Amazon Virtual Private Cloud

AWS PrivateLink

Amazon Virtual Private Cloud: AWS PrivateLink

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

Amazon の商標およびトレードドレスは、Amazon のものではない製品またはサービスと関連付けてはならず、また、お客様に混乱を招くような形や Amazon の信用を傷つけたり失わせたりする形で使用することはできません。Amazon が所有しない商標はすべてそれぞれの所有者に所属します。所有者は必ずしも Amazon と提携していたり、関連しているわけではありません。また、Amazon の後援を受けているとはかぎりません。

Table of Contents

AWS PrivateLink とは 1
- VPC エンドポイントの概念 1
- VPC エンドポイントを使用する 2
- エンドポイント設定の例 2
- エンドポイントの料金 2

VPC エンドポイント 3
- インターフェイスエンドポイント 3
  - インターフェイスエンドポイントのプライベート DNS 5
  - インターフェイスエンドポイントのプロパティと制限 7
  - オンプレミスのデータセンターへの接続 8
  - インターフェイスエンドポイントのライフサイクル 8
  - インターフェイスエンドポイントのアベイラビリティーゾーンに関する考慮事項 8
  - 使用可能な AWS のサービス名を表示する 8
  - インターフェイスエンドポイントの作成 9
  - インターフェイスエンドポイントを表示する 13
  - インターフェイスエンドポイントの通知を作成および管理する 13
  - インターフェイスエンドポイントを介したサービスへアクセスする 14
  - インターフェイスエンドポイントを作成する 15
- Gateway Load Balancer エンドポイント 17
  - Gateway Load Balancer のエンドポイントのプロパティおよび制限 18
  - Gateway Load Balancer エンドポイントのライフサイクル 19
  - Gateway Load Balancer エンドポイントの料金 19
  - Gateway Load Balancer エンドポイントを作成する 19
  - Gateway Load Balancer エンドポイントを表示する 20
  - Gateway Load Balancer エンドポイントのタグを追加または削除する 20
- ゲートウェイエンドポイント 21
  - ゲートウェイエンドポイントの料金 22
  - ゲートウェイエンドポイントのルーティング 22
  - ゲートウェイエンドポイントの制限 24
  - Amazon S3 におけるエンドポイント 25
  - Amazon DynamoDB のエンドポイント 32
  - ゲートウェイエンドポイントを作成する 35
  - セキュリティグループを変更する 37
  - ゲートウェイエンドポイントを変更する 37
  - ゲートウェイエンドポイントタグを追加または削除する 38
- シークレットへのアクセスを制御する 39
  - VPC エンドポイントポリシーを使用する 39
  - セキュリティグループ 40
- VPC エンドポイントを削除する 40

VPC エンドポイントサービス 41
- インターフェイスエンドポイントの VPC エンドポイントサービス 41
  - エンドポイントサービスのアベイラビリティーゾーンに関する考慮事項 43
  - エンドポイントサービスの DNS 名 43
  - オンプレミスのデータセンターへ接続する 8
  - VPC ピア接続を介してサービスへアクセスする 44
  - 接続情報のプロキシプロトコルを使用する 44
  - ルールと制限 44
- Gateway Load Balancer エンドポイントの VPC エンドポイントサービス 45
  - アベイラビリティーゾーンの考慮事項 46
  - ルールと制限 47
- インターフェイスエンドポイントの VPC エンドポイントサービス設定を作成する 47
- Gateway Load Balancer エンドポイントの VPC エンドポイントサービス設定を作成する 48
- エンドポイントサービスのアクセス権限を追加または削除する 49
- エンドポイントサービス設定を変更 51

エンドポイントの接続リクエストを承諾または拒否する 52
エンドポイントサービスの通知を作成および管理する 53
VPC エンドポイントサービスタグを追加または削除する 56
エンドポイントサービス設定を削除する 56
Identity and access management 58
プライベート DNS 名 61
ドメイン名の検証に関する考慮事項 62
VPC エンドポイントサービスのプライベート DNS 名の検証 62
ドメインの DNS サーバーに TXT レコードを追加する 63
既存の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 64
エンドポイントサービスのプライベート DNS 名設定を表示する 64
エンドポイントサービスのプライベート DNS 名ドメインの検証を手動で開始する 65
エンドポイントサービスのプライベート DNS 名を削除する 66
プライベート DNS 名のドメイン検証 TXT レコード 66
ドメインの検証に関する一般的な問題のトラブルシューティング 68
ドメインの検証に関する問題 68
ドメインの検証に関する設定を確認する方法 69
AWS PrivateLink をサポートするサービス 70
使用可能な AWS のサービス名を表示する 74
クォータ 76

AWS PrivateLink および VPC エンドポイント

AWS PrivateLink は、高可用性のスケーラブルなテクノロジーであり、サポートされている AWS のサービス、他の AWS アカウントでホストされているサービス (VPC エンドポイントサービス)、およびサポートされている AWS Marketplace パートナーサービスに VPC をプライベートに接続できます。サービスと通信するのに、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、および AWS Site-to-Site VPN 接続は不要です。したがって、VPC はパブリックインターネットに公開されません。

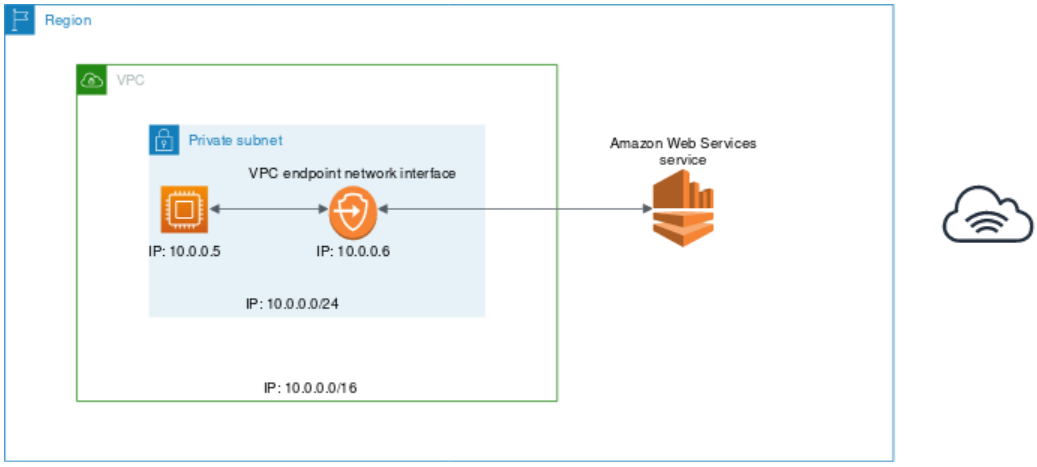
AWS PrivateLink を使用する独自の VPC エンドポイントサービスを作成し、このサービスにアクセスすることを他の AWS のお客様に許可できます。

VPC エンドポイントの概念

VPC エンドポイントの主な概念は次のとおりです。

- VPC エンドポイント — サービスへのプライベート接続を可能にする VPC 内のエントリポイント。VPC エンドポイントのさまざまなタイプを次に示します。サポートされるサービスにより要求される VPC エンドポイントのタイプを作成します。
  - ゲートウェイエンドポイント (p. 21)
  - インターフェイスエンドポイント (p. 3)
  - Gateway Load Balancer エンドポイント (p. 17)
- エンドポイントサービス — VPC 内の独自のアプリケーションまたはサービスです。他の AWS プリンシパルは、その VPC からエンドポイントサービスへのエンドポイントを作成できます。

AWS PrivateLink を使用するには、サービスの VPC エンドポイントを VPC 内に作成します。サポートされるサービスにより要求される VPC エンドポイントのタイプを作成します。これによって Elastic Network Interface がサブネットに作成され、そのプライベート IP アドレスがサービスへのトラフィックのエントリポイントとなります。以下の図表は、 AWS PrivateLink をサポートする AWS サービスに VPC を安全に接続するための基本的なアーキテクチャです。



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 — VPC エンドポイントへのアクセスに使用するウェブインターフェイスを提供します。
- AWS Command Line Interface (AWS CLI) — Amazon VPC を含む一連のさまざまな AWS のサービス用のコマンドを提供します。AWS CLI は、Windows、macOS、Linux でサポートされています。AWS Command Line Interface: 詳細については、「」を参照してください。
- AWS SDK — 言語固有の API を提供します。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、AWS SDK をご参照ください。
- 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 リファレンスを参照してください。

エンドポイント設定の例

AWS PrivateLink および VPC ピアリングの例については、Amazon VPC ユーザーガイドの例: AWS PrivateLink と VPC ピアリングを使用するサービスを参照してください。

エンドポイントの料金

エンドポイントの料金の詳細については、 AWS PrivateLink の料金を参照してください。

VPC エンドポイント

VPC エンドポイントを使用すると、Virtual Private Cloud (VPC) とサポートされているサービスの間の接続が有効になります。インターネットゲートウェイ、NAT デバイス、VPN 接続、および AWS Direct Connect 接続は必要ありません。したがって、VPC はパブリックインターネットに公開されません。

VPC エンドポイントは仮想デバイスです。これらは水平にスケールされ、冗長で、可用性の高い VPC コンポーネントです。VPC エンドポイントのさまざまなタイプを次に示します。サポートされるサービスにより要求される 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

インターフェイスエンドポイント (p. 3)は、サブネットの IP アドレス範囲のプライベート IP アドレスを持つ Elastic Network Interface です。これは、AWS 所有、または AWS 顧客またはパートナーが所有する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します。 AWS PrivateLink と統合される AWS サービスのリストについては、 AWS PrivateLink をサポートするサービス (p. 70) を参照してください。

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。

Gateway Load Balancer エンドポイント

Gateway Load Balancer エンドポイント (p. 17)は、サブネットの IP アドレス範囲のプライベート IP アドレスを持つ Elastic Network Interface です。トラフィックをインターセプトし、Gateway Load Balancer を使用して設定したネットワークまたはセキュリティサービスにルーティングするエントリポイントとして機能します。Gateway Load Balancer エンドポイントは、ルートテーブル内のルートのターゲットとして指定します。Gateway Load Balancer のエンドポイントは、Gateway Load Balancer を使用して設定されているエンドポイントサービスについてのみサポートされています。

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。

ゲートウェイエンドポイント

ゲートウェイエンドポイント (p. 21)は、AmazonS3 または DynamoDB のいずれかに向かうトラフィックに使用されるルートテーブル内のルートのターゲットであるゲートウェイです。

ゲートウェイエンドポイントは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。2 つのオプションの比較については、Amazon S3 ユーザーガイドの「Amazon S3 の VPC エンドポイントのタイプ」を参照してください。

インターフェイス VPC エンドポイント (AWS PrivateLink)

インターフェイス VPC エンドポイント (インターフェイスエンドポイント) では、 AWS PrivateLink を使用するサービスに接続できます。これらのサービスには、AWS の一部のサービス、他の AWS のお客様およびパートナーによって各自の VPC でホストされるサービス (エンドポイントサービスと呼ばれます)、およびサポートされている AWS Marketplace パートナーサービスが含まれます。サービスの所有者はサービスプロバイダです。インターフェイスエンドポイントを作成するプリンシパルとしてのユーザーは、サービスコンシューマーです。

以下は、インターフェイスエンドポイントの一般的な設定手順です。

1. インターフェイスエンドポイントを作成する先の VPC を選択し、接続先の AWS のサービス、エンドポイントサービス、または AWS Marketplace サービスの名前を指定します。
2. インターフェイスエンドポイントを使用する VPC 内のサブネットを選択します。この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。エンドポイントネットワークインターフェイスには、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。この IP アドレスは、インターフェイスエンドポイントが削除されるまで保持されます。サービスでサポートされている複数のアベイラビリティーゾーンに複数のサブネットを指定すると、アベイラビリティーゾーンの障害からインターフェイスエンドポイントをより確実に回復できます。この場合は、指定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。

   Note

   エンドポイントネットワークインターフェイスは、リクエスタによって管理されるネットワークインターフェイスです。このインターフェイスはアカウントで表示できますが、お客様自身で管理することはできません。詳細については、「リクエスタマネージド型のネットワークインターフェイス」を参照してください。
3. 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指定します。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ネットワークインターフェイスへのトラフィックを制御します。セキュリティグループを指定しないと、VPC のデフォルトのセキュリティグループが関連付けられます。
4. (オプションの AWS のサービスと AWS Marketplace パートナーサービスのみ) デフォルトの DNS ホスト名を使用してサービスにリクエストを行うには、エンドポイントのプライベート DNS (p. 5) を有効にします。

   Important

   AWS のサービスおよび AWS Marketplace パートナーサービス用に作成されたエンドポイントに対しては、プライベート DNS がデフォルトで有効になります。
   プライベート DNS は、同じ VPC とアベイラビリティーゾーンまたはローカルゾーンにある他のサブネットで有効になっています。
5. サービスプロバイダーとコンシューマーが別のアカウントにある場合、アベイラビリティーゾーン ID を使用してインターフェイスエンドポイントのアベイラビリティーゾーンを識別する方法の詳細については、「the section called “インターフェイスエンドポイントのアベイラビリティーゾーンに関する考慮事項” (p. 8)」を参照してください。
6. インターフェイスエンドポイントの作成後、サービスプロバイダーによって承諾されると、そのインターフェイスエンドポイントが使用可能になります。サービスプロバイダは、リクエストを自動または手動で承諾するようにサービスを設定する必要があります。通常、AWS のサービスおよび AWS Marketplace のサービスは、エンドポイントのすべてのリクエストを自動的に承諾します。エンドポイントのライフサイクルの詳細については、「インターフェイスエンドポイントのライフサイクル (p. 8)」を参照してください。

エンドポイントでは、VPC 内のリソースに対するリクエストをサービスからは開始できません。エンドポイントは、VPC 内のリソースから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。サービスとエンドポイントを統合する前に、サービス固有の設定や制限について、サービス固有の VPC エンドポイントのドキュメントをご確認ください。

目次

- インターフェイスエンドポイントのプライベート DNS (p. 5)
- インターフェイスエンドポイントのプロパティと制限 (p. 7)
- オンプレミスのデータセンターへの接続 (p. 8)
- インターフェイスエンドポイントのライフサイクル (p. 8)
- インターフェイスエンドポイントのアベイラビリティーゾーンに関する考慮事項 (p. 8)
- 使用可能な AWS のサービス名を表示する (p. 8)
- インターフェイスエンドポイントの作成 (p. 9)

- インターフェイスエンドポイントを表示する (p. 13)
- インターフェイスエンドポイントの通知を作成および管理する (p. 13)
- インターフェイスエンドポイントを介したサービスへアクセスする (p. 14)
- インターフェイスエンドポイントを作成する (p. 15)

インターフェイスエンドポイントのプライベート DNS

Important

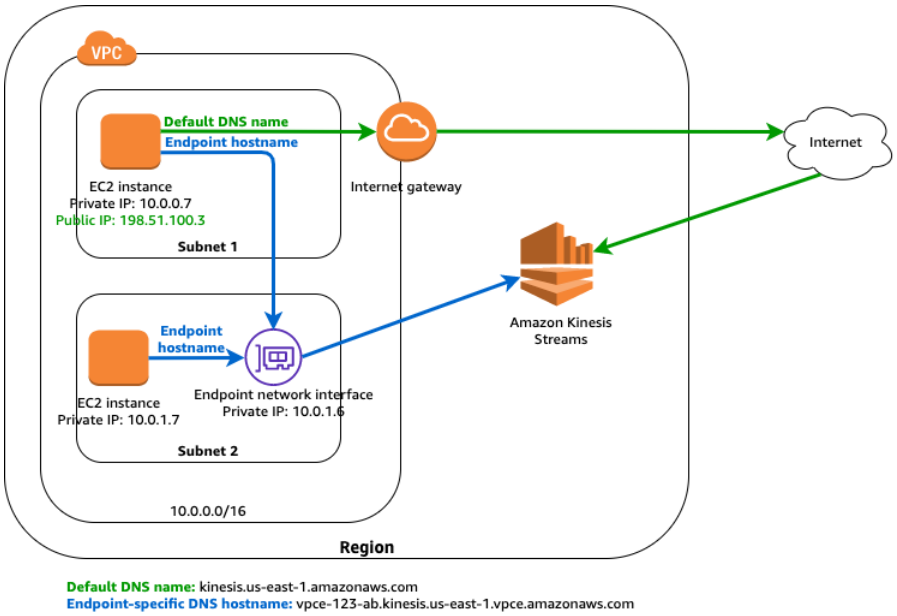
プライベート DNS は、Amazon S3 インターフェイスエンドポイントについてはサポートされていません。

インターフェイスエンドポイントを作成すると、サービスとの通信に使用できるエンドポイント固有の DNS ホスト名が生成されます。AWS のサービスおよび AWS Marketplace パートナーサービスの場合、プライベート DNS オプション (デフォルトで有効) は、プライベートホストゾーンを VPC と関連付けます。ホストゾーンにはサービスのデフォルトの DNS 名 (`ec2.us-east-1.amazonaws.com` など) のレコードセットが含まれており、VPC のエンドポイントネットワークインターフェイスのプライベート IP アドレスに解決されます。これにより、エンドポイント固有の DNS ホスト名ではなく、デフォルトの DNS 名を使用してサービスにリクエストを行うことができます。たとえば、既存のアプリケーションから AWS のサービスにリクエストを行う場合、インターフェイスエンドポイントを介して引き続きリクエストを行うことができます。設定の変更は必要ありません。

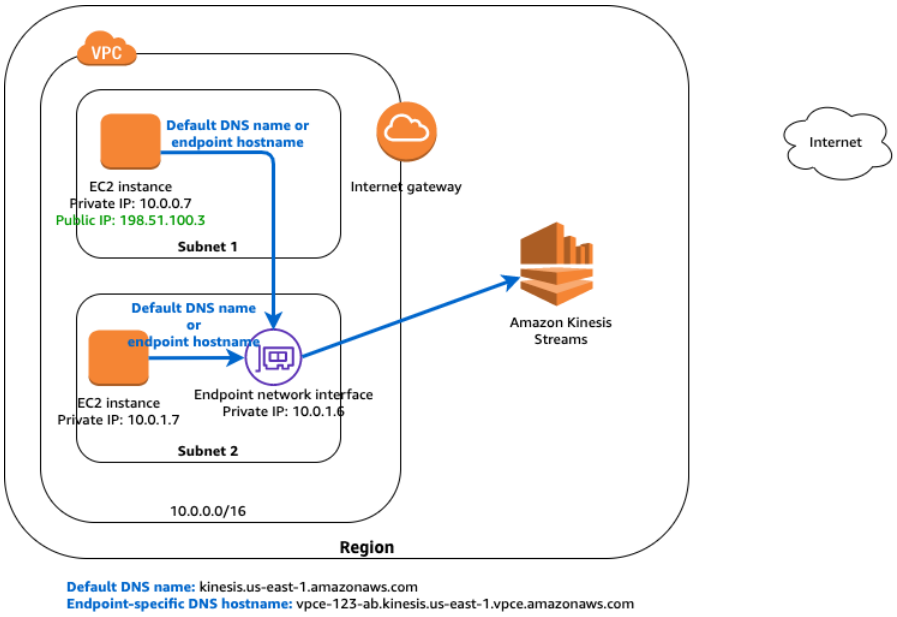
次の図に示す例では、サブネット 2 に Amazon Kinesis Data Streams のインターフェイスエンドポイントとエンドポイントネットワークインターフェイスがあります。インターフェイスエンドポイントのプライベート DNS は無効になっています。サブネットのルートテーブルには、次のルートがあります。

サブネット 1	
送信先	ターゲット
10.0.0.0/16	ローカル
0.0.0.0/0	internet-gateway-id
サブネット 2	
送信先	ターゲット
10.0.0.0/16	ローカル

いずれかのサブネットのインスタンスは、エンドポイント固有の DNS ホスト名を使用して、インターフェイスエンドポイントを介して Amazon Kinesis Data Streams にリクエストを送信できます。サブネット 1 のインスタンスは、そのデフォルトの DNS 名を使用して AWS リージョンのパブリック IP アドレス空間経由で Amazon Kinesis Data Streams と通信できます。



次の図では、エンドポイントのプライベート DNS が有効になっています。いずれかのサブネットのインスタンスは、デフォルトの DNS ホスト名またはエンドポイント固有の DNS ホスト名を使用して、インターフェイスエンドポイントを介して Amazon Kinesis Data Streams にリクエストを送信できます。



Important

プライベート DNS を使用するには、VPC 属性の`true` および `enableDnsHostnames` を `enableDnsSupport` に設定する必要があります。詳細については、「VPC の DNS サポートを更新する」を参照してください。IAM ユーザーは、ホストゾーンを操作するアクセス許可が必要です。詳細については、Route 53 に対する認証とアクセスコントロールに関する記事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プロパティと制限

インターフェイスエンドポイントを使用するには、そのプロパティと現在の制限に注意する必要があります。

- 各インターフェイスエンドポイントで選択できるサブネットは、アベイラビリティーゾーンあたり 1 つのみです。
- インターフェイスエンドポイントを介したサービスへのアクセスは、一部のアベイラビリティーゾーンでサポートされない場合があります。サポートされるアベイラビリティーゾーンを確認するには、describe-vpc-endpoint-services コマンドまたは Amazon VPC コンソールを使用してください。詳細については、「」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作成 (p. 9)
- インターフェイスエンドポイントを作成する場合、エンドポイントはアカウントにマッピングされているアベイラビリティーゾーンに作成され、他のアカウントからは独立したものになります。サービスプロバイダーとコンシューマーが別のアカウントにある場合、アベイラビリティーゾーン ID を使用してインターフェイスエンドポイントのアベイラビリティーゾーンを識別する方法の詳細については、「the section called “インターフェイスエンドポイントのアベイラビリティーゾーンに関する考慮事項” (p. 8)」を参照してください。
- サービスプロバイダーとコンシューマーが異なるアカウントを持ち、複数のアベイラビリティーゾーンを使用する場合に、コンシューマーが VPC エンドポイントサービス情報を表示すると、レスポンスには共通のアベイラビリティーゾーンのみが含まれます。たとえば、サービスプロバイダーアカウントが `us-east-1a` と `us-east-1c` を使用し、コンシューマーが `us-east-1a` と `us-east-1b` を使用する場合、レスポンスには共通のアベイラビリティーゾーン `us-east-1a` にある VPC エンドポイントサービスが含まれます。
- デフォルトでは、各インターフェイスエンドポイントは、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でき、最大 40 Gbps までバーストできます。アプリケーションでより高いバーストや持続的な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。
- サブネットのネットワーク ACL でトラフィックが制限される場合、エンドポイントネットワークインターフェイスを通じてトラフィックを送信できないことがあります。サブネットの CIDR ブロックに出入りするトラフィックを許可する適切なルールを追加してください。
- エンドポイントネットワークインターフェイスに関連付けられている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と、サービスと通信する VPC 内のリソース間の通信が許可されていることを確認します。AWS CLI などのコマンドラインツールが VPC 内のリソースから AWS のサービスに HTTPS 経由でリクエストを実行できるようにするには、セキュリティグループがインバウンド HTTPS (ポート 443) トラフィックを許可する必要があります。
- インターフェイスエンドポイントは TCP トラフィックのみをサポートします。
- エンドポイントを作成するときは、接続先のサービスへのアクセスを制御するエンドポイントポリシーを、エンドポイントにアタッチできます。詳細については、「ポリシーのベストプラクティス」および「the section called “シークレットへのアクセスを制御する” (p. 39)」を参照してください。
- エンドポイントサービスのサービス固有の制限を確認します。
- 参加者は、所有していない VPC に Amazon Route53 Resolver エンドポイントを作成することはできません。VPC 所有者だけが、インバウンドエンドポイントなどの VPC レベルのリソースを作成できます。
- 同じリージョン内のエンドポイントのみがサポートされています。別のリージョンで、VPC とサービス間のエンドポイントを作成することはできません。
- 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。
- 1 つの VPC から別の VPC にエンドポイントを転送したり、1 つのサービスから別のサービスにエンドポイントを転送することはできません。
- VPC あたりに作成できるエンドポイントの数にはクォータがあります。詳細については、「」を参照してください AWS PrivateLink のクォータ (p. 76)

オンプレミスのデータセンターへの接続

インターフェイスエンドポイントとオンプレミスのデータセンター間の接続には、次のタイプの接続を使用できます。

- AWS Direct Connect
- AWS Site-to-Site VPN

インターフェイスエンドポイントのライフサイクル

インターフェイスエンドポイントは、その作成時 (エンドポイントの接続リクエスト) を始まりとして、様々な段階を経過します。段階ごとに、サービスコンシューマーとサービスプロバイダが実行できるアクションを伴う場合があります。

以下のルールが適用されます。

- サービスプロバイダは、インターフェイスエンドポイントのリクエストを自動または手動で承諾するようにサービスを設定できます。通常、AWS のサービスおよび AWS Marketplace のサービスは、エンドポイントのすべてのリクエストを自動的に承諾します。
- サービスプロバイダは、サービスへのインターフェイスエンドポイントを削除できません。インターフェイスエンドポイントを削除できるのは、インターフェイスエンドポイント接続をリクエストしたサービスコンシューマーのみです。
- サービスプロバイダーは、承諾後の `available` 状態になっているインターフェイスエンドポイントを (手動または自動で) 拒否できます。

インターフェイスエンドポイントのアベイラビリティーゾーンに関する考慮事項

インターフェイスエンドポイントを作成する場合、エンドポイントはアカウントにマッピングされているアベイラビリティーゾーンに作成され、他のアカウントからは独立したものになります。サービスプロバイダーとコンシューマーが別のアカウントにある場合、アベイラビリティーゾーン ID を使用してインターフェイスエンドポイントのアベイラビリティーゾーンを一意に一貫して識別します。例えば、`use1-az1` は `us-east-1` リージョンのアベイラビリティーゾーン ID であり、すべての AWS アカウントで同じ場所にマッピングされます。アベイラビリティーゾーン ID の詳細については、AWS RAM ユーザーガイドのリソースの AZ ID を参照するか、describe-availability-zones を使用してください。

インターフェイスエンドポイントを介したサービスへのアクセスは、一部のアベイラビリティーゾーンでサポートされない場合があります。次のいずれかのオペレーションを使用して、サービスに対してサポートされているアベイラビリティーゾーンを確認できます。

- describe-vpc-endpoint-services (AWS CLI)
- DescribeVpcEndpointServices (API)
- インターフェイスエンドポイントを作成するときの Amazon VPC コンソール。詳細については、「」を参照してくださいthe section called “インターフェイスエンドポイントの作成” (p. 9)

使用可能な AWS のサービス名を表示する

Amazon VPC コンソールを使用してエンドポイントを作成すると、使用可能な AWS のサービス名のリストを取得できます。

AWS CLI を使用してエンドポイントを作成する場合、describe-vpc-endpoint-services コマンドを使用してサービス名を表示し、create-vpc-endpoint コマンドを使用してエンドポイントを作成できます。

Console

コンソールを使用して利用可能な AWS のサービスを表示するには

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]、[Create Endpoint] の順に選択します。
3. [Service Name (サービス名)] セクションに、使用可能なサービスが表示されます。

Command line

AWS CLI を使用して利用可能な AWS のサービスを表示するには

- describe-vpc-endpoint-services コマンドを使用して、接続可能なサービスのリストを取得します。`ServiceType` フィールドは、インターフェイ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介してサービスに接続するかどうかを示します。`ServiceName` フィールドはサービス名を示します。次の例では、すべてのインターフェイスエンドポイントの名前と所有者を一覧表示します。

```
aws ec2 describe-vpc-endpoint-services --filter "Name=service-
type,Values=Interface" --query "ServiceDetails[*].[ServiceName, Owner]" --output
 table
```

```
-------------------------------------------------------------------
|                   DescribeVpcEndpointServices                   |
+-----------------------------------------------------+-----------+
|  aws.sagemaker.us-west-2.notebook                   |  amazon   |
|  aws.sagemaker.us-west-2.studio                     |  amazon   |
|  com.amazonaws.us-west-2.access-analyzer            |  amazon   |
|  com.amazonaws.us-west-2.acm-pca                    |  amazon   |
...
```

AWS Tools for Windows PowerShell を使用して利用可能な AWS のサービスを表示するには

- Get-EC2VpcEndpointService

API を使用して利用可能な AWS のサービスを表示するには

- DescribeVpcEndpointServices

インターフェイスエンドポイントの作成

インターフェイスエンドポイントを作成するには、インターフェイスエンドポイントを作成する先の VPC と、接続を確立する先のサービスを指定する必要があります。

AWS のサービスまたは AWS Marketplace パートナーサービスの場合、デフォルトの DNS ホスト名を使用してサービスにリクエストできるように、エンドポイントのプライベート DNS (p. 5)をオプションで有効にすることができます。

Important

AWS のサービスおよび AWS Marketplace パートナーサービス用に作成されたエンドポイントに対しては、プライベート DNS がデフォルトで有効になります。

Console

AWS のサービスへのインターフェイスエンドポイントをコンソールで作成するには

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]、[Create Endpoint] の順に選択します。
3. [Service category] (サービスカテゴリ) で、[AWS services] (AWS のサービス) が選択されていることを確認します。
4. [Service Name] で、接続先のサービスを選択します。[タイプ] で、タイプが [インターフェイス] になっていることを確認します。
5. 次の情報を入力し、[Create endpoint] を選択します。

   - [VPC] で、エンドポイントを作成する先の VPC を選択します。
   - [Subnets] で、エンドポイントネットワークインターフェイスを作成する先のサブネット (アベイラビリティーゾーン) を選択します。

     AWS の一部のサービスは、一部のアベイラビリティーゾーンでサポートされていない場合があります。
   - インターフェイスエンドポイントのプライベート DNS を有効にするには、[Enable DNS Name] (DNS 名を有効にする) でチェックボックスを選択します。

     > **Important**
     >
     > プライベート DNS は、Amazon S3 インターフェイスエンドポイントについてはサポートされていません。

     このオプションは、デフォルトで有効になっています。オプションとしてプライベート DNS を使用するには、VPC 属性の`true` および `enableDnsHostnames` を `enableDnsSupport` に設定する必要があります。詳細については、「VPC の DNS サポートを更新する」を参照してください。
   - [Security group] 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。
   - (オプション) タグを追加または削除します。

     [タグの追加] [タグの追加] を選択して、以下を実行します。
     - [キー] にはキー名を入力します。
     - [値] にキー値を入力します。

     [タグの削除] タグのキーと値の右側にある削除ボタン ("x") を選択します。

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には、接続先のサービスの名前を指定する必要があります。この名前は、サービスプロバイダから取得できます。

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]、[Create Endpoint] の順に選択します。
3. [Service category] で、[Find service by name] を選択します。
4. [Service Name] にサービスの名前 (`com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc` など) を入力し、[Verify] を選択します。
5. 次の情報を入力し、[Create endpoint] を選択します。

   - [VPC] で、エンドポイントを作成する先の VPC を選択します。
   - [Subnets] で、エンドポイントネットワークインターフェイスを作成する先のサブネット (アベイラビリティーゾーン) を選択します。

当該サービスは一部のアベイラビリティーゾーンでサポートされない場合があります。

- [Security group] 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。
- (オプション) タグを追加または削除します。

  [タグの追加] [タグの追加] を選択して、以下を実行します。
  - [キー] にはキー名を入力します。
  - [値] にキー値を入力します。

  [タグの削除] タグのキーと値の右側にある削除ボタン ("x") を選択します。

AWS Marketplace 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. AWS Marketplace の PrivateLink ページにアクセスし、SaaS (Software-as-a-Service) プロバイダーのサービスをサブスクライブします。インターフェイスエンドポイントをサポートするサービスには、エンドポイントを介して接続するオプションが含まれています。
2. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
3. ナビゲーションペインで、[Endpoints]、[Create Endpoint] の順に選択します。
4. [Service category] (サービスカテゴリ) で、[Your AWS Marketplace services] (AWS Marketplace のサービス) を選択します。
5. サブスクライブした AWS Marketplace サービスを選択します。
6. 次の情報を入力し、[Create endpoint] を選択します。

   - [VPC] で、エンドポイントを作成する先の VPC を選択します。
   - [Subnets] で、エンドポイントネットワークインターフェイスを作成する先のサブネット (アベイラビリティーゾーン) を選択します。

     当該サービスは一部のアベイラビリティーゾーンでサポートされない場合があります。
   - [Security group] 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。
   - (オプション) タグを追加または削除します。

     [タグの追加] [タグの追加] を選択して、以下を実行します。
     - [キー] にはキー名を入力します。
     - [値] にキー値を入力します。

     [タグの削除] タグのキーと値の右側にある削除ボタン ("x") を選択します。

Command line

AWS CLI 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. describe-vpc-endpoint-services コマンドを使用して使用可能なサービスのリストを取得します。返された出力で、接続先のサービスの名前をメモします。`ServiceType` フィールドは、インターフェイ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介してサービスに接続するかどうかを示します。`ServiceName` フィールドはサービス名を示します。
2. 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 コマンドを使用し、VPC ID、VPC エンドポイント (インターフェイス) のタイプ、サービス名、エンドポイントを使用するサブネット、および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指定します。

   次の例では、Elastic Load Balancing サービスへのインターフェイスエンドポイントを作成します。

```
aws ec2 create-vpc-endpoint --vpc-id vpc-ec43eb89 --vpc-endpoint-type Interface
 --service-name com.amazonaws.us-east-1.elasticloadbalancing --subnet-id subnet-
abababab --security-group-id sg-1a2b3c4d
```

```
{
    "VpcEndpoint": {
        "PolicyDocument": "{\n  \"Statement\": [\n    {\n      \"Action\": \"*\",
 \n      \"Effect\": \"Allow\", \n      \"Principal\": \"*\", \n      \"Resource\":
 \"*\"\n    }\n  ]\n}",
        "VpcId": "vpc-ec43eb89",
        "NetworkInterfaceIds": [
            "eni-bf8aa46b"
        ],
        "SubnetIds": [
            "subnet-abababab"
        ],
        "PrivateDnsEnabled": true,
        "State": "pending",
        "ServiceName": "com.amazonaws.us-east-1.elasticloadbalancing",
        "RouteTableIds": [],
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-1a2b3c4d"
            }
        ],
        "VpcEndpointId": "vpce-088d25a4bbf4a7abc",
        "VpcEndpointType": "Interface",
        "CreationTimestamp": "2017-09-05T20:14:41.240Z",
        "DnsEntries": [
            {
                "HostedZoneId": "Z7HUB22UULQXV",
                "DnsName": "vpce-088d25a4bbf4a7abc-
ks83awe7.elasticloadbalancing.us-east-1.vpce.amazonaws.com"
            },
            {
                "HostedZoneId": "Z7HUB22UULQXV",
                "DnsName": "vpce-088d25a4bbf4a7abc-ks83awe7-us-
east-1a.elasticloadbalancing.us-east-1.vpce.amazonaws.com"
            },
            {
                "HostedZoneId": "Z1K56Z6FNPJRR",
                "DnsName": "elasticloadbalancing.us-east-1.amazonaws.com"
            }
        ]
    }
}
```

また、次の例では、別のアカウントの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します (エンドポイントサービス名はサービスプロバイダから提供します)。

```
aws ec2 create-vpc-endpoint --vpc-id vpc-ec43eb89 --vpc-endpoint-type Interface
 --service-name com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc --subnet-
id subnet-abababab --security-group-id sg-1a2b3c4d
```

返された出力で、privateDnsNames フィールドの値をメモします。これらの DNS 名を使用して AWS のサービスにアクセスできます。

AWS Tools for Windows PowerShell を使用して、利用可能なサービスを記述し、VPC エンドポイントを作成するには

- Get-EC2VpcEndpointService
- New-EC2VpcEndpoint

API を使用して、利用可能なサービスを記述し、VPC エンドポイントを作成するには

- DescribeVpcEndpointServices
- CreateVpcEndpoint

インターフェイスエンドポイントを表示する

インターフェイスエンドポイントの作成後に、その関連情報を表示できます。

Console

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に関する情報を表示するには

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、インターフェイス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に関する情報を表示するには、[Details] を選択します。[DNS Names] に、サービスへのアクセスに使用する DNS 名サービスが表示されます。
4. インターフェイスエンドポイントの作成先のサブネットと、各サブネットのエンドポイントネットワークインターフェイスの ID を表示するには、[Subnets] を選択します。
5. 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たセキュリティグループを表示するには、[Security Groups] を選択します。

Command line

AWS CLI を使用してインターフェイスエンドポイントを記述するには

- エンドポイントは、describe-vpc-endpoints コマンドを使用して記述できます。

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-088d25a4bbf4a7abc
```

AWS Tools for PowerShell または API を使用して VPC エンドポイントを記述するには

- Get-EC2VpcEndpoint (Tools for Windows PowerShell)
- DescribeVpcEndpoints (Amazon EC2 クエリ API)

インターフェイスエンドポイントの通知を作成および管理する

通知を作成して、インターフェイスエンドポイントで発生する特定のイベントに関するアラートを受信できます。たとえば、サービスプロバイダがインターフェイスエンドポイントを承諾したときに E メールを受信できます。通知を作成するには、Amazon SNS トピックを通知に関連付ける必要があります。この SNS トピックへの受信登録を行い、エンドポイントイベントの発生時に E メール通知を受信できます。

通知に使用する Amazon SNS トピックには、ユーザーに代わって通知を発行することを Amazon の VPC エンドポイントサービスに許可するトピックポリシーが必要です。トピックポリシーには、次のステートメントを必ず含めます。詳細については、Amazon Simple Notification Service デベロッパーガイドの「Amazon SNS での Identity and Access Management」を参照してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account:topic-name"
    }
  ]
}
```

Command line

AWS CLI を使用して通知を作成または管理するには

1. 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 コマンドを使用します。次の例に示すように、SNS トピックの ARN、通知されるイベント、エンドポイントの ID を指定します。

```
aws ec2 create-vpc-endpoint-connection-notification --connection-notification-
arn arn:aws:sns:us-east-2:123456789012:EndpointNotification --connection-events
 Accept Reject --vpc-endpoint-id vpce-123abc3420c1931d7
```

2. 通知を表示するには、describe-vpc-endpoint-connection-notifications コマンドを使用します。

```
aws ec2 describe-vpc-endpoint-connection-notifications
```

3. 通知の SNS トピックまたはエンドポイントイベントを変更するには、modify-vpc-endpoint-connection-notification コマンドを使用します。

```
aws ec2 modify-vpc-endpoint-connection-notification --connection-notification-
id vpce-nfn-008776de7e03f5abc --connection-events Accept --connection-notification-
arn arn:aws:sns:us-east-2:123456789012:mytopic
```

4. 通知を削除するには、delete-vpc-endpoint-connection-notifications コマンドを使用します。

```
aws ec2 delete-vpc-endpoint-connection-notifications --connection-notification-
ids vpce-nfn-008776de7e03f5abc
```

インターフェイスエンドポイントを介したサービスへアクセスする

インターフェイスエンドポイントの作成後に、エンドポイント URL を介して、サポートされているサービスにリクエストを送信できます。以下を使用できます。

- エンドポイントのプライベート DNS (プライベートホストゾーン。AWS のサービスおよび AWS Marketplace パートナーサービスにのみ適用可能) を有効にした場合は、リージョンにおける AWS のサービスのデフォルト DNS ホスト名。例えば、 。`ec2.us-east-1.amazonaws.com`

Important

プライベート DNS は、Amazon S3 インターフェイスエンドポイントについてはサポートされていません。

- インターフェイスエンドポイント用に生成したエンドポイント固有のリージョン DNS ホスト名。このホスト名には、一意のエンドポイント識別子、サービス識別子、リージョン、および vpce.amazonaws.com が含まれます。例えば、 。vpce-0fe5b17a0707d6abc-29p5708s.ec2.us-east-1.vpce.amazonaws.com
- エンドポイントが使用できるアベイラビリティーゾーンごとに生成したエンドポイント固有のゾーン DNS ホスト名。このホスト名には、アベイラビリティーゾーンが含まれます。例えば、 。vpce-0fe5b17a0707d6abc-29p5708s-us-east-1a.ec2.us-east-1.vpce.amazonaws.comアーキテクチャでアベイラビリティーゾーンが分離されている場合 (たとえば障害抑制のためや、リージョン内データ転送コスト削減のため)、このオプションを使用できます。

  ゾーン DNS ホスト名に対するリクエストは、サービスプロバイダアカウントの対応するアベイラビリティーゾーンの口ケーションに送信されますが、ご使用のアカウントと同じアベイラビリティーゾーン名ではない場合があります。詳細については、「リージョンとアベイラビリティーゾーンの概念」を参照してください。
- VPC のエンドポイントネットワークインターフェイスのプライベート IP アドレス。

リージョン別およびゾーン別 DNS 名を取得するには、「インターフェイスエンドポイントを表示する (p. 13)」を参照してください。

例えば、Elastic Load Balancing へのインターフェイスエンドポイントがあるサブネットで、プライベート DNS オプションを有効にしていない場合は、インスタンスの次の AWS CLI コマンドを使用してロードバランサーを記述します。このコマンドでは、エンドポイント固有のリージョン DNS ホスト名を使用して、インターフェイスエンドポイントによりリクエストを行います。

```
aws elbv2 describe-load-balancers --endpoint-url https://vpce-0f89a33420c193abc-bluzidnv.elasticloadbalancing.us-east-1.vpce.amazonaws.com/
```

プライベート DNS オプションを有効にした場合、エンドポイント URL をリクエストに指定する必要はありません。AWS CLI では、リージョンの AWS サービスのデフォルトエンドポイント (elasticloadbalancing.us-east-1.amazonaws.com) を使用します。

インターフェイスエンドポイントを作成する

インターフェイスエンドポイントの次の属性を変更できます。

- インターフェイスエンドポイントが配置されているサブネット
- 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られているセキュリティグループ
- タグ
- プライベート DNS オプション

  Note

  プライベート DNS を有効にすると、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。
- エンドポイントポリシー (サービスでサポートされている場合)

インターフェイスエンドポイントのサブネットを削除すると、サブネットの対応するエンドポイントネットワークインターフェイスが削除されます。

Console

インターフェイスエンドポイントの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] を選択し、インターフェイスエンドポイントを選択します。
3. [Actions]、[Manage Subnets] の順に選択します。
4. 必要に応じてサブネットを選択または選択解除し、[Modify Subnets] を選択します。

インターフェイスエンドポイントに関連付けられているセキュリティグループを追加または削除するには

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、インターフェイスエンドポイントを選択します。
3. [Actions]、[Manage security groups] の順に選択します。
4. 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、[保存] を選択します。

インターフェイスエンドポイントタグを追加または削除するには

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、[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、[アクション]、[タグの追加/編集] の順に選択します。
4. タグを追加または削除します。

   [タグの追加] [タグの作成] を選択して、以下を実行します。

   - [キー] にはキー名を入力します。
   - [値] にキー値を入力します。

   [タグの削除] タグのキーと値の右側にある削除ボタン ("x") を選択します。

プライベート DNS 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] を選択し、インターフェイスエンドポイントを選択します。
3. [Actions (アクション)]、[Modify Private DNS names (プライベート DNS 名の変更)] の順に選択します。
4. 必要に応じてオプションを設定し、[Modify Private DNS names] (プライベート DNS 名の変更) を選択します。

エンドポイントポリシーを更新するには

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、インターフェイスエンドポイントを選択します。
3. [Actions]、[Edit policy] の順に選択します。

4. [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指定します。[Save] を選択します。

Command line

AWS CLI を使用して VPC エンドポイントを変更するには

1. describe-vpc-endpoints コマンドを使用してインターフェイスエンドポイントの ID を取得します。

```
aws ec2 describe-vpc-endpoints
```

2. 次の例では、modify-vpc-endpoint コマンドを使用してサブネット `subnet-aabb1122` をインターフェイスエンドポイントに追加します。

```
aws ec2 modify-vpc-endpoint --vpc-endpoint-id vpce-0fe5b17a0707d6abc --add-subnet-
id subnet-aabb1122
```

AWS Tools for Windows PowerShell または API を使用して VPC エンドポイントを変更するには

- Edit-EC2VpcEndpoint (AWS Tools for Windows PowerShell)
- ModifyVpcEndpoint (Amazon EC2 クエリ API)

AWS Tools for Windows PowerShell または API を使用して VPC エンドポイントタグを追加または削除するには

- tag-resource (AWS CLI)
- TagResource (AWS Tools for Windows PowerShell)
- untag-resource (AWS CLI)
- TagResource (AWS Tools for Windows PowerShell)

Gateway Load Balancer エンドポイント (AWS PrivateLink)

Gateway Load Balancer エンドポイントは、トラフィックをインターセプトし、セキュリティ検査などのために Gateway Load Balancer を使用して設定したサービスにルーティングすることを可能にします。サービスの所有者はサービスプロバイダーです。Gateway Load Balancer エンドポイントを作成するプリンシパルとしてのユーザーは、サービスコンシューマーです。

Gateway Load Balancer エンドポイントを設定するための一般的な手順は次のとおりです。

1. Gateway Load Balancer エンドポイントサービスが設定されていることを確認します。詳細については、「」を参照してくださいGateway Load Balancer エンドポイントの VPC エンドポイントサービス (p. 45)
2. Gateway Load Balancer エンドポイントを作成する VPC を選択し、サービスの名前を指定します。
3. Gateway Load Balancer エンドポイントを使用する VPC 内のサブネットを選択します。この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。エンドポイントネットワークインターフェイスには、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。この IP アドレスは、Gateway Load Balancer エンドポイントが削除されるまで保持されます。

Note

エンドポイントネットワークインターフェイスは、リクエスタによって管理されるネットワークインターフェイスです。このインターフェイスはアカウントで表示できますが、お客様自身で管理することはできません。詳細については、「リクエスタマネージド型のネットワークインターフェイス」を参照してください。

4. Gateway Load Balancer エンドポイントの作成後、サービスプロバイダーによって承諾されると、その Gateway Load Balancer エンドポイントが使用可能になります。サービスプロバイダーは、リクエストを自動または手動で承諾するようにサービスを設定できます。
5. トラフィックが Gateway Load Balancer エンドポイントをポイントするように、サブネットルートテーブルとゲートウェイルートテーブルを設定します。詳細については、Amazon VPC ユーザーガイドの「Gateway Load Balancer エンドポイントへのルーティング」を参照してください。

目次

- Gateway Load Balancer のエンドポイントのプロパティおよび制限 (p. 18)
- Gateway Load Balancer エンドポイントのライフサイクル (p. 19)
- Gateway Load Balancer エンドポイントの料金 (p. 19)
- Gateway Load Balancer エンドポイントを作成する (p. 19)
- Gateway Load Balancer エンドポイントを表示する (p. 20)
- Gateway Load Balancer エンドポイントのタグを追加または削除する (p. 20)

Gateway Load Balancer のエンドポイントのプロパティおよび制限

Gateway Load Balancer エンドポイントを使用するには、以下の事項に留意してください。

- 各 Gateway Load Balancer エンドポイントにつき、VPC 内で選択できるアベイラビリティーゾーン (サブネット) は 1 つだけです。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、そのサブネットに新しい Gateway Load Balancer エンドポイントを作成します。サービスのアベイラビリティーゾーンごとに 1 つの Gateway Load Balancer エンドポイントを作成できます。ただし、作成できるのは、Gateway Load Balancer がサポートしているアベイラビリティーゾーンに対してのみです。
- 各 Gateway Load Balancer エンドポイントは、最大 40 Gbps の最大帯域幅をサポートします。
- サブネットのネットワーク ACL でトラフィックが制限される場合、Gateway Load Balancer エンドポイントを通じてトラフィックを送信できないことがあります。サブネットの CIDR ブロックに出入りするトラフィックを許可する適切なルールを追加してください。
- セキュリティグループはサポートされません。
- エンドポイントポリシーはサポートされていません。
- Gateway Load Balancer エンドポイントを介したサービスへのアクセスは、一部のアベイラビリティーゾーンでサポートされない場合があります。サポートされるアベイラビリティーゾーンを確認するには、describe-vpc-endpoint-services コマンドまたは Amazon VPC コンソールを使用してください。詳細については、「」を参照してくださいGateway Load Balancer エンドポイントを作成する (p. 19)
- Gateway Load Balancer エンドポイントを作成する場合、エンドポイントはアカウントにマッピングされているアベイラビリティーゾーンに作成され、他のアカウントからは独立したものになります。サービスプロバイダーとコンシューマーが別のアカウントにある場合、アベイラビリティーゾーン ID を使用してエンドポイントのアベイラビリティーゾーンを一意に一貫して識別します。例えば、`use1-az1` は `us-east-1` リージョンのアベイラビリティーゾーン ID であり、すべての AWS アカウントで同じ場所にマッピングされます。アベイラビリティーゾーン ID の詳細については、AWS RAM ユーザーガイドのリソースの AZ ID を参照するか、describe-availability-zonesを使用してください。

- 同じアベイラビリティー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ーゾーンに Gateway Load Balancer エンドポイントを作成することをお勧めします。
- 同じリージョン内のエンドポイントのみがサポートされています。別のリージョンで、VPC とサービス間のエンドポイントを作成することはできません。
- 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。
- 1 つの VPC から別の VPC にエンドポイントを転送したり、1 つのサービスから別のサービスにエンドポイントを転送することはできません。
- VPC あたりに作成できるエンドポイントの数にはクォータがあります。詳細については、「」を参照してください AWS PrivateLink のクォータ (p. 76)

Gateway Load Balancer エンドポイントのライフサイクル

Gateway Load Balancer エンドポイントは、その作成時 (エンドポイントの接続リクエスト) を始まりとして、様々な段階を経過します。段階ごとに、サービスコンシューマーとサービスプロバイダが実行できるアクションを伴う場合があります。

以下のルールが適用されます。

- サービスプロバイダーは、Gateway Load Balancer エンドポイントのリクエストを自動または手動で承諾するようにサービスを設定できます。
- サービスプロバイダーは、サービスへの Gateway Load Balancer エンドポイントを削除できません。Gateway Load Balancer エンドポイントを削除できるのは、接続をリクエストしたサービスコンシューマーのみです。
- サービスプロバイダーは、Gateway Load Balancer エンドポイントが受け入れられ、`available` 状態である場合に、そのエンドポイントを拒否できます。

Gateway Load Balancer エンドポイントの料金

サービスへの Gateway Load Balancer エンドポイントの作成と使用には料金がかかります。時間単位の使用料金とデータ処理料金が適用されます。詳細については、 AWS PrivateLink 料金を参照してください。Gateway Load Balancer エンドポイントの総数を表示するには、Amazon VPC コンソールまたは AWS CLI を使用します。

Gateway Load Balancer エンドポイントを作成する

Gateway Load Balancer エンドポイントを作成するには、エンドポイントを作成する先の VPC と、接続を確立する先のサービスを指定する必要があります。

Console

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]、[Create Endpoint] の順に選択します。
3. [Service category] で、[Find service by name] を選択します。
4. [Service Name] (サービス名) にサービスの名前を入力し、[Verify] (検証) を選択します。
5. 次の情報を入力し、[Create endpoint] を選択します。

   - [VPC] で、エンドポイントを作成する先の VPC を選択します。

- [Subnets] (サブネット) で、Gateway Load Balancer エンドポイントを作成するサブネット (アベイラビリティーゾーン) を選択します。
- (オプション) タグを追加するには、[Add Tag] (タグの追加) を選択して、タグのキーと値を指定します。

Command line

AWS CLI 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 コマンドを使用して、VPC ID、VPC エンドポイントのタイプ (Gateway Load Balancer)、サービス名、および Gateway Load Balancer エンドポイントを作成するサブネットを指定します。

```
aws ec2 create-vpc-endpoint --vpc-endpoint-type GatewayLoadBalancer --vpc-id vpc-id --
subnet-ids subnet-id --service-name gateway-load-balancer-service-name
```

AWS Tools for Windows PowerShell または API を使用して VPC エンドポイントを作成するには

- New-EC2VpcEndpoint
- CreateVpcEndpoint

Gateway Load Balancer エンドポイントを表示する

Gateway Load Balancer エンドポイントを作成したら、そのエンドポイントに関する情報を表示できます。

Console

コンソールを使用して Gateway Load Balancer エンドポイントに関する情報を表示するには

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、Gateway Load Balancer エンドポイントを選択します。
3. [Details] を選択します。
4. Gateway Load Balancer エンドポイントの作成先のサブネットと、エンドポイントネットワークインターフェイスの ID を表示するには、[Subnets] (サブネット) を選択します。

Command line

コマンドラインツールまたは API を使用して Gateway Load Balancer エンドポイントを記述するには

- describe-vpc-endpoints (AWS CLI)
- Get-EC2VpcEndpoint (Tools for Windows PowerShell)
- DescribeVpcEndpoints (Amazon EC2 クエリ API)

Gateway Load Balancer エンドポイントのタグを追加または削除する

Gateway Load Balancer エンドポイントのタグを追加または削除できます。

Console

タグを追加または削除するには

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、[エンドポイント] を選択します。
3. Gateway Load Balancer エンドポイントを選択し、[Actions] (アクション)、[Add/Edit Tags] (タグの追加/編集) の順に選択します。
4. タグを追加または削除します。

   [タグの追加] [タグの作成] を選択して、以下を実行します。

   - [キー] にはキー名を入力します。
   - [値] にキー値を入力します。

   [タグの削除] タグのキーと値の右側にある削除ボタン ("x") を選択します。

Command line

コマンドラインツールまたは API を使用してタグを追加または削除するには

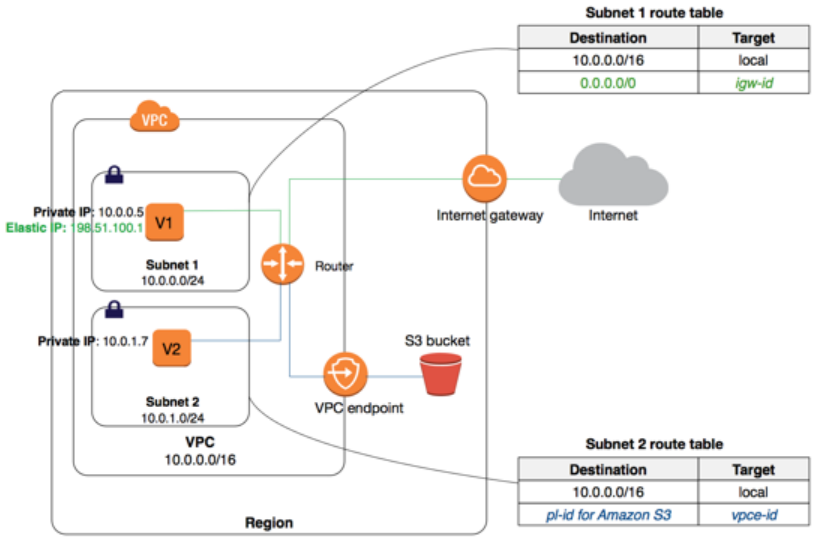
- create-tags および delete-tags を使用します (AWS CLI)。
- New-EC2Tag および Remove-EC2Tag を使用します (AWS Tools for Windows PowerShell)
- CreateTags および DeleteTags を使用します。(Amazon EC2 クエリ API)

ゲートウェイ VPC エンドポイント

ゲートウェイエンドポイントを作成して設定するには、以下の一般的な手順に従います。

1. エンドポイントを作成する VPC および接続先のサービスを指定します。サービスは、AWS マネージドプレフィックスリスト (リージョンのサービスの名前と ID) によって識別されます。AWS プレフィックスリストの ID の形式は `pl-xxxxxxx` で、AWS プレフィックスリストの名前の形式は「com.amazonaws.*region*.*service*」です。AWS プレフィックスリスト名 (サービス名) を使用してエンドポイントを作成します。
2. エンドポイントにエンドポイントポリシーをアタッチし、接続先の一部のサービスまたはすべてのサービスへのアクセスを許可します。詳細については、「」を参照してくださいVPC エンドポイントポリシーを使用する (p. 39)
3. サービスへのルートを作成する 1 つ以上のルートテーブルを指定します。ルートテーブルは、VPC と他のサービスの間のトラフィックのルーティングを制御します。これらのルートテーブルのいずれかに関連付けられている各サブネットはエンドポイントにアクセスでき、これらのサブネット内のインスタンスからサービスへのトラフィックはエンドポイント経由でルーティングされます。

以下の図では、サブネット 2 のインスタンスはゲートウェイエンドポイントを介して Amazon S3 にアクセスできます。



1 つの VPC 内に複数のエンドポイントを (複数のサービス用などに) 作成できます。また、1 つのサービス用に複数のエンドポイントを作成し、複数のルートテーブルを使用して、この同じサービスに複数のサブネットから異なるアクセスポリシーを適用することもできます。

エンドポイントを作成した後は、エンドポイントにアタッチされたエンドポイントポリシーを変更し、エンドポイントで使用されるルートテーブルを追加または削除できます。

目次

- ゲートウェイエンドポイントの料金 (p. 22)
- ゲートウェイエンドポイントのルーティング (p. 22)
- ゲートウェイエンドポイントの制限 (p. 24)
- Amazon S3 におけるエンドポイント (p. 25)
- Amazon DynamoDB のエンドポイント (p. 32)
- ゲートウェイエンドポイントを作成する (p. 35)
- セキュリティグループを変更する (p. 37)
- ゲートウェイエンドポイントを変更する (p. 37)
- ゲートウェイエンドポイントタグを追加または削除する (p. 38)

ゲートウェイエンドポイントの料金

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。データ転送とリソースの使用量に対する標準料金が適用されます。料金の詳細については、「Amazon EC2 料金表」を参照してください。

ゲートウェイエンドポイントのルーティング

エンドポイントを作成または変更するときは、エンドポイントを通じてサービスにアクセスするために使用する VPC ルートテーブルを指定します。ルートは、サービス (`pl-xxxxxxxx`) の AWS プレフィックスリスト ID を指定する送信先と、エンドポイント ID (`vpce-xxxxxxxx`) を持つターゲットを含む各ルートテーブルに自動的に追加されます。その例を以下に示します。

送信先	ターゲット
10.0.0.0/16	ローカル

送信先	ターゲット
pl-1a2b3c4d	vpce-11bb22cc

プレフィックスリスト ID は、サービスで使用されるパブリック IP アドレスの範囲を論理的に表します。特定の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、自動的にそのエンドポイントを使用してサービスにアクセスします。特定のルートテーブルに関連付けられていないサブネットは、エンドポイントを使用しません。これにより、他のサブネットのリソースをエンドポイントとは別に維持することができます。

サービスの現在のパブリック IP アドレス範囲を表示するには、describe-prefix-lists コマンドを使用しますが公開した現在の IP アドレス範囲のリストを表示できます。

> Note
>
> サービスのパブリック IP アドレス範囲は変更される場合があります。サービスの現在の IP アドレス範囲に基づき、ルーティングまたはその他の決定を行う前に、その影響について検討してください。

以下のルールが適用されます。

- ルートテーブル内の異なるサービスへの複数のエンドポイントルート、または異なるルートテーブル内の同じサービスへの複数のエンドポイントルートを持つことができます。ただし、1 つのルートテーブルに同じサービス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。たとえば、VPC で Amazon S3 への 2 つのエンドポイントを作成する場合、同じルートテーブルで両方のエンドポイントのエンドポイントルートを作成することはできません。
- ルートテーブル API を使用するか、Amazon VPC コンソールの [ルートテーブル] ページを使用して、ルートテーブルでエンドポイントルートを明示的に追加、変更、または削除することはできません。ルートテーブルをエンドポイントに関連付けて、エンドポイントルートを追加することのみできます。エンドポイントに関連付けられたルートテーブルを変更するには、エンドポイントを変更 (p. 37)します。
- エンドポイントルートは、エンドポイントからルートテーブルの関連付けを (エンドポイントを変更することで) 削除するか、エンドポイントを削除するときに自動的に削除されます。

AWS では、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)。インターネットゲートウェイを指すすべてのインターネットトラフィック (`0.0.0.0/0`) に対する既存のルートがルートテーブルにある場合、サービスを宛先とするすべ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。これは、サービスの IP アドレス範囲が `0.0.0.0/0` よりも具体的であるためです。他のすべてのインターネットトラフィックでは、他のリージョンのサービスへのトラフィックも含めて、インターネットゲートウェイが使用されます。

ただし、インターネットゲートウェイまたは NAT デバイスを指す IP アドレス範囲に対するより具体的な既存のルートがある場合は、そのルートが優先されます。サービスで使用されている IP アドレス範囲と同じ IP アドレス範囲への既存のルートがある場合、そのルートが優先されます。

例: ルートテーブルのエンドポイントルート

このシナリオでは、インターネットゲートウェイを指すすべてのインターネットトラフィック (`0.0.0.0/0`) に対する既存のルートがルーティングテーブルにあります。AWS の別のサービスを宛先とするサブネットからのトラフィックは、インターネットゲートウェイを使用します。

送信先	ターゲット
10.0.0.0/16	ローカル
0.0.0.0/0	igw-1a2b3c4d

サポートされた AWS のサービスへのエンドポイントを作成し、ルートテーブルをエンドポイントに関連付けます。エンドポイントルートがルートテーブルに自動的に追加され、送信先は `pl-1a2b3c4d` となります (これがエンドポイントの作成先サービスを表す場合)。これで、同じリージョンでこの AWS のサービスを宛先とするサブネットからのトラフィックはエンドポイントに移動し、インターネットゲートウェイには移動しません。他のすべてのインターネットトラフィック (他のサービスを宛先とするトラフィックや、他のリージョンの AWS のサービスを宛先とするトラフィックなど) は、インターネットゲートウェイに移動します。

送信先	ターゲット
10.0.0.0/16	ローカル
0.0.0.0/0	igw-1a2b3c4d
pl-1a2b3c4d	vpce-11bb22cc

例: エンドポイントに対するルートテーブルの調整

このシナリオでは、`54.123.165.0/24` は Amazon S3 IP アドレス範囲にあり、サブネットのインスタンスがインターネットゲートウェイ経由で Amazon S3 バケットと通信するようにルートテーブルを設定しました。`54.123.165.0/24` を持つルートを宛先として追加し、インターネットゲートウェイをターゲットとして追加します。次に、エンドポイントを作成し、このルートテーブルをエンドポイントに関連付けます。エンドポイントルートがルートテーブルに自動的に追加されます。次に、describe-prefix-lists コマンドを使用して、Amazon S3 の IP アドレス範囲を表示します。この範囲は `54.123.160.0/19` で、これはインターネットゲートウェイを指している範囲ほど具体的ではありません。つまり、IP アドレス範囲 `54.123.165.0/24` へのトラフィックは引き続きインターネットゲートウェイを使用し、エンドポイントを使用しないことになります (Amazon S3 のパブリック IP アドレス範囲がこのまま変わらない場合)。

送信先	ターゲット
10.0.0.0/16	ローカル
54.123.165.0/24	igw-1a2b3c4d
pl-1a2b3c4d	vpce-11bb22cc

同じリージョンの Amazon S3 へのすべてのトラフィックがエンドポイントを通じてルーティングされるようにするには、ルートテーブルのルートを調整する必要があります。そのためには、インターネットゲートウェイへのルートを削除します。これで、同じリージョンの Amazon S3 へのすべてのトラフィックはエンドポイントを使用し、ルートテーブルに関連付けられたサブネットはプライベートサブネットになります。

送信先	ターゲット
10.0.0.0/16	ローカル
pl-1a2b3c4d	vpce-11bb22cc

ゲートウェイエンドポイントの制限

ゲートウェイエンドポイントを使用するには、現在の制限に注意する必要があります。

- ネットワーク ACL のアウトバウンドルールで AWS プレフィックスリスト ID を使用して、エンドポイントで指定されたサービスへのアウトバウンドトラフィックを許可または拒否することはできません。

ネットワーク ACL ルールがトラフィックを制限する場合は、代わりにサービスの CIDR ブロック (IP アドレス範囲) を指定する必要があります。ただし、アウトバウンドセキュリティグループのルールで AWS プレフィックスリスト ID を使用できます。詳細については、「」を参照してくださいセキュリティグループ (p. 40)

- 同じリージョン内のエンドポイントのみがサポートされています。別のリージョンで、VPC とサービス間のエンドポイントを作成することはできません。
- 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。
- 1 つの VPC から別の VPC にエンドポイントを転送したり、1 つのサービスから別のサービスにエンドポイントを転送することはできません。
- VPC あたりに作成できるエンドポイントの数にはクォータがあります。詳細については、「」を参照してください AWS PrivateLink のクォータ (p. 76)
- 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、AWS Direct Connect 接続、または VPC の ClassicLink 接続の他方の側にあるリソースは、エンドポイントを使用してエンドポイントサービスのリソースと通信することはできません。
- VPC 内で DNS 解決を有効にするか、ご自身で所有する DNS サーバーを使用している場合は、Amazon S3 などの必要なサービスに送られる DNS リクエストが により維持される IP アドレスに正しく解決されていることを確認する必要がありますAWS 詳細については、Amazon VPC ユーザーガイドの VPC での DNS の使用およびアマゾン ウェブ サービスの全般的なリファレンスの AWS IP アドレス範囲を参照してください。
- エンドポイントサービスのサービス固有の制限を確認します。

Amazon S3 固有のルールと制限の詳細については、「Amazon S3 におけるエンドポイント (p. 25)」を参照してください。

DynamoDB 固有のルールと制限の詳細については、「Amazon DynamoDB のエンドポイント (p. 32)」を参照してください。

Amazon S3 におけるエンドポイント

既に VPC から Amazon S3 リソースへのアクセスを設定している場合、エンドポイントの設定後に、引き続き Amazon S3 DNS 名を使用してそれらのリソースにアクセスできます。ただし、以下のことに注意してください。

- エンドポイントには、Amazon S3 リソースにアクセスするエンドポイントの使用を管理するポリシーがあります。デフォルトのポリシーでは、任意の AWS アカウント からの認証情報を使用して、VPC 内のユーザーまたはサービスによる、任意の Amazon S3 リソースへのアクセスが許可されます。これには、VPC が関連付けられているアカウントとは別の AWS アカウント の Amazon S3 リソースが含まれます。詳細については、「」を参照してくださいVPC エンドポイントでサービスへのアクセスを制御する (p. 39)
- 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。
- IAM ポリシーまたはバケットポリシーを使用して VPC IPv4 CIDR 範囲 (プライベート IPv4 アドレス範囲) からのアクセスを許可することはできません。VPC CIDR ブロックは重複または同じになる場合があり、それによって予期しない結果が発生する可能性があります。したがって、VPC エンドポイントを介した Amazon S3 へのリクエストに、IAM ポリシーの `aws:SourceIp` 条件を使用することはできません。これはユーザーとロールの IAM ポリシー、およびバケットポリシーに適用されます。ステートメントに `aws:SourceIp` 条件が含まれる場合、値は指定した IP アドレスまたは IP アドレス範囲に一致しません。代わりに、以下を実行できます。

  - ルートテーブルを使用して、エンドポイントを通じて Amazon S3 内のリソースにアクセスできるインスタンスを制御します。
  - バケットポリシーの場合、特定のエンドポイントまたは特定の VPC へのアクセスを制限できます。詳細については、「」を参照してくださいAmazon S3 バケットポリシー (p. 30)
- 現在、エンドポイントはクロスリージョンのリクエストをサポートしていません。必ずバケットと同じリージョンでエンドポイントを作成してください。Amazon S3 コンソールを使用するか、get-bucket-location コマンドを使用して、バケットの場所を見つけることができます。リージョン固有の Amazon S3 エンドポイントを使用してバケットにアクセスします (例: `mybucket.s3.us-west-2.amazonaws.com`)。Amazon S3 のリージョン固有のエンドポイントの詳細については、アマゾン ウェブ サービスの全般的なリファレンスの「Amazon Simple Storage Service (S3)」を参照してください。AWS CLI を使用して Amazon S3 にリクエストを実行する場合は、デフォルトリージョンをバケットと同じリージョンに設定するか、またはリクエストで `--region` パラメータを使用します。

  Note

  Amazon S3 向けの米国スタンダードリージョンは、`us-east-1` リージョンにマッピングされているものとして扱います。
- 現在、エンドポイントは IPv4 トラフィックでのみサポートされています。

Amazon S3 でエンドポイントを使用する前に、次の一般的な制限を読んだことも確認します: 「ゲートウェイエンドポイントの制限 (p. 24)」。S3 バケットの作成と表示については、Amazon Simple Storage Service ユーザーガイドの「S3 バケットを作成する方法」および「S3 バケットのプロパティを表示する方法」を参照してください。

VPC の他の AWS のサービスを使用する場合は、特定のタスクに S3 バケットが使用される可能性があります。必ず、エンドポイントのポリシーで Amazon S3 へのフルアクセス (デフォルトのポリシー) を許可するか、またはそれらのサービスで使用される特定のバケットへのアクセスを許可します。または、これらのいずれのサービスによっても使用されないサブネットでのみエンドポイントを作成し、サービスが継続してパブリック IP アドレスを使用して S3 バケットにアクセスできるようにします。

次の表は、エンドポイントによって影響を受ける可能性のある AWS のサービスと、各サービスに固有の情報を示しています。

AWS のサービス	注意
Amazon AppStream 2.0	エンドポイントポリシーでは、ユーザーのコンテンツを保存するために AppStream 2.0 で使用される特定のバケットへのアクセスを許可する必要があります。詳細については、Amazon AppStream 2.0 管理ガイドの「ホームフォルダおよびアプリケーション設定の永続化に Amazon S3 VPC エンドポイントを使用する」を参照してください。
AWS CloudFormation	待機条件またはカスタムリソースリクエストに応答する必要があるリソースが VPC にある場合、エンドポイントポリシーで、少なくともこれらのリソースで使用される特定のバケットへのアクセスを許可する必要があります。詳細については、「AWS CloudFormation VPC エンドポイントの設定」を参照してください。
CodeDeploy	エンドポイントポリシーでは、Amazon S3 へのフルアクセス、または CodeDeploy のデプロイ用に作成した S3 バケットへのアクセスを許可する必要があります。

AWS のサービス	注意
Elastic Beanstalk	エンドポイントポリシーでは、少なくとも Elastic Beanstalk アプリケーションに使用された S3 バケットへのアクセスを許可する必要があります。詳細については、AWS Elastic Beanstalk デベロッパーガイドの Amazon S3 で Elastic Beanstalk を使用するを参照してください。
Amazon EMR	エンドポイントポリシーでは、Amazon EMR で使用される Amazon Linux リポジトリおよびその他のバケットへのアクセスを許可する必要があります。詳細については、Amazon EMR 管理ガイドの「プライベートサブネットの最小 Amazon S3 ポリシー」を参照してください。
AWS OpsWorks	エンドポイントポリシーでは、少なくとも で使用される特定のバケットへのアクセスを許可する必要がありますAWS OpsWorks 詳細については、AWS OpsWorks ユーザーガイドの VPC でのスタックの実行を参照してください。
AWS Systems Manager	エンドポイントポリシーで、AWS リージョンのパッチベースラインオペレーションのために Patch Manager によって使用される Amazon S3 バケットへのアクセスを許可する必要があります。これらのバケットには、パッチベースラインサービスによって取得され、インスタンスで実行されるコードが含まれます。詳細については、AWS Systems Manager ユーザーガイドの仮想プライベートクラウドエンドポイントの作成を参照してください。 オペレーションのために SSM Agentで必要な S3 バケットのアクセス許可のリストについては、AWS Systems Manager ユーザーガイドの SSM Agentの最小 S3 バケットアクセス許可を参照してください。
Amazon Elastic Container Registry	エンドポイントポリシーでは、Docker イメージレイヤーを保存するために Amazon ECR で使用される Amazon S3 バケットへのアクセスを許可する必要があります。詳細については、Amazon Elastic Container Registry ユーザーガイドの Amazon ECR の最小 Amazon S3 バケットアクセス許可に関する記事を参照してください。
Amazon WorkDocs	WorkSpaces または EC2 インスタンスで Amazon WorkDocs クライアントを使用している場合、エンドポイントポリシーでは、Amazon S3 へのフルアクセスを許可する必要があります。

AWS のサービス	注意
WorkSpaces	WorkSpaces は Amazon S3 に直接依存しません。ただし、WorkSpaces ユーザーにインターネットアクセスを提供する場合は、他の企業のウェブサイト、HTML メール、およびインターネットサービスが Amazon S3 に依存している可能性があることに注意してください。エンドポイントポリシーで Amazon S3 へのフルアクセスを許可し、これらのサービスが引き続き正しく動作できるようにします。

VPC と S3 バケット間のトラフィックは、Amazon ネットワークを離れません。

Amazon S3 のエンドポイントポリシー

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。詳細については、「」を参照してくださいVPC エンドポイントポリシーを使用する (p. 39) ビジネスニーズに合ったポリシー制限は、ユーザーが決定します。

> Important
>
> すべてのタイプのポリシー (IAM ユーザーポリシー、エンドポイントポリシー、S3 バケットポリシー、および Amazon S3 ACL ポリシー (存在する場合)) では、Amazon S3 が成功するために必要なアクセス許可を付与する必要があります。
> AWS では、特定の呼び出し元に対してエンドポイントの使用を制限する場合は、VPC エンドポイントポリシーで IAM `Principal` 要素ではなく IAM 条件を使用することをお勧めします。このような条件の例としては `aws:PrincipalArn`、`aws:PrincipalAccount`、`aws:PrincipalOrgId` や `aws:PrincipalOrgPaths` があります。条件コンテキストキーの詳細については、AWS Identity and Access Management 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。

Example 例: 特定のバケットへのアクセスの制限

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 で S3 バケットを使用する他の AWS サービスがある場合に便利です。指定されたバケットのみへのアクセスを制限するポリシーの例を次に示します。

```
{
  "Effect": "Allow",
  "Action": [
     "s3:ListBucket",
     "s3:GetObject",
     "s3:PutObject"
  ],
  "Resource": [
     "arn:aws:s3:::example-bucket",
     "arn:aws:s3:::example-bucket/*"
  ]
}
```

Example 例: この VPC エンドポイントの使用をアカウントの特定の IAM ロールに制限する

VPC エンドポイントの使用を特定の IAM ロールに制限するポリシーを作成できます。指定されたアカウントの指定されたロールへのアクセスを制限する例を次に示します。

```
{
  "Sid": "Restrict-acess-to-specific-IAM-role",
```

```
  "Effect": "Allow",
  "Principal": "*",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "ArnEquals": {
      "aws:PrincipalArn": "arn:aws:iam::111122223333:role/SomeRole"
    }
  }
}
```

Example 例: この VPC エンドポイントの使用を特定のアカウントのユーザーに制限する

VPC エンドポイントの使用を特定のアカウントに制限するポリシーを作成できます。指定されたアカウントのユーザーへのアクセスを制限する例を次に示します。

```
{
  "Sid": "AllowCallersFromAccount111122223333",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:PrincipalAccount": "111122223333"
    }
  }
}
```

Example 例: Amazon Linux AMI リポジトリへのアクセスの有効化

Amazon Linux AMI リポジトリは、各リージョン内の Amazon S3 バケットです。VPC 内のインスタンスが、エンドポイント経由でリポジトリにアクセスできるようにする場合、それらのバケットへのアクセスを有効にするエンドポイントポリシーを作成します。

次のポリシーでは、Amazon Linux リポジトリへのアクセスが許可されます。

`region` は、実際の AWS リージョン (us-east-1 など) に置き換える必要があります。

```
{
  "Statement": [
    {
      "Sid": "AmazonLinuxAMIRepositoryAccess",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::packages.region.amazonaws.com/*",
        "arn:aws:s3:::repo.region.amazonaws.com/*"
      ]
    }
  ]
}
```

次のポリシーでは、Amazon Linux 2 のリポジトリへのアクセスが許可されます。

`region` は、実際の AWS リージョン (us-east-1 など) に置き換える必要があります。

```
{
  "Statement": [
```

```
    {
      "Sid": "AmazonLinux2AMIRepositoryAccess",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amazonlinux.region.amazonaws.com/*"
        "arn:aws:s3:::amazonlinux-2-repos-region/*"
      ]
    }
  ]
}
```

Amazon S3 バケットポリシー

バケットポリシーを使用して、特定のエンドポイント、VPC、IP アドレス範囲、または AWS アカウントからバケットへのアクセスを制御できます。

VPC エンドポイントを介した Amazon S3 へのリクエストに、バケットポリシーの `aws:SourceIp` 条件を使用することはできません。条件が、指定した IP アドレスまたは IP アドレス範囲のいずれにも一致しない場合、Amazon S3 バケットに対しリクエストを作成するときに望ましくない影響が生じる可能性があります。以下に例を示します。

- `Deny` 効果と `NotIpAddress` 条件を持つバケットポリシーがある場合、そのポリシーは単一、または制限された IP アドレス範囲のみからのアクセスを許可するためのものです。エンドポイントを通じてバケットに送られるリクエストは、ポリシー内の他の制約が一致すると仮定して、`NotIpAddress` 条件が必ず一致し、ステートメントの効果が適用されます。バケットへのアクセスは拒否されます。
- `Deny` 効果と `IpAddress` 条件を持つバケットポリシーがある場合、そのポリシーは単一、または制限された IP アドレス範囲のみへのアクセスを拒否するためのものです。エンドポイントを通じてバケットに送られるリクエストには、条件は一致せず、ステートメントは適用されません。`IpAddress` 条件がなくてもアクセスを許可するステートメントが他にあると仮定して、バケットへのアクセスが許可されます。

代わりに `aws:VpcSourceIp` を使用して、特定の IP アドレス範囲からのアクセスを制御できます。

IAM ユーザーがバケットポリシーを操作できるようにするには、`s3:GetBucketPolicy` および `s3:PutBucketPolicy` アクションを使用するアクセス許可を付与する必要があります。

Amazon S3 のバケットポリシーの詳細については、Amazon Simple Storage Service ユーザーガイドの「バケットポリシーとユーザーポリシーの使用」を参照してください。

Example 例: 特定の エンドポイントへのアクセスの制限

`aws:sourceVpce` 条件を使用して、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。以下に、エンドポイント `vpce-1a2b3c4d` からバケット `example_bucket` にアクセスできるようにする S3 バケットポリシーの例を示します。指定されたエンドポイントを使用していない場合、ポリシーによりバケットへのすべてのアクセスが拒否されます。`aws:sourceVpce` 条件では VPC エンドポイントリソースに ARN を必要とせず、エンドポイント ID のみを必要とします。

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
```

```
      "Resource": ["arn:aws:s3:::example_bucket",
                   "arn:aws:s3:::example_bucket/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

Example 例: 特定の VPC へのアクセスの制限

aws:sourceVpc 条件を使用して、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、すべてのエンドポイントについて S3 バケットへのアクセスを管理する場合に便利です。以下に、vpc-111bbb22 およびそのオブジェクトへのアクセスを VPC example_bucket に許可するポリシーの例を示します。指定された VPC を使用していない場合、ポリシーによりバケットへのすべてのアクセスが拒否されます。aws:sourceVpc 条件では、VPC リソースへの ARN は必要なく、VPC ID のみが必要です。

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPC-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "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の制限

aws:VpcSourceIp 条件を使用して、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。以下に、example_bucket およびそのオブジェクトへのアクセスを 172.31.0.0/16 に許可するポリシーの例を示します。このポリシーでは、他の IP アドレス範囲からのバケットへのアクセスを拒否します。

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPC-CIDR-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::example_bucket",
                   "arn:aws:s3:::example_bucket/*"],
      "Condition": {
        "NotIpAddress": {
          "aws:VpcSourceIp": "172.31.0.0/16"
        }
```

```
      }
    }
  ]
}
```

Example 例: 特定の AWS アカウント のバケットへのアクセスの制限

`s3:ResourceAccount` 条件を使用して、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。これは、VPC 内のクライアントが、お客様が所有していないバケットにアクセスすることを制限したい場合に役立ちます。`111122223333` のアカウント ID で、単一の AWS アカウント が所有するリソースへのアクセスを制限するポリシーの例は次のとおりです。

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-bucket-in-specific-account-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "StringNotEquals": {
          "s3:ResourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

Amazon DynamoDB のエンドポイント

すでに VPC から DynamoDB テーブルへのアクセスを設定している場合、ゲートウェイエンドポイントの設定後は、通常のように引き続きテーブルにアクセスすることができます。ただし、以下のことに注意してください。

- エンドポイントには、DynamoDB リソースにアクセスするエンドポイントの使用を管理するポリシーがあります。デフォルトポリシーでは、VPC 内のあらゆるユーザーまたはサービスは、どの AWS アカウントの認証情報を使用しても、すべての DynamoDB リソースにアクセスできます。詳細については、「」を参照してくださいVPC エンドポイントでサービスへのアクセスを制御する (p. 39)
- DynamoDB はリソースベースのポリシー (テーブル上など) をサポートしません。DynamoDB へのアクセスはエンドポイントポリシーと、個別の IAM ユーザーとロールの IAM ポリシーを通じて管理されます。
- 現在、エンドポイントはクロスリージョンのリクエストをサポートしていません。必ず DynamoDB テーブルと同じリージョンでエンドポイントを作成してください
- 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 VPC の EC2 インスタンスのプライベート IP アドレスと、エンドポイントを通じて実行されるアクションのエンドポイント ID が含まれます。
- 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。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 DynamoDB 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。

DynamoDB でエンドポイントを使用する前に、次の一般的な制限を読んだことも確認します。「ゲートウェイエンドポイントの制限 (p. 24)」。

ゲートウェイ VPC エンドポイントの作成の詳細については、「ゲートウェイ VPC エンドポイント (p. 21)」を参照してください。

DynamoDB のエンドポイントポリシー

エンドポイントは、接続先の一部のサービスまたはすべてのサービスへのアクセスを許可することができるエンドポイントにアタッチする IAM ポリシーです。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。

> Important
>
> すべてのタイプのポリシー (IAM ユーザーポリシーとエンドポイントポリシー) では、DynamoDB へのアクセスが成功するために必要なアクセス許可を付与する必要があります。

Example 例: 読み取り専用アクセス

VPC エンドポイントを通じて、DynamoDB テーブルの一覧表示と記述のみにアクションを制限するポリシーを作成できます。

```
{
  "Statement": [
    {
      "Sid": "ReadOnly",
      "Principal": "*",
      "Action": [
        "dynamodb:DescribeTable",
        "dynamodb:ListTables"
      ],
      "Effect": "Allow",
      "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。この例では、エンドポイントポリシーでは、`StockTable` のみへのアクセスが許可されます。

```
{
  "Statement": [
    {
      "Sid": "AccessToSpecificTable",
      "Principal": "*",
      "Action": [
        "dynamodb:Batch*",
        "dynamodb:Delete*",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Update*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:dynamodb:us-east-1:123456789012:table/StockTable"
    }
  ]
}
```

IAM ポリシーを使用して DynamoDB へのアクセスをコントロールする

IAM ユーザー、グループ、またはロールの IAM ポリシーを作成して、特定の VPC エンドポイントのみから DynamoDB テーブルへのアクセスを制限できます。これを行うには、IAM ポリシーでテーブルリソースの `aws:sourceVpce` 条件キーを使用できます。

DynamoDB へのアクセス管理の詳細については、Amazon DynamoDB デベロッパーガイドのAmazon DynamoDB に対する認証とアクセスコントロールに関する記事を参照してください。

Example 例: 特定のエンドポイントからのアクセスの制限

この例では、エンドポイント `vpce-11aa22bb` を通じてアクセスした場合を除き、ユーザーは DynamoDB テーブルを操作するアクセス許可を拒否されます。

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

Example 例: この VPC エンドポイントの使用をアカウントの特定の IAM ロールに制限する

VPC エンドポイントの使用を特定の IAM ロールに制限するポリシーを作成できます。以下は、アカウント `SomeRole` 内の `111122223333` へのアクセスを制限する例です。

```
{
  "Sid": "Restrict-acess-to-specific-IAM-role",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "ArnEquals": {
      "aws:PrincipalArn": "arn:aws:iam::111122223333:role/SomeRole"
    }
  }
}
```

Example 例: この VPC エンドポイントの使用を特定のアカウントのユーザーに制限する

VPC エンドポイントの使用を特定のアカウントに制限するポリシーを作成できます。以下は、アカウント `111122223333` のユーザーへのアクセスを制限する例です。

```
{
  "Sid": "AllowCallersFromAccount111122223333",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
```

```
      "aws:PrincipalAccount": "111122223333"
    }
  }
}
```

ゲートウェイエンドポイントを作成する

エンドポイントを作成するには、エンドポイントを作成する VPC と、接続を確立するサービスを指定する必要があります。

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]、[Create Endpoint] の順に選択します。
3. [Service Name] で、接続先のサービスを選択します。DynamoDB または Amazon S3 へのゲートウェイエンドポイントを作成するには、[タイプ] 例に [ゲートウェイ] と表示されていることを確認します。
4. 次の情報を入力し、[Create endpoint] を選択します。
   - [VPC] で、エンドポイントを作成する先の VPC を選択します。
   - [Configure route tables] 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。選択したルートテーブルに、サービスへのトラフィックを対象とするルートが自動的に追加されます。
   - [Policy] で、ポリシーのタイプを選択します。デフォルトのオプションである [Full Access] のみそのまま使用して、サービスへのフルアクセスを許可できます。または、[Custom (カスタム)] を選択し、AWS Policy Generator を使用してカスタムポリシーを作成するか、独自のポリシーをカスタムウィンドウに入力することもできます。
   - (オプション) タグを追加または削除します。

     [タグの追加] [タグの追加] を選択して、以下を実行します。
     - [キー] にはキー名を入力します。
     - [値] にキー値を入力します。

     [タグの削除] タグのキーと値の右側にある削除ボタン ("x") を選択します。

エンドポイントの作成後に、その関連情報を表示できます。

コンソールを使用してゲートウェイエンドポイントに関する情報を表示するには

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. エンドポイントに関する情報を表示するには、[Summary] を選択します。サービスの AWS プレフィックスリスト名は [Service] (サービス) ボックスで取得できます。
4. エンドポイントで使用するルートテーブルに関する情報を表示するには、[Route Tables] を選択します。
5. エンドポイントにアタッチされた IAM ポリシーを表示するには、[ポリシー] を選択します。

   Note

   [Policy] タブでは、エンドポイントのポリシーのみが表示されます。ここには、エンドポイントを操作するアクセス許可を持っている IAM ユーザー用の IAM ポリシーに関する情報は表示されません。また、サービス固有のポリシー (たとえば S3 バケットポリシー) も表示されません。

AWS CLI を使用してエンドポイントを作成および表示するには

1. describe-vpc-endpoint-services コマンドを使用して使用可能なサービスのリストを取得します。返された出力で、接続先のサービスの名前をメモします。`serviceType` フィールドは、インターフェイ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介してサービスに接続するかどうかを示します。

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

```
{
    "serviceDetailSet": [
        {
            "serviceType": [
                {
                    "serviceType": "Gateway"
                }
            ...
```

2. ゲートウェイエンドポイント (Amazon S3 など) を作成するには、create-vpc-endpoint コマンドを使用して、VPC ID、サービス名、およびエンドポイントを使用するルートテーブルを指定します。オプションとして、`--policy-document` パラメータを使用してサービスへのアクセスを制御するカスタムポリシーを指定できます。このパラメータを使用しない場合は、サービスへのフルアクセスを許可するデフォルトのポリシーがアタッチされます。

   Amazon S3 の場合は、`--vpc-endpoint-type` パラメータを `Gateway` に設定する必要があります。

```
aws ec2 create-vpc-endpoint --vpc-id vpc-1a2b3c4d --service-name com.amazonaws.us-
east-1.s3 --route-table-ids rtb-11aa22bb --vpc-endpoint-type Gateway
```

3. describe-vpc-endpoints コマンドを使用してエンドポイントを記述します。

```
aws ec2 describe-vpc-endpoints
```

AWS Tools for Windows PowerShell または API を使用して使用可能なサービスを記述するには

- Get-EC2VpcEndpointService (AWS Tools for Windows PowerShell)
- DescribeVpcEndpointServices (Amazon EC2 クエリ API)

AWS Tools for Windows PowerShell または API を使用して VPC エンドポイントを作成するには

- New-EC2VpcEndpoint (AWS Tools for Windows PowerShell)
- CreateVpcEndpoint (Amazon EC2 クエリ API)

AWS Tools for Windows PowerShell または API を使用して VPC エンドポイントを記述するには

- Get-EC2VpcEndpoint (AWS Tools for Windows PowerShell)
- DescribeVpcEndpoints (Amazon EC2 クエリ API)

セキュリティグループを変更する

インスタンスに関連付けられた VPC セキュリティグループでアウトバウンドトラフィックが制限されている場合は、AWS サービスへのトラフィックをインスタンスから送信することを許可するルールを追加する必要があります。

ゲートウェイエンドポイントのアウトバウンドルールを追加するには

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、[Security Groups] を選択します。
3. VPC セキュリティグループを選択して、[Outbound rules (アウトバウンドルール)] タブを選択し、[Edit outbound rules (アウトバウンドルールの編集)] を選択します。
4. [Type] リストからトラフィックのタイプを選択し、必要に応じてポート範囲を入力します。たとえば、インスタンスを使用して Amazon S3 からオブジェクトを取得する場合、[タイプ] リストから [HTTPS] を選択します。
5. [Destination] で、`pl-` の入力を開始して、使用可能な AWS サービスのプレフィクスリスト ID と名前のリストを表示します。AWS のサービスのプレフィックスリスト ID を選択するか、入力します。
6. [Save] を選択します。

コマンドラインまたは API を使用して、AWS のサービスのプレフィックスリスト名、ID、および IP アドレス範囲を取得するには

- describe-prefix-lists (AWS CLI)
- Get-EC2PrefixList (AWS Tools for Windows PowerShell)
- DescribePrefixLists (Amazon EC2 クエリ API)

ゲートウェイエンドポイントを変更する

ゲートウェイエンドポイントを変更するには、そのポリシーを変更または削除し、エンドポイントで使用されているルートテーブルを追加または削除します。

既存の Amazon S3 ゲートウェイエンドポイントをインターフェイスエンドポイントに移行する場合は、Amazon S3 インターフェイスエンドポイントを作成した後、Amazon S3 ゲートウェイエンドポイントを削除します。詳細については、「the section called “インターフェイスエンドポイントの作成” (p. 9)」および「the section called “VPC エンドポイントを削除する” (p. 40)」を参照してください。

ゲートウェイエンドポイントに関連付けられている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] を選択し、エンドポイントを選択します。
3. [Actions]、[Edit policy] の順に選択します。
4. [Full Access] を選択すると、フルアクセスを許可できます。または、[Custom (カスタム)] を選択し、AWS Policy Generator を使用してカスタムポリシーを作成するか、独自のポリシーをカスタムウィンドウに入力します。完了したら、[Save] を選択します。

   Note

   変更が適用されるまで数分かかることがあります。

ゲートウェイエンドポイントで使用されるルートテーブルを追加または削除するには

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 (アクション)]、[Manage Route Tables (ルートテーブルの管理)] の順に選択します。
4. 該当するルートテーブルを選択または選択解除し、[ルートテーブルの変更] を選択します。

AWS CLI 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

1. describe-vpc-endpoints コマンドを使用してゲートウェイエンドポイントの ID を取得します。

```
aws ec2 describe-vpc-endpoints
```

2. 次の例では、modify-vpc-endpoint コマンドを使用してルートテーブル `rtb-aaa222bb` をゲートウェイエンドポイントに関連付け、ポリシードキュメントをリセットします。

```
aws ec2 modify-vpc-endpoint --vpc-endpoint-id vpce-1a2b3c4d --add-route-table-ids rtb-aaa222bb --reset-policy
```

AWS Tools for Windows PowerShell または API を使用して VPC エンドポイントを変更するには

- Edit-EC2VpcEndpoint (AWS Tools for Windows PowerShell)
- ModifyVpcEndpoint (Amazon EC2 クエリ API)

ゲートウェイエンドポイントタグを追加または削除する

タグはゲートウェイインターフェイスを識別する方法を提供します。タグを追加または削除できます。

ゲートウェイエンドポイントタグを追加または削除するには

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、[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し、[アクション]、[タグの追加/編集] の順に選択します。
4. タグを追加または削除します。

   [タグの追加] [タグの作成] を選択して、以下を実行します。
   - [キー] にはキー名を入力します。
   - [値] にキー値を入力します。

   [タグの削除] タグのキーと値の右側にある削除ボタン ("x") を選択します。

AWS Tools for Windows PowerShell または API を使用してタグを追加または削除するには

- create-tags (AWS CLI)
- CreateTags (AWS Tools for Windows PowerShell)
- delete-tags (AWS CLI)
- DeleteTags (AWS Tools for Windows PowerShell)

VPC エンドポイントでサービスへのアクセスを制御する

インターフェイスまたはゲートウェイエンドポイントの作成時にエンドポイントポリシーをアタッチし、接続先のサービスへのアクセスを制御できます。エンドポイントのポリシーは、JSON 形式で記述される必要があります。すべて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るわけではありません。

Amazon S3 への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できます。詳細については、「」を参照してくださいAmazon S3 バケットポリシー (p. 30)

目次

- VPC エンドポイントポリシーを使用する (p. 39)
- セキュリティグループ (p. 40)

VPC エンドポイントポリシーを使用する

VPC エンドポイントポリシーは、エンドポイントの作成時または変更時にエンドポイントにアタッチする IAM リソースポリシーです。エンドポイントの作成時にポリシーをアタッチしない場合、サービスへのフルアクセスを許可するデフォルトのポリシーがアタッチされます。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、エンドポイントはサービスへのフルアクセスを許可します。エンドポイントポリシーは、IAM ユーザーポリシーやサービス固有のポリシー (S3 バケットポリシーなど) を上書き、または置き換えません。これは、エンドポイントから指定されたサービスへのアクセスを制御するための別のポリシーです。

1 つのエンドポイントに複数のポリシーを関連付けることはできません。ただし、ポリシーはいつでも変更できます。ポリシーを変更した場合、変更が適用されるまで数分かかることがあります。ポリシーの詳細については、IAM ユーザーガイドの「IAM でのポリシーとアクセス許可」を参照してください。

エンドポイントポリシーは、他の IAM ポリシーと同様にすることができます。ただし、以下のことに注意してください。

- 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。ゲートウェイエンドポイントに関する追加情報については、「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 (p. 39)」を参照してください。
- エンドポイントポリシーのサイズが 20,480 文字を超えることはできません (空白を含む)。

エンドポイントポリシーをサポートするサービスの詳細については、「 AWS PrivateLink をサポートするサービス (p. 70)」を参照してください。

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

ゲートウェイエンドポイントに適用されるエンドポイントポリシーの場合、`Principal` を `"AWS":"account-ID"` 形式または `"AWS":"arn:aws:iam::account-ID:root"` 形式で指定すると、アカウントのすべての IAM ユーザーとロールにアクセス権が付与されるのではなく、アカウントのルートユーザーにのみアクセス権が付与されます。

`Principal` 要素に Amazon リソースネーム (ARN) を指定すると、ポリシーの保存時に ARN は一意のプリンシパル ID に変換されます。

Amazon S3 および DynamoDB のエンドポイントのポリシーの例については、以下のトピックを参照してください。

- Amazon S3 のエンドポイントポリシー (p. 28)
- DynamoDB のエンドポイントポリシー (p. 33)

セキュリティグループ

インターフェイスエンドポイントの作成時に、VPC で作成されたエンドポイントネットワークインターフェイスにセキュリティグループを関連付けることができます。セキュリティグループを指定しないと、エンドポイントネットワークインターフェイスには、VPC のデフォルトのセキュリティグループが自動的に関連付けられます。セキュリティグループのルールが、エンドポイントネットワークインターフェイスと VPC 内のリソース (サービスと通信するリソース) との通信を許可することを確認する必要があります。

ゲートウェイエンドポイントについては、セキュリティグループのアウトバウンドルールが制限されている場合、VPC からエンドポイントで指定されたサービスへのアウトバウンドトラフィックを許可するルールを追加する必要があります。これを行うには、アウトバウンドルールでサービスの AWS プレフィックスリスト ID を送信先として使用できます。詳細については、「」を参照してくださいセキュリティグループを変更する (p. 37)

セキュリティグループは、Gateway Load Balancer のエンドポイントには適用されません。

VPC エンドポイントを削除する

エンドポイントが不要になった場合には、それを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、エンドポイントで使用されていたルートテーブル内のエンドポイントルートも削除されます。ただし、エンドポイントを含む VPC に関連付けられたセキュリティグループには影響しません。インターフェイスエンドポイントまたは Gateway Load Balancer エンドポイントを削除すると、エンドポイント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。

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。

VPC 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)
- DeleteVpcEndpoints (Amazon EC2 クエリ API)

VPC エンドポイントサービス (AWS PrivateLink)

VPC で独自のアプリケーションを作成し、これを AWS PrivateLink を使用するサービス (エンドポイントサービス) として設定できます。他の AWS プリンシパルは、サービスのタイプに応じて、インターフェイス VPC エンドポイント (p. 3)または Gateway Load Balancer エンドポイント (p. 17)を使用して、VPC からエンドポイントサービスへの接続を作成できます。お客様はサービスプロバイダであり、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。

目次

- インターフェイスエンドポイントの VPC エンドポイントサービス (p. 41)
- Gateway Load Balancer エンドポイントの VPC エンドポイントサービス (p. 45)
- インターフェイスエンドポイントの VPC エンドポイントサービス設定を作成する (p. 47)
- Gateway Load Balancer エンドポイントの VPC エンドポイントサービス設定を作成する (p. 48)
- エンドポイントサービスのアクセス権限を追加または削除する (p. 49)
- エンドポイントサービス設定を変更 (p. 51)
- エンドポイントの接続リクエストを承諾または拒否する (p. 52)
- エンドポイントサービスの通知を作成および管理する (p. 53)
- VPC エンドポイントサービスタグを追加または削除する (p. 56)
- エンドポイントサービス設定を削除する (p. 56)

インターフェイスエンドポイントの VPC エンドポイントサービス

インターフェイスエンドポイント用のエンドポイントサービスの一般的な作成手順は次のとおりです。

1. VPC でアプリケーションの Network Load Balancer を作成し、これを、サービスを使用可能にするサブネット (アベイラビリティーゾーン) ごとに設定します。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。または、Application Load Balancer を Network Load Balancer のターゲットとして設定し、Application Load Balancer がリクエストをサービスにルーティングするようにできます。詳細については、「Network Load Balancer のユーザーガイド」を参照してください。

   サービスは、リージョン内のすべてのアベイラビリティーゾーンに設定することをお勧めします。
2. VPC エンドポイントのサービス設定を作成し、Network Load Balancer を指定します。

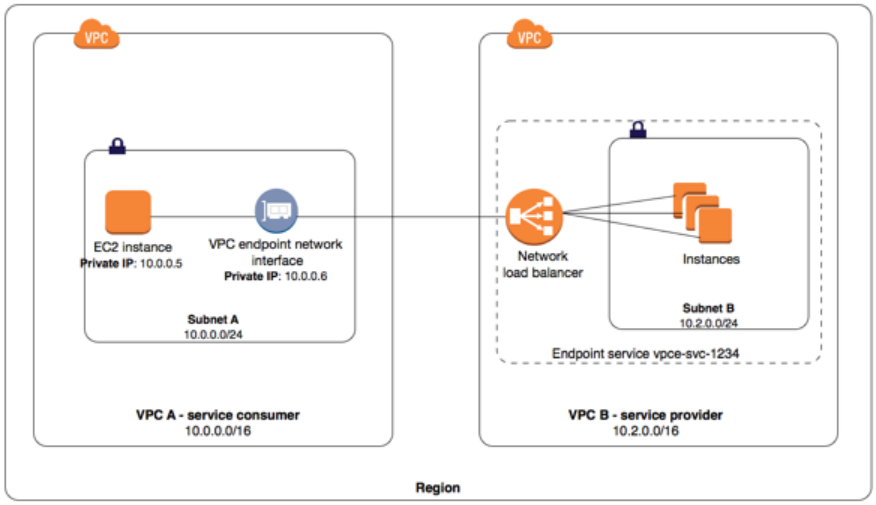
サービスコンシューマーからサービスに接続するための一般的な手順は以下のとおりです。

1. 特定のサービスコンシューマー (AWS アカウント、IAM ユーザー、および IAM ロール) に対して、エンドポイントサービスへの接続を作成するためのアクセス許可を付与します。
2. アクセス権限を付与されたサービスコンシューマーは、サービスへのインターフェイスエンドポイントを (必要に応じて) サービスが設定されている各アベイラビリティーゾーンで作成します。

3. 接続を有効にするには、インターフェイスエンドポイント接続リクエストを承諾します。デフォルトでは、接続リクエストは手動で承諾する必要があります。ただし、接続リクエストが自動的に承諾されるように、エンドポイントサービスの承諾設定を指定できます。

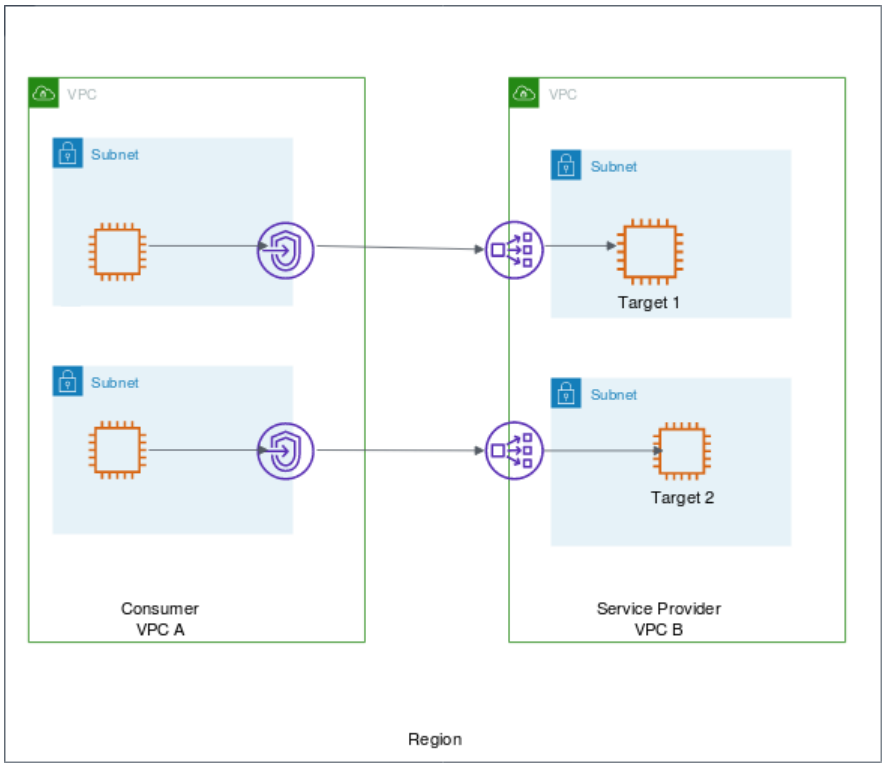
アクセス許可と承諾設定を組み合わせると、サービスにアクセスできるサービスコンシューマー (AWS プリンシパル) を管理するうえで役立ちます。たとえば、信頼している選択されたプリンシパルにアクセス許可を付与して自動的にすべての接続リクエストを承諾するか、プリンシパルのより広範なグループにアクセス許可を付与して、信頼している特定の接続リクエストを手動で承諾できます。

次の図で、VPC B のアカウント所有者はサービスプロバイダーで、サブネット B のインスタンスでサービスを実行しています。VPC B の所有者は、サブネット B のインスタンスをターゲットとして指す Network Load Balancer が関連付けられたサービスエンドポイント (vpce-svc-1234) を使用します。VPC A のサブネット A のインスタンスは、インターフェイスエンドポイントを使用してサブネット B のサービスにアクセスします。



低レイテンシーと耐障害性を確保するため、Network Load Balancer を使用して AWS リージョンの各アベイラビリティーゾーンにターゲットを置くことをお勧めします。ゾーン DNS ホスト名 (p. 14)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ための高可用性を実現するために、クロスゾーン負荷分散を使用できます。クロスゾーン負荷分散を使用すると、ロードバランサーを使用して有効なすべてのアベイラビリティーゾーンの登録済みターゲットにトラフィックを分散できます。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。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アカウントに適用されることがあります。

以下の図では、VPC B の所有者はサービスプロバイダーであり、2 つの異なるアベイラビリティーゾーンにターゲットを置く Network Load Balancer を設定しています。サービスコンシューマー (VPC A) は、自分の VPC で同じ 2 つのアベイラビリティーゾーンにインターフェイスエンドポイントを作成しました。VPC A のインスタンスからサービスへのリクエストには、いずれかのインターフェイスエンドポイントが使用されます。



サービスを設定し、サービスコンシューマーが VPC ピア接続経由でサービスにアクセスできるようにする例については、Amazon VPC ユーザーガイドの例: AWS PrivateLink と VPC ピアリングを使用するサービスを参照してください。

エンドポイントサービスのアベイラビリティーゾーンに関する考慮事項

エンドポイントサービスを作成する場合、サービスはアカウントにマッピングされたアベイラビリティーゾーンに作成され、他のアカウントからは独立したものになります。サービスプロバイダーとコンシューマーが別のアカウントにある場合、アベイラビリティーゾーン ID を使用して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一意に一貫して識別します。例えば、`use1-az1` は、`us-east-1` リージョンの AZ ID で、すべての AWS アカウントで同じ場所にマッピングされます。アベイラビリティーゾーン ID の詳細については、AWS RAM ユーザーガイドのリソースの AZ ID を参照するか、describe-availability-zones を使用してください。

サービスプロバイダーとコンシューマーが異なるアカウントを持ち、複数のアベイラビリティーゾーンを使用する場合に、コンシューマーが VPC エンドポイントサービス情報を表示すると、レスポンスには共通のアベイラビリティーゾーンのみが含まれます。たとえば、サービスプロバイダーアカウントが `us-east-1a` と `us-east-1c` を使用し、コンシューマーが `us-east-1a` と `us-east-1b` を使用する場合、レスポンスには共通のアベイラビリティーゾーン `us-east-1a` にある VPC エンドポイントサービスが含まれます。

エンドポイントサービスの DNS 名

VPC エンドポイントサービスを作成すると、サービスとの通信に使用できるエンドポイント固有の DNS ホスト名が AWS によって生成されます。これらの名前には、VPC エンドポイント ID、アベイラビリティーゾーン名、およびリージョン名が含まれます。例えば、vpce-1234-abcdev-us-east-1.vpce-svc-123345.us-east-1.vpce.amazonaws.com です。デフォルトでは、コンシューマーはその DNS 名でサービスにアクセスし、通常はアプリケーション設定を変更する必要があります。

エンドポイントサービスが AWS サービス用の場合、または AWS Marketplace で利用可能なサービスの場合は、デフォルトの DNS 名があります。その他のサービスの場合、サービスプロバイダはプライベート DNS 名を設定して、ユーザーがアプリケーションを変更せずに既存の DNS 名を使用してサービスにアクセスできるようにします。詳細については、「」を参照してくださいプライベート DNS 名 (p. 61)

サービスプロバイダは、IAM ポリシーステートメントで ec2: VpceServicePrivateDnsName 条件コンテキストキーを使用して、作成できるプライベート DNS 名を制御できます。詳細については、IAM ユーザーガイドの「Amazon EC2 で定義されるアクション」を参照してください。

プライベート DNS 名の要件

サービスプロバイダは、新しいエンドポイントサービスまたは既存のエンドポイントサービスのプライベート DNS 名を指定できます。プライベート DNS 名を使用するには、この機能を有効にしてからプライベート DNS 名を指定します。コンシューマーがプライベート DNS 名を使用できるようにするには、ドメイン/サブドメインの管理権があることを検証する必要があります。ドメインの所有権の検証は、Amazon VPC コンソールまたは API を使用して開始できます。ドメインの所有権の検証が完了すると、コンシューマーはプライベート DNS 名を使用してエンドポイントにアクセスします。

オンプレミスのデータセンターへ接続する

インターフェイスエンドポイントとオンプレミスのデータセンター間の接続には、次のタイプの接続を使用できます。

- AWS Direct Connect
- AWS Site-to-Site VPN

VPC ピア接続を介してサービスへアクセスする

VPC エンドポイントとの VPC ピア接続を使用すると、VPC ピア接続全体でコンシューマーにプライベートアクセスを許可できます。詳細については、Amazon VPC ユーザーガイドの例: AWS PrivateLink と VPC ピアリングを使用するサービスを参照してください。

接続情報のプロキシプロトコルを使用する

Network Load Balancer は、ソース IP アドレスをアプリケーション (サービス) に提供します。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、Network Load Balancer ノードのプライベート IP アドレスです。

サービスコンシューマーの IP アドレスおよび対応するインターフェイスエンドポイント ID が必要な場合は、ロードバランサーでプロキシプロトコルを有効化し、プロキシプロトコルヘッダーからクライアント IP アドレスを取得します。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。

ルールと制限

エンドポイントサービスを使用するには、現在のルールおよび制限に注意する必要があります。

- エンドポイントサービスは、TCP 経由の IPv4 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は、エンドポイント固有の DNS ホスト名を使用して、エンドポイントサービスまたはプライベート DNS 名にアクセスできます。
- エンドポイントサービスが複数の Network Load Balancer に関連付けられている場合、特定のアベイラビリティーゾーンでは、インターフェイスエンドポイントは 1 つのロードバランサーとのみ接続を確立します。

- エンドポイントサービスでは、関連付けられたネットワークロードバランサーは一意の各ターゲット (IP アドレスとポート) に対して 55,000 の同時接続または 1 分あたり約 55,000 の接続をサポートできます。これらの接続数を超えた場合、ポート割り当てエラーが発生する可能性が高くなります。ポート割り当てエラーを修正するには、ターゲットグループにさらに多くのターゲットを追加します。Network Load Balancer のターゲットグループの詳細については、Network Load Balancer のユーザーガイドの「Network Load Balancer のターゲットグループ」および「ターゲットグループへのターゲットの登録」を参照してください。
- アカウントのアベイラビリティーゾーンは、別のアカウントのアベイラビリティーゾーンと同じ場所にマッピングされない可能性があります。たとえば、あるアカウントのアベイラビリティーゾーン `us-east-1a` は別のアカウントのアベイラビリティーゾーン `us-east-1a` と同じ場所にはない可能性があります。詳細については、「リージョンとゾーン」を参照してください。エンドポイントサービスを設定すると、アカウントにマッピングされるようにアベイラビリティーゾーンで設定されます。
- 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のみ使用できます。
- エンドポイントサービスのサービス固有の制限を確認します。
- エンドポイントサービスのセキュリティのベストプラクティスと例を確認します。詳細については、「ポリシーのベストプラクティス」と「the section called “シークレットへのアクセスを制御する” (p. 39)」を参照してください。

Gateway Load Balancer エンドポイントの VPC エンドポイントサービス

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。その後、Gateway Load Balancer を VPC エンドポイントサービスとして設定し、他の AWS プリンシパルが Gateway Load Balancer エンドポイントを介してサービスにアクセスできるようにします。

Gateway Load Balancer エンドポイント用のエンドポイントサービスを作成する一般的な手順は次のとおりです。

1. 仮想アプライアンスの Gateway Load Balancer を作成します。詳細については、「Gateway Load Balancer の開始方法」をご参照ください。

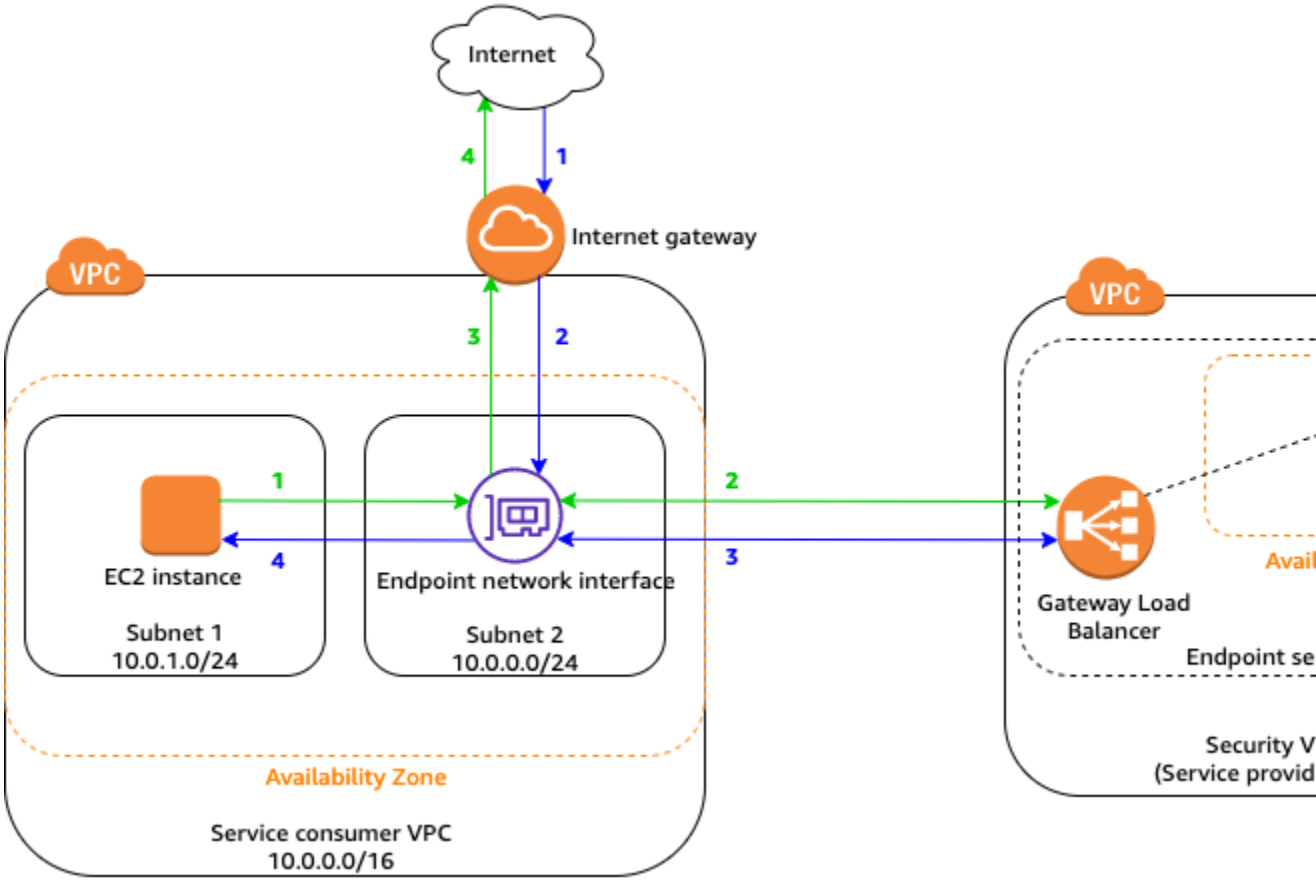
   サービスは、リージョン内のすべてのアベイラビリティーゾーンに設定することをお勧めします。
2. VPC エンドポイントのサービス設定を作成し、Gateway Load Balancer を指定します。

サービスコンシューマーからサービスに接続するための一般的な手順は以下のとおりです。

1. 特定のサービスコンシューマー (AWS アカウント、IAM ユーザー、および IAM ロール) に対して、エンドポイントサービスへの接続を作成するためのアクセス許可を付与します。
2. アクセス許可を付与されたサービスコンシューマーは、サービスへの Gateway Load Balancer エンドポイント (p. 17)を作成します。
3. 接続を有効にするには、エンドポイント接続リクエストを承諾します。デフォルトでは、接続リクエストは手動で承諾する必要があります。ただし、接続リクエストが自動的に承諾されるように、エンドポイントサービスの承諾設定を指定できます。

次の例では、セキュリティ VPC のGateway Load Balancer の背後にセキュリティアプライアンスのフリートが設定されています。エンドポイントサービスは、Gateway Load Balancer 用に設定されています。サービスコンシューマー VPC の所有者は、VPC 内のサブネット 2 に Gateway Load Balancer エンドポイントを作成します (エンドポイントネットワークインターフェイスで表されます)。インターネット

ゲートウェイを経由して VPC に入るすべてのトラフィックは、まずセキュリティ VPC での検査のために Gateway Load Balancer エンドポイントにルーティングされ、その後に送信先サブネットにルーティングされます。同様に、サブネット 1 の EC2 インスタンスから出るすべてのトラフィックは、セキュリティ VPC での検査のために 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にルーティングされます。



このシナリオのルーティング設定の詳細については、Amazon VPC ユーザーガイドの「Gateway Load Balancer エンドポイントへのルーティング」を参照してください。

アベイラビリティーゾーンの考慮事項

エンドポイントサービスを作成する場合、サービスはアカウントにマッピングされたアベイラビリティーゾーンに作成され、他のアカウントからは独立したものになります。サービスプロバイダーとコンシューマーが別のアカウントにある場合、アベイラビリティーゾーン ID を使用して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一意に一貫して識別します。例えば、`use1-az1` は、`us-east-1` リージョンの AZ ID で、すべての AWS アカウントで同じ場所にマッピングされます。アベイラビリティーゾーン ID の詳細については、AWS RAM ユーザーガイドのリソースの AZ ID を参照するか、describe-availability-zones を使用してください。

サービスプロバイダーとコンシューマーが異なるアカウントを持ち、複数のアベイラビリティーゾーンを使用する場合に、コンシューマーが VPC エンドポイントサービス情報を表示すると、レスポンスには共通のアベイラビリティーゾーンのみが含まれます。たとえば、サービスプロバイダーアカウントが `us-east-1a` と `us-east-1c` を使用し、コンシューマーが `us-east-1a` と `us-east-1b` を使用する場合、レスポンスには共通のアベイラビリティーゾーン `us-east-1a` にある VPC エンドポイントサービスが含まれます。

ルールと制限

Gateway Load Balancer エンドポイント用のエンドポイントサービスを使用するには、現在のルールおよび制限に注意してください。

- 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、特定のアベイラビリティーゾーンでは、Gateway Load Balancer エンドポイントは 1 つのロードバランサーとのみ接続を確立します。
- プライベート DNS 名はサポートされていません。
- アカウントのアベイラビリティーゾーンは、別のアカウントのアベイラビリティーゾーンと同じ場所にマッピングされない可能性があります。たとえば、あるアカウントのアベイラビリティーゾーン `us-east-1a` は別のアカウントのアベイラビリティーゾーン `us-east-1a` と同じ場所にはない可能性があります。詳細については、「リージョンとゾーン」を参照してください。エンドポイントサービスを設定すると、アカウントにマッピングされるようにアベイラビリティーゾーンで設定されます。

インターフェイスエンドポイントの VPC エンドポイントサービス設定を作成する

Amazon VPC コンソールまたはコマンドラインを使用して、エンドポイントサービス設定を作成できます。VPC エンドポイントの制限の詳細については、Amazon VPC ユーザーガイドの制限を参照してください。

開始する前に、VPC 内にサービス用の Network Load Balancer が 1 つ以上作成されていることを確認します。詳細については、Network Load Balancer ユーザーガイドの「Network Load Balancer の開始方法」を参照してください。

オプションとして、サービスへのインターフェイスエンドポイント接続リクエストを手動で承諾するように設定で指定することもできます。通知を作成 (p. 53)し、接続リクエストがあった場合はアラートを受信できます。接続を承諾しない場合、サービスコンシューマーはサービスにアクセスできません。

> Note
>
> 承諾設定にかかわらず、サービスコンシューマーでは、サービスへの接続を作成するアクセス許可 (p. 49)も必要です。

エンドポイントサービス設定の作成後に、アクセス権限を追加し、サービスコンシューマーがサービスへのインターフェイスエンドポイントを作成できるようにします。

Console

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、[エンドポイントサービス]、[エンドポイントサービスを作成] の順に選択します。
3. [ロードバランサーのタイプ] で、[ネットワーク] を選択します。
4. [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。
5. [Require acceptance for endpoint] チェックボックスをオンにして、サービスへの接続リクエストを手動で承諾します。それ以外の場合は、エンドポイント接続は自動的に承諾されます。
6. [プライベート DNS 名を有効にする] では、チェックボックスを選択してプライベート DNS 名をサービスに関連付けてから、プライベート DNS 名を入力します。
7. (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。

8. [Create] を選択します。

AWS CLI

エンドポイントサービスを作成するには

create-vpc-endpoint-service-configuration コマンドを使用し、Network Load Balancer の ARN を 1 つ以上指定します。オプションで、サービスへの接続に承諾が必要かどうか、およびサービスがプライベート DNS 名を持つかどうかを指定できます。

```
aws ec2 create-vpc-endpoint-service-configuration --network-load-balancer-arns
 arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/nlb-
vpce/e94221227f1ba532 --acceptance-required --privateDnsName exampleservice.com
```

以下は出力例です。

```
{
    "ServiceConfiguration": {
        "ServiceType": [
            {
                "ServiceType": "Interface"
            }
        ],
        "NetworkLoadBalancerArns": [
            "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/nlb-
vpce/e94221227f1ba532"
        ],
        "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-03d5ebb7d9579a2b3",
        "ServiceState": "Available",
        "ServiceId": "vpce-svc-03d5ebb7d9579a2b3",
        "PrivateDnsName": "exampleService.com",
        "AcceptanceRequired": true,
        "AvailabilityZones": [
            "us-east-1d"
        ],
        "BaseEndpointDnsNames": [
            "vpce-svc-03d5ebb7d9579a2b3.us-east-1.vpce.amazonaws.com"
        ]
    }
}
```

Tools for Windows PowerShell

エンドポイントサービスを作成するには

New-EC2VpcEndpointServiceConfiguration を使用します。

API

エンドポイントサービスを作成するには

CreateVpcEndpointServiceConfiguration を使用します。

Gateway Load Balancer エンドポイントの VPC エンドポイントサービス設定を作成する

Amazon VPC コンソールまたはコマンドラインを使用して、エンドポイントサービス設定を作成できます。開始する前に、VPC 内にサービス用の Gateway Load Balancer が 1 つ以上作成されていることを確認します。詳細については、「Gateway Load Balancer の開始方法」をご参照ください。

オプションとして、サービスへの Gateway Load Balancer エンドポイント接続リクエストを手動で承諾するように設定で指定することもできます。通知を作成 (p. 53)し、接続リクエストがあった場合はアラートを受信できます。接続を承諾しない場合、サービスコンシューマーはサービスにアクセスできません。

エンドポイントサービス設定の作成後に、アクセス許可 (p. 49)を追加し、サービスコンシューマーがサービスへの Gateway Load Balancer エンドポイントを作成できるようにします。

Console

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、[エンドポイントサービス]、[エンドポイントサービスを作成] の順に選択します。
3. [ロードバランサーのタイプ] で、[ゲートウェイ] を選択します。
4. [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。
5. [Require acceptance for endpoint] チェックボックスをオンにして、サービスへの接続リクエストを手動で承諾します。それ以外の場合は、エンドポイント接続は自動的に承諾されます。
6. (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。
7. [Create] を選択します。

AWS CLI

エンドポイントサービスを作成するには

create-vpc-endpoint-service-configuration コマンドを使用し、Gateway Load Balancer の ARN を 1 つ以上指定します。オプションとして、サービスへの接続に承諾を必要とするかどうかを指定できます。

```
aws ec2 create-vpc-endpoint-service-configuration --gateway-load-balancer-arns gateway-load-balancer-arn --no-acceptance-required
```

Tools for Windows PowerShell

エンドポイントサービスを作成するには

New-EC2VpcEndpointServiceConfiguration を使用します。

API

エンドポイントサービスを作成するには

CreateVpcEndpointServiceConfiguration を使用します。

エンドポイントサービスのアクセス権限を追加または削除する

エンドポイントサービス設定の作成後に、どのサービスコンシューマーがサービスへのインターフェイスエンドポイントまたは Gateway Load Balancer エンドポイントを作成できるかを制御できます。サービスコンシューマーは、IAM プリンシパル (IAM ユーザー、IAM ロール、および AWS アカウント) です。プリンシパルのアクセス権限を追加または削除するには、Amazon リソースネーム (ARN) が必要です。

- AWS アカウント (およびアカウントのすべてのプリンシパル) の場合、ARN の形式は `arn:aws:iam::aws-account-id:root` です。
- 特定の IAM ユーザーの場合、ARN の形式は `arn:aws:iam::aws-account-id:user/user-name` です。
- 特定の IAM ロールの場合、ARN の形式は `arn:aws:iam::aws-account-id:role/role-name` です。

> **Note**
>
> アクセス許可を [anyone can access] (誰でもアクセス可能) に設定し、承諾モデルを [accept all requests] (すべてのリクエストを受け入れる) に設定すると、ロードバランサーを公開したことになります。AWS アカウントは簡単に取得できるため、パブリック IP アドレスがない場合でも、ロードバランサーにアクセスできるユーザーについて実質的な制限はありません。

Console

エンドポイントサービスの許可を追加または削除するには

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、[アクション]、[プリンシパルを許可] の順に選択します。
4. アクセス権限を追加する先のプリンシパルの ARN を指定します。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。プリンシパルを削除するには、エントリの横にある [削除] を選択します。

   すべてのプリンシパルにアクセス権限を追加するには、`*` を指定します。これにより、すべての AWS アカウントのすべてのプリンシパルで、エンドポイントサービスへのエンドポイントを作成できます。
5. [プリンシパルを許可] を選択します。

AWS CLI

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 コマンドを使用します。プリンシパルに 1 つ以上の ARN を追加するための `--add-allowed-principals` パラメータを指定します。

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-svc-03d5ebb7d9579a2b3
 --add-allowed-principals '["arn:aws:iam::123456789012:root"]'
```

エンドポイントサービスに追加した許可を表示するには

describe-vpc-endpoint-service-permissions コマンドを使用します。

```
aws ec2 describe-vpc-endpoint-service-permissions --service-id vpce-
svc-03d5ebb7d9579a2b3
```

以下は出力例です。

```
{
    "AllowedPrincipals": [
        {
            "PrincipalType": "Account",
            "Principal": "arn:aws:iam::123456789012:root"
        }
    ]
```

```
}
```

エンドポイントサービスの許可を削除するには

modify-vpc-endpoint-service-permissions コマンドを使用します。プリンシパルの 1 つ以上の ARN を削除するための `--remove-allowed-principals` パラメータを指定します。

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-svc-03d5ebb7d9579a2b3
 --remove-allowed-principals '["arn:aws:iam::123456789012:root"]'
```

Tools for Windows PowerShell

エンドポイントサービスの許可を追加または削除するには

Edit-EC2EndpointServicePermission を使用します。

API

エンドポイントサービスの許可を追加または削除するには

ModifyVpcEndpointServicePermissions を使用します。

エンドポイントサービス設定を変更

エンドポイントサービス設定を変更するには、エンドポイントサービスに関連付けられたロードバランサーを変更したり、エンドポイントサービスへの接続リクエストに承諾を必要とするかどうかを変更したりします。

エンドポイントサービスにエンドポイントがアタッチされている場合、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。

Console

エンドポイントサービスのロードバランサーを変更するには

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、[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、[アクション]、[ロードバランサーの関連付けまたは関連付けの解除] の順に選択します。
4. 必要に応じてロードバランサーを選択または選択解除し、[変更を保存] を選択します。

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、[アクション]、[エンドポイント承諾設定を変更] の順に選択します。
4. [承諾が必要] を選択または選択解除してから、[変更を保存] を選択します。

AWS CLI

エンドポイントサービスのロードバランサーを変更するには

modify-vpc-endpoint-service-configuration を使用します。次の例では、`--remove-network-load-balancer-arn` パラメータを使用して Network Load Balancer を削除します。

```
aws ec2 modify-vpc-endpoint-service-configuration --service-
id vpce-svc-09222513e6e77dc86 --remove-network-load-balancer-arn
 arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/nlb-
vpce/e94221227f1ba532
```

承諾が必要かどうかを変更するには

modify-vpc-endpoint-service-configuration コマンドを使用し、`--acceptance-required` または `--no-acceptance-required` を指定します。

```
aws ec2 modify-vpc-endpoint-service-configuration --service-id vpce-
svc-09222513e6e77dc86 --no-acceptance-required
```

Tools for Windows PowerShell

エンドポイントサービス設定を変更するには

Edit-EC2VpcEndpointServiceConfiguration を使用します。

API

エンドポイントサービス設定を変更するには

ModifyVpcEndpointServiceConfiguration を使用します。

エンドポイントの接続リクエストを承諾または拒否する

エンドポイントサービスの作成後に、アクセス権限を追加したサービスコンシューマーは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または Gateway Load Balancer エンドポイントを作成できます。詳細については、「インターフェイス VPC エンドポイント (AWS PrivateLink) (p. 3)」および「Gateway Load Balancer エンドポイント (AWS PrivateLink) (p. 17)」を参照してください。

接続リクエストに承諾を要することを指定した場合は、エンドポイントサービスへのエンドポイントの接続リクエストを手動で承諾または拒否する必要があります。エンドポイントを承諾すると、そのエンドポイントは `available` になります。検証ステータスの変更が完了し、`available` 状態になるまでに時間がかかる場合があることにご留意ください。

エンドポイントの接続は、それが `available` 状態になった後で、拒否することができます。

Console

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. [エンドポイント接続] タブで、エンドポイントを選択します。接続リクエストを承諾するには、[アクション]、[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。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。

AWS CLI

承諾が保留中のエンドポイント接続を表示するには

describe-vpc-endpoint-connect コマンドを使用し、pendingAcceptance 状態でフィルタリングします。

```
aws ec2 describe-vpc-endpoint-connections --filters Name=vpc-endpoint-
state,Values=pendingAcceptance
```

以下は出力例です。

```
{
    "VpcEndpointConnections": [
        {
            "VpcEndpointId": "vpce-0c1308d7312217abc",
            "ServiceId": "vpce-svc-03d5ebb7d9579a2b3",
            "CreationTimestamp": "2017-11-30T10:00:24.350Z",
            "VpcEndpointState": "pendingAcceptance",
            "VpcEndpointOwner": "123456789012"
        }
    ]
}
```

エンドポイント接続リクエストを承諾するには

accept-vpc-endpoint-connections コマンドを使用し、エンドポイント ID とエンドポイントサービス ID を指定します。

```
aws ec2 accept-vpc-endpoint-connections --service-id vpce-svc-03d5ebb7d9579a2b3 --vpc-
endpoint-ids vpce-0c1308d7312217abc
```

エンドポイント接続リクエストを拒否するには

reject-vpc-endpoint-connections コマンドを使用します。

```
aws ec2 reject-vpc-endpoint-connections --service-id vpce-svc-03d5ebb7d9579a2b3 --vpc-
endpoint-ids vpce-0c1308d7312217abc
```

Tools for Windows PowerShell

接続リクエストを承諾または拒否するには

Confirm-EC2EndpointConnection および Deny-EC2EndpointConnection を使用します。

API

接続リクエストを承諾または拒否するには

AcceptVpcEndpointConnections および RejectVpcEndpointConnections を使用します。

エンドポイントサービスの通知を作成および管理する

エンドポイントサービスにアタッチしたエンドポイントで特定のイベントが発生した場合に、アラートを受信するための通知を作成できます。たとえば、エンドポイントサービスに対するエンドポイント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。通知を作成するには、Amazon SNS トピックを通知に関連付ける必要があります。この SNS トピックへの受信登録を行い、エンドポイントイベント

の発生時に E メール通知を受信できます。詳細については、Amazon Simple Notification Service デベロッパーガイドを参照してください。

通知に使用する Amazon SNS トピックには、Amazon VPC エンドポイントサービスがユーザーに代わって通知を発行することを許可するトピックポリシーが必要です。トピックポリシーには、次のステートメントを必ず含めます。詳細については、Amazon Simple Notification Service デベロッパーガイドの「Amazon SNS トピックへのアクセスの管理」を参照してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account:topic-name"
    }
  ]
}
```

Console

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てから、[通知] タブを選択します。
4. [通知を作成] を選択します。
5. [通知 ARN] で、通知に関連付ける SNS トピックの ARN を選択します。
6. [イベント] で、通知を受け取る対象のエンドポイントイベントを選択します。
7. [通知を作成] を選択します。

通知を作成した後、その設定を変更できます。

エンドポイントサービスの通知を変更するには

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てから、[通知] タブを選択します。
4. 通知を選択してから、[アクション]、[通知を変更] の順に選択します。
5. 必要に応じて SNS トピックまたはエンドポイントイベントを変更します。
6. [Save changes] (変更を保存) をクリックします。

通知が不要になった場合は、それを削除できます。

通知を削除するには

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てから、[通知] タブを選択します。
4. 通知を選択してから、[アクション]、[通知を削除] 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 CLI

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 コマンドを使用します。SNS トピックの ARN、通知されるイベント、エンドポイントサービスの ID を指定します。

```
aws ec2 create-vpc-endpoint-connection-notification --connection-notification-
arn arn:aws:sns:us-east-2:123456789012:VpceNotification --connection-events Connect
 Accept Delete Reject --service-id vpce-svc-1237881c0d25a3abc
```

以下は出力例です。

```
{
    "ConnectionNotification": {
        "ConnectionNotificationState": "Enabled",
        "ConnectionNotificationType": "Topic",
        "ServiceId": "vpce-svc-1237881c0d25a3abc",
        "ConnectionEvents": [
            "Reject",
            "Accept",
            "Delete",
            "Connect"
        ],
        "ConnectionNotificationId": "vpce-nfn-008776de7e03f5abc",
        "ConnectionNotificationArn": "arn:aws:sns:us-
east-2:123456789012:VpceNotification"
    }
}
```

通知を表示するには

describe-vpc-endpoint-connection-notifications コマンドを使用します。

```
aws ec2 describe-vpc-endpoint-connection-notifications
```

通知の SNS トピックまたはエンドポイントイベントを変更するには

modify-vpc-endpoint-connection-notification コマンドを使用します。

```
aws ec2 modify-vpc-endpoint-connection-notification --connection-notification-id vpce-
nfn-008776de7e03f5abc --connection-events Accept Reject --connection-notification-
arn arn:aws:sns:us-east-2:123456789012:mytopic
```

通知を削除するには

delete-vpc-endpoint-connection-notifications コマンドを使用します。

```
aws ec2 delete-vpc-endpoint-connection-notifications --connection-notification-
ids vpce-nfn-008776de7e03f5abc
```

Tools for Windows PowerShell

通知を作成および管理するには

以下を使用します。

- New-EC2VpcEndpointConnectionNotification
- Get-EC2EndpointConnectionNotification
- Edit-EC2VpcEndpointConnectionNotification
- Remove-EC2EndpointConnectionNotification

API

通知を作成および管理するには

以下を使用します。

- CreateVpcEndpointConnectionNotification
- DescribeVpcEndpointConnectionNotifications
- ModifyVpcEndpointConnectionNotification
- DeleteVpcEndpointConnectionNotifications

VPC エンドポイントサービスタグを追加または削除する

タグは VPC エンドポイントサービスを識別する方法を提供します。タグを追加または削除できます。

Console

VPC エンドポイントサービスタグを追加または削除するには

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. VPC エンドポイントサービスを選択し、[アクション]、[タグを管理] の順に選択します。
4. タグを追加または削除します。

   [タグを追加] [新しいタグを追加] を選択し、タグのキーと値を入力します。

   [タグを削除] タグのキーと値の右側にある [削除] を選択します。

AWS CLI

create-tags および delete-tags を使用します。

API

CreateTags および DeleteTags を使用します。

エンドポイントサービス設定を削除する

エンドポイントサービス設定を削除できます。設定を削除しても、VPC でホストされているアプリケーションや関連付けられたロードバランサーは削除されません。

エンドポイントサービス設定を削除する前に、サービスにアタッチされている `available` または `pending-acceptance` の VPC エンドポイントを拒否する必要があります。詳細については、「エンドポイントの接続リクエストを承諾または拒否する (p. 52)」を参照してください。

Console

エンドポイントサービス設定を削除するには

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。

AWS CLI

エンドポイントサービス設定を削除するには

delete-vpc-endpoint-service-configurations コマンドを使用します。サービスの ID を指定します。

```
aws ec2 delete-vpc-endpoint-service-configurations --service-ids vpce-
svc-03d5ebb7d9579a2b3
```

Tools for Windows PowerShell

エンドポイントサービス設定を削除するには

Remove-EC2EndpointServiceConfiguration を使用します。

API

エンドポイントサービス設定を削除するには

DeleteVpcEndpointServiceConfigurations を使用します。

VPC エンドポイントおよび VPC エンドポイントサービスの Identity and Access Management

IAM を使用して、VPC エンドポイントおよび VPC エンドポイントサービスへのアクセスを管理します。

VPC エンドポイントの使用を制御する

デフォルトでは、IAM 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、削除するアクセス権限をユーザーに付与する IAM ユーザー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 “シークレットへのアクセスを制御する” (p. 39)」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:accountId:vpc/*",
                "arn:aws:ec2:region:accountId:security-group/*",
                "arn:aws:ec2:region:accountId:subnet/*",
                "arn:aws:ec2:region:accountId:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:accountId: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:accountId: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:accountId:vpc/*",
                "arn:aws:ec2:region:accountId:security-group/*",
                "arn:aws:ec2:region:accountId:subnet/*",
                "arn:aws:ec2:region:accountId:route-table/*"
            ]
        },
        {
```

```
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:accountId:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.region.s3"
                    ]
                }
            }
        }
    ]
}
```

エンドポイントサービスのプライベート DNS 名

VPC エンドポイントサービスを作成すると、サービスとの通信に使用できるエンドポイント固有の DNS ホスト名が生成されます。これらの名前には、VPC エンドポイント ID、アベイラビリティーゾーン名、および「vpce-1234-abcdev-us-east-1.vpce-svc-123345.us-east-1.vpce.amazonaws.com」などのリージョン名が含まれます。デフォルトでは、コンシューマーはその DNS 名でサービスにアクセスし、通常はアプリケーション設定を変更する必要があります。

エンドポイントサービスが AWS サービス用の場合、または AWS Marketplace で利用可能なサービスの場合は、デフォルトの DNS 名があります。その他のサービスの場合、サービスプロバイダはプライベート DNS 名を設定して、ユーザーがアプリケーションを変更せずに既存の DNS 名を使用してサービスにアクセスできるようにします。詳細については、「VPC エンドポイントサービス (p. 41)」を参照してください。

サービスプロバイダは、新しいエンドポイントサービスまたは既存のエンドポイントサービスのプライベート DNS 名を指定できます。プライベート DNS 名を使用するには、この機能を有効にしてからプライベート DNS 名を指定します。コンシューマーがプライベート DNS 名を使用できるようにするには、ドメイン/サブドメインの管理権があることを検証する必要があります。ドメインの所有権の検証は、Amazon VPC コンソールまたは API を使用して開始できます。ドメインの所有権の検証が完了すると、コンシューマーはプライベート DNS 名を使用してエンドポイントにアクセスします。

ドメインを検証するには、パブリックホスト名、またはパブリック DNS プロバイダーが必要です。

プライベート DNS 名は、Gateway Load Balancer エンドポイント用に作成するエンドポイントサービスではサポートされません。

大まかな手順は次のとおりです。

1. プライベート DNS 名を追加します。詳細については、「the section called “インターフェイスエンドポイントの VPC エンドポイントサービス設定を作成する” (p. 47)」または「the section called “既存の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” (p. 64)」を参照してください。
2. DNS サーバーレコードに必要な [Domain verification value (ドメイン検証値)]と [Domain verification name (ドメイン検証名)] をメモします。詳細については、「the section called “エンドポイントサービスのプライベート DNS 名設定を表示する” (p. 64)」を参照してください。
3. DNS サーバーにレコードを追加します。詳細については、「the section called “VPC エンドポイントサービスのプライベート DNS 名の検証” (p. 62)」を参照してください。
4. プライベート DNS 名を検証します。詳細については、「the section called “エンドポイントサービスのプライベート DNS 名ドメインの検証を手動で開始する” (p. 65)」を参照してください。

Amazon VPC コンソールまたは Amazon VPC API を使用して、検証プロセスを管理できます。

- the section called “VPC エンドポイントサービスのプライベート DNS 名の検証” (p. 62)
- the section called “既存の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” (p. 64)
- the section called “エンドポイントサービスのプライベート DNS 名を削除する” (p. 66)
- the section called “エンドポイントサービスのプライベート DNS 名設定を表示する” (p. 64)
- Amazon VPC プライベート DNS 名のドメイン検証 TXT レコード (p. 66)

ドメイン名の検証に関する考慮事項

ドメインの所有権の検証に関する次の重要な点に注意してください。

- コンシューマーは、検証ステータスが [verified] である場合にのみ、プライベート DNS 名を使用してエンドポイントサービスにアクセスできます。
- 検証ステータスが [verified] から [pendingVerification] または [failed] に変更された場合、既存のコンシューマー接続は残りますが、新しい接続リクエストはすべて拒否されます。

  Important

  [検証済] 状態ではなくなったエンドポイントサービスへの接続を懸念するサービスプロバイダーに対しては、DescribeVpcEndpoints を使用して検証状態を定期的に確認することをお勧めします。この確認は、1 日に 1 回以上実行することをお勧めします。
- 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。
- 新しいエンドポイントサービスまたは既存のエンドポイントサービスのプライベート DNS 名を指定できます。
- パブリックドメインネームサーバーのみを使用できます。
- ドメイン名には、「*.myexampleservice.com」などのワイルドカードを使用できます。
- エンドポイントサービスごとにドメインの所有権の検証を個別に実行する必要があります。
- 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。RFC 1034 で規定されているように、各 DNS ラベルには最大で 63 文字を指定することができ、ドメイン名全体の合計文字数は 255 を超えることはできません。

  追加のサブドメインを追加する場合は、サブドメインまたはドメインを検証する必要があります。たとえば、a.example.com があり、example.com を検証したとします。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。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。
- ドメイン名は小文字にする必要があります。

VPC エンドポイントサービスのプライベート DNS 名の検証

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システム (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。各 TXT レコードは名前と値で構成されます。

ドメインの所有権の検証を開始すると、TXT レコードで使用する名前と値が割り当てられます。たとえば、ドメインが myexampleservice.com の場合、生成する TXT レコードの設定は次のようになります。

エンドポイントプライベート DNS 名の TXT レコード

ドメインの検証名	タイプ	ドメインの検証値
_vpce:aksldja21i1	TXT	vpce:asjdakjshd78126eu21

指定した [Domain verivication name (ドメイン検証名)] と [Domain verification value (ドメイン検証値)] を使用して、TXT レコードをドメイン の DNS サーバーに追加します。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。

DNS プロバイダが 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、[Domain verification name (ドメイン検証名)] から _aksldja21i1 を省略できます。この場合、上記の例では、TXT レコード名は _aksldja21i1.myexampleservice.com ではなく、myexampleservice.com になります。

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。このセクションでは、Route 53 に TXT レコードを追加する手順と、他の DNS プロバイダー向けの一般的な手順を示します。

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. [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. [Details (詳細)] タブで、[Domain verification value (ドメイン検証値)] と [Domain verification name (ドメイン検証名)] の横に表示される値をメモします。
5. 検証対象のドメインが Route 53 の DNS サービスを使用しており、Route 53 用の同じアカウントで AWS Management Console にサインインしている場合は、Amazon VPC コンソール内からすぐに DNS サーバーを更新できます。

   別の DNS プロバイダーを使用する場合、DNS レコードを更新する手順は、使用する DNS またはウェブホスティングプロバイダーによって異なります。次のテーブルでは、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を示しています。このリストにすべてが網羅されているわけではなく、このリストに含まれているからといって、他社の製品やサービスを支援または推奨するものではありません。お使いのプロバイダがこの表にない場合でも、エンドポイントでそのドメインを使用できる可能性があります。

DNS/ホスティングプロバイダー	ドキュメントのリンク
GoDaddy	Add a TXT record (外部リンク)
Dreamhost	カスタム DNS レコードを追加する方法 (外部リンク)
Cloudflare	Managing DNS records in CloudFlare (外部リンク)
HostGator	HostGator/eNom で DNS レコードを管理する (外部リンク)
Namecheap	ドメインの TXT/SPF/DKIM/DMARC レコードを追加する方法 (外部リンク)
Names.co.uk	ドメイン DNS 設定の変更 (外部リンク)
Wix	Wix アカウントの TXT レコードの追加または更新 (外部リンク)

   検証が完了すると、Amazon VPC コンソールのドメインのステータスが [保留中] から [検証済] に変わります。
6. これで、VPC エンドポイントサービスにプライベートドメイン名を使用できるようになりました。

DNS 設定が正しく更新されない場合、ドメインのステータスは [Details (詳細)] タブに [failed] と表示されます。この場合は、「the section called “ドメインの検証に関する一般的な問題のトラブルシューティン

グ" (p. 68)」のトラブルシューティングに関するページにあるステップを完了します。TXT レコードが正しく作成されたことを検証したら、操作をやり直します。

既存の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

新規または既存のエンドポイントサービスに対してエンドポイントサービスのプライベート DNS 名を変更できます。

名前を更新したら、DNS サーバー上のドメインのエントリを更新します。DNS サーバーを自動的にポーリングして、レコードがサーバーに存在することを検証します。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。詳細については、「the section called "プライベート DNS 名のドメイン検証 TXT レコード" (p. 66)」および「the section called "VPC エンドポイントサービスのプライベート DNS 名の検証" (p. 62)」を参照してください。

Console

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、[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。
4. [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。
5. [Save changes] (変更を保存) をクリックします。

AWS CLI

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 を使用します。

API

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

ModifyVpcEndpointServiceConfiguration を使用します。

エンドポイントサービスのプライベート DNS 名設定を表示する

エンドポイントサービスに対してエンドポイントサービスプライベート DNS 名を表示できます。

Console

エンドポイントサービスのプライベート DNS 名設定を表示するには

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、エンドポイントサービスを選択します。
3. [Details (詳細)] タブには、プライベート DNS ドメインの所有権チェックに関する次の情報が表示されます。
   - Domain verification status (ドメイン検証ステータス): 検証ステータス。
   - Domain verification type (ドメイン検証タイプ): 検証タイプ。
   - Domain verification value (ドメイン検証値): DNS 値。
   - Domain verification name (ドメイン検証名): レコードサブドメインの名前。

AWS CLI

エンドポイントサービスのプライベート DNS 名設定を表示するには

describe-vpc-endpoint-service-configurations を使用します。

API

エンドポイントサービスのプライベート DNS 名設定を表示するには

DescribeVpcEndpointServiceConfigurations を使用します。

エンドポイントサービスのプライベート DNS 名ドメインの検証を手動で開始する

サービスプロバイダは、コンシューマーがプライベート DNS 名を使用する前に、プライベート DNS 名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。

Console

プライベート DNS 名ドメインの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、[アクション]、[プライベート DNS 名のドメインの所有権を検証] の順に選択します。
4. 確認を求められたら、「**`verify`**」と入力し、[検証] を選択します。

   DNS 設定が正しく更新されていない場合、ドメインの検証ステータスは「失敗」になります。この場合は、「the section called "ドメインの検証に関する一般的な問題のトラブルシューティング" (p. 68)」のトラブルシューティングに関するページにあるステップを完了します。

AWS CLI

プライベート DNS 名ドメインの検証プロセスを開始するには

start-vpc-endpoint-service-private-dns-verification を使用します。

API

プライベート DNS 名ドメインの検証プロセスを開始するには

StartVpcEndpointServicePrivateDnsVerification を使用します。

エンドポイントサービスのプライベート DNS 名を削除する

エンドポイントサービスのプライベート DNS 名は、サービスへの接続がなくなった場合にのみ削除できます。

Console

エンドポイントサービスのプライベート DNS 名を削除するには

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、[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。
4. [プライベート DNS 名をサービスに関連付ける] をクリアします。
5. [Save changes] (変更を保存) をクリックします。

AWS CLI

エンドポイントサービスのプライベート DNS 名を削除するには

modify-vpc-endpoint-service-configuration を使用します。

API

エンドポイントサービスのプライベート DNS 名を削除するには

ModifyVpcEndpointServiceConfiguration を使用します。

Amazon VPC プライベート DNS 名のドメイン検証 TXT レコード

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システム (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。各 TXT レコードは名前と値で構成されます。

Amazon VPC コンソールまたは API を使用してドメインの所有権の検証を開始すると、TXT レコードで使用する名前と値が割り当てられます。たとえば、ドメインが myexampleservice.com である場合、Amazon VPC で生成される TXT レコード設定は次のようになります。

エンドポイントプライベート DNS 名の TXT レコード

ドメインの検証名	タイプ	ドメインの検証値
_vpce:aksldja21i1.myexampleservice.com	TXT	vpce:asjdakjshd78126eu21

指定した [Domain verivication name (ドメイン検証名)] と [Domain verification value (ドメイン検証値)] を使用して、TXT レコードをドメイン の DNS サーバーに追加します。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、Amazon VPC ドメインの所有権の検証は完了です。

DNS プロバイダが 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、[Domain verification name (ドメイン検証名)] にドメイン名を使用できます。この場合、前の例では、TXT レコード名は myexampleservice.com になります。

ドメインの所有権の検証の設定に関するトラブルシューティング情報と確認手順については、「プライベート DNS ドメインの検証に関する一般的な問題のトラブルシューティング (p. 68)」を参照してください。

Amazon Route 53

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。このセクションでは、Route 53 に TXT レコードを追加する手順と、他の DNS プロバイダー向けの一般的な手順を示します。

TXT レコードを Route 53 マネージドドメインの DNS レコードに追加するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. [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. [Details (詳細)] タブで、[Domain verification value (ドメイン検証値)] と [Domain verification name (ドメイン検証名)] の横に表示される値をメモします。
5. Amazon Route 53 コンソールで、ホストゾーンのレコードを作成します。レコードの作成方法の詳細については、Amazon Route 53 デベロッパーガイドの「Amazon Route 53 コンソールを使用したレコードの作成」を参照してください。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 (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。
   - [値/トラフィックのルーティング先] に、Amazon VPC コンソールからの [ドメイン検証値] を入力します。
6. Amazon VPC コンソールの [エンドポイントサービス] ページの [詳細] タブで、エンドポイントの [ドメイン検証ステータス] 列の値を確認します。ステータスが [pending verification (検証の保留中)] である場合は、[refresh (更新)] を選択します。ステータス列の値が [verified (検証済み)] になるまで、このプロセスを繰り返します。検証プロセスは手動で開始できます。詳細については、「the section called “エンドポイントサービスのプライベート DNS 名ドメインの検証を手動で開始する” (p. 65)」を参照してください。

Generic procedures for other DNS providers

DNS 設定に TXT レコードを追加する手順は、プロバイダーによって異なります。詳しい手順については、DNS プロバイダーのドキュメントを参照してください。このセクションでは、ドメインの DNS 設定に TXT レコードを追加する場合の基本的なステップの概要を提供します。

ドメインの DNS サーバーに TXT レコードを追加するには (一般的な手順)

1. DNS プロバイダーのウェブサイトに移動します。ドメインで利用している DNS プロバイダーがわからない場合は、無料の Whois サービスを使用して検索できます。
2. プロバイダーのウェブサイトでアカウントにサインインします。
3. ドメインの DNS レコードを更新するためのページを見つけます。通常、このページの名前は「DNS Records」、「DNS Zone File」、「Advanced DNS」などになっています。不確かな場合は、プロバイダのドキュメントを参照してください。
4. で名前と値が指定された TXT レコードを追加しますAWS

   Important

   DNS プロバイダーによっては、DNS レコードの末尾にドメイン名が自動的に付加される場合があります。既にドメイン名が含まれているレコード (_pmBGN/7Mjnf.example.com など) を追加すると、ドメイン名が重複したレコード

(_pmBGN/7Mjnfexample.com.example.com など) になる場合があります。ドメイン名の重複を避けるには、DNS レコードのドメイン名の末尾にピリオドを追加します。こうすることで、DNS プロバイダにレコード名が完全修飾されている (つまり、ドメイン名に対して相対的でなくなる) ことを示し、DNS プロバイダによってドメイン名が追加されないようにします。

5. 変更を保存します。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。

プライベート DNS ドメインの検証に関する一般的な問題のトラブルシューティング

Amazon VPC でエンドポイントサービスのプライベート DNS ドメイン名を検証するには、Amazon VPC コンソールまたは API を使用してプロセスを開始します。このセクションには、検証プロセスに関する問題の解決に役立つ情報が含まれています。

ドメインの検証に関する一般的な問題

ドメインを検証しようとしたときに問題が発生した場合は、以下の考えられる原因と解決策を確認してください。

- 所有していないドメインを検証しようとした場合。所有していないドメインを検証することはできません。
- TXT レコード名でのアンダースコアの使用が DNS プロバイダによって許可されていない場合。一部の DNS プロバイダは、ドメインの DNS レコード名にアンダースコア文字を含めることを許可していません。これがお客様のプロバイダに当てはまる場合は、TXT レコード名から _amazovpc を削除できます。
- DNS プロバイダが TXT レコードの末尾にドメイン名を追加した場合。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。たとえば、属性名が _amazonvpc.example.com のレコードを作成した場合、プロバイダはドメイン名を追加して、_amazonvpc.example.com.example.com とする場合があります。ドメイン名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。この手順では、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 プロバイダが DNS レコードの値を変更した場合。一部のプロバイダは、小文字のみを使用するように DNS レコードの値を自動的に変更します。ドメインが検証されるのは、ドメインの所有権の検証プロセスを開始したときに入力した値と属性値が正確に一致する検証レコードが検出された場合のみです。ドメインの DNS プロバイダーが小文字のみを使用するように TXT レコード値を変更した場合、追加のサポートを DNS プロバイダーまでお問い合わせください。
- 同じドメインを複数回検証する必要がある場合。異なるリージョンで送信する場合や、同じドメインを使用して複数の AWS アカウントから送信している場合は、ドメインを複数回検証する必要が生じることがあります。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ない場合、2 つのドメインを確認できることがあります。DNS プロバイダーによって許可される場合、同じ TXT レコードに複数の属性値を割り当てることができます。たとえば、DNS が Amazon Route 53 によって管理されている場合、以下の手順を実行して、同じ TXT レコードに対して複数の値をセットアップできます。

  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)] ボックスで、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。たとえば、「_asnbcdasd」で検証してから、「asnbcdasd」で検証します。このソリューションの欠点は、同じドメインを 2 回しか確認できないことです。

ドメインの検証に関する設定を確認する方法

次の手順を使用すると、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。この手順では、Windows および Linux で使用できる nslookup ツールを使用します。Linux では、dig を使用することもできます。

これらの手順に示すコマンドは、Windows 7 で実行されています。使用されているサンプルのドメインは、example.com です。

この手順では、最初にドメインにサービスを提供する DNS サーバーを見つけます。次に、これらのサーバーに対して、TXT レコードを表示するためのクエリを実行します。ドメインにサービスを提供する DNS サーバーに対してクエリを実行する理由は、これらのサーバーには他の DNS サーバーに伝達されるまでに時間のかかるドメインの最新情報が格納されているためです。

ドメイン所有権の検証 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. 次のステップを実行して、ドメインのネームサーバーを見つけます。

   a. コマンドラインに移動します。Windows 7 でコマンドラインに移動するには、[スタート] を選択し、「cmd」と入力します。Linux ベースのオペレーティングシステムでは、ターミナルウィンドウを開きます。

   b. コマンドプロンプトで、次のように入力します。ここで、<domain> はドメインを示します。

   ```
   nslookup -type=NS <domain>
   ```

   たとえば、ドメインが example.com の場合、コマンドは以下のようになります。

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

   コマンドの出力に、ドメインにサービスを提供しているネームサーバーのリストが表示されます。次のステップでは、これらのサーバーの 1 つに対してクエリを実行します。

2. 次のステップを実行して、TXT レコードが適切に発行されていることを確認します。

   a. コマンドプロンプトで、次のように入力します。ここで、<domain> はドメインを示し、<name server> はステップ 1 で見つけたネームサーバーの 1 つを示します。

   ```
   nslookup -type=TXT  _aksldja21i1.<domain> <name server>
   ```

   _aksldja21i1.example.com の例で、ステップ 1 で見つけたネームサーバーが ns1.name-server.net の場合は、次のように入力します。

   ```
   nslookup -type=TXT  _aksldja21i1.example.com ns1.name-server.net
   ```

   b. コマンドの出力の `text =` に続く文字列が、Amazon VPC コンソールのアイデンティティリストでドメインを選択すると表示される TXT 値と一致することを確認します。

   この例では、_aksldja21i1.example.com の下で値が `asjdakjshd78126eu21` の TXT レコードを探します。レコードが正しく発行されている場合、次のようなコマンド出力が得られます。

   ```
   _aksldja21i1.example.com text = "asjdakjshd78126eu21"
   ```

AWS PrivateLink と統合できる AWS のサービス

次のサービスが AWS PrivateLink と統合されています。インターフェイスエンドポイント (p. 3)を作成して、これらのサービスに接続できます。

サービスが AWS PrivateLink と統合されているものの、VPC エンドポイントポリシーをサポートしていない場合、[VPC endpoint policies] (VPC エンドポイントポリシー) 列に [No] (いいえ) と表示されます。VPC エンドポイントポリシーをサポートするサービスのドキュメントを参照するには、[はい] リンクを選択します。

AWS のサービス	VPC エンドポイントポリシー
Amazon API Gateway	はい
Amazon AppStream 2.0	いいえ
AWS App Mesh	いいえ
Application Auto Scaling	はい
Amazon Athena	はい
AWS Audit Manager	はい
Amazon Aurora	はい
AWS Auto Scaling	はい
Amazon Braket	はい
AWS Certificate Manager Private Certificate Authority	はい
Amazon Cloud Directory	はい
AWS CloudFormation	いいえ
AWS CloudHSM	はい
AWS CloudTrail	いいえ
Amazon CloudWatch	はい
Amazon CloudWatch Events	はい
Amazon CloudWatch Logs	はい
AWS CodeArtifact	はい
AWS CodeBuild	はい

AWS のサービス	VPC エンドポイントポリシー
AWS CodeCommit	はい
AWS CodeDeploy	はい
Amazon CodeGuru Profiler	いいえ
Amazon CodeGuru Reviewer	いいえ
AWS CodePipeline	いいえ
AWS CodeStar connections	はい
Amazon Comprehend	はい
Amazon Comprehend Medical	はい
AWS Config	はい
Amazon Connect Customer Profiles	はい
AWS Database Migration Service	はい
AWS Data Exchange	はい
AWS DataSync	いいえ
AWS Device Farm	いいえ
Amazon DevOps Guru	はい
Amazon EBS ダイレクト API	いいえ
Amazon EC2	はい
EC2 Image Builder	はい
Amazon EC2 Auto Scaling	はい
AWS Elastic Beanstalk	はい
Amazon Elastic File System	はい
Elastic Load Balancing	はい
Amazon Elastic Container Registry	はい
Amazon Elastic Container Service	はい
Amazon EMR	はい
Amazon EventBridge	はい

AWS のサービス	VPC エンドポイントポリシー
AWS Fault Injection Simulator	✓ はい
Amazon FinSpace	✓ はい
Amazon Fraud Detector	✓ はい
AWS Glue	✓ はい
AWS Identity and Access Management Access Analyzer	✓ はい
Amazon HealthLake	✓ はい
AWS IoT Core	✗ いいえ
AWS IoT Core for LoRaWAN	✗ いいえ
AWS IoT Greengrass	✓ はい
AWS IoT SiteWise	✗ いいえ
Amazon Kendra	✓ はい
AWS Key Management Service	✓ はい
Amazon Keyspaces (Apache Cassandra 向け)	✓ はい
Amazon Kinesis Data Firehose	✓ はい
Amazon Kinesis Data Streams	✓ はい
AWS Lake Formation	✓ はい
AWS Lambda	✓ はい
AWS License Manager	✓ はい
Amazon Lookout for Equipment	✓ はい
Amazon Lookout for Vision	✓ はい
Amazon Managed Blockchain	✗ いいえ
Amazon Managed Workflows for Apache Airflow	✓ はい
Amazon Nimble Studio	✓ はい
AWS Proton	✓ はい
Amazon QLDB	✓ はい
Amazon RDS	✓ はい

AWS のサービス	VPC エンドポイントポリシー
Amazon RDS Data API	はい
Amazon Redshift	はい
Amazon Rekognition	はい
Amazon S3	はい
Amazon S3 マルチリージョンアクセスポイント	はい
Amazon SageMaker および Amazon SageMaker ランタイム	はい
Amazon SageMaker ノートブック	はい
AWS Secrets Manager	はい
AWS Security Token Service	はい
AWS Server Migration Service	いいえ
AWS Service Catalog	いいえ
Amazon SES	いいえ
Amazon SNS	はい
Amazon SQS	はい
AWS Step Functions	はい
AWS Systems Manager	はい
AWS Storage Gateway	いいえ
Amazon Textract	はい
Amazon Transcribe	はい
Amazon Transcribe Medical	はい
AWS Transfer for SFTP	いいえ
Amazon WorkSpaces	はい
AWS X-Ray	はい
他の AWS アカウントによってホストされるエンドポイントサービス (p. 41)	いいえ
サポートされる AWS Marketplace パートナーサービス	いいえ

使用可能な AWS のサービス名を表示する

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。

次のコマンドを実行して、ゲートウェイまたはインターフェイスエンドポイントのサービス名のリストを取得できます。service-type フィルターに指定できる値は、Interface と Gateway です。--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 --filter Name=service-type,Values=service-type --
query ServiceNames
```

次に、インターフェイスエンドポイントをサポートするサービスを表示する例を示します。

```
aws ec2 describe-vpc-endpoint-services --filter Name=service-type,Values=Interface --query
 ServiceNames
```

出力例を次に示します。

```
    "aws.sagemaker.us-east-1.notebook",
    "aws.sagemaker.us-east-1.studio",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.acm-pca",
    "com.amazonaws.us-east-1.airflow.api",
    "com.amazonaws.us-east-1.airflow.env",
    "com.amazonaws.us-east-1.airflow.ops",
    "com.amazonaws.us-east-1.application-autoscaling",
    "com.amazonaws.us-east-1.appmesh-envoy-management",
    "com.amazonaws.us-east-1.appstream.api",
    "com.amazonaws.us-east-1.appstream.streaming",
    "com.amazonaws.us-east-1.aps-workspaces",
    "com.amazonaws.us-east-1.athena",
...
```

サービス名を確認したら、次のコマンドを使用して詳細情報を表示できます。

```
aws ec2 describe-vpc-endpoint-services --service-name service-name
```

次の例では、us-east-1 リージョン内の Amazon S3 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。service-type フィルターは、Amazon S3 ゲートウェイエンドポイントを出力から除外します。

```
aws ec2 describe-vpc-endpoint-services --service-name "com.amazonaws.us-east-1.s3" --filter
 Name=service-type,Values=Interface --region us-east-1
```

出力例を次に示します。

```
{
    "ServiceDetails": [
        {
            "ServiceName": "com.amazonaws.us-east-1.s3",
            "ServiceId": "vpce-svc-081d84efcdc7bac15",
            "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": [
                "s3.us-east-1.vpce.amazonaws.com"
            ],
            "VpcEndpointPolicySupported": true,
            "AcceptanceRequired": false,
            "ManagesVpcEndpoints": false,
            "Tags": []
        }
    ],
    "ServiceNames": [
        "com.amazonaws.us-east-1.s3"
    ]
}
```

AWS PrivateLink のクォータ

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「クォータの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	調整可能	コメント
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 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
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。
VPC エンドポイントポリシーのサイズ	20,480 文字	いいえ	VPC エンドポイントポリシーのサイズには空白文字が含まれます

以下は、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、各インターフェイスエンドポイントは、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でき、最大 40 Gbps までバーストできます。アプリケーションでより高いバーストや持続的な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。
- VPC エンドポイントは、FRAG_NEEDEDICMP パケットを生成しないため、パス MTU 検出 (PMTUD) はサポートされません。
- 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。