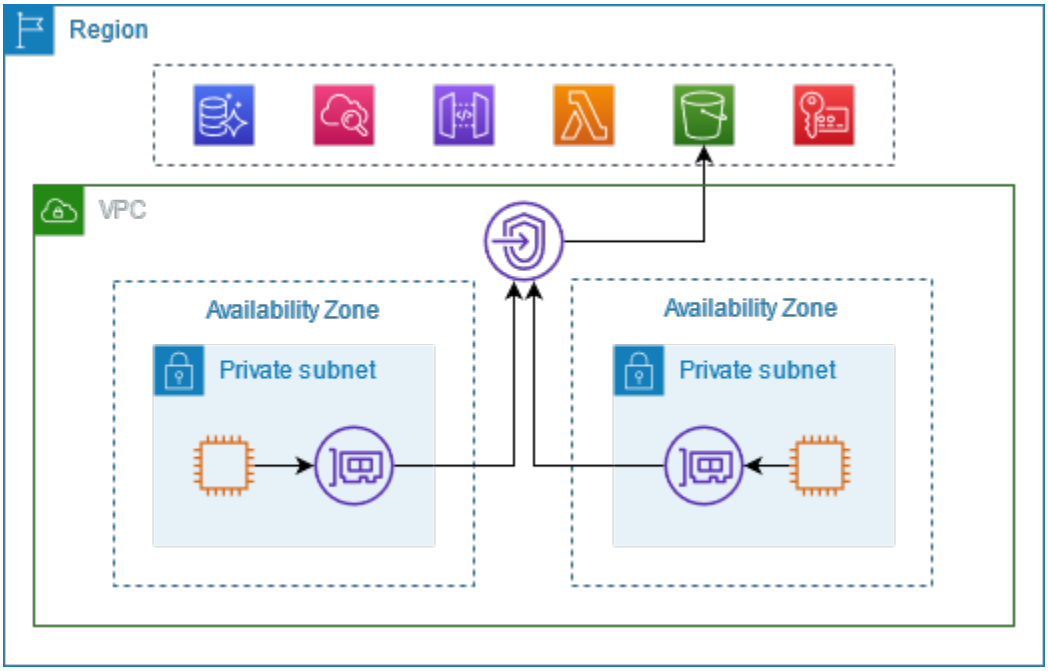
パブリックサービスエンドポイント経由でアクセスする

次の図は、インスタンスがパブリックサービスエンドポイント AWS のサービス を介して にアクセスする方法を示しています。パブリックサブネットのインスタンス AWS のサービス から へのトラフィックは、 のインターネットゲートウェイにルーティングVPCされ、次に にルーティングされます AWS のサービス。プライベートサブネットのインスタンス AWS のサービス から へのトラフィックは、NATゲートウェイにルーティングされ、次に のインターネットゲートウェイにルーティングされVPC、次に にルーティングされます AWS のサービス。このトラフィックはインターネットゲートウェイを通過しますが、 AWS ネットワークを離れることはありません。



経由で接続する AWS PrivateLink

次の図は、インスタンスが AWS のサービス にアクセスする方法を示しています AWS PrivateLink。まず、 ネットワークインターフェイス AWS のサービス を使用して、 のサブネットVPCと 間の接続を確立するインターフェイスVPCエンドポイントを作成します。宛てのトラフィック AWS のサービス は、 を使用してエンドポイントネットワークインターフェイスのプライベート IP アドレスに解決されDNS、VPCエンドポイントと 間の接続 AWS のサービス を使用して に送信されます AWS のサービス。



AWS のサービス は自動的に接続リクエストを受け入れます。サービスは、VPCエンドポイントを介してリソースへのリクエストを開始できません。

DNS ホスト名

ほとんどの AWS のサービス は、次の構文を持つパブリックリージョンエンドポイントを提供します。

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

例えば、us-east-2 CloudWatch の Amazon のパブリックエンドポイントは次のとおりです。

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

では AWS PrivateLink、プライベートエンドポイントを使用してトラフィックを サービスに送信します。インターフェイスVPCエンドポイントを作成すると、 AWS のサービス からの との通信に使用できるリージョン名とゾーンDNS名が作成されますVPC。

インターフェイスVPCエンドポイントのリージョンDNS名には、次の構文があります。

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

ゾーンDNS名には次の構文があります。

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

のインターフェイスVPCエンドポイントを作成するときに AWS のサービス、プライベート DNSを有効にできます。プライベート を使用するとDNS、インターフェイスエンドポイントを介したプライベート接続を活用しながら、パブリックVPCエンドポイントDNSの名前を使用してサービスにリクエストを引き続き行うことができます。詳細については、「the section called “DNS 解像度”」を参照してください。

次のdescribe-vpc-endpointsコマンドは、インターフェイスエンドポイントのDNSエントリを表示します。

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

プライベートDNS名が有効になってい CloudWatch る Amazon のインターフェイスエンドポイントの出力例を次に示します。最初のエントリは、リージョンレベルのプライベートエンドポイントです。次の 3 つのエントリは、ゾーンレベルのプライベートエンドポイントです。最後のエントリは、隠れたプライベートホストゾーンからのもので、パブリックエンドポイントに対するリクエストを、エンドポイントのネットワークインターフェイスのプライベート IP アドレスに解決します。

```
[
    [
        {
            "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"
        }
    ]
]
```

DNS 解像度

インターフェイスVPCエンドポイント用に作成するDNSレコードはパブリックです。したがって、これらのDNS名前はパブリックに解決可能です。ただし、 の外部からのDNSリクエストはエンドポイントネットワークインターフェイスのプライベート IP アドレスをVPC返すため、 にアクセスできる場合を除き、これらの IP アドレスを使用してエンドポイントサービスにアクセスすることはできませんVPC。

プライベート DNS

インターフェイスVPCエンドポイントDNSでプライベートを有効にし、 VPCでDNSホスト名とDNS解像度の両方が有効になっている場合、非表示の AWSマネージドプライベートホストゾーンが作成されます。ホストゾーンには、 のエンドポイントネットワークインターフェイスのプライベート IP アドレスに解決されるサービスのデフォルトDNS名のレコードセットが含まれていますVPC。したがって、パブリックリージョンエンドポイント AWS のサービス を使用して にリクエストを送信する既存のアプリケーションがある場合、それらのリクエストはエンドポイントネットワークインターフェイスを通過するようになり、それらのアプリケーションに変更を加える必要がありません。

VPC エンドポイントのプライベートDNS名を有効にすることをお勧めします AWS のサービス。これにより、 を介して行われたリクエストなど、パブリックサービスエンドポイントを使用するリクエストが AWS SDKエンドポイントに解決されますVPC。

Amazon はVPC、Route 53 Resolver と呼ばれる 用のDNSサーバーを提供しています。Route 53 Resolver は、プライベートホストゾーンのローカルVPCドメイン名とレコードを自動的に解決します。ただし、 の外部から Route 53 Resolver を使用することはできませんVPC。オンプレミスネットワークからVPCエンドポイントにアクセスする場合は、Route 53 Resolver エンドポイントと Resolver ルールを使用できます。詳細については、「AWS Transit GatewayAWS PrivateLink と の統合 Amazon Route 53 Resolver」を参照してください。

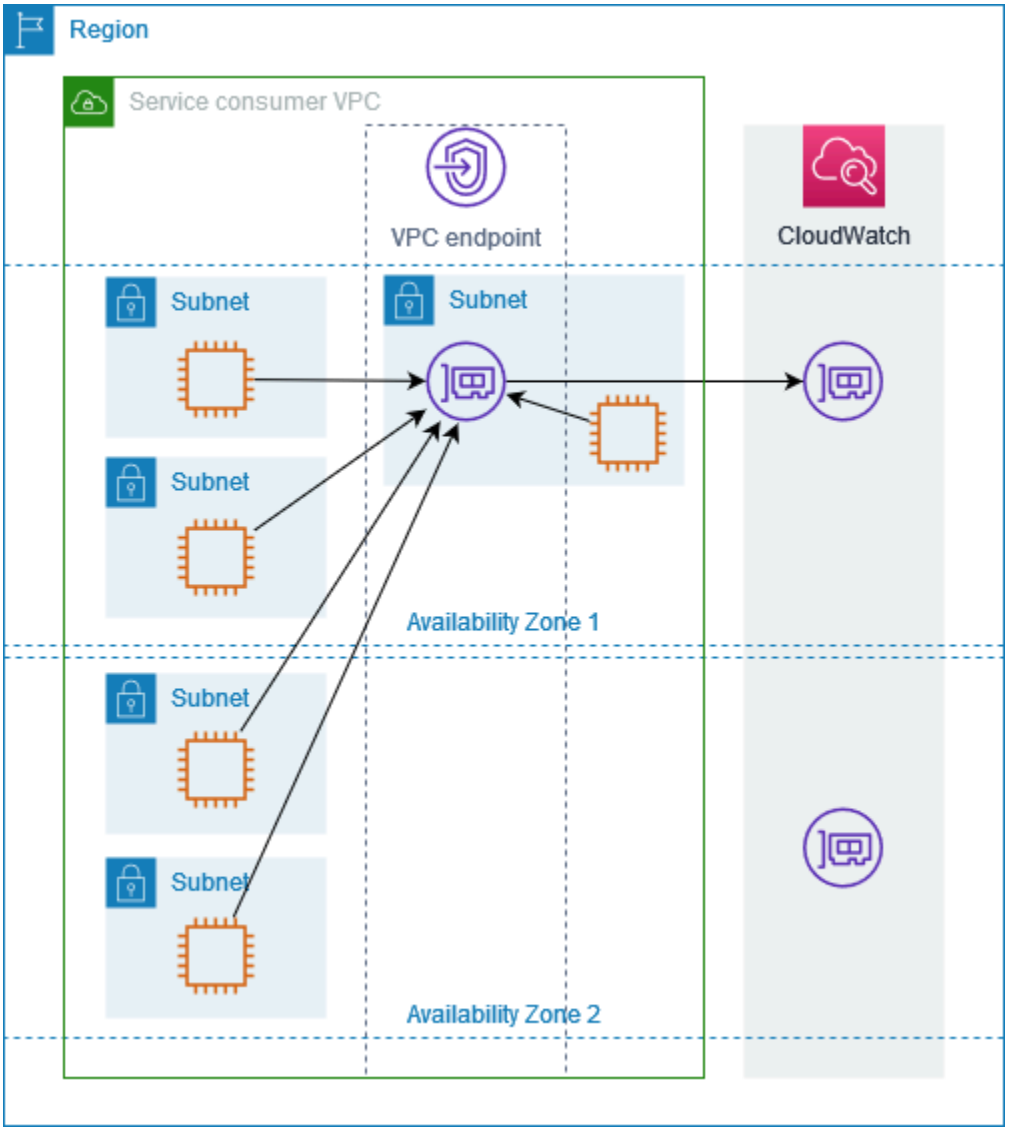
サブネットとアベイラビリティーゾーン

アベイラビリティーゾーンごとに 1 つのサブネットを使用してVPCエンドポイントを設定できます。サブネット内のエンドポイントのVPCエンドポイントネットワークインターフェイスを作成します。エンドポイントの IP アドレスタイプに基づいて、サブネットから各エンドポイントネットワークインターフェイスに IP アドレスを割り当てます。 VPCエンドポイントネットワークインターフェイスの IP アドレスは、VPCエンドポイントの存続期間中は変更されません。

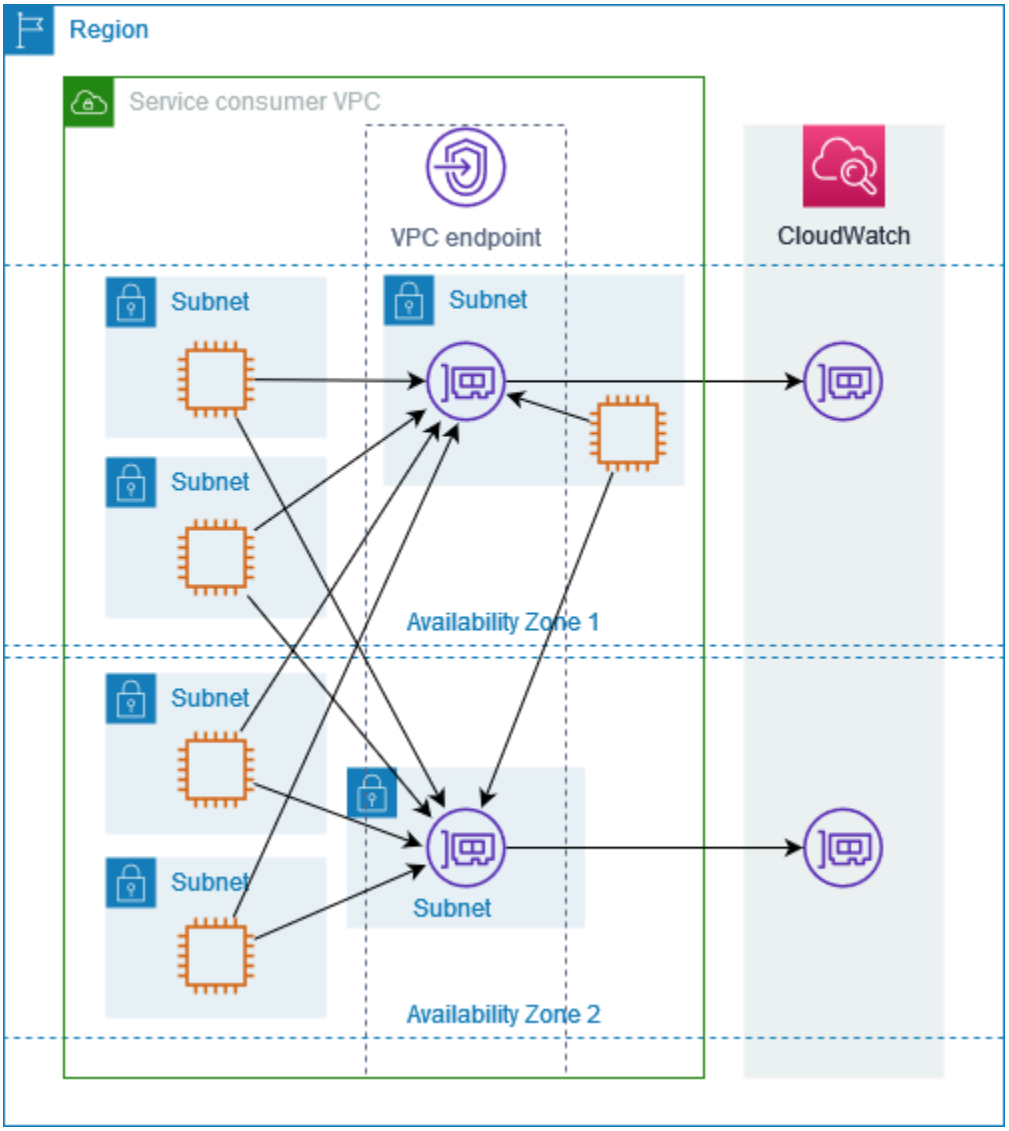
本番環境では、高い可用性と耐障害性を実現するには、以下をお勧めします。

- VPC エンドポイントごとに少なくとも 2 つのアベイラビリティーゾーンを設定し、これらのアベイラビリティーゾーン AWS のサービス の にアクセスする必要があるリソースを AWS デプロイします。
- VPC エンドポイントのプライベートDNS名を設定します。
- パブリックエンドポイントとも呼ばれるリージョンDNS名 AWS のサービス を使用して にアクセスします。

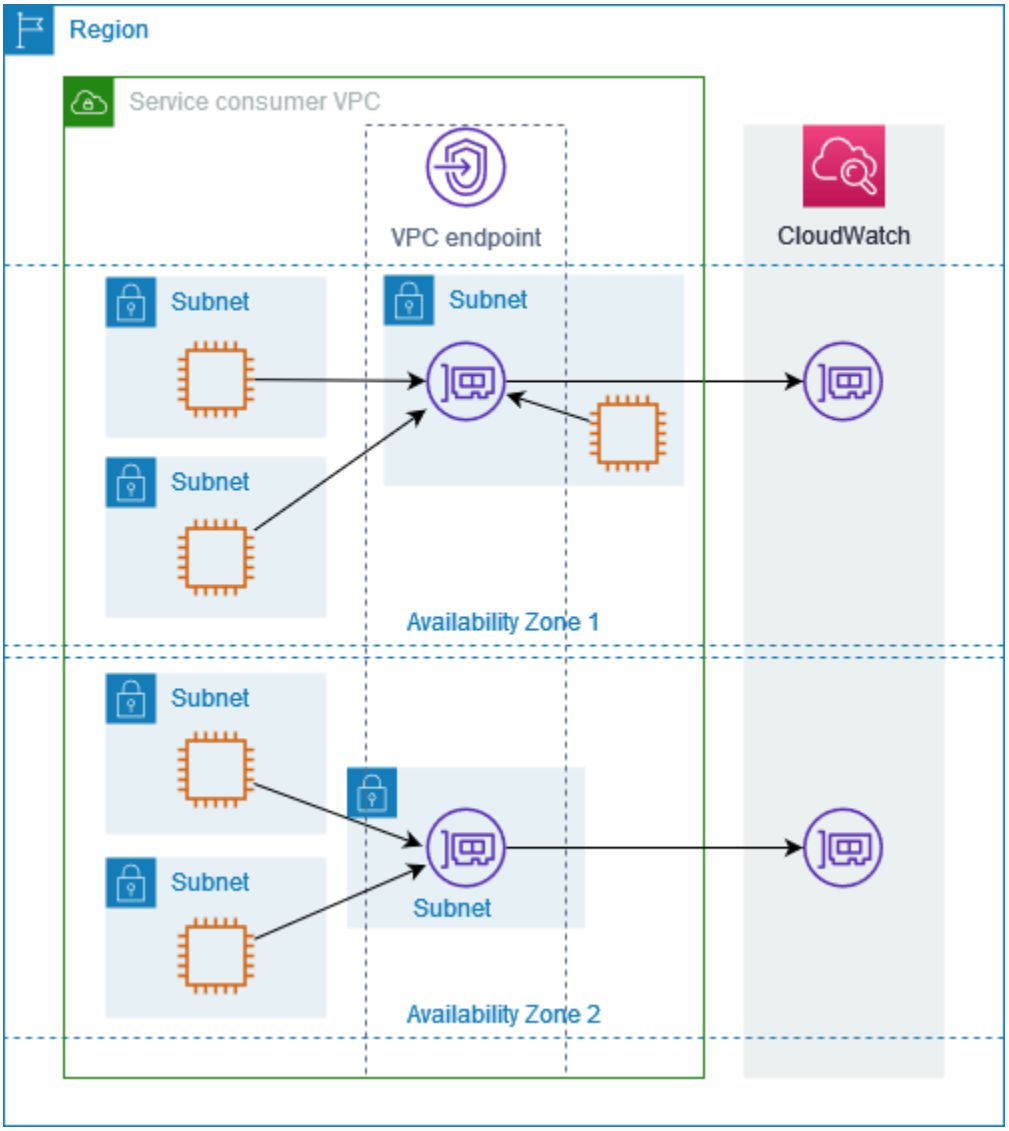
次の図は、単一のアベイラビリティーゾーンにVPCエンドポイントネットワークインターフェイス CloudWatch を持つ Amazon のエンドポイントを示しています。のサブネット内のいずれかのリソースがパブリックエンドポイントを使用して Amazon CloudWatch VPCにアクセスすると、トラフィックはエンドポイントネットワークインターフェイスの IP アドレスに解決されます。これには、他のアベイラビリティーゾーン内のサブネットからのトラフィックが含まれます。ただし、アベイラビリティーゾーン 1 に障害が発生した場合、アベイラビリティーゾーン 2 のリソースは Amazon にアクセスできなくなります CloudWatch。



次の図は、2 つのアベイラビリティーゾーンにVPCエンドポイントネットワークインターフェイス CloudWatch を持つ Amazon のエンドポイントを示しています。のサブネット内のいずれかのリソースがパブリックエンドポイント CloudWatch を使用して Amazon VPCにアクセスすると、ラウンドロビンアルゴリズムを使用してそれらのリソースを交互に操作する正常なエンドポイントネットワークインターフェイスが選択されます。次に、選択したエンドポイントネットワークインターフェイスの IP アドレスへのトラフィックを解決します。



ユースケースに適している場合は、同じアベイラビリティーゾーン内のエンドポイントネットワークインターフェイスを使用して、リソースから AWS のサービス にトラフィックを送信できます。そのためには、プライベートゾーンエンドポイントまたはエンドポイントネットワークインターフェイスの IP アドレスを使用します。



IP アドレスのタイプ

AWS のサービス は、パブリックエンドポイントIPv6を介して をサポートしていない場合でも、プライベートエンドポイントIPv6を介して をサポートできます。をサポートするエンドポイントは、AAAAレコードでDNSクエリに応答IPv6できます。

インターフェイスエンドポイントIPv6で を有効にするための要件

- は、サービスエンドポイントを 経由で利用可能に AWS のサービス する必要がありますIPv6。詳細については、「the section called “IPv6 サポートを表示する”」を参照してください。
- インターフェイスエンドポイントの IP アドレスのタイプは、次に説明するように、インターフェイスエンドポイントのサブネットと互換性がある必要があります。

- IPv4 – エンドポイントネットワークインターフェイスにIPv4アドレスを割り当てます。このオプションは、選択したすべてのサブネットにIPv4アドレス範囲がある場合にのみサポートされます。
- IPv6 – エンドポイントネットワークインターフェイスにIPv6アドレスを割り当てます。このオプションは、選択したすべてのサブネットがサブネットIPv6のみの場合にのみサポートされます。
- デュアルスタック — エンドポイントネットワークインターフェイスに IPv4と IPv6 アドレスの両方を割り当てます。このオプションは、選択したすべてのサブネットに IPv4と の両方のIPv6アドレス範囲がある場合にのみサポートされます。

インターフェイスVPCエンドポイントが をサポートしている場合IPv4、エンドポイントネットワークインターフェイスには IPv4 アドレスがあります。インターフェイスVPCエンドポイントが をサポートしている場合IPv6、エンドポイントネットワークインターフェイスには IPv6 アドレスがあります。エンドポイントネットワークインターフェイスのIPv6アドレスにインターネットからアクセスできません。IPv6 アドレスを使用してエンドポイントネットワークインターフェイスを記述する場合は、 `denyAllIgwTraffic` が有効になっていることに注意してください。

AWS のサービス と統合する AWS PrivateLink

以下は と AWS のサービス 統合されています AWS PrivateLink。VPC エンドポイントを作成して、独自の で実行されているかのように、これらのサービスにプライベートに接続できますVPC。

AWS のサービス 列のリンクを選択すると、 と統合するサービスのドキュメントが表示されます AWS PrivateLink。サービス名列には、インターフェイスVPCエンドポイントの作成時に指定したサービス名が含まれているか、サービスがエンドポイントを管理することを示します。

AWS のサービス	サービス名
Access Analyzer	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 のサービス	サービス名
AWS App Mesh	com.amazonaws.*region*.appmesh
	com.amazonaws*region*。appmesh-envoy-management
AWS App Runner	com.amazonaws.*region*.apprunner
AWS App Runner サービス	com.amazonaws.*region*.apprunner.requests
Application Auto Scaling	com.amazonaws*region*..application-autoscaling
AWS Application Discovery Service	com.amazonaws*region*.discovery
	com.amazonaws*region*.arsenal-discovery
AWS アプリケーション移行サービス	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 データ交換	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.*region*.bedrock

AWS のサービス	サービス名
	com.amazonaws.*region*.bedrock-agent
	com.amazonaws*region*。bedrock-agent-runtime
	com.amazonaws.*region*.bedrock-runtime
AWS Billing and Cost Management	com.amazonaws.*region*.billing
	com.amazonaws.*region*.freetier
	com.amazonaws.*region*.tax
AWS Billing Conductor	com.amazonaws.*region*.billingconductor
Amazon Braket	com.amazonaws*region*.braket
AWS クリーンルーム	com.amazonaws.*region*.cleanrooms
AWS Clean Rooms ML	com.amazonaws.*region*.cleanrooms-ml
AWS Cloud Control API	com.amazonaws.*region*.cloudcontrolapi
	com.amazonaws.*region*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.*region*.servicediscovery
	com.amazonaws.*region*.servicediscovery-fips
	com.amazonaws*region*.data-servicediscovery
	com.amazonaws*region*。data-servicediscovery-fips
AWS CloudTrail	com.amazonaws.*region*cloudtrail

AWS のサービス	サービス名
Amazon CloudWatch	com.amazonaws*region*..application-signals
	com.amazonaws*region*..applicationinsights
	com.amazonaws*region*.evidently
	com.amazonaws*region*.evidently-dataplane
	com.amazonaws.*region*.internetmonitor
	com.amazonaws.*region*.internetmonitor-fips
	com.amazonaws*region*.monitoring
	com.amazonaws.*region*.networkflowmonitor
	com.amazonaws.*region*.networkflowmonitorreports
	com.amazonaws.*region*.networkmonitor
	com.amazonaws*region*..observabilityadmin
	com.amazonaws.*region*.rum
	com.amazonaws.*region*.rum-dataplane
	com.amazonaws*region*..synthetics
	com.amazonaws.*region*.synthetics-fips
Amazon CloudWatch ログ	com.amazonaws.*region*.logs
AWS CodeArtifact	com.amazonaws.*region*.codeartifact.api
	com.amazonaws.*region*.codeartifact.repositories
AWS CodeBuild	com.amazonaws.*region*.codebuild
	com.amazonaws.*region*.codebuild-fips

AWS のサービス	サービス名
AWS CodeCommit	com.amazonaws.*region*.codecommit
	com.amazonaws.*region*.codecommit-fips
	com.amazonaws*region*.git-codecommit
	com.amazonaws*region*。git-codecommit-fips
AWS CodeConnections	com.amazonaws*region*..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
Amazon CodeGuru Reviewer	com.amazonaws.*region*.codeguru-reviewer
AWS CodePipeline	com.amazonaws.*region*.codepipeline
Amazon Comprehend	com.amazonaws*region*.comprehend
Amazon Comprehend Medical	com.amazonaws*region*..comprehend™
AWS Compute Optimizer	com.amazonaws*region*.compute-optimizer
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

AWS のサービス	サービス名
	com.amazonaws.*region*.wisdom
AWS Connector Service	com.amazonaws*region*..awsconnector
AWS Control Catalog	com.amazonaws.*region*.controlcatalog
AWS Cost Explorer	com.amazonaws*region*.ce
AWS Cost Optimization Hub	com.amazonaws*region*。cost-optimization-hub
AWS Data Exchange	com.amazonaws*region*..dataexchange
AWS Data Exports	com.amazonaws*region*。bcm-data-exports
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*region*..datazone
AWS Deadline Cloud	com.amazonaws*region*..deadline.management
	com.amazonaws*region*.deadline.scheduling
DevOpsAmazonGuru	com.amazonaws*region*.devops-guru
AWS Directory Service	com.amazonaws*region*.ds
	com.amazonaws*region*.ds-data
Amazon DocumentDB	com.amazonaws.*region*.rds
Amazon DynamoDB	com.amazonaws.*region*.dynamodb
	com.amazonaws.*region*.dynamodb-fips

AWS のサービス	サービス名
Amazon EBS direct APIs	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
Elastic Load Balancing	com.amazonaws.*region*.elasticloadbalancing
Amazon ElastiCache	com.amazonaws*region*..elasticache
	com.amazonaws*region*..elasticache-fips
AWS Elemental MediaConnect	com.amazonaws*region*..mediaconnect

AWS のサービス	サービス名
Amazon EMR	com.amazonaws*region*..elasticmapreduce
EMRでの Amazon EKS	com.amazonaws*region*.emr-containers
Amazon EMR Serverless	com.amazonaws*region*.emr-serverless
	com.amazonaws.*region*emr-serverless-services.livy
Amazon EMRWAL	com.amazonaws*region*.emrwal.prod
AWS エンドユーザーメッセージング ソーシャル	com.amazonaws*region*..social-messaging
AWS Entity Resolution	com.amazonaws*region*.entityresolution
Amazon EventBridge	com.amazonaws.*region*.events
	com.amazonaws.*region*.pipes
	com.amazonaws.*region*.pipes-data
	com.amazonaws.*region*.pipes-fips
	com.amazonaws*region*..schemas
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

AWS のサービス	サービス名
Amazon FSx	com.amazonaws*region*..fsx
	com.amazonaws*region*..fsx-fips
AWS Glue	com.amazonaws.*region*.glue
	com.amazonaws*region*.glue.dashboard
AWS Glue DataBrew	com.amazonaws*region*..databrew
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
	com.amazonaws.*region*.guardduty-data
	com.amazonaws*region*。guardduty-data-fips
	com.amazonaws.*region*.guardduty-fips
AWS HealthImaging	com.amazonaws*region*。dicom-medical-imaging
	com.amazonaws*region*..="-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

AWS のサービス	サービス名
	com.amazonaws*region*..workflows-omics
AWS Identity and Access Management (IAM)	com.amazonaws.iam
IAM アイデンティティセンター	com.amazonaws.*region*.identitystore
IAM Roles Anywhere	com.amazonaws.*region*.rolesanywhere
Amazon Inspector	com.amazonaws.*region*.inspector2
	com.amazonaws.*region*.inspector-scan
AWS IoT Core	com.amazonaws*region*.iot.data
	com.amazonaws*region*.iot.credentials
	com.amazonaws*region*.iot.fleethub.api
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

AWS のサービス	サービス名
Amazon Kendra	com.amazonaws.*region*.kendra
	aws.api.*region*.kendra ランク付け
AWS Key Management Service	com.amazonaws.*region*.kms
	com.amazonaws.*region*.kms-fips
Amazon Keyspaces (Apache Cassandra 向け)	com.amazonaws*region*..cassandra
	com.amazonaws*region*..cassandra-fips
Amazon Kinesis Data Streams	com.amazonaws.*region*.kinesis-streams
	com.amazonaws*region*。kinesis-streams-fips
AWS Lake Formation	com.amazonaws.*region*.lakeformation
AWS Lambda	com.amazonaws*region*.lambda
AWS Launch Wizard	com.amazonaws*region*..launchwizard
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-linux-subscriptions
	com.amazonaws.*region*.license-manager-linux-subscriptions-fips
	com.amazonaws*region*。license-manager-user-subscriptions

AWS のサービス	サービス名
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.*region*.apptest
	com.amazonaws.*region*.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 Streaming for Apache Kafka	com.amazonaws*region*.kafka
	com.amazonaws*region*..kafka-fips
Amazon Managed Workflows for Apache Airflow	com.amazonaws*region*.airflow.api
	com.amazonaws*region*.airflow.api-fips
	com.amazonaws.airflow*region*.env
	com.amazonaws*region*.airflow.env-fips
	com.amazonaws.*region*airflow.ops
AWS Management Console	com.amazonaws.*region*.console

AWS のサービス	サービス名
	com.amazonaws.*region*.signin
Amazon MemoryDB	com.amazonaws*region*.memory-db
	com.amazonaws*region*.memorydb-fips
AWS Migration Hub Orchestrator	com.amazonaws*region*.migrationhub-orchestrator
AWS Migration Hub Refactor Spaces	com.amazonaws*region*..refactor-spaces
Migration Hub 戦略レコメンデーション	com.amazonaws*region*.migrationhub-strategy
Amazon MQ	com.amazonaws*region*.mq
Amazon Neptune Analytics	com.amazonaws*region*..neptune-graph
	com.amazonaws*region*。neptune-graph-data
	com.amazonaws*region*。neptune-graph-fips
AWS Network Firewall	com.amazonaws*region*..network-firewall
	com.amazonaws*region*。network-firewall-fips
Amazon OpenSearch サービス	これらのエンドポイントはサービス管理されています
AWS Organizations	com.amazonaws*region*..organizations
	com.amazonaws*region*.organizations-fips
AWS Outposts	com.amazonaws.*region*.outposts
AWS Panorama	com.amazonaws*region*..panorama
AWS Payment Cryptography	com.amazonaws.*region*. Payment-cryptography.controlplane

AWS のサービス	サービス名
	com.amazonaws.*region*. Payment-cryptography.datapl ane
AWS PCS	com.amazonaws.*region*.pcs
	com.amazonaws*region*..pcs-fips
Amazon Personalize	com.amazonaws*region*.personalize
	com.amazonaws.*region*.personalize-events
	com.amazonaws*region*..personalize-runtime
Amazon Pinpoint	com.amazonaws*region*.pinpoint
	com.amazonaws.*region*.pinpoint-sms-voice-v2
Amazon Polly	com.amazonaws.*region*.polly
AWS の料金表	com.amazonaws*region*.pricing.api
AWS プライベート 5G	com.amazonaws*region*..private-networks
AWS Private Certificate Authority	com.amazonaws*region*.acm-pca
	com.amazonaws*region*。pca-connector-ad
	com.amazonaws*region*。pca-connector-scep
AWS Proton	com.amazonaws*region*.proton
Amazon Q Business	aws.api.*region*.qbusiness
Amazon Q Developer	com.amazonaws.*region*.codewhisperer
	com.amazonaws.*region*.q
	com.amazonaws*region*..qapps

AWS のサービス	サービス名
Amazon Q ユーザーサブスクリプション	com.amazonaws.*region*service.user-subscriptions
Amazon QLDB	com.amazonaws*region*.qldb.session
Amazon QuickSight	com.amazonaws*region*.quicksight-website
Amazon RDS	com.amazonaws.*region*.rds
Amazon RDS データ API	com.amazonaws.*region*.rds-data
Amazon RDS Performance Insights	com.amazonaws.*region*.pi
	com.amazonaws*region*..pi-fips
AWS re:Post Private	com.amazonaws*region*.repostspace
ごみ箱	com.amazonaws*region*.rbin
Amazon Redshift	com.amazonaws*region*.redshift
	com.amazonaws*region*..redshift-fips
	com.amazonaws*region*.redshift-serverless
	com.amazonaws*region*。redshift-serverless-fips
Amazon Redshift データ API	com.amazonaws*region*.redshift-data
	com.amazonaws*region*。redshift-data-fips
Amazon Rekognition	com.amazonaws*region*.rekognition
	com.amazonaws*region*..rekognition-fips
	com.amazonaws.*region*.streaming-rekognition
	com.amazonaws*region*。streaming-rekognition-fips
AWS Resource Access Manager	com.amazonaws.*region*.ram

AWS のサービス	サービス名
AWS Resource Groups	com.amazonaws*region*..resource-groups
	com.amazonaws*region*。resource-groups-fips
AWS RoboMaker	com.amazonaws*region*..robomaker
Amazon S3	com.amazonaws.*region*.s3
	com.amazonaws.*region*.s3tables
Amazon S3 マルチリージョンアクセスポイント	com.amazonaws.s3-global.accesspoint
Amazon S3 on Outposts	com.amazonaws.*region*.s3-outposts
Amazon SageMaker AI	aws.sagemaker.*region*.experiments
	aws.sagemaker.*region*.notebook
	aws.sagemaker*region*..partner-app
	aws.sagemaker*region*..studio
	com.amazonaws*region*。sagemaker-data-science-assistant
	com.amazonaws*region*.sagemaker.api
	com.amazonaws*region*.sagemaker.api-fips
	com.amazonaws.*region*.sagemaker.featurestore-runtime
	com.amazonaws*region*.sagemaker.metrics
	com.amazonaws*region*.sagemaker.runtime
	com.amazonaws*region*.sagemaker.runtime-fips

AWS のサービス	サービス名
Savings Plans	com.amazonaws.*region*.savingsplans
AWS Secrets Manager	com.amazonaws*region*..secretsmanager
AWS Security Hub	com.amazonaws*region*.securityhub
AWS Security Token Service	com.amazonaws*region*.sts
AWS Serverless Application Repository	com.amazonaws.*region*.serverlessrepo
Service Catalog	com.amazonaws.*region*.servicecatalog
	com.amazonaws.*region*.servicecatalog-appregistry
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 Supply Chain	com.amazonaws.*region*.scn
AWS Systems Manager	com.amazonaws.*region*.ec2messages
	com.amazonaws*region*..ssm

AWS のサービス	サービス名
	com.amazonaws*region*.ssm-contacts
	com.amazonaws*region*..ssm-incidents
	com.amazonaws*region*.ssm-quicksetup
	com.amazonaws*region*.ssmmessages
AWS 通信ネットワークビルダー	com.amazonaws*region*..tnb
Amazon Textract	com.amazonaws*region*.textract
	com.amazonaws*region*..textract-fips
Amazon Timestream	com.amazonaws*region*..timestream.ingest-*cell*
	com.amazonaws*region*.timestream.query-*cell*
Amazon Timestream for InfluxDB	com.amazonaws*region*.timestream-infuxdb
	com.amazonaws*region*。timestream-influxdb-fips
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

AWS のサービス	サービス名
Amazon VPC Lattice	com.amazonaws*region*..vpc-lattice
AWS Well-Architected Tool	com.amazonaws*region*.wellarchitected
Amazon WorkMail	com.amazonaws*region*.workmail
Amazon WorkSpaces	com.amazonaws*region*..workspaces
Amazon Workspaces セキュアブラウザ	com.amazonaws*region*..workspaces-web
	com.amazonaws*region*。workspaces-web-fips
Amazon WorkSpaces シンクライアント	com.amazonaws*region*.thinclient.api
AWS X-Ray	com.amazonaws*region*..xray

使用可能な AWS のサービス の名前を表示する

describe-vpc-endpoint-services コマンドを使用して、VPCエンドポイントをサポートするサービス名を表示できます。

次の例では、指定したリージョンでインターフェイスエンドポイント AWS のサービス をサポートする を表示します。--query オプションは、出力をサービス名に制限します

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

出力例を次に示します。

```
[
    "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",
    ...
]
```

サービスに関する情報を表示する

サービス名を取得したら、 describe-vpc-endpoint-services コマンドを使用して各エンドポイントサービスに関する詳細情報を表示できます。

次の例では、指定したリージョンの Amazon CloudWatch インターフェイスエンドポイントに関する情報を表示します。

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

出力例を次に示します。VpcEndpointPolicySupported は、エンドポイントポリシーがサポートされているかどうかを示し、SupportedIpAddressTypes は、どの IP アドレスタイプがサポートされているかを示します。

```
{
    "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"
    ]
}
```

エンドポイントポリシーのサポートを表示する

サービスがエンドポイントポリシーをサポートしているかどうかを確認するには、 describe-vpc-endpoint-services コマンドを呼び出して の値を確認しますVpcEndpointPolicySupported。指定できる値は true および false です。

次の例では、指定したサービスが指定したリージョン内のエンドポイントポリシーをサポートしているかどうかをチェックします。--query オプションは、出力を VpcEndpointPolicySupported の値に制限します。

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

以下は出力例です。

```
True
```

次の例では、指定されたリージョンでエンドポイントポリシー AWS のサービス をサポートする を一覧表示します。--query オプションは、出力をサービス名に制限します Windows コマンドプロンプトを使用してこのコマンドを実行するには、クエリ文字列を囲む一重引用符を削除し、行継続文字を \ から ^ に変更します。

```
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'
```

以下は出力例です。

```
[
    "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",
    ...
]
```

次の例では AWS のサービス 、指定したリージョンでエンドポイントポリシーをサポートしていない を一覧表示します。--query オプションは、出力をサービス名に制限します Windows コマンドプロンプトを使用してこのコマンドを実行するには、クエリ文字列を囲む一重引用符を削除し、行継続文字を \ から ^ に変更します。

```
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'
```

以下は出力例です。

```
[
    "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-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.deviceadvisor.iot",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.email-smtp",
    "com.amazonaws.us-east-1.glue.dashboard",
    "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.neptune-graph-fips",
    "com.amazonaws.us-east-1.outposts",
    "com.amazonaws.us-east-1.pipes-data",
    "com.amazonaws.us-east-1.q",
    "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"
]
```

IPv6 サポートを表示する

次のdescribe-vpc-endpoint-servicesコマンドを使用して、指定したリージョンIPv6で AWS のサービス アクセスできる を表示できます。--query オプションは、出力をサービス名に制限します

```
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
```

出力例を次に示します。

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.api.us-east-1.qbusiness",
    "com.amazonaws.us-east-1.account",
    "com.amazonaws.us-east-1.applicationinsights",
    "com.amazonaws.us-east-1.apprunner",
    "com.amazonaws.us-east-1.aps",
    "com.amazonaws.us-east-1.aps-workspaces",
    "com.amazonaws.us-east-1.arsenal-discovery",
    "com.amazonaws.us-east-1.athena",
    "com.amazonaws.us-east-1.backup",
    "com.amazonaws.us-east-1.braket",
    "com.amazonaws.us-east-1.cloudcontrolapi",
    "com.amazonaws.us-east-1.cloudcontrolapi-fips",
    "com.amazonaws.us-east-1.cloudhsmv2",
    "com.amazonaws.us-east-1.compute-optimizer",
    "com.amazonaws.us-east-1.codeartifact.api",
    "com.amazonaws.us-east-1.codeartifact.repositories",
    "com.amazonaws.us-east-1.cost-optimization-hub",
    "com.amazonaws.us-east-1.data-servicediscovery",
    "com.amazonaws.us-east-1.data-servicediscovery-fips",
    "com.amazonaws.us-east-1.datasync",
    "com.amazonaws.us-east-1.discovery",
    "com.amazonaws.us-east-1.drs",
    "com.amazonaws.us-east-1.ebs",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.eks-auth",
    "com.amazonaws.us-east-1.elasticbeanstalk",
    "com.amazonaws.us-east-1.elasticbeanstalk-health",
    "com.amazonaws.us-east-1.execute-api",
    "com.amazonaws.us-east-1.glue",
    "com.amazonaws.us-east-1.grafana",
    "com.amazonaws.us-east-1.groundstation",
    "com.amazonaws.us-east-1.internetmonitor".
    "com.amazonaws.us-east-1.internetmonitor-fips".
    "com.amazonaws.us-east-1.iotfleetwise",
    "com.amazonaws.us-east-1.kinesis-firehose",
    "com.amazonaws.us-east-1.lakeformation",
    "com.amazonaws.us-east-1.m2".
```

```
    "com.amazonaws.us-east-1.macie2".
    "com.amazonaws.us-east-1.networkflowmonitor".
    "com.amazonaws.us-east-1.networkflowmonitorreports".
    "com.amazonaws.us-east-1.pca-connector-scep",
    "com.amazonaws.us-east-1.pcs",
    "com.amazonaws.us-east-1.pcs-fips",
    "com.amazonaws.us-east-1.pi",
    "com.amazonaws.us-east-1.pi-fips",
    "com.amazonaws.us-east-1.polly",
    "com.amazonaws.us-east-1.quicksight-website",
    "com.amazonaws.us-east-1.rbin",
    "com.amazonaws.us-east-1.s3-outposts",
    "com.amazonaws.us-east-1.sagemaker.api",
    "com.amazonaws.us-east-1.securityhub",
    "com.amazonaws.us-east-1.servicediscovery",
    "com.amazonaws.us-east-1.servicediscovery-fips",
    "com.amazonaws.us-east-1.synthetics".
    "com.amazonaws.us-east-1.synthetics-fips".
    "com.amazonaws.us-east-1.textract",
    "com.amazonaws.us-east-1.textract-fips",
    "com.amazonaws.us-east-1.timestream-influxdb",
    "com.amazonaws.us-east-1.timestream-influxdb-fips",
    "com.amazonaws.us-east-1.trustedadvisor",
    "com.amazonaws.us-east-1.workmail",
    "com.amazonaws.us-east-1.xray"
]
```

インターフェイスVPCエンドポイント AWS のサービス を使用して にアクセスする

インターフェイスVPCエンドポイントを作成して AWS PrivateLink、多くの を含む のサービスに接続できます AWS のサービス。概要については、the section called “概念” および アクセス AWS のサービス を参照してください。

から指定したサブネットごとにVPC、サブネットにエンドポイントネットワークインターフェイスを作成し、サブネットアドレス範囲からプライベート IP アドレスを割り当てます。エンドポイントのネットワークインターフェイスは、リクエスタマネージドネットワークインターフェイスです。AWS アカウントで表示できますが、自ら管理することはできません。

時間単位の使用料金とデータ処理料金が課金されます。詳細については、「インターフェイスエンドポイントの料金」を参照してください。

内容

前提条件

- で にアクセスするリソースをデプロイ AWS のサービス しますVPC。
- プライベート を使用するにはDNS、 のDNSホスト名とDNS解決を有効にする必要がありますVPC。詳細については、「Amazon VPCユーザーガイド」のDNS「属性の表示と更新」を参照してください。
- インターフェイスエンドポイントIPv6で を有効にするには、 が 経由のアクセスをサポート AWS のサービス している必要がありますIPv6。詳細については、「the section called “IP アドレスのタイプ”」を参照してください。
- エンドポイントネットワークインターフェイスのセキュリティグループを作成し、 のリソースからの予想されるトラフィックを許可しますVPC。たとえば、 が にHTTPSリクエストを送信 AWS CLI できるようにするには AWS のサービス、セキュリティグループがインバウンドHTTPSトラフィックを許可する必要があります。
- リソースがネットワーク を持つサブネットにある場合はACL、ネットワークが のリソースVPCとエンドポイントネットワークインターフェイス間のトラフィックACLを許可していることを確認します。
- AWS PrivateLink リソースにはクォータがあります。詳細については、「AWS PrivateLink クォータ」を参照してください。

VPC エンドポイントを作成する

に接続するインターフェイスVPCエンドポイントを作成するには、次の手順に従います AWS のサービス。

のインターフェイスエンドポイントを作成するには AWS のサービス

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。

3. [エンドポイントの作成] を選択します。
4. タイプ で、 AWS サービスを選択します。
5. [Service name] (サービス名) で、サービスを選択します。詳細については、「the section called “統合するサービス”」を参照してください。
6. にはVPC、 にアクセスする VPC を選択します AWS のサービス。
7. ステップ 5 で Amazon S3 のサービス名を選択し、プライベートDNSサポートを設定する場合は、「追加設定」、DNS「名前を有効にする」を選択します。この選択を行うと、インバウンドエンドポイントDNSに対してのみプライベートを有効にするも自動的に選択されます。Amazon S3 のインターフェイスエンドポイントに対してのみ、インバウンド Resolver エンドポイントDNSでプライベートを設定できます。Amazon S3 のゲートウェイエンドポイントがなく、インバウンドエンドポイントDNSに対してのみプライベートを有効にするを選択した場合、この手順の最後のステップを試みるとエラーが表示されます。

   ステップ 5 で、Amazon S3 以外のサービスのサービス名を選択した場合、追加設定、Enable DNS name がすでに選択されています。デフォルトを維持することをお勧めします。これにより、 を介して行われたリクエストなど、パブリックサービスエンドポイントを使用するリクエストが AWS SDKエンドポイントに解決されますVPC。
8. サブネット で、エンドポイントネットワークインターフェイスを作成するサブネットを選択します。アベイラビリティーゾーンごとに 1 つのサブネットを選択できます。同じアベイラビリティーゾーンから複数のサブネットを選択することはできません。詳細については、「the section called “サブネットとアベイラビリティーゾーン”」を参照してください。

   デフォルトでは、サブネットの IP アドレス範囲から IP アドレスを選択し、エンドポイントのネットワークインターフェースに割り当てます。IP アドレスを自分で選択するには、IP アドレスを指定するを選択します。サブネットCIDRブロックの最初の 4 つの IP アドレスと最後の IP アドレスは内部使用のために予約されているため、エンドポイントネットワークインターフェイスに指定することはできません。
9. [IP address type] (IP アドレスのタイプ) で、次のオプションから選択します。

   - IPv4 – エンドポイントネットワークインターフェイスにIPv4アドレスを割り当てます。このオプションは、選択したすべてのサブネットにIPv4アドレス範囲があり、サービスがIPv4リクエストを受け入れる場合にのみサポートされます。
   - IPv6 – エンドポイントネットワークインターフェイスにIPv6アドレスを割り当てます。このオプションは、選択したすべてのサブネットがサブネットIPv6のみで、サービスがIPv6リクエストを受け入れる場合にのみサポートされます。

- デュアルスタック — エンドポイントネットワークインターフェイスに IPv4と IPv6 アドレスの両方を割り当てます。このオプションは、選択したすべてのサブネットに IPv4と の両方のIPv6アドレス範囲があり、サービスが IPv4と の両方のIPv6リクエストを受け入れる場合にのみサポートされます。

10. [Security groups] (セキュリティグループ) で、エンドポイントネットワークインターフェイスに関連付けるセキュリティグループを選択します。デフォルトでは、 のデフォルトのセキュリティグループを関連付けますVPC。
11. ポリシーで、インターフェイスエンドポイントを介したすべてのリソースに対するすべてのプリンシパルによるすべてのオペレーションを許可するには、フルアクセスを選択します。アクセスを制限するには、カスタム を選択し、ポリシーを入力します。このオプションは、サービスがVPCエンドポイントポリシーをサポートしている場合にのみ使用できます。詳細については、「エンドポイントポリシー」を参照してください。
12. (オプション) タグを追加するには、[新しいタグを追加] を選択し、そのタグのキーと値を入力します。
13. [エンドポイントの作成] を選択します。

コマンドラインを使用してインターフェイスエンドポイントを作成するには

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint (Windows 用のツール PowerShell)

共有サブネット

自分と共有されているサブネットのVPCエンドポイントを作成、説明、変更、または削除することはできません。ただし、共有されているサブネットでVPCエンドポイントを使用できます。

ICMP

インターフェイスエンドポイントは ping リクエストに応答しません。代わりに、nc または nmap コマンドを使用できます。

インターフェイスエンドポイントを設定する

インターフェイスVPCエンドポイントを作成したら、その設定を更新できます。

タスク

- サブネットの追加または削除
- セキュリティグループを関連付ける
- VPC エンドポイントポリシーを編集する
- プライベートDNS名を有効にする
- タグの管理

サブネットの追加または削除

インターフェイスエンドポイントのアベイラビリティゾーンごとに 1 つのサブネットを選択できます。サブネットを追加すると、サブネットにエンドポイントのネットワークインターフェイスが作成され、サブネットの IP アドレス範囲からプライベート IP アドレスが割り当てられます。サブネットを削除すると、そのエンドポイントのネットワークインターフェイスも削除されます。詳細については、「the section called “サブネットとアベイラビリティーゾーン”」を参照してください。

コンソールを使用してサブネットを変更するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. インターフェイスエンドポイントを選択します。
4. [Actions] (アクション)、[Manage subnets] (サブネットを管理) の順に選択します。
5. 必要に応じてアベイラビリティーゾーンを選択または選択解除します。アベイラビリティーゾーンごとに、サブネットを 1 つ選択します。デフォルトでは、サブネットの IP アドレス範囲から IP アドレスを選択し、エンドポイントのネットワークインターフェースに割り当てます。エンドポイントネットワークインターフェイスの IP アドレスを選択するには、IP アドレスの指定を選択し、サブネットIPv4アドレス範囲からアドレスを入力します。エンドポイントサービスがをサポートしている場合はIPv6、サブネットIPv6アドレス範囲からアドレスを入力することもできます。

   このエンドポイントのエンドポイントネットワークインターフェイスがすでにあるサブネットの IP アドレスを指定するとVPC、エンドポイントネットワークインターフェイスは新しいものに置き換えられます。このプロセスでは、サブネットとVPCエンドポイントが一時的に切断されます。
6. [Modify subnets] (サブネットを変更) を選択します。

コマンドラインを使用してサブネットを変更するには

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint (Windows 用のツール PowerShell)

セキュリティグループを関連付ける

インターフェイスエンドポイント用にネットワークインターフェイスに関連付けられているセキュリティグループを変更できます。セキュリティグループルールは、 のリソースからエンドポイントネットワークインターフェイスに許可されるトラフィックを制御しますVPC。

コンソールを使用してセキュリティグループを変更するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. インターフェイスエンドポイントを選択します。
4. [Actions]、[Manage security groups] の順に選択します。
5. 必要に応じて、セキュリティグループを選択または選択解除します。
6. [Modify security groups] (セキュリティグループを変更) を選択します。

コマンドラインを使用してセキュリティグループを変更するには

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint (Windows 用のツール PowerShell)

VPC エンドポイントポリシーを編集する

がエンドポイントポリシー AWS のサービス をサポートしている場合は、エンドポイントのエンドポイントポリシーを編集できます。エンドポイントポリシーを更新した後、変更が有効になるまでに数分かかる場合があります。詳細については、「エンドポイントポリシー」を参照してください。

コンソールを使用してエンドポイントポリシーを変更するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. インターフェイスエンドポイントを選択します。

4. [Actions] (アクション)、[Manage policy] (ポリシーを管理) の順に選択します。
5. [Full Access] (フルアクセス) を選択してサービスへのフルアクセスを許可するか、[Custom] (カスタム) を選択してカスタムポリシーをアタッチします。
6. [Save] を選択します。

コマンドラインを使用してエンドポイントポリシーを変更するには

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint (Windows 用のツール PowerShell)

プライベートDNS名を有効にする

VPC エンドポイントのプライベートDNS名を有効にすることをお勧めします AWS のサービス。これにより、 を介して行われたリクエストなど、パブリックサービスエンドポイントを使用するリクエストが AWS SDKエンドポイントに解決されますVPC。

プライベートDNS名を使用するには、 のDNSホスト名とDNS解決の両方を有効にする必要がありますVPC。プライベートDNS名を有効にした後、プライベート IP アドレスが使用可能になるまでに数分かかる場合があります。プライベートDNS名を有効にしたときに作成するDNSレコードはプライベートです。したがって、プライベートDNS名はパブリックに解決できません。

コンソールを使用してプライベートDNS名オプションを変更するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. インターフェイスエンドポイントを選択します。
4. アクション、プライベートDNS名の変更を選択します。
5. 必要に応じて、[Enable for this endpoint] (このエンドポイントを有効にする) を選択または選択解除します。
6. サービスが Amazon S3 の場合、前のステップでこのエンドポイントに対して有効にするを選択すると、インバウンドエンドポイントDNSに対してのみプライベートを有効にするも選択されます。標準のプライベートDNS機能を使用する場合は、インバウンドエンドポイントに対してDNSのみプライベートを有効にする を選択します。Amazon S3 のインターフェイスエンドポイントに加えて Amazon S3 のゲートウェイエンドポイントがなく、インバウンドエンドポイントDNSに対してのみプライベートを有効にするを選択した場合、次のステップで変更を保存する

とエラーが表示されます。詳細については、「the section called “プライベート DNS”」を参照してください。

7. [Save changes] (変更の保存) をクリックします。

コマンドラインを使用してプライベートDNS名オプションを変更するには

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint (Windows 用のツール PowerShell)

タグの管理

インターフェイスエンドポイントにタグを付けて、識別しやすくしたり、組織のニーズに応じて分類したりできます。

コンソールを使用してタグを管理するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. インターフェイスエンドポイントを選択します。
4. [Actions] (アクション)、[Manage tags] (タグの管理) を選択します。
5. 追加するタグごとに、[Add new tag] (新しいタグを追加) を選択し、タグキーとタグ値を入力します。
6. タグを削除するには、タグのキーと値の右側にある [Remove] (削除) を選択します。
7. [Save] を選択します。

コマンドラインを使用してタグを管理するには

- create-tags および delete-tags (AWS CLI)
- New-EC2Tag および Remove-EC2Tag (Tools for Windows PowerShell)

インターフェイスエンドポイントイベントのアラートを受け取る

通知を作成して、インターフェイスエンドポイントに関連する特定のイベントに関するアラートを受信できます。例えば、接続リクエストが承諾または拒否されたときに E メールを受信できます。

タスク

- SNS 通知を作成する
- アクセスポリシーを追加する
- キーポリシーを追加

SNS 通知を作成する

通知用の Amazon SNSトピックを作成し、トピックにサブスクライブするには、次の手順に従います。

コンソールを使用してインターフェイスエンドポイントの通知を作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. インターフェイスエンドポイントを選択します。
4. [Notifications] (通知) タブで、[Create notification] (通知の作成) を選択します。
5. 通知 ARNで、作成したSNSトピックARNの を選択します。
6. イベントをサブスクライブするには、[Events] (イベント) から選択します。
   - [Connect] (接続) – サービスコンシューマーがインターフェイスエンドポイントを作成しました。これは、接続リクエストをサービスプロバイダーに送信します。
   - [Accept] (承諾) – サービスプロバイダーが接続リクエストを受け入れました。
   - [Reject] (拒否) – サービスプロバイダーが接続リクエストを拒否しました。
   - [Delete] (削除) — サービスコンシューマーがインターフェイスエンドポイントを削除しました。
7. [通知を作成] を選択します。

コマンドラインを使用してインターフェイスエンドポイントの通知を作成するには

- create-vpc-endpoint-connection通知 (AWS CLI)
- New-EC2VpcEndpointConnectionNotification (Windows 用のツール PowerShell)

アクセスポリシーを追加する

Amazon SNSトピックにアクセスポリシーを追加して、 がユーザーに代わって通知を発行 AWS PrivateLink できるようにします。次に例を示します。詳細については、「Amazon SNSトピックのアクセスポリシーを編集するにはどうすればよいですか？」を参照してください。aws:SourceArn および aws:SourceAccount グローバル条件キーを使用して、混乱した代理問題に対して保護します。

```
{
  "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"
        }
      }
    }
  ]
}
```

キーポリシーを追加

暗号化されたSNSトピックを使用している場合、 オペレーションを呼び出す AWS KMS APIには、KMSキーのリソースポリシーが AWS PrivateLink を信頼する必要があります。以下は、キーポリシーの例です。

```
{
  "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"
        }
      }
    }
  ]
}
```

インターフェースエンドポイントを削除する

VPC エンドポイントの使用が終了したら、削除できます。インターフェイスエンドポイントを削除すると、そのエンドポイントのネットワークインターフェイスも削除されます。

コンソールを使用してインターフェイスエンドポイントを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. インターフェイスエンドポイントを選択します。
4. アクション、VPCエンドポイントの削除を選択します。
5. 確認を求められたら、**delete** をクリックします。
6. [削除] を選択します。

コマンドラインを使用してインターフェイスエンドポイントを削除するには

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint (Windows 用のツール PowerShell)

ゲートウェイエンドポイント

ゲートウェイVPCエンドポイントは、 にインターネットゲートウェイやNATデバイスを必要とすることなく、Amazon S3 および DynamoDB への信頼性の高い接続を提供しますVPC。ゲートウェイエンドポイントは、他のタイプのVPCエンドポイントとは異なり AWS PrivateLink、 を使用しません。

Amazon S3 と DynamoDB は、ゲートウェイエンドポイントとインターフェイスエンドポイントの両方をサポートしています。オプションの比較については、以下を参照してください。

- Amazon S3 のVPCエンドポイントのタイプ
- Amazon DynamoDB のVPCエンドポイントのタイプ

料金

ゲートウェイエンドポイントは追加料金なしで使用できます。

内容

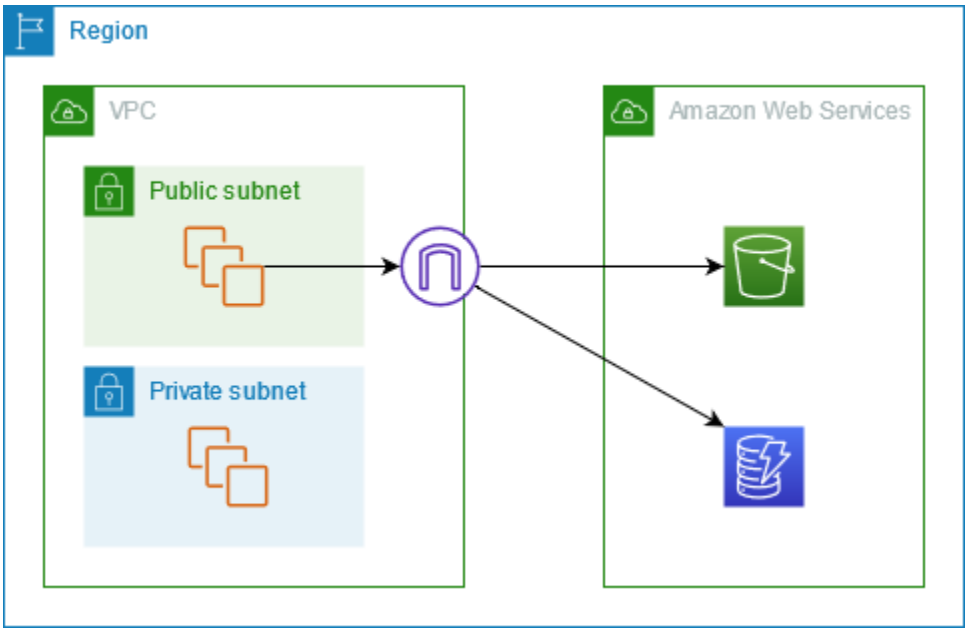
概要

Amazon S3 と DynamoDB には、パブリックサービスエンドポイントまたはゲートウェイエンドポイントを通じてアクセスできます。この概要では、これらの方法を比較します。

インターネットゲートウェイ経由でアクセスする

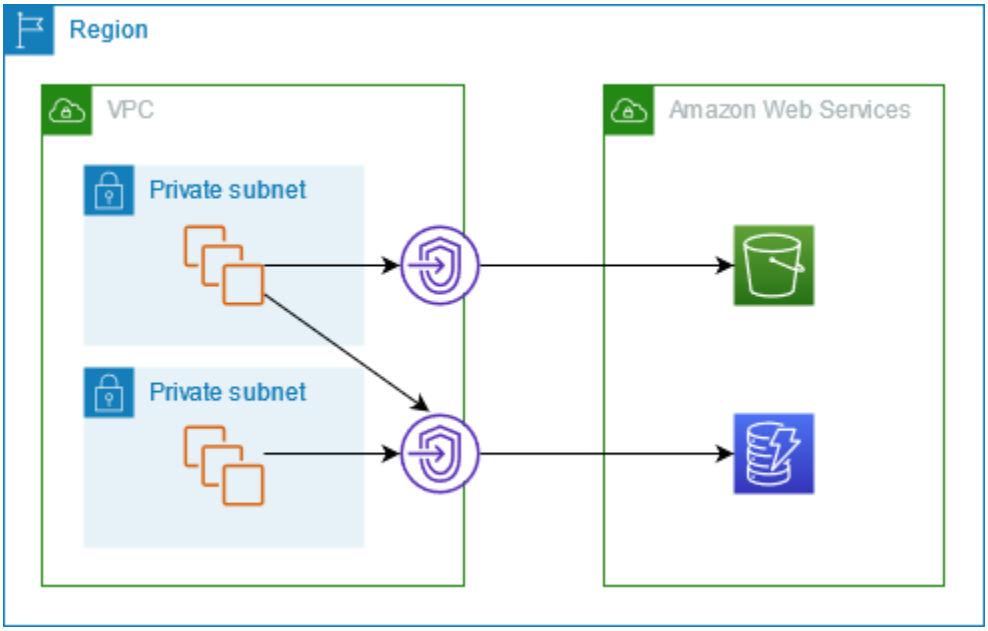
次の図は、インスタンスがパブリックサービスエンドポイントを通じて Amazon S3 および DynamoDB にアクセスする方法を示しています。パブリックサブネットのインスタンスから Amazon S3 または DynamoDB へのトラフィックは、 のインターネットゲートウェイにルーティングVPCされ、その後 サービスにルーティングされます。定義上、プライベートサブネットにはインターネットゲートウェイへのルートがないため、プライベートサブネットのインスタンスは Amazon

S3 や DynamoDB にトラフィックを送信できません。プライベートサブネット内のインスタンスが Amazon S3 または DynamoDB にトラフィックを送信できるようにするには、NATデバイスをパブリックサブネットに追加し、プライベートサブネット内のトラフィックをNATデバイスにルーティングします。Amazon S3 または DynamoDB へのトラフィックがインターネットゲートウェイを通過する間は、 AWS ネットワークを離れません。



ゲートウェイエンドポイント経由でアクセスする

次の図は、インスタンスがゲートウェイエンドポイントを通じて Amazon S3 および DynamoDB にアクセスする方法を示しています。から Amazon S3 または DynamoDB VPCへのトラフィックは、ゲートウェイエンドポイントにルーティングされます。各サブネットルートテーブルには、サービスのプレフィックスリストを使用して、サービス宛てのトラフィックをゲートウェイエンドポイントに送信するルートが必要です。詳細については、「Amazon VPCユーザーガイド」のAWS「 マネージドプレフィックスリスト」を参照してください。



ルーティング

ゲートウェイエンドポイントを作成するときは、有効にするサブネットのVPCルートテーブルを選択します。次のルートは、選択した各ルートテーブルに自動的に追加されます。送信先は が所有するサービスのプレフィックスリスト AWS であり、ターゲットはゲートウェイエンドポイントです。

デスティネーション	ターゲット
prefix_list_id	*gateway_endpoint_id*

考慮事項

- ルートテーブルに追加されたエンドポイントルートは確認できますが、変更または削除できません。エンドポイントルートをルートテーブルに追加するには、それをゲートウェイエンドポイントに関連付けます。ルートテーブルとゲートウェイエンドポイントの関連付けを解除するか、ゲートウェイエンドポイントを削除すると、エンドポイントルートが削除されます。
- ゲートウェイエンドポイントに関連付けられたルートテーブルに関連付けられたサブネットのすべてのインスタンスは、ゲートウェイエンドポイントを使用してサービスにアクセスします。これらのルートテーブルに関連付けられていないサブネット内のインスタンスは、ゲートウェイエンドポイントではなくパブリックサービスエンドポイントを使用します。
- ルートテーブルには、Amazon S3 へのエンドポイントルートと DynamoDB へのエンドポイントルートの両方を含めることができます。同じサービス (Amazon S3 または DynamoDB) へのエン

ドポイントルートを複数のルートテーブルに含めることができます。1 つのルートテーブルに同じサービス (Amazon S3 または DynamoDB) への複数のエンドポイントルートを持つことはできません。

- 当社は、トラフィックと一致する最も具体的なルートを使用して、トラフィックをルーティングする方法を決定します (最長プレフィックス一致)。エンドポイントルートのあるルートテーブルの場合、これは次のことを意味します。
  - すべてのインターネットトラフィック (0.0.0.0/0) をインターネットゲートウェイに送信するルートがある場合、現在のリージョンのサービス (Amazon S3 または DynamoDB) 宛てのトラフィックでエンドポイントルートが優先されます。別の 宛てのトラフィックは、インターネットゲートウェイ AWS のサービス を使用します。
  - プレフィックスリストはリージョンに固有であるため、別のリージョンのサービス (Amazon S3 または DynamoDB) 宛てのトラフィックはインターネットゲートウェイに送信されます。
  - 同じリージョンにサービス (Amazon S3 または DynamoDB) の正確な IP アドレス範囲を指定するルートがある場合は、そのルートがエンドポイントルートよりも優先されます。

セキュリティ

インスタンスがゲートウェイエンドポイントを介して Amazon S3 または DynamoDB にアクセスする場合、インスタンスはパブリックエンドポイントを使用してサービスにアクセスします。これらのインスタンスのセキュリティグループは、サービスとの間のトラフィックを許可する必要があります。以下は、アウトバウンドルールの例です。サービスのプレフィックスリストの ID を参照します。

デスティネーション	プロトコル	ポート範囲
prefix_list_id	TCP	443

これらのインスタンスACLsのサブネットのネットワークでは、 サービスとの間のトラフィックも許可する必要があります。以下は、アウトバウンドルールの例です。ネットワークACLルールでプレフィックスリストを参照することはできませんが、プレフィックスリストからサービスの IP アドレス範囲を取得できます。

デスティネーション	プロトコル	ポート範囲
service_cidr_block_1	TCP	443

デスティネーション	プロトコル	ポート範囲
service_cidr_block_2	TCP	443
service_cidr_block_3	TCP	443

Amazon S3 のゲートウェイエンドポイント

ゲートウェイVPCエンドポイントVPCを使用して、 から Amazon S3 にアクセスできます。ゲートウェイエンドポイントを作成したら、 から Amazon S3 VPCへのトラフィックのルートテーブルにターゲットとして追加できます。

ゲートウェイエンドポイントは追加料金なしで使用できます。

Amazon S3 は、ゲートウェイエンドポイントとインターフェイスエンドポイントの両方をサポートしています。ゲートウェイエンドポイントを使用すると、 にインターネットゲートウェイやNATデバイスを必要とせずにVPC、 から Amazon S3 にアクセスできVPC、追加料金はかかりません。ただし、ゲートウェイエンドポイントは、オンプレミスネットワーク、他の AWS リージョンVPCsのピアリング接続、またはトランジットゲートウェイ経由のアクセスを許可しません。このようなシナリオでは、追加料金で利用できるインターフェイスエンドポイントを使用する必要があります。詳細については、Amazon S3ユーザーガイド」の「Amazon S3 のVPCエンドポイントのタイプ」を参照してください。 Amazon S3

内容

考慮事項

- ゲートウェイエンドポイントは、それを作成したリージョンでのみ使用できます。必ず S3 バケットと同じリージョンにゲートウェイエンドポイントを作成してください。

- Amazon DNSサーバーを使用している場合は、 のDNSホスト名とDNS解像度の両方を有効にする必要がありますVPC。独自のDNSサーバーを使用している場合は、Amazon S3 へのリクエストがによって維持される IP アドレスに正しく解決されていることを確認します AWS。
- ゲートウェイエンドポイントを通じて Amazon S3 にアクセスするインスタンスのセキュリティグループのルールは、Amazon S3 との間のトラフィックを許可する必要があります。Amazon S3 のプレフィックスリスト ID は、セキュリティグループルールで参照できます。
- ゲートウェイエンドポイントを介して Amazon S3 にアクセスするインスタンスのサブネットACLのネットワークは、Amazon S3 との間のトラフィックを許可する必要があります。ネットワークACLルールでプレフィックスリストを参照することはできませんが、Amazon S3 のプレフィックスリストから Amazon S3 の IP アドレス範囲を取得できます。
- S3 バケットへのアクセス AWS のサービス を必要とする を使用しているかどうかを確認します。例えば、サービスがログファイルを含むバケットへのアクセスを要求したり、EC2インスタンスにドライバーやエージェントをダウンロードしたりする必要がある場合があります。その場合は、エンドポイントポリシーで、 AWS のサービス または リソースが `s3:GetObject`アクションを使用してこれらのバケットにアクセスすることを許可していることを確認します。
- VPC エンドポイントを通過する Amazon S3 へのリクエストには、ID ポリシーまたはバケットポリシーで `aws:SourceIp`条件を使用することはできません。代わりに `aws:VpcSourceIp` 条件を使用してください。または、ルートテーブルを使用して、VPCエンドポイントを介して Amazon S3 にアクセスできるEC2インスタンスを制御することもできます。
- ゲートウェイエンドポイントはIPv4トラフィックのみをサポートします。
- Amazon S3 が受信した影響を受けるサブネット内のインスタンスからのソースIPv4アドレスは、パブリックIPv4アドレスから のプライベートIPv4アドレスに変更されますVPC。エンドポイントはネットワークルートを切り替え、開いているTCP接続を切断します。パブリックIPv4アドレスを使用した以前の接続は再開されません。エンドポイントの作成または変更は、重要なタスクが実行中でないときに行うことをお勧めします。または、接続の障害後に、ソフトウェアが Amazon S3 に自動的に再接続できることをテストするようお勧めします。
- エンドポイント接続を から拡張することはできませんVPC。VPN 接続、VPCピアリング接続、トランジットゲートウェイ、または AWS Direct Connect 内の接続の反対側のリソースは、ゲートウェイエンドポイントを使用して Amazon S3 と通信VPCすることはできません。
- アカウントには、リージョンあたり 20 個のゲートウェイエンドポイントのデフォルトクォータがあり、調整可能です。また、 あたりのゲートウェイエンドポイントは 255 に制限されていますVPC。

プライベート DNS

Amazon S3 のゲートウェイエンドポイントとインターフェイスエンドポイントの両方を作成するときに、コストを最適化DNSするようにプライベートを設定できます。

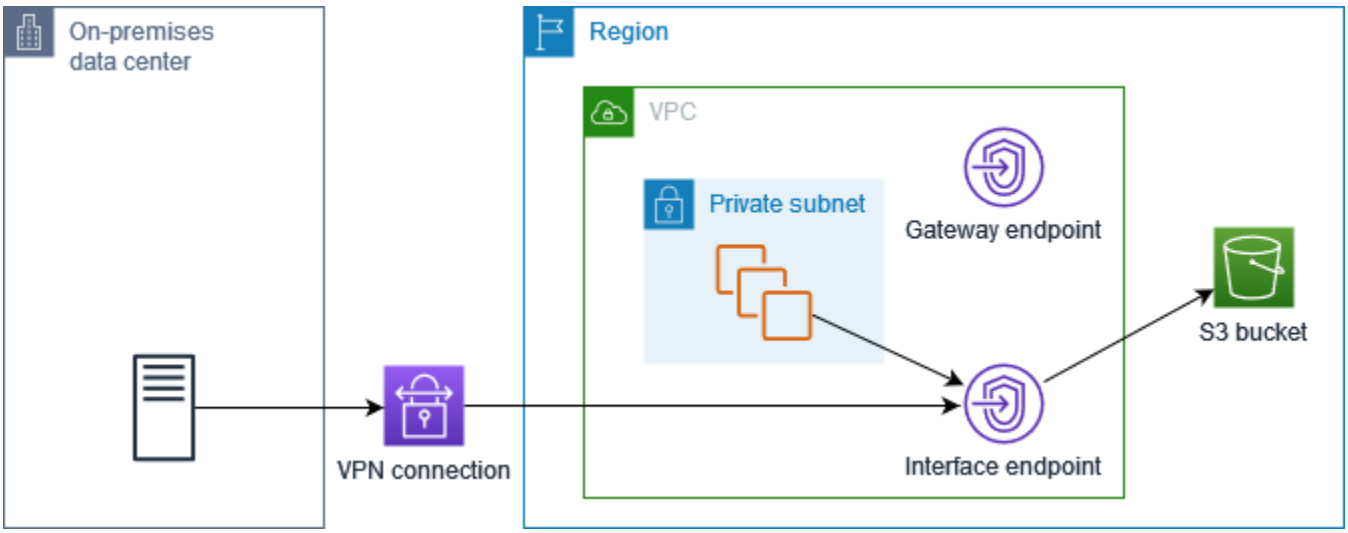
Route 53 Resolver

Amazon は、Route 53 Resolver と呼ばれるDNSサーバーを に提供しますVPC。Route 53 Resolver は、プライベートホストゾーンのローカルVPCドメイン名とレコードを自動的に解決します。ただし、 の外部から Route 53 Resolver を使用することはできませんVPC。Route 53 には、 の外部から Route 53 Resolver を使用できるように、Resolver エンドポイントと Resolver ルールが用意されていますVPC。インバウンド Resolver エンドポイントは、オンプレミスネットワークから Route 53 Resolver にDNSクエリを転送します。アウトバウンド Resolver エンドポイントは、Route 53 Resolver からオンプレミスネットワークにDNSクエリを転送します。

インバウンドリゾルバーエンドポイントDNSにのみプライベートを使用するように Amazon S3 のインターフェイスエンドポイントを設定すると、インバウンドリゾルバーエンドポイントが作成されます。インバウンド Resolver エンドポイントは、オンプレミスからインターフェイスエンドポイントのプライベート IP アドレスへのDNSクエリを Amazon S3 に解決します。また、Route 53 ResolverのALIASレコードを Amazon S3 のパブリックホストゾーンに追加します。これにより、 からのDNSクエリが Amazon S3 パブリック IP アドレスにVPC解決され、ゲートウェイエンドポイントにトラフィックがルーティングされます。

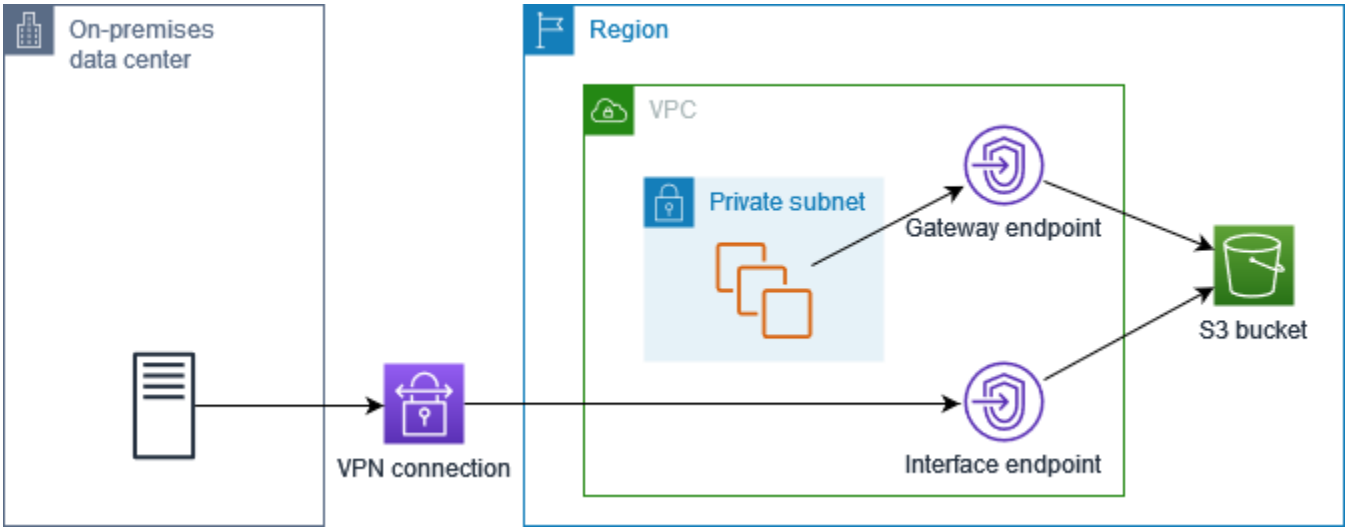
プライベート DNS

Amazon S3 DNSのインターフェイスエンドポイントにプライベートを設定しても、インバウンド Resolver エンドポイントDNSにのみプライベートを設定しない場合、オンプレミスネットワークとの両方からのリクエストは、インターフェイスエンドポイントVPCを使用して Amazon S3 にアクセスします。したがって、ゲートウェイエンドポイントを追加料金なしで使用せずにVPC、 からのトラフィックにインターフェイスエンドポイントを使用する料金が発生します。



インバウンドリゾルバーエンドポイントのプライベートDNSのみ

インバウンド Resolver エンドポイントに対してDNSのみプライベートを設定する場合、オンプレミスネットワークからのリクエストはインターフェイスエンドポイントを使用して Amazon S3 にアクセスし、 からのリクエストはゲートウェイエンドポイントVPCを使用して Amazon S3 にアクセスします。そのため、ゲートウェイエンドポイントを使用できないトラフィックにのみインターフェイスエンドポイントの使用料を支払うので、コストを最適化できます。



プライベートを設定する DNS

Amazon S3 DNSのインターフェイスエンドポイントのプライベートは、作成時または作成後に設定できます。詳細については、「the section called “VPC エンドポイントを作成する” (作成中に設定)」または「the section called “プライベートDNS名を有効にする” (作成後に設定)」を参照してください。

ゲートウェイエンドポイントを作成する

次の手順を使用して、Amazon S3 に接続するゲートウェイエンドポイントを作成します。

コンソールを使用してゲートウェイエンドポイントを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. [エンドポイントの作成] を選択します。
4. [Service category] (サービスカテゴリ) で、AWS のサービス を選択します。
5. サービスで、フィルタータイプ = ゲートウェイを追加し、com.amazonaws.*region*.s3 を選択します。
6. でVPC、エンドポイントVPCを作成する を選択します。
7. [Route tables] (ルートテーブル) で、エンドポイントで使用するルートテーブルを選択します。サービス宛てのトラフィックをエンドポイントのネットワークインターフェイスにポイントするルートが自動的に追加されます。
8. ポリシー では、フルアクセス を選択して、VPCエンドポイント上のすべてのリソースに対するすべてのプリンシパルによるすべてのオペレーションを許可します。それ以外の場合は、カスタム を選択して、プリンシパルがVPCエンドポイント経由でリソースに対してアクションを実行するためのアクセス許可を制御するVPCエンドポイントポリシーをアタッチします。
9. (オプション) タグを追加するには、[新しいタグを追加] を選択し、そのタグのキーと値を入力します。
10. [エンドポイントの作成] を選択します。

コマンドラインを使用してゲートウェイエンドポイントを作成するには

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint (Windows 用のツール PowerShell)

バケットポリシーを使用してアクセスを制御する

バケットポリシーを使用して、特定のエンドポイント、、VPCsIP アドレス範囲、および からバケットへのアクセスを制御できます AWS アカウント。これらの例では、ユースケースに必要なアクセスを許可するポリシーステートメントがあることを前提としています。

Example 例: 特定のエンドポイントへのアクセスを制限する

aws:sourceVpce 条件キーを使用して、特定のエンドポイントへのアクセスを制限するバケットポリシーを作成できます。次のポリシーは、指定されたゲートウェイエンドポイントが使用された場合を除き、指定されたアクションでの指定バケットへのアクセスを拒否します。このポリシーは、指定されたアクションでの AWS Management Consoleを介した指定バケットへのアクセスをブロックすることに注意してください。

```
{
  "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 例: 特定の へのアクセスを制限する VPC

aws:sourceVpc 条件キーVPCsを使用して、特定の へのアクセスを制限するバケットポリシーを作成できます。これは、同じ に複数のエンドポイントが設定されている場合に便利ですVPC。次のポリシーは、リクエストが指定された から送信されない限り、指定されたアクションを使用して指定されたバケットへのアクセスを拒否しますVPC。このポリシーは、指定されたアクションでの AWS Management Consoleを介した指定バケットへのアクセスをブロックすることに注意してください。

```
{
  "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 例: 特定の IP アドレス範囲へのアクセスを制限する

aws:VpcSourceIp 条件キーを使用して、特定の IP アドレス範囲へのアクセスを制限するポリシーを作成できます。次のポリシーは、リクエストが指定された IP アドレスからのものである場合を除き、指定されたアクションでの指定バケットへのアクセスを拒否します。このポリシーは、指定されたアクションでの AWS Management Consoleを介した指定バケットへのアクセスをブロックすることに注意してください。

```
{
  "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 例: 特定の のバケットへのアクセスを制限する AWS アカウント

`s3:ResourceAccount` 条件キーを使用して、特定の AWS アカウント の S3 バケットへのアクセスを制限するポリシーを作成できます。次のポリシーは、指定された AWS アカウントによって S3 バケットが所有されている場合を除き、指定されたアクションでの S3 バケットへのアクセスを拒否します。

```
{
  "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"
        }
      }
    }
  ]
}
```

ルートテーブルを関連付ける

ゲートウェイエンドポイントに関連付けられているルートテーブルを変更できます。ルートテーブルを関連付けると、サービス宛てのトラフィックをエンドポイントのネットワークインターフェイスにポイントするルートが自動的に追加されます。ルートテーブルの関連付けを解除すると、エンドポイントルートはルートテーブルから自動的に削除されます。

コンソールを使用してルートテーブルを関連付けるには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. ゲートウェイエンドポイントを選択する
4. [Actions]、[Manage route tables] の順に選択します。
5. 必要に応じて、ルートテーブルを選択または選択解除します。
6. [Modify route tables] (ルートテーブルを変更) を選択します。

コマンドラインを使用してルートテーブルを関連付けるには

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint (Tools for Windows PowerShell)

VPC エンドポイントポリシーを編集する

ゲートウェイエンドポイントのエンドポイントポリシーを編集して、エンドポイントVPC経由で から Amazon S3 へのアクセスを制御できます。デフォルトポリシーでは、フルアクセスを許可します。詳細については、「エンドポイントポリシー」を参照してください。

コンソールを使用してエンドポイントポリシーを変更するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. ゲートウェイエンドポイントを選択する
4. [Actions] (アクション)、[Manage policy] (ポリシーを管理) の順に選択します。
5. [Full Access] (フルアクセス) を選択してサービスへのフルアクセスを許可するか、[Custom] (カスタム) を選択してカスタムポリシーをアタッチします。
6. [Save] を選択します。

Amazon S3 にアクセスするためのエンドポイントのポリシーの例は次のとおりです。

Example 例: 特定のバケットへのアクセスを制限する

特定の S3 バケットへのアクセスを制限するポリシーを作成できます。これは、 AWS のサービス に S3 バケットVPCを使用する他の がある場合に便利です。

```
{
  "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 例: 特定のIAMロールへのアクセスを制限する

特定のIAMロールへのアクセスを制限するポリシーを作成できます。aws:PrincipalArn を使用してプリンシパルへのアクセスを許可する必要があります。

```
{
  "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 例: 特定のアカウントのユーザーへのアクセスを制限する

特定のアカウントへのアクセスを制限するポリシーを作成できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-callers-from-specific-account",
      "Effect": "Allow",
      "Principal": "*",
```

```
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      }
    }
  ]
}
```

ゲートウェイエンドポイントを削除する

不要になったゲートウェイエンドポイントは、削除することができます。ゲートウェイエンドポイントを削除すると、エンドポイントルートがサブネットルートテーブルから削除されます。

プライベートDNSが有効になっている場合、ゲートウェイエンドポイントを削除することはできません。

コンソールを使用してゲートウェイエンドポイントを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. ゲートウェイエンドポイントを選択する
4. アクション、VPCエンドポイントの削除を選択します。
5. 確認を求められたら、**delete** をクリックします。
6. [削除] を選択します。

コマンドラインを使用してゲートウェイエンドポイントを削除するには

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint (Windows 用のツール PowerShell)

Amazon DynamoDB のゲートウェイエンドポイント

ゲートウェイVPCエンドポイントVPCを使用して、 から Amazon DynamoDB にアクセスできます。ゲートウェイエンドポイントを作成したら、 から DynamoDB VPCへのトラフィックのルートテーブルにターゲットとして追加できます。

ゲートウェイエンドポイントは追加料金なしで使用できます。

DynamoDB は、ゲートウェイエンドポイントとインターフェイスエンドポイントの両方をサポートしています。ゲートウェイエンドポイントを使用すると、 にインターネットゲートウェイやNATデバイスを必要とせずにVPC、 から DynamoDB にアクセスできVPC、追加料金はかかりません。ただし、ゲートウェイエンドポイントは、オンプレミスネットワーク、他の AWS リージョンVPCsのピアリング接続、またはトランジットゲートウェイ経由のアクセスを許可しません。このようなシナリオでは、追加料金で利用できるインターフェイスエンドポイントを使用する必要があります。詳細については、「Amazon DynamoDB デベロッパーガイド」の「DynamoDB のVPCエンドポイントのタイプ」を参照してください。 DynamoDB

内容

- 考慮事項
- ゲートウェイエンドポイントを作成する
- IAM ポリシーを使用してアクセスを制御する
- ルートテーブルを関連付ける
- VPC エンドポイントポリシーを編集する
- ゲートウェイエンドポイントを削除する

考慮事項

- ゲートウェイエンドポイントは、それを作成したリージョンでのみ使用できます。必ず DynamoDB テーブルと同じリージョンにゲートウェイエンドポイントを作成してください。
- Amazon DNSサーバーを使用している場合は、 のDNSホスト名とDNS解像度の両方を有効にする必要がありますVPC。独自のDNSサーバーを使用している場合は、DynamoDB へのリクエストがによって維持される IP アドレスに正しく解決されていることを確認します AWS。
- ゲートウェイエンドポイントを通じて DynamoDB にアクセスするインスタンスのセキュリティグループのルールは、DynamoDB との間のトラフィックを許可する必要があります。DynamoDB のプレフィックスリスト ID は、セキュリティグループルールで参照できます。
- ゲートウェイエンドポイントを介して DynamoDB にアクセスするインスタンスのサブネットACLのネットワークは、DynamoDB との間のトラフィックを許可する必要があります。ネットワークACLルールでプレフィックスリストを参照することはできませんが、DynamoDB の IP アドレス範囲は DynamoDB のプレフィックスリストから取得できます。

- AWS CloudTrail を使用して DynamoDB オペレーションをログに記録する場合、ログファイルには、サービスコンシューマー内のEC2インスタンスのプライベート IP アドレスVPCと、エンドポイントを介して実行されるリクエストのゲートウェイエンドポイントの ID が含まれます。
- ゲートウェイエンドポイントはIPv4トラフィックのみをサポートします。
- 影響を受けるサブネット内のインスタンスの送信元IPv4アドレスは、 からパブリックIPv4アドレスからプライベートIPv4アドレスに変更されますVPC。エンドポイントはネットワークルートを切り替え、開いているTCP接続を切断します。パブリックIPv4アドレスを使用した以前の接続は再開されません。ゲートウェイエンドポイントの作成または変更は、重要なタスクが実行中でないときに行うことをお勧めします。または、接続が切断された場合にソフトウェアが DynamoDB に自動的に再接続できることを確認するためにテストしてください。
- エンドポイント接続を から拡張することはできませんVPC。VPN 接続、VPCピアリング接続、トランジットゲートウェイ、または AWS Direct Connect 内の接続の反対側のリソースは、ゲートウェイエンドポイントを使用して DynamoDB と通信VPCすることはできません。
- アカウントには、リージョンあたり 20 個のゲートウェイエンドポイントのデフォルトクォータがあり、調整可能です。また、 あたりのゲートウェイエンドポイントは 255 に制限されていますVPC。

ゲートウェイエンドポイントを作成する

次の手順を使用して、DynamoDB に接続するゲートウェイエンドポイントを作成します。

コンソールを使用してゲートウェイエンドポイントを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. [エンドポイントの作成] を選択します。
4. [Service category] (サービスカテゴリ) で、AWS のサービス を選択します。
5. サービスで、フィルタータイプ = ゲートウェイを追加し、com.amazonaws.*region*.dynamodb を選択します。
6. でVPC、エンドポイントVPCを作成する を選択します。
7. [Route tables] (ルートテーブル) で、エンドポイントで使用するルートテーブルを選択します。サービス宛てのトラフィックをエンドポイントのネットワークインターフェイスにポイントするルートが自動的に追加されます。
8. ポリシー では、フルアクセス を選択して、VPCエンドポイント上のすべてのリソースに対するすべてのプリンシパルによるすべてのオペレーションを許可します。それ以外の場合は、カスタ

ム を選択して、プリンシパルがVPCエンドポイント経由でリソースに対してアクションを実行するためのアクセス許可を制御するVPCエンドポイントポリシーをアタッチします。

9. (オプション) タグを追加するには、[新しいタグを追加] を選択し、そのタグのキーと値を入力します。
10. [エンドポイントの作成] を選択します。

コマンドラインを使用してゲートウェイエンドポイントを作成するには

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint (Windows 用のツール PowerShell)

IAM ポリシーを使用してアクセスを制御する

IAM ポリシーを作成して、特定のVPCエンドポイントを使用して DynamoDB テーブルにアクセスできるIAMプリンシパルを制御できます。

Example 例: 特定のエンドポイントへのアクセスを制限する

aws:sourceVpce 条件キーを使用して、特定のVPCエンドポイントへのアクセスを制限するポリシーを作成できます。次のポリシーは、指定されたVPCエンドポイントが使用されていない限り、アカウントの DynamoDB テーブルへのアクセスを拒否します。この例では、ユースケースに必要なアクセスを許可するポリシーステートメントがあることを前提としています。

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

```
}
```

Example 例: 特定のIAMロールからのアクセスを許可する

特定のIAMロールを使用してアクセスを許可するポリシーを作成できます。次のポリシーは、指定されたIAMロールへのアクセスを許可します。

```
{
   "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 例: 特定のアカウントからのアクセスを許可する

特定のアカウントからのアクセスのみを許可するポリシーを作成できます。次のポリシーでは、指定されたアカウントのユーザーに対するアクセス権を付与します。

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

```
            }
         }
      }
   ]
}
```

ルートテーブルを関連付ける

ゲートウェイエンドポイントに関連付けられているルートテーブルを変更できます。ルートテーブルを関連付けると、サービス宛てのトラフィックをエンドポイントのネットワークインターフェイスにポイントするルートが自動的に追加されます。ルートテーブルの関連付けを解除すると、エンドポイントルートはルートテーブルから自動的に削除されます。

コンソールを使用してルートテーブルを関連付けるには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. ゲートウェイエンドポイントを選択する
4. [Actions]、[Manage route tables] の順に選択します。
5. 必要に応じて、ルートテーブルを選択または選択解除します。
6. [Modify route tables] (ルートテーブルを変更) を選択します。

コマンドラインを使用してルートテーブルを関連付けるには

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint (Windows 用のツール PowerShell)

VPC エンドポイントポリシーを編集する

ゲートウェイエンドポイントのエンドポイントポリシーを編集して、エンドポイントVPC経由で から DynamoDB へのアクセスを制御できます。デフォルトポリシーでは、フルアクセスを許可します。詳細については、「エンドポイントポリシー」を参照してください。

コンソールを使用してエンドポイントポリシーを変更するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。

3. ゲートウェイエンドポイントを選択する
4. [Actions] (アクション)、[Manage policy] (ポリシーを管理) の順に選択します。
5. [Full Access] (フルアクセス) を選択してサービスへのフルアクセスを許可するか、[Custom] (カスタム) を選択してカスタムポリシーをアタッチします。
6. [Save] を選択します。

コマンドラインを使用してゲートウェイエンドポイントを変更するには

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint (Windows 用のツール PowerShell)

DynamoDB にアクセスするためのエンドポイントのポリシーの例は次のとおりです。

Example 例: 読み取り専用アクセスを許可する

アクセスを読み取り専用アクセスに制限するポリシーを作成できます。次のポリシーは、DynamoDB テーブルを一覧表示および説明するための許可を付与します。

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

Example 例: 特定のテーブルへのアクセスの制限

特定の DynamoDB テーブルへのアクセスを制限するポリシーを作成できます。次のポリシーは、指定された DynamoDB テーブルへのアクセスを許可します。

```
{
```

```
  "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"
    }
  ]
}
```

ゲートウェイエンドポイントを削除する

不要になったゲートウェイエンドポイントは、削除することができます。ゲートウェイエンドポイントを削除すると、エンドポイントルートがサブネットルートテーブルから削除されます。

コンソールを使用してゲートウェイエンドポイントを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. ゲートウェイエンドポイントを選択する
4. アクション、VPCエンドポイントの削除を選択します。
5. 確認を求められたら、**delete** をクリックします。
6. [削除] を選択します。

コマンドラインを使用してゲートウェイエンドポイントを削除するには

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint (Windows 用のツール PowerShell)

経由で SaaS 製品にアクセスする AWS PrivateLink

を使用すると AWS PrivateLink、SaaS 製品にプライベートでアクセスでき、独自の で実行されているかのようにアクセスできますVPC。

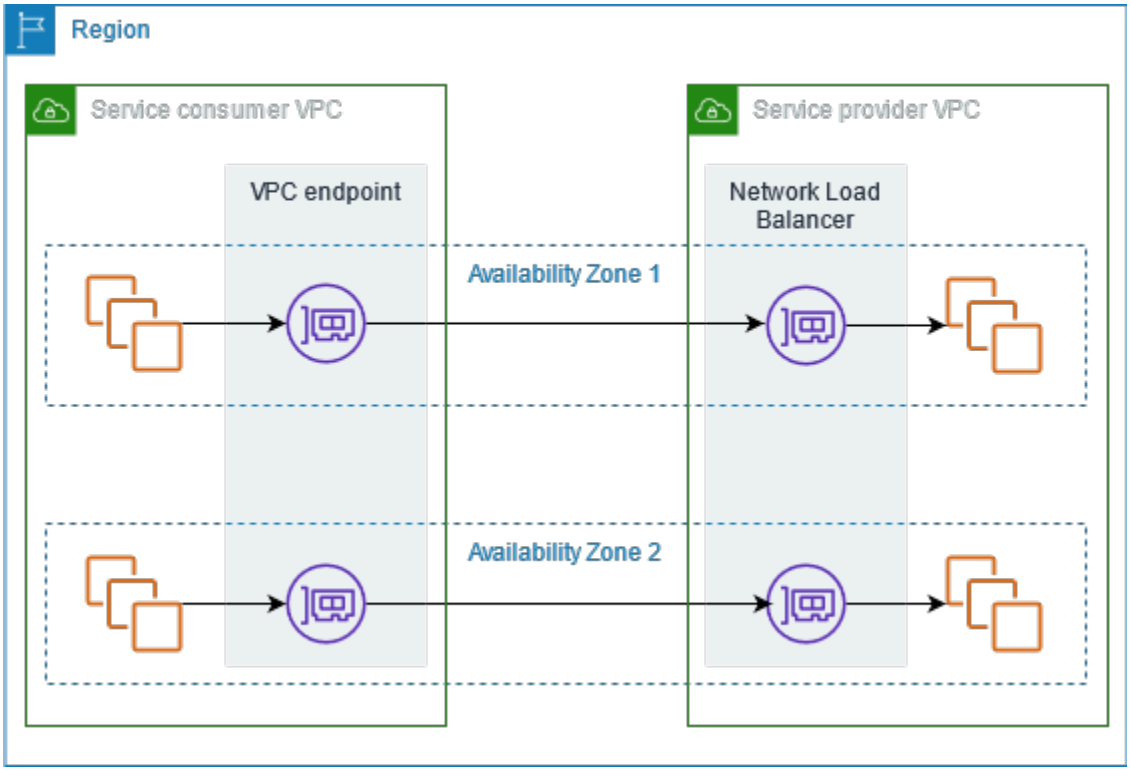
内容

概要

AWS PrivateLink を通じて を搭載した SaaS 製品を検出、購入、プロビジョニングできます AWS Marketplace。詳細については、「 を使用して SaaS アプリケーションに安全かつプライベートにアクセスする AWS PrivateLink」を参照してください。

また、 AWS パートナー AWS PrivateLink から を搭載した SaaS 製品を見つけることもできます。詳細については、「AWS PrivateLink パートナー」を参照してください。

次の図は、VPCエンドポイントを使用して SaaS 製品に接続する方法を示しています。サービスプロバイダーはエンドポイントサービスを作成し、お客様にエンドポイントサービスへのアクセス権を付与します。サービスコンシューマーは、 の 1 つ以上のサブネットVPCとVPCエンドポイントサービス間の接続を確立するインターフェイスエンドポイントを作成します。



インターフェイスエンドポイントの作成

以下の手順を使用して、SaaS 製品に接続するインターフェイスVPCエンドポイントを作成します。

要件

サービスをサブスクライブします。

パートナーサービスへのインターフェイスエンドポイントを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. [エンドポイントの作成] を選択します。
4. サービスを購入した場合は AWS Marketplace、次の操作を行います。
   a. タイプ で、 AWS Marketplace サービスを選択します。
   b. サービスを選択します。
5. AWS Service Ready 指定でサービスをサブスクライブした場合は、次の操作を行います。
   a. タイプ で、PrivateLink 準備完了パートナーサービス を選択します。

b. サービスの名前を入力し、サービスの検証を選択します。

6. でVPC、製品にアクセスする VPC を選択します。
7. サブネット で、エンドポイントネットワークインターフェイスを作成するサブネットを選択します。
8. [Security groups] (セキュリティグループ) で、エンドポイントネットワークインターフェイスに関連付けるセキュリティグループを選択します。セキュリティグループルールでは、 のリソースVPCとエンドポイントネットワークインターフェイス間のトラフィックを許可する必要があります。
9. (オプション) タグを追加するには、[新しいタグを追加] を選択し、そのタグのキーと値を入力します。
10. [エンドポイントの作成] を選択します。

インターフェイスエンドポイントを設定するには

インターフェイスエンドポイントの設定については、「the section called “インターフェイスエンドポイントを設定する”」を参照してください。

経由で仮想アプライアンスにアクセスする AWS PrivateLink

Gateway Load Balancer を使用して、ネットワーク仮想アプライアンスのフリートにトラフィックを分散できます。アプライアンスは、セキュリティ検査、コンプライアンス、ポリシー制御、およびその他のネットワークサービスに使用できます。Gateway Load Balancer は、VPCエンドポイントサービスを作成するときに指定します。他の AWS プリンシパルは、Gateway Load Balancer エンドポイントを作成することにより、エンドポイントサービスにアクセスします。

料金

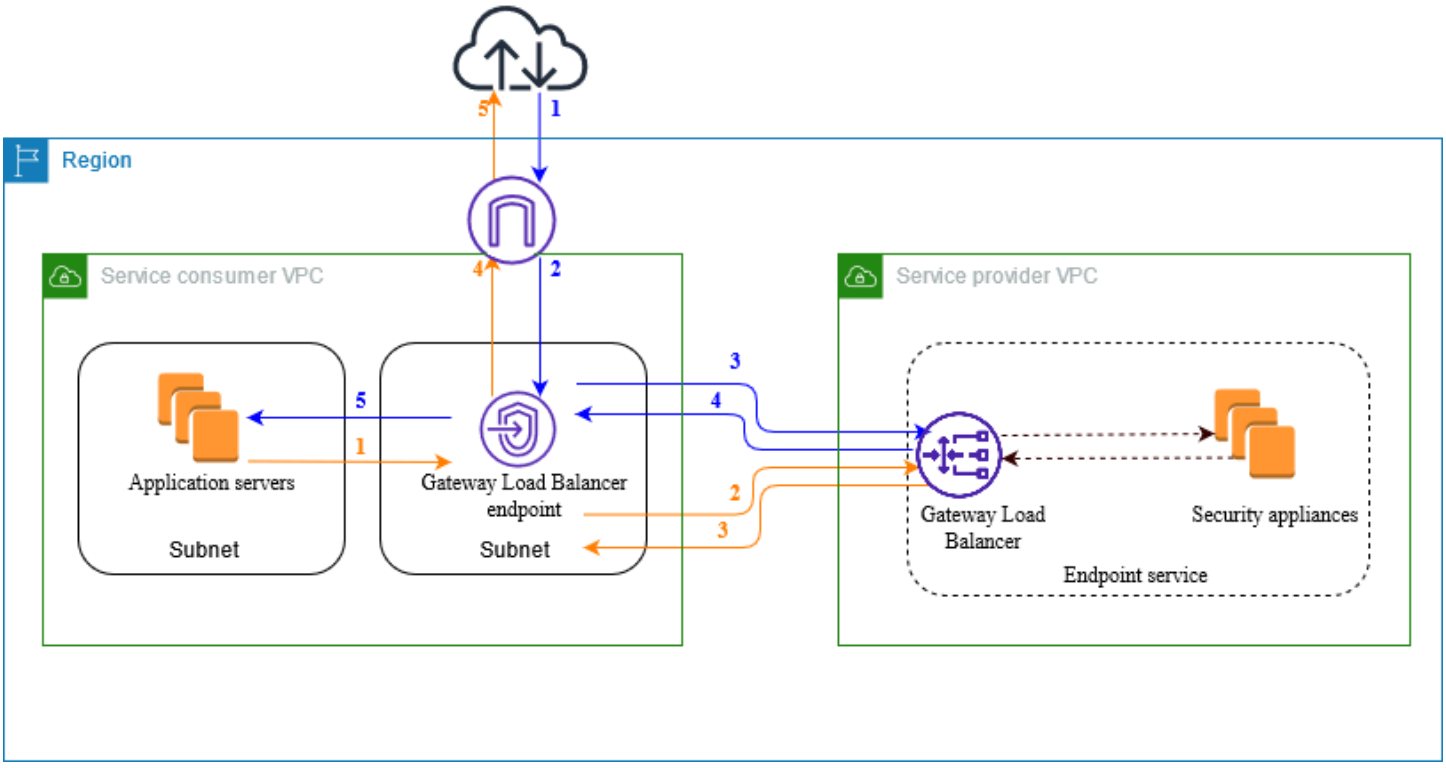
Gateway Load Balancer エンドポイントが各アベイラビリティーゾーンでプロビジョニングされる 1 時間ごとに課金されます。また、処理されたデータの GB ごとに課金されます。詳細については、「AWS PrivateLink 料金」を参照してください。

内容

詳細については、「Gateway Load Balancer の開始方法」をご参照ください。

概要

次の図は、アプリケーションサーバーが を介してセキュリティアプライアンスにアクセスする方法を示しています AWS PrivateLink。アプリケーションサーバーは、サービスコンシューマー のサブネットで実行されますVPC。Gateway Load Balancer エンドポイントは、同じ の別のサブネットに作成しますVPC。インターネットゲートウェイVPCを介してサービスコンシューマーに入るすべてのトラフィックは、まず検査のために Gateway Load Balancer エンドポイントにルーティングされ、次に宛先サブネットにルーティングされます。同様に、アプリケーションサーバーから出るすべてのトラフィックは、検査のために Gateway Load Balancer エンドポイントにルーティングされ、その後にインターネットゲートウェイを通じたルーティングによって戻ります。



インターネットからアプリケーションサーバーへのトラフィック (青い矢印):

1. トラフィックはインターネットゲートウェイVPCを介してサービスコンシューマーに入ります。
2. トラフィックは、ルートテーブルの設定に基づいて Gateway Load Balancer エンドポイントに送信されます。
3. トラフィックは、セキュリティアプライアンスを介して検査のために Gateway Load Balancer に送信されます。
4. 検査後、トラフィックは Gateway Load Balancer エンドポイントに戻されます。
5. トラフィックは、ルートテーブルの設定に基づいてアプリケーションサーバーに送信されます。

アプリケーションサーバーからインターネットへのトラフィック (オレンジの矢印):

1. トラフィックは、ルートテーブルの設定に基づいて Gateway Load Balancer エンドポイントに送信されます。
2. トラフィックは、セキュリティアプライアンスを介して検査のために Gateway Load Balancer に送信されます。
3. 検査後、トラフィックは Gateway Load Balancer エンドポイントに戻されます。
4. トラフィックは、ルートテーブルの設定に基づいてインターネットゲートウェイに送信されます。

5. トラフィックはインターネットにルーティングされます。

IP アドレスのタイプ

サービスプロバイダーは、セキュリティアプライアンスが のみをサポートしている場合でも IPv6、IPv4、IPv6、または IPv4と の両方を介してサービスコンシューマーがサービスエンドポイントを利用できるようにしますIPv4。デュアルスタックサポートを有効にすると、既存のコンシューマーは引き続き IPv4を使用してサービスにアクセスでき、新しいコンシューマーは IPv6 を使用してサービスにアクセスすることを選択できます。

Gateway Load Balancer エンドポイントが をサポートしている場合IPv4、エンドポイントネットワークインターフェイスには IPv4 アドレスがあります。Gateway Load Balancer エンドポイントがをサポートしている場合IPv6、エンドポイントネットワークインターフェイスには IPv6 アドレスがあります。エンドポイントネットワークインターフェイスのIPv6アドレスにインターネットからアクセスできません。IPv6 アドレスを使用してエンドポイントネットワークインターフェイスを記述する場合は、 `denyAllIgwTraffic` が有効になっていることに注意してください。

エンドポイントサービスIPv6で を有効にするための要件

- エンドポイントサービスの VPCおよび サブネットには、関連付けられたIPv6CIDRブロックが必要です。
- エンドポイントサービスの Gateway Load Balancer は、dualstack IP アドレスタイプを使用する必要があります。セキュリティアプライアンスはIPv6トラフィックをサポートする必要はありません。

Gateway Load Balancer エンドポイントIPv6で を有効にするための要件

- エンドポイントサービスには、 IPv6 サポートを含む IP アドレスタイプが必要です。
- Gateway Load Balancer エンドポイントの IP アドレスのタイプは、次に説明するように、Gateway Load Balancer エンドポイントのサブネットと互換性がある必要があります。
  - IPv4 – エンドポイントネットワークインターフェイスにIPv4アドレスを割り当てます。このオプションは、選択したすべてのサブネットにIPv4アドレス範囲がある場合にのみサポートされます。
  - IPv6 – エンドポイントネットワークインターフェイスにIPv6アドレスを割り当てます。このオプションは、選択したすべてのサブネットがサブネットIPv6のみの場合にのみサポートされます。

- デュアルスタック — エンドポイントネットワークインターフェイスに IPv4と IPv6 アドレスの両方を割り当てます。このオプションは、選択したすべてのサブネットに IPv4と の両方のIPv6アドレス範囲がある場合にのみサポートされます。
- サービスコンシューマー内のサブネットのルートテーブルVPCはIPv6トラフィックをルーティングし、ACLsこれらのサブネットのネットワークはIPv6トラフィックを許可する必要があります。

ルーティング

トラフィックをエンドポイントサービスにルーティングするには、その ID を使用して Gateway Load Balancer エンドポイントをルートテーブルでターゲットとして指定します。上図では、次のようにルートをルートテーブルに追加します。IPv6 ルートはデュアルスタック設定に含まれていることに注意してください。

インターネットゲートウェイのルートテーブル

このルートテーブルには、アプリケーションサーバー宛てのトラフィックを Gateway Load Balancer エンドポイントに送信するルートが必要です。

デスティネーション	ターゲット
VPC IPv4 CIDR	ローカル
VPC IPv6 CIDR	ローカル
Application subnet IPv4 CIDR	*vpc-endpoint-id*
Application subnet IPv6 CIDR	*vpc-endpoint-id*

アプリケーションサーバーを備えたサブネットのルートテーブル

このルートテーブルには、アプリケーションサーバーからのすべてのトラフィックを Gateway Load Balancer エンドポイントに送信するルートが必要です。

デスティネーション	ターゲット
VPC IPv4 CIDR	ローカル
VPC IPv6 CIDR	ローカル

デスティネーション	ターゲット
0.0.0.0/0	*vpc-endpoint-id*
::/0	*vpc-endpoint-id*

Gateway Load Balancer エンドポイントを含むサブネットのルートテーブル

このルートテーブルは、検査から返されるトラフィックを最終的な宛先に送信する必要があります。インターネットから発信されたトラフィックの場合、ローカルルートはそのトラフィックをアプリケーションサーバーに送信します。アプリケーションサーバーを起点とするトラフィックについては、すべてのトラフィックをインターネットゲートウェイに送信するルートを追加します。

デスティネーション	ターゲット
VPC IPv4 CIDR	ローカル
VPC IPv6 CIDR	ローカル
0.0.0.0/0	*internet-gateway-id*
::/0	*internet-gateway-id*

検査システムを Gateway Load Balancer エンドポイントサービスとして作成する

エンドポイントサービスと呼ばれる AWS PrivateLink、 を利用した独自のサービスを作成できます。お客様はサービスプロバイダーであり、サービスへの接続を作成する AWS プリンシパルはサービスコンシューマーです。

エンドポイントサービスには、Network Load Balancer または Gateway Load Balancer のいずれかが必要です。この場合、Gateway Load Balancer を使用してエンドポイントサービスを作成します。Network Load Balancer を使用してエンドポイントサービスを作成する方法の詳細については、「エンドポイントサービスを作成する」を参照してください。

内容

- 前提条件
- エンドポイントサービスを作成する
- エンドポイントサービスを使用できるようにする

考慮事項

- エンドポイントサービスは、そのサービスを作成したリージョンで使用できます。
- サービスコンシューマーがエンドポイントサービスに関する情報を取得すると、サービスプロバイダーと共通するアベイラビリティゾーンのみが表示されます。サービスプロバイダーとサービスコンシューマーが異なるアカウントにある場合、us-east-1a などのアベイラビリティゾーン名は、各 AWS アカウントの異なる物理アベイラビリティゾーンにマッピングされる可能性があります。AZ を使用してIDs、サービスのアベイラビリティーゾーンを一貫して識別できます。詳細については、「Amazon EC2ユーザーガイド」の「AZIDs」を参照してください。
- AWS PrivateLink リソースにはクォータがあります。詳細については、「AWS PrivateLink クォータ」を参照してください。

前提条件

- サービスが利用可能なアベイラビリティーゾーンに少なくとも 2 つのサブネットVPCを持つサービスプロバイダーを作成します。1 つのサブネットはセキュリティアプライアンスインスタンス用で、もう 1 つは Gateway Load Balancer 用です。
- サービスプロバイダー に Gateway Load Balancer を作成しますVPC。エンドポイントサービスでIPv6サポートを有効にする場合は、Gateway Load Balancer でデュアルスタックサポートを有効にする必要があります。詳細については、「Gateway Load Balancer の開始方法」をご参照ください。
- サービスプロバイダーでセキュリティアプライアンスを起動VPCし、ロードバランサーターゲットグループに登録します。

エンドポイントサービスを作成する

Gateway Load Balancer を使用してエンドポイントサービスを作成するには、次の手順を使用します。

コンソールを使用してエンドポイントサービスを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
3. [Create endpoint service]] (エンドポイントサービスの作成) を選択します。
4. [Load balancer type] (ロードバランサーのタイプ) で、[Gateway] を選択します。
5. [Available load balancers] (使用可能なロードバランサー) で、お使いの Gateway Load Balancer を選択します。
6. エンドポイントサービスへの接続リクエストが手動で承諾されなければならないようにするために、[Require acceptance for endpoint] (エンドポイントの承諾を要求) で、[Acceptance required] (承諾が必要) を選択します。それ以外の場合、これらのリクエストは自動的に受け入れられます。
7. [Supported IP address types] (サポートされている IP アドレスのタイプ) で、次のいずれかを実行します。
   - 選択 IPv4 — エンドポイントサービスがIPv4リクエストを受け入れるようにします。
   - 選択 IPv6 — エンドポイントサービスがIPv6リクエストを受け入れるようにします。
   - Select IPv4 and IPv6 – エンドポイントサービスが IPv4 および IPv6リクエストの両方を受け入れるようにします。
8. (オプション) タグを追加するには、[新しいタグを追加] を選択し、そのタグのキーと値を入力します。
9. [Create] (作成) を選択します。

コマンドラインを使用してエンドポイントサービスを作成するには

- create-vpc-endpoint-service設定 (AWS CLI)
- New-EC2VpcEndpointServiceConfiguration (Windows 用のツール PowerShell)

エンドポイントサービスを使用できるようにする

サービスプロバイダーは、自社のサービスをサービスコンシューマーが使用できるようにするために、次のことを行う必要があります。

- 各サービスコンシューマーがエンドポイントサービスに接続できるようにする許可を追加します。詳細については、「the section called “許可を管理する”」を参照してください。

- サービスの名前とサポートされているアベイラビリティゾーンをサービスコンシューマーに伝え、サービスに接続するためにインターフェイスエンドポイントを作成できるようにします。詳細については、以下の手順を参照してください。
- サービスコンシューマーからのエンドポイント接続リクエストを受け入れます。詳細については、「the section called “接続リクエストを承諾または拒否する”」を参照してください。

AWS プリンシパルは、Gateway Load Balancer エンドポイントを作成することで、エンドポイントサービスにプライベートに接続できます。詳細については、「Gateway Load Balancer エンドポイントを作成する」を参照してください。

Gateway Load Balancer エンドポイントを使用して検査システムにアクセスする

ゲートウェイ ロードバランサー エンドポイントを作成して、 AWS PrivateLinkを利用するエンドポイントサービスに接続できます。

から指定したサブネットごとにVPC、サブネットにエンドポイントネットワークインターフェイスを作成し、サブネットアドレス範囲からプライベート IP アドレスを割り当てます。エンドポイントネットワークインターフェイスは、リクエスタが管理するネットワークインターフェイスです。 で表示できますが AWS アカウント、自分で管理することはできません。

時間単位の使用料金とデータ処理料金が課金されます。詳細については、Gateway Load Balancer エンドポイントの料金を参照してください。

内容

- 考慮事項
- 前提条件
- エンドポイントの作成
- ルーティングを設定する
- タグの管理
- Gateway Load Balancer エンドポイントを削除する

考慮事項

- サービスコンシューマー で選択できるアベイラビリティーゾーンは 1 つだけですVPC。このサブネットを後で変更することはできません。別のサブネットで Gateway Load Balancer エンドポイントを使用するには、新しい Gateway Load Balancer エンドポイントを作成する必要があります。
- サービスごとに 1 つのアベイラビリティゾーンについて単一の Gateway Load Balancer エンドポイントを作成できます。Gateway Load Balancer がサポートするアベイラビリティゾーンを選択する必要があります。サービスプロバイダーとサービスコンシューマーが異なるアカウントにある場合、`us-east-1a` などのアベイラビリティゾーン名は、各 AWS アカウントの異なる物理アベイラビリティゾーンにマッピングされる可能性があります。AZ を使用してIDs、サービスのアベイラビリティーゾーンを一貫して識別できます。詳細については、「Amazon EC2ユーザーガイド」の「AZIDs」を参照してください。
- エンドポイントサービスを使用する前に、サービスプロバイダーは接続リクエストを受け入れる必要があります。サービスは、VPCエンドポイントVPCを介して 内のリソースへのリクエストを開始できません。エンドポイントは、 のリソースによって開始されたトラフィックへのレスポンスのみを返しますVPC。
- 各 Gateway Load Balancer エンドポイントは、アベイラビリティゾーンあたり最大 10 Gbps の帯域幅をサポートし、最大 100 Gbps まで自動的にスケールアップします。
- エンドポイントサービスが複数の Gateway Load Balancer に関連付けられている場合、Gateway Load Balancer エンドポイントは、アベイラビリティゾーンごとに 1 つのロードバランサーのみとの接続を確立します。
- 同じアベイラビリティゾーン内にトラフィックを維持するには、トラフィックの送信先となる各アベイラビリティゾーンに Gateway Load Balancer エンドポイントを作成することをお勧めします。
- Network Load Balancer クライアント IP 保存は、ターゲットが Network Load Balancer VPCと同じ にある場合でも、トラフィックが Gateway Load Balancer エンドポイントを介してルーティングされる場合、サポートされません。
- アプリケーションサーバーと Gateway Load Balancer エンドポイントが同じサブネットにある場合、NACLルールはアプリケーションサーバーから Gateway Load Balancer エンドポイントへのトラフィックについて評価されます。
- Egress-Only インターネットゲートウェイで Gateway Load Balancer を使用すると、IPv6トラフィックはドロップされます。代わりに、インターネットゲートウェイとインバウンドファイアウォールルールを使用してください。

- AWS PrivateLink リソースにはクォータがあります。詳細については、「AWS PrivateLink クォータ」を参照してください。

前提条件

- サービスにアクセスするアベイラビリティーゾーンに少なくとも 2 つのサブネットVPCを持つサービスコンシューマーを作成します。1 つのサブネットはアプリケーションサーバー用で、もう 1 つは Gateway Load Balancer エンドポイント用です。
- エンドポイントサービスでサポートされているアベイラビリティーゾーンを確認するには、 コンソールまたは describe-vpc-endpoint-services コマンドを使用してエンドポイントサービスを記述します。
- リソースがネットワーク を持つサブネットにある場合はACL、ネットワークがエンドポイントネットワークインターフェイスと 内のリソース間のトラフィックACLを許可していることを確認しますVPC。

エンドポイントの作成

次の手順を使用して、検査システムのエンドポイントサービスに接続する Gateway Load Balancer エンドポイントを作成します。

コンソールを使用して Gateway Load Balancer エンドポイントを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. [エンドポイントの作成] を選択します。
4. タイプ で、 NLBsと を使用するエンドポイントサービスGWLBsを選択します。
5. [Service name] (サービス名) にサービスの名前を入力し、[Verify service] (サービスを検証) を選択します。
6. でVPC、エンドポイントサービスにアクセスする VPC を選択します。
7. サブネットで、エンドポイントネットワークインターフェイスを作成するサブネットを 1 つ選択します。
8. [IP address type] (IP アドレスのタイプ) で、次のオプションから選択します。

   - IPv4 – エンドポイントネットワークインターフェイスにIPv4アドレスを割り当てます。このオプションは、選択したサブネットにIPv4アドレス範囲がある場合にのみサポートされます。

- IPv6 – エンドポイントネットワークインターフェイスにIPv6アドレスを割り当てます。このオプションは、選択したサブネットがIPv6唯一のサブネットである場合にのみサポートされます。
- デュアルスタック — エンドポイントネットワークインターフェイスに IPv4と IPv6 アドレスの両方を割り当てます。このオプションは、選択したサブネットに IPv4と の両方のIPv6アドレス範囲がある場合にのみサポートされます。

9. (オプション) タグを追加するには、[新しいタグを追加] を選択し、そのタグのキーと値を入力します。
10. [エンドポイントの作成] を選択します。初期ステータスは、`pending acceptance` です。

コマンドラインを使用して Gateway Load Balancer エンドポイントを作成するには

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint (Windows 用のツール PowerShell)

ルーティングを設定する

サービスコンシューマー のルートテーブルを設定するには、次の手順に従いますVPC。これにより、セキュリティアプライアンスは、アプリケーションサーバー宛てのインバウンドトラフィックに対してセキュリティ検査を実行できます。詳細については、「the section called “ルーティング”」を参照してください。

コンソールを使用してルーティングを設定するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Route Tables] を選択します。
3. インターネットゲートウェイのルートテーブルを選択し、以下を実行します。
   a. [アクション]、[ポリシーの編集] の順に選択します。
   b. をサポートしている場合はIPv4、ルートの追加を選択します。Destination に、アプリケーションサーバーのサブネットの IPv4 CIDR ブロックを入力します。ターゲット で、VPCエンドポイントを選択します。
   c. をサポートしている場合はIPv6、ルートの追加を選択します。Destination に、アプリケーションサーバーのサブネットの IPv6 CIDR ブロックを入力します。ターゲット で、VPCエンドポイントを選択します。

d. [Save changes] (変更の保存) をクリックします。

4. アプリケーションサーバーを含むサブネットのルートテーブルを選択し、以下を実行します。

   a. [アクション]、[ポリシーの編集] の順に選択します。

   b. をサポートしている場合はIPv4、ルートの追加を選択します。[送信先] に「**0.0.0.0/0**」と入力します。ターゲット で、VPCエンドポイントを選択します。

   c. をサポートしている場合はIPv6、ルートの追加を選択します。[送信先] に「**::/0**」と入力します。ターゲット で、VPCエンドポイントを選択します。

   d. [Save changes] (変更の保存) をクリックします。

5. Gateway Load Balancer エンドポイントを持つサブネットのルートテーブルを選択し、以下を実行します。

   a. [アクション]、[ポリシーの編集] の順に選択します。

   b. をサポートしている場合はIPv4、ルートの追加を選択します。[送信先] に「**0.0.0.0/0**」と入力します。[Target] (ターゲット) で、インターネットゲートウェイを選択します。

   c. をサポートしている場合はIPv6、ルートの追加を選択します。[送信先] に「**::/0**」と入力します。[Target] (ターゲット) で、インターネットゲートウェイを選択します。

   d. [Save changes] (変更の保存) をクリックします。

コマンドラインを使用してルーティングを設定するには

- create-route (AWS CLI)
- New-EC2Route (Windows 用のツール PowerShell)

タグの管理

Gateway Load Balancer エンドポイントにタグを付けて、識別しやすくしたり、組織のニーズに応じて分類したりできます。

コンソールを使用してタグを管理するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. インターフェイスエンドポイントを選択します。
4. [Actions] (アクション)、[Manage tags] (タグの管理) を選択します。

5. 追加するタグごとに、[Add new tag] (新しいタグを追加) を選択し、タグキーとタグ値を入力します。
6. タグを削除するには、タグのキーと値の右側にある [Remove] (削除) を選択します。
7. [Save] を選択します。

コマンドラインを使用してタグを管理するには

- create-tags および delete-tags (AWS CLI)
- New-EC2Tag および Remove-EC2Tag (Tools for Windows PowerShell)

Gateway Load Balancer エンドポイントを削除する

不要になったエンドポイントは、削除することができます。Gateway Load Balancer エンドポイントを削除すると、エンドポイントのネットワークインターフェイスも削除されます。エンドポイントをポイントするルートテーブルにルートがある場合、Gateway Load Balancer エンドポイントは削除できません。

Gateway Load Balancer エンドポイントを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Endpoints] を選択し、エンドポイントを選択します。
3. [Actions]、[Delete Endpoint] の順に選択します。
4. 確認画面で、[Yes, Delete] を選択します。

Gateway Load Balancer エンドポイントを削除するには

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

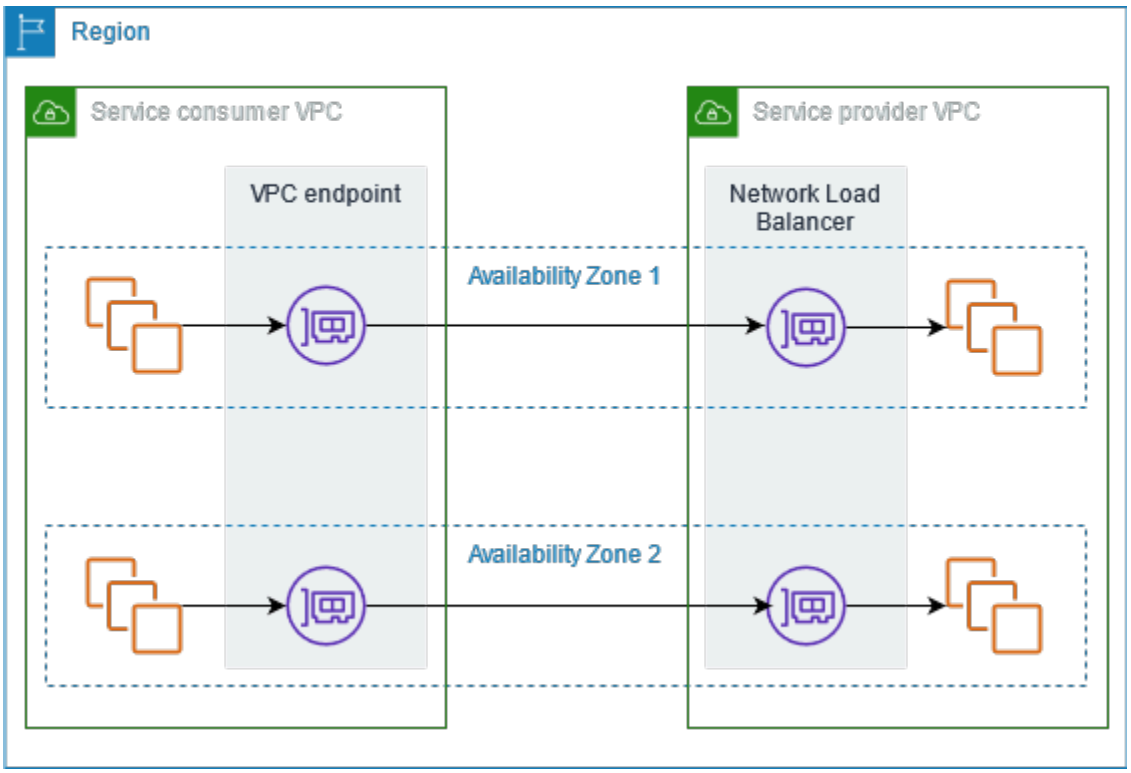
を通じてサービスを共有する AWS PrivateLink

エンドポイントサービスと呼ばれる独自の AWS PrivateLink 搭載サービスをホストし、他の AWS のお客様と共有できます。

内容

概要

次の図は、 でホストされているサービスを他の AWS のお客様 AWS と共有する方法と、それらのお客様がサービスに接続する方法を示しています。サービスプロバイダーは、サービスフロントエンド VPCとして に Network Load Balancer を作成します。次に、VPCエンドポイントサービス設定を作成するときに、このロードバランサーを選択します。特定の AWS プリンシパルにアクセス許可を付与して、サービスに接続できるようにします。サービスコンシューマーとして、顧客はインターフェイスVPCエンドポイントを作成します。これにより、 VPCとエンドポイントサービスから選択したサブネット間の接続が確立されます。ロードバランサーは、サービスコンシューマーからリクエストを受け取ってサービスをホスティングしているターゲットにルーティングします。



低レイテンシーと高可用性を得るために、少なくとも 2 つのアベイラビリティーゾーンでサービスを使用可能にすることをお勧めします。

DNS ホスト名

サービスプロバイダーがVPCエンドポイントサービスを作成すると、 はサービスのエンドポイント固有のDNSホスト名 AWS を生成します。これらの名前の構文は次のとおりです。

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

us-east-2 リージョンのVPCエンドポイントサービスのDNSホスト名の例を次に示します。

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

サービスコンシューマーがインターフェイスVPCエンドポイントを作成すると、サービスコンシューマーがエンドポイントサービスと通信するために使用できるリージョン名とゾーンDNS名が作成されます。リージョンレベルの名前の構文は次のとおりです。

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

ゾーンレベルの名前の構文は次のとおりです。

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

プライベート DNS

サービスプロバイダーはエンドポイントサービスのプライベートDNS名を関連付けることもできます。これにより、サービスコンシューマーは既存のDNS名前を使用してサービスに引き続きアクセスできます。サービスプロバイダーがプライベートDNS名をエンドポイントサービスに関連付けると、サービスコンシューマーはインターフェイスエンドポイントのプライベートDNS名を有効にできます。サービスプロバイダーがプライベート を有効にしていない場合DNS、サービスコンシューマーはVPCエンドポイントサービスのパブリックDNS名を使用するようにアプリケーションを更新する必要がある場合があります。詳細については、「DNS 名前の管理」を参照してください。

クロスリージョンアクセス

サービスプロバイダーは、1 つのリージョンでサービスをホストし、サポートされているリージョンのセットで利用可能にすることができます。サービスコンシューマーは、エンドポイントの作成時にサービスリージョンを選択します。

アクセス許可

- デフォルトでは、IAMエンティティには、エンドポイントサービスを複数のリージョンで使用できるようにしたり、リージョン間でエンドポイントサービスにアクセスしたりするアクセス許可はありません。クロスリージョンアクセスに必要なアクセス許可を付与するために、IAM管理者はアクセス`vpce:AllowMultiRegion`許可のみのアクションを許可するIAMポリシーを作成できます。
- エンドポイントサービスの作成時にIAMエンティティがサポート対象リージョンとして指定できるリージョンを制御するには、 `ec2:VpceSupportedRegion`条件キーを使用します。
- IAM エンティティがVPCエンドポイントの作成時にサービスリージョンとして指定できるリージョンを制御するには、 `ec2:VpceServiceRegion`条件キーを使用します。

考慮事項

- サービスプロバイダーは、オプトインリージョンをエンドポイントサービスのサポートされているリージョンとして追加する前に、オプトインリージョンにオプトインする必要があります。
- エンドポイントサービスは、ホストリージョンからアクセスできる必要があります。サポートされているリージョンのセットからホストリージョンを削除することはできません。冗長性を確保する

ために、エンドポイントサービスを複数のリージョンにデプロイし、エンドポイントサービスごとにクロスリージョンアクセスを有効にすることができます。

- サービスコンシューマーは、エンドポイントのサービスリージョンとして選択する前に、オプトインリージョンにオプトインする必要があります。可能な限り、サービスコンシューマーは、クロスリージョン接続ではなくリージョン内接続を使用してサービスにアクセスすることをお勧めします。リージョン内接続により、レイテンシーとコストが低くなります。
- サービスプロバイダーがサポートされているリージョンのセットからリージョンを削除した場合、サービスコンシューマーは新しいエンドポイントを作成するときにそのリージョンをサービスリージョンとして選択できません。これは、このリージョンをサービスリージョンとして使用する既存のエンドポイントからのエンドポイントサービスへのアクセスには影響しないことに注意してください。
- 高可用性を実現するには、プロバイダーとコンシューマーの両方が少なくとも 2 つのアベイラビリティーゾーンを使用する必要があります。クロスリージョンアクセスでは、プロバイダーとコンシューマーが同じアベイラビリティーゾーンを使用する必要はありません。
- クロスリージョンアクセスでは、 はアベイラビリティーゾーン間のフェイルオーバー AWS PrivateLink を管理します。リージョン間のフェイルオーバーは管理されません。
- クロスリージョンアクセスは、わかりやすいDNS名前 AWS Marketplace のサービスではサポートされていません。
- クロスリージョンアクセスは、TCPアイドルタイムアウト用にカスタム値が設定された Network Load Balancer ではサポートされていません。
- クロスリージョンアクセスはUDP、フラグメント化ではサポートされていません。

IP アドレスのタイプ

サービスプロバイダーは、バックエンドサーバーが のみをサポートしている場合でも IPv6、IPv4、IPv6、または IPv4と の両方を介してサービスコンシューマーがサービスエンドポイントを利用できるようにしますIPv4。デュアルスタックサポートを有効にすると、既存のコンシューマーは引き続き IPv4を使用してサービスにアクセスでき、新しいコンシューマーは IPv6 を使用してサービスにアクセスすることを選択できます。

インターフェイスVPCエンドポイントが をサポートしている場合IPv4、エンドポイントネットワークインターフェイスには IPv4 アドレスがあります。インターフェイスVPCエンドポイントが をサポートしている場合IPv6、エンドポイントネットワークインターフェイスには IPv6 アドレスがあります。エンドポイントネットワークインターフェイスのIPv6アドレスにインターネットからアクセス

できません。IPv6 アドレスを使用してエンドポイントネットワークインターフェイスを記述する場合は、 `denyAllIgwTraffic` が有効になっていることに注意してください。

エンドポイントサービスIPv6で を有効にするための要件

- エンドポイントサービスの VPCおよび サブネットには、関連付けられたIPv6CIDRブロックが必要です。
- エンドポイントサービスのすべての Network Load Balancers は、dualstack IP アドレスのタイプを使用する必要があります。ターゲットはIPv6トラフィックをサポートする必要はありません。サービスがプロキシプロトコルバージョン 2 ヘッダーからソース IP アドレスを処理する場合は、IPv6アドレスを処理する必要があります。

インターフェイスエンドポイントIPv6で を有効にするための要件

- エンドポイントサービスはIPv6リクエストをサポートしている必要があります。
- インターフェイスエンドポイントの IP アドレスのタイプは、次に説明するように、インターフェイスエンドポイントのサブネットと互換性がある必要があります。
  - IPv4 – エンドポイントネットワークインターフェイスにIPv4アドレスを割り当てます。このオプションは、選択したすべてのサブネットにIPv4アドレス範囲がある場合にのみサポートされます。
  - IPv6 – エンドポイントネットワークインターフェイスにIPv6アドレスを割り当てます。このオプションは、選択したすべてのサブネットがサブネットIPv6のみの場合にのみサポートされます。
  - デュアルスタック — エンドポイントネットワークインターフェイスに IPv4と IPv6 アドレスの両方を割り当てます。このオプションは、選択したすべてのサブネットに IPv4と の両方のIPv6アドレス範囲がある場合にのみサポートされます。

DNS インターフェイスエンドポイントの IP アドレスタイプの記録

インターフェイスエンドポイントがサポートするDNSレコード IP アドレスタイプによって、作成するDNSレコードが決まります。インターフェイスエンドポイントのDNSレコード IP アドレスタイプは、以下で説明するように、インターフェイスエンドポイントの IP アドレスタイプと互換性がある必要があります。

- IPv4 – プライベート、リージョン、およびゾーンDNS名のレコードを作成します。IP アドレスタイプは IPv4またはデュアルスタックである必要があります。

- IPv6 – プライベート、リージョン、およびゾーンDNS名のAAAAレコードを作成します。IP アドレスタイプは IPv6またはデュアルスタックである必要があります。
- デュアルスタック – プライベート、リージョン、およびゾーンDNS名の A レコードと AAAAレコードを作成します。IP アドレスのタイプは [Dualstack] である必要があります。

によるサービスの作成 AWS PrivateLink

エンドポイントサービスと呼ばれる AWS PrivateLink、 を利用した独自のサービスを作成できます。お客様はサービスプロバイダーであり、お客様のサービスへの接続を作成する AWS プリンシパルはサービスコンシューマーです。

エンドポイントサービスには、Network Load Balancer または Gateway Load Balancer のいずれかが必要です。ロードバランサーは、サービスコンシューマーからリクエストを受け取ってサービスにルーティングします。この場合、Network Load Balancer を使用してエンドポイントサービスを作成します。Gateway Load Balancer を使用してエンドポイントサービスを作成する方法の詳細については、「仮想アプライアンスにアクセスする」を参照してください。

内容

考慮事項

- エンドポイントサービスは、そのサービスを作成したリージョンで使用できます。コンシューマーは、クロスリージョンアクセスを有効にした場合、またはピアリングまたはトランジットゲートウェイを使用している場合、他のリージョンからサービスにアクセスできます。 VPC
- サービスコンシューマーがエンドポイントサービスに関する情報を取得すると、サービスプロバイダーと共通するアベイラビリティゾーンのみが表示されます。サービスプロバイダーとサービスコンシューマーが異なるアカウントにある場合、us-east-1a などのアベイラビリティゾーン名は、各 AWS アカウントの異なる物理アベイラビリティゾーンにマッピングされる可能性があります。AZ を使用してIDs、サービスのアベイラビリティーゾーンを一貫して識別できます。詳細については、「Amazon EC2ユーザーガイド」の「AZIDs」を参照してください。

- サービスコンシューマーがインターフェイスエンドポイントを介してトラフィックをサービスに送信する場合、アプリケーションに提供されるソース IP アドレスは、サービスコンシューマーの IP アドレスではなく、ロードバランサーノードのプライベート IP アドレスです。ロードバランサーでプロキシプロトコルを有効にすると、プロキシプロトコルヘッダーからサービスコンシューマーのアドレスとインターフェイスエンドポイントIDsの を取得できます。詳細については、Network Load Balancer ユーザーガイドの「Proxy Protocol」を参照してください。
- Network Load Balancer は単一のエンドポイントサービスに関連付けることができますが、エンドポイントサービスは複数の Network Load Balancer に関連付けることができます。
- エンドポイントサービスが複数の Network Load Balancer に関連付けられている場合、各エンドポイントネットワークインターフェイスは 1 つのロードバランサーに関連付けられます。エンドポイントネットワークインターフェイスからの最初の接続が開始されると、エンドポイントネットワークインターフェイスと同じアベイラビリティーゾーンにあるいずれかの Network Load Balancer がランダムに選択されます。このエンドポイントネットワークインターフェイスからの以降のすべての接続リクエストは、この選択されたロードバランサーを使用します。どのロードバランサーが選択されてもコンシューマーがエンドポイントサービスを正常に使用できるように、エンドポイントサービスのすべてのロードバランサーに同じリスナーとターゲットグループ設定を使用することをお勧めします。
- AWS PrivateLink リソースにはクォータがあります。詳細については、「AWS PrivateLink クォータ」を参照してください。

前提条件

- サービスが使用可能になる各アベイラビリティーゾーンに少なくとも 1 つのサブネットを持つエンドポイントサービスVPC用の を作成します。
- サービスコンシューマーがVPCエンドポイントサービスのIPv6インターフェイスエンドポイントを作成できるようにするには、 VPC および サブネットにIPv6CIDRブロックが関連付けられている必要があります。
- で Network Load Balancer を作成しますVPC。サービスコンシューマー向けにサービスを使用可能にするアベイラビリティゾーンごとに 1 つのサブネットを選択します。低レイテンシーとフォールトトレランスのために、リージョン内の少なくとも 2 つのアベイラビリティーゾーンでサービスを使用可能にすることをお勧めします。
- Network Load Balancer にセキュリティグループがある場合は、クライアントの IP アドレスからのインバウンドトラフィックを許可する必要があります。または、経由するトラフィックのインバウンドセキュリティグループルールの評価を無効にすることもできます AWS PrivateLink。詳細

については、「User Guide for Network Load Balancers」の「Security groups」を参照してください。

- エンドポイントサービスがIPv6リクエストを受け入れることができるようにするには、Network Load Balancer でデュアルスタック IP アドレスタイプを使用する必要があります。ターゲットはIPv6トラフィックをサポートする必要はありません。詳細については、「Network Load Balancer のユーザーガイド」の「IP アドレスのタイプ」を参照してください。

  プロキシプロトコルバージョン 2 ヘッダーからソース IP アドレスを処理する場合は、IPv6アドレスを処理できることを確認します。
- サービスを使用可能にする各アベイラビリティゾーンでインスタンスを起動し、ロードバランサーのターゲットグループに登録します。有効なすべてのアベイラビリティーゾーンでインスタンスを起動しない場合は、クロスゾーン負荷分散を有効にして、ゾーンDNSホスト名を使用してサービスにアクセスするサービスコンシューマーをサポートできます。クロスゾーン負荷分散を有効にすると、リージョン内データ転送料金が適用されます。詳細については、「User Guide for Network Load Balancers」の「Cross-zone load balancing」を参照してください。

エンドポイントサービスを作成する

Network Load Balancer を使用してエンドポイントサービスを作成するには、次の手順を使用します。

コンソールを使用してエンドポイントサービスを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
3. [Create endpoint service]] (エンドポイントサービスの作成) を選択します。
4. [Load balancer type] (ロードバランサーのタイプ) で、[Network] を選択します。
5. [使用可能なロードバランサー] で、エンドポイントサービスに関連付ける Network Load Balancer を選択します。選択したロードバランサーで有効になっているアベイラビリティーゾーンを確認するには、「選択したロードバランサーの詳細、含まれるアベイラビリティーゾーン」を参照してください。エンドポイントサービスは、これらのアベイラビリティーゾーンで利用できます。
6. (オプション) エンドポイントサービスをホストされているリージョン以外のリージョンから利用できるようにするには、サービスリージョンからリージョンを選択します。詳細については、「the section called “クロスリージョンアクセス”」を参照してください。

7. エンドポイントサービスへの接続リクエストが手動で承諾されなければならないようにするために、[Require acceptance for endpoint] (エンドポイントの承諾を要求) で、[Acceptance required] (承諾が必要) を選択します。それ以外の場合、これらのリクエストは自動的に受け入れられます。
8. プライベートDNS名を有効にする で、プライベートDNS名をサービスに関連付ける を選択して、サービスコンシューマーがサービスにアクセスするために使用できるプライベートDNS名を関連付け、プライベートDNS名を入力します。それ以外の場合、サービスコンシューマーはが提供するエンドポイント固有のDNS名前を使用できます AWS。サービスコンシューマーがプライベートDNS名を使用する前に、サービスプロバイダーはドメインを所有していることを確認する必要があります。詳細については、「DNS 名前の管理」を参照してください。
9. [Supported IP address types] (サポートされている IP アドレスのタイプ) で、次のいずれかを実行します。

   - 選択 IPv4 — エンドポイントサービスがIPv4リクエストを受け入れるようにします。
   - 選択 IPv6 — エンドポイントサービスがIPv6リクエストを受け入れるようにします。
   - Select IPv4 and IPv6 – エンドポイントサービスが IPv4 および IPv6リクエストの両方を受け入れるようにします。
10. (オプション) タグを追加するには、[新しいタグを追加] を選択し、そのタグのキーと値を入力します。
11. [Create] (作成) を選択します。

コマンドラインを使用してエンドポイントサービスを作成するには

- create-vpc-endpoint-service-configuration (AWS CLI)
- New-EC2VpcEndpointServiceConfiguration (Windows 用のツール PowerShell)

サービスコンシューマーがエンドポイントサービスを使用できるようにする

AWS プリンシパルは、インターフェイスエンドポイントを作成することで、VPCエンドポイントサービスにプライベートに接続できます。サービスプロバイダーは、自社のサービスをサービスコンシューマーが使用できるようにするために、次のことを行う必要があります。

- 各サービスコンシューマーがエンドポイントサービスに接続できるようにする許可を追加します。詳細については、「the section called “許可を管理する”」を参照してください。

- サービスの名前とサポートされているアベイラビリティゾーンをサービスコンシューマーに伝え、サービスに接続するためにインターフェイスエンドポイントを作成できるようにします。詳細については、「the section called “サービスコンシューマーとしてエンドポイントサービスに接続する”」を参照してください。
- サービスコンシューマーからのエンドポイント接続リクエストを受け入れます。詳細については、「the section called “接続リクエストを承諾または拒否する”」を参照してください。

サービスコンシューマーとしてエンドポイントサービスに接続する

サービスコンシューマーは、次の手順を使用して、エンドポイントサービスに接続するためのインターフェイスエンドポイントを作成します。

コンソールを使用してインターフェイスエンドポイントを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. [エンドポイントの作成] を選択します。
4. Type で、 NLBsと を使用するエンドポイントサービスGWLBsを選択します。
5. サービス名にサービスの名前 (例: `com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`) を入力し、サービスの検証を選択します。
6. (オプション) エンドポイントリージョン以外のリージョンで利用可能なエンドポイントサービスに接続するには、サービスリージョン、クロスリージョンエンドポイントの有効化、リージョンを選択します。詳細については、「the section called “クロスリージョンアクセス”」を参照してください。
7. でVPC、エンドポイントサービスにアクセスする VPC を選択します。
8. サブネット で、エンドポイントネットワークインターフェイスを作成するサブネットを選択します。
9. [IP address type] (IP アドレスのタイプ) で、次のオプションから選択します。

    - IPv4 – エンドポイントネットワークインターフェイスにIPv4アドレスを割り当てます。このオプションは、選択したすべてのサブネットにIPv4アドレス範囲があり、エンドポイントサービスがIPv4リクエストを受け入れる場合にのみサポートされます。
    - IPv6 – エンドポイントネットワークインターフェイスにIPv6アドレスを割り当てます。このオプションは、選択したすべてのサブネットがサブネットIPv6のみで、エンドポイントサービスがIPv6リクエストを受け入れる場合にのみサポートされます。

- デュアルスタック — エンドポイントネットワークインターフェイスに IPv4と IPv6 アドレスの両方を割り当てます。このオプションは、選択したすべてのサブネットに IPv4と の両方のIPv6アドレス範囲があり、エンドポイントサービスが IPv4と の両方のIPv6リクエストを受け入れる場合にのみサポートされます。

10. DNS レコード IP タイプでは、次のオプションから選択します。

    - IPv4 – プライベート、リージョン、およびゾーンDNS名のレコードを作成します。IP アドレスタイプは IPv4またはデュアルスタックである必要があります。
    - IPv6 – プライベート、リージョン、およびゾーンDNS名のAAAAレコードを作成します。IP アドレスタイプは IPv6またはデュアルスタックである必要があります。
    - デュアルスタック – プライベート、リージョン、およびゾーンDNS名の A レコードと AAAA レコードを作成します。IP アドレスのタイプは [Dualstack] である必要があります。
    - サービス定義 — プライベート、リージョン、およびゾーンDNS名用のレコードと、リージョン名とゾーンDNS名用のAAAAレコードを作成します。IP アドレスのタイプは [Dualstack] である必要があります。

11. [Security group] (セキュリティグループ) で、エンドポイントネットワークインターフェイスに関連付けるセキュリティグループを選択します。
12. [エンドポイントの作成] を選択します。

コマンドラインを使用してインターフェイスエンドポイントを作成するには

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint (Windows 用のツール PowerShell)

エンドポイントサービスを設定する

エンドポイントサービスを作成したら、その設定を更新できます。

タスク

- 許可を管理する
- 接続リクエストを承諾または拒否する
- ロードバランサーを管理する
- プライベートDNS名を関連付ける
- サポートされているリージョンを変更する

- サポートされている IP アドレスのタイプを変更する
- タグの管理

許可を管理する

アクセス許可と承認設定の組み合わせにより、エンドポイントサービスにアクセスできるサービスコンシューマー (AWS プリンシパル) を制御できます。例えば、信頼している特定のプリンシパルに許可を付与して自動的にすべての接続リクエストを承諾するか、プリンシパルのより広範なグループに許可を付与して、信頼している特定の接続リクエストを手動で承諾できます。

デフォルトでは、サービスコンシューマーはエンドポイントサービスを使用できません。特定のAWS プリンシパルがVPCエンドポイントサービスに接続するためのインターフェイスエンドポイントを作成できるようにするアクセス許可を追加する必要があります。 AWS プリンシパルのアクセス許可を追加するには、その Amazon リソースネーム () が必要ですARN。次のリストには、サポートされている AWS プリンシパルARNsの例が含まれています。

ARNs AWS プリンシパルの

AWS アカウント（ アカウント内のすべてのプリンシパルを含む ）

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

ロール

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

ユーザー

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

すべての のすべてのプリンシパル AWS アカウント

*

考慮事項

- すべてのユーザーにエンドポイントサービスにアクセスするための許可を付与し、すべてのリクエストを受け入れるようにエンドポイントサービスを設定すると、パブリック IP アドレスがなくてもロードバランサーはパブリックになります。
- アクセス許可を削除しても、エンドポイントと以前に受け入れられたサービス間の既存の接続には影響しません。

コンソールを使用してエンドポイントサービスの許可を管理するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
3. エンドポイントサービスを選択し、[Allow principals] (プリンシパルを許可) タブを選択します。
4. 許可を追加するには、[Allow principals] (プリンシパルを許可) を選択します。プリンシパルを追加する場合は、プリンシパルARNの を入力します。さらにプリンシパルを追加するには、[プリンシパルを追加] を選択します。プリンシパルの追加が完了したら、[Allow principals] (プリンシパルを許可) を選択します。
5. 許可を削除するには、プリンシパルを選択し、[Actions] (アクション)、[Delete] (削除) を選択します。確認を求められたら、**`delete`**と入力し、[削除] を選択します。

コマンドラインを使用してエンドポイントサービスの許可を追加するには

- modify-vpc-endpoint-service- アクセス許可 (AWS CLI)
- Edit-EC2EndpointServicePermission (Tools for Windows PowerShell)

接続リクエストを承諾または拒否する

アクセス許可と承認設定の組み合わせにより、エンドポイントサービスにアクセスできるサービスコンシューマー (AWS プリンシパル) を制御できます。例えば、信頼している特定のプリンシパルに許可を付与して自動的にすべての接続リクエストを承諾するか、プリンシパルのより広範なグループに許可を付与して、信頼している特定の接続リクエストを手動で承諾できます。

接続リクエストを自動的に受け入れるようにエンドポイントサービスを設定できます。それ以外の場合、手動で承諾または拒否する必要があります。接続リクエストを承諾しない場合、サービスコンシューマーはエンドポイントサービスにアクセスできません。

すべてのユーザーにエンドポイントサービスにアクセスするための許可を付与し、すべてのリクエストを受け入れるようにエンドポイントサービスを設定すると、パブリック IP アドレスがなくてもロードバランサーはパブリックになります。

接続リクエストが承認または拒否されたときに通知を受け取ることができます。詳細については、「the section called “エンドポイントサービスイベントのアラートを受け取る”」を参照してください。

コンソールを使用して承諾の設定を変更するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
3. エンドポイントサービスを選択します。
4. [Actions]、[Modify endpoint acceptance setting] の順に選択します。
5. [Acceptance required] (承認が必要) を選択または選択解除します。
6. [Save changes] (変更の保存) を選択します。

コマンドラインを使用して承諾の設定を変更するには

- modify-vpc-endpoint-service-configuration (AWS CLI)
- Edit-EC2VpcEndpointServiceConfiguration (Windows 用のツール PowerShell)

コンソールを使用して接続リクエストを承諾または拒否するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
3. エンドポイントサービスを選択します。
4. [Endpoint connections] (エンドポイント接続) タブで、エンドポイント接続を選択します。
5. 接続リクエストを承諾するには、[Actions] (アクション)、[Accept endpoint connection request] (エンドポイント接続リクエストを承諾) の順に選択します。確認を求められたら、**`accept`** と入力し、[Accept] (承諾) を選択します。
6. 接続リクエストを拒否するには、[アクション]、[エンドポイント接続リクエストを拒否] の順に選択します。確認を求められたら、**`reject`** と入力し、[Reject] (拒否) を選択します。

コマンドラインを使用して接続リクエストを承諾または拒否するには

- accept-vpc-endpoint-connections または reject-vpc-endpoint-connections (AWS CLI)
- Approve-EC2EndpointConnection または Deny-EC2EndpointConnection (Tools for Windows PowerShell)

ロードバランサーを管理する

エンドポイントサービスに関連付けられているロードバランサーを管理できます。エンドポイントサービスにエンドポイントが接続されている場合、ロードバランサーの関連付けを解除することはできません。

Network Load Balancer の別のアベイラビリティーゾーンを有効にすると、エンドポイントサービスのアベイラビリティーゾーンも有効にすることができます。エンドポイントサービスのアベイラビリティーゾーンを有効にすると、サービスコンシューマーはそのアベイラビリティーゾーンからインターフェイスVPCエンドポイントにサブネットを追加できます。

コンソールを使用してエンドポイントサービスのロードバランサーを管理するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
3. エンドポイントサービスを選択します。
4. [Actions] (アクション)、[Associate or disassociate load balancers] (ロードバランサーの関連付け/関連付けの解除) の順に選択します。
5. 必要に応じてエンドポイントサービス設定を変更します。以下に例を示します。
   - ロードバランサーのチェックボックスをオンにすると、エンドポイントサービスに関連付けられます。
   - ロードバランサーのチェックボックスをオフにすると、エンドポイントサービスとの関連付けを解除します。少なくとも 1 つのロードバランサーを選択する必要があります。
   - ロードバランサーの別のアベイラビリティーゾーンを最近有効にした場合は、[含まれるアベイラビリティーゾーン] の下に表示されます。次のステップで変更を保存すると、新しいアベイラビリティーゾーンのエンドポイントサービスが有効になります。
6. [変更を保存] を選択します。

コマンドラインを使用してエンドポイントサービスのロードバランサーを管理するには

- modify-vpc-endpoint-service-configuration (AWS CLI)
- Edit-EC2VpcEndpointServiceConfiguration (Tools for Windows PowerShell)

ロードバランサーで最近有効になったアベイラビリティーゾーンでエンドポイントサービスを有効にするには、エンドポイントサービスの ID を使用してコマンドを呼び出します。

プライベートDNS名を関連付ける

プライベートDNS名をエンドポイントサービスに関連付けることができます。プライベートDNS名を関連付けたら、DNSサーバー上のドメインのエントリを更新する必要があります。サービスコンシューマーがプライベートDNS名を使用する前に、サービスプロバイダーはドメインを所有していることを確認する必要があります。詳細については、「DNS 名前の管理」を参照してください。

コンソールを使用してエンドポイントサービスのプライベートDNS名を変更するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
3. エンドポイントサービスを選択します。
4. アクション、プライベートDNS名の変更を選択します。
5. プライベートDNS名をサービスに関連付けるを選択し、プライベートDNS名を入力します。
   - ドメイン名には小文字を使用する必要があります。
   - ドメイン名にはワイルドカードを使用できます (例: **`*.myexampleservice.com`**)。
6. [Save changes] (変更の保存) をクリックします。
7. 検証ステータスが検証されると、プライベートDNS名はサービスコンシューマーが使用できる状態になります。検証ステータスが変更された場合、新しい接続リクエストは拒否されますが、既存の接続には影響しません。

コマンドラインを使用してエンドポイントサービスのプライベートDNS名を変更するには

- modify-vpc-endpoint-service-configuration (AWS CLI)
- Edit-EC2VpcEndpointServiceConfiguration (Tools for Windows PowerShell)

コンソールを使用してドメイン検証プロセスを開始するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
3. エンドポイントサービスを選択します。
4. アクション、プライベートDNS名のドメイン所有権の検証を選択します。
5. 確認を求められたら、「**`verify`**」と入力し、[検証] を選択します。

コマンドラインを使用してドメイン検証プロセスを開始するには

- start-vpc-endpoint-service-private-dns-verification (AWS CLI)
- Start-EC2VpcEndpointServicePrivateDnsVerification (Windows 用のツール PowerShell)

サポートされているリージョンを変更する

エンドポイントサービスでサポートされているリージョンのセットを変更できます。オプトインリージョンを追加する前に、オプトインする必要があります。エンドポイントサービスをホストするリージョンを削除することはできません。

リージョンを削除すると、サービスコンシューマーはそれをサービスリージョンとして指定する新しいエンドポイントを作成できません。リージョンを削除しても、サービスリージョンとして指定する既存のエンドポイントには影響しません。リージョンを削除するときは、そのリージョンからの既存のエンドポイント接続を拒否することをお勧めします。

エンドポイントサービスでサポートされているリージョンを変更するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
3. エンドポイントサービスを選択します。
4. アクション、サポートされているリージョンの変更を選択します。
5. 必要に応じてリージョンを選択および選択解除します。
6. [Save changes] (変更の保存) をクリックします。

サポートされている IP アドレスのタイプを変更する

エンドポイントサービスでサポートされている IP アドレスのタイプを変更できます。

考慮事項

エンドポイントサービスがIPv6リクエストを受け入れることができるようにするには、Network Load Balancer でデュアルスタック IP アドレスタイプを使用する必要があります。ターゲットはIPv6トラフィックをサポートする必要はありません。詳細については、「Network Load Balancer のユーザーガイド」の「IP アドレスのタイプ」を参照してください。

コンソールを使用してサポートされている IP アドレスのタイプを変更するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
3. VPC エンドポイントサービスを選択します。
4. [Actions] (アクション)、[Modify supported IP address types] (サポートされる IP アドレスのタイプを変更) を選択します。
5. [Supported IP address types] (サポートされている IP アドレスのタイプ) で、次のいずれかを実行します。
   - 選択 IPv4 — エンドポイントサービスがIPv4リクエストを受け入れるようにします。
   - 選択 IPv6 — エンドポイントサービスがIPv6リクエストを受け入れるようにします。
   - Select IPv4 and IPv6 – エンドポイントサービスが IPv4と の両方のIPv6リクエストを受け入れるようにします。
6. [Save changes] (変更の保存) をクリックします。

コマンドラインを使用してサポートされている IP アドレスのタイプを変更するには

- modify-vpc-endpoint-service-configuration (AWS CLI)
- Edit-EC2VpcEndpointServiceConfiguration (Tools for Windows PowerShell)

タグの管理

リソースにタグを付けて、識別しやすくしたり、組織のニーズに応じて分類したりできます。

コンソールを使用してエンドポイントサービスのタグを管理するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
3. VPC エンドポイントサービスを選択します。
4. [Actions] (アクション)、[Manage tags] (タグの管理) を選択します。
5. 追加するタグごとに、[Add new tag] (新しいタグを追加) を選択し、タグキーとタグ値を入力します。
6. タグを削除するには、タグのキーと値の右側にある [Remove] (削除) を選択します。
7. [Save] を選択します。

コンソールを使用してエンドポイント接続のタグを管理するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
3. VPC エンドポイントサービスを選択し、エンドポイント接続タブを選択します。
4. エンドポイント接続を選択後、[Actions] (アクション)、[Manage tags] (タグを管理) の順に選択します。
5. 追加するタグごとに、[Add new tag] (新しいタグを追加) を選択し、タグキーとタグ値を入力します。
6. タグを削除するには、タグのキーと値の右側にある [Remove] (削除) を選択します。
7. [Save] を選択します。

コンソールを使用してエンドポイントサービスの許可のタグを管理するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
3. VPC エンドポイントサービスを選択し、プリンシパルを許可タブを選択します。
4. プリンシパルを選択し、[Actions] (アクション)、[Manage tags] (タグを管理) の順に選択します。
5. 追加するタグごとに、[Add new tag] (新しいタグを追加) を選択し、タグキーとタグ値を入力します。
6. タグを削除するには、タグのキーと値の右側にある [Remove] (削除) を選択します。
7. [Save] を選択します。

コマンドラインを使用してタグを追加および削除するには

- create-tags および delete-tags (AWS CLI)
- New-EC2Tag および Remove-EC2Tag (Tools for Windows PowerShell)

VPC エンドポイントサービスDNSの名前を管理する

サービスプロバイダーは、エンドポイントサービスのプライベートDNS名を設定できます。サービスプロバイダーがパブリックエンドポイントを介して、エンドポイントサービスとしてサービスを利

用できるようにするとします。サービスプロバイダーがパブリックエンドポイントDNSの名前をエンドポイントサービスのプライベートDNS名として使用している場合、サービスコンシューマーは同じクライアントアプリケーションを使用してパブリックエンドポイントまたはエンドポイントサービスに変更を加えることなくアクセスできます。リクエストがサービスコンシューマー から送信された場合VPC、プライベートDNSサーバーはDNS名前をエンドポイントネットワークインターフェイスの IP アドレスに解決します。それ以外の場合、パブリックDNSサーバーはパブリックエンドポイントにDNS名前を解決します。

エンドポイントサービスのプライベートDNS名を設定する前に、ドメインの所有権の検証チェックを実行して、ドメインを所有していることを証明する必要があります。

考慮事項

- エンドポイントサービスにはプライベートDNS名を 1 つだけ含めることができます。
- コンシューマーがサービスに接続するためのインターフェイスエンドポイントを作成すると、プライベートホストゾーンが作成され、サービスコンシューマー に関連付けられますVPC。エンドポイントサービスのプライベートDNS名をエンドポイントのリージョンDNS名にマッピングするCNAMEレコードをプライベートホストゾーンに作成しますVPC。コンシューマーがサービスのパブリックDNS名にリクエストを送信すると、プライベートDNSサーバーはエンドポイントネットワークインターフェイスの IP アドレスにリクエストを解決します。
- ドメインを検証するには、パブリックホスト名またはパブリックDNSプロバイダーが必要です。
- サブドメインのドメインを検証できます。たとえば、a.example.com ではなく、 example.comを検証できます。各DNSラベルは最大 63 文字で、ドメイン名全体が合計 255 文字を超えることはできません。

  追加のサブドメインを追加する場合は、サブドメインまたはドメインを検証する必要があります。たとえば、a.example.com があり、example.com を検証したとします。b.example.com をプライベートDNS名として追加します。サービスコンシューマーがこの名前を使用できるようにするには、example.com または b.example.com を検証する必要があります。
- プライベートDNS名は Gateway Load Balancer エンドポイントではサポートされていません。

ドメインの所有権の検証

ドメインは、DNSプロバイダーを通じて管理する一連のドメイン名サービス (DNS) レコードに関連付けられます。TXT レコードは、ドメインに関する追加情報を提供するDNSレコードの一種です。名前と値から構成されます。検証プロセスの一環として、パブリックドメインのDNSサーバーにTXTレコードを追加する必要があります。

ドメインDNSの設定でTXTレコードの存在が検出されると、ドメインの所有権の検証は完了です。

レコードを追加したら、Amazon VPCコンソールを使用してドメイン検証プロセスのステータスを確認できます。ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。エンドポイントサービスを選択し、[Details] (詳細) タブで [Domain verification status] (ドメイン検証ステータス) の値を確認します。ドメイン検証が保留中の場合は、数分待ってから画面を更新してください。必要に応じて、検証プロセスを手動で開始できます。アクション、プライベートDNS名のドメイン所有権の検証を選択します。

検証ステータスが検証されると、プライベートDNS名はサービスコンシューマーが使用できる状態になります。検証ステータスが変更された場合、新しい接続リクエストは拒否されますが、既存の接続には影響しません。

検証ステータスが [failed] (失敗) の場合は、「the section called “ドメインの検証に関する問題をトラブルシューティングする”」を参照してください。

名前と値を取得する

TXT レコードで使用する名前と値が提供されています。例えば、情報は AWS Management Console で入手できます。エンドポイントサービスを選択し、エンドポイントサービスの [Details] (詳細) タブで、[Domain verification name] (ドメイン検証名) と [Domain verification value] (ドメイン検証値) を確認します。次の describe-vpc-endpoint-service-configurations AWS CLI コマンドを使用して、指定されたエンドポイントサービスのプライベートDNS名の設定に関する情報を取得することもできます。

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

以下は出力例です。TXT レコードを作成するNameときは、 Valueと を使用します。

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

例えば、ドメイン名が example.com で、`Value` と `Name` が前述の出力例に示されているとします。次の表は、TXTレコード設定の例です。

名前	タイプ	値
_6e86v84tqgqubxbwii1m.example.com	TXT	vpce:l6p0ERxlTt45jevFwOCp

ベースドメイン名が既に使用されている可能性があるため、レコードサブドメインとして `Name` を使用することをお勧めします。ただし、DNSプロバイダーがDNSレコード名にアンダースコアを含めることを許可していない場合は、「_6e86v84tqgqubxbwii1m」を省略し、TXTレコードに「example.com」を使用できます。

「_6e86v84tqgqubxbwii1m.example.com」を検証したら、サービスコンシューマーは「example.com」またはサブドメイン (「service.example.com」や「my.service.example.com」など) を使用できます。

ドメインのDNSサーバーにTXTレコードを追加する

ドメインのDNSサーバーにTXTレコードを追加する手順は、DNSサービスを提供するユーザーによって異なります。DNS プロバイダーは Amazon Route 53 または別のドメイン名レジストラである可能性があります。

Amazon Route 53

パブリックホストゾーンのレコードを作成します。以下の値を使用します。

- レコードタイプで、 を選択しますTXT。
- TTL (秒) には、 と入力します**1800**。
- [ルーティングポリシー] で、[シンプルルーティング] を選択します。
- [Record name] (レコード名) で、ドメインまたはサブドメインを入力します。
- [Value/Route traffic to] (値/トラフィックのルーティング先) には、ドメイン検証の値を入力します。

詳細については、「Amazon Route 53 デベロッパーガイド」の「Create records using the console」(コンソールを使用してレコードを作成する) を参照してください。

一般的な手順

DNS プロバイダーのウェブサイトに移動し、アカウントにサインインします。ドメインのDNSレコードを更新するページを見つけます。指定した名前と値を持つTXTレコードを追加します。DNS レコードの更新が有効になるまでに最大 48 時間かかることがありますが、多くの場合、より早く有効になります。

具体的な手順については、DNSプロバイダーのドキュメントを参照してください。次の表に、いくつかの一般的なDNSプロバイダーのドキュメントへのリンクを示します。このリストは、包括的であることを意図されたものではなく、これらの企業が提供する製品またはサービスの推奨を目的としたものでもありません。

DNS/ホスティングプロバイダー	ドキュメントのリンク
GoDaddy	TXTレコードを追加する
Dreamhost	カスタムDNSレコードの追加
Cloudflare	DNSレコードの管理
HostGator	HostGator/ を使用してDNSレコードを管理するeNom
Namecheap	ドメインのTXT/SPF/DKIM/DMARCレコードを追加する方法
Names.co.uk	ドメインDNSの設定の変更
Wix	Wix アカウントでのTXTレコードの追加または更新

TXT レコードが公開されているかどうかを確認する

次の手順を使用して、プライベートDNSネームドメインの所有権検証TXTレコードがDNSサーバーに正しく発行されていることを確認できます。Windows および Linux で使用できる nslookup コマンドを実行します。

ドメインにサービスを提供するDNSサーバーをクエリします。これらのサーバーにはドメインの最新情報 up-to-dateが含まれているためです。ドメイン情報が他のDNSサーバーに伝達されるまでに時間がかかります。

TXT レコードがDNSサーバーに発行されていることを確認するには

1. 次のコマンドを使用して、ドメインのネームサーバーを見つけます。

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

   出力に、ドメインにサービスを提供しているネームサーバーが示されます。次のステップで、これらのサーバーのいずれかをクエリします。

2. 次のコマンドを使用してTXTレコードが正しく発行されていることを確認します。ここで、*name_server*は前のステップで見つけたネームサーバーの 1 つです。

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

3. 前のステップの出力で、後続の文字列がTXT値`text =`と一致することを確認します。

   この例では、レコードが正しく発行されている場合、出力には次が含まれます。

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

ドメインの検証に関する問題をトラブルシューティングする

ドメインの検証プロセスが失敗した場合、次の情報は問題をトラブルシューティングするのに役立ちます。

- DNS プロバイダーがTXTレコード名にアンダースコアを許可しているかどうかを確認します。DNS プロバイダーがアンダースコアを許可していない場合は、ドメイン検証名 (例: "_6e86v84tqgqubxbwii1m") をTXTレコードから省略できます。
- DNS プロバイダーがドメイン名をTXTレコードの末尾に追加したかどうかを確認します。一部のDNSプロバイダーは、ドメインの名前をTXTレコードの属性名に自動的に追加します。ドメイン名の重複を回避するには、TXTレコードの作成時にドメイン名の末尾にピリオドを追加します。これにより、ドメイン名をTXTレコードに追加する必要がないことがDNSプロバイダーに通知されます。
- DNS プロバイダーが小文字のみを使用するようにDNSレコード値を変更したかどうかを確認します。提供された値と完全に一致する属性値を持つ検証レコードがある場合にのみ、ドメインを検証します。DNS プロバイダーがTXTレコード値を小文字のみを使用するように変更した場合は、サポートを依頼してください。

- 複数のリージョンまたは複数の AWS アカウントをサポートしているため、ドメインを複数回確認する必要がある場合があります。DNS プロバイダーが同じ属性名を持つ複数のTXTレコードを持つことを許可していない場合は、DNSプロバイダーが同じTXTレコードに複数の属性値を割り当てることができるかどうかを確認します。例えば、 DNSが Amazon Route 53 によって管理されている場合、次の手順を使用できます。

  1. Route 53 コンソールで、最初のリージョンでドメインを検証したときに作成したTXTレコードを選択します。
  2. [Value] (値) で、既存の属性値の末尾に移動し、Enter キーを押します。
  3. 追加のリージョンの属性値を追加し、レコードセットを保存します。

  DNS プロバイダーで同じTXTレコードに複数の値を割り当てることが許可されていない場合は、TXTレコードの属性名の 値で 1 回、属性名から削除された値で 1 回ドメインを検証できます。ただし、同じドメインは 2 回まで検証できます。

エンドポイントサービスイベントのアラートを受け取る

通知を作成して、エンドポイントサービスに関連する特定のイベントに関するアラートを受信できます。例えば、接続リクエストが承諾または拒否されたときに E メールを受信できます。

タスク

- SNS 通知を作成する
- アクセスポリシーを追加する
- キーポリシーを追加

SNS 通知を作成する

次の手順を使用して、通知用の Amazon SNSトピックを作成し、トピックをサブスクライブします。

コンソールを使用してエンドポイントサービスの通知を作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
3. エンドポイントサービスを選択します。
4. [Notifications] (通知) タブで、[Create notification] (通知の作成) を選択します。

5. 通知 ARNで、作成したSNSトピックARNの を選択します。
6. イベントをサブスクライブするには、[Events] (イベント) から選択します。
   - [Connect] (接続) – サービスコンシューマーがインターフェイスエンドポイントを作成しました。これは、接続リクエストをサービスプロバイダーに送信します。
   - [Accept] (承諾) – サービスプロバイダーが接続リクエストを受け入れました。
   - [Reject] (拒否) – サービスプロバイダーが接続リクエストを拒否しました。
   - [Delete] (削除) — サービスコンシューマーがインターフェイスエンドポイントを削除しました。
7. [通知を作成] を選択します。

コマンドラインを使用してエンドポイントサービスの通知を作成するには

- create-vpc-endpoint-connection通知 (AWS CLI)
- New-EC2VpcEndpointConnectionNotification (Windows 用のツール PowerShell)

アクセスポリシーを追加する

次のような通知をユーザーに代わって AWS PrivateLink が発行できるようにするアクセスポリシーを SNSトピックに追加します。詳細については、「Amazon SNSトピックのアクセスポリシーを編集するにはどうすればよいですか？」を参照してください。`aws:SourceArn` および `aws:SourceAccount` グローバル条件キーを使用して、混乱した代理問題に対して保護します。

```
{
  "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"
        }
      }
    }
  ]
}
```

キーポリシーを追加

暗号化されたSNSトピックを使用している場合、 オペレーションを呼び出す AWS KMS APIには、KMSキーのリソースポリシーが AWS PrivateLink を信頼する必要があります。以下は、キーポリシーの例です。

```
{
  "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"
        }
      }
    }
  ]
}
```

エンドポイントサービスを削除する

不要になったエンドポイントサービスは、削除することができます。`available` または `pending-acceptance` 状態のエンドポイントサービスに接続されているエンドポイントがある場合、エンドポイントサービスを削除することはできません。

エンドポイントサービスを削除しても、関連付けられているロードバランサーは削除されず、ロードバランサーのターゲットグループに登録されているアプリケーションサーバーには影響しません。

コンソールを使用してエンドポイントサービスを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
3. エンドポイントサービスを選択します。
4. [アクション]、[エンドポイントサービスを削除] の順に選択します。
5. 確認を求められたら、**delete**と入力し、[削除] を選択します。

コマンドラインを使用してエンドポイントサービスを削除するには

- delete-vpc-endpoint-service- 設定 (AWS CLI)
- Remove-EC2EndpointServiceConfiguration (Windows 用のツール PowerShell)

経由で VPCリソースにアクセスする AWS PrivateLink

リソースVPCエンドポイント (VPCリソースエンドポイント) VPCを使用して、別の のリソースにプライベートにアクセスできます。リソースエンドポイントを使用すると、データベース、ノードのクラスター、インスタンス、アプリケーションエンドポイント、ドメイン名ターゲット、または別の VPC またはオンプレミス環境のプライベートサブネットにある IP アドレスなどのVPCリソースにプライベートかつ安全にアクセスできます。リソースエンドポイントがない場合は、インターネットゲートウェイを に追加するVPCか、 AWS PrivateLink インターフェイスエンドポイントと Network Load Balancer を使用してリソースにアクセスする必要があります。リソースエンドポイントはロードバランサーを必要としないため、VPCリソースに直接アクセスできます。VPC リソースはリソース設定で表されます。リソース設定はリソースゲートウェイに関連付けられています。

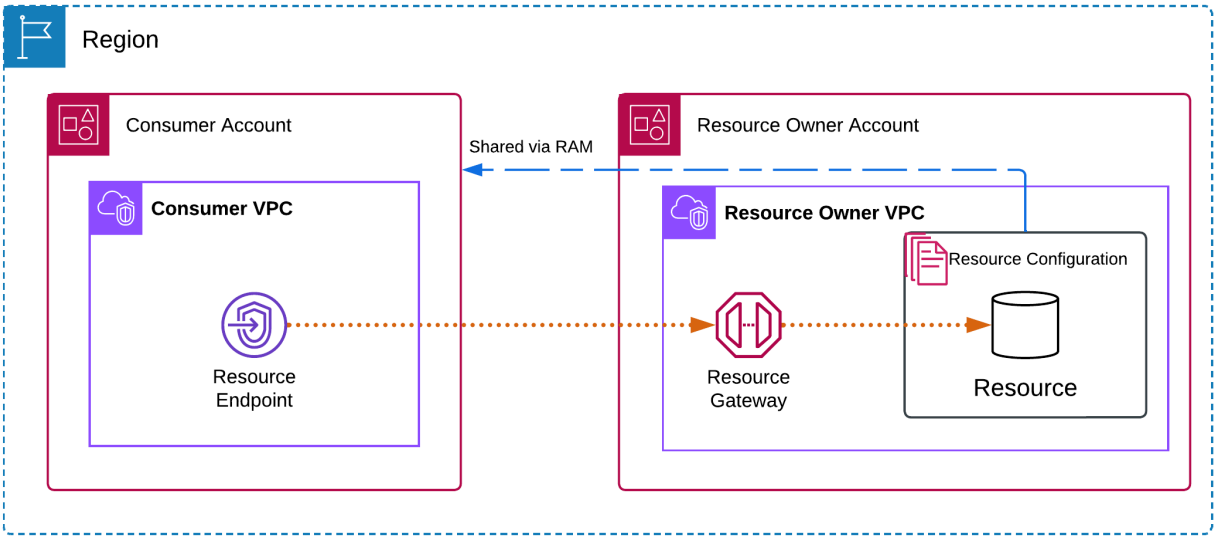
料金

リソースエンドポイントを使用してリソースにアクセスすると、リソースVPCエンドポイントがプロビジョニングされる 1 時間ごとに課金されます。また、 リソースにアクセスすると、処理されるデータの GB ごとに課金されます。詳細については、AWS PrivateLink の料金を参照してください。リソース設定とリソースゲートウェイを使用してリソースへのアクセスを有効にすると、リソースゲートウェイによって処理された GB ごとのデータに対して課金されます。詳細については、Amazon VPC Lattice の料金を参照してください。

内容

概要

アカウントのリソース、または別のアカウントから共有されているリソースにアクセスできます。リソースにアクセスするには、リソースVPCエンドポイントを作成します。これにより、ネットワークインターフェイスを使用して、 内のサブネットVPCとリソース間の接続が確立されます。リソース宛てのトラフィックは、 を使用してリソースエンドポイントのネットワークインターフェイスのプライベート IP アドレスに解決されDNS、リソースゲートウェイを介してVPCエンドポイントとリソース間の接続を使用してリソースに送信されます。



考慮事項

- TCP トラフィックがサポートされています。 UDPトラフィックはサポートされていません。
- ネットワーク接続は、リソースVPCエンドポイントを含む から開始する必要があり、リソースVPCを含む から開始することはできません。リソースの VPCは、エンドポイント へのネットワーク接続を開始できませんVPC。
- サポートされている ARNベースのリソースは Amazon RDSリソースのみです。

DNS ホスト名

では AWS PrivateLink、プライベートエンドポイントを使用して リソースにトラフィックを送信します。リソースVPCエンドポイントを作成すると、 VPCおよびオンプレミスからリソースと通信するために使用できるリージョンDNS名 (デフォルトDNS名と呼ばれる) が作成されます。リソースVPCエンドポイントのデフォルトDNS名には、次の構文があります。

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

を使用する一部のリソース設定のリソースVPCエンドポイントを作成するときにARNs、プライベート DNSを有効にできます。プライベート ではDNS、リソースVPCエンドポイントを介したプライベート接続を活用しながら、 AWS サービスによってリソースにプロビジョニングされたDNS名前を使用してリソースへのリクエストを続行できます。詳細については、「the section called “DNS 解像度”」を参照してください。

次のdescribe-vpc-endpoint-associationsコマンドは、リソースエンドポイントのDNSエントリを表示します。

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

プライベートDNS名が有効になっている Amazon RDS データベースのリソースエンドポイントの出力例を次に示します。最初のエントリはデフォルトDNS名です。2 番目のエントリは、パブリックエンドポイントへのリクエストをエンドポイントネットワークインターフェイスのプライベート IP アドレスに解決する、隠しプライベートホストゾーンからのエントリです。

```
"DnsEntry": {
                "DnsName": "vpce-1234567890abcdefg-
snra-1234567890abcdefg.rcfg-abcdefgh123456789.4232ccc.vpc-lattice-rsc.us-
east-1.on.aws",
                "HostedZoneId": "ABCDEFGH123456789000"
            },
"PrivateDnsEntry": {
                "DnsName": "database-5-test.cluster-ro-example.us-
east-1.rds.amazonaws.com",
                "HostedZoneId": "A1B2CD3E4F5G6H8I91234"
            }
```

DNS 解像度

リソースVPCエンドポイント用に作成するDNSレコードはパブリックです。したがって、これらのDNS名前はパブリックに解決可能です。ただし、 の外部からのDNSリクエストVPCは、リソースエンドポイントのネットワークインターフェイスのプライベート IP アドレスを返します。これらのDNS名前を使用して、リソースエンドポイントVPCがある 、、VPNまたは Direct Connect にアクセスできる限り、オンプレミスからリソースにアクセスできます。

プライベート DNS

リソースVPCエンドポイントDNSでプライベートを有効にし、 VPCでDNSホスト名とDNS解像度の両方が有効になっている場合、カスタムDNS名を使用してリソース設定の非表示 AWSのマネージドプライベートホストゾーンが作成されます。ホストゾーンには、リソースのデフォルトDNS名のレコードセットが含まれており、 のリソースエンドポイントのネットワークインターフェイスのプライベート IP アドレスに解決されますVPC。

Amazon はVPC、Route 53 Resolver と呼ばれる 用のDNSサーバーを提供しています。Route 53 Resolver は、プライベートホストゾーンのローカルVPCドメイン名とレコードを自動的に解決します。ただし、 の外部から Route 53 Resolver を使用することはできませんVPC。オンプレミスネットワークからVPCエンドポイントにアクセスする場合は、デフォルトDNS名を使用するか、Route 53 Resolver エンドポイントと Resolver ルールを使用できます。詳細については、「 AWS Transit GatewayAWS PrivateLink と の統合 Amazon Route 53 Resolver」を参照してください。

サブネットとアベイラビリティーゾーン

アベイラビリティーゾーンごとに 1 つのサブネットを使用してVPCエンドポイントを設定できます。サブネット内のエンドポイントのVPCエンドポイントネットワークインターフェイスを作成します。エンドポイントの IP アドレスタイプに基づいて、サブネットから各エンドポイントネットワークインターフェイスに IP アドレスを割り当てます。 VPC各サブネットに割り当てられる IP アドレスの数は、リソース設定の数によって異なります。本稼働環境では、高可用性と耐障害性を実現するために、VPCエンドポイントごとに少なくとも 2 つのアベイラビリティーゾーンを設定することをお勧めします。

IP アドレスのタイプ

リソースエンドポイントは、IPv4、IPv6、またはデュアルスタックアドレスをサポートできます。をサポートするエンドポイントは、 AAAAレコードでDNSクエリに応答IPv6できます。リソースエンドポイントの IP アドレスタイプは、以下で説明するように、リソースエンドポイントのサブネットと互換性がある必要があります。

- IPv4 – エンドポイントネットワークインターフェイスにIPv4アドレスを割り当てます。このオプションは、選択したすべてのサブネットにIPv4アドレス範囲がある場合にのみサポートされます。
- IPv6 – エンドポイントネットワークインターフェイスにIPv6アドレスを割り当てます。このオプションは、選択したすべてのサブネットがサブネットIPv6のみの場合にのみサポートされます。

- デュアルスタック — エンドポイントネットワークインターフェイスに IPv4と IPv6 アドレスの両方を割り当てます。このオプションは、選択したすべてのサブネットに IPv4と の両方のIPv6アドレス範囲がある場合にのみサポートされます。

リソースVPCエンドポイントが をサポートしている場合IPv4、エンドポイントネットワークインターフェイスには IPv4 アドレスがあります。リソースVPCエンドポイントが をサポートしている場合IPv6、エンドポイントネットワークインターフェイスには IPv6 アドレスがあります。エンドポイントネットワークインターフェイスのIPv6アドレスにインターネットからアクセスできません。IPv6 アドレスを使用してエンドポイントネットワークインターフェイスを記述する場合は、`denyAllIgwTraffic` が有効になっていることに注意してください。

リソースVPCエンドポイントを介してリソースにアクセスする

VPC リソースエンドポイントを使用して、ドメイン名、IP アドレス、Amazon RDS データベースなどのリソースにアクセスできます。リソースエンドポイントは、リソースへのプライベートアクセスを提供します。リソースエンドポイントを作成するときは、シングル、グループ、または タイプのリソース設定を指定しますARN。リソースエンドポイントは、1 つのリソース設定にのみ関連付けることができます。リソース設定は、単一のリソースまたはリソースのグループを表すことができます。

前提条件

リソースエンドポイントを作成するには、次の前提条件を満たす必要があります。

- 自分が作成したリソース設定、または を通じて別のアカウントから共有されたリソース設定が必要です AWS RAM。
- リソース設定が別のアカウントから共有されている場合は、リソース設定を含むリソース共有を確認して承諾する必要があります。詳細については、「AWS RAM ユーザーガイド」の「招待の承諾と拒否」を参照してください。

VPC リソースエンドポイントを作成する

VPC リソースエンドポイントを作成するには、次の手順に従います。

VPC リソースエンドポイントを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。

2. ナビゲーションペインで、[エンドポイント] を選択します。
3. [エンドポイントの作成] を選択します。
4. エンドポイントを見つけて管理しやすくするために、名前を指定できます。
5. Type で、Resources を選択します。
6. リソース設定で、共有されたリソース設定を選択します。
7. ネットワーク設定で、リソースにアクセスする VPC を選択します。
8. プライベートDNSサポートを設定する場合は、「追加設定」、DNS「名前を有効にする」を選択します。この機能を使用するには、 属性 DNSホスト名を有効にする と DNS サポートを有効にする で が有効になっていることを確認しますVPC。
9. [エンドポイントの作成] を選択します。

コマンドラインを使用してリソースエンドポイントを作成するには

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint (Tools for Windows PowerShell)

リソースエンドポイントの管理

リソースエンドポイントを作成したら、その設定を更新できます。

タスク

- エンドポイントを削除します
- エンドポイントを更新します。

エンドポイントを削除します

VPC エンドポイントの使用が終了したら、削除できます。

コンソールを使用してエンドポイントを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. エンドポイントを選択します。
4. アクション、VPCエンドポイントの削除を選択します。

5. 確認を求められたら、**delete** をクリックします。
6. [削除] を選択します。

コマンドラインを使用してエンドポイントを削除するには

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint (Windows 用のツール PowerShell)

エンドポイントを更新します。

VPC エンドポイントを更新できます。

コンソールを使用してエンドポイントを更新するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. エンドポイントを選択します。
4. アクションを選択し、適切なオプションを選択します。
5. コンソールの手順に従って更新を送信します。

コマンドラインを使用してエンドポイントを更新するには

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint (Windows 用のツール PowerShell)

リソースのVPCリソース設定

リソース設定は、他の VPCsおよびアカウントのクライアントにアクセスできるようにするリソースまたはリソースのグループを表します。リソース設定を定義することで、他の VPCsおよび アカウントのクライアントVPCから のリソースへのプライベートで安全な単一方向のネットワーク接続を許可できます。リソース設定は、トラフィックを受信するリソースゲートウェイに関連付けられます。

内容

- リソース設定のタイプ

- リソースゲートウェイ
- リソース定義
- プロトコル
- ポート範囲
- リソースへのアクセス
- サービスネットワークタイプとの関連付け
- サービスネットワークのタイプ
- を使用したリソース設定の共有 AWS RAM
- モニタリング
- Lattice VPC でリソース設定を作成する
- Lattice VPC リソース設定の関連付けを管理する

リソース設定のタイプ

リソース設定には、いくつかのタイプがあります。さまざまなタイプは、さまざまな種類のリソースを表すのに役立ちます。タイプは次のとおりです。

- 単一リソース設定: IP アドレスまたはドメイン名。個別に共有できます。
- グループリソース設定: ノードのクラスターを表す子リソース設定のコレクション。個別に共有できます。
- 子リソース設定: グループリソース設定のメンバー。IP アドレスまたはドメイン名を表します。個別に共有することはできません。また、グループの一部としてのみ共有できます。グループからシームレスに追加および削除できます。追加すると、グループにアクセスできるユーザーが自動的にアクセスできるようになります。
- ARN リソース設定: AWS サービスによってプロビジョニングされるサポートされているリソースタイプを表します。子リソース設定は によって自動的に管理されます AWS。

リソースゲートウェイ

リソース設定はリソースゲートウェイに関連付けられています。リソースゲートウェイは、リソースVPCがある への進入ポイントENIsとして機能する のセットです。複数のリソース設定を同じリソースゲートウェイに関連付けることができます。他の VPCsまたは アカウントのクライアントが のリソースにアクセスするとVPC、リソースはその のリソースゲートウェイからローカルに送信されるトラフィックを確認しますVPC。

リソース定義

リソース設定で、次のいずれかの方法でリソースを識別します。

- Amazon リソースネーム別 (ARN) : AWS サービスによってプロビジョニングされるサポートされているリソースタイプは、 によって識別できますARN。例えば、Amazon RDS データベースなどです。
- ドメイン名ターゲット別: パブリックに解決可能な任意のドメイン名。
- IP アドレスによる: IPv4および ではIPv6、 IPsでのみサポートVPCされます。

プロトコル

リソース設定を作成するときに、リソースがサポートするプロトコルを定義できます。現在、 TCP プロトコルのみがサポートされています。

ポート範囲

リソース設定を作成するときに、リクエストを受け入れるポートを定義できます。他のポートでのクライアントアクセスは許可されません。

リソースへのアクセス

コンシューマーは、VPCエンドポイントまたはサービスネットワークVPCを使用して、 からリソース設定に直接アクセスできます。コンシューマーは、 から、自分のアカウントにあるリソース設定VPC、または を介して別のアカウントから共有されているリソース設定へのアクセスを有効にすることができます AWS RAM。

- リソース設定に直接アクセスする

  でリソースタイプ (リソースエンドポイント) のエンドポイントを作成して AWS PrivateLink VPCVPC、 からリソース設定にプライベートにアクセスできますVPC。リソースエンドポイントの作成方法の詳細については、「 AWS PrivateLinkユーザーガイド」の「 VPCリソースへのアクセス」を参照してください。
- サービスネットワークを介したリソース設定へのアクセス

  リソース設定をサービスネットワークに関連付け、 VPCをサービスネットワークに接続できます。VPC をサービスネットワークに接続するには、関連付けを使用するか、 AWS PrivateLink サービスネットワークVPCエンドポイントを使用します。

サービスネットワークの関連付けの詳細については、「Lattice VPC サービスネットワークの関連付けを管理する」を参照してください。

サービスネットワークVPCエンドポイントの詳細については、 AWS PrivateLink ユーザーガイドの「サービスネットワークへのアクセス」を参照してください。

サービスネットワークタイプとの関連付け

リソース設定をコンシューマーアカウントと共有する場合、例えば Account-B は を介して AWS RAM、リソースVPCエンドポイントまたはサービスネットワークを介してリソース設定に直接アクセスできます。

サービスネットワークを介してリソース設定にアクセスするには、Account-B はリソース設定をサービスネットワークに関連付ける必要があります。サービスネットワークはアカウント間で共有できます。したがって、Account-B はサービスネットワーク (リソース設定が関連付けられている) を Account-C と共有し、Account-C からリソースにアクセスできるようにします。

このような推移的な共有を防ぐために、アカウント間で共有可能なサービスネットワークにリソース設定を追加できないように指定できます。これを指定すると、Account-B は、共有されているサービスネットワークにリソース設定を追加したり、将来別のアカウントと共有したりできなくなります。

サービスネットワークのタイプ

リソース設定を Account-B などの別のアカウントと共有する場合、Account-B は AWS RAM 3 つの方法のいずれかでリソースにアクセスできます。

- リソースタイプ (リソースVPCエンドポイント) のVPCエンドポイントの使用。
- タイプのサービスネットワーク (サービスネットワークVPCエンドポイント) のVPCエンドポイントを使用する。
- サービスネットワークのVPC関連付けの使用。

サービスネットワークVPCエンドポイントとサービスネットワークのVPC関連付けでは、リソース設定をアカウント B のサービスネットワークに配置する必要があります。 サービスネットワークはアカウント間で共有できます。したがって、Account-B はサービスネットワーク (リソース設定を含む) を Account-C と共有し、Account-C からリソースにアクセスできるようにします。 このような推移的な共有を防ぐために、アカウント間で共有可能なサービスネットワークにリソース設定が追加されないようにすることができます。これを禁止すると、Account-B は、共有されているサービス

ネットワークまたは別のアカウントと共有できるサービスネットワークにリソース設定を追加できなくなります。

を使用したリソース設定の共有 AWS RAM

リソース設定は と統合されています AWS Resource Access Manager。を介して、リソース設定を別のアカウントと共有できます AWS RAM。リソース設定を AWS アカウントと共有すると、そのアカウントのクライアントはリソースにプライベートにアクセスできます。のリソース共有を使用して、リソース設定を共有できます AWS RAM。

AWS RAM コンソールを使用して、追加されたリソース共有、アクセスできる共有リソース、およびリソースを共有している AWS アカウントを表示します。詳細については、「 AWS RAM ユーザーガイド」の「共有されているリソース」を参照してください。

リソース設定VPCと同じアカウントの別の からリソースにアクセスするには、リソース設定を共有する必要はありません AWS RAM。

モニタリング

リソース設定でモニタリングログを有効にできます。ログの送信先を選択できます。

Lattice VPC でリソース設定を作成する

コンソールを使用してリソース設定を作成します。

コンソールを使用してリソース設定を作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインの PrivateLink と Lattice で、リソース設定を選択します。
3. リソース設定の作成 を選択します。
4. AWS アカウント内で一意の名前を入力します。リソース設定の作成後にこの名前を変更することはできません。
5. 設定タイプで、単一または子リソースのリソースまたは子リソースのグループのリソースを選択します。
6. 以前に作成したリソースゲートウェイを選択するか、今すぐ作成します。
7. このリソース設定が表すリソースの識別子を選択します。
8. リソースを共有するポート範囲を選択します。

9. 関連付け設定で、このリソース設定を共有可能なサービスネットワークに関連付けることができるかどうかを指定します。
10. 共有リソース設定で、このリソースにアクセスできるプリンシパルを識別するリソース共有を選択します。
11. (オプション) リソース設定に対するリクエストとレスポンスをモニタリングする場合は、モニタリングでリソースアクセスログと配信先を有効にします。
12. (オプション) タグを追加するには、[新しいタグを追加] を選択し、そのタグのキーと値を入力します。
13. リソース設定の作成 を選択します。

を使用してリソース設定を作成するには AWS CLI

create-resource-configuration コマンドを使用します。

Lattice VPC リソース設定の関連付けを管理する

リソース設定を共有するコンシューマーアカウントとアカウントの およびクライアントは、リソースVPCエンドポイントを直接使用するか、サービスネットワークエンドポイントを介してリソース設定にアクセスできます。その結果、リソース設定にはエンドポイントの関連付けとサービスネットワークの関連付けが含まれます。

サービスネットワークの関連付けを管理する

サービスネットワークの関連付けを作成または削除します。

コンソールを使用してサービスネットワークの関連付けを管理するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインの PrivateLink と Lattice で、リソース設定を選択します。
3. リソース設定の名前を選択して、その詳細ページを開きます。
4. サービスネットワークの関連付けタブを選択します。
5. [関連付けを作成] を選択します。
6. VPC Lattice サービスネットワークからサービスネットワークを選択します。サービスネットワークを作成するには、Lattice VPC ネットワークの作成を選択します。
7. (オプション) タグを追加するには、[サービス関連付けのタグ] を展開して、[新しいタグを追加] を選択し、タグキーとタグ値を入力します。

8. [Save changes] (変更の保存) をクリックします。
9. 関連付けを削除するには、関連付けのチェックボックスを選択し、アクション、削除を選択します。確認を求められたら、**confirm**と入力し、[削除] を選択します。

を使用してサービスネットワークの関連付けを作成するには AWS CLI

create-service-network-resource-association コマンドを使用します。

を使用してサービスネットワークの関連付けを削除するには AWS CLI

delete-service-network-resource-association コマンドを使用します。

VPC エンドポイントの関連付けを管理する

VPC エンドポイントの関連付けを管理します。

コンソールを使用してVPCエンドポイントの関連付けを管理するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインの PrivateLink と Lattice で、リソース設定を選択します。
3. リソース設定の名前を選択して、その詳細ページを開きます。
4. エンドポイントの関連付けタブを選択します。
5. 関連付け ID を選択して、詳細ページを開きます。ここから、関連付けを変更または削除できます。
6. 新しいエンドポイントの関連付けを作成するには、左側のナビゲーションペインのPrivateLink「」と「Lattice」に移動し、「エンドポイント」を選択します。
7. エンドポイントの作成 を選択します。
8. に接続するリソース設定を選択しますVPC。
9. VPC、サブネット、およびセキュリティグループを選択します。
10. (オプション) VPCエンドポイントにタグを付けるには、新しいタグを追加を選択し、タグキーとタグ値を入力します。
11. [エンドポイントの作成] を選択します。

を使用してVPCエンドポイントの関連付けを作成するには AWS CLI

create-vpc-endpoint コマンドを使用します。

を使用してVPCエンドポイントの関連付けを削除するには AWS CLI

delete-vpc-endpoint コマンドを使用します。

Lattice VPC のリソースゲートウェイ

リソースゲートウェイは、VPCリソースが存在する への進入ポイントです。複数のアベイラビリティーゾーンにまたがります。リソースにすべてのアベイラビリティーゾーンからアクセスできるようにするには、できるだけ多くのアベイラビリティーゾーンにまたがるリソースゲートウェイを作成する必要があります。

内のリソースを他の VPCsまたは アカウントからVPCアクセスできるようにする場合は、 にリソースゲートウェイVPCが必要です。共有するすべてのリソースは、リソースゲートウェイに関連付けられます。他の VPCsまたは アカウントのクライアントが のリソースにアクセスするとVPC、リソースはその のリソースゲートウェイからローカルに送信されるトラフィックを確認しますVPC。トラフィックのソース IP は、リソースゲートウェイの IP です。リソースゲートウェイに複数の IP アドレスを割り当てることで、リソースとのネットワーク接続を増やすことができます。内の複数のリソースを同じリソースゲートウェイに関連付けるVPCことができます。

リソースゲートウェイは、負荷分散機能を提供しません。

内容

- セキュリティグループ
- IP アドレスのタイプ
- Lattice VPC でリソースゲートウェイを作成する
- Lattice VPC でリソースゲートウェイを削除する

セキュリティグループ

セキュリティグループをリソースゲートウェイにアタッチできます。リソースゲートウェイのセキュリティグループルールは、リソースゲートウェイからリソースへのアウトバウンドトラフィックを制御します。

リソースゲートウェイからデータベースリソースに流れるトラフィックに推奨されるアウトバウンドルール

リソースゲートウェイからリソースにトラフィックを流れるには、リソースで受け入れられるリスナープロトコルとポート範囲のアウトバウンドルールを作成する必要があります。

デスティネーション	プロトコル	ポート範囲	コメント
CIDR range for resource	TCP	3306	リソースゲートウェイからデータベースへのトラフィックを許可します。

IP アドレスのタイプ

リソースゲートウェイにはIPv4、、、IPv6またはデュアルスタックのアドレスを含めることができます。リソースゲートウェイの IP アドレスタイプは、以下で説明するように、リソースゲートウェイのサブネットおよびリソースの IP アドレスタイプと互換性がある必要があります。

- IPv4 – ゲートウェイネットワークインターフェイスにIPv4アドレスを割り当てます。このオプションは、選択したすべてのサブネットにIPv4アドレス範囲があり、リソースにもIPv4アドレスがある場合にのみサポートされます。
- IPv6 – ゲートウェイネットワークインターフェイスにIPv6アドレスを割り当てます。このオプションは、選択したすべてのサブネットがサブネットIPv6のみであり、リソースにIPv6アドレスがある場合にのみサポートされます。
- デュアルスタック — IPv4と IPv6 アドレスの両方をゲートウェイネットワークインターフェイスに割り当てます。このオプションは、選択したすべてのサブネットに IPv4と IPv6 アドレス範囲の両方があり、リソースに IPv4または IPv6 アドレスがある場合にのみサポートされます。

リソースゲートウェイの IP アドレスタイプは、リソースにアクセスするクライアントまたはVPCエンドポイントの IP アドレスタイプとは無関係です。

Lattice VPC でリソースゲートウェイを作成する

コンソールを使用してリソースゲートウェイを作成します。

コンソールを使用してリソースゲートウェイを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインの PrivateLink と Lattice で、リソースゲートウェイを選択します。
3. リソースゲートウェイの作成 を選択します。
4. AWS アカウント内で一意の名前を入力します。

5. リソースゲートウェイの IP のタイプを選択します。
6. リソースVPCがある を選択します。
7. からサービスネットワークVPCへのインバウンドトラフィックを制御するには、最大 5 つのセキュリティグループを選択します。
8. (オプション) タグを追加するには、[新しいタグを追加] を選択し、そのタグのキーと値を入力します。
9. リソースゲートウェイの作成 を選択します。

を使用してリソースゲートウェイを作成するには AWS CLI

create-resource-gateway コマンドを使用します。

Lattice VPC でリソースゲートウェイを削除する

コンソールを使用してリソースゲートウェイを削除します。

コンソールを使用してリソースゲートウェイを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインの PrivateLink と Lattice で、リソースゲートウェイを選択します。
3. 削除するリソースゲートウェイのチェックボックスを選択し、アクション、削除を選択します。確認を求められたら、**confirm**と入力し、[削除] を選択します。

を使用してリソースゲートウェイを削除するには AWS CLI

delete-resource-gateway コマンドを使用します。

経由でサービスネットワークにアクセスする AWS PrivateLink

サービスネットワークVPCエンドポイント (サービスネットワークエンドポイント) VPCを使用して、 からサービスネットワークにプライベートに接続できます。サービスネットワークエンドポイントを使用すると、サービスネットワークに関連付けられているリソースとサービスにプライベートかつ安全にアクセスできます。このようにして、単一のVPCエンドポイントを介して複数のリソースとサービスにプライベートにアクセスできます。

サービスネットワークは、リソース設定と Lattice VPC サービスの論理的なコレクションです。サービスネットワークエンドポイントを使用すると、サービスネットワークを に接続しVPC、それらのリソースやサービスに VPCまたはオンプレミスからプライベートにアクセスできます。サービスネットワークエンドポイントを使用すると、1 つのサービスネットワークに接続できます。から複数のサービスネットワークに接続するにはVPC、複数のサービスネットワークエンドポイントを作成し、それぞれが異なるサービスネットワークを指しています。

サービスネットワークは AWS Resource Access Manager () と統合されていますAWS RAM。を介して、サービスネットワークを別のアカウントと共有できます AWS RAM。サービスネットワークを別の AWS アカウントと共有すると、そのアカウントはサービスネットワークエンドポイントを作成してサービスネットワークに接続できます。リソース共有を使用してサービスネットワークを共有できます AWS RAM。

AWS RAM コンソールを使用して、追加したリソース共有、アクセスできる共有サービスネットワーク、リソースを共有した AWS アカウントを表示します。詳細については、「 AWS RAM ユーザーガイド」の「自分と共有されているリソース」を参照してください。

料金

サービスネットワークに関連付けられているリソース設定については、時間単位で請求されます。また、サービスネットワークVPCエンドポイントを介してリソースにアクセスすると、処理されるデータの GB ごとに課金されます。サービスネットワークVPCエンドポイント自体に対して時間単位で課金されることはありません。詳細については、Amazon VPC Lattice の料金を参照してください。

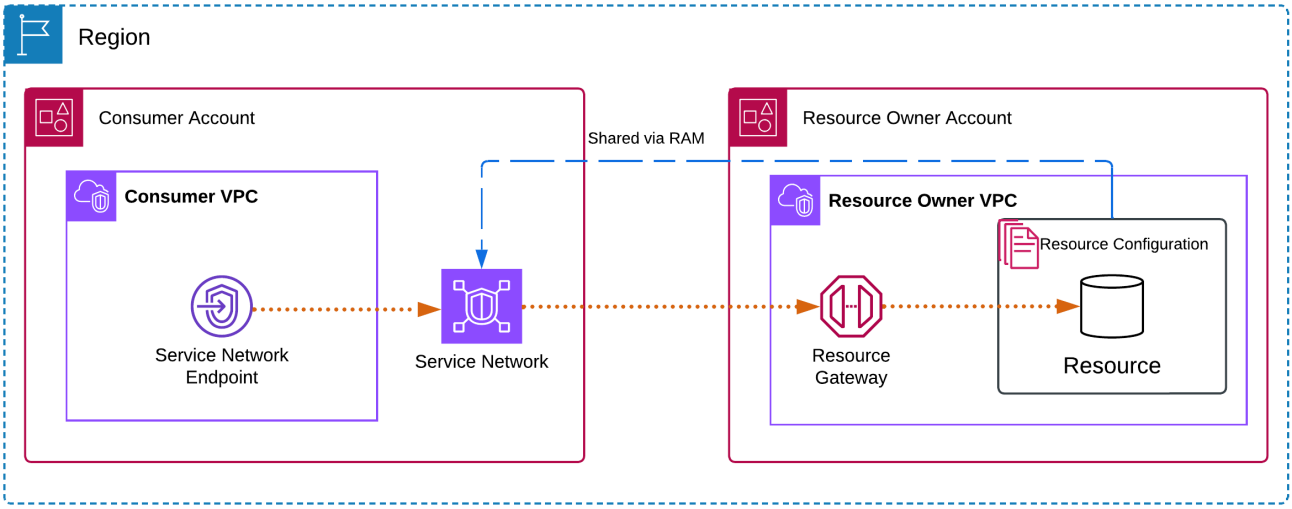
内容

- DNS 解像度
- プライベート DNS
- サブネットとアベイラビリティーゾーン
- IP アドレスのタイプ
- サービスネットワークエンドポイント経由でサービスネットワークにアクセスする
- サービスネットワークエンドポイントの管理

概要

独自のサービスネットワークを作成することも、別のアカウントからサービスネットワークを共有することもできます。どちらの方法でも、サービスネットワークエンドポイントを作成して、 から接続できますVPC。サービスネットワークを作成し、リソース設定を関連付ける方法の詳細については、「Amazon Lattice VPC ユーザーガイド」を参照してください。

次の図は、 のサービスネットワークエンドポイントがサービスネットワークVPCにアクセスする方法を示しています。



ネットワーク接続は、サービスネットワークエンドポイントVPCを持つ からのみ、サービスネットワーク内のリソースとサービスに開始できます。リソースとサービスVPCがある は、エンドポイント へのネットワーク接続を開始できませんVPC。

DNS ホスト名

では AWS PrivateLink、プライベートエンドポイントを使用してサービスネットワークにトラフィックを送信します。サービスネットワークVPCエンドポイントを作成すると、リソースとサービスごとにリージョンDNS名 (デフォルトDNS名と呼ばれる) が作成されます。この名前を使用して、 VPC とオンプレミスからリソースとサービスと通信できます。

サービスネットワーク内のリソースのデフォルトDNS名には、次の構文があります。

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

service-network の Lattice サービスのデフォルトDNS名には、次の構文があります。

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

サービスネットワークに を使用するリソース設定がある場合はARNs、プライベート DNSを有効にできます。プライベート を使用するとDNS、サービスネットワークVPCエンドポイントを介したプライベート接続を活用しながら、サービスによって AWS リソースにプロビジョニングされたDNS名前を使用してリソースへのリクエストを続行できます。詳細については、「the section called “DNS 解像度”」を参照してください。

DNS 解像度

サービスネットワークエンドポイントを作成すると、サービスネットワークに関連付けられているリソース設定と Lattice サービスごとにDNS名前が作成されます。これらのDNSレコードはパブリックです。したがって、これらのDNS名前はパブリックに解決可能です。ただし、 の外部からのDNSリクエストVPCは、サービスネットワークエンドポイントのネットワークインターフェイスのプライベート IP アドレスを返します。これらのDNS名前を使用して、サービスネットワークエンドポイントVPCがある に、 VPNまたは Direct Connect 経由でアクセスできる限り、オンプレミスからリソースとサービスにアクセスできます。

プライベート DNS

サービスネットワークVPCエンドポイントDNSでプライベートを有効にし、 VPCでDNSホスト名とDNS解像度の両方が有効になっている場合、カスタムDNS名を持つリソース設定に対して、非表示AWSのマネージドプライベートホストゾーンが作成されます。ホストゾーンには、 のサービスネッ

トワークエンドポイントのネットワークインターフェイスのプライベート IP アドレスに解決するリソースのデフォルトDNS名のレコードセットが含まれていますVPC。

Amazon はVPC、Route 53 Resolver と呼ばれる 用のDNSサーバーを提供しています。Route 53 Resolver は、プライベートホストゾーンのローカルVPCドメイン名とレコードを自動的に解決します。ただし、 の外部から Route 53 Resolver を使用することはできませんVPC。オンプレミスネットワークからVPCエンドポイントにアクセスする場合は、デフォルトDNS名を使用するか、Route 53 Resolver エンドポイントと Resolver ルールを使用できます。詳細については、「AWS Transit GatewayAWS PrivateLink と の統合 Amazon Route 53 Resolver」を参照してください。

サブネットとアベイラビリティーゾーン

アベイラビリティーゾーンごとに 1 つのサブネットを使用してVPCエンドポイントを設定できます。サブネット内のエンドポイントのVPCエンドポイントネットワークインターフェイスを作成します。エンドポイントの IP アドレスタイプに基づいて、サブネットから各エンドポイントネットワークインターフェイスに IP アドレスを割り当てます。 VPC本稼働環境では、高可用性と耐障害性を実現するために、VPCエンドポイントごとに少なくとも 2 つのアベイラビリティーゾーンを設定することをお勧めします。

IP アドレスのタイプ

サービスネットワークエンドポイントはIPv4、、IPv6、またはデュアルスタックアドレスをサポートできます。をサポートするエンドポイントは、 AAAAレコードでDNSクエリに応答IPv6できます。サービスネットワークエンドポイントの IP アドレスタイプは、以下で説明するように、リソースエンドポイントのサブネットと互換性がある必要があります。

- IPv4 – エンドポイントネットワークインターフェイスにIPv4アドレスを割り当てます。このオプションは、選択したすべてのサブネットにIPv4アドレス範囲がある場合にのみサポートされます。
- IPv6 – エンドポイントネットワークインターフェイスにIPv6アドレスを割り当てます。このオプションは、選択したすべてのサブネットがサブネットIPv6のみの場合にのみサポートされます。
- デュアルスタック — エンドポイントネットワークインターフェイスに IPv4と IPv6 アドレスの両方を割り当てます。このオプションは、選択したすべてのサブネットに IPv4と の両方のIPv6アドレス範囲がある場合にのみサポートされます。

サービスネットワークVPCエンドポイントが をサポートしている場合IPv4、エンドポイントネットワークインターフェイスには IPv4 アドレスがあります。サービスネットワークVPCエンドポイント

が をサポートしている場合IPv6、エンドポイントネットワークインターフェイスには IPv6 アドレスがあります。エンドポイントネットワークインターフェイスのIPv6アドレスにインターネットからアクセスできません。IPv6 アドレスを使用してエンドポイントネットワークインターフェイスを記述する場合は、 `denyAllIgwTraffic` が有効になっていることに注意してください。

サービスネットワークエンドポイント経由でサービスネットワークにアクセスする

サービスネットワークエンドポイントを使用してサービスネットワークにアクセスできます。サービスネットワークエンドポイントは、サービスネットワーク内のリソース設定とサービスへのプライベートアクセスを提供します。

前提条件

サービスネットワークエンドポイントを作成するには、次の前提条件を満たす必要があります。

- 自分で作成したサービスネットワーク、または を介して別のアカウントから共有されたサービスネットワークが必要です AWS RAM。
- サービスネットワークが別のアカウントから共有されている場合は、サービスネットワークを含むリソース共有を確認して承諾する必要があります。詳細については、「AWS RAM ユーザーガイド」の「招待の承諾と拒否」を参照してください。

サービスネットワークエンドポイントを作成する

共有されたサービスネットワークにアクセスするためのサービスネットワークエンドポイントを作成します。

サービスネットワークエンドポイントを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. [エンドポイントの作成] を選択します。
4. エンドポイントを見つけて管理しやすくするために、名前を指定できます。
5. タイプ で、サービスネットワークを選択します。
6. サービスネットワークで、共有されたサービスネットワークを選択します。
7. ネットワーク設定で、サービスネットワークにアクセスする VPC を選択します。

8. プライベートDNSサポートを設定する場合は、「追加設定」、DNS「名前を有効にする」を選択します。この機能を使用するには、 属性 DNSホスト名を有効にする と DNS サポートを有効にする が に対して有効になっていることを確認しますVPC。
9. [エンドポイントの作成] を選択します。

コマンドラインを使用してサービスネットワークエンドポイントを作成するには

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint (Windows 用のツール PowerShell)

サービスネットワークエンドポイントの管理

サービスネットワークエンドポイントを作成したら、その設定を更新できます。

タスク

- エンドポイントを削除します
- サービスネットワークエンドポイントを更新する

エンドポイントを削除します

VPC エンドポイントの使用が終了したら、削除できます。

コンソールを使用してエンドポイントを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. サービスネットワークエンドポイントを選択します。
4. アクション、VPCエンドポイントの削除を選択します。
5. 確認を求められたら、**delete** をクリックします。
6. [削除] を選択します。

コマンドラインを使用してエンドポイントを削除するには

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

サービスネットワークエンドポイントを更新する

VPC エンドポイントを更新できます。

コンソールを使用してエンドポイントを更新するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. エンドポイントを選択します。
4. アクションを選択し、適切なオプションを選択します。
5. コンソールの手順に従って更新を送信します。

コマンドラインを使用してエンドポイントを更新するには

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint (Windows 用のツール PowerShell)

の Identity and Access Management AWS PrivateLink

AWS Identity and Access Management （ IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。 IAM管理者は、誰を認証 (サインイン) し、誰に AWS PrivateLink リソースの使用を承認する (アクセス許可を付与 AWS のサービス する) かを制御します。 IAMは、追加料金なしで使用できる です。

内容

対象者

AWS Identity and Access Management （ IAM) の使用方法は、作業内容によって異なります AWS PrivateLink。

サービスユーザー – AWS PrivateLink サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が与えられます。さらに多くの AWS PrivateLink 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。

サービス管理者 – 社内の AWS PrivateLink リソースを担当している場合は、通常、 へのフルアクセスがあります AWS PrivateLink。サービスユーザーがどの AWS PrivateLink 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後で、サービスユーザーのアクセス許可を変更するために、IAM 管理者にリクエストを送信する必要があります。IAM の基本概念については、このページの情報を確認します。

IAM 管理者 – IAM管理者は、アクセスを管理するポリシーの作成方法の詳細について確認する場合があります AWS PrivateLink。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、 IAM ユーザーとして AWS アカウントのルートユーザー、または IAMロールを引き受けることによって、認証 (にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center （ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーティッド ID の例です。フェデレーテッドアイデンティティ としてサインインする場合、管理者は以前に IAM ロールを使用して ID フェデレーションを設定しています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 AWS サインイン ユーザーガイド」の「 にサインインする方法 AWS アカウント」を参照してください。

AWS プログラムで にアクセスする場合、 はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨される方法を使用してリクエストに署名する方法の詳細については、「 IAMユーザーガイド」のAWS API「リクエストの署名バージョン 4」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。たとえば、 では、アカウントのセキュリティを強化するために多要素認証 (MFA) を使用する AWS ことをお勧めします。詳細については、「 AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「 IAMユーザーガイド」のAWS 「 での多要素認証IAM」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、IAMユーザー ガイドの「ルートユーザー資格情報が必要なタスク」を参照してください。

フェデレーテッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、ID プロバイダーとのフェデレーションを使用して一時的な認証情報 AWS のサービス を使用して にアクセスすることを要求します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、アイデンティティセンターディレクトリのユーザー、または ID ソースを通じて提供された認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID がアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成することも、独自の ID ソース内のユーザーとグループのセットに接続して同期し、すべての AWS アカウント とアプリケーションで使用できるようにすることもできます。IAM Identity Center の詳細については、「 AWS IAM Identity Center ユーザーガイド」のIAM「Identity Center とは」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を持つIAMユーザーを作成するのではなく、一時的な認証情報を使用することをお勧めします。ただし、IAMユーザーとの長期的な認証情報を必要とする特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、IAMユーザーガイドの「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーのコレクションを指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、 という名前のグループを作成しIAMAdmins、そのグループにIAMリソースを管理するアクセス許可を付与できます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「 IAMユーザーガイド」のIAM「 ユーザーのユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーに関連付けられていません。で IAMロールを一時的に引き受けるには AWS Management Console、ユーザーから IAMロール (コンソール) に切り替えることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム を使用しますURL。ロールを使用する方法の詳細については、「 IAMユーザーガイド」の「ロールを引き受ける方法」を参照してください。

IAM ロールと一時認証情報は、次の状況で役立ちます。

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールの詳細については、「 ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) のロールを作成する」を参照してください。 IAM IAM Identity Center を使用する場合は、アクセス許可セットを設定します。ID が認証後にアクセスできる内容を制御するために、IAMIdentity Center はアクセス許可セットを のロールに関連付けますIAM。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「Permission sets」を参照してください。
- 一時的なIAMユーザーアクセス許可 – IAM ユーザーまたはロールは、 IAMロールを引き受けて、特定のタスクに対して異なるアクセス許可を一時的に引き受けることができます。
- クロスアカウントアクセス IAMロールを使用して、自分のアカウントのリソースにアクセスすることを別のアカウントの信頼済みプリンシパルに許可できます。クロスアカウントアクセスを許可する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (ロールをプロキシとして使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスのロールとリソースベースのポリシーの違いについては、「 IAMユーザーガイド」の「 でのクロスアカウントリソースアクセスIAM」を参照してください。
- クロスサービスアクセス — 一部の は、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、サービスで呼び出しを行うと、そのサービスが Amazon でアプリケーションを実行EC2したり、Amazon S3 にオブジェクトを保存したりするのが一般的です。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用してアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用すると、別のサービスで別のアクションを開始するアクションを実行できます。 FASは、 を呼び出すプリンシパルのアクセス許可をリクエストと組み合わせて使用し AWS のサービス、ダウンストリームサービス AWS のサービス にリクエストを送信します。 FAS リクエストは、他の AWS のサービス またはリソー

スとのやり取りを完了する必要があるリクエストをサービスが受信した場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

- サービスロール – サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける IAMロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「 IAMユーザーガイド」の「 にアクセス許可を委任するロールを作成する AWS のサービス」を参照してください。
- サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、 サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

- Amazon で実行されているアプリケーション EC2 – IAMロールを使用して、EC2インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。 AWS ロールをEC2インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時認証情報を取得することができます。詳細については、「 ユーザーガイド」の「 IAMロールを使用して Amazon EC2インスタンスで実行されているアプリケーションにアクセス許可を付与する」を参照してください。IAM

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは のオブジェクト AWS であり、アイデンティティまたはリソースに関連付けられると、そのアクセス許可を定義します。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーはJSON、ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「 IAMユーザーガイド」のJSON「ポリシーの概要」を参照してください。

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM管理者は、リソースで必要なアクションを実行するためのアクセス許可をユーザーに付与する IAMポリシーを作成できます。その後、管理者はロールに IAMポリシーを追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションのアクセス許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS からロール情報を取得できます API。

アイデンティティベースのポリシー

アイデンティティベースのポリシーは、 IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできるJSONアクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「 IAMユーザーガイド」の「カスタマー管理ポリシーによるカスタムIAMアクセス許可の定義」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。管理ポリシーまたはインラインポリシーを選択する方法については、「 IAMユーザーガイド」の「管理ポリシーとインラインポリシーの選択」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースにアタッチするJSONポリシードキュメントです。リソースベースポリシーの例としては、IAMロール信頼ポリシーや Amazon S3 バケットポリシーなどがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーIAMでは、 から AWS 管理ポリシーを使用することはできません。

アクセスコントロールリスト (ACLs)

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。 ACLsは、ポリシードキュメント形式を使用しませんが、リソースベースのJSONポリシーに似ています。

Amazon S3、 AWS WAF、および Amazon VPCは、 をサポートするサービスの例ですACLs。の詳細についてはACLs、Amazon Simple Storage Service デベロッパーガイドの「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 – アクセス許可の境界は、アイデンティティベースのポリシーがIAMエンティティ (IAM ユーザーまたはロール) に付与できるアクセス許可の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、IAM ユーザー ガイドの「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) の最大アクセス許可を指定するJSONポリシーです AWS Organizations。 AWS Organizations は、ビジネスが所有する複数の AWS アカウント をグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCPs) をアカウントの一部またはすべてに適用できます。は、各 を含むメンバーアカウントのエンティティのアクセス許可SCPを制限します AWS アカウントのルートユーザー。Organizations と の詳細についてはSCPs、「 AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」を参照してください。
- リソースコントロールポリシー (RCPs) – 所有する各リソースにアタッチされたJSONポリシーを更新することなく、アカウント内のリソースに対して使用可能なアクセス許可の上限を設定するために使用できるIAMポリシーRCPsです。は、メンバーアカウントのリソースのアクセス許可RCPを制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。をサポートする のリストを含む Organizations と の詳細についてはRCPs、「 AWS Organizations ユーザーガイドRCPs」の AWS のサービス「リソースコントロールポリシー (RCPs) 」を参照してください。

- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、IAM ユーザーガイドの「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関係する場合に がリクエストを許可するかどうか AWS を決定する方法については、「 IAMユーザーガイド」の「ポリシーの評価ロジック」を参照してください。

と AWS PrivateLink の連携方法 IAM

IAM を使用して へのアクセスを管理する前に AWS PrivateLink、 で使用できるIAM機能を確認してください AWS PrivateLink。

IAM 機能	AWS PrivateLink サポート
アイデンティティベースポリシー	はい
リソースベースのポリシー	あり
ポリシーアクション	はい
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	あり
ACLs	不可
ABAC (ポリシー内のタグ)	あり
一時的な認証情報	はい
プリンシパル権限	はい

IAM 機能	AWS PrivateLink サポート
サービスロール	いいえ
サービスリンクロール	いいえ

AWS PrivateLink およびその他の がほとんどの IAM 機能と AWS のサービス どのように連携するかの概要を把握するには、IAM「 ユーザーガイド」のAWS 「 と連携する のサービスIAM」を参照してください。

のアイデンティティベースのポリシー AWS PrivateLink

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースのポリシーは、 IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできるJSONアクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「 IAMユーザーガイド」の「カスタマー管理ポリシーを使用してカスタムIAMアクセス許可を定義する」を参照してください。

IAM のアイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、またアクションが許可または拒否される条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素については、「 IAMユーザーガイド」の「 IAMJSONポリシー要素リファレンス」を参照してください。

のアイデンティティベースのポリシーの例 AWS PrivateLink

AWS PrivateLink アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいのアイデンティティベースのポリシーの例 AWS PrivateLink。

内のリソースベースのポリシー AWS PrivateLink

リソースベースのポリシーのサポート: あり

リソースベースのポリシーは、リソースにアタッチするJSONポリシードキュメントです。リソースベースポリシーの例としては、IAMロール信頼ポリシーや Amazon S3 バケットポリシーなどがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの

場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、全体のアカウント、または別のアカウントの IAM エンティティを、リソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる場合 AWS アカウント、信頼されたアカウントのIAM管理者は、リソースへのアクセス許可をプリンシパルエンティティ (ユーザーまたはロール) に付与する必要もあります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、「 IAMユーザーガイド」の「 でのクロスアカウントリソースアクセスIAM」を参照してください。

AWS PrivateLink サービスは、エンドポイントポリシーと呼ばれるリソースベースのポリシーの 1 つのタイプをサポートします。エンドポイントポリシーは、どの AWS プリンシパルがエンドポイントを使用してエンドポイントにアクセスするのかを制御します。詳細については、「the section called “エンドポイントポリシー”」を参照してください。

のポリシーアクション AWS PrivateLink

ポリシーアクションのサポート:あり

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action`要素は、ポリシーでアクセスを許可または拒否するために使用できるアクションを記述します。ポリシーアクションの名前は通常、関連する AWS APIオペレーションと同じです。一致するAPIオペレーションがないアクセス許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

EC2 名前空間のアクション

の一部のアクション AWS PrivateLink は、Amazon EC2 の一部ですAPI。これらのポリシーアクションでは、 ec2 プレフィックスを使用します。詳細については、「Amazon EC2APIリファレンス」の「 AWS PrivateLink アクション」を参照してください。

vpce 名前空間のアクション

AWS PrivateLink には、AllowMultiRegionアクセス許可のみのアクションも用意されています。このポリシーアクションでは、 vpce プレフィックスを使用します。

のポリシーリソース AWS PrivateLink

ポリシーリソースのサポート: あり

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Policy ResourceJSON要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

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

のポリシー条件キー AWS PrivateLink

サービス固有のポリシー条件キーのサポート: あり

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルが、どのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。たとえば、IAM ユーザー名でタグ付けされている場合のみ、リソースにアクセスする IAM ユーザーアクセス許可を付与できます。詳細については、IAMユーザーガイドの「 IAMポリシーエレメント: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートしています。すべての AWS グローバル条件キーを確認するには、「 IAMユーザーガイド」のAWS 「 グローバル条件コンテキストキー」を参照してください。

以下の条件キーは、 に固有です AWS PrivateLink。

- `ec2:VpceMultiRegion`
- `ec2:VpceServiceName`
- `ec2:VpceServiceOwner`
- `ec2:VpceServicePrivateDnsName`
- `ec2:VpceServiceRegion`
- `ec2:VpceSupportedRegion`

詳細については、「Amazon の条件キーEC2」を参照してください。

ACLs の AWS PrivateLink

をサポートACLs： いいえ

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。 ACLsは、ポリシードキュメント形式を使用しませんが、リソースベースのJSONポリシーに似ています。

ABAC と AWS PrivateLink

サポート ABAC (ポリシー内のタグ): はい

属性ベースのアクセスコントロール (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。では AWS、これらの属性はタグと呼ばれます。タグは、IAMエンティティ (ユーザーまたはロー

ル) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、 の最初のステップですABAC。次に、プリンシパルのタグがアクセスしようとしているリソースのタグと一致する場合に、オペレーションを許可するABACポリシーを設計します。

ABAC は、急速に成長している環境や、ポリシー管理が面倒な状況で役に立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

の詳細についてはABAC、「 IAMユーザーガイド」のABAC「認可によるアクセス許可の定義」を参照してください。をセットアップする手順を含むチュートリアルを表示するにはABAC、「 ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用する」を参照してください。 IAM

での一時的な認証情報の使用 AWS PrivateLink

一時的な認証情報のサポート: あり

一部の AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報と AWS のサービス 連携する などの詳細については、「 IAMユーザーガイド」のAWS のサービス 「 と連携する IAM 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合は、一時的な認証情報を使用します。たとえば、会社のシングルサインオン (SSO) リンク AWS を使用してにアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えの詳細については、「 IAMユーザーガイド」の「ユーザーからIAMロールへの切り替え (コンソール) 」を参照してください。

一時的な認証情報は、 AWS CLI または を使用して手動で作成できます AWS API。その後、これらの一時的な認証情報を使用してアクセスすることができます AWS。 AWS では、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することをお勧めします。詳細については、「」の「一時的なセキュリティ認証情報IAM」を参照してください。

のクロスサービスプリンシパル許可 AWS PrivateLink

転送アクセスセッションをサポート (FAS): はい

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用すると、別のサービスで別のアクションを開始するアクションを実行できます。 FASは、 を呼び出すプリンシパルのアクセス許可をリクエストと組み合わせて使用し AWS のサービス、ダウンストリームサービス AWS のサービス にリクエストを送信します。 FAS リクエストは、他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストをサービスが受信した場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

のサービスロール AWS PrivateLink

サービスロールのサポート: なし

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロール です。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「 IAMユーザーガイド」の「 にアクセス許可を委任するロールを作成する AWS のサービス」を参照してください。

のサービスにリンクされたロール AWS PrivateLink

サービスにリンクされたロールのサポート: なし

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、 サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

のアイデンティティベースのポリシーの例 AWS PrivateLink

デフォルトでは、 ユーザーおよびロールには、 AWS PrivateLink リソースを作成または変更する権限はありません。また、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、または を使用してタスクを実行することはできません AWS API。IAM管理者は、リソースで必要なアクションを実行するためのアクセス許可をユーザーに付与する IAMポリシーを作成できます。その後、管理者はロールに IAMポリシーを追加し、ユーザーはロールを引き受けることができます。

これらのポリシードキュメント例を使用してIAMアイデンティティベースのJSONポリシーを作成する方法については、「 IAMユーザーガイド」のIAM「ポリシーの作成 (コンソール) 」を参照してください。

各リソースタイプの の形式など AWS PrivateLink、 で定義されるアクションとリソースタイプの詳細については、「サービス認可リファレンス」のARNs「Amazon のアクション、リソース、および条件キーEC2」を参照してください。

例

- VPC エンドポイントの使用を制御する
- サービス所有者に基づいてVPCエンドポイントの作成を制御する
- VPC エンドポイントサービスに指定できるプライベートDNS名を制御する
- VPC エンドポイントサービスに指定できるサービス名を制御する

VPC エンドポイントの使用を制御する

デフォルトでは、 ユーザーにはエンドポイントを使用するためのアクセス権限がありません。エンドポイントを作成、変更、説明、および削除する許可をユーザーに付与する、アイデンティティベースのポリシーを作成できます。以下に例を示します。

```
{
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect": "Allow",
            "Action":"ec2:*VpcEndpoint*",
            "Resource":"*"
        }
    ]
}
```

VPC エンドポイントを使用して サービスへのアクセスを制御する方法については、「」を参照してくださいthe section called “エンドポイントポリシー”。

サービス所有者に基づいてVPCエンドポイントの作成を制御する

`ec2:VpceServiceOwner` 条件キーを使用して、サービスの所有者 (`amazon`、`aws-marketplace`、またはアカウント ID) に基づいて作成できるVPCエンドポイントを制御できます。

次の例では、指定されたサービス所有者でVPCエンドポイントを作成するアクセス許可を付与します。この例を使用するには、リージョン、アカウント ID、およびサービス所有者を置き換えます。

```
{
    "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"
                    ]
                }
            }
        }
    ]
}
```

VPC エンドポイントサービスに指定できるプライベートDNS名を制御する

`ec2:VpceServicePrivateDnsName` 条件キーを使用して、VPCエンドポイントサービスに関連付けられたプライベートDNS名に基づいて、変更または作成できるVPCエンドポイントサービスを制御できます。次の例では、指定されたプライベートDNS名でVPCエンドポイントサービスを作成するアクセス許可を付与します。この例を使用するには、リージョン、アカウント ID、プライベートDNS名を置き換えます。

```
{
```

```
    "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"
                    ]
                }
            }
        }
    ]
}
```

VPC エンドポイントサービスに指定できるサービス名を制御する

ec2:VpceServiceName 条件キーを使用して、VPCエンドポイントサービス名に基づいて作成できるVPCエンドポイントを制御できます。次の例では、指定されたサービス名でVPCエンドポイントを作成するアクセス許可を付与します。この例を使用するには、リージョン、アカウント ID、およびサービス名を置き換えます。

```
{
    "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"
                    ]
                }
            }
        }
    ]
}
```

VPC エンドポイントポリシーを使用してエンドポイントへのアクセスを制御する

エンドポイントポリシーは、VPCエンドポイントにアタッチして、エンドポイントを使用して にアクセスできる AWS プリンシパルを制御するリソースベースのポリシーです AWS のサービス。

エンドポイントポリシーは、アイデンティティベースのポリシーやリソースベースのポリシーを上書き、または置き換えません。例えば、インターフェイスエンドポイントを使用して Amazon S3 に接続する場合は、Amazon S3 バケットポリシーを使用して、特定のエンドポイントまたは特定の からバケットへのアクセスを制御することもできますVPCs。

内容

- 考慮事項
- デフォルトのエンドポイントポリシー
- インターフェイスエンドポイントのポリシー
- ゲートウェイエンドポイントのプリンシパル
- VPC エンドポイントポリシーを更新する

考慮事項

- エンドポイントポリシーは、JSONポリシー言語を使用するIAMポリシードキュメントです。エンドポイントポリシーには、プリンシパル要素を含める必要があります。エンドポイントポリシーのサイズは 20,480 文字 (空白を含む) を超えることはできません。
- のインターフェイスまたはゲートウェイエンドポイントを作成するときに AWS のサービス、エンドポイントに 1 つのエンドポイントポリシーをアタッチできます。いつでもエンドポイントポリシーの更新ができます。エンドポイントポリシーをアタッチしない場合、デフォルトのエンドポイントポリシーがアタッチされます。
- すべての がエンドポイントポリシー AWS のサービス をサポートしているわけではありません。AWS のサービス がエンドポイントポリシーをサポートしていない場合は、サービスの任意のエンドポイントへのフルアクセスを許可します。詳細については、「the section called “エンドポイントポリシーのサポートを表示する”」を参照してください。
- 以外のVPCエンドポイントサービスのエンドポイントを作成すると AWS のサービス、エンドポイントへのフルアクセスが許可されます。
- ワイルドカード文字 (* または ?) または数値条件演算子を、システム生成識別子 (`aws:PrincipalAccount` または `aws:SourceVpc` など) を参照するグローバルコンテキストキーで使用することはできません。
- 文字列条件演算子を使用する場合は、各ワイルドカード文字の前後に少なくとも 6 つの連続した文字を使用する必要があります。
- リソースまたは条件要素ARNで を指定する場合、 のアカウント部分にはアカウント ID またはワイルドカード文字を含めるARNことができますが、両方を含めることはできません。

デフォルトのエンドポイントポリシー

デフォルトのエンドポイントポリシーでは、エンドポイントへのフルアクセスが許可されています。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*"
        }
    ]
```

```
}
```

インターフェイスエンドポイントのポリシー

のエンドポイントポリシーの例については AWS のサービス、「」を参照してくださいthe section called “統合するサービス”。表の最初の列には、各 の AWS PrivateLink ドキュメントへのリンクが含まれています AWS のサービス。がエンドポイントポリシー AWS のサービス をサポートしている場合、そのドキュメントにはエンドポイントポリシーの例が含まれています。

ゲートウェイエンドポイントのプリンシパル

ゲートウェイエンドポイントでは、Principal 要素を * に設定する必要があります。プリンシパルを指定するには、aws:PrincipalArn 条件キーを使用します。

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

次の形式でプリンシパルを指定すると、アカウントのすべてのユーザーとロールではなく、 AWS アカウントのルートユーザー のみにアクセスが許可されます。

```
"AWS": "account_id"
```

ゲートウェイエンドポイントのエンドポイントポリシーの例については、次を参照してください。

- Amazon S3 におけるエンドポイント
- DynamoDB のエンドポイント

VPC エンドポイントポリシーを更新する

次の手順を使用して、 AWS のサービス のエンドポイントポリシーを更新します。エンドポイントポリシーを更新した後、変更が有効になるまでに数分かかる場合があります。

コンソールを使用してエンドポイントポリシーを変更するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。

2. ナビゲーションペインで、[エンドポイント] を選択します。
3. VPC エンドポイントを選択します。
4. [Actions] (アクション)、[Manage policy] (ポリシーを管理) の順に選択します。
5. [Full Access] (フルアクセス) を選択してサービスへのフルアクセスを許可するか、[Custom] (カスタム) を選択してカスタムポリシーをアタッチします。
6. [Save] を選択します。

コマンドラインを使用してエンドポイントポリシーを変更するには

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint (Windows 用のツール PowerShell)

AWS の 管理ポリシー AWS PrivateLink

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースにアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できます。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) が更新されます。 AWS AWS のサービス は、新しい が起動されたとき、または既存のサービスで新しいAPIオペレーションが利用可能になったときに、 AWS 管理ポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「AWS 管理ポリシー」を参照してください。

AWS PrivateLinkAWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始した AWS PrivateLink 以降の の AWS マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動通知については、 AWS PrivateLink ドキュメント履歴ページのRSSフィードにサブスクライブしてください。

変更	説明	日付
AWS PrivateLink が変更の追跡を開始しました	AWS PrivateLink が AWS マネージドポリシーの変更の追跡を開始しました。	2021 年 3 月 1 日

CloudWatch の メトリクス AWS PrivateLink

AWS PrivateLink は、インターフェイスエンドポイント、Gateway Load Balancer エンドポイント、およびエンドポイントサービスのデータポイントを Amazon に発行 CloudWatch します。CloudWatch を使用すると、これらのデータポイントに関する統計を、メトリクスと呼ばれる時系列データの順序付けられたセットとして取得できます。メトリクスは監視対象の変数、データポイントは時間の経過と共に変わる変数の値と考えることができます。各データポイントには、タイムスタンプと、オプションの測定単位が関連付けられています。

メトリクスを使用して、システムが正常に実行されていることを確認できます。たとえば、指定したメトリクスをモニタリングする CloudWatch アラームを作成し、メトリクスが許容範囲外になった場合にアクション (E メールアドレスへの通知の送信など) を開始できます。

すべてのインターフェイスエンドポイント、Gateway Load Balancer エンドポイント、およびエンドポイントサービスに関するメトリクスが発行されます。ゲートウェイエンドポイントに関するメトリクスは発行されません。デフォルトでは、 は追加コストなしで 1 分間隔でメトリクスを CloudWatch AWS PrivateLink に送信します。

詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

内容

エンドポイントのメトリクスとディメンション

`AWS/PrivateLinkEndpoints` 名前空間には、インターフェイスエンドポイントと Gateway Load Balancer エンドポイントに関する以下のメトリクスが含まれます。

メトリクス	説明
`ActiveConnections`	アクティブな同時接続の数。これには、SYN_SENT および ESTABLISHED状態の接続が含まれます。

メトリクス	説明
	レポート条件: エンドポイントが 1 分間の期間内にトラフィックを受信した。 統計値: 最も有用な統計値は Average、Maximum、および Minimum です。 ディメンション • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id
BytesProcessed	エンドポイントとエンドポイントサービスの間で交換されたバイト数 (両方向を集約)。これは、エンドポイントの所有者に料金が請求されるバイト数です。請求書には、この値が GB 単位で表示されます。 レポート条件: エンドポイントが 1 分間の期間内にトラフィックを受信した。 統計値: 最も有用な統計値は Average、Sum、Maximum、および Minimum です。 ディメンション • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id

メトリクス	説明
NewConnections	エンドポイント経由で確立された新しい接続の数。 レポート条件: エンドポイントが 1 分間の期間内にトラフィックを受信した。 統計値: 最も有用な統計値は Average、Sum、Maximum、および Minimum です。 ディメンション • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id
PacketsDropped	エンドポイントがドロップしたパケットの数。このメトリクスは、すべてのパケットドロップをキャプチャしない場合があります。値の増加は、エンドポイントまたはエンドポイントサービスが正常ではないことを示している可能性があります。 レポート条件: エンドポイントが 1 分間の期間内にトラフィックを受信した。 統計値: 最も有用な統計値は Average、Sum、および Maximum です。 ディメンション • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id

メトリクス	説明
RstPacketsReceived	エンドポイントによって受信されたRSTパケットの数。値の増加は、エンドポイントサービスが正常ではないことを示している可能性があります。 レポート条件: エンドポイントが 1 分間の期間内にトラフィックを受信した。 統計値: 最も有用な統計値は Average、Sum、および Maximum です。 ディメンション • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id

これらのメトリクスをフィルタリングするには、以下のディメンションを使用します。

ディメンション	説明
Endpoint Type	エンドポイントタイプ (Interface | GatewayLoadBalancer) でメトリクスデータをフィルタリングします。
Service Name	サービス名でメトリクスデータをフィルタリングします。
Subnet Id	サブネットでメトリクスデータをフィルタリングします。
VPC Endpoint Id	VPC エンドポイントでメトリクスデータをフィルタリングします。
VPC Id	VPC によってメトリクスデータをフィルタリングします。

エンドポイントサービスのメトリクスとディメンション

AWS/PrivateLinkServices 名前空間には、エンドポイントサービスに関する以下のメトリクスが含まれています。

メトリクス	説明
ActiveConnections	エンドポイント経由のクライアントからターゲットへのアクティブな接続の最大数。値の増加は、ロードバランサーにターゲットを追加する必要があることを示している可能性があります。 レポート条件: エンドポイントサービスに接続されたエンドポイントが 1 分間の期間内にトラフィックを送信した。 統計値: 最も有用な統計値は Average および Maximum です。 ディメンション • Service Id • Az, Service Id • Load Balancer Arn, Service Id • Az, Load Balancer Arn, Service Id • Service Id, VPC Endpoint Id
BytesProcessed	エンドポイントサービスとエンドポイントとの間で交換されたバイト数 (両方向)。 レポート条件: エンドポイントサービスに接続されたエンドポイントが 1 分間の期間内にトラフィックを送信した。 統計値: 最も有用な統計値は Average、Sum、および Maximum です。 ディメンション • Service Id • Az, Service Id • Load Balancer Arn, Service Id • Az, Load Balancer Arn, Service Id • Service Id, VPC Endpoint Id
EndpointsCount	エンドポイントサービスに接続されているエンドポイントの数。 レポート条件: 5 分間の期間内にゼロ以外の値がある。

メトリクス	説明
	統計値: 最も有用な統計値は Average および Maximum です。 ディメンション • Service Id
NewConnections	エンドポイント経由で確立されたクライアントからターゲットへの新しい接続の数。値の増加は、ロードバランサーにターゲットを追加する必要があることを示している可能性があります。 レポート条件: エンドポイントサービスに接続されたエンドポイントが 1 分間の期間内にトラフィックを送信した。 統計値: 最も有用な統計値は Average、Sum、および Maximum です。 ディメンション • Service Id • Az, Service Id • Load Balancer Arn, Service Id • Az, Load Balancer Arn, Service Id • Service Id, VPC Endpoint Id

メトリクス	説明
RstPacketsSent	エンドポイントサービスによってエンドポイントに送信されたRSTパケットの数。値の増加は、正常ではないターゲットが存在することを示している可能性があります。 レポート条件: エンドポイントサービスに接続されたエンドポイントが 1 分間の期間内にトラフィックを送信した。 統計値: 最も有用な統計値は Average、Sum、および Maximum です。 ディメンション • Service Id • Az, Service Id • Load Balancer Arn, Service Id • Az, Load Balancer Arn, Service Id • Service Id, VPC Endpoint Id

これらのメトリクスをフィルタリングするには、以下のディメンションを使用します。

ディメンション	説明
Az	アベイラビリティーゾーン別にメトリクスデータをフィルタリングします。
Load Balancer Arn	ロードバランサーでメトリクスデータをフィルタリングします。
Service Id	エンドポイントサービスでメトリクスデータをフィルタリングします。
VPC Endpoint Id	VPC エンドポイントでメトリクスデータをフィルタリングします。

CloudWatch メトリクスを表示する

これらの CloudWatch メトリクスは、Amazon VPCコンソール、 CloudWatch コンソール、または を使用して AWS CLI 次のように表示できます。

Amazon VPCコンソールを使用してメトリクスを表示するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[エンドポイント] を選択します。エンドポイントを選択してから、[Monitoring] (モニタリング) タブを選択します。
3. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。エンドポイントサービスを選択してから、[Monitoring] (モニタリング) タブを選択します。

CloudWatch コンソールを使用してメトリクスを表示するには

1. で CloudWatch コンソールを開きますhttps://console.aws.amazon.com/cloudwatch/。
2. ナビゲーションペインで Metrics (メトリクス) を選択します。
3. AWS/PrivateLinkEndpoints 名前空間を選択します。
4. AWS/PrivateLinkServices 名前空間を選択します。

を使用してメトリクスを表示するには AWS CLI

以下の list-metrics コマンドを使用して、インターフェイスエンドポイントと Gateway Load Balancer エンドポイントに利用できるメトリクスをリストします。

```
aws cloudwatch list-metrics --namespace AWS/PrivateLinkEndpoints
```

以下の list-metrics コマンドを使用して、エンドポイントサービスに利用できるメトリクスをリストします。

```
aws cloudwatch list-metrics --namespace AWS/PrivateLinkServices
```

組み込み Contributor Insights ルールを使用する

AWS PrivateLink には、エンドポイントサービス用の Contributor Insights ルールが組み込まれており、サポートされている各メトリクスの最大の寄稿者であるエンドポイントを見つけるのに役立ちます。詳細については、「Amazon CloudWatch ユーザーガイド」の「Contributor Insights」を参照してください。

AWS PrivateLink には、次のルールが用意されています。

- `VpcEndpointService-ActiveConnectionsByEndpointId-v1` - アクティブな接続の数でエンドポイントをランク付けします。
- `VpcEndpointService-BytesByEndpointId-v1` - 処理されたバイト数でエンドポイントをランク付けします。
- `VpcEndpointService-NewConnectionsByEndpointId-v1` - 新しい接続の数でエンドポイントをランク付けします。
- `VpcEndpointService-RstPacketsByEndpointId-v1` – エンドポイントに送信されたRSTパケット数でエンドポイントをランク付けします。

組み込みルールを使用する前に、それを有効にする必要があります。ルールを有効にすると、コントリビューターデータの収集が開始されます。Contributor Insights の料金については、「Amazon CloudWatch 料金表」を参照してください。

Contributor Insights を使用するには、次の許可が必要です。

- `cloudwatch:DeleteInsightRules` – Contributor Insights のルールを削除するため。
- `cloudwatch:DisableInsightRules` – Contributor Insights ルールを無効にするため。
- `cloudwatch:GetInsightRuleReport` – データを取得するため。
- `cloudwatch:ListManagedInsightRules` – 使用可能な Contributor Insights ルールを一覧表示するため。
- `cloudwatch:PutManagedInsightRules` – Contributor Insights のルールを有効にするため。

タスク

- Contributor Insights のルールを有効にする
- Contributor Insights のルールを無効にする
- Contributor Insights のルールを削除する

Contributor Insights のルールを有効にする

AWS Management Console または AWS PrivateLink を使用するための組み込みルールを有効にするには、次の手順を使用します AWS CLI。

コンソール AWS PrivateLink を使用して の Contributor Insights ルールを有効にするには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。

2. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
3. エンドポイントサービスを選択します。
4. [Contributor Insights] タブで、[Enable] (有効にする) を選択します。
5. (オプション) デフォルトでは、すべてのルールが有効になっています。特定のルールのみを有効にするには、有効にしないルールを選択し、[Actions] (アクション)、[Disable rule] (ルールを無効にする) の順に選択します。確認を求められたら、 の無効化 を選択します。

AWS PrivateLink を使用して の Contributor Insights ルールを有効にするには AWS CLI

1. 次のように list-managed-insight-rules コマンドを使用して、使用可能なルールを列挙します。`--resource-arn` オプションで、エンドポイントサービスの ARN を指定します。

```
aws cloudwatch list-managed-insight-rules --resource-arn
 arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-svc-0123456789EXAMPLE
```

2. `list-managed-insight-rules` コマンドの出力で、`TemplateName` フィールドからテンプレートの名前をコピーします。このフィールドの例を次に示します。

```
"TemplateName": "VpcEndpointService-NewConnectionsByEndpointId-v1"
```

3. ルールを有効にするには、次のように put-managed-insight-rules コマンドを使用します。エンドポイントサービスのテンプレート名と ARN を指定する必要があります。

```
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
```

Contributor Insights のルールを無効にする

の組み込みルールは AWS PrivateLink いつでも無効にできます。ルールを無効にすると、コントリビューターデータの収集は停止されますが、既存のコントリビューターデータは 15 日間が経過するまで保持されます。ルールを無効にした後、再度有効にしてコントリビューターデータの収集を再開することができます。

コンソール AWS PrivateLink を使用して の Contributor Insights ルールを無効にするには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。

2. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
3. エンドポイントサービスを選択します。
4. [Contributor Insights] タブで、[Disable all] (すべて無効にする) を選択してすべてのルールを無効にします。または、[Rules] (ルール) パネルを展開し、無効にするルールを選択してから、[Actions] (アクション)、[Disable rule] (ルールを無効にする) の順に選択します
5. 確認を求められたら、 の無効化 を選択します。

AWS PrivateLink を使用して の Contributor Insights ルールを無効にするには AWS CLI

disable-insight-rules コマンドを使用してルールを無効にします。

Contributor Insights のルールを削除する

AWS Management Console または AWS PrivateLink を使用するための組み込みルールを削除するには、次の手順に従います AWS CLI。ルールを削除すると、コントリビューターデータの収集が停止され、既存のコントリビューターデータが削除されます。

コンソール AWS PrivateLink を使用して の Contributor Insights ルールを削除するには

1. で CloudWatch コンソールを開きますhttps://console.aws.amazon.com/cloudwatch/。
2. ナビゲーションペインで、[Insights] (インサイト)、[Contributor Insights] の順に選択します。
3. [Rules] (ルール) パネルを展開し、ルールを選択します。
4. [Actions] (アクション)、[Delete rule] (ルールを削除) を選択します。
5. 確認を求めるメッセージが表示されたら、[削除] を選択します。

AWS PrivateLink を使用して の Contributor Insights ルールを削除するには AWS CLI

delete-insight-rules コマンドを使用してルールを削除します。

AWS PrivateLink クォータ

AWS アカウントには、 AWS サービスごとに、以前は制限と呼ばれていたデフォルトのクォータがあります。特に明記されていない限り、クォータは地域固有です。一部のクォータについては引き上げをリクエストできますが、その他のクォータについては引き上げることはできません。リソースごとに適用されるクォータの引き上げをリクエストすると、引き上げられたクォータはそのリージョン内のすべてのリソースに適用されます。

クォータの引き上げをリクエストするには、「Service Quotas ユーザーガイド」の「クォータ引き上げリクエスト」を参照してください。

リクエストのスロットリング

の API アクション AWS PrivateLink は Amazon EC2 の一部ですAPI。Amazon EC2 は、API リクエストを AWS アカウント レベルでスロットリングします。詳細については、「Amazon EC2 デベロッパーガイド」の「リクエストスロットリング」を参照してください。さらに、API リクエストは組織レベルでスロットリングされ、パフォーマンスが向上します AWS PrivateLink。を使用して AWS Organizations いて、アカウントレベルの API 制限内で`RequestLimitExceeded`エラーコードが表示される場合は、「多数の API 呼び出しを行う AWS アカウントを識別する方法」を参照してください。サポートが必要な場合は、アカウントチームに問い合わせるか、VPC サービスと VPC Endpoints カテゴリを使用してテクニカルサポートケースを開きます。`RequestLimitExceeded` エラーコードのイメージを必ずアタッチしてください。

VPCエンドポイントのクォータ

AWS アカウントには、VPC エンドポイントに関連する次のクォータがあります。

名前	デフォルト	引き上げ可能	コメント
VPC あたりのインターフェイスと Gateway Load Balancer エンドポイント	50	可能	これは、VPC 内のインターフェイスエンドポイントと Gateway Load Balancer エンドポイントの合計クォータです。
リージョンあたりのゲートウェイVPCエンドポイント	20	可能	VPC ワードあたり最大 255 のゲートウェイエンドポイントを作成できます
VPC エンドポイントポリシーあたりの文字数	20,480	なし	空白を含む VPC エンドポイントポリシーの最大サイズ

VPC エンドポイントを通過するトラフィックには、次の考慮事項が適用されます。

- デフォルトでは、各 VPC エンドポイントはアベイラビリティーゾーンあたり最大 10 Gbps の帯域幅をサポートし、自動的に最大 100 Gbps まで拡張できます。VPC エンドポイントの最大帯域幅は、すべてのアベイラビリティーゾーンに負荷を分散する場合、アベイラビリティーゾーンの数に 100 Gbps を掛けたものです。アプリケーションでより高いスループットが必要な場合は、 AWS サポートにお問い合わせください。
- ネットワーク接続の最大送信単位 (MTU) は、VPC エンドポイントを通過できる最大許容パケットのサイズをバイト単位で表したものです。MTU が大きいほど、1 つのパケットで渡すことができるデータが多くなります。VPC エンドポイントは、8500 バイトの MTU をサポートします。VPC エンドポイントに到着したサイズが 8500 バイトを超えるパケットはドロップされます。
- パスMTU検出 (PMTUD) はサポートされていません。VPC エンドポイントは、次の ICMP メッセージを生成しません: `Destination Unreachable: Fragmentation needed and Don't Fragment was Set` (タイプ 3、コード 4)。
- VPCエンドポイントは、すべてのパケットに最大セグメントサイズ (MSS) クランプを適用します。詳細については、RFC879」を参照してください。

のドキュメント履歴 AWS PrivateLink

次の表に、 のリリースを示します AWS PrivateLink。

変更	説明	日付
リソースとサービスネットワークにアクセスする	AWS PrivateLink は、 とアカウントの境界を越えてリソースVPCとサービスネットワークへのアクセスをサポートします。	2024 年 12 月 1 日
クロスリージョンアクセス	サービスプロバイダーは、1 つのリージョンでサービスをホストし、一連の AWS リージョンで利用可能にすることができます。サービスコンシューマーは、エンドポイントの作成時にサービスリージョンを選択します。	2024 年 11 月 26 日
指定された IP アドレス	エンドポイントを作成または変更するときに、VPCエンドポイントネットワークインターフェイスの IP アドレスを指定できます。	2023 年 8 月 17 日
IPv6 のサポート	Gateway Load Balancer エンドポイントサービスと Gateway Load Balancer エンドポイントは、 IPv4 アドレスと IPv6 アドレスの両方をサポートするかIPv6、アドレスのみをサポートするように設定できます。	2022 年 12 月 12 日

Contributor Insights	組み込みの Contributor Insights ルールを使用して、CloudWatch メトリクスの上位の寄稿者である特定のエンドポイントを特定できます AWS PrivateLink。	2022 年 8 月 18 日
IPv6 のサポート	サービスプロバイダーは、バックエンドサービスが のみをサポートしている場合でも、エンドポイントサービスがIPv6リクエストを受け入れるようにできますIPv4。エンドポイントサービスがIPv6リクエストを受け入れると、サービスコンシューマーはインターフェイスエンドポイントIPv6のサポートを有効にして、 経由でエンドポイントサービスにアクセスできるようになりますIPv6。	2022 年 5 月 11 日
CloudWatch メトリクス	AWS PrivateLink は、インターフェイスエンドポイント、Gateway Load Balancer エンドポイント、エンドポイントサービスの CloudWatch メトリクスを発行します。	2022 年 1 月 27 日
Gateway Load Balancer エンドポイント	で Gateway Load Balancer エンドポイントを作成して VPC、Gateway Load Balancer を使用して設定したVPCエンドポイントサービスにトラフィックをルーティングできます。	2020 年 11 月 10 日

VPC エンドポイントポリシー	サービスのインターフェイスVPCエンドポイントに IAM ポリシーを AWS アタッチして、サービスへのアクセスを制御できます。	2020 年 3 月 23 日
VPCエンドポイントとエンドポイントサービスの条件キー	EC2 条件キーを使用して、VPCエンドポイントとエンドポイントサービスへのアクセスを制御できます。	2020 年 3 月 6 日
作成時にVPCエンドポイントとエンドポイントサービスにタグを付ける	VPC エンドポイントとエンドポイントサービスを作成するときにタグを追加できます。	2020 年 2 月 5 日
プライベートDNS名	プライベートDNS名VPC を使用して、 内から AWS PrivateLink ベースのサービスにアクセスできます。	2020 年 1 月 6 日
VPC エンドポイントサービス	独自のエンドポイントサービスを作成し、インターフェイスVPCエンドポイントを介して他のユーザー AWS アカウント やユーザーがサービスに接続できるようにします。AWS Marketplaceで、エンドポイントサービスのサブスクリプションを提供できます。	2017 年 11 月 28 日
のインターフェイスVPCエンドポイント AWS のサービス	インターネットゲートウェイやNATデバイスを使用 AWS PrivateLink せずに、 と統合する に接続する AWS のサービス インターフェイスエンドポイントを作成できます。	2017 年 11 月 8 日

VPC DynamoDB の エンドポイント	インターネットゲートウェイやNATデバイスを使用VPCせずに、 から Amazon DynamoDB にアクセスするゲートウェイVPCエンドポイントを作成できます。	2017 年 8 月 16 日
VPC Amazon S3 の エンドポイント	インターネットゲートウェイやNATデバイスを使用VPCせずに、 から Amazon S3 にアクセスするゲートウェイVPCエンドポイントを作成できます。	2015 年 5 月 11 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。