AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

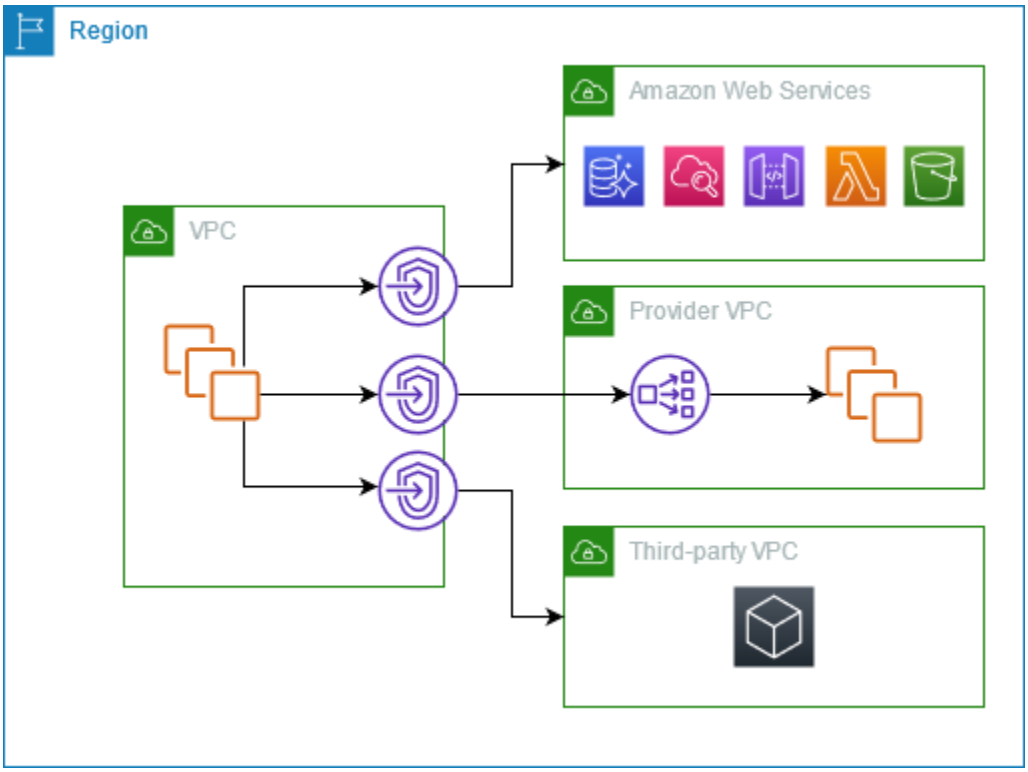
とは AWS PrivateLink

AWS PrivateLink は、VPC 内にあるかのように VPC を サービスにプライベートに接続するために使用できる、可用性が高くスケーラブルなテクノロジーです。プライベートサブネットからのサービ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、 AWS Site-to-Site VPN または接続を使用する必要はありません。したがって、ユーザーが VPC から到達可能な特定の API エンドポイント、サイト、およびサービスを制御することになります。

ユースケース

VPC エンドポイントを作成して、VPC 内のリソースを と統合するサービスに接続できます 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。

次の図では、左の VPC には、プライベートサブネットに複数の EC2 インスタンスと 3 つのインターフェイス VPC エンドポイントがあります。最上位の VPC エンドポイントは に接続します AWS のサービス。中間 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。下部の 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。



詳細はこちら

- 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 エンドポイントを使用する

以下のいずれかを使用して、VPC エンドポイントの作成、アクセス、および管理ができます。

- 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 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、次の AWS PrivateLink リソースを参照してください。
  - AWS::EC2::VPCEndpoint
  - AWS::EC2::VPC EndpointConnection通知
  - AWS::EC2::VPCEndpointService
  - AWS::EC2::VPC アクセスEndpointService許可
  - AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS SDKs — 言語固有の APIs。 SDK は、署名の計算、リクエストの再試行処理、エラー処理など、接続のさまざまな詳細を処理します。詳細については、「 で構築するツール AWS」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 API アクションを提供します。クエリ API の使用は、Amazon VPC にアクセスする最も直接的な方法です。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 EC2 API 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

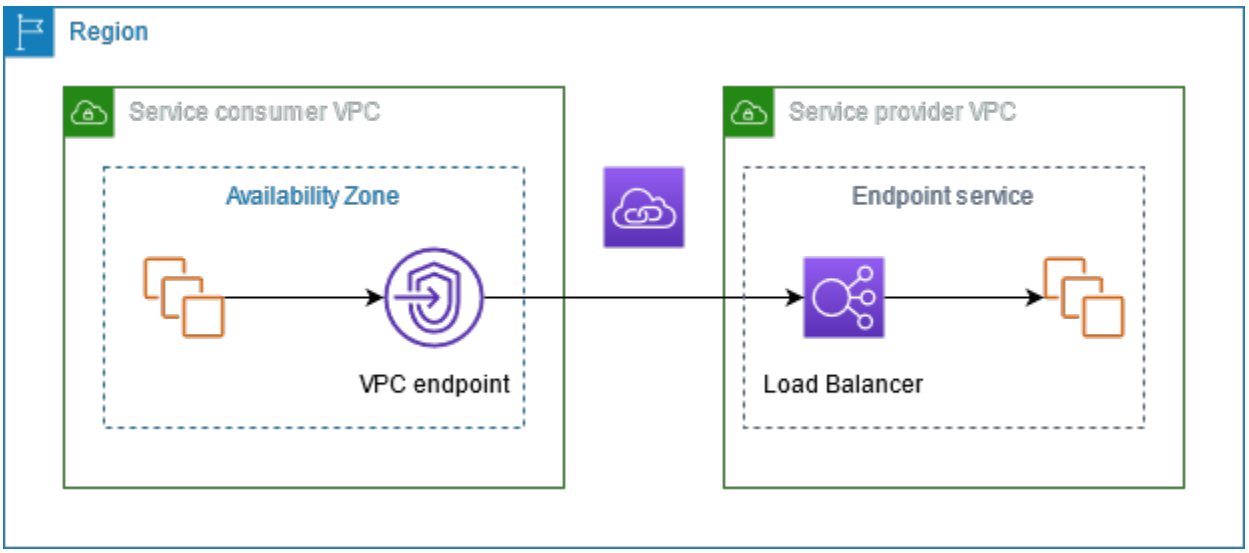
Amazon VPC を使用して、論理的に分離された仮想ネットワークである仮想プライベートクラウド (VPC) を定義できます。VPC で AWS リソースを起動できます。VPC 内のリソースがその VPC の外部にあるリソースに接続することを許可できます。例えば、VPC にインターネットゲートウェイを追加してインターネットへのアクセスを許可したり、VPN 接続を追加してオンプレミスネットワークへのアクセスを許可したりします。または、 AWS PrivateLink を使用して、VPC 内のリソースがプライベート IP アドレスを使用して他の VPCs内のサービスに接続できるようにします。これは、それらのサービスが VPC 内で直接ホストされているかのように行われます。

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

次の図は、 AWS PrivateLink の仕組みの概要を示しています。サービスコンシューマーは、サービスプロバイダーがホストする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 VPC エンドポイントを作成します。



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、およびその他の 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。

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

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 エンドポイントを作成するときに、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、 の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。

サービスコンシューマー

サービスのユーザーは、サービスコンシューマーです。サービスコンシューマーは、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からエンドポイントサービスにアクセスできます。

概念

- VPC 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 エンドポイント

サービスコンシューマーは、VPC エンドポイントを作成して、VPC をエンドポイントサービスに接続します。サービスコンシューマーは、VPC エンドポイントを作成するときに、エンドポイントサービスの名前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。エンドポイントサービスにより要求される VPC エンドポイントを作成する必要があります。

- `Interface` - エンドポイント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 エンドポイントサービス宛てのトラフィックは DNS を使用して解決されます。
- `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、VPC から Gateway Load Balancer エンドポイント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。

別のタイプの VPC エンドポイントである `Gateway` があり、これはゲートウェイ エンドポイントを作成してトラフィックを Amazon S3 または DynamoDB に送信します。ゲートウェイエンドポイントは AWS PrivateLink、他のタイプの VPC エンドポイントとは異なり、 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

エンドポイントの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宛ての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各サブネットに、エンドポイントのネットワークインターフェイスを作成します。

VPC エンドポイントが IPv4 をサポートしている場合、エンドポイントのネットワークインターフェイスは IPv4 アドレスを持ちます。VPC エンドポイントが IPv6 をサポートしている場合、エンドポイントのネットワークインターフェイスは IPv6 アドレスを持ちます。エンドポイントの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することはできません。エンドポイントのネットワークインターフェイスを IPv6 アドレスで記述する場合は、`denyAllIgwTraffic` が有効になっていることに注意してください。

エンドポイントの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。

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。これは、VPC エンドポイントを使用して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、すべてのリソースに対して、VPC エンドポイント経由での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

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 エンドポイントの可能な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 エンドポイントが使用可能です。
- 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可能にできませんでした。
- 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、その処理が進行中です。
- Deleted - VPC エンドポイントが削除されました。

AWS PrivateLink 接続

VPC からのトラフィックは、VPC エンドポイントとエンドポイントサービス間の接続を使用してエンドポイントサービスに送信されます。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、 AWS ネットワーク内に留まります。

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。

インターフェイス VPC エンドポイントでは、サービスコンシューマーは、VPC エンドポイントを使用してエンドポイントサービスにアクセスできる IAM プリンシパルの制御を、エンドポイントポリシーを使用して行うことができます。

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、VPC 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。

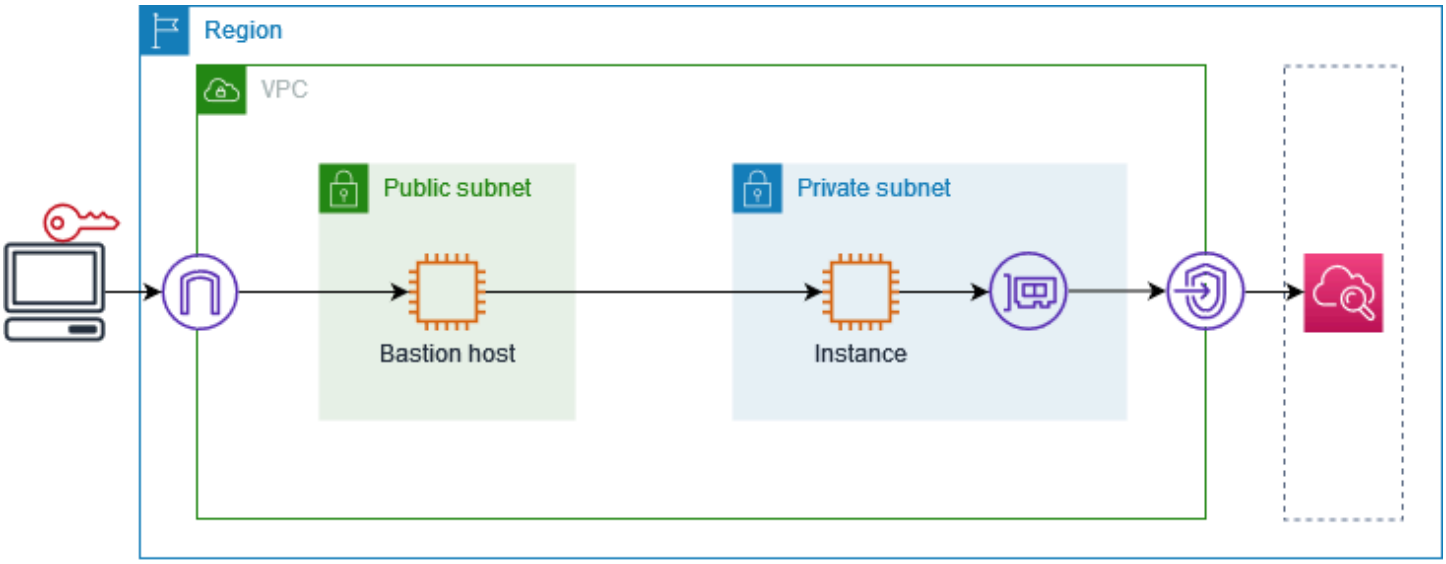
ドメイントラフィックを VPC エンドポイントにルーティングするように Amazon Route 53 を設定できます。詳細については、「ドメイン名を使用してトラフィックを VPC エンドポイントにルーティングする」を参照してください。

Route 53 を使用して、分割期間 DNS を設定できます。この DNS では、パブリックウェブサイトとを利用した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 VPC 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が、VPC の外部からのリクエスト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、「トラフィックをルーティングするための DNS メカニズムおよび AWS PrivateLink デプロイのフェイルオーバーの有効化」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` ファイルが踏み台ホストではなくコンピュータに存在するため、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、 宛て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: サブネットを持つ VPC 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 1: サブネットを持つ VPC 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を持つ VPC を作成します。

VPC を作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. [Create VPC (VPC の作成)] を選択します。
3. [Resources to create] (作成するリソース) で、[VPC and more] (VPC など) を選択します。
4. [名前タグの自動生成] に、VPC の名前を入力します。
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. [Create VPC (VPC の作成)] を選択します。

ステップ 2: インスタンスを起動する

前のステップで作成した VPC を使用して、パブリックサブネットの踏み台ホストとプライベートサブネットの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セキュリティグループを、踏み台ホストに作成します。
- 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セキュリティグループを、インスタンスに作成します。

- IAM インスタンスプロファイルを作成し、CloudWatchReadOnlyアクセス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. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. [インスタンスを起動] 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. [VPC] で、ユーザーの VPC を選択します。
   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. [インスタンスを起動] を選択します。

インスタンスを起動するには

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. [インスタンスを起動] 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. [VPC] で、ユーザーの VPC を選択します。
   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 instance profile] (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. [インスタンスを起動] を選択します。

ステップ 3: CloudWatch アクセスをテストする

次の手順を使用して、インスタンスが にアクセスできないことを確認します CloudWatch。これを行うには、 の読み取り専用 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、VPC 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
```

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 コマンドをもう一度試します。

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

に接続する 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

への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。例えば、VPC CIDR 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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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. [Service] (サービス) で、com.amazonaws.*region*.monitoring を選択します。
7. [VPC] で、自分の VPC を選択します。
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. [Security group] (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. [Policy] (ポリシー) で [Full access] (フルアクセス) を選択して、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 VPC エンドポイント経由の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
```

空の結果のレスポンスであっても、レスポンスが返された場合は、 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 への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` オプションで、VPC エンドポイントを作成したリージョンが指定されている。

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. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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)、[Delete VPC endpoints] (VPC エンドポイントを削除) 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。

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、インターネットゲートウェイを VPC に追加して、トラフィックが VPC から AWS のサービスに到達できるようにする必要があります。この設定がネットワークセキュリティ要件と連携しない場合は、 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 AWS のサービス かのように VPC を 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 の料金」を参照してください。

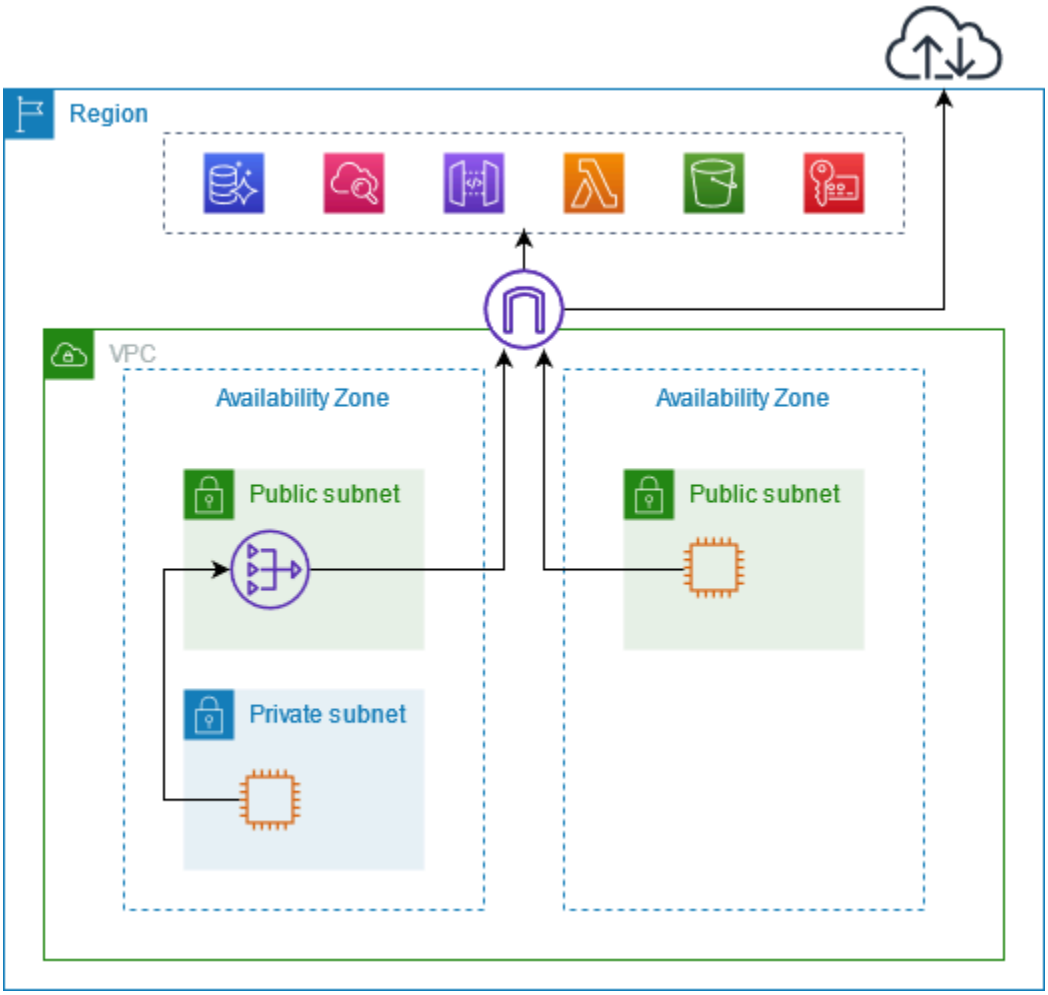
内容

概要

パブリックサービスエンドポイント AWS のサービス を介して 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。

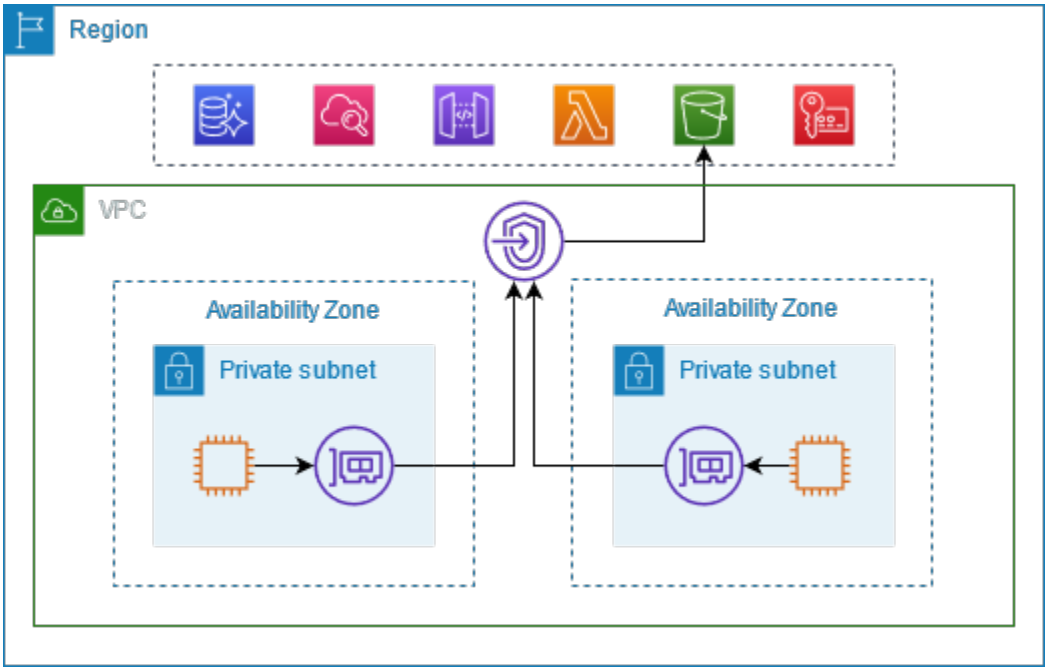
パブリックサービスエンドポイント経由でアクセスする

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、VPC のインターネットゲートウェイにルーティングされ、その後 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から AWS のサービス へのトラフィックは、NAT ゲートウェイ、VPC のためにインターネットゲートウェイ、 AWS のサービス の順にルーティングされます。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 を介して にアクセスする方法を示しています AWS PrivateLink。まず、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 内のサブネットと 間の接続が、ネットワークインターフェイス AWS のサービス を使用して確立されます。宛てのトラフィック AWS のサービス は、DNS 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、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 は接続リクエストを自動的に受け入れます。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することはできません。

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、VPC AWS のサービス からの との通信に使用できるリージョンおよびゾーン DNS 名が作成されます。

インターフェイス VPC エンドポイントのリージョンレベルの DNS 名の構文は次のとおりです。

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

ゾーンレベルの DNS 名の構文は次のとおりです。

```
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 DNS では、インターフェイス 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、パブリックエンドポイントの DNS 名を使用してサービスへの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 解決”」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る Amazon のインターフェイスエンドポイントの出力例 CloudWatch 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 解決

インターフェイス VPC エンドポイント用に作成される DNS レコードはパブリックです。したがって、これらの DNS 名はパブリックに解決可能です。ただし、VPC 外部からの DNS リクエストは引き続き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 アドレスを返すため、VPC にアクセスできない限り、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。

プライベート DNS

インターフェイス VPC エンドポイントでプライベート DNS を有効にし、VPC で DNS ホスト名と DNS 解決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。ホストゾーンにはサービスのデフォルトの DNS 名のレコードセットが含まれており、VPC の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。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はありません。

の 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、 AWS SDK 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 VPC エンドポイントに解決されます。

Amazon は、「Route 53 Resolver」と呼ばれる VPC 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、VPC の外部から Route 53 Resolver を使用することはできません。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したい場合は、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 Gateway と の統合 AWS PrivateLink 」を参照してください Amazon Route 53 Resolver。

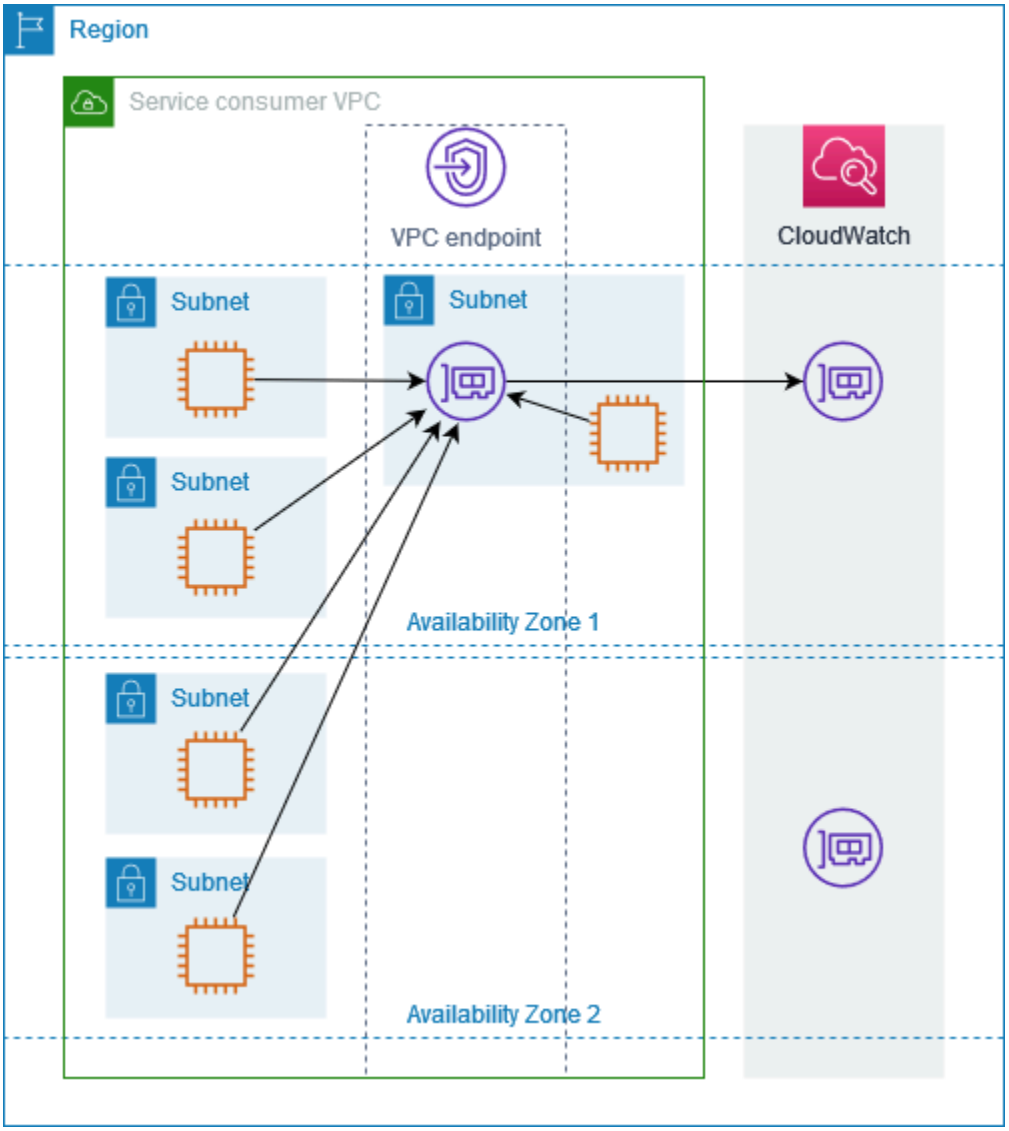
サブネットとアベイラビリティーゾーン

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 VPC エンドポイント用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ます。VPC 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。エンドポイントの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。

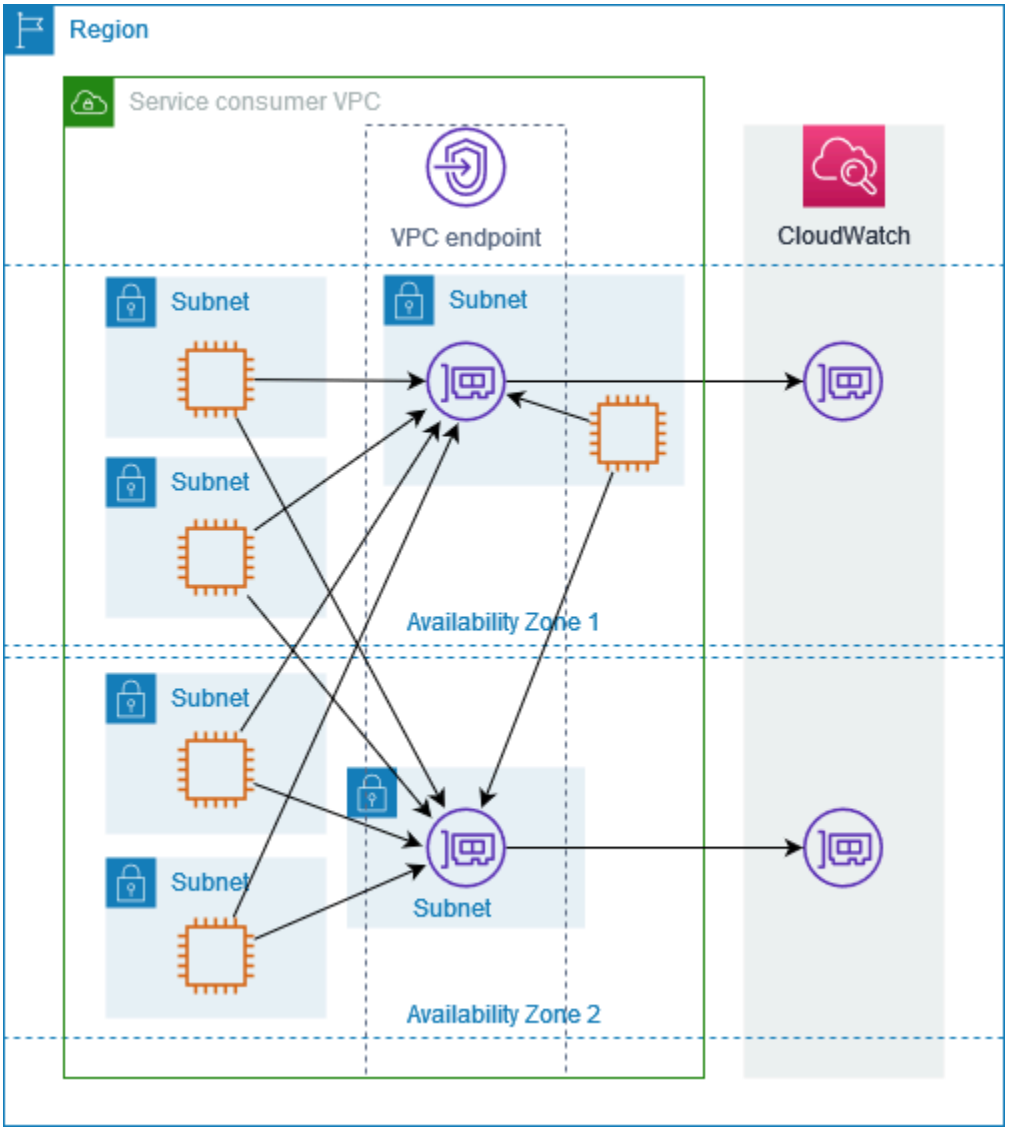
本番環境では、高い可用性と耐障害性を実現するには、以下をお勧めします。

- 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デプロイします AWS 。
- 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。

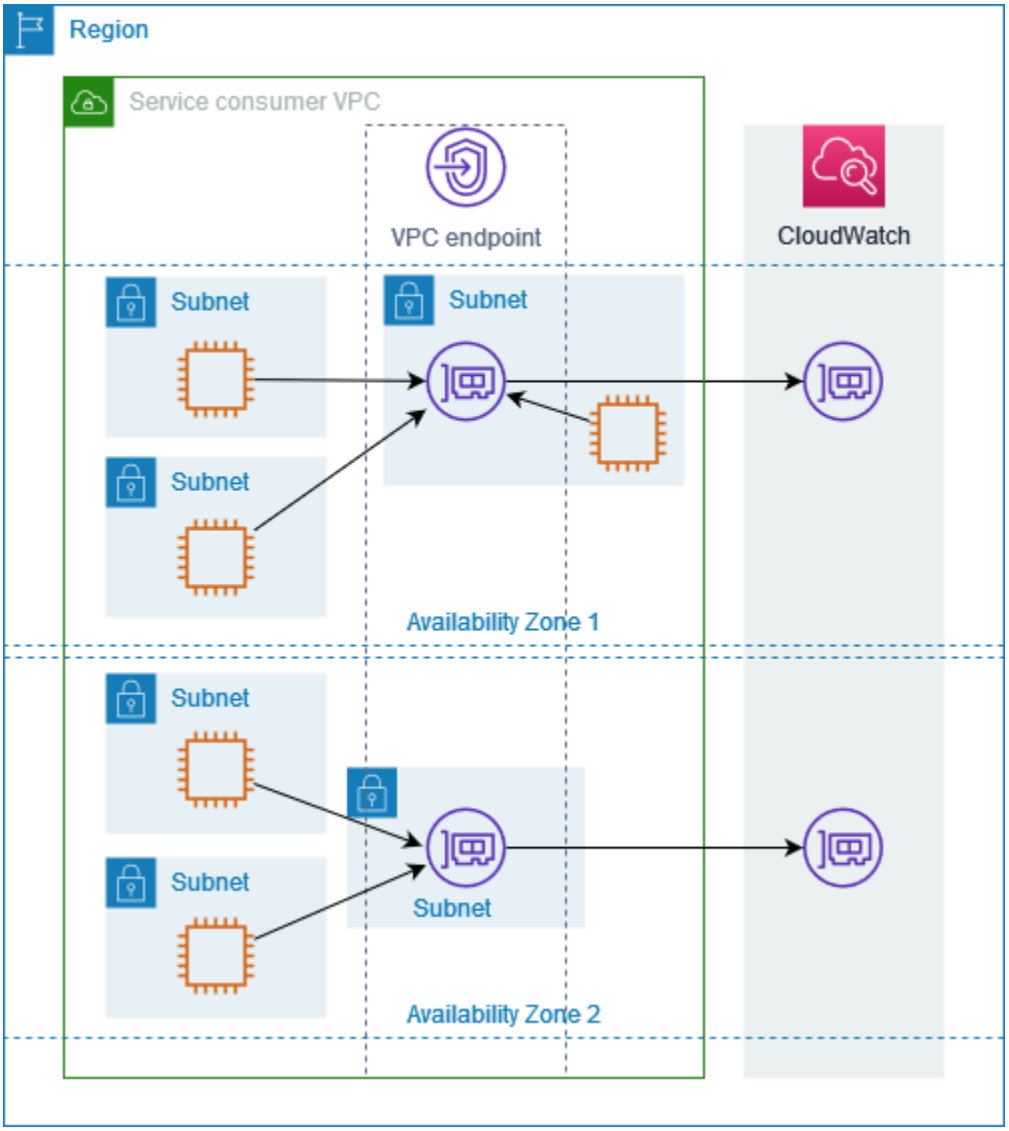
次の図は、単一のアベイラビリティーゾーンにエンドポイントネットワークインターフェイス CloudWatch を持つ Amazon の VPC エンドポイントを示しています。VPC 内のサブネット内のいずれかのリソースがパブリックエンドポイントを使用して Amazon CloudWatch にアクセスすると、トラフィックはエンドポイントネットワークインターフェイスの IP アドレスに解決されます。これには、他のアベイラビリティーゾーン内のサブネットからのトラフィックが含まれます。ただし、アベイラビリティーゾーン 1 に障害が発生した場合、アベイラビリティーゾーン 2 のリソースは Amazon 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 VPC エンドポイントを示しています。VPC 内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 にアクセスする場合、ラウンドロビンアルゴリズムを使用してそれらの間で交互に動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を選択します。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を介して IPv6 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を介して IPv6 をサポートできます。IPv6 をサポートするエンドポイントは、AAAA レコードを使用して DNS クエリに応答できます。

インターフェイスエンドポイント用に IPv6 を有効にするための要件

- は、サービスエンドポイントを IPv6 経由で利用可能に AWS のサービス する必要があります。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] — IPv4 アドレスをエンドポイントの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 アドレス範囲がある場合にのみサポートされます。
- [IPv6] — IPv6 アドレスをエンドポイントの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が IPv6 のみのサブネットである場合にのみサポートされます。
- [Dualstack] — IPv4 と IPv6 の両方のアドレスをエンドポイントの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 の両方の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 IPv4 をサポートしている場合、エンドポイントのネットワークインターフェイスは IPv4 アドレスを持ちます。インターフェイス VPC エンドポイントが IPv6 をサポートしている場合、エンドポイントのネットワークインターフェイスは IPv6 アドレスを持ちます。エンドポイントの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することはできません。エンドポイントのネットワークインターフェイスを IPv6 アドレスで記述する場合は、`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

以下が 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 VPC 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することができます。

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

AWS のサービス	サービス名
	com.amazonaws.*region*.appconfigdata
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 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
	com.amazonaws.*region.*bedrock-agent

AWS のサービス	サービス名
	com.amazonaws.*region*.bedrock-agent-runtime
	com.amazonaws.*region*.bedrock-runtime
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 クリーンルーム 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
Amazon CloudWatch	com.amazonaws.region.evidently
	com.amazonaws.region.evidently-dataplane
	com.amazonaws.region.monitoring
	com.amazonaws.region.rum

AWS のサービス	サービス名
	com.amazonaws.region.rum-dataplane
	com.amazonaws.region.synthetics
Amazon CloudWatch Logs	com.amazonaws.region.logs
Amazon CloudWatch Network Monitor	com.amazonaws.*region*.networkmonitor
AWS CodeArtifact	com.amazonaws.region.codeartifact.api
	com.amazonaws.region.codeartifact.repositories
AWS CodeBuild	com.amazonaws.region.codebuild
	com.amazonaws.region.codebuild-fips
AWS CodeCommit	com.amazonaws.region.codecommit
	com.amazonaws.region.codecommit-fips
	com.amazonaws.region.git-codecommit
	com.amazonaws.region.git-codecommit-fips
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 CodeWhisperer	com.amazonaws.*region*.codewhisperer

AWS のサービス	サービス名
Amazon Comprehend	com.amazonaws.region.comprehend
Amazon Comprehend Medical	com.amazonaws.region.comprehendmedical
AWS Config	com.amazonaws.region.config
Amazon Connect	com.amazonaws.region.app-integrations
	com.amazonaws.region.cases
	com.amazonaws.region.connect-campaigns
	com.amazonaws.region.profile
	com.amazonaws.region.voiceid
	com.amazonaws.region.wisdom
AWS Connector Service	com.amazonaws.region.awsconnector
AWS Control Catalog	com.amazonaws.*region.*controlcatalog
AWS Data Exchange	com.amazonaws.region.dataexchange
Amazon Data Firehose	com.amazonaws.region.kinesis-firehose
AWS Database Migration Service	com.amazonaws.region.dms
	com.amazonaws.region.dms-fips
AWS DataSync	com.amazonaws.region.datasync
Amazon DataZone	com.amazonaws.*region*.datazone
AWS Deadline Cloud	com.amazonaws.*region.*deadline.management
	com.amazonaws.*region* .deadline.scheduling
Amazon DevOpsGuru	com.amazonaws.region.devops-guru

AWS のサービス	サービス名
AWS Directory Service	com.amazonaws.*region*.ds
Amazon DynamoDB	com.amazonaws.*region*.dynamodb
Amazon EBS ダイレクト API	com.amazonaws.region.ebs
「Amazon EC2」	com.amazonaws.region.ec2
Amazon EC2 Auto Scaling	com.amazonaws.region.autoscaling
EC2 Image Builder	com.amazonaws.region.imagebuilder
Amazon ECR	com.amazonaws.region.ecr.api
	com.amazonaws.region.ecr.dkr
Amazon ECS	com.amazonaws.region.ecs
	com.amazonaws.region.ecs-agent
	com.amazonaws.region.ecs-telemetry
Amazon EKS	com.amazonaws.region.eks
	com.amazonaws.*region*.eks-auth
AWS Elastic Beanstalk	com.amazonaws.region.elasticbeanstalk
	com.amazonaws.region.elasticbeanstalk-health
AWS Elastic Disaster Recovery	com.amazonaws.region.drs
Amazon Elastic File System	com.amazonaws.region.elasticfilesystem
	com.amazonaws.region.elasticfilesystem-fips
Amazon Elastic Inference	com.amazonaws.region.elastic-inference.runtime
Elastic Load Balancing	com.amazonaws.region.elasticloadbalancing

AWS のサービス	サービス名
Amazon ElastiCache	com.amazonaws.region.elasticache
	com.amazonaws.region.elasticache-fips
AWS Elemental MediaConnect	com.amazonaws.*region*.mediaconnect
Amazon EMR	com.amazonaws.region.elasticmapreduce
Amazon EMR on EKS	com.amazonaws.region.emr-containers
Amazon EMR Serverless	com.amazonaws.region.emr-serverless
Amazon EMR WAL	com.amazonaws.*region* .emrwal.prod
AWS Entity Resolution	com.amazonaws.*region*.entityresolution
Amazon EventBridge	com.amazonaws.region.events
	com.amazonaws.*region* .pipes-data
AWS Fault Injection Service	com.amazonaws.region.fis
Amazon FinSpace	com.amazonaws.region.finspace
	com.amazonaws.region.finspace-api
Amazon Forecast	com.amazonaws.region.forecast
	com.amazonaws.region.forecastquery
	com.amazonaws.region.forecast-fips
	com.amazonaws.region.forecastquery-fips
Amazon Fraud Detector	com.amazonaws.region.frauddetector
Amazon FSx	com.amazonaws.region.fsx
	com.amazonaws.region.fsx-fips

AWS のサービス	サービス名
AWS Glue	com.amazonaws.region.glue
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-data
	com.amazonaws.*region*.guardduty-data-fips
AWS HealthImaging	com.amazonaws.*region* .dicom- Medical-imaging
	com.amazonaws.*region*.medical-imaging
	com.amazonaws.*region*.runtime-medical-imaging
AWS HealthLake	com.amazonaws.region.healthlake
AWS HealthOmics	com.amazonaws.*region*.analytics-omics
	com.amazonaws.*region*.control-storage-omics
	com.amazonaws.*region*.storage-omics
	com.amazonaws.*region*.tags-omics
	com.amazonaws.*region*.workflows-omics
IAM 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
AWS IoT Core	com.amazonaws.region.iot.data

AWS のサービス	サービス名
	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
Amazon Kendra	com.amazonaws.region.kendra
	aws.api.region.kendra-ranking
AWS Key Management Service	com.amazonaws.region.kms
	com.amazonaws.*region*.kms-fips
Amazon Keyspaces (Apache Cassandra 向け)	com.amazonaws.region.cassandra
	com.amazonaws.region.cassandra-fips
Amazon Kinesis Data Streams	com.amazonaws.region.kinesis-streams

AWS のサービス	サービス名
AWS Lake Formation	com.amazonaws.region.lakeformation
AWS Lambda	com.amazonaws.region.lambda
Amazon Lex	com.amazonaws.*region*.models-v2-lex
	com.amazonaws.*region*.runtime-v2-lex
AWS License Manager	com.amazonaws.*region*.license-manager
	com.amazonaws.*region*.license-manager-fips
	com.amazonaws.*region*.license-manager-user-subscriptions
Amazon Lookout for Equipment	com.amazonaws.*region*.lookoutequipment
Amazon Lookout for Metrics	com.amazonaws.*region*.lookoutmetrics
Amazon Lookout for Vision	com.amazonaws.*region*.lookoutvision
Amazon Macie	com.amazonaws.*region*.macie2
AWS Mainframe Modernization	com.amazonaws.*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 Workflows for Apache Airflow	com.amazonaws.*region*.airflow.api

AWS のサービス	サービス名
	com.amazonaws.*region*.airflow.env
	com.amazonaws.*region*.airflow.ops
AWS Management Console	com.amazonaws.*region*.console
	com.amazonaws.*region*.signin
Amazon MemoryDB for Redis	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 Neptune Analytics	com.amazonaws.*region*.neptune-graph
Amazon Nimble Studio	com.amazonaws.*region*.nimble
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
	com.amazonaws.*region*.payment-cryptography.dataplane

AWS のサービス	サービス名
Amazon Personalize	com.amazonaws.*region*.personalize
	com.amazonaws.*region*.personalize-events
	com.amazonaws.*region*.personalize-runtime
AWS Supply Chain	com.amazonaws.*region* .scn
Amazon Pinpoint	com.amazonaws.*region*.pinpoint
	com.amazonaws.*region*.pinpoint-sms-voice-v2
Amazon Polly	com.amazonaws.*region*.polly
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
AWS Proton	com.amazonaws.*region*.proton
Amazon Q Business	aws.api.*region*.qbusiness
Amazon QLDB	com.amazonaws.*region*.qldb.session
Amazon QuickSight	com.amazonaws.*region*.quicksight-website
Amazon RDS	com.amazonaws.*region*.rds
Amazon RDS Data API	com.amazonaws.*region*.rds-data
AWS re: プライベートの投稿	com.amazonaws.*region*.repostspace
Amazon Redshift	com.amazonaws.*region*.redshift
	com.amazonaws.*region*.redshift-fips
Amazon Redshift Data API	com.amazonaws.*region*.redshift-data

AWS のサービス	サービス名
	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 RoboMaker	com.amazonaws.*region*.robomaker
Amazon S3	com.amazonaws.region.s3
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	aws.sagemaker.*region*.notebook
	aws.sagemaker.*region*.studio
	com.amazonaws.*region*.sagemaker.api
	com.amazonaws.*region*.sagemaker.featurestore-runtime
	com.amazonaws.*region*.sagemaker.metrics
	com.amazonaws.*region*.sagemaker.runtime
	com.amazonaws.*region*.sagemaker.runtime-fips
AWS Secrets Manager	com.amazonaws.*region*.secretsmanager
AWS Security Hub	com.amazonaws.*region*.securityhub
AWS Security Token Service	com.amazonaws.*region*.sts

AWS のサービス	サービス名
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 Systems Manager	com.amazonaws.*region*.ec2messages
	com.amazonaws.*region*.ssm
	com.amazonaws.*region*.ssm-contacts
	com.amazonaws.*region*.ssm-incidents
	com.amazonaws.*region*.ssmmessages
AWS 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

AWS のサービス	サービス名
Amazon Timestream	com.amazonaws.*region*.timestream.ingest-*cell*
	com.amazonaws.*region*.timestream.query-*cell*
InfluxDB 用の Amazon Timestream	com.amazonaws.*region* .timestream-infuxdb
Amazon Transcribe	com.amazonaws.*region*.transcribe
	com.amazonaws.*region*.transcribestreaming
Amazon Transcribe Medical	com.amazonaws.*region*.transcribe
	com.amazonaws.*region*.transcribestreaming
AWS Transfer for SFTP	com.amazonaws.*region*.transfer
	com.amazonaws.*region*.transfer.server
Amazon Translate	com.amazonaws.*region*.translate
AWS Trusted Advisor	com.amazonaws.*region*.trustedadvisor
Amazon Verified Permissions	com.amazonaws.*region*.verifiedpermissions
Amazon VPC Lattice	com.amazonaws.*region*.vpc-lattice
Amazon WorkSpaces	com.amazonaws.region.workspaces
Amazon WorkSpaces 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 VpcEndpointPolicySupported の値をチェックします。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 、指定され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",
    "com.amazonaws.us-east-1.cleanrooms-ml",
    "com.amazonaws.us-east-1.cloudtrail",
    "com.amazonaws.us-east-1.codeguru-profiler",
    "com.amazonaws.us-east-1.codeguru-reviewer",
    "com.amazonaws.us-east-1.codepipeline",
    "com.amazonaws.us-east-1.codewhisperer",
    "com.amazonaws.us-east-1.datasync",
    "com.amazonaws.us-east-1.datazone",
    "com.amazonaws.us-east-1.deadline.management",
    "com.amazonaws.us-east-1.deadline.scheduling",
    "com.amazonaws.us-east-1.deviceadvisor.iot",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.elastic-inference.runtime",
    "com.amazonaws.us-east-1.email-smtp",
    "com.amazonaws.us-east-1.grafana-workspace",
    "com.amazonaws.us-east-1.iot.credentials",
    "com.amazonaws.us-east-1.iot.data",
    "com.amazonaws.us-east-1.iotwireless.api",
    "com.amazonaws.us-east-1.lorawan.cups",
    "com.amazonaws.us-east-1.lorawan.lns",
    "com.amazonaws.us-east-1.macie2",
    "com.amazonaws.us-east-1.neptune-graph",
    "com.amazonaws.us-east-1.nimble",
    "com.amazonaws.us-east-1.organizations",
    "com.amazonaws.us-east-1.outposts",
    "com.amazonaws.us-east-1.pipes-data",
    "com.amazonaws.us-east-1.redshift-data",
    "com.amazonaws.us-east-1.redshift-data-fips",
    "com.amazonaws.us-east-1.refactor-spaces",
```

```
    "com.amazonaws.us-east-1.sagemaker.runtime-fips",
    "com.amazonaws.us-east-1.storagegateway",
    "com.amazonaws.us-east-1.transfer",
    "com.amazonaws.us-east-1.transfer.server",
    "com.amazonaws.us-east-1.verifiedpermissions"
]
```

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の IPv6 経由で 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.athena",
    "com.amazonaws.us-east-1.data-servicediscovery",
    "com.amazonaws.us-east-1.data-servicediscovery-fips",
    "com.amazonaws.us-east-1.eks-auth",
    "com.amazonaws.us-east-1.glue",
    "com.amazonaws.us-east-1.lakeformation",
    "com.amazonaws.us-east-1.quicksight-website",
    "com.amazonaws.us-east-1.s3-outposts",
    "com.amazonaws.us-east-1.servicediscovery",
    "com.amazonaws.us-east-1.servicediscovery-fips",
    "com.amazonaws.us-east-1.timestream-influxdb"
]
```

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。

VPC から指定した各サブネット内にエンドポイントの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

- VPC の にアクセスするリソース AWS のサービス をデプロイします。
- プライベート DNS を使用するには、VPC の DNS ホスト名と DNS 解決を有効にする必要があります。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で IPv6 を有効にするには、 が IPv6 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。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。
- VPC 内のリソースからの予想されるトラフィックを許可する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ます。例えば、 が HTTPS リクエストを に送信 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 ACL を持つサブネットにある場合は、ネットワーク ACL が VPC 内のリソース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 エンドポイントの作成

次の手順を使用して、 AWS のサービス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。

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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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. [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. [VPC] で、 AWS のサービスにアクセスする VPC を選択します。
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 名を有効にする] を選択します。この選択を行うと、自動的に [インバウンドエンドポイントでのみプライベート DNS を有効にする] が選択されます。Amazon S3 のインターフェイスエンドポイントにのみ、インバウンド Resolver エンドポイントでプライベート DNS 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に対してのみプライベート DNS 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は、[追加設定] の [DNS 名を有効にする] が既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、 AWS SDK 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 VPC エンドポイントに解決されます。
8. [Subnets] (サブネット) で、 AWS のサービスにアクセス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。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。

選択した各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ースの IP アドレスを選択するには、[IP アドレスの指定] を選択し、サブネットアドレス範囲から IPv4 アドレスを入力します。エンドポイントサービスが IPv6 をサポートしている場合は、サブネットアドレス範囲から IPv6 アドレスを入力することもできます。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] — IPv4 アドレスをエンドポイントの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 の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] — IPv6 アドレスをエンドポイントの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が IPv6 のみのサブネットで、サービスが IIPv6 リクエストを受け入れる場合にのみサポートされます。
   - [Dualstack] — IPv4 と IPv6 の両方のアドレスをエンドポイントの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 の両方のアドレス範囲があり、サービスが IPv4 リクエストと IPv6 リクエストの両方を受け入れる場合にのみサポートされます。

10. [セキュリティグループ] で、VPC 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、VPC のデフォルトセキュリティグループが関連付けられます。

11. [Policy] (ポリシー) で [Full access] (フルアクセス) を選択して、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 VPC エンドポイント経由の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、[Custom] (カスタム) を選択して、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にプリンシパルが持つ許可を制御する VPC エンドポイントポリシーをアタッチします。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 (Tools for Windows PowerShell)

共有サブネット

自分と共有されているサブネットで 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、VPC エンドポイントを使用することはできます。

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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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ースの IP アドレスを選択するには、[IP アドレスの指定] を選択し、サブネットアドレス範囲から IPv4 アドレスを入力します。エンドポイントサービスが IPv6 をサポートしている場合は、サブネットアドレス範囲から IPv6 アドレスを入力することもできます。

   この VPC 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ースがすでに存在するサブネットの IP アドレスを指定すると、エンドポイントのネットワークインターフェースが新しく置き換わります。このプロセスにより、サブネットと VPC エンドポイントは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 (Tools for Windows 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は、VPC のリソースからエンドポイントのネットワークインターフェイスに対して許可されているトラフィックを制御します。

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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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 (Tools for Windows 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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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. [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ポリシーを変更するには

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

プライベート DNS 名を有効にする

の 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、 AWS SDK 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 VPC エンドポイントに解決されます。

プライベート DNS 名を使用するには、VPC 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。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される DNS レコードはプライベートです。そのため、プライベート DNS 名はパブリックに解決可能ではありません。

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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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)、[Modify private DNS name] (プライベート DNS 名の変更) の順に選択します。
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有効にする] を選択すると、[インバウンドエンドポイントに対してのみプライベート DNS 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でのみプライベート DNS を有効にする] をオフにします。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に対してのみプライベート DNS を有効にする] を選択すると、次のステップで変更を保存するときに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. [変更の保存] を選択します。

コマンドラインを使用してプライベート DNS 名のオプションを変更するには

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint (Tools for Windows 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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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. [保存] 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

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

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の通知を作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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. [Notification ARN] (通知 ARN) で、作成した SNS トピックの ARN 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-notification (AWS CLI)
- New-EC2VpcEndpointConnectionNotification (Tools for Windows 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次のような通知を発行 AWS PrivateLink できるようにします。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、KMS キーのリソースポリシーは AWS KMS API オペレーションを呼び出す AWS PrivateLink ために 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

不要になった VPC エンドポイントは、削除することができます。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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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)、[Delete VPC endpoints] (VPC エンドポイントを削除) の順に選択します。
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 (Tools for Windows 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、VPC 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、Amazon S3 および DynamoDB への信頼性の高い接続を提供します。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。

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

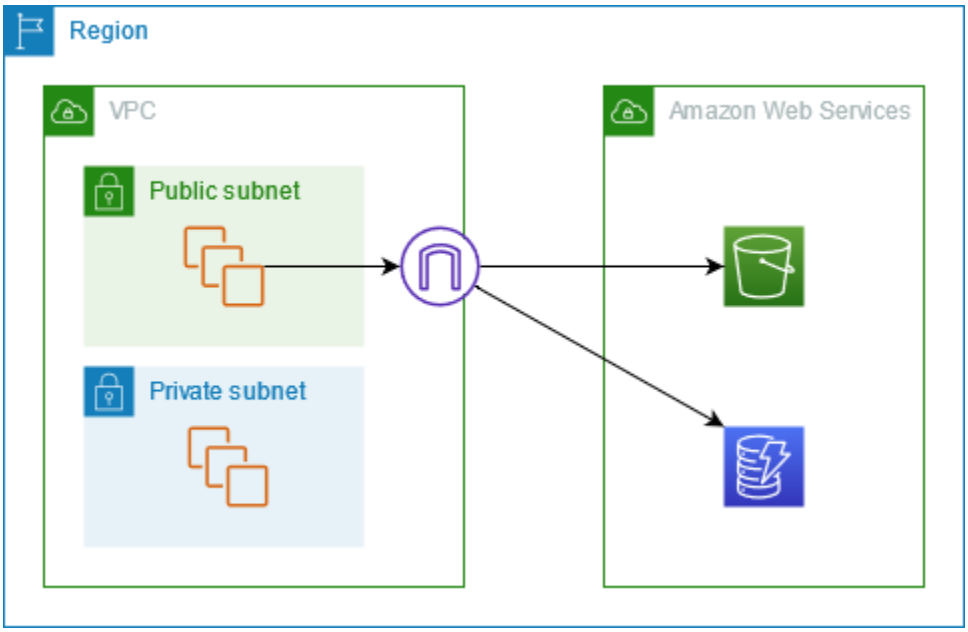
- Amazon S3 のゲートウェイエンドポイント
- Amazon DynamoDB のゲートウェイエンドポイント

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。

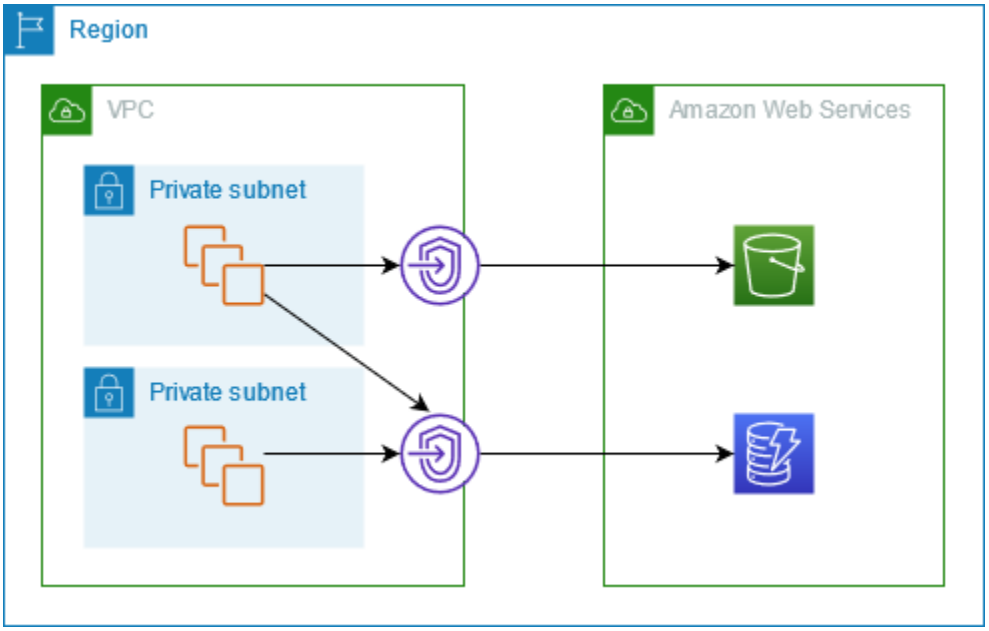
インターネットゲートウェイ経由でアクセスする

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、VPC のためにインターネットゲートウェイにルーティングされ、その後に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、パブリックサブネットに NAT デバイスを追加し、プライベートサブネットのトラフィックを NAT デバイスにルーティングする必要があります。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。VPC から Amazon S3 または DynamoDB 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の提供」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であり AWS 、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のサブネットにおけるネットワーク ACL でも、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。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 アドレス範囲は取得できます。

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
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 エンドポイントを使用して、VPC 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、そのエンドポイントをルートテーブル内のターゲットとして、VPC から Amazon S3 に送信されるトラフィック用に追加できます。

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して、VPC 用の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、VPC から Amazon S3 にアクセスすることができます。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 リージョンのピア接続された VPCs、またはトランジットゲートウェイから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 における VPC エンドポイントのタイプ」を参照してください。

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、VPC 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。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 AWSによって維持されている IP アドレスに正しく解決されることを確認してください。
- 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通じて Amazon S3 にアクセスするインスタンスのサブネットのネットワーク ACL 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 IP アドレス範囲は Amazon S3 のプレフィックスリストから取得できます。
- 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必要とする場合や、ドライバーまたはエージェントを EC2 インスタンスにダウンロード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 へのリクエストでは、アイデンティティポリシーおよび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。ルートテーブルを使用して、VPC エンドポイントから 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 によって受信される、影響を受けるサブネット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 VPC のプライベート IPv4 アドレスに変更されます。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。
- エンドポイントの接続を、VPC から延長することはできません。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 VPC 内の AWS Direct Connect 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、VPC あたりのゲートウェイエンドポイントの数は 255 に制限されています。

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、プライベート DNS を設定してコストを最適化できます。

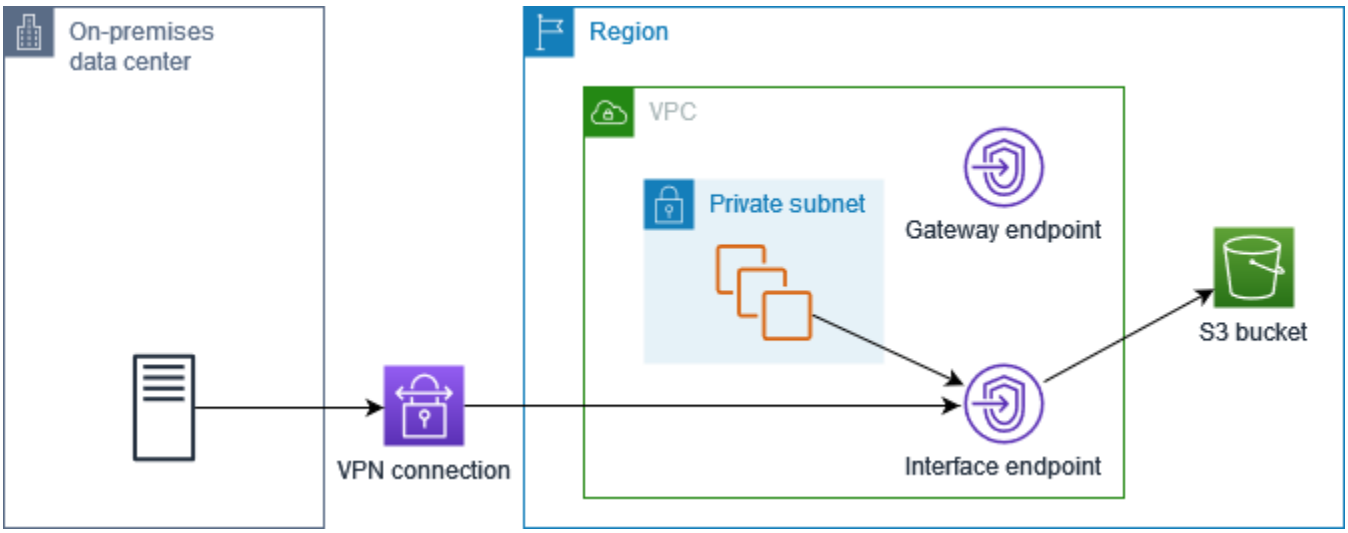
Route 53 Resolver

Amazon は、「Route 53 Resolver」と呼ばれる VPC 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、VPC の外部から Route 53 Resolver を使用することはできません。Route 53 は、VPC の外から Route 53 Resolver を使用できるように、Resolver エンドポイントと Resolver ルールを提供します。インバウンド Resolver エンドポイントは、DNS クエリをオンプレミスネットワークから Route 53 Resolver に転送します。アウトバウンド Resolver エンドポイントは、Route 53 Resolver から DNS クエリをオンプレミスネットワークに転送します。

Amazon S3 のインターフェイスエンドポイントをインバウンド Resolver エンドポイントにのみプライベート DNS を使用するように設定すると、インバウンド Resolver 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、オンプレミスからの Amazon S3 への DNS クエリを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て、VPC からの DNS クエリが Amazon S3 のパブリック IP アドレスに解決され、トラフィックがゲートウェイエンドポイントにルーティングされるようにします。

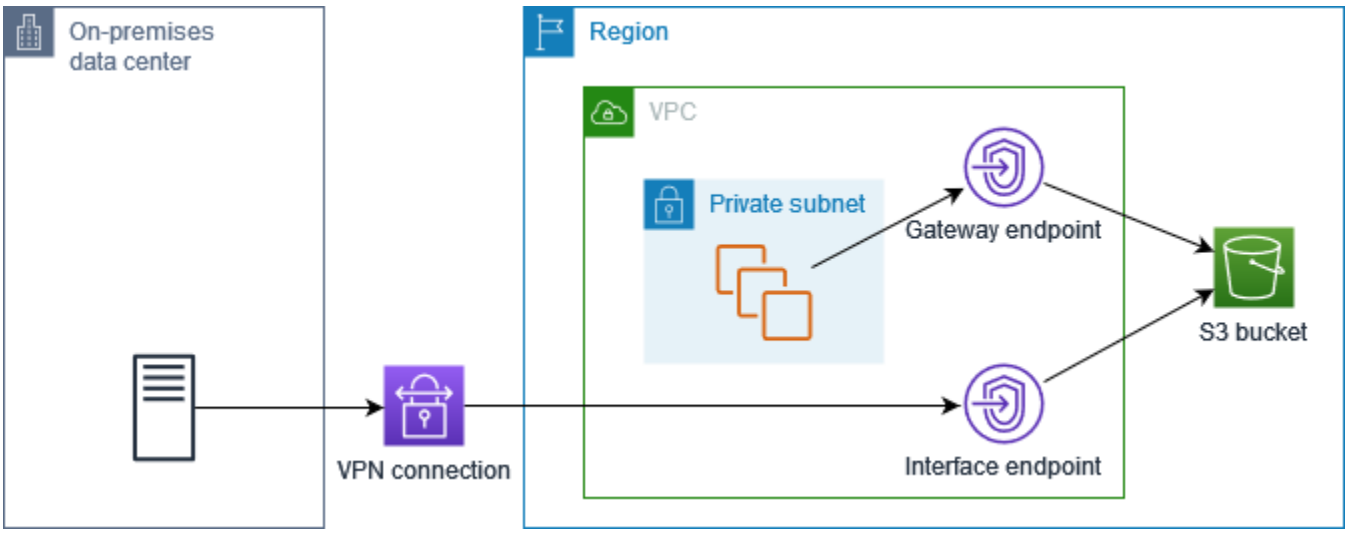
プライベート DNS

Amazon S3 のインターフェイスエンドポイントにはプライベート DNS を設定し、インバウンドの Resolver エンドポイントにのみプライベート DNS を設定しない場合、オンプレミスネットワークと VPC 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を使用して Amazon S3 にアクセスします。そのため、追加料金なしでゲートウェイエンドポイントを使用する代わりに、VPC からのトラフィックにはインターフェイスエンドポイントを使用するため料金が発生します。



インバウンド Resolver エンドポイント専用のプライベート DNS

インバウンドの Resolver エンドポイントのみにプライベート DNS 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、VPC からのリクエストはゲートウェイエンドポイントを使用して 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 DNS の設定

Amazon S3 のインターフェイスエンドポイントのプライベート DNS 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 エンドポイントの作成” (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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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 = Gateway を追加し、com.amazonaws.*region* .s3 を選択します。
6. [VPC] で、エンドポイントを作成する先の VPC 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. [Policy] (ポリシー) で [Full access] (フルアクセス) を選択して、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 VPC エンドポイント経由の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、[Custom] (カスタム) を選択して、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にプリンシパルが持つ許可を制御する 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 (Tools for Windows 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、VPCs、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 VPC へのアクセスを制限する

aws:sourceVpc 条件キーを使用して、特定の VPC 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 VPC で複数のエンドポイントを設定済みである場合に便利です。次のポリシーは、リクエストが指定された VPC 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",
      "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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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、VPC から Amazon S3 へのエンドポイント経由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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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. [保存] 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、VPC AWS のサービス 内に S3 バケットを使用する他の 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 が有効になった場合、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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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)、[Delete VPC endpoints] (VPC エンドポイントを削除) の順に選択します。
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 (Tools for Windows PowerShell)

Amazon DynamoDB のゲートウェイエンドポイント

ゲートウェイ VPC エンドポイントを使用して、VPC 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、そのエンドポイントをルートテーブル内のターゲットとして、VPC から DynamoDB に送信されるトラフィック用に追加できます。

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ます。ゲートウェイエンドポイントを使用すると、VPC 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、追加コストもかかりません。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 リージョンのピア接続された VPCs、またはトランジットゲートウェイから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、VPC 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。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 AWSによって維持されている IP アドレスに正しく解決されることを確認してください。
- 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通じて DynamoDB にアクセスするインスタンスのサブネットのネットワーク ACL 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 VPC 内の EC2 インスタンスのプライベート IP アドレスと、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 VPC のプライベート IPv4 アドレスに変更されます。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。
- エンドポイントの接続を、VPC から延長することはできません。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 VPC 内の AWS Direct Connect 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、VPC あたりのゲートウェイエンドポイントの数は 255 に制限されています。

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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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. [VPC] で、エンドポイントを作成する先の VPC 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. [Policy] (ポリシー) で [Full access] (フルアクセス) を選択して、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 VPC エンドポイント経由の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、[Custom] (カスタム) を選択して、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にプリンシパルが持つ許可を制御する 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 (Tools for Windows 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",
         "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 ロールに対するアクセス権を付与します。

```
{
   "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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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、VPC から DynamoDB へのエンドポイント経由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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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. [保存] 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 (Tools for Windows 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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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)、[Delete VPC endpoints] (VPC エンドポイントを削除) の順に選択します。
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 (Tools for Windows PowerShell)

経由で SaaS 製品にアクセスする AWS PrivateLink

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

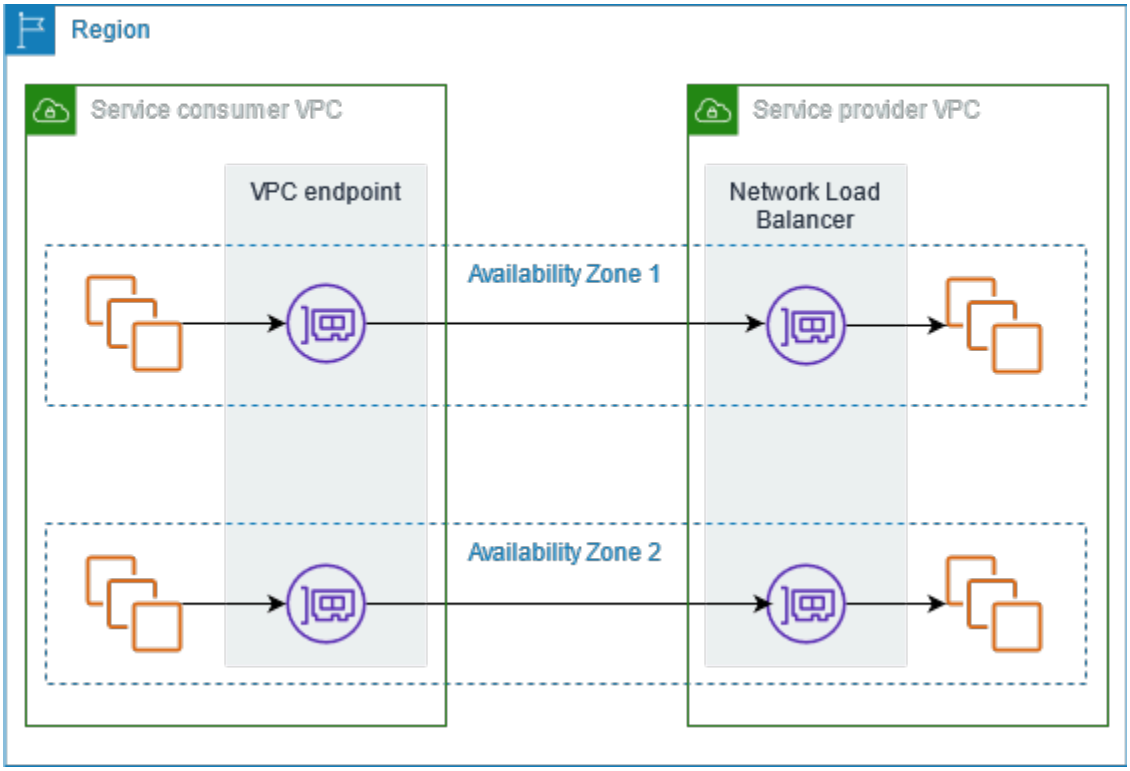
内容

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、「: AWS Marketplace- PrivateLink」を参照してください。

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として、VPC 内の 1 つ以上のサブネットと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 VPC 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

次の手順を使用して、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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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. からサービスを購入した場合は AWS Marketplace、次の操作を行います。
    a. [Service category] (サービスカテゴリ) で、[AWS Marketplace services] (のサービス) を選択します。
    b. サービスの名前を入力します。
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. サービスカテゴリ 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、[Verify service] (サービスを検証) を選択します。

6. [VPC] で、製品にアクセスする VPC を選択します。
7. [Subnets] (サブネット) で、製品にアクセス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。
8. [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。セキュリティグループのルールは、VPC 内のリソースとエンドポイントの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。VPC エンドポイントサービスを作成するときに、Gateway Load Balancer を指定します。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

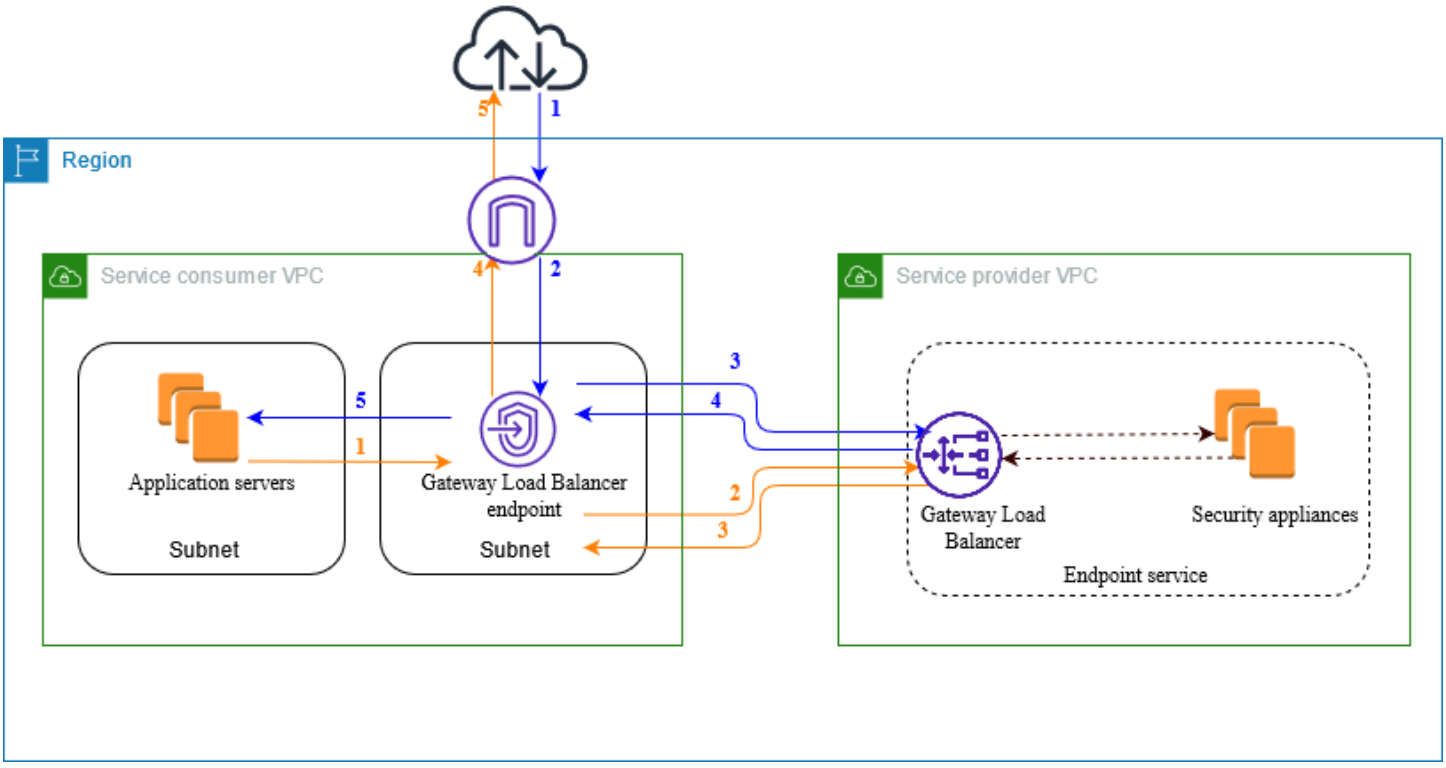
Gateway Load Balancer エンドポイントが各アベイラビリティーゾーンでプロビジョニングされる 1 時間ごとに課金されます。また、処理されたデータの GB ごとに課金されます。詳細については、「AWS PrivateLink の料金」を参照してください。

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 VPC のサブネットで実行されます。同じ VPC の別のサブネットで Gateway Load Balancer エンドポイントを作成します。インターネットゲートウェイを経由してサービスコンシューマー VPC 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、その後、送信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を介してサービスコンシューマー VPC 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、自社のセキュリティアプライアンスが IPv4 のみをサポートしている場合でも、IPv4、IPv6、または IPv4 と IPv6 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使用できるようにすることができます。dualstack 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できます。

Gateway Load Balancer エンドポイントが IPv4 をサポートしている場合、エンドポイントのネットワークインターフェイスは IPv4 アドレスを持ちます。Gateway Load Balancer エンドポイントが IPv6 をサポートしている場合、エンドポイントのネットワークインターフェイスは IPv6 アドレスを持ちます。エンドポイントの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することはできません。エンドポイントのネットワークインターフェイスを IPv6 アドレスで記述する場合は、`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用に IPv6 を有効にするための要件

- エンドポイントサービスの VPC とサブネットには、IPv6 CIDR ブロックが関連付けられている必要があります。
- 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 エンドポイントで IPv6 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 アドレスのタイプが必要です。
- 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] — IPv4 アドレスをエンドポイントの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 アドレス範囲がある場合にのみサポートされます。

  - [IPv6] — IPv6 アドレスをエンドポイントの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が IPv6 のみのサブネットである場合にのみサポートされます。
  - [Dualstack] — IPv4 と IPv6 の両方のアドレスをエンドポイントの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 の両方の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 VPC のサブネットのルートテーブルは IPv6 トラフィックをルーティングする必要があり、これらのサブネットのネットワーク ACL 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。dualstack の設定には IPv6 ルートが含まれています。

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
############ IPv4 CIDR	*vpc-endpoint-id*
############ 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
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、 を使用する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

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 ID を使用して、サービスのアベイラビリティ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IDs」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

- サービスを使用可能にするアベイラビリティゾーンに 2 つ以上のサブネットを持つサービスプロバイダー VPC 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 VPC で Gateway Load Balancer を作成します。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 dualstack の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の VPC でセキュリティアプライアンスを起動し、ロードバランサーのターゲットグループに登録します。

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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
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。
   - [IPv4] を選択 – エンドポイントサービスが IPv4 リクエストを受け入れることができるようにします。
   - [IPv6] を選択 – 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します。
   - [IPv4] と [IPv6] を選択 – エンドポイントサービスが IPv4 と IPv6 の両方のリクエストを受け入れることができるようにします。
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. [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 (Tools for Windows 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。

VPC から指定した各サブネット内にエンドポイントの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 VPC で選択できるアベイラビリティゾーンは 1 つだけです。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 ID を使用して、サービスのアベイラビリティ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IDs」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 エンドポイントを介して VPC 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、VPC 内のリソースによって開始されたトラフィックに対してのみレスポンスを返します。
- 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。
- ターゲットが Network Load Balancer と同じ VPC にあっても、トラフィックがゲートウェイロードバランサーエンドポイントを介してルーティングされる場合、Network Load Balancer のクライアント IP の保存はサポートされません。
- 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ゾーンに少なくとも 2 つのサブネットを持つサービスコンシューマー VPC 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 ACL を持つサブネットにある場合は、ネットワーク ACL がエンドポイントのネットワークインターフェイスと VPC 内のリソース間のトラフィックを許可していることを確認します。

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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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、[Other endpoint services] (その他のエンドポイントサービス) 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. [VPC] で、エンドポイントを作成する先の VPC を選択します。
7. [Subnets] (サブネット) で、エンドポイントを作成するサブネットを選択します。
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] — IPv4 アドレスをエンドポイントの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 アドレス範囲がある場合にのみサポートされます。

- [IPv6] — IPv6 アドレスをエンドポイントの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が IPv6 のみのサブネットである場合にのみサポートされます。
- [Dualstack] — IPv4 と IPv6 の両方のアドレスをエンドポイントの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 の両方の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 (Tools for Windows PowerShell)

ルーティングを設定する

次の手順を使用して、サービスコンシューマー VPC のルートテーブルを設定します。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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
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. IPv4 をサポートしている場合は、[Add route] (ルートを追加) を選択します。[Destination] (送信先) 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。[Target] (ターゲット) で、VPC エンドポイントを選択します。
   c. IPv6 をサポートしている場合は、[Add route] (ルートを追加) を選択します。[Destination] (送信先) 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。[Target] (ターゲット) で、VPC エンドポイントを選択します。

d. [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. IPv4 をサポートしている場合は、[Add route] (ルートを追加) 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、VPC エンドポイントを選択します。

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

   d. [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. IPv4 をサポートしている場合は、[Add route] (ルートを追加) 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. IPv6 をサポートしている場合は、[Add route] (ルートを追加) 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. [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 (Tools for Windows 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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。

2. ナビゲーションペインで、[Endpoints] (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. [保存] 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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
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)

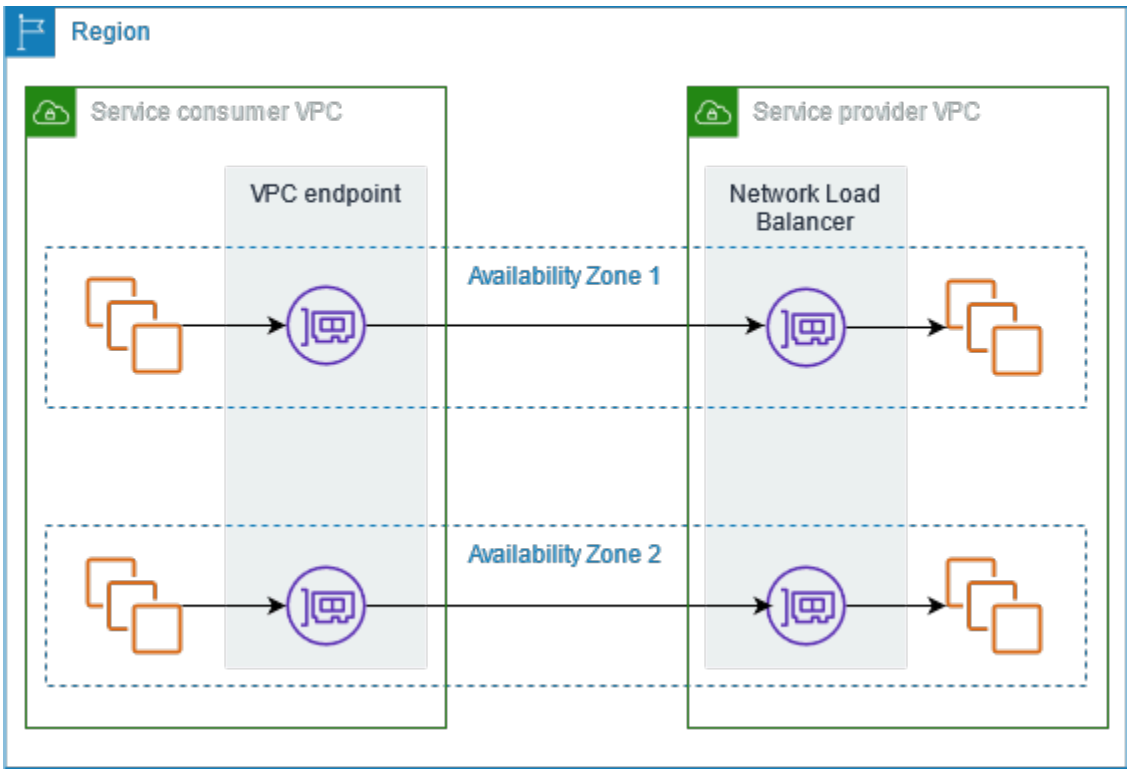
を通じてサービスを共有する AWS PrivateLink

エンドポイントサービス と呼ばれる独自の AWS PrivateLink サービス をホストし、他の の AWS 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として、サービスのフロントエンドとして VPC で Network Load Balancer を作成します。その後、VPC エンドポイントサービスの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、お客様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 から選択したサブネットとエンドポイントサービス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レベルおよびゾーンレベルの 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.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-zone.endpoint_service_id.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にプライベート 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 名を使用して引き続きサービスにアクセスできます。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た場合、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 DNS を有効にしていない場合、サービスコンシューマーは VPC エンドポイントサービス用にパブリック 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 名を管理する」を参照してください。

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 IPv4 のみをサポートしている場合でも、IPv4、IPv6、または IPv4 と IPv6 の両方を介してサービスエンドポイントをサービスコンシューマーが使用できるようにすることができます。dualstack 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できます。

インターフェイス VPC エンドポイントが IPv4 をサポートしている場合、エンドポイントのネットワークインターフェイスは IPv4 アドレスを持ちます。インターフェイス VPC エンドポイントが IPv6 をサポートしている場合、エンドポイントのネットワークインターフェイスは IPv6 アドレスを持ちます。エンドポイントの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することはできません。エンドポイントのネットワークインターフェイスを IPv6 アドレスで記述する場合は、`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用に IPv6 を有効にするための要件

- エンドポイントサービスの VPC とサブネットには、IPv6 CIDR ブロックが関連付けられている必要があります。
- 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 ヘッダーのソース IP アドレスを処理する場合、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用に IPv6 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する必要があります。
- 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] — IPv4 アドレスをエンドポイントの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 アドレス範囲がある場合にのみサポートされます。
  - [IPv6] — IPv6 アドレスをエンドポイントの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が IPv6 のみのサブネットである場合にのみサポートされます。
  - [Dualstack] — IPv4 と IPv6 の両方のアドレスをエンドポイントの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 の両方のアドレス範囲がある場合にのみサポートされます。

インターフェイスエンドポイントの DNS レコード IP アドレスのタイプ

インターフェイスエンドポイントがサポートする DNS レコードの IP アドレスのタイプによって、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 IP アドレスのタイプと互換性がある必要があります。

- [IPv4] — プライベート、リージョンレベル、ゾーンレベルの DNS 名の A レコードを作成します。IP アドレスのタイプは [IPv4] または [Dualstack] である必要があります。
- [IPv6] — プライベート、リージョンレベル、ゾーンレベルの DNS 名の AAAA レコードを作成します。IP アドレスのタイプは [IPv6] または [Dualstack] である必要があります。
- [Dualstack] — プライベート、リージョンレベル、ゾーンレベルの DNS 名の A および 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、 を使用する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。VPC ピアリングを使用して、他のリージョンからエンドポイントサービスにアクセスできます。
- エンドポイントサービスは、TCP 経由のトラフィックのみをサポートします。
- 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 ID を使用して、サービスのアベイラビリティ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IDs」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の ID 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。
- 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

- サービスを使用可能にする各アベイラビリティ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用に VPC を作成します。
- サービスコンシューマーがエンドポイントサービス用に IPv6 インターフェイス VPC エンドポイントを作成できるようにするには、VPC とサブネットに IPv6 CIDR ブロックが関連付けられている必要があります。
- VPC でNetwork Load Balancer を作成します。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、 経由の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、「Network Load Balancer ユーザーガイド」の「セキュリティグループ」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 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。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 ヘッダーから送信元 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てください。
- 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。すべての有効なアベイラビリティゾーンでインスタンスを起動しない場合、クロスゾーン負荷分散を有効にして、ゾーンレベルの DNS ホスト名を使用するサービスコンシューマーがサービスにアクセスするの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、「Network Load Balancer ユーザーガイド」の「クロスゾーン負荷分散」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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
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。含まれているアベイラビリティーゾーンには、選択した Network Load Balancer で有効になっているアベイラビリティーゾーンが一覧表示されます。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使用できます。
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. [Enable private DNS name] (プライベート DNS 名を有効にする) で、[Associate a private DNS name with the service] (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 によって提供されるエンドポイント固有の DNS 名を使用できます 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 名を管理する」を参照してください。
8. [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。

   - [IPv4] を選択 – エンドポイントサービスが IPv4 リクエストを受け入れることができるようにします。
   - [IPv6] を選択 – 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します。
   - [IPv4] と [IPv6] を選択 – エンドポイントサービスが IPv4 と IPv6 の両方のリクエストを受け入れることができるようにします。

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. [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 (Tools for Windows 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 VPC 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。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、次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。

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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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、[Other endpoint services] (その他のエンドポイントサービス) を選択します。

5. [Service name] (サービス名) にサービスの名前 (`com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc` など) を入力し、[Verify service] (サービスを検証) を選択します。
6. VPC で、エンドポイントを作成する先の VPC を選択します。
7. [Subnets] (サブネット) で、エンドポイントサービスにアクセスするサブネット (アベイラビリティゾーン) を選択します。
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] — IPv4 アドレスをエンドポイントの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 の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] — IPv6 アドレスをエンドポイントの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が IPv6 のみのサブネットで、エンドポイントサービスが IIPv6 リクエストを受け入れる場合にのみサポートされます。
   - [Dualstack] — IPv4 と IPv6 の両方のアドレスをエンドポイントの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 の両方のアドレス範囲があり、エンドポイントサービスが IPv4 リクエストと IPv6 リクエストの両方を受け入れる場合にのみサポートされます。

9. [DNS record IP type] (DNS レコードの IP のタイプ) で、次のオプションから選択します。

   - [IPv4] — プライベート、リージョンレベル、ゾーンレベルの DNS 名の A レコードを作成します。IP アドレスのタイプは [IPv4] または [Dualstack] である必要があります。
   - [IPv6] — プライベート、リージョンレベル、ゾーンレベルの DNS 名の AAAA レコードを作成します。IP アドレスのタイプは [IPv6] または [Dualstack] である必要があります。
   - [Dualstack] — プライベート、リージョンレベル、ゾーンレベルの DNS 名の A および 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。
   - [Service defined] (定義されたサービス) — プライベート、リージョンレベル、ゾーンレベルの DNS 名に A レコードを作成し、リージョンレベルおよびゾーンレベルの DNS 名に 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。

10. [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。
11. [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 (Tools for Windows 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
- ロードバランサーの管理
- プライベート DNS 名を関連付ける
- 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を組み合わせることで、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 VPC 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 (ARN) が必要です。次のリストには、サポートされている AWS プリンシパルの ARN 例が含まれています。

AWS プリンシパルARNs

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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
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。[Principals to add] (追加するプリンシパル) で、プリンシパルの ARN 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-permissions (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を組み合わせることで、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。

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。

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。
- 既に承諾されたリクエストを拒否しても、エンドポイントとサービス間の接続には影響しません。

コンソールを使用して承諾の設定を変更するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
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 (Tools for Windows 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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
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)

ロードバランサーの管理

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を有効にすることもできます。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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
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。例:
    - ロードバランサーのチェックボックスをオンにして、エンドポイントサービスに関連付けます。

- ロードバランサーとエンドポイントサービスの関連付けを解除するには、このチェックボックスをオフにします。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。
- ロードバランサーで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、インクルード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. [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 を指定して 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 名を管理する」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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
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)、[Modify private DNS name] (プライベート DNS 名の変更) の順に選択します。
5. [Associate a private DNS name with the service] (プライベート DNS 名をサービスに関連付ける) を選択して、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. [変更の保存] をクリックします。

7. プライベート DNS 名は、検証ステータスが [verified] (検証済み) になると、サービスコンシューマーによる使用が可能となります。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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
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) を選択し、[Verify domain ownership for private DNS name] (プライベート DNS 名のドメイン所有権を検証) 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 (Tools for Windows PowerShell)

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

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。
   - [IPv4] を選択 – エンドポイントサービスが IPv4 リクエストを受け入れることができるようにします。
   - [IPv6] を選択 – 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します。
   - [IPv4] と [IPv6] を選択 – エンドポイントサービスが IPv4 と IPv6 の両方のリクエストを受け入れることができるようにします。
6. [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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
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. [保存] 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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
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、[Endpoint connections] (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. [保存] 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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
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、[Allow principals] (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. [保存] 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の DNS 名を管理する

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エンドポイントサービスのプライベート DNS 名として既存のパブリック DNS 名を使用する場合、サービスコンシューマーは、既存のパブリック DNS 名を使用するアプリケーションを変更する必要はありません。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はプライベート DNS 名を 1 つだけ持つことができます。
- サービスコンシューマーの VPC 内のサーバーのみがプライベート DNS 名を解決できるようにするため、プライベート DNS 名の A レコードを作成しないでください。
- 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ません。
- 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 文字を超えないようにする必要があります。

  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。次に、b.example.com をプライベート DNS 名として追加するとします。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。

ドメインの所有権の検証

お客様のドメインは、DNS プロバイダーを介して管理する一連のドメインネームサービス (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一種の DNS レコードです。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。

その TXT レコードがドメインの DNS 設定内にあることが検出されると、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。[Actions] (アクション) を選択し、[Verify domain ownership for private DNS name] (プライベート DNS 名のドメイン所有権を検証) を選択します。

プライベート DNS 名は、検証ステータスが [verified] (検証済み) になると、サービスコンシューマーによる使用が可能となります。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ときに `Value` と `Name` 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。次のテーブルは、TXT レコード設定の例です。

名前	タイプ	値
_6e86v84tqgqubxbwii1m.example.com	TXT	vpce:l6p0E RxlTt45jevFwOCp

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、単に「example.com」を TXT レコードで使用できます。

「_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 プロバイダ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、[TXT] を選択します。
- [TTL (seconds)] (TTL (秒)) に **1800** と入力します。
- [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。指定された名前と値で 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には、最大 48 時間かかることがありますが、多くの場合それよりも大幅に早く有効になります。

より具体的な方法については、DNS プロバイダーのドキュメントを参照してください。次のテーブルには、いくつかの主要なプロバイダーに関するドキュメントへのリンクが記載されています。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 レコードを管理する
HostGator	HostGator/eNom で DNS レコードを管理する
Namecheap	ドメインの TXT/SPF/DKIM/DMARC レコードを追加する方法
Names.co.uk	ドメインの DNS 設定の変更
Wix	Wix アカウントの TXT レコードの追加または更新

TXT レコードが発行されているかを確認する

次のステップを使用して、プライベート DNS 名ドメインの所有権の検証 TXT レコードが DNS サーバーに正しく発行されているかどうかを検証できます。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 サーバーにはドメイン up-to-date の最新情報が含まれているため、これらのサーバーにクエリを実行します。ドメイン情報が他の DNS サーバーに伝達されるまでには時間がかかります。

TXT レコードが DNS サーバーに公開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、前の手順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、`text =` に続く文字列が TXT 値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 レコード名でアンダースコアを許可しているかどうかを確認してください。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、TXT レコードからドメイン検証名 (例：「_6e86v84tqgqubxbwii1m」) を省略できます。
- DNS プロバイダーが TXT レコードの末尾にドメイン名を追加したかどうかを確認します。一部の DNS プロバイダは、TXT レコードの属性名にドメイン名を自動的に追加します。ドメイン名のこの重複を避けるために、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。これは、ドメイン名を TXT レコードに追加する必要はないことを DNS プロバイダーに伝えます。
- DNS プロバイダーが、小文字のみを使用するように DNS レコードの値を変更していない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 レコードの値を小文字のみを使用するように変更した場合は、その DNS プロバイダーにお問い合わせください。
- 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の複数の 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

ることを許可しているかどうかを確認してください。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、最初のリージョンの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。

お客様の 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再度ドメインを検証することができます。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、トピックに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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
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. [Notification ARN] (通知 ARN) で、作成した SNS トピックの ARN 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-notification (AWS CLI)
- New-EC2VpcEndpointConnectionNotification (Tools for Windows PowerShell)

アクセスポリシーを追加する

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次のような通知を発行 AWS PrivateLink できるようにします。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、KMS キーのリソースポリシーは AWS KMS API オペレーションを呼び出す AWS PrivateLink ために 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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
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-configurations (AWS CLI)
- Remove-EC2EndpointServiceConfiguration (Tools for Windows 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する) かを制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

内容

対象者

AWS Identity and Access Management (IAM) の使用方法は、 で行う作業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しておくと、管理者に適切な許可をリクエストするうえで役立ちます。

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、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。

IAM 管理者 - 管理者は、 AWS PrivateLinkへのアクセスを管理するポリシーの書き込み方法の詳細について確認する場合があります。

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。フェデレーティッドアイデンティティとしてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。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、「 ユーザーガイド」の「 へのサインイン AWS アカウント方法AWS サインイン 」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 Software Development Kit (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を自分で署名する方法の詳細については、IAM ユーザーガイドの API AWS リクエストの署名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。例えば、 AWS では、多要素認証 (MFA) を使用してアカウントのセキュリティを向上させる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「Multi-factor authentication」(多要素認証) および『IAM ユーザーガイド』の「AWSにおける多要素認証 (MFA) の使用」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「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーティ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、一時的な認証情報を使用して にアクセスするための ID プロバイダーとのフェデレーションの使用を要求 AWS のサービス 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 にアクセスすると 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て、すべての AWS アカウント とアプリケーションで使用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「What is IAM Identity Center?」(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保有する IAM ユーザーを作成する代わりに、一時認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な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 ユーザーの集団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、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する権限を与えることができます。

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、ロールでは一時的な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 (ロールではなく) の作成が適している場合」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、特定のユーザーには関連付けられていません。ロール を切り替える AWS Management Console ことで、 で IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、 または AWS API AWS CLI オペレーションを呼び出すか、カスタム URL を使用します。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「IAM ロールの使用」を参照してください。

IAM ロールと一時的な認証情報は、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アイデンティティに権限を割り当てるには、ロールを作成してそのロールの権限を定義します。フェデレーティッドアイデンティティが認証されると、そのアイデンティティはロールに関連付けられ、ロールで定義されている権限が付与されます。フェデレーションの詳細については、『IAM ユーザーガイド』の「サードパーティーアイデンティティプロバイダー向けロールの作成」 を参照してください。IAM アイデンティティセンターを使用する場合、権限セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。権限セットの詳細については、『AWS IAM Identity Center ユーザーガイド』の「権限セット」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで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、別のアカウントの人物 (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権を付与する主な方法は、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) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスにおける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「IAM ロールとリソースベースのポリシーとの相違点」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、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの権限、サービスロール、またはサービスにリンクされた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 でアクションを実行する場合 AWS、ユーザーは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際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがありま

す。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストリクエストリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の 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受け取っ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「AWS のサービスにアクセス許可を委任するロールの作成」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権限を表示できますが、編集することはできません。

- Amazon EC2 で実行されているアプリケーション – 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的な認証情報を取得できます。詳細については、『IAM ユーザーガイド』の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して権限を付与する」を参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、『IAM ユーザーガイド』の「(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?」を参照してください。

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、 AWS ID またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 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 ポリシー概要」を参照してください。

管理者は AWS JSON ポリシーを使用して、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んなリソースにどんな条件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権限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継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの権限を定義します。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 API からロール情報を取得できます。

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 権限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「IAM ポリシーの作成」を参照してください。

アイデンティティベースポリシーは、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。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、『IAM ユーザーガイド』の「マネージドポリシーとインラインポリシーの比較」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、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。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制御できます。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では、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための権限を持つかをコントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、 AWS WAF、および Amazon VPC は、ACLs。ACL の詳細については、『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によって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限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。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) に対する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、 AWS アカウント ビジネスが所有する複数の 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 (SCP) を一部またはすべてのアカウントに適用できます。SCP 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を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、『AWS Organizations ユーザーガイド』の「SCP の仕組み」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与する場合に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「ポリシー評価ロジック」を参照してください。

が IAM と AWS PrivateLink 連携する方法

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 機能について学びます AWS PrivateLink。

で使用できる IAM の機能 AWS PrivateLink

IAM 機能	AWS PrivateLink サポート
アイデンティティベースのポリシー	Yes
リソースベースのポリシー	はい
ポリシーアクション	Yes
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	はい
ACL	No
ABAC (ポリシー内のタグ)	はい
一時的な認証情報	Yes
プリンシパル権限	Yes
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 連携する方法の概要を把握するには、IAM ユーザーガイドのAWS 「IAM と連携する のサービス」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 AWS PrivateLink

アイデンティティベースポリシーをサポートする	Yes

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 権限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「IAM ポリシーの作成」を参照してください。

IAM 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、およびアクションを許可または拒否す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「IAM JSON ポリシーの要素のリファレンス」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	はい

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。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制御できます。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、アカウント全体、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 にある場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。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追加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「IAM ロールとリソースベースのポリシーとの相違点」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 1 種類のリソースベースのポリシーをサポートします。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に対するサポート	はい

管理者は AWS JSON ポリシーを使用して、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んなリソースにどんな条件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`要素には、ポリシー内の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が記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない権限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。

AWS PrivateLink は API 名前空間を Amazon EC2 と共有します。のポリシーアクションは、アクションの前に次のプレフィックス AWS PrivateLink を使用します。

```
ec2
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

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

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、Describe という単語で始まるすべてのアクションを指定するには、次のアクションを含めます。

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

AWS PrivateLink アクションのリストを確認するには、Amazon EC2 API リファレンス」の「AWS PrivateLink アクション」を参照してください。詳細については、「サービス認証リファレンス」の「Amazon EC2 で定義されるアクション」を参照してください。

のポリシーリソース AWS PrivateLink

ポリシーリソースに対するサポート	はい

管理者は AWS JSON ポリシーを使用して、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どのような条件でアクションを実行できるかということです。

Resource JSON ポリシー要素は、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、リソースレベルの権限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	はい

管理者は AWS JSON ポリシーを使用して、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んなリソースにどんな条件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することで、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 要素を指定するか、1 つの Condition 要素に複数のキーを指定すると、 AWS 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。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、『IAM ユーザーガイド』の「IAM ポリシーの要素: 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:VpceServiceName`
- `ec2:VpceServiceOwner`
- `ec2:VpceServicePrivateDnsName`

どのアクションおよびリソースと条件キーを使用できるかについては、「Amazon EC2 で定義されるアクション」を参照してください。

ACLs AWS PrivateLink

ACL のサポート	No

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための権限を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

での ABAC AWS PrivateLink

ABAC のサポート (ポリシー内のタグ)	はい

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義するアクセス許可戦略です。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、ABAC の最初の手順です。その後、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した場合に操作を許可するように ABAC ポリシーを設計します。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

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はいです。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。

ABAC の詳細については、『IAM ユーザーガイド』の「ABAC とは?」を参照してください。ABAC をセットアップするステップを説明するチュートリアルについては、「IAM ユーザーガイド」の「属性に基づく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。

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	はい

一部の は、一時的な認証情報を使用してサインインすると機能 AWS のサービス しません。一時的な認証情報 AWS のサービス を使用する 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「IAM と連携する 」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、一時的な認証情報を使用します。例えば、会社の Single Sign-On (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。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「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 AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用して . AWS recommends にアクセスできます AWS。この際、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、「IAM の一時的セキュリティ認証情報」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

フォワードアクセスセッション (FAS) をサポート	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際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストリクエストリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の 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受け取っ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	いいえ

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「AWS のサービスにアクセス許可を委任するロールの作成」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	いいえ

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権限を表示できますが、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 AWS API を使用してタスクを実行することはできません。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権限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。

これらサンプルの JSON ポリシードキュメントを使用して、IAM 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「IAM ポリシーの作成」を参照してください。

各リソースタイプの ARN 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、「サービス認証リファレンス」のAmazon EC2 のアクション、リソース、および条件キー」を参照してください。 ARNs

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く 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 名の制御
- VPC エンドポイントサービスに指定できるサービス名の制御

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。次に例を示します。

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

```
            "Effect": "Allow",
            "Action":"ec2:*VpcEndpoint*",
            "Resource":"*"
        }
    ]
}
```

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

サービス所有者に基づく 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 名の制御

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、およびプライベート 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の制御

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"
                    ]
                }
            }
        }
    ]
}
```

エンドポイントポリシーを使用して VPC 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、Amazon S3 に接続するためにインターフェイスエンドポイン

トを使用する場合、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 VPC からのバケットへのアクセスを制御することもできます。

内容

考慮事項

- エンドポイントポリシーは、IAM ポリシー言語を使用する JSON 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場合 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。
- AWS のサービス 以外のエンドポイントサービスの VPC エンドポイントを作成すると、エンドポイントへのフルアクセスが許可されます。

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"
    }
}
```

プリンシパルを次の形式で指定すると、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 のみにアクセス許可が付与されます。

```
"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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (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. [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ポリシーを変更するには

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

AWS PrivateLink の 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、およびエンドポイントサービスのデータポイントを Amazon CloudWatch に発行します。CloudWatch では、それらのデータポイントについての統計を、順序付けられた時系列データのセット (メトリクスと呼ばれる) 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、メトリクスが許容範囲外になる場合、CloudWatch アラームを作成して、指定されたメトリクスを監視し、アクション (E メールアドレスに通知を送信するなど) を開始することができます。

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、AWS PrivateLink はメトリクスを 1 分間隔で CloudWatch に送信し、これに追加料金はかかりません。

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 状態と 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	エンドポイントが受信した 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 で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がエンドポイントに送信した 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。

すべての CloudWatch メトリクスを表示する

これらの CloudWatch メトリクスは、以下のように Amazon VPC コンソール、CloudWatch コンソール、または AWS CLI を使用することによって表示できます。

Amazon VPC コンソールを使用してメトリクスを表示する

1. Amazon VPCコンソール(https://console.aws.amazon.com/vpc/)を開きます。
2. ナビゲーションペインで、[Endpoints] (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. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
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。

AWS CLI を使用してメトリクスを表示する

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 は、どのエンドポイントがサポートされている各メトリクスの最大コントリビューターであるかを把握できるように、エンドポイントサービス用の組み込み Contributor Insights ルールを提供します。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 は、次のルールを提供します。

- `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 パケットの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 の料金」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 CLI のいずれかを使用して AWS PrivateLink 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。

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

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

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

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` オプションには、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。テンプレート名とエンドポイントサービスの 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

AWS PrivateLink の組み込みルールは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。

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

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

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

ルールを無効にするには、disable-insight-rules コマンドを使用します。

Contributor Insights のルールを削除する

AWS Management Console または AWS CLI のいずれかを使用して AWS PrivateLink の組み込みルールを削除するには、次の手順を使用します。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。

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

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
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 CLI を使用して AWS PrivateLink の Contributor Insights ルールを削除するには

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

以下の表は、アカウントに対してリージョン別に適用される AWS PrivateLink リソースのクォータ (以前は制限と呼ばれていたもの) の一覧を示しています。特に明記されていない限り、これらのクォータの引き上げをリクエストできます。詳細については、「Service Quotas ユーザーガイド」の「クォータ引き上げのリクエスト」を参照してください。

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。

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および Gateway Load Balancer エンドポイント	50	はい	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 エンドポイントの数	20	はい	VPC ごとに最大 255 個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	20,480	いいえ	VPC エンドポイントポリシーの最大サイズ (スペースを含む)

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

- 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、最大 100 Gbps まで自動的にスケールアップします。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の VPC エンドポイントの最大帯域幅は、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) とは、VPC エンドポイントを通じて渡すことができる最大許容パケットサイズ (バイト単位) です。MTU が大きいほど、より多くのデータを単一のパケットで渡すことができます。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達したサイズが 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、`Destination Unreachable: Fragmentation needed and Don't Fragment was Set` (タイプ 3、コード 4) などの ICMP メッセージを生成しません。
- VPC エンドポイントは、すべてのパケットに対して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
指定された IP アドレス	VPC エンドポイントを作成または変更するときに、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 サポート	Gateway Load Balancer エンドポイントサービスと Gateway Load Balancer エンドポイントを、IPv4 アドレスと IPv6 アドレスの両方、または 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、の 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 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 IPv4 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することができます。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、サービスコンシューマーはインターフェイスエン	2022 年 5 月 11 日

	ドポイントの IPv6 サポートを有効にして、IPv6 経由でエンドポイントサービスにアクセスできます。	
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	VPC 内に Gateway Load Balancer エンドポイントを作成して、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	AWS のサービスのインターフェイス VPC エンドポイントに IAM ポリシーをアタッチして、その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 エンドポイントおよび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
VPC エンドポイントおよびエンドポイントサービスの作成時にタグを付ける	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、タグを追加することができます。	2020 年 2 月 5 日

プライベート DNS 名	プライベート DNS 名を使用して、VPC 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て、他の AWS アカウント とユーザーがインターフェイス VPC エンドポイント経由で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
DynamoDB の VPC エンドポイント	ゲートウェイ VPC エンドポイントを作成して、インターネットゲートウェイや NAT デバイスを使用せずに、VPC から Amazon DynamoDB にアクセスすることができます。	2017 年 8 月 16 日
Amazon S3 の VPC エンドポイント	ゲートウェイ VPC エンドポイントを作成して、インターネットゲートウェイや NAT デバイスを使用せずに、VPC から Amazon S3 にアクセスすることができます。	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。