Amazon Virtual Private Cloud

ユーザーガイド

API Version 2013-02-01

アマゾン ウェブ サービス

Amazon Virtual Private Cloud: ユーザーガイド

アマゾン ウェブ サービス

Amazon VPC とは

Amazon Virtual Private Cloud（Amazon VPC）を使用すると、定義した仮想ネットワーク内にアマゾンウェブ サービス（AWS）リソースを起動できます。仮想ネットワークは、ご自身のデータセンターで操作していた従来のネットワークとよく似ていますが、AWS のスケーラブルなインフラストラクチャを使用できるというメリットがあります。

Topics

Amazon VPC の概念

Amazon VPC を開始する場合、この仮想ネットワークの重要な概念と、ご自身のネットワークとの類似点または相違点を理解する必要があります。このセクションでは、Amazon VPC の重要な概念について簡単に説明します。

Amazon VPC は、Amazon EC2 のネットワーキングレイヤーです。Amazon EC2 を始めて使う場合は、Amazon EC2 の概要をご覧ください。」（*Amazon Elastic Compute Cloud User Guide*）でその概要を確認してください。

VPC とサブネット

Virtual Private Cloud（VPC）は、AWS アカウント専用の仮想ネットワークです。VPC は、AWS クラウドの他の仮想ネットワークから論理的に切り離されており、VPC 内には、Amazon EC2 リソースなどの AWS リソースを起動できます。VPC は設定できます。例えば、IP アドレス範囲の選択、サブネットの作成、ルートテーブル、ネットワークゲートウェイ、セキュリティの設定などが可能です。

*サブネット*は、VPC の IP アドレスの範囲です。AWS リソースは、選択したサブネット内に起動できます。インターネットに接続する必要があるリソースにはパブリックサブネットを、インターネットに接続されないリソースにはプライベートサブネットを使用してください。

各サブネットでの AWS リソースの保護には、セキュリティグループ、ネットワークアクセスコントロールリスト (ACL) など、複数のセキュリティレイヤーを使用できます。詳細については、「VPC のセキュリティ (p. 68)」を参照してください。

サポートされているプラットフォーム

EC2-Classic と EC2-VPC の 2 つのプラットフォームが、インスタンスの起動先プラットフォームとしてサポートされています。詳細については、「*Amazon Elastic Compute Cloud User Guide*」の「Supported Platforms」を参照してください。

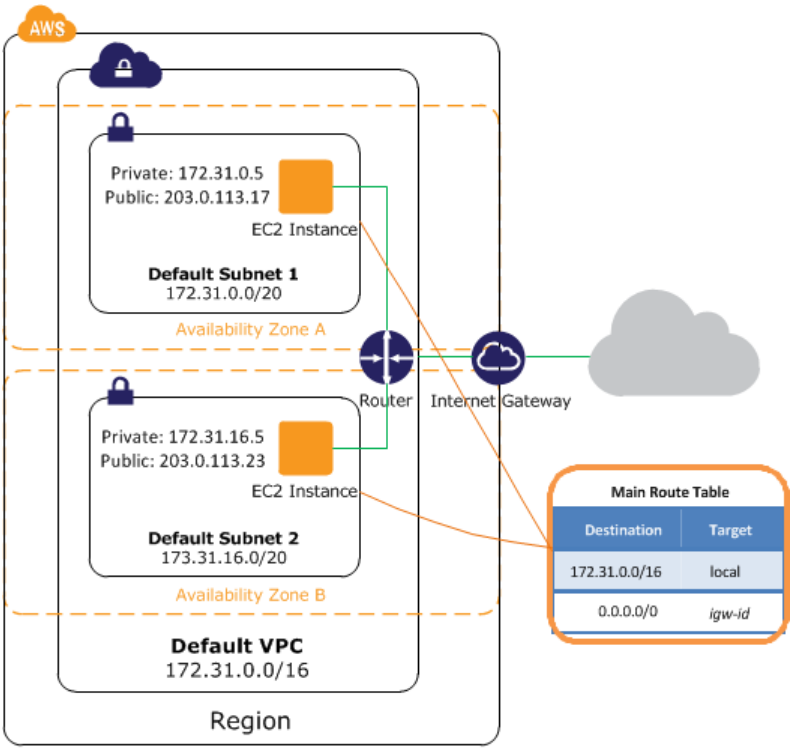
デフォルトの VPC では、EC2-VPC の高度な機能と EC2-Classic の使いやすさの両方のメリットを得られます。If you have a default VPC and don't specify a subnet when you launch an instance, the instance is launched into your default VPC. You can launch instances into your default VPC without needing to know anything about Amazon VPC.

詳細については、「デフォルトの VPC とサブネット (p. 61)」を参照してください。

インターネットにアクセスする

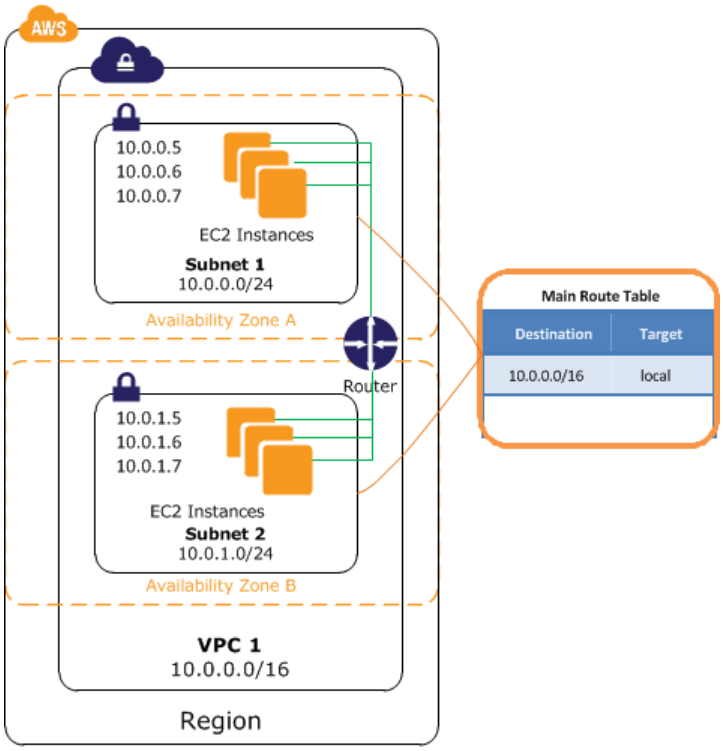
VPC 内に起動するインスタンスが VPC 外のリソースにどのようにアクセスするかをコントロールします。

デフォルトのサブネット内に起動するインスタンスはそれぞれ、プライベート IP アドレスとパブリック IP アドレスを持っています。これらのインスタンスは、インターネットゲートウェイを介してインターネットと通信できます。インターネットゲートウェイを使用すると、インスタンスが Amazon EC2 ネットワークエッジを介してインターネットに接続できます。デフォルトの VPC にはインターネットゲートウェイが含まれます。

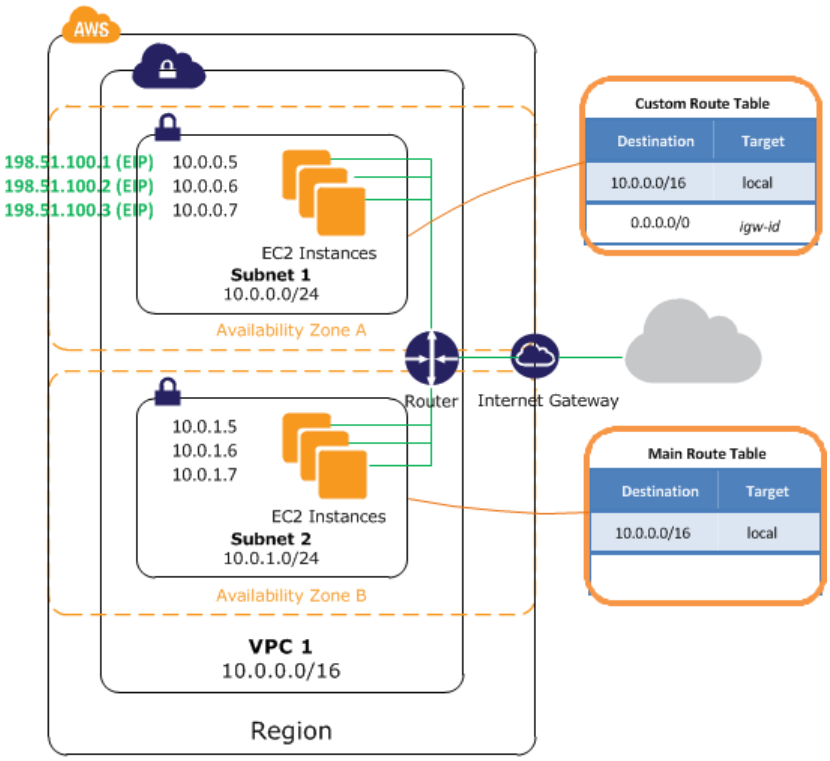


デフォルト以外のサブネット内に起動するインスタンスはそれぞれプライベート IP アドレスを持っていますが、パブリック IP アドレスについては、起動時に特別に割り当てない限り、ありません。これ

らのインスタンスは相互に通信できますが、インターネットや、Amazon Simple Storage Service（Amazon S3）などの他の AWS 製品にはアクセスできません。



デフォルト以外のサブネットで起動するインスタンスのインターネットアクセスを有効にするには、インターネットゲートウェイをその VPC にアタッチし（その VPC がデフォルトの VPC でない場合）、インスタンスに Elastic IP アドレスを関連付けます。



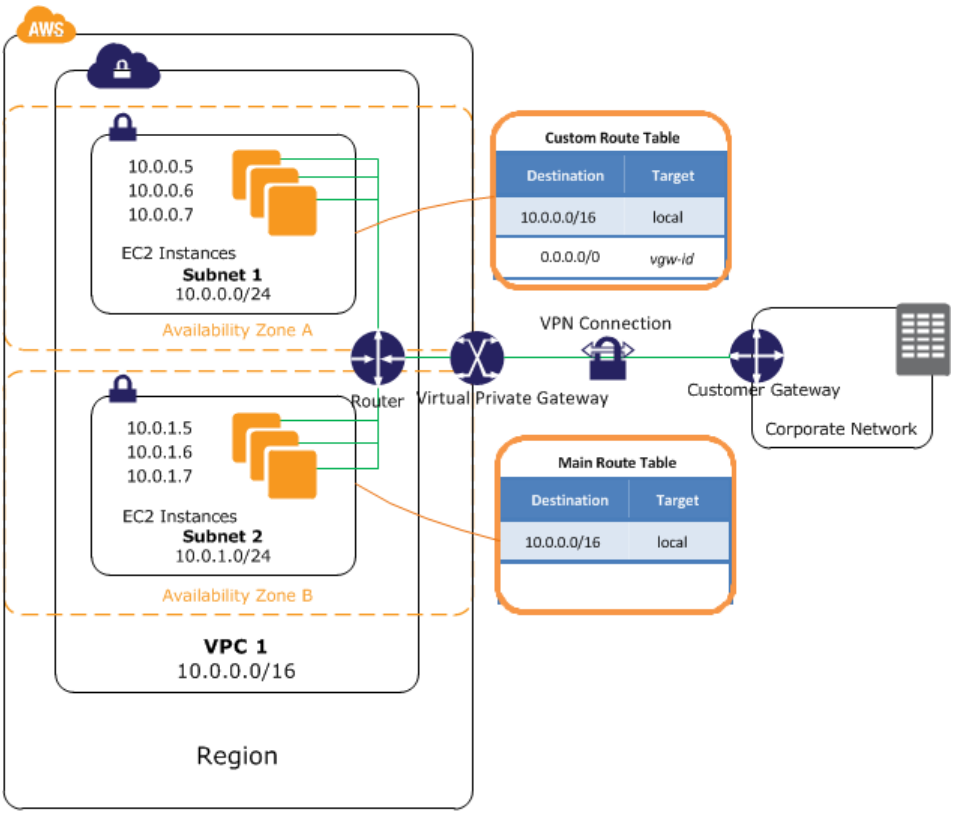
また、ネットワークアドレス変換 (NAT)インスタンスを使用して、VPC のインスタンスによるインターネットへのアウトバウンド接続の開始を許可し、インターネットからの未承諾のインバウンド接続を拒否することもできます。NAT では、複数のプライベート IP アドレスが 1 つのパブリック IP アドレスにマップされます。NAT インスタンスは Elastic IP アドレスを持ち、インターネットゲートウェイを介してインターネットに接続されます。プライベートサブネットのインスタンスをインターネットに接続するには、この NAT インスタンスを使用します。これにより、トラフィックがインスタンスからインターネットゲートウェイにルーティングされ、すべての応答がインスタンスにルーティングされます。

VPC におけるルーティングと NAT の詳細については、「ルートテーブル (p. 106)」および「NAT インスタンス (p. 122)」を参照してください。

企業ネットワークまたはホームネットワークにアクセスする

オプションで、IPsec ハードウェア VPN 接続を使用して、VPC をご自身の企業データセンターに接続し、AWS クラウドをデータセンターの拡張機能にすることができます。

VPN 接続は、VPC にアタッチされている VPG と、データセンターに配置されているカスタマーゲートウェイで構成されています。VPG は、VPN 接続の Amazon 側の VPN コンセントレーターです。カスタマーゲートウェイは、VPN 接続のお客様側の物理デバイスまたはソフトウェアアプライアンスです。



詳細については、「VPC へのハードウェア仮想プライベートゲートウェイの追加 (p. 137)」を参照してください。

Amazon VPC を操作する

AWS では、複数の方法で Amazon VPC を操作できます。

- AWS マネジメントコンソール
- コマンドラインインターフェイス
- API アクション

AWS マネジメントコンソール

AWS マネジメントコンソールを使用すると、VPC、サブネット、ゲートウェイの追加や削除など、Amazon VPC 関連のタスクを実行できます。Amazon VPC コンソールの詳細については、「Amazon VPC 入門」を参照してください。

コマンドラインインターフェイス

Amazon VPC のコマンドラインインターフェイスには、Java ランタイム環境を使用する一連のシンプルなコマンドが用意されています。Amazon VPC のコマンドは、Amazon EC2 API ツールインターフェイスに含まれます。コマンドラインインターフェイスの使用開始の詳細については、「*Amazon Elastic Compute Cloud User Guide*」の「コマンドラインツールの使用を開始する」を参照してください。

Amazon EC2 および Amazon VPC のコマンドの詳細については、「*Amazon Elastic Compute Cloud Command Line Reference*」の「List of API Tools by Function」を参照してください。

API

Amazon VPC アクションは Amazon EC2 WSDL に含まれ、Amazon EC2 ウェブサービスエンドポイントを使用しています。Amazon VPC API アクションに対するリクエスト認証は、Amazon EC2 API アクションに対するリクエスト認証と同じように動作します。API アクションを使用する方法の詳細については、「*Amazon Elastic Compute Cloud User Guide*」の「API リクエストを行う」を参照してください。Amazon EC2 および Amazon VPC API アクションの詳細については、「*Amazon Elastic Compute Cloud API Reference*」の「List of Actions by Function」を参照してください。

Amazon VPC の請求方法

Amazon VPC は追加料金なしで使用できます。使用するインスタンスおよびその他の Amazon EC2 機能に対して標準料金がかかります。ハードウェア VPN 接続を作成する場合は、VPN が VPC に接続されている時間に対して時間単位で料金が発生します。詳細については、「Amazon VPC 料金表」および「Amazon EC2 料金表」を参照してください。

Amazon VPC 制限

プロビジョニングできる Amazon VPC コンポーネントの数には制限があります。コンポーネント数の上限を引き上げるように申請することができます。コンポーネント数の上限と、上限の引き上げを申請する詳細については、「Amazon VPC 制限 (p. 159)」を参照してください。

次のステップ

Amazon VPC の実践的な入門ガイドについては、チュートリアル「Amazon VPC 入門」を参照してください。

Amazon VPC の基本的なシナリオについては、「Amazon VPC の利用シナリオ (p. 8)」を参照してください。VPC とサブネットは、お客様のニーズに合わせて他の方法でも設定できます。他のシナリオの詳細については、「Amazon Virtual Private Cloud Connectivity Options」を参照してください。

他の AWS 製品での Amazon VPC の使用については、次のドキュメントを参照してください。

製品	関連トピック
Amazon EC2	Amazon EC2 と Amazon VPC
Amazon ElastiCache	Amazon VPC で ElastiCache を使用する
Amazon RDS	Amazon RDS と Amazon VPC
Amazon Redshift	VPC でクラスターを管理する
Auto Scaling	Amazon VPC 内に自動スケールインスタンスを起動する
Elastic Load Balancing	Amazon VPC で ELB を展開する
Amazon EMR	Amazon VPC で EMR ジョブフローを実行する
Elastic Beanstalk	Amazon VPC で AWS Elastic Beanstalk を使用する

以下の表は、本サービスを利用する際に役立つ関連リソースをまとめたものです。

リソース	説明
Amazon Virtual Private Cloud Connectivity Options	ネットワーク接続のオプションの概要が記載されているホワイトペーパーです。
AWS Developer Resources	A central starting point to find documentation, code samples, release notes, and other information to help you create innovative applications with AWS.
Amazon VPC Discussion Forum	A community-based forum for discussing technical questions related to Amazon VPC.
Amazon VPC Release Notes	A high-level overview of the current release.
AWS Support Center	The home page for AWS Support.
Contact Us	A central contact point for inquiries concerning AWS billing, accounts, and events.

Amazon VPC の利用シナリオ

このセクションでは、Amazon VPC を利用するための基本シナリオについて説明します。シナリオごとに次を提供します。

- 基本コンポーネントが示されている図
- VPC とサブネットに関する情報
- サブネットのルーティングテーブルに関する情報
- 推奨セキュリティグループのルールに関する情報
- シナリオの実装手順

次の表では、基本シナリオについて説明します。

シナリオ	用途
シナリオ 1: 1 つのパブリックサブネットのみを持つ VPC (p. 9)	ブログや簡単なウェブサイトなど、単層でパブリックなウェブアプリケーションを実行します。
シナリオ 2: パブリックサブネットとプライベートサブネットを持つ VPC (p. 16)	2 つ目のサブネットでパブリックにはアクセスできないバックエンドサーバーを維持しながら、単層でパブリックなウェブアプリケーションを実行します。
シナリオ 3: パブリックサブネットとプライベートサブネット、およびハードウェア VPN アクセスを持つ VPC (p. 28)	データセンターをクラウドに拡張し、さらに、VPC からインターネットに直接アクセスします。
シナリオ 4: 1 つのプライベートサブネットのみ、およびハードウェア VPN アクセスを持つ VPC (p. 42)	データセンターをクラウドに拡張し、ネットワークをインターネットに公開せずに、Amazon のインフラストラクチャを利用します。

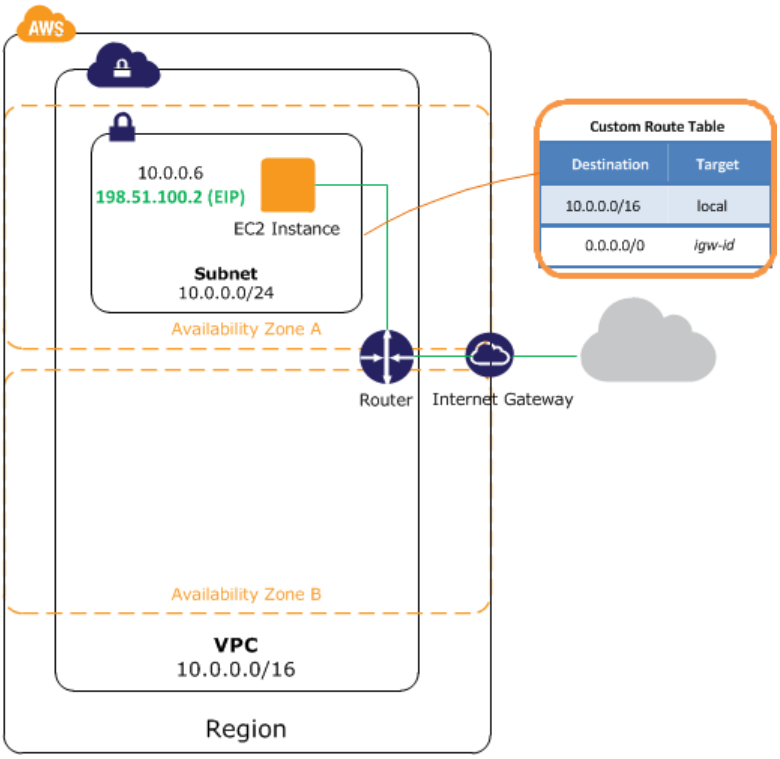
シナリオ 1: 1 つのパブリックサブネットのみを持つ VPC

このシナリオの設定には、1 つのパブリックサブネットを持つ Virtual Private Cloud (VPC) と、インターネットを介した通信を有効にするインターネットゲートウェイが含まれます。この設定は、ブログや簡単なウェブサイトなど、単層でパブリックなウェブアプリケーションを実行する必要がある場合にお勧めします。

Topics

シナリオ 1 の設定

次の図は、このシナリオの設定に重要なコンポーネントを示しています。



Note

「*Amazon Virtual Private Cloud Getting Started Guide*」の演習が完了している場合、すでにこのシナリオは Amazon VPC コンソールの VPC ウィザードを使用して実装されています。

シナリオ 1 の基本コンポーネント

次のリストでは、このシナリオの設定図で示されている基本コンポーネントについて説明します。

- サイズ/16 (サンプル CIDR: 10.0.0.0/16) の Virtual Private Cloud (VPC) 。65,536 個のプライベート IP アドレスを提供します。
- サイズ/24 (サンプル CIDR: 10.0.0.0/24) のサブネット。256 個のプライベート IP アドレスを提供します。
- インターネットゲートウェイ。VPC をインターネット、および Amazon Simple Storage Service (Amazon S3) などの他の AWS サービスに接続します。
- サブネット範囲のプライベート IP アドレス (例: 10.0.0.6) と Elastic IP アドレス (例: 198.51.100.2) を持つインスタンス。前者はインスタンスが VPC 内の他のインスタンスと通信できるようにし、後者はインターネットからインスタンスにアクセスできるようにします。
- サブネットのインスタンスが VPC 内の他のインスタンスと通信できるようにするルートテーブルエントリと、サブネットのインスタンスがインターネットで直接通信できるようにするルートテーブルエントリ。

サブネットの詳細については、「VPC とサブネット (p. 52)」および「VPC の IP アドレス指定 (p. 101)」を参照してください。インターネットゲートウェイの詳細については、「インターネットゲートウェイを VPC に追加する (p. 117)」を参照してください。

Tip

各インスタンスを Elastic IP アドレスに割り当てずに、VPC のインスタンスがインターネットで通信できるようにするには、NAT インスタンスを使用します。NAT インスタンスの設定の詳細については、「シナリオ 2: パブリックサブネットとプライベートサブネットを持つ VPC (p. 16)」または「NAT インスタンス (p. 122)」を参照してください。

シナリオ 1 のルーティング

VPC には暗示的なルーターがあります (このシナリオの設定図を参照) 。このシナリオでは、VPC ウィザードによって、送信先が VPC 外のアドレスであるトラフィックすべてをインターネットゲートウェイにルーティングするルートテーブルを作成し、それをサブネットに関連付けます。これを行わない場合は、ご自身でルートテーブルを作成し、関連付ける必要があります。

次の表は、このシナリオの設定図で使用されているサンプルアドレスが、ルートテーブルではどのように表示されるかを示しています。1 行目は、VPC のローカルルーティングのエントリを示しています。このエントリによって、VPC 内のインスタンスが相互に通信できるようになります。2 行目は、他のすべてのサブネットトラフィックをインターネットゲートウェイにルーティングするエントリを示しています。これは、AWS によって割り当てられた識別子を使用して指定されます。

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

シナリオのセキュリティ 1

AWS provides two features that you can use to increase security in your VPC: *security groups* and *network ACLs*. Both features enable you to control the inbound and outbound traffic for your instances, but security groups work at the instance level, while network ACLs work at the subnet level. Security groups alone

can meet the needs of many VPC users. However, some VPC users decide to use both security groups and network ACLs to take advantage of the additional layer of security that network ACLs provide. For more information about security groups and network ACLs and how they differ, see VPC のセキュリティ (p. 68).

シナリオ 1 では、セキュリティグループを使用します。ネットワーク ACL は使用しません。

推奨されるセキュリティグループのルール

VPC にはデフォルトのセキュリティグループが用意されており、この初期設定では、すべてのアウトバウンドトラフィックと、セキュリティグループに割り当てられているインスタンス間のすべてのトラフィックが許可されます。インスタンスを起動するときにセキュリティグループを指定しないと、そのインスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。デフォルトのセキュリティグループのルールは変更できますが、ウェブサーバーに必要なルールは、VPC 内に起動する他のインスタンスには有効でない可能性があります。したがって、セキュリティグループを作成し、パブリックサブネットのウェブサーバーで使用することをお勧めします。

`WebServerSG` という名前のセキュリティグループを作成し、必要に応じてルールを変更し、VPC 内にインスタンスを起動するときにセキュリティグループを指定します。デフォルトでは、新しいセキュリティグループには、すべてのトラフィックがインスタンスを出ることを許可するアウトバウンドルールのみが設定されています。任意のインバウンドトラフィックを許可するには、またはアウトバウンドトラフィックを制限するには、ルールを追加する必要があります。

次の表では、WebServerSG グループのインバウンドルールについて説明します。ウェブサーバーがアウトバウンド通信を開始しないため、デフォルトのアウトバウンドルールは削除されます。

インバウンド			
送信元	プロトコル	ポート範囲	コメント
0.0.0.0/0	TCP	80	任意の場所からウェブサーバーへのインバウンド HTTP アクセスを許可する
0.0.0.0/0	TCP	443	任意の場所からウェブサーバーへのインバウンド HTTPS アクセスを許可する
ネットワークのパブリック IP アドレスの範囲	TCP	22	(Linux インスタンス) ネットワークからのインバウンド SSH アクセスを許可する
ネットワークのパブリック IP アドレスの範囲	TCP	3389	(Windows インスタンス) ネットワークからのインバウンド RDP アクセスを許可する

Tip

サービスを使用して、ローカルコンピュータのパブリック IP アドレスを取得することもできます。IP アドレスを提供するサービスを検索するには、検索フレーズ「what is my IP address」を使用します。ISP 経由、またはファイアウォールの内側から静的 IP アドレスなしで接続している場合は、クライアントコンピュータで使用されている IP アドレスの範囲を見つける必要があります。

VPC のデフォルトのセキュリティグループには、割り当てられたインスタンスが相互に通信することを自動的に許可するルールがあります。VPC のインスタンス間でその種類の通信を許可するには、セキュリティグループに以下のようなルールを追加する必要があります。

インバウンド			
送信元	プロトコル	ポート範囲	コメント
セキュリティグループ ID (sg-*xxxxxxxx*)	すべて	すべて	このセキュリティグループに割り当てられた他のインスタンスからのインバウンドトラフィックを許可する

シナリオ 1 を実装する

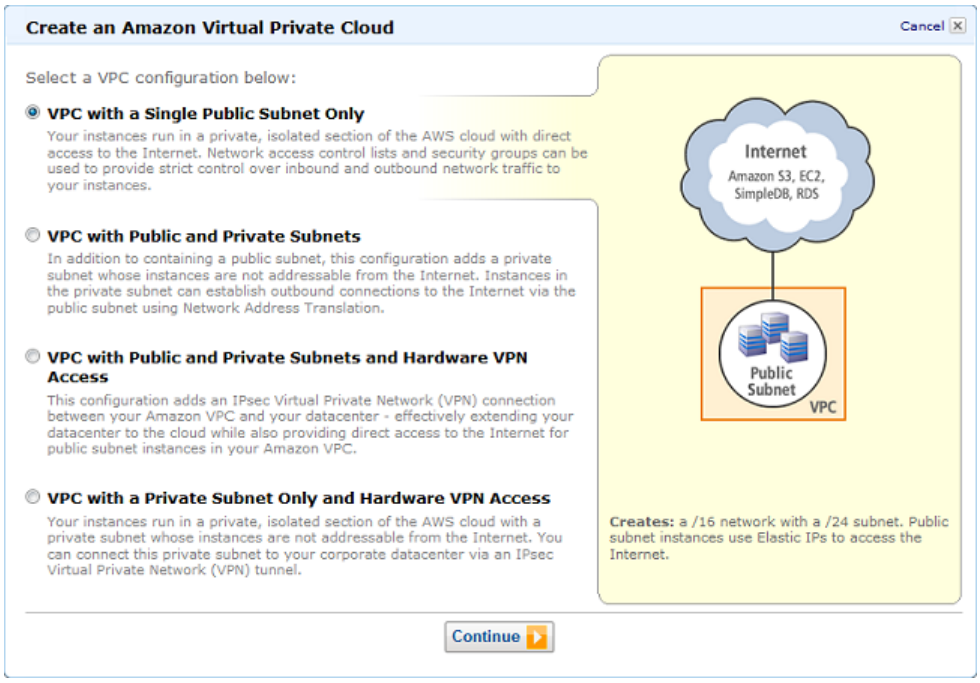
次のプロセスにしたがって、VPC ウィザードを使用してシナリオを実装します。

Tip

「Amazon Virtual Private Cloud Getting Started Guide」でも同じ手順を確認できますが、一部の手順がさらに詳しく説明されています。

VPC ウィザードを使用してシナリオ 1 を実装するには

1. VPC、サブネット、およびインターネットゲートウェイを設定する。
   a. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
   b. ナビゲーションペインで [VPC Dashboard] をクリックします。
   c. ダッシュボードの [Your Virtual Private Cloud] 領域で、[Get started creating a VPC] をクリックします。VPC リソースがない場合は、[Start VPC Wizard] をクリックします。
   d. 最初のオプション [VPC with a Single Public Subnet Only] を選択し、[Continue] をクリックします。



e. 確認ページに、選択した CIDR の範囲と設定が表示されます。必要に応じて設定を変更し、[Create VPC] をクリックして、VPC、サブネット、インターネットゲートウェイ、およびルートテーブルを作成します。

2. WebServerSG セキュリティグループを作成し、ルールを追加する。

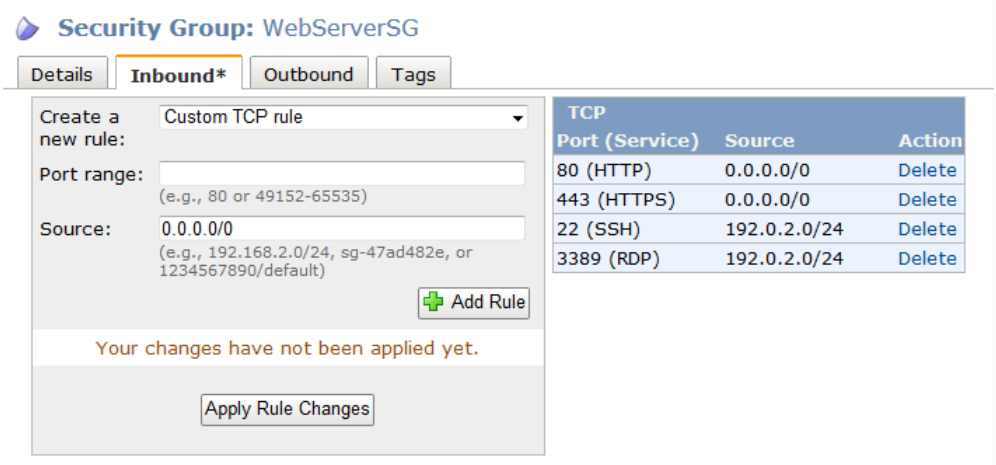
a. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
b. ナビゲーションペインで [Security Groups] をクリックします。
c. [Create Security Group] ボタンをクリックします。
d. セキュリティグループの名前として `WebServerSG` を指定し、説明を入力します。[VPC] メニューで VPC の ID を選択し、[Yes, Create] をクリックします。
e. 先ほど作成した WebServerSG セキュリティグループを選択します。詳細ペインには、セキュリティグループに関する情報のタブと、インバウンドルールおよびアウトバウンドルールを操作するためのタブがあります。
f. [Inbound] タブで、次の手順を実行します。

- [Create a new rule] リストで `HTTP` を選択し、[Source] が `0.0.0.0/0` であることを確認して、[Add Rule] をクリックします。
- [Create a new rule] リストから `HTTPS` を選択し、[Source] が `0.0.0.0/0` であることを確認して、[Add Rule] をクリックします。
- [Create a new rule] リストで SSH (Linux の場合) または RDP (Windows の場合) を選択します。[Source] ボックスで、ネットワークのパブリック IP アドレス範囲を指定し、[Add Rule] をクリックします (このアドレス範囲を知らない場合は、`0.0.0.0/0` を使用してテストすることができます。プロダクションでは、インスタンスへのアクセスを特定の IP アドレスまたはアドレス範囲のみに許可します) 。

Tip

お客様の会社で Linux インスタンスと Windows インスタンスが両方とも使用されている場合は、SSH および RDP の双方に対してアクセス権を追加できます。

- [Apply Rule Changes] をクリックし、そのインバウンドルールを適用します。



g. [Outbound] タブで、すべてのアウトバウンドトラフィックを有効にするデフォルトルールを検索し、[Delete] をクリックして、[Apply Rule Changes] をクリックします。

3. VPC 内にインスタンスを起動する:

   a. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
   b. ダッシュボードで、[Launch Instance] ボタンをクリックします。
   c. [Create a New Instance] ページで [Quick Launch Wizard] を選択し、[Continue] をクリックします。ウィザードの指示にしたがって操作します。インスタンスの名前を指定し、キーペア、AMI の順に選択し、[Continue] をクリックします。
   d. [Edit Details] をクリックします。[Instance Details] で [Launch into a VPC] を選択し、サブネットを指定します。[Security Settings] で、手順 2 で作成したセキュリティグループを選択します。`WebServerSG`
   e. （オプション）デフォルトでは、デフォルトではない VPC に起動するインスタンスには、パブリック IP アドレスは割り当てられません。インスタンスへの接続を可能にするには、ここでパブリック IP アドレスを割り当てることも、Elastic IP アドレスをアロケートし、インスタンス起動後にそれをインスタンスに割り当てることもできます。現段階でパブリック IP アドレスを割り当てるには、[Advanced Details] に進み、[Assign Public IP] チェックボックスがオンになっていることを確認します。

      Note

      パブリック IP アドレスは、デバイスインデックスが eth0 になっている単一の新しいネットワークインターフェイスにしか割り当てることはできません。詳細については、「起動中のパブリック IP アドレスの割り当て (p. 102)」を参照してください。

   f. [Save Details] をクリックします。
   g. 選択した設定を確認します。必要に応じて設定を変更し、[Launch] をクリックします。

4. 手順 3 の中でインスタンスにパブリック IP アドレスを割り当てなかった場合、インスタンスに接続することはできません。Elastic IP アドレスをインスタンスに割り当てる。

   a. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
   b. ナビゲーションペインで [Elastic IPs] をクリックします。
   c. [Allocate New Address] ボタンをクリックします。
   d. [EIP used in] リストで VPC を選択し、[Yes, Allocate] をクリックします。
   e. リストで Elastic IP アドレスを選択し、[Associate Address] ボタンをクリックします。
   f. [Associate Address] ダイアログボックスで、アドレスを関連付けるインスタンスを選択し、[Yes, Associate] をクリックします。

これで、VPC のインスタンスに接続できるようになりました。Linux インスタンスに接続する方法については、「*Amazon Elastic Compute Cloud User Guide*」の Connect to Your Linux Instance を参照してください。Windows インスタンスに接続する方法については、「*Amazon Elastic Compute Cloud Microsoft Windows Guide*」の Connect to Your Windows Instance を参照してください。

シナリオ 2: パブリックサブネットとプライベートサブネットを持つ VPC

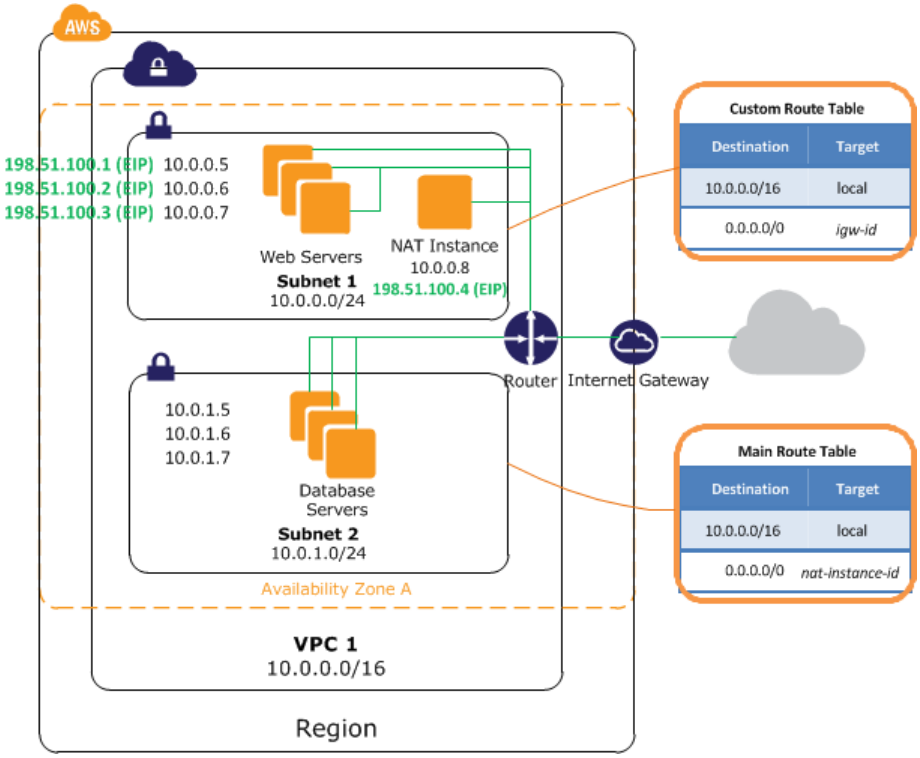
このシナリオの設定には、パブリックサブネットとプライベートサブネットを持つ Virtual Private Cloud（VPC）が含まれます。このシナリオは、パブリックにはアクセスできないバックエンドサーバーを維持しながら、パブリックなウェブアプリケーションを実行する場合にお勧めします。一般的な例としては、パブリックサブネットのウェブサーバーとプライベートサブネットのデータベースサーバーを持つ多階層のウェブサイトが挙げられます。ウェブサーバーがデータベースサーバーと通信できるように、セキュリティとルーティングを設定できます。

パブリックサブネットのインスタンスはインターネットから直接インバウンドトラフィックを受信できますが、プライベートサブネットのインスタンスはこれができません。また、パブリックサブネットのインスタンスはアウトバウンドトラフィックを直接インターネットに送信できますが、プライベートサブネットのインスタンスはできません。代わりに、プライベートサブネットのインスタンスは、パブリックサブネット内に起動するネットワークアドレス変換（NAT）インスタンスを使用して、インターネットにアクセスできます。

Topics

シナリオ 2 の設定

次の図は、このシナリオの設定に重要なコンポーネントを示しています。



シナリオ 2 の基本コンポーネント

次のリストでは、このシナリオの設定図で示されている基本コンポーネントについて説明します。

- サイズ/16（サンプル CIDR: 10.0.0.0/16）の Virtual Private Cloud（VPC）。65,536 個のプライベート IP アドレスを提供します。
- サイズ/24（サンプル CIDR: 10.0.0.0/24）のパブリックサブネット。256 個のプライベート IP アドレスを提供します。
- サイズ/24（サンプル CIDR: 10.0.1.0/24）のプライベートサブネット。256 個のプライベート IP アドレスを提供します。
- インターネットゲートウェイ。VPC をインターネット、および Amazon Simple Storage Service（Amazon S3）などの他の AWS サービスに接続します。
- サブネット範囲のプライベート IP アドレス（例: 10.0.0.5、10.0.1.5）を持つインスタンス。そのインスタンスが VPC 内で相互に、および他のインスタンスと通信できるようにします。パブリックサブネットのインスタンスにも Elastic IP アドレス（例: 198.51.100.1）が含まれ、インターネットからそのインスタンスにアクセスできるようにします。プライベートサブネットのインスタンスは、インターネットからの受信トラフィックを受け取る必要がないバックエンドサーバーです。ただし、NAT インスタンスを使用して、リクエストをインターネットに送信できます（次の箇条書きを参照）。
- 独自の Elastic IP アドレスを持つネットワークアドレス変換（NAT）インスタンス。プライベートサブネットのインスタンスが、リクエストをインターネットに送信できるようにします（例: ソフトウェアのアップデート用）。
- パブリックサブネットに関連付けられているカスタムルートテーブル。このルートテーブルには、サブネットのインスタンスが VPC 内の他のインスタンスと通信できるようにするエントリと、サブネットのインスタンスがインターネットと直接通信できるようにするエントリが含まれます。
- プライベートサブネットに関連付けられているメインルートテーブル。このルートテーブルには、サブネットのインスタンスが VPC 内の他のインスタンスと通信できるようにするエントリと、サブネットのインスタンスが NAT インスタンスを介してインターネットと通信できるようにするエントリが含まれます。

サブネットの詳細については、「VPC とサブネット (p. 52)」および「VPC の IP アドレス指定 (p. 101)」を参照してください。インターネットゲートウェイの詳細については、「インターネットゲートウェイを VPC に追加する (p. 117)」を参照してください。NAT の詳細については、「NAT インスタンス (p. 122)」を参照してください。

Tip

プロキシとして動作する拠点サーバーをパブリックサブネットに設定すると、プライベートサブネットでインスタンスを管理するのに役立ちます。例えば、パブリックサブネットで SSH ポートフォーワード機能または RDP ゲートウェイを設定し、ご自身のネットワークからデータベースサーバーに向かうトラフィックをプロキシできます。

シナリオ 2 のルーティング

VPC には暗示的なルーターがあります (このシナリオの設定図を参照) 。このシナリオでは、VPC ウィザードによって、プライベートサブネットで使用されるメインルートテーブルを更新し、カスタムルートテーブルを作成してパブリックサブネットに関連付けます。これを行わない場合は、ご自身でルートテーブルを作成し、関連付ける必要があります。

このシナリオでは、各サブネットから AWS に向かう (例えば、Amazon EC2 または Amazon S3 エンドポイントに向かう) すべてのトラフィックが、インターネットゲートウェイを介して流れます。プライベートサブネットのデータベースサーバーには Elastic IP アドレスがありません。したがって、インターネットからのトラフィックを直接受け取ることはできません。ただし、パブリックサブネットで NAT インスタンスを使用すれば、データベースサーバーでインターネットトラフィックを送受信できます。

追加のサブネットを作成した場合、そのサブネットはデフォルトでメインルートテーブルを使用します。つまり、デフォルトではプライベートサブネットです。サブネットをパブリックにする必要がある場合、関連付けられているルートテーブルはいつでも変更できます。

以下の表は、このシナリオのルートテーブルを示しています。

メインルートテーブル

1 行目は、VPC のローカルルーティングのエントリを示しています。このエントリによって、VPC 内のインスタンスが相互に通信できるようになります。2 行目は、他のすべてのサブネットトラフィックを NAT インスタンスに送信するエントリを示しています。これは、AWS によって割り当てられた識別子 (ネットワークインターフェイス `eni-1a2b3c4d`、インスタンス `i-1a2b3c4d` など) を使用して指定されます。

送信先	ターゲット
`10.0.0.0/16`	ローカル
`0.0.0.0/0`	eni-*xxxxxxxx* / i-*xxxxxxxx*

カスタムルートテーブル

1 行目は、VPC のローカルルーティングのエントリを示しています。このエントリによって、この VPC 内のインスタンスが相互に通信できるようになります。2 行目は、他のすべてのサブネットトラフィックを、インターネットゲートウェイを介してインターネットにルーティングするエントリを示しています。これは、AWS によって割り当てられた識別子 (`igw-1a2b3d4d` など) を使用して指定されます。

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

シナリオ 2 のセキュリティ

AWS provides two features that you can use to increase security in your VPC: *security groups* and *network ACLs*. Both features enable you to control the inbound and outbound traffic for your instances, but security groups work at the instance level, while network ACLs work at the subnet level. Security groups alone can meet the needs of many VPC users. However, some VPC users decide to use both security groups and network ACLs to take advantage of the additional layer of security that network ACLs provide. For more information about security groups and network ACLs and how they differ, see VPC のセキュリティ (p. 68).

シナリオ 2 では、セキュリティグループを使用します。ネットワーク ACL は使用しません。

推奨セキュリティグループ

VPC に用意されているデフォルトのセキュリティグループの初期設定では、すべてのインバウンドトラフィックが拒否され、すべてのアウトバウンドトラフィックと、そのグループに割り当てられているインスタンス間のすべてのトラフィックが許可されます。インスタンスを起動するときにセキュリティグループを指定しないと、そのインスタンスはデフォルトのセキュリティグループに自動的に割り当てられます。

このシナリオでは、デフォルトのセキュリティグループを変更するのではなく、以下のセキュリティグループを作成することをお勧めします。

- WebServerSG – パブリックサブネットのウェブサーバーの場合
- NATSG – パブリックサブネットの NAT インスタンスの場合
- DBServerSG – プライベートサブネットのデータベースサーバーの場合

セキュリティグループに割り当てられたインスタンスのサブネットは様々です。ただし、このシナリオでは、各セキュリティグループがインスタンスの役割の種類に対応しており、役割ごとにインスタンスが特定のサブネットに属さなければなりません。したがって、このシナリオでは、1 つのセキュリティグループに割り当てられたインスタンスはすべて、同じサブネットに属しています。

VPC のデフォルトのセキュリティグループには、割り当てられたインスタンスが相互に通信することを自動的に許可するルールがあります。異なるセキュリティグループを使用するときに VPC のインスタンス間でその種類の通信を許可するには、セキュリティグループに以下のようなルールを追加する必要があります。

インバウンド			
送信元	プロトコル	ポート範囲	コメント
セキュリティグループの ID	すべて	すべて	このセキュリティグループに割り当てられた他のインスタンスからのインバウンドトラフィックを許可する

WebServerSG、NATSG、および DBServerSG セキュリティグループを作成する

WebServerSG セキュリティグループと DBServerSG セキュリティグループは互いに参照し合うので、ルールを追加する前に、このシナリオで必要なすべてのセキュリティグループを作成します。

WebServerSG、NATSG、および DBServerSG セキュリティグループを作成するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Security Groups] をクリックします。
3. [Create Security Group] ボタンをクリックします。
4. [Create Security Group] ダイアログボックスで、セキュリティグループ名として `WebServerSG` を指定し、説明を入力します。[VPC] リストで VPC の ID を選択し、[Yes, Create] をクリックします。
5. 再度 [Create Security Group] ボタンをクリックします。
6. [Create Security Group] ダイアログボックスで、セキュリティグループ名として `NATSG` を指定し、説明を入力します。[VPC] リストで VPC の ID を選択し、[Yes, Create] をクリックします。
7. 再度 [Create Security Group] ボタンをクリックします。
8. [Create Security Group] ダイアログボックスで、セキュリティグループ名として `DBServerSG` を指定し、説明を入力します。[VPC] リストで VPC の ID を選択し、[Yes, Create] をクリックします。

次のセクションでは、各セキュリティグループの推奨ルールと、そのルールを追加する方法について説明します。

ルールを WebServerSG セキュリティグループに追加する

WebServerSG セキュリティグループは、パブリックサブネット内にウェブサーバーを起動するときに指定するセキュリティグループです。次の表では、このセキュリティグループの推奨ルールについて説明します。このルールにより、ウェブサーバーがインターネットトラフィックを受信したり、ご利用のネットワークから SSH または RDP トラフィックを受信したりできます。また、そのウェブサーバーは、プライベートサブネットのデータベースサーバーへの読み込みおよび書き込みリクエストを開始することもできます。ウェブサーバーがアウトバウンド通信を開始しないため、デフォルトのアウトバウンドルールは削除されます。

WebServerSG: 推奨ルール

インバウンド			
送信元	プロトコル	ポート範囲	コメント
0.0.0.0/0	TCP	80	任意の場所からウェブサーバーへのインバウンド HTTP アクセスを許可する
0.0.0.0/0	TCP	443	任意の場所からウェブサーバーへのインバウンド HTTPS アクセスを許可する
ネットワークのパブリック IP アドレス範囲	TCP	22	ネットワークから Linux インスタンスへのインバウンド SSH アクセス (インターネットゲートウェイ経由) を許可する

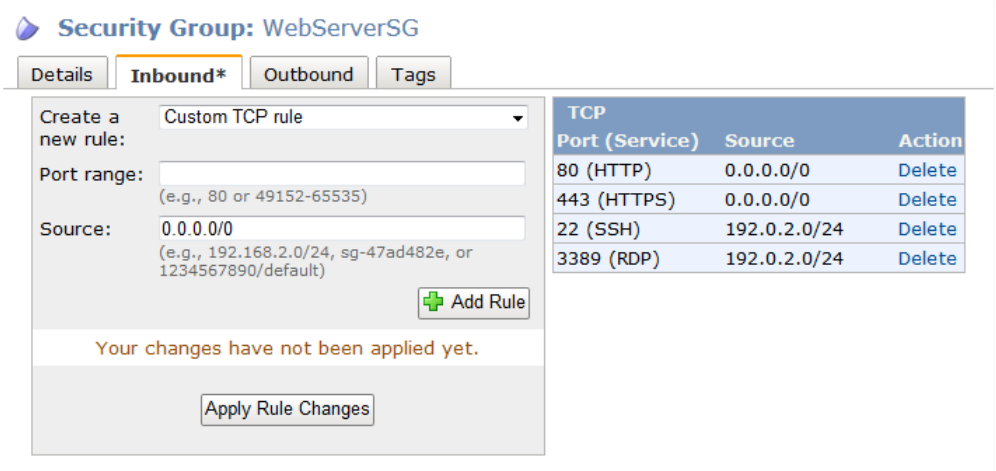
ネットワークのパブリック IP アドレス範囲	TCP	3389	ネットワークから Windows インスタンスへのインバウンド RDP アクセス（インターネットゲートウェイ経由）を許可する
アウトバウンド			
送信先	プロトコル	ポート範囲	コメント
DBServerSG セキュリティグループの ID	TCP	1433	DBServerSG に割り当てられたデータベースサーバーへのアウトバウンド Microsoft SQL Server アクセスを許可する
DBServerSG セキュリティグループの ID	TCP	3306	DBServerSG に割り当てられたデータベースサーバーへのアウトバウンド MySQL アクセスを許可する

Note

グループには SSH アクセスと RDP アクセスの両方、および Microsoft SQL Server アクセスと MySQL アクセスの両方が含まれます。この場合は、Linux（SSH および MySQL）または Windows（RDP および Microsoft SQL Server）に対するルールのみで十分かもしれません。

ルールを WebServerSG セキュリティグループに追加するには

1. 作成した WebServerSG セキュリティグループを選択します。詳細ペインに、セキュリティグループの詳細と、インバウンドルールおよびアウトバウンドルールを操作するためのタブが表示されます。
2. 次に示すように、[Inbound] タブを使用して、インバウンドトラフィックのルールを追加します。
   a. [Create a new rule] リストで `HTTP` を選択します。[Source] が `0.0.0.0/0` であることを確認し、[Add Rule] をクリックします。[Apply Rules Changes] ボタンが有効で、"Your changes have not been applied yet" というテキストが表示されています。インバウンドトラフィックに対して必要なルールをすべて追加したら、[Apply Rule Changes] をクリックしてルールを追加します。
   b. [Create a new rule] リストから `HTTPS` を選択します。[Source] が `0.0.0.0/0` であることを確認し、[Add Rule] をクリックします。
   c. [Create a new rule] リストから `SSH` を選択します。[Source] ボックスで、ネットワークのパブリック IP アドレス範囲（この例では `192.0.2.0/24` を使用）を指定し、[Add Rule] をクリックします。
   d. [Create a new rule] リストから `RDP` を選択します。[Source] ボックスで、ネットワークのパブリック IP 範囲を指定し、[Add Rule] をクリックします。
   e. [Apply Rule Changes] をクリックします。



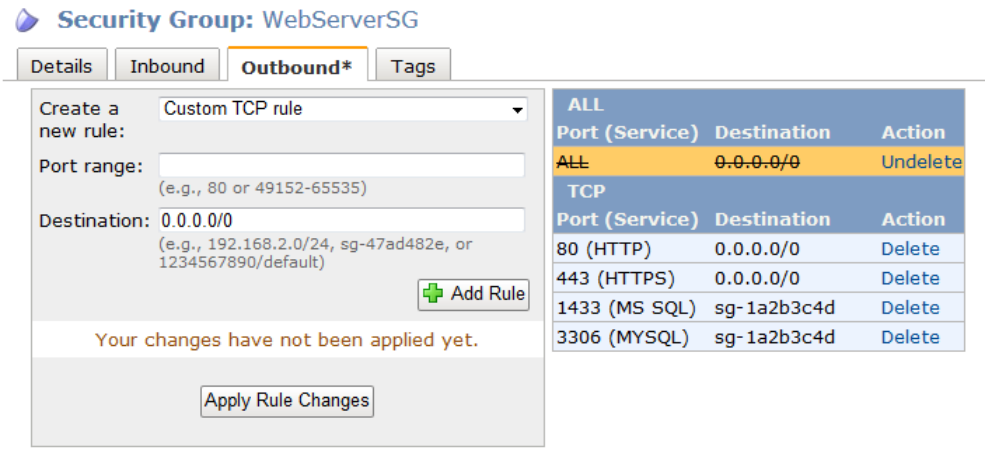
3. 次に示すように、[Outbound] タブを使用して、アウトバウンドトラフィックのルールを追加します。

   a. すべてのアウトバウンドトラフィックを有効にするデフォルトのルールを見つけ、[Delete] をクリックします。

   b. [Create a new rule] リストで MS SQL を選択します。[Destination] ボックスで、DBServerSG セキュリティグループの ID を指定し、[Add Rule] をクリックします。

   c. [Create a new rule] リストで MySQL を選択します。[Destination] ボックスで、DBServerSG セキュリティグループの ID を指定し、[Add Rule] をクリックします。

   d. [Apply Rule Changes] をクリックします。



ルールを NATSG セキュリティグループに追加する

NATSG セキュリティグループは、パブリックサブネット内に NAT インスタンスを起動するときに指定するセキュリティグループです。次の表では、このセキュリティグループの推奨ルールについて説明します。このルールにより、NAT インスタンスがプライベートサブネットのインスタンスからインターネット宛てのトラフィックを受信したり、ご利用のネットワークから SSH または RDP トラフィック

を受信したりできます。また、NAT インスタンスは、ネットワークにトラフィックを送信することもできます。これにより、プライベートサブネットのインスタンスがソフトウェア更新を取得できます。

NATSG: 推奨ルール

インバウンド			
送信元	プロトコル	ポート範囲	コメント
10.0.1.0/24	TCP	80	プライベートサブネットのデータベースサーバーからのインバウンド HTTP トラフィックを許可する
10.0.1.0/24	TCP	443	プライベートサブネットのデータベースサーバーからのインバウンド HTTPS トラフィックを許可する
ネットワークのパブリック IP アドレス範囲	TCP	22	ネットワークから NAT インスタンスへのインバウンド SSH アクセス (インターネットゲートウェイ経由) を許可する
アウトバウンド			
送信先	プロトコル	ポート範囲	コメント
0.0.0.0/0	TCP	80	インターネットへのアウトバウンド HTTP アクセス (インターネットゲートウェイ経由) を許可する
0.0.0.0/0	TCP	443	インターネットへのアウトバウンド HTTPS アクセス (インターネットゲートウェイ経由) を許可する

推奨ルールを NATSG セキュリティグループに追加するには

1. 作成した NATSG セキュリティグループを選択します。詳細ペインに、セキュリティグループの詳細と、インバウンドルールおよびアウトバウンドルールを操作するためのタブが表示されます。
2. 次に示すように、[Inbound] タブを使用して、インバウンドトラフィックのルールを追加します。
   a. [Create a new rule] リストで HTTP を選択します。[Source] ボックスで、プライベートサブネットの IP アドレス範囲を指定し、[Add Rule] をクリックします。
   b. [Create a new rule] リストで HTTPS を選択します。[Source] ボックスで、プライベートサブネットの IP アドレス範囲を指定し、[Add Rule] をクリックします。
   c. [Create a new rule] リストで SSH を選択します。[Source] ボックスで、ネットワークのパブリック IP アドレス範囲を指定し、[Add Rule] をクリックします。
   d. [Apply Rule Changes] をクリックします。
3. [Outbound] タブで、すべてのアウトバウンドトラフィックを有効にするデフォルトルールを検索し、[Delete] をクリックして、[Apply Rule Changes] をクリックします。
4. 次に示すように、[Outbound] タブを使用して、アウトバウンドトラフィックのルールを追加します。
   a. すべてのアウトバウンドトラフィックを有効にするデフォルトのルールを見つけ、[Delete] をクリックします。

b. [Create a new rule] リストから HTTP を選択します。[Destination] が 0.0.0.0/0 であることを確認し、[Add Rule] をクリックします。
c. [Create a new rule] リストで HTTPS を選択します。[Destination] が 0.0.0.0/0 であることを確認し、[Add Rule] をクリックします。
d. [Apply Rule Changes] をクリックします。

ルールを DBServerSG セキュリティグループに追加する

DBServerSG セキュリティグループは、プライベートサブネット内にデータベースサーバーを起動するときに指定するセキュリティグループです。次の表では、このセキュリティグループの推奨ルールについて説明します。このルールにより、ウェブサーバーからの読み込みおよび書き込みデータベースリクエストが許可されます。また、インターネットへのトラフィックを開始することもできます (ルートテーブルは、そのトラフィックを NAT インスタンスに送信し、その後、インターネットゲートウェイを介してインターネットに転送します) 。

DBServerSG: 推奨ルール

インバウンド			
送信元	プロトコル	ポート範囲	コメント
WebServerSG セキュリティグループの ID	TCP	1433	DBServerSG に割り当てられたデータベースサーバーへの、WebServerSG に割り当てられたウェブサーバーの Microsoft SQL Server アクセスを許可する
WebServerSG セキュリティグループの ID	TCP	3306	DBServerSG に割り当てられたデータベースサーバーへの、WebServerSG に割り当てられたウェブサーバーの MySQL アクセスを許可する
アウトバウンド			
送信先	プロトコル	ポート範囲	コメント
0.0.0.0/0	TCP	80	インターネットへのアウトバウンド HTTP アクセス (例: ソフトウェアのアップデート用) を許可する
0.0.0.0/0	TCP	443	インターネットへのアウトバウンド HTTPS アクセス (例: ソフトウェアのアップデート用) を許可する

推奨ルールを DBServerSG セキュリティグループに追加するには

1. 作成した DBServerSG セキュリティグループを選択します。詳細ペインに、セキュリティグループの詳細と、インバウンドルールおよびアウトバウンドルールを操作するためのタブが表示されます。
2. [Inbound] タブで、[Create a new rule] リストから MS SQL を選択します。[Source] ボックスで、WebServerSG セキュリティグループの ID を指定し、[Add Rule] をクリックします。
3. [Inbound] タブで、[Create a new rule] リストから MYSQL を選択します。[Source] ボックスで、WebServerSG セキュリティグループの ID を指定し、[Add Rule] をクリックします。

4. [Apply Rule Changes] をクリックします。
5. 次に示すように、[Outbound] タブを使用して、アウトバウンドトラフィックのルールを追加します。

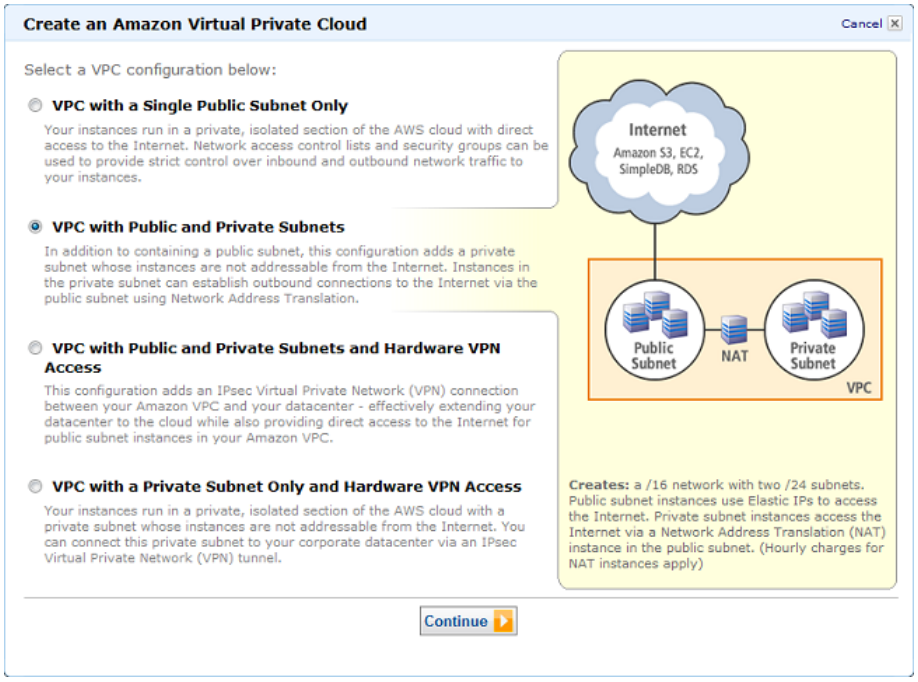
   a. すべてのアウトバウンドトラフィックを有効にするデフォルトのルールを見つけ、[Delete] をクリックします。
   b. [Create a new rule] リストから HTTP を選択します。[Destination] が 0.0.0.0/0 であることを確認し、[Add Rule] をクリックします。
   c. [Create a new rule] リストで HTTPS を選択します。[Destination] が 0.0.0.0/0 であることを確認し、[Add Rule] をクリックします。
   d. [Apply Rule Changes] をクリックします。

シナリオ 2 を実装する

次のプロセスにしたがって、VPC ウィザードを使用してシナリオ 2 を実装します。

VPC ウィザードを使用してシナリオ 2 を実装するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [VPC Dashboard] をクリックします。
3. ダッシュボードの [Your Virtual Private Cloud] 領域で、[Get started creating a VPC] をクリックします。VPC リソースがない場合は、[Start VPC Wizard] をクリックします。
4. 2 つ目のオプション [VPC with Public and Private Subnets] を選択し、[Continue] をクリックします。

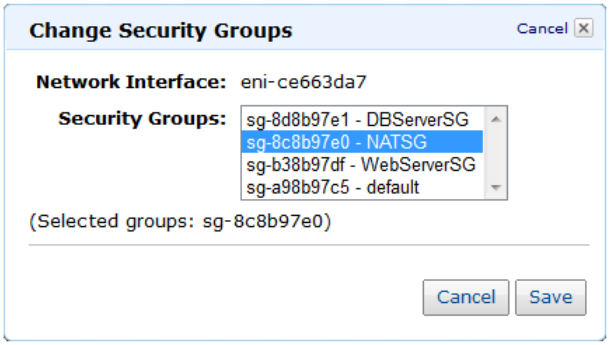


5. 確認ページで情報を確認します。必要に応じて情報を変更し、[Create VPC] をクリックして、VPC、サブネット、インターネットゲートウェイ、およびルートテーブルを作成し、パブリックサブネット内に NAT インスタンスを起動します。

VPC ウィザードは、NAT インスタンスを起動したときに、VPC のデフォルトのセキュリティグループを使用しました。この NAT インスタンスは、NATSG セキュリティグループに関連付ける必要があります。

NAT インスタンスのセキュリティグループを変更するには

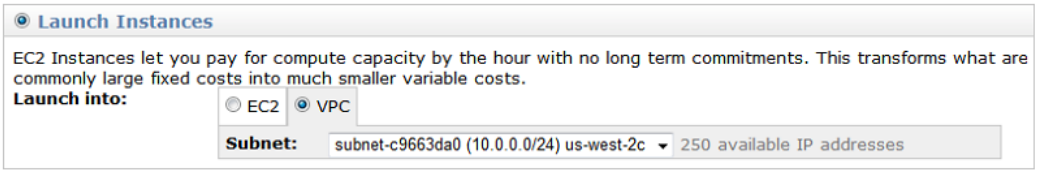
1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. ナビゲーションペインで [Network Interfaces] をクリックします。
3. リストから NAT インスタンスのネットワークインターフェイスを選択し、[Actions] リストで [Change Security Groups] を選択します。
4. [Change Security Groups] ダイアログボックスで、作成した NATSG セキュリティグループ（「シナリオ 2 のセキュリティ (p. 19)」を参照）を [Security Groups] リストから選択し、[Save] をクリックします。



VPC 内にインスタンスを起動できます。VPC 外でのインスタンスの起動について既によくわかっている場合は、VPC 内へのインスタンスの起動に関して必要な情報は大体把握できています。

インスタンスを起動するには（ウェブサーバーまたはデータベースサーバー）

1. WebServerSG および DBServerSG セキュリティグループをまだ作成していない場合は作成します（「シナリオ 2 のセキュリティ (p. 19)」を参照）。このセキュリティグループのいずれかを、インスタンスの起動時に指定します。
2. Classic ウィザードを起動します。
   a. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
   b. ダッシュボードで [Launch Instance] ボタンをクリックします。
   c. [Create a New Instance] ページで、[Classic Wizard] を選択し、[Continue] をクリックします。
3. [CHOOSE AN AMI] ページの [Quick Start] タブに、Amazon マシンイメージ（AMI）と呼ばれる基本的な設定のリストが表示されます。使用する AMI を選択し、[Select] ボタンをクリックします。
4. [INSTANCE DETAILS] ページの [Launch Instances] で、インスタンスを起動するサブネットを選択します。例えば、パブリックサブネット内にウェブサーバーを起動し、プライベートサブネット内にデータベースサーバーを起動します。このページの他のデフォルトの設定はそのままにして、[Continue] をクリックします。



5. （オプション）デフォルトでは、デフォルトではないサブネット内に起動するインスタンスは、パブリック IP アドレスを受信しません。インスタンスへの接続を可能にするには、ここでパブリック IP アドレスを割り当てることも、Elastic IP アドレスをアロケートし、インスタンス起動後にそれをインスタンスに割り当てることもできます。現段階でパブリック IP アドレスを割り当てるには、2 番目の [INSTANCE DETAILS] ページの [Number of Network Interfaces] セクションで、[Assign Public IP] チェックボックスをオンにし、[Continue] をクリックします。

   Note

   パブリック IP アドレスは、デバイスインデックスが eth0 になっている単一の新しいネットワークインターフェイスにしか割り当てることはできません。詳細については、「起動中のパブリック IP アドレスの割り当て (p. 102)」を参照してください。

6. 次に表示される [INSTANCE DETAILS] ページでデフォルトの設定を使用するには、各ページで [Continue] をクリックするだけです。
7. [CREATE A KEY PAIR] ページで、作成済みの既存のキーペアから選択するか、ウィザードの指示にしたがって新しいキーペアを作成します。
8. [Configure Firewall] ページで、インスタンスのセキュリティグループを選択し（ウェブサーバーの場合は `WebServerSG`、データベースサーバーの場合は `DBServerSG`）、[Continue] をクリックします。
9. 設定を確認します。選択した内容でよければ、[Launch] をクリックします。

手順 5 でパブリック IP アドレスをインスタンスに割り当てていない場合、インスタンスへの接続は不可能です。パブリックサブネットのインスタンスにアクセスするには、そのインスタンスに Elastic IP アドレスを割り当てておく必要があります。

To allocate an Elastic IP address and assign it to an instance

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. Click Elastic IPs in the navigation pane.
3. Click the Allocate New Address button.
4. In the Allocate New Address dialog box, in the EIP used in list, select VPC, and then click Yes, Allocate.
5. Select the Elastic IP address from the list, and then click the Associate Address button.
6. In the Associate Address dialog box, select the network interface or instance. Select the address to associate the Elastic IP address with from the corresponding Private IP Address list, and then click Yes, Associate.

これで、VPC のインスタンスに接続できるようになりました。Linux インスタンスに接続する方法については、「*Amazon Elastic Compute Cloud User Guide*」の Connect to Your Linux Instance を参照してください。Windows インスタンスに接続する方法については、「*Amazon Elastic Compute Cloud Microsoft Windows Guide*」の Connect to Your Windows Instance を参照してください。

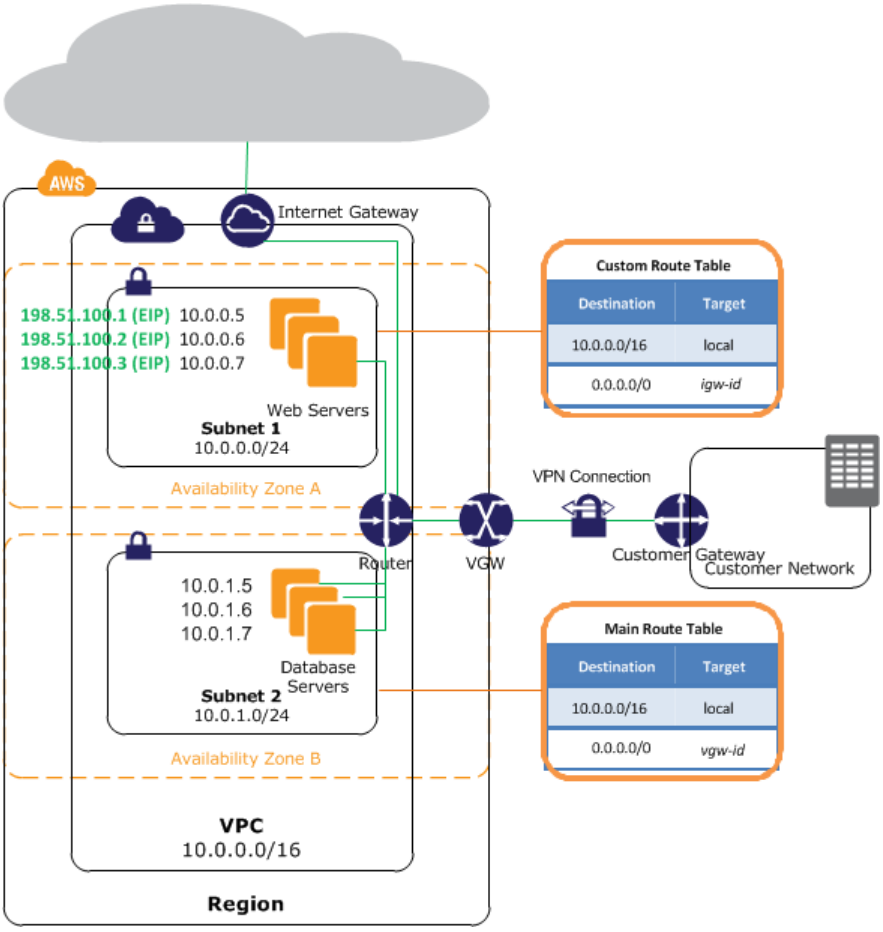
シナリオ 3: パブリックサブネットとプライベートサブネット、およびハードウェア VPN アクセスを持つ VPC

このシナリオの設定には、パブリックサブネットとプライベートサブネットを持つ Virtual Private Cloud（VPC）、および IPsec VPN トンネルを介した独自のネットワークとの通信を有効にする仮想プライベートゲートウェイが含まれます。このシナリオは、ネットワークをクラウドに拡張し、さらに、VPC からインターネットに直接アクセスする必要がある場合にお勧めします。このシナリオを使用すると、スケーラブルなウェブフロントエンドを持つ多階層のアプリケーションをパブリックサブネットで実行し、IPsec VPN 接続によりネットワークに接続されているプライベートサブネットにデータを保存できます。

Topics

シナリオ 3 の設定

次の図は、このシナリオの設定に重要なコンポーネントを示しています。



Important

「*Amazon Virtual Private Cloud Network Administrator Guide*」では、このシナリオに関して、ネットワーク管理者が、お客様の VPN 接続で Amazon VPC カスタマーゲートウェイを設定する際に行う必要があることを説明しています。

シナリオ 3 の基本的な設定

次のリストでは、このシナリオの設定図で示されている基本コンポーネントについて説明します。

- サイズ/16 (サンプル CIDR: 10.0.0.0/16) の Virtual Private Cloud (VPC) 。65,536 個のプライベート IP アドレスを提供します。
- サイズ/24 (サンプル CIDR: 10.0.0.0/24) のパブリックサブネット。256 個のプライベート IP アドレスを提供します。
- サイズ/24 (サンプル CIDR: 10.0.1.0/24) の VPN のみのサブネット。256 個のプライベート IP アドレスを提供します。
- インターネットゲートウェイ。VPC をインターネット、および Amazon Simple Storage Service (Amazon S3) などの他の AWS サービスに接続します。
- VPC とネットワークの間の VPN 接続。この VPN 接続は、仮想プライベートゲートウェイとカスタマーゲートウェイで構成され、前者は VPN 接続の Amazon 側、後者はお客様側に配置されています。

- サブネット範囲のプライベート IP アドレス (例: 10.0.0.5 と 10.0.1.5) を持つインスタンス。そのインスタンスが VPC 内で相互に、および他のインスタンスと通信できるようにします。パブリックサブネットのインスタンスにも Elastic IP アドレス (例: 198.51.100.1) が含まれ、インターネットからそのインスタンスにアクセスできるようにします。VPN のみのサブネットのインスタンスは、インターネットからの受信トラフィックを受け取る必要がないバックエンドサーバーです。ただし、ネットワークからのトラフィックを送受信できます。
- パブリックサブネットに関連付けられているカスタムルートテーブル。このルートテーブルには、サブネットのインスタンスが VPC 内の他のインスタンスと通信できるようにするエントリと、サブネットのインスタンスがインターネットと直接通信できるようにするエントリが含まれます。
- VPN のみのサブネットに関連付けられているメインルートテーブル。ルートテーブルには、サブネットのインスタンスが VPC 内の他のインスタンスと通信できるようにするエントリと、サブネットのインスタンスがネットワークと直接通信できるようにするエントリが含まれます。

サブネットの詳細については、「VPC とサブネット (p. 52)」および「VPC の IP アドレス指定 (p. 101)」を参照してください。インターネットゲートウェイの詳細については、「インターネットゲートウェイを VPC に追加する (p. 117)」を参照してください。VPN 接続の詳細については、「VPC へのハードウェア仮想プライベートゲートウェイの追加 (p. 137)」を参照してください。カスタマーゲートウェイの設定の詳細については、「*Amazon Virtual Private Cloud Network Administrator Guide*」を参照してください。

シナリオ 3 のルーティング

VPC には暗示的なルーターがあります (このシナリオの設定図を参照) 。このシナリオでは、VPC ウィザードによって、VPN のみのサブネットで使用されるメインルートテーブルを更新し、カスタムルートテーブルを作成してパブリックサブネットに関連付けます。これを行わない場合は、ご自身でルートテーブルを作成し、関連付ける必要があります。

VPN のみのサブネットのインスタンスはインターネットに直接接続することはできません。インターネット宛てのトラフィックはすべて、まず仮想プライベートゲートウェイを経由してネットワークに向かいます。そこでは、ファイアウォールと企業のセキュリティポリシーが適用されます。インスタンスが AWS 宛てのトラフィック (Amazon S3 または Amazon EC2 API へのリクエストなど) を送信する場合、リクエストは仮想プライベートゲートウェイを介してネットワークに向かい、AWS に到達する前にインターネットに達する必要があります。

Tip

ネットワークからのトラフィックで、パブリックサブネットのインスタンスの Elastic IP アドレスに向かうものはすべて、仮想プライベートゲートウェイではなく、インターネットを経由します。代わりに、ネットワークからのトラフィックでパブリックサブネットに向かうものが仮想プライベートゲートウェイを経由できるように、ルートとセキュリティグループのルールを設定することができます。

VPN 接続は、静的にルーティングされた VPN 接続または動的にルーティングされた VPN 接続 (BGP を使用) のいずれかとして設定されます。静的なルーティングを選択すると、VPN 接続を作成するときに、ネットワークの IP プレフィックスを手動で入力するように求められます。動的なルーティングを選択すると、IP プレフィックスは、BGP を使用して VPC の仮想プライベートゲートウェイに自動的にアドバタイズされます。

以下の表は、このシナリオのルートテーブルを示しています。

メインルートテーブル

1 行目は、VPC のローカルルーティングのエントリを示しています。このエントリによって、VPC 内のインスタンスが相互に通信できるようになります。2 行目は、プライベートサブネットからの他のすべてのサブネットトラフィックを、仮想プライベートゲートウェイを介してネットワークにルーティン

グするエントリを示しています。これは、AWS によって割り当てられた識別子 (vgw-1a2b3c4d など) を使用して指定されます。

送信先	ターゲット
10.0.0.0/16	ローカル
0.0.0.0/0	vgw-*xxxxxxxx*

カスタムルートテーブル

1 行目は、VPC のローカルルーティングのエントリを示しています。このエントリによって、VPC 内のインスタンスが相互に通信できるようになります。2 行目は、パブリックサブネットからの他のすべてのサブネットトラフィックを、インターネットゲートウェイを介してインターネットにルーティングするエントリを示しています。これは、AWS によって割り当てられた識別子 (igw-1a2b3c4d など) を使用して指定されます。

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

代替ルーティング

プライベートサブネットのインスタンスをインターネットにアクセスする場合、サブネットのインターネット宛てのトラフィックが、パブリックサブネットのネットワークアドレス変換 (NAT) インスタンスに向かうようにルーティングを設定することもできます。NAT インスタンスは、VPN のみのサブネットのインスタンスが、リクエストをインターネットゲートウェイ経由で送信できるようにします (例: ソフトウェアのアップデート用)。プライベートサブネットのインターネット宛てのトラフィックが NAT インスタンスにアクセスできるようにするには、メインルートテーブルを次のように更新する必要があります。

メインルートテーブル

1 行目は、VPC のローカルルーティングのエントリを示しています。2 行目は、ネットワーク宛てのサブネットトラフィックを、仮想プライベートゲートウェイにルーティングするエントリを示しています。これは、AWS によって割り当てられた識別子 (vgw-1a2b3c4d など) を使用して指定されます。3 行目は、他のすべてのサブネットトラフィックを NAT インスタンスに送信します。これは、AWS によって割り当てられた識別子 (i-1a2b3c4d など) によって指定されます。

送信先	ターゲット
10.0.0.0/16	ローカル
172.16.0.0/12	vgw-*xxxxxxxx*
0.0.0.0/0	i-*xxxxxxxx*

手動による NAT インスタンスの設定については、「NAT インスタンス (p. 122)」を参照してください。VPC ウィザードを使用した NAT インスタンスの設定については、「シナリオ 2: パブリックサブネットとプライベートサブネットを持つ VPC (p. 16)」を参照してください。

シナリオ 3 のセキュリティ

AWS provides two features that you can use to increase security in your VPC: *security groups* and *network ACLs*. Both features enable you to control the inbound and outbound traffic for your instances, but security groups work at the instance level, while network ACLs work at the subnet level. Security groups alone can meet the needs of many VPC users. However, some VPC users decide to use both security groups and network ACLs to take advantage of the additional layer of security that network ACLs provide. For more information about security groups and network ACLs and how they differ, see VPC のセキュリティ (p. 68).

シナリオ 3 では、セキュリティグループを使用します。ネットワーク ACL は使用しません。

Topics

推奨セキュリティグループ

VPC に用意されているデフォルトのセキュリティグループの初期設定では、すべてのインバウンドトラフィックが拒否され、すべてのアウトバウンドトラフィックと、セキュリティグループに割り当てられているインスタンス間のすべてのトラフィックが許可されます。インスタンスを起動するときにセキュリティグループを指定しないと、そのインスタンスはデフォルトのセキュリティグループに自動的に割り当てられます。

このシナリオでは、デフォルトのセキュリティグループを変更するのではなく、以下のセキュリティグループを作成することをお勧めします。

- WebServerSG – パブリックサブネットのウェブサーバーの場合
- DBServerSG – VPN のみのサブネットのデータベースサーバーの場合

セキュリティグループに割り当てられたインスタンスのサブネットは様々です。ただし、このシナリオでは、各セキュリティグループがインスタンスの役割の種類に対応しており、役割ごとにインスタンスが特定のサブネットに属さなければなりません。したがって、このシナリオでは、1 つのセキュリティグループに割り当てられたインスタンスはすべて、同じサブネットに属しています。

VPC のデフォルトのセキュリティグループには、割り当てられたインスタンスが相互に通信することを自動的に許可するルールがあります。異なるセキュリティグループを使用するときに VPC のインスタンス間でその種類の通信を許可するには、セキュリティグループに以下のようなルールを追加する必要があります。

インバウンド			
送信元	プロトコル	ポート範囲	コメント
セキュリティグループの ID	すべて	すべて	このセキュリティグループに割り当てられた他のインスタンスからのインバウンドトラフィックを許可する

WebServerSG および DBServerSG セキュリティグループを作成する

WebServerSG セキュリティグループと DBServerSG セキュリティグループは互いに参照し合うので、ルールを追加する前に、このシナリオで必要なすべてのセキュリティグループを作成します。

WebServerSG および DBServerSG セキュリティグループを作成するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Security Groups] をクリックします。
3. [Create Security Group] ボタンをクリックします。
4. [Create Security Group] ダイアログボックスで、セキュリティグループ名として `WebServerSG` を指定し、説明を入力します。[VPC] リストで VPC の ID を選択し、[Yes, Create] をクリックします。
5. 再度 [Create Security Group] ボタンをクリックします。
6. [Create Security Group] ダイアログボックスで、セキュリティグループ名として `DBServerSG` を指定し、説明を入力します。[VPC] リストで VPC の ID を選択し、[Yes, Create] をクリックします。

次のセクションでは、各セキュリティグループの推奨ルールと、そのルールを追加する方法について説明します。

ルールを WebServerSG セキュリティグループに追加する

WebServerSG セキュリティグループは、パブリックサブネット内にウェブサーバーを起動するときに指定するセキュリティグループです。次の表では、このセキュリティグループの推奨ルールについて説明します。このルールにより、ウェブサーバーがインターネットトラフィックを受信したり、ご利用のネットワークから SSH または RDP トラフィックを受信したりできます。また、このウェブサーバーは、VPN のみのサブネット内のデータベースサーバーインスタンスへの読み込みおよび書き込みリクエストを開始することもできます。

WebServerSG: 推奨ルール

インバウンド			
送信元	プロトコル	ポート範囲	コメント
0.0.0.0/0	TCP	80	任意の場所からウェブサーバーへのインバウンド HTTP アクセスを許可する
0.0.0.0/0	TCP	443	任意の場所からウェブサーバーへのインバウンド HTTPS アクセスを許可する
ネットワークのパブリック IP アドレス範囲	TCP	22	ネットワークから Linux インスタンスへのインバウンド SSH アクセス（インターネットゲートウェイ経由）を許可する
ネットワークのパブリック IP アドレス範囲	TCP	3389	ネットワークから Windows インスタンスへのインバウンド RDP アクセス（インターネットゲートウェイ経由）を許可する

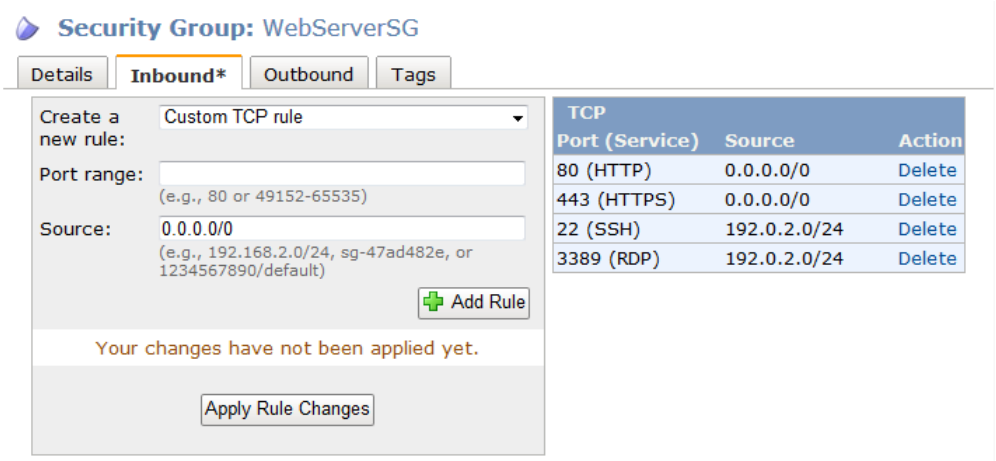
アウトバウンド			
DBServerSG セキュリティグループの ID	TCP	1433	DBServerSG に割り当てられたデータベースサーバーへのアウトバウンド Microsoft SQL Server アクセスを許可する
DBServerSG セキュリティグループの ID	TCP	3306	DBServerSG に割り当てられたデータベースサーバーへのアウトバウンド MySQL アクセスを許可する

Note

グループには SSH アクセスと RDP アクセスの両方、および Microsoft SQL Server アクセスと MySQL アクセスの両方が含まれます。この場合は、Linux (SSH および MySQL) または Windows (RDP および Microsoft SQL Server) に対するルールのみで十分かもしれません。

推奨ルールを WebServerSG セキュリティグループに追加するには

1. 作成した WebServerSG セキュリティグループを選択します。詳細ペインに、セキュリティグループの詳細と、インバウンドルールおよびアウトバウンドルールを操作するためのタブが表示されます。
2. 次に示すように、[Inbound] タブを使用して、インバウンドトラフィックのルールを追加します。
   a. [Create a new rule] リストで HTTP を選択します。[Source] が 0.0.0.0/0 であることを確認し、[Add Rule] をクリックします。[Apply Rules Changes] ボタンが有効で、"Your changes have not been applied yet" というテキストが表示されています。インバウンドトラフィックに対して必要なルールをすべて追加したら、[Apply Rule Changes] をクリックしてルールを追加します。
   b. [Create a new rule] リストから HTTPS を選択します。[Source] が 0.0.0.0/0 であることを確認し、[Add Rule] をクリックします。
   c. [Create a new rule] リストから SSH を選択します。[Source] ボックスで、ネットワークのパブリック IP アドレス範囲 (この例では 192.0.2.0/24 を使用) を指定し、[Add Rule] をクリックします。
   d. [Create a new rule] リストで RDP を選択します。[Source] ボックスで、ネットワークのパブリック IP アドレス範囲を指定し、[Add Rule] をクリックします。
   e. [Apply Rule Changes] をクリックします。



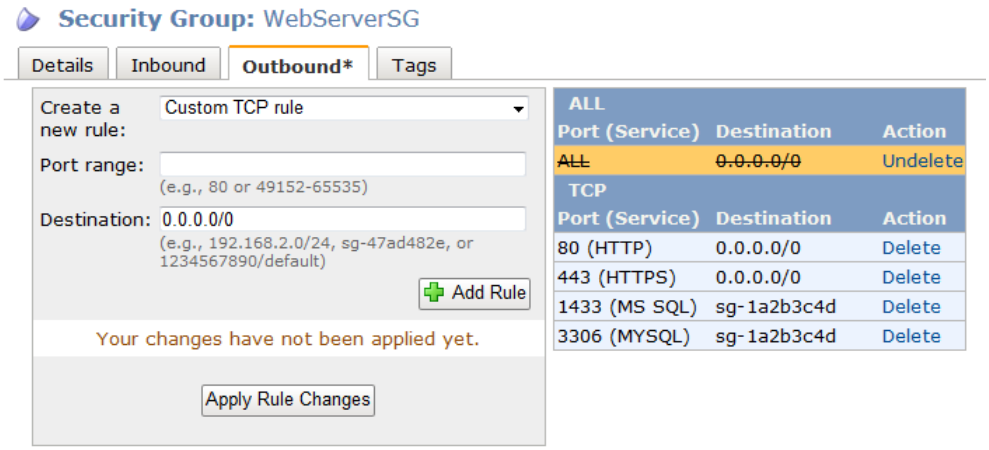
3. 次に示すように、[Outbound] タブを使用して、アウトバウンドトラフィックのルールを追加します。

   a. すべてのアウトバウンドトラフィックを有効にするデフォルトのルールを見つけ、[Delete] をクリックします。

   b. [Create a new rule] リストで MS SQL を選択します。[Destination] ボックスで、DBServerSG セキュリティグループの ID を指定し、[Add Rule] をクリックします。

   c. [Create a new rule] リストで MySQL を選択します。[Destination] ボックスで、DBServerSG セキュリティグループの ID を指定し、[Add Rule] をクリックします。

   d. [Apply Rule Changes] をクリックします。



ルールを DBServerSG セキュリティグループに追加する

DBServerSG セキュリティグループは、VPN のみのサブネット内にデータベースサーバーを起動するときに指定するセキュリティグループです。次の表では、このセキュリティグループの推奨ルールについて説明します。このルールにより、ウェブサーバーからの Microsoft SQL Server と MySQL の読み取りおよび書き込みリクエストと、ご利用のネットワークからの SSH および RDP トラフィックが許可されます。また、データベースサーバーは、インターネットへのトラフィックを開始することもできます (ルートテーブルは、そのトラフィックを仮想プライベートゲートウェイを介して送信します)。

DBServerSG: 推奨ルール

インバウンド			
送信元	プロトコル	ポート範囲	コメント
WebServerSG セキュリティグループの ID	TCP	1433	DBServerSG に割り当てられたデータベースサーバーへの、WebServerSG に割り当てられたウェブサーバーの Microsoft SQL Server アクセスを許可する

WebServerSG セキュリティグループの ID	TCP	3306	DBServerSG に割り当てられたデータベースサーバーへの、WebServerSG に割り当てられたウェブサーバーの MySQL アクセスを許可する
ネットワークのパブリック IP アドレス範囲	TCP	22	ネットワークから Linux インスタンスへのインバウンド SSH トラフィック（仮想プライベートゲートウェイ経由）を許可する
ネットワークのパブリック IP アドレス範囲	TCP	3389	ネットワークから Windows インスタンスへのインバウンド RDP トラフィック（仮想プライベートゲートウェイ経由）を許可する
アウトバウンド			
送信先	プロトコル	ポート範囲	コメント
0.0.0.0/0	TCP	80	仮想プライベートゲートウェイ経由のインターネットへのアウトバウンド HTTP アクセス（例: ソフトウェアのアップデート用）を許可する
0.0.0.0/0	TCP	443	仮想プライベートゲートウェイ経由のインターネットへのアウトバウンド HTTPS アクセス（例: ソフトウェアのアップデート用）を許可する

推奨ルールを DBServerSG セキュリティグループに追加するには

1. 作成した DBServerSG セキュリティグループを選択します。詳細ペインに、セキュリティグループの詳細と、インバウンドルールおよびアウトバウンドルールを操作するためのタブが表示されます。
2. 次に示すように、[Inbound] タブを使用して、インバウンドトラフィックのルールを追加します。
   a. [Create a new rule] リストで SSH を選択します。[Source] ボックスで、ネットワークの IP アドレス範囲を指定し、[Add Rule] をクリックします。
   b. [Create a new rule] リストから RDP を選択します。[Source] ボックスで、ネットワークの IP アドレス範囲を指定し、[Add Rule] をクリックします。
   c. [Create a new rule] リストから MS SQL を選択します。[Source] ボックスで、WebServerSG セキュリティグループの ID を指定し、[Add Rule] をクリックします。
   d. [Create a new rule] リストから MYSQL を選択します。[Source] ボックスで、WebServerSG セキュリティグループの ID を指定し、[Add Rule] をクリックします。
   e. [Apply Rule Changes] をクリックします。
3. 次に示すように、[Outbound] タブを使用して、アウトバウンドトラフィックのルールを追加します。
   a. すべてのアウトバウンドトラフィックを有効にするデフォルトのルールを見つけ、[Delete] をクリックします。
   b. [Create a new rule] リストから HTTP を選択します。[Destination] が 0.0.0.0/0 であることを確認し、[Add Rule] をクリックします。

c. [Create a new rule] リストで HTTPS を選択します。[Destination] が 0.0.0.0/0 であることを確認し、[Add Rule] をクリックします。
d. [Apply Rule Changes] をクリックします。

シナリオ 3 を実装する

次のプロセスにしたがって、VPC ウィザードを使用してシナリオ 3 を実装します。

カスタマーゲートウェイを準備するには

1. カスタマーゲートウェイとして使用するアプライアンスを特定します。テストしたデバイスの詳細については、Amazon Virtual Private Cloud のよくある質問を参照してください。カスタマーゲートウェイの要件の詳細については、「Amazon Virtual Private Cloud Network Administrator Guide」を参照してください。
2. カスタマーゲートウェイの外部インターフェイスのインターネットルーティングが可能な IP アドレスを取得します。このアドレスは静的である必要があります。また、ネットワークアドレス変換（NAT）を実行するデバイスの背後のアドレスを使用することはできません。
3. 仮想プライベートゲートウェイへの VPN 接続にアドバタイズする内部 IP 範囲のリスト（CIDR 注記内）を収集します（静的にルーティングされた VPN 接続を使用する場合）。詳細については、「VPN のルーティングオプション (p. 140)」を参照してください。

VPC ウィザードを使用してシナリオ 3 を実装するには

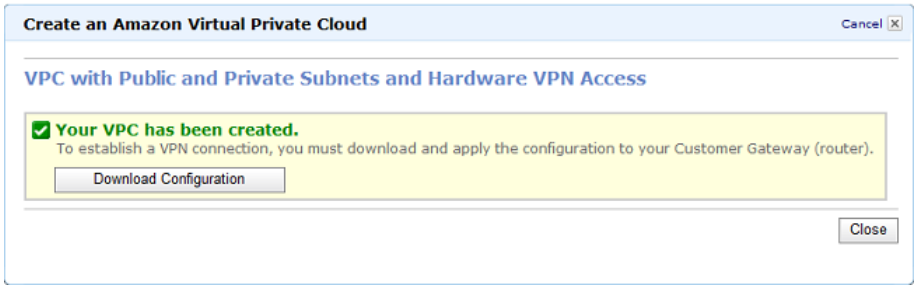
1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [VPC Dashboard] をクリックします。
3. ダッシュボードの [Your Virtual Private Cloud] 領域で、[Get started creating a VPC] をクリックします。VPC リソースがない場合は、[Start VPC Wizard] をクリックします。
4. 3 つ目のオプション [VPC with Public and Private Subnets and Hardware VPN Access] を選択し、[Continue] をクリックします。

5. [Create an Amazon Virtual Private Cloud] ダイアログボックスで、次の手順を実行し、[Continue] をクリックします。

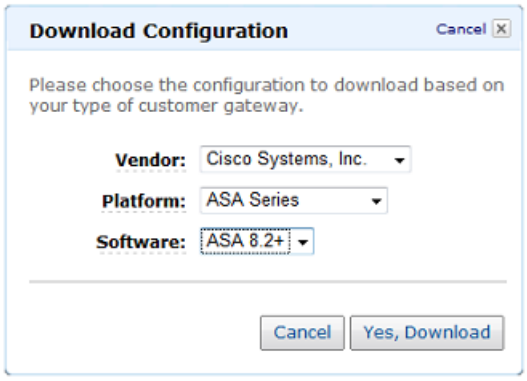
   - [IP Address] で、VPN ルーターのパブリック IP アドレスを指定します。
   - [Specify the routing for the VPN Connection] で、次のように、ルーティングオプションのいずれかを選択します。
     - VPN ルーターでボーダーゲートウェイプロトコル（BGP）がサポートされている場合は、[Use dynamic routing （requires BGP）] を選択します。
     - VPN ルーターが BGP をサポートしていない場合は、[Use static routing] をクリックします。[IP Prefix] で、ネットワークに対して各 IP プレフィックスを追加します。

   選択対象のオプションの詳細については、Amazon Virtual Private Cloud のよくある質問を参照してください。動的ルーティングと静的ルーティングの詳細については、「VPN のルーティングオプション (p. 140)」を参照してください。

6. 確認ページで情報を確認します。必要に応じて設定を変更し、[Create VPC] をクリックして、VPC、サブネット、ルートテーブル、インターネットゲートウェイ、および VPN 接続を作成します。
7. ウィザードが完了したら、確認ダイアログボックスが表示されます。このダイアログボックスには、カスタマーゲートウェイの設定をダウンロードするためのボタンが示されています。[Download Configuration] をクリックします。



8. [Download Configuration] ダイアログボックスで、カスタマーゲートウェイ、プラットフォーム、およびソフトウェアバージョンのベンダーを選択し、[Yes, Download] をクリックします。

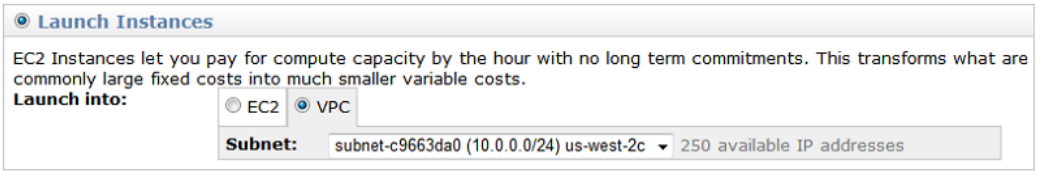


9. VPN 設定が含まれるテキストファイルを保存し、「Amazon Virtual Private Cloud Network Administrator Guide」と一緒にネットワーク管理者に提供します。VPN は、ネットワーク管理者がカスタマーゲートウェイを設定するまで動作しません。

ネットワーク管理者がカスタマーゲートウェイを設定したら、VPC 内にインスタンスを起動できます。VPC 外でのインスタンスの起動について既によくわかっている場合は、VPC 内へのインスタンスの起動に関して必要な情報は大体把握できています。

インスタンスを起動するには（ウェブサーバーまたはデータベースサーバー）

1. WebServerSG および DBServerSG セキュリティグループをまだ作成していない場合は作成します（「シナリオ 3 のセキュリティ (p. 32)」を参照）。このセキュリティグループのいずれかを、インスタンスの起動時に指定します。
2. Classic ウィザードを起動します。
   a. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
   b. ダッシュボードで [Launch Instance] ボタンをクリックします。
   c. [Create a New Instance] ページで、[Classic Wizard] を選択し、[Continue] をクリックします。
3. [CHOOSE AN AMI] ページの [Quick Start] タブに、Amazon マシンイメージ（AMI）と呼ばれる基本的な設定のリストが表示されます。使用する AMI を選択し、[Select] ボタンをクリックします。
4. [INSTANCE DETAILS] ページの [Launch Instances] で、インスタンスを起動するサブネットを選択します。例えば、パブリックサブネット内にウェブサーバーを起動し、プライベートサブネット内にデータベースサーバーを起動します。このページの他のデフォルトの設定はそのままにして、[Continue] をクリックします。



5. （オプション）デフォルトでは、デフォルトではないサブネット内に起動するインスタンスは、パブリック IP アドレスを受信しません。インスタンスへの接続を可能にするには、ここでパブリック IP アドレスを割り当てることも、Elastic IP アドレスをアロケートし、インスタンス起動後にそれをインスタンスに割り当てることもできます。現段階でパブリック IP アドレスを割り当てるには、2 番目の [INSTANCE DETAILS] ページの [Number of Network Interfaces] セクションで、[Assign Public IP] チェックボックスをオンにし、[Continue] をクリックします。

   Note

   パブリック IP アドレスは、デバイスインデックスが eth0 になっている単一の新しいネットワークインターフェイスにしか割り当てることはできません。詳細については、「起動中のパブリック IP アドレスの割り当て (p. 102)」を参照してください。

6. 次に表示される [INSTANCE DETAILS] ページでデフォルトの設定を使用するには、各ページで [Continue] をクリックするだけです。
7. [CREATE A KEY PAIR] ページで、作成済みの既存のキーペアから選択するか、ウィザードの指示にしたがって新しいキーペアを作成します。
8. [Configure Firewall] ページで、インスタンスのセキュリティグループを選択し（ウェブサーバーの場合は `WebServerSG`、データベースサーバーの場合は `DBServerSG`）、[Continue] をクリックします。
9. 設定を確認します。選択した内容でよければ、[Launch] をクリックします。

VPN のみのサブネットで実行されているインスタンスについては、ネットワークから Ping を実行して接続をテストします。詳細については、「インスタンスのエンドツーエンド接続のテスト (p. 145)」を参照してください。

手順 5 でパブリック IP アドレスをインスタンスに割り当てていない場合、インスタンスへの接続は不可能です。パブリックサブネットのインスタンスにアクセスするには、そのインスタンスに Elastic IP アドレスを割り当てておく必要があります。

To allocate an Elastic IP address and assign it to an instance

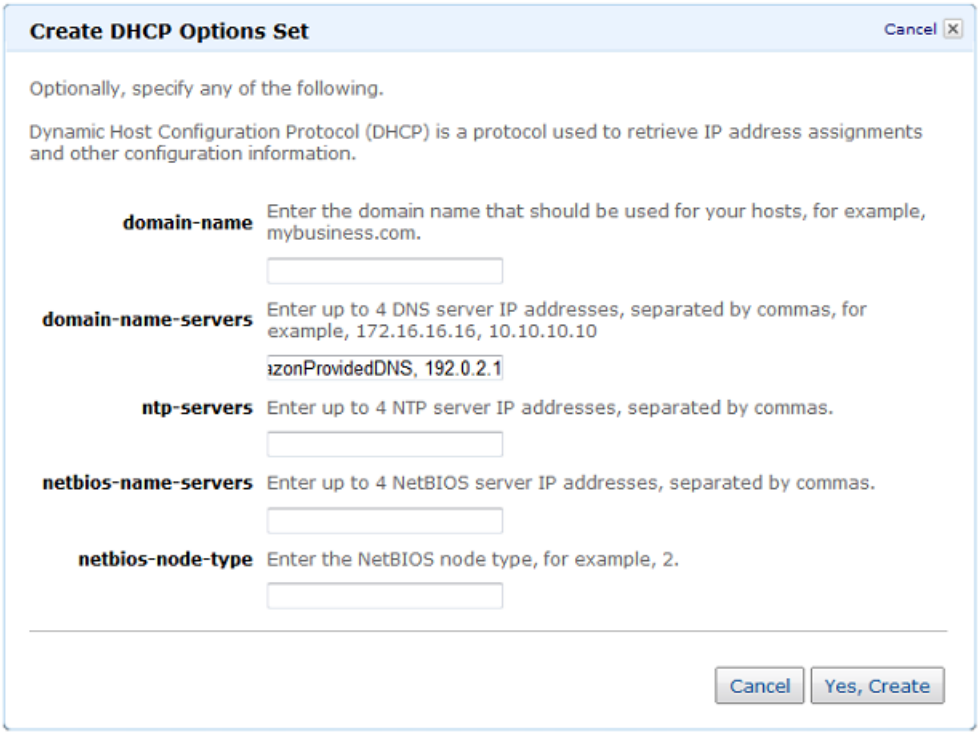
1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. Click Elastic IPs in the navigation pane.
3. Click the Allocate New Address button.
4. In the Allocate New Address dialog box, in the EIP used in list, select VPC, and then click Yes, Allocate.
5. Select the Elastic IP address from the list, and then click the Associate Address button.
6. In the Associate Address dialog box, select the network interface or instance. Select the address to associate the Elastic IP address with from the corresponding Private IP Address list, and then click Yes, Associate.

シナリオ 3 では、パブリックサブネットがインターネットのサーバーと通信できるようにする DNS サーバーが必要です。また、VPN のみのサブネットがネットワーク内のサーバーと通信できるようにする DNS サーバーも別に必要です。

VPC には、domain-name-servers=AmazonProvidedDNS を持つ DHCP オプションセットが自動的に用意されます。これは Amazon によって提供される DNS サーバーで、VPC の任意のパブリックサブネットがインターネットゲートウェイを介してインターネットと通信できるようにします。また、ご自身の DNS サーバーを提供し、VPC が使用する DNS サーバーのリストに追加する必要があります。オプションセットは変更できないので、ご自身の DNS サーバーと Amazon DNS サーバーの両方が含まれる DHCP オプションセットを作成し、この新しい DHCP オプションセットをするように VPC を更新する必要があります。

DHCP オプションを更新するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [DHCP Options Sets] をクリックします。
3. [Create DHCP Options Set] ボタンをクリックします。
4. [Create DHCP Options Set] ダイアログボックスの [domain-name-servers] ボックスで、Amazon DNS サーバー（AmazonProvidedDNS）のアドレスとご自身の DNS サーバーのアドレスをカンマで区切って指定し、[Yes, Create] をクリックします。この例ではご自身の DNS サーバーは 192.0.2.1 です。



5. ナビゲーションペインで [Your VPCs] をクリックします。
6. VPC を選択し、[Change DHCP Options Set] ボタンをクリックします。
7. [Change DHCP Options Set] ダイアログボックスで、新しいオプションセットの ID をリストから選択し、[Yes, Change] をクリックします。
8. （オプション）これで VPC が新しい DHCP オプションセットを使用するようになったので、両方の DNS サーバーにアクセスできます。VPC が使用している元のオプションセットは、必要に応じて削除できます。

これで、VPC のインスタンスに接続できるようになりました。Linux インスタンスに接続する方法については、「*Amazon Elastic Compute Cloud User Guide*」の Connect to Your Linux Instance を参照してください。Windows インスタンスに接続する方法については、「*Amazon Elastic Compute Cloud Microsoft Windows Guide*」の Connect to Your Windows Instance を参照してください。

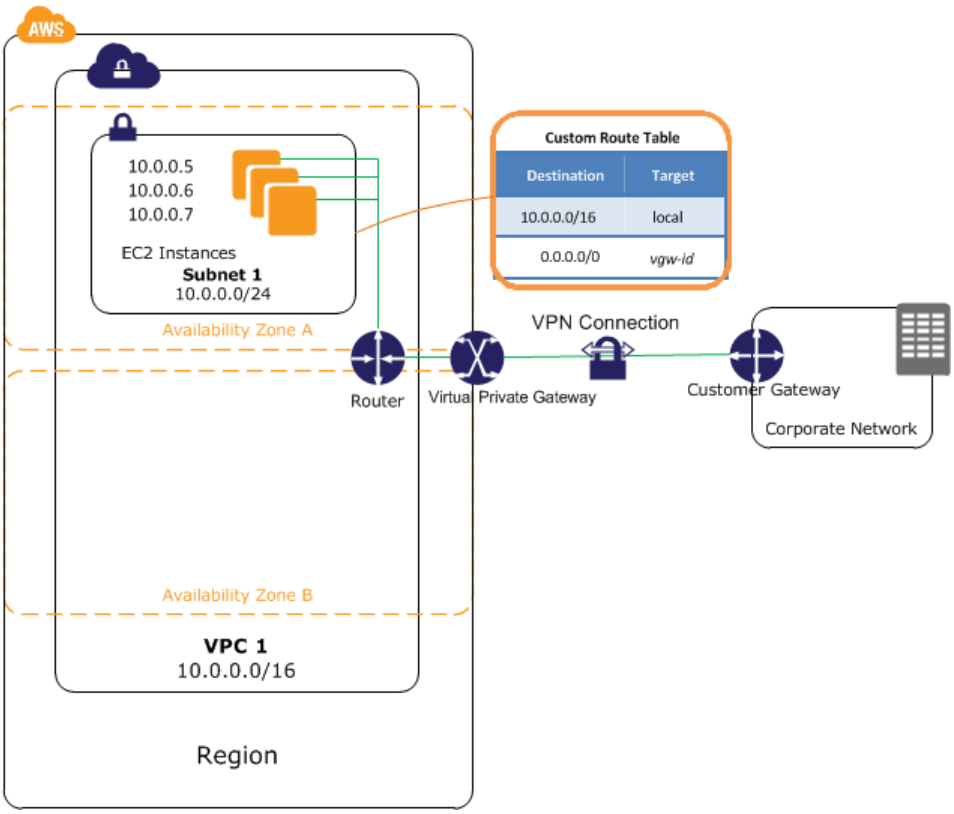
シナリオ 4: 1 つのプライベートサブネットのみ、およびハードウェア VPN アクセスを持つ VPC

このシナリオの設定には、1 つのプライベートサブネットを持つ Virtual Private Cloud（VPC）、および IPsec VPN トンネルを介した独自のネットワークとの通信を有効にする仮想プライベートゲートウェイが含まれます。インターネット経由の通信を有効にするインターネットゲートウェイはありません。このシナリオは、ネットワークをインターネットに公開せずに、Amazon のインフラストラクチャを使用してネットワークをクラウドに拡張したい場合にお勧めします。

Topics

シナリオ 4 の設定

次の図は、このシナリオの設定に重要なコンポーネントを示しています。



Important

「*Amazon Virtual Private Cloud Network Administrator Guide*」では、このシナリオに関して、ネットワーク管理者が、お客様の VPN 接続で Amazon VPC カスタマーゲートウェイを設定する際に行う必要があることを説明しています。

シナリオ 4 の基本コンポーネント

次のリストでは、このシナリオの設定図で示されている基本コンポーネントについて説明します。

- サイズ/16 (サンプル CIDR: 10.0.0.0/16) の Virtual Private Cloud (VPC) 。65,536 個のプライベート IP アドレスを提供します。
- サイズ/24 (サンプル CIDR: 10.0.0.0/24) の VPN のみのサブネット。256 個のプライベート IP アドレスを提供します。
- VPC とネットワークの間の VPN 接続。この VPN 接続は、仮想プライベートゲートウェイとカスタマーゲートウェイで構成され、前者は VPN 接続の Amazon 側、後者はお客様側に配置されています。

- サブネット範囲のプライベート IP アドレス (例: 10.0.0.5、10.0.0.6、および 10.0.0.7) を持つインスタンス。そのインスタンスが VPC 内で相互に、および他のインスタンスと通信できるようにします。
- サブネットのインスタンスが VPC 内の他のインスタンスと通信できるようにするルートテーブルエントリと、サブネットのインスタンスがネットワークと直接通信できるようにするルートテーブルエントリ。

サブネットの詳細については、「VPC とサブネット (p. 52)」および「VPC の IP アドレス指定 (p. 101)」を参照してください。VPN 接続の詳細については、「VPC へのハードウェア仮想プライベートゲートウェイの追加 (p. 137)」を参照してください。カスタマーゲートウェイの設定の詳細については、「*Amazon Virtual Private Cloud Network Administrator Guide*」を参照してください。

シナリオ 4 のルーティング

VPC には暗示的なルーターがあります (このシナリオの設定図を参照)。このシナリオでは、VPC ウィザードによって、送信先が VPC 外のアドレスであるトラフィックすべてを VPN 接続にルーティングするルートテーブルを作成し、それをサブネットに関連付けます。これを行わない場合は、ご自身でルートテーブルを作成し、関連付ける必要があります。

次の表は、このシナリオの設定図で使用されているサンプルアドレスが、ルートテーブルではどのように表示されるかを示しています。1 行目は、VPC のローカルルーティングのエントリを示しています。このエントリによって、この VPC 内のインスタンスが相互に通信できるようになります。2 行目は、他のすべてのサブネットトラフィックを仮想プライベートゲートウェイにルーティングするエントリを示しています。これは、AWS によって割り当てられた識別子 (`vgw-1a2b3c4d` など) を使用して指定されます。

送信先	ターゲット
10.0.0.0/16	ローカル
0.0.0.0/0	vgw-*xxxxxxxx*

VPN 接続は、静的にルーティングされた VPN 接続または動的にルーティングされた VPN 接続 (BGP を使用) のいずれかとして設定されます。静的なルーティングを選択すると、VPN 接続を作成するときに、ネットワークの IP プレフィックスを手動で入力するように求められます。動的なルーティングを選択すると、IP プレフィックスは、BGP を使用して VPC に自動的にアドバタイズされます。

VPN のインスタンスはインターネットに直接接続することはできません。インターネットあてのトラフィックはすべて、まず仮想プライベートゲートウェイを経由してネットワークに向かいます。そこでは、ファイアウォールと企業のセキュリティポリシーが適用されます。インスタンスが AWS 宛てのトラフィック (Amazon S3 または Amazon EC2 へのリクエストなど) を送信する場合、リクエストは仮想プライベートゲートウェイを介してネットワークに向かい、AWS に到達する前にインターネットに達する必要があります。

シナリオ 4 のセキュリティ

AWS provides two features that you can use to increase security in your VPC: *security groups* and *network ACLs*. Both features enable you to control the inbound and outbound traffic for your instances, but security groups work at the instance level, while network ACLs work at the subnet level. Security groups alone can meet the needs of many VPC users. However, some VPC users decide to use both security groups and network ACLs to take advantage of the additional layer of security that network ACLs provide. For more information about security groups and network ACLs and how they differ, see VPC のセキュリティ (p. 68).

シナリオ 4 では、VPC に対してデフォルトのセキュリティグループを使用します。ネットワーク ACL は使用しません。

推奨セキュリティグループのルール

VPC に用意されているデフォルトのセキュリティグループの初期設定では、すべてのインバウンドトラフィックが拒否され、すべてのアウトバウンドトラフィックと、セキュリティグループに割り当てられているインスタンス間のすべてのトラフィックが許可されます。デフォルトのセキュリティグループにインバウンドルールを追加して、ネットワークからの SSH トラフィック (Linux) とリモートデスクトップトラフィック (Windows) を許可するためことをお勧めします。

Important

デフォルトのセキュリティグループでは、割り当てられたインスタンスが相互に通信するように自動的に許可されます。したがって、これを許可するためのルールを追加する必要はありません。異なるセキュリティグループを使用する場合は、これを許可するためのルールを追加する必要があります。

次の表では、VPC のデフォルトのセキュリティグループに追加する必要があるインバウンドルールについて説明します。

デフォルトのセキュリティグループ: 推奨ルール

インバウンド			
送信元	プロトコル	ポート範囲	コメント
ネットワークのプライベート IP アドレスの範囲	TCP	22	(Linux インスタンス) ネットワークからのインバウンド SSH トラフィックを許可する
ネットワークのプライベート IP アドレスの範囲	TCP	3389	(Windows インスタンス) ネットワークからのインバウンド RDP トラフィックを許可する

シナリオ 4 を実装する

次のプロセスにしたがって、VPC ウィザードを使用してシナリオ 4 を実装します。

カスタマーゲートウェイを準備するには

1. カスタマーゲートウェイとして使用するアプライアンスを特定します。テストしたデバイスのリストについては、Amazon Virtual Private Cloud のよくある質問を参照してください。カスタマーゲートウェイの要件の詳細については、「*Amazon Virtual Private Cloud Network Administrator Guide*」を参照してください。
2. カスタマーゲートウェイの外部インターフェイスのインターネットルーティングが可能な IP アドレスを取得します。このアドレスは静的である必要があります。また、ネットワークアドレス変換 (NAT) を実行するデバイスの背後のアドレスを使用することはできません。
3. 仮想プライベートゲートウェイへの VPN 接続にアドバタイズする内部 IP 範囲のリスト (CIDR 注記内) を収集します (静的にルーティングされた VPN 接続を使用する場合)。詳細については、「VPN のルーティングオプション (p. 140)」を参照してください。

次に、次の手順で説明する VPC ウィザードを使用して、VPC と VPN 接続を作成します。

VPC ウィザードを使用してシナリオ 4 を実装するには

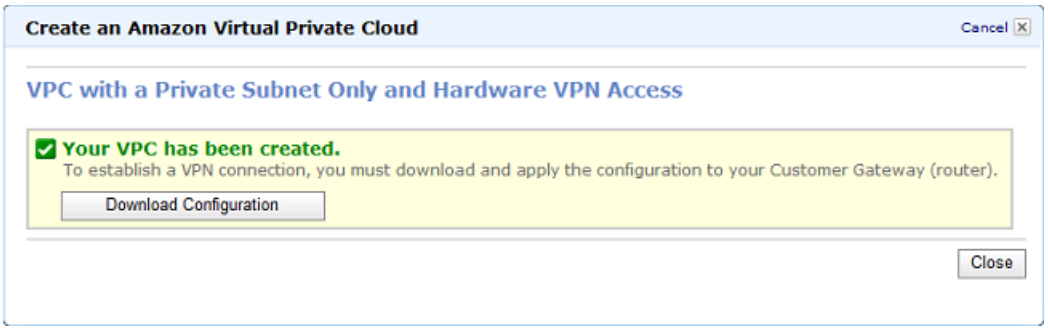
1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [VPC Dashboard] をクリックします。
3. ダッシュボードの [Your Virtual Private Cloud] 領域で、[Get started creating a VPC] をクリックします。VPC リソースがない場合は、[Start VPC Wizard] をクリックします。
4. 4 つ目のオプション [VPC with a Private Subnet Only and Hardware VPN Access] を選択し、[Continue] をクリックします。

5. [Create an Amazon Virtual Private Cloud] ダイアログボックスで、次の手順を実行し、[Continue] をクリックします。

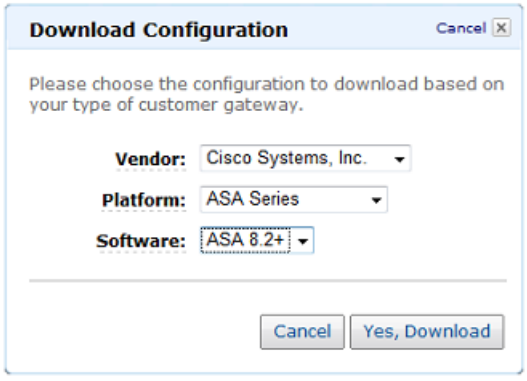
   - [IP Address] で、VPN ルーターのパブリック IP アドレスを指定します。
   - [Specify the routing for the VPN Connection] で、次のように、ルーティングオプションのいずれかを選択します。
     - VPN ルーターでボーダーゲートウェイプロトコル (BGP) がサポートされている場合は、[Use dynamic routing （ requires BGP)] を選択します。
     - VPN ルーターが BGP をサポートしていない場合は、[Use static routing] を選択します。[IP Prefix] で、ネットワークに対して各 IP プレフィックスを追加します。

   選択対象のオプションの詳細については、Amazon Virtual Private Cloud のよくある質問を参照してください。動的ルーティングと静的ルーティングの詳細については、「VPN のルーティングオプション (p. 140)」を参照してください。

6. 確認ページで情報を確認します。必要に応じて設定を変更し、[Create VPC] をクリックして、VPC、サブネット、ルートテーブル、および VPN 接続を作成します。
7. ウィザードが完了したら、確認ダイアログボックスが表示されます。このダイアログボックスには、カスタマーゲートウェイの設定をダウンロードするためのボタンが示されています。[Download Configuration] をクリックします。



8. [Download Configuration] ダイアログボックスで、カスタマーゲートウェイ、プラットフォーム、およびソフトウェアバージョンのベンダーを選択し、[Yes, Download] をクリックします。



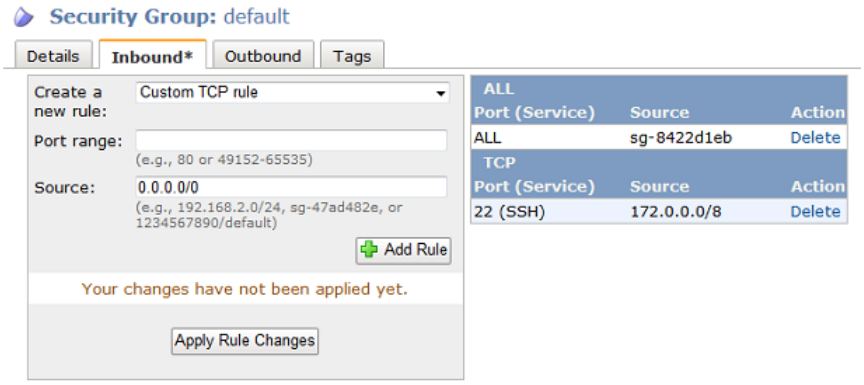
9. VPN 設定が含まれるテキストファイルを保存し、「*Amazon Virtual Private Cloud Network Administrator Guide*」と一緒にネットワーク管理者に提供します。VPN は、ネットワーク管理者がカスタマーゲートウェイを設定するまで動作しません。

このシナリオでは、ネットワークからの SSH およびリモートデスクトップ (RDP) アクセスを許可する新しいインバウンドルールで、デフォルトのセキュリティグループを更新する必要があります。インスタンスがアウトバウンド通信を開始しない場合、デフォルトのアウトバウンドルールを削除することができます。注意: デフォルトのセキュリティグループの初期設定では、すべてのインバウンドトラフィックがブロックされ、すべてのアウトバウンドトラフィックが許可されます。また、そのグループに割り当てられているインスタンスが相互に通信できます。

デフォルトのセキュリティグループのルールを更新するには

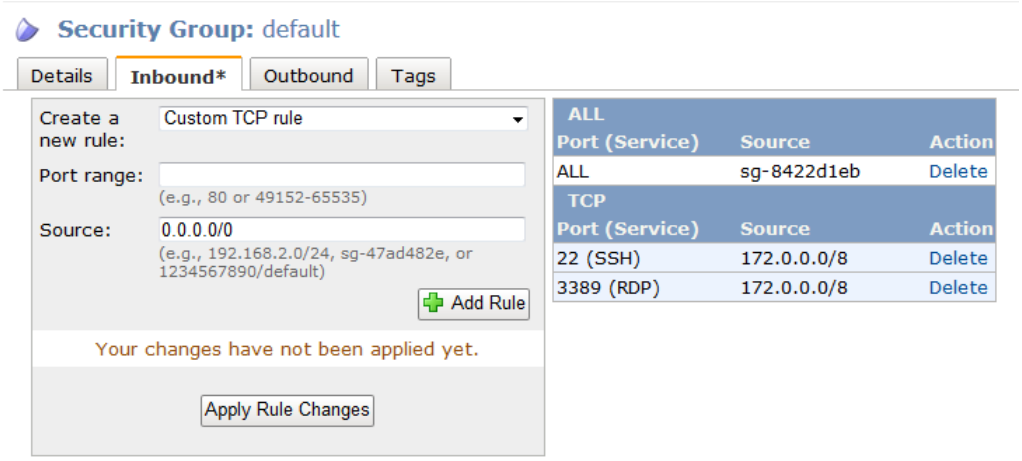
1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Security Groups] をクリックし、VPC のデフォルトのセキュリティグループを選択します。詳細ペインに、セキュリティグループの詳細と、インバウンドルールおよびアウトバウンドルールを操作するためのタブが表示されます。
3. ネットワークからグループへアクセスするインバウンド SSH のルールを追加します。

   a. [Inbound] タブで、[Create a new rule] ドロップダウンリストから SSH を選択します。
   b. [Source] ボックスに、ネットワークのプライベート IP アドレス範囲を入力します。
   c. [Add Rule] をクリックします。
   ルールは [Inbound] タブに追加されます。ただし、[Apply Rule Changes] をクリックするまでグループには適用されません (この作業は、すべてのインバウンドルールを追加してから行います) 。



4. ネットワークからグループへのインバウンド RDP アクセスのルールを追加します。

   a. [Inbound] タブで、[Create a new rule] ドロップダウンリストから RDP を選択します。
   b. [Source] ボックスに、ネットワークのプライベート IP アドレス範囲を入力します。
   c. [Add Rule] をクリックします。

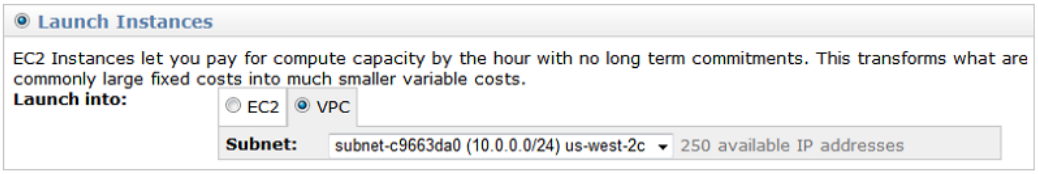


5. [Apply Rule Changes] をクリックします。
6. [Outbound] タブで、すべてのアウトバウンドトラフィックを有効にするデフォルトルールを検索し、[Delete] をクリックして、[Apply Rule Changes] をクリックします。

ネットワーク管理者がカスタマーゲートウェイを設定したら、VPC 内にインスタンスを起動できます。VPC 外でのインスタンスの起動について既によくわかっている場合は、VPC 内へのインスタンスの起動に関して必要な情報は大体把握できています。

インスタンスを起動するには

1. Classic ウィザードを起動します。
   a. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
   b. ダッシュボードで [Launch Instance] ボタンをクリックします。
   c. [Create a New Instance] 画面で、[Classic Wizard] を選択し、[Continue] をクリックします。
2. [CHOOSE AN AMI] ページの [Quick Start] タブに、Amazon マシンイメージ (AMI) と呼ばれる基本的な設定のリストが表示されます。使用する AMI を選択し、[Select] ボタンをクリックします。
3. [INSTANCE DETAILS] ページの [Launch Instances] で、インスタンスを起動するサブネットを選択します。このページの他のデフォルトの設定はそのままにして、[Continue] をクリックします。



4. 次に表示される [INSTANCE DETAILS] 数ページでデフォルトの設定を使用するには、各ページで [Continue] をクリックするだけです。
5. [CREATE A KEY PAIR] ページで、作成済みの既存のキーペアから選択するか、ウィザードの指示にしたがって新しいキーペアを作成します。
6. [CONFIGURE FIREWALL] ページで、デフォルトのセキュリティグループを選択し、[Continue] をクリックします。
7. 設定を確認します。選択した内容でよければ、[Launch] をクリックします。

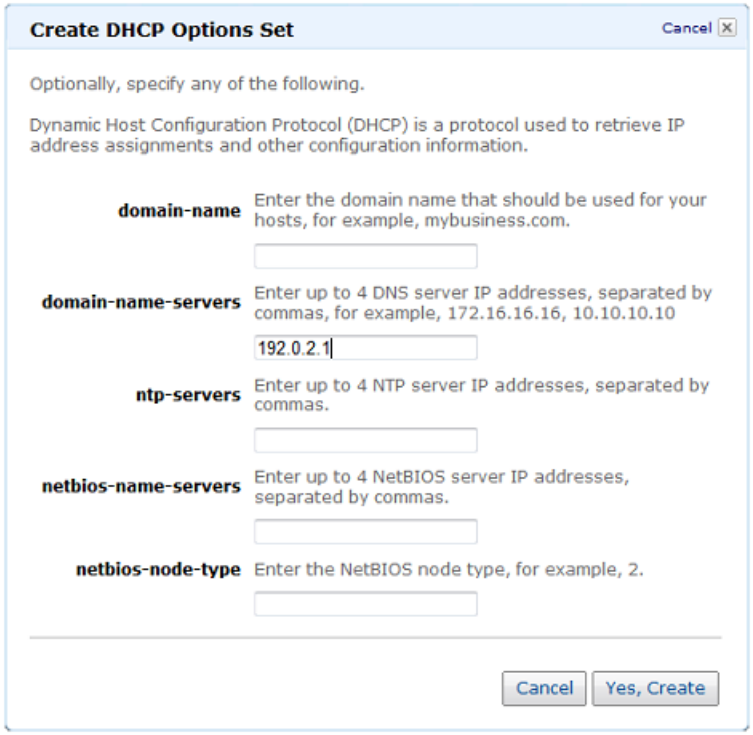
シナリオ 4 では、VPN のみのサブネットがネットワークのサーバーと通信できるようにする DNS サーバーが必要です。ご自身の DNS サーバーが含まれる DHCP オプションセットを新しく作成し、そのオプションセットを使用するように VPC を設定する必要があります。

Note

VPC には、domain-name-servers=AmazonProvidedDNS を持つ DHCP オプションセットが自動的に用意されます。これは Amazon によって提供される DNS サーバーで、VPC の任意のパブリックサブネットがインターネットゲートウェイを介してインターネットと通信できるようにします。シナリオ 4 では、パブリックサブネットは使用しないので、この DHCP オプションセットは必要ありません。

DHCP オプションを更新するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [DHCP Options Sets] をクリックします。
3. [Create DHCP Options Set] ボタンをクリックします。
4. [Create DHCP Options Set] ダイアログボックスの [domain-name-servers] ボックスに、ご自身の DNS サーバーのアドレスを入力し、[Yes, Create] をクリックします。この例ではご自身の DNS サーバーは 192.0.2.1 です。



5. ナビゲーションペインで [Your VPCs] をクリックします。
6. VPC を選択し、[Change DHCP Options Set] ボタンをクリックします。
7. [Change DHCP Options Set] ダイアログボックスで、新しいオプションセットの ID をリストから選択し、[Yes, Change] をクリックします。
8. （オプション）これで VPC は新しい DHCP オプションセットを使用するようになりました。したがって VPC では DNS サーバーが使用されます。VPC が使用している元のオプションセットは、必要に応じて削除できます。

これで SSH または RDP を使用して、VPC のインスタンスに接続できるようになりました。Linux インスタンスに接続する方法については、「*Amazon Elastic Compute Cloud User Guide*」の Connect to Your Linux Instance を参照してください。Windows インスタンスに接続する方法については、「*Amazon Elastic Compute Cloud Microsoft Windows Guide*」の Connect to Your Windows Instance を参照してください。

VPC とサブネット

Amazon Virtual Private Cloud (Amazon VPC) の使用を開始するには、VPC およびサブネットを作成します。VPC とサブネットの概要については、「Amazon VPC とは (p. 1)」を参照してください。

Topics
- VPC (p. 52)
- VPC のサブネット (p. 56)

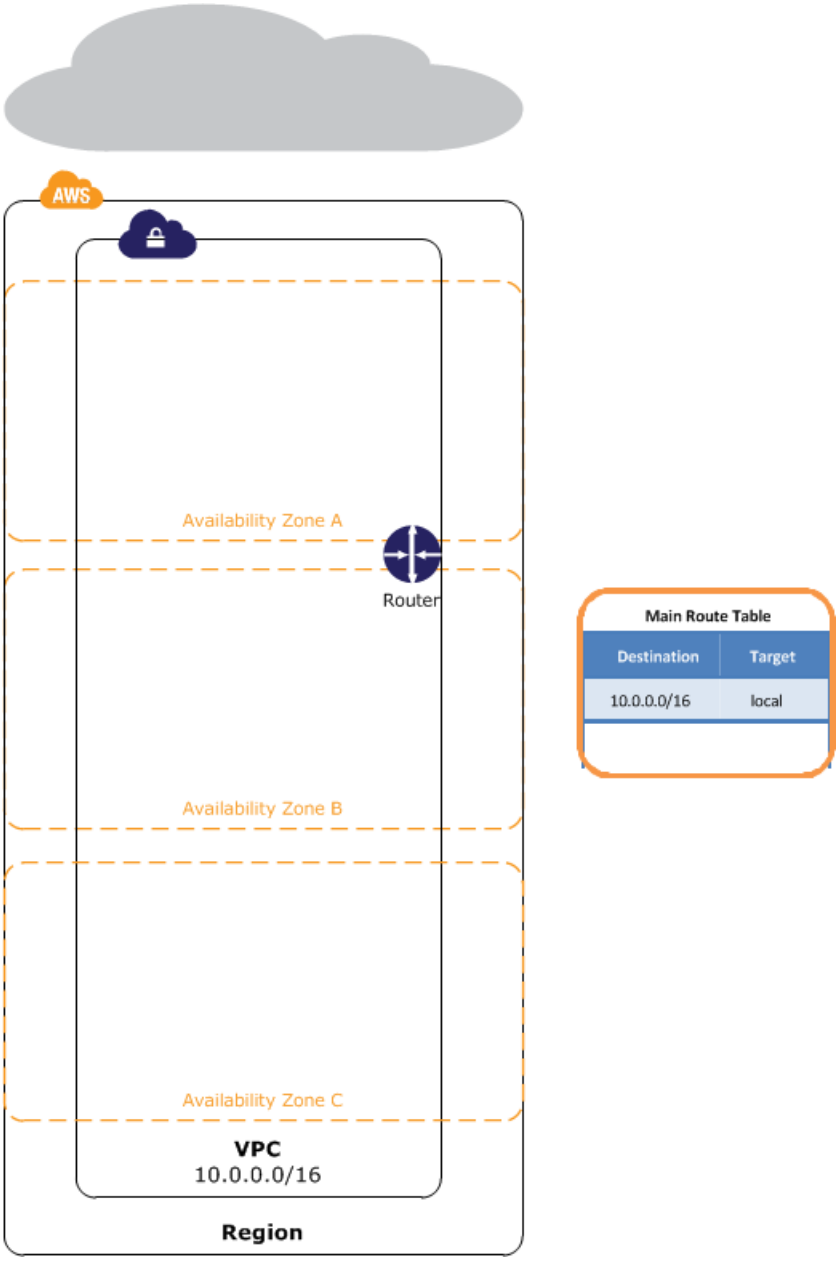
VPC

VPC を作成するときに、その VPC に対して、一連の IP アドレスを Classless Inter-Domain Routing (CIDR) ブロックの形式で指定します (例: `10.0.0.0/16`)。CIDR 表記と「`/16`」の意味について詳しくは、Wikipedia の Classless Inter-Domain Routing を参照してください。

Topics
- 新しい VPC (p. 52)
- VPC のサイズ設定 (p. 53)
- VPC と企業またはホームネットワークの間の接続 (p. 54)
- VPC を作成する (p. 54)
- VPC を削除する (p. 55)

新しい VPC

次の図は、デフォルトのルートテーブルを持つ新しい VPC を示します。



VPC 内にインスタンスを起動する前に、サブネットを追加しておく必要があります。

VPC のサイズ設定

1 つの CIDR ブロックを VPC に割り当てることができます。許可されているのは、/28 ネットマスクから /16 ネットマスクの間のブロックサイズです。つまり、VPC には 16 ~ 65,536 個の IP アドレスを含めることができます。一度作成した VPC のサイズは変更できません。VPC のサイズが小さすぎてニーズに対応できない場合は、VPC 内のすべてのインスタンスを終了し、その VPC を削除してから、大きな VPC を新しく作成する必要があります。詳細については、「VPC を削除する (p. 55)」を参照してください。

VPC と企業またはホームネットワークの間の接続

オプションで、VPC と企業またはホームネットワークの間の接続を設定できます。VPC 内に、ネットワークのプレフィックスの 1 つと重複する IP アドレスプレフィックスがある場合、そのネットワークのプレフィックスへのトラフィックはドロップされます。例えば、次の環境があるとします。

- CIDR ブロック `10.0.0.0/16` を持つ VPC
- CIDR ブロック `10.0.1.0/24` を持つ VPC 内のサブネット
- IP アドレス `10.0.1.4` と `10.0.1.5` を持つサブネットで実行されているインスタンス
- CIDR ブロック `10.0.37.0/24` と `10.1.38.0/24` が使用されているオンプレミスホストネットワーク

VPC 内のこれらのインスタンスが、`10.0.37.0/24` アドレス空間のホストと通信しようとすると、そのトラフィックはドロップされます。これは、`10.0.37.0/24` が、VPC に割り当てられている、より大きなプレフィックス (`10.0.0.0/16`) の一部だからです。一方、`10.1.38.0/24` 空間のホストとは通信できます。そのブロックは `10.0.0.0/16` の一部ではないからです。

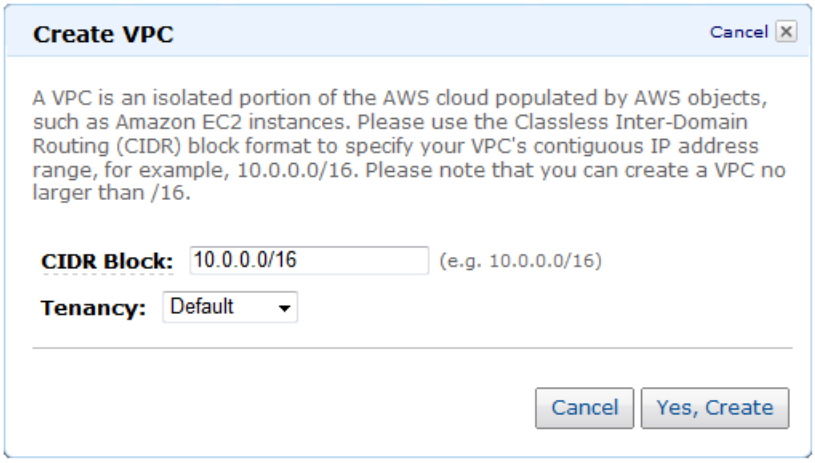
したがって、作成する VPC の CIDR 範囲は、今後予想される拡大に十分に対応でき、かつ企業またはホームネットワークにある現在または今後のどのサブネットとも重複しないようにすることをお勧めします。

VPC を作成する

Amazon VPC コンソールを使用して VPC を作成するには、[Create VPC] ダイアログボックスか VPC ウィザードを使用します。次の手順では、[Create VPC] ダイアログボックスを使用して VPC のみを作成します。その後、サブネット、ゲートウェイ、およびルーティングテーブルを追加する必要があります。VPC ウィザードを使用して VPC と、そのサブネット、ゲートウェイ、およびルーティングテーブルを一度に作成する方法については、「Amazon VPC の利用シナリオ (p. 8)」を参照してください。

VPC を作成するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Your VPCs] をクリックします。
3. [Create VPC] をクリックします。
4. [Create VPC] ダイアログボックスで、必要に応じて以下の VPC の詳細を指定し、[Yes, Create] をクリックします。
   - VPC の CIDR ブロックを指定します。
   - テナント属性オプションを選択します (例えば、シングルテナントのハードウェアでインスタンスが確実に動作するように保証する専用のテナント属性) 。ハードウェア専有のインスタンスの詳細については、「EC2 ハードウェア専有インスタンスの使用 (p. 152)」を参照してください。



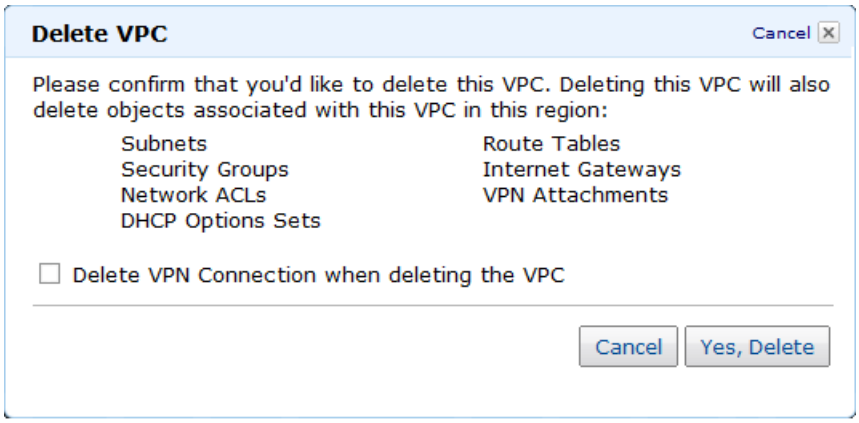
VPC を削除する

VPC はいつでも削除できます (VPC が小さすぎる場合など) 。ただし、まず、VPC 内のすべてのインスタンスを終了する必要があります。VPC を削除すると、VPC のすべてのコンポーネント (サブネット、セキュリティグループ、ネットワーク ACL、ルートテーブル、インターネットゲートウェイ、DHCP オプション) が削除されます。

VPN 接続がある場合、その接続または VPN に関連する他のコンポーネント (カスタマーゲートウェイ、仮想プライベートゲートウェイなど) を削除する必要はありません。他の VPC でカスタマーゲートウェイを使用する予定がある場合は、VPN 接続とゲートウェイは保持することをお勧めします。それ以外の場合、VPN 接続を新しく作成したら、ネットワーク管理者がカスタマーゲートウェイを設定する必要があります。

VPC を削除するには

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. VPC のすべてのインスタンスを終了します。
3. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
4. ナビゲーションペインで [Your VPCs] をクリックします。
5. 削除する VPC を選択し、[Delete] をクリックします。
6. VPN 接続を削除する必要がある場合は、それを行うオプションを選択します。それ以外の場合、そのオプションはオフのままにしておきます。[Yes, Delete] をクリックします。



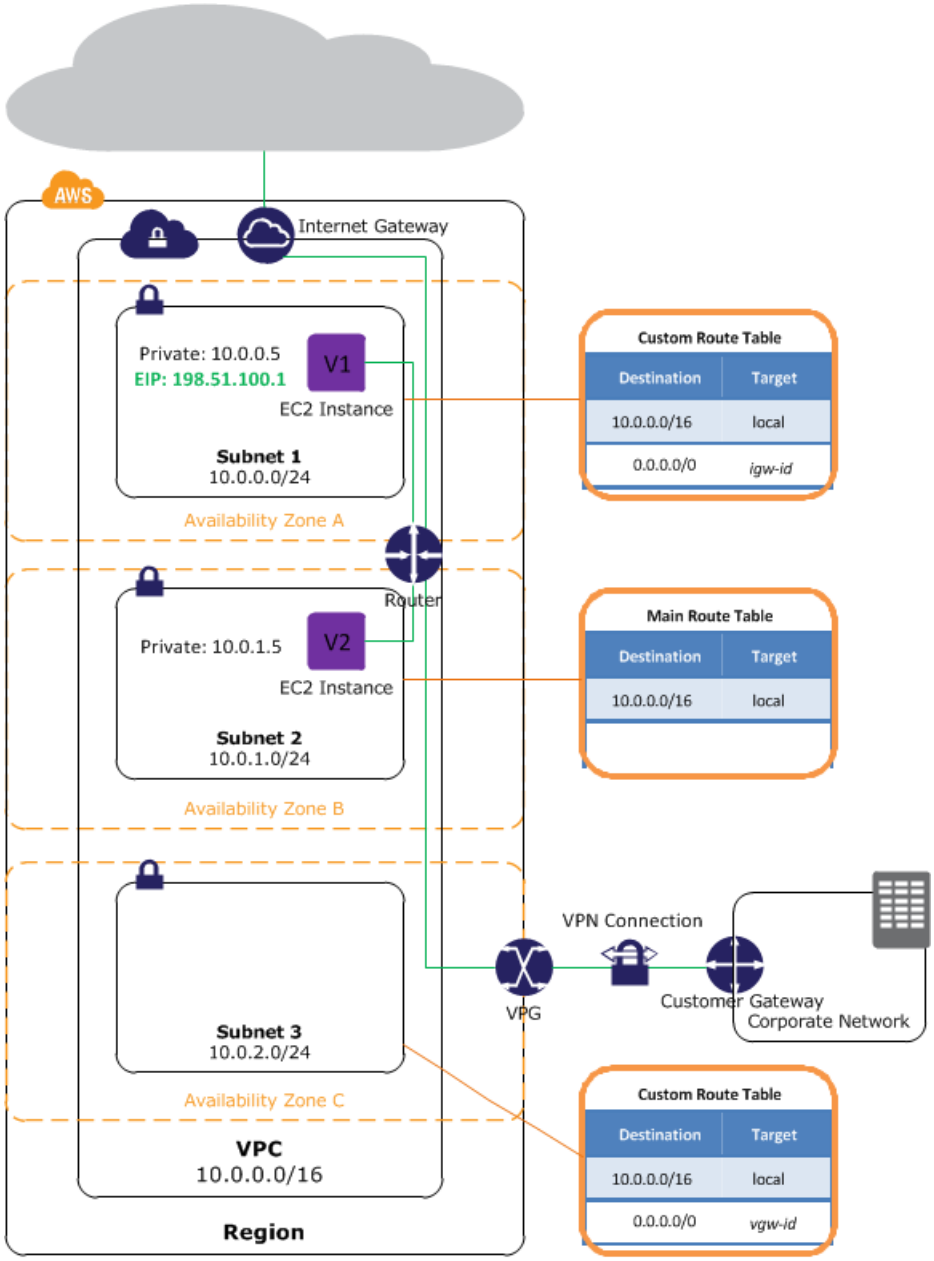
VPC のサブネット

複数のアベイラビリティーゾーンにまたがる VPC を作成できます。詳細については、「VPC を作成する (p. 54)」を参照してください。VPC を作成したら、アベイラビリティーゾーンごとに 1 つ以上のサブネットを追加します。各サブネットが完全に 1 つのアベイラビリティーゾーン内に含まれている必要があります。1 つのサブネットが複数のゾーンにまたがることはできません。アベイラビリティゾーンとは、他のアベイラビリティーゾーンで発生した障害から切り離すために作られた場所です。個別のアベイラビリティーゾーンでインスタンスを起動することにより、1 つの場所で発生した障害からアプリケーションを保護できます。AWS では、各サブネットに固有の ID が割り当てられます。

Topics

サブネットを持つ VPC

次の図は、複数のアベイラビリティーゾーンにある複数のサブネットで設定された VPC を示しています。オプションとして、インターネットゲートウェイを追加してインターネットによる通信を有効にしたり、仮想プライベートネットワーク (VPN) 接続を追加してご使用のネットワークとの通信を有効にしたりできます。詳細については「Amazon VPC の利用シナリオ (p. 8)」、「インターネットゲートウェイを VPC に追加する (p. 117)」または「VPC へのハードウェア仮想プライベートゲートウェイの追加 (p. 137)」をご参照ください。



サブネットのサイズ設定

サブネットを作成するときに、そのサブネットの CIDR ブロックを指定します。サブネットの CIDR ブロックは、VPC のサブネットが 1 つの場合、VPC の CIDR ブロックと同じにすることも、あるいは複数のサブネットを有効にするサブネットと同じにすることもできます。VPC に複数のサブネットを作成する場合、サブネットの CIDR ブロックは重複してはいけません。

例えば、CIDR ブロック `10.0.0.0/24` を持つ VPC を作成した場合、その VPC では 256 個の IP アドレスがサポートされます。この CIDR ブロックは 2 つのサブネットに分割でき、それぞれのサブネットで 128 個の IP アドレスがサポートされています。一方のサブネットでは CIDR ブロック `10.0.0.0/25` (アドレス `10.0.0.0` ~ `10.0.0.127`) が、もう一方のサブネットでは CIDR ブロック `10.0.0.128/25` (アドレス `10.0.0.128` ~ `10.0.0.255`) が使用されます。

Important

各サブネットの CIDR ブロック内にある IP アドレスのうち、最初の 4 個と最後の 1 個は両方とも AWS によって予約されています。これらのアドレスをユーザーが使用することはできません。

サブネット CIDR ブロックの計算に役立つツールは多数あります。よく使用されるツールについては、http://www.subnet-calculator.com/cidr.php を参照してください。また、ネットワーク技術グループが、サブネットに指定する CIDR ブロックを特定することもできます。

サブネットのルーティング

設計上、各サブネットをルートテーブルに関連付ける必要があります。サブネットを出るアウトバウンドトラフィックに対して許可されるルートは、このテーブルによって指定されます。作成するすべてのサブネットが、VPC のメインルートテーブルに自動的に関連付けられます。この関連付けを変更し、メインルートテーブルのコンテンツを変更できます。詳細については、「ルートテーブル (p. 106)」を参照してください。

サブネットのトラフィックがインターネットゲートウェイにルーティングされる場合、そのサブネットは*パブリックサブネット*と呼ばれます。前の図では、サブネット 1 がパブリックサブネットです。サブネット 1 に関連付けられたルートテーブルは、すべてのトラフィック (`0.0.0.0/0`) をインターネットゲートウェイ (例: `igw-1a2b3c4d`) にルーティングします。インスタンス V1 には Elastic IP アドレスがあるのため、インターネットからアクセスできます。

インターネットゲートウェイへのルートがないサブネットは、*プライベートサブネット*と呼ばれます。前の図では、サブネット 2 がプライベートサブネットです。インスタンス V2 はインターネットにアクセスできませんが、VPC の他のインスタンスにはアクセスできます。ネットワークアドレス変換 (NAT) インスタンスを使用して、VPC のインスタンスによるインターネットへのアウトバウンド接続の開始を許可し、インターネットからの未承諾のインバウンド接続を拒否できます。Elastic IP アドレスは限られた数しかアロケートできないため、静的なパブリック IP アドレスを必要とするインスタンスが多く存在する場合は、NAT インスタンスの使用をお勧めします。詳細については、「NAT インスタンス (p. 122)」を参照してください。

インターネットゲートウェイへのルートがなく、トラフィックが仮想プライベートゲートウェイにルーティングされているサブネットは、*VPN のみのサブネット*と呼ばれます。前の図では、サブネット 3 が VPN のみのサブネットです。サブネット 3 に関連付けられたルートテーブルは、すべてのトラフィック (`0.0.0.0/0`) を仮想プライベートゲートウェイ (例: `vgw-1a2b3c4d`) にルーティングします。

サブネットのセキュリティ

AWS provides two features that you can use to increase security in your VPC: *security groups* and *network ACLs*. Both features enable you to control the inbound and outbound traffic for your instances, but security groups work at the instance level, while network ACLs work at the subnet level. Security groups alone can meet the needs of many VPC users. However, some VPC users decide to use both security groups and network ACLs to take advantage of the additional layer of security that network ACLs provide. For more information about security groups and network ACLs and how they differ, see VPC のセキュリティ (p. 68).

設計により、各サブネットをネットワーク ACL に関連付ける必要があります。作成するサブネットはすべて、VPC のデフォルトのネットワーク ACL に自動的に関連付けられます。この関連付けを変更し、デフォルトのネットワーク ACL のコンテンツを変更できます。詳細については、「ネットワーク ACL (p. 77)」を参照してください。

サブネットを VPC に追加する

新しいサブネットを VPC に追加するとき、サブネットに必要なルーティングとセキュリティを設定する必要があります。この作業は、このセクションで説明するように手動で行うことも、「Amazon VPC の利用シナリオ (p. 8)」で説明するように VPC ウィザードで設定することもできます。

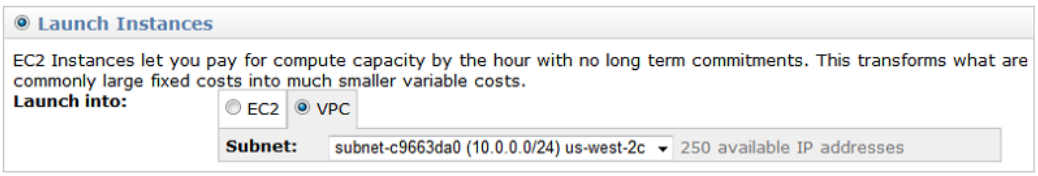
サブネットを VPC に追加するには

1. サブネットを作成します。
   a. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
   b. ナビゲーションペインで [Subnets] をクリックします。
   c. [Create Subnet] をクリックします。
   d. [Create Subnet] ダイアログボックスで [VPC] を選択し、[アベイラビリティーゾーン] を選択し、サブネットの CIDR 範囲を指定してから、[Yes, Create] をクリックします。
2. サブネットのルーティングを設定します。例えば、インターネットゲートウェイまたは NAT インスタンスへのルートを追加できます。詳細については、「ルートテーブル (p. 106)」を参照してください。
3. （オプション）必要に応じて、セキュリティグループを作成または変更します。詳細については、「VPC のセキュリティグループ (p. 70)」を参照してください。
4. （オプション）必要に応じて、ネットワーク ACL を作成または変更します。ネットワーク ACL の詳細については、「ネットワーク ACL (p. 77)」を参照してください。

サブネット内にインスタンスを起動する

サブネット内にインスタンスを起動するには

1. Classic ウィザードを起動します。
   a. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
   b. ダッシュボードで、[Launch Instance] をクリックします。
   c. [Create a New Instance] ページで、[Classic Wizard] を選択し、[Continue] をクリックします。
2. [CHOOSE AN AMI] ページの [Quick Start] タブに、Amazon マシンイメージ（AMI）と呼ばれる基本的な設定のリストが表示されます。使用する AMI を選択し、その [Select] ボタンをクリックします。
3. [INSTANCE DETAILS] ページの [Launch Instances] で、インスタンスを起動するサブネットを選択します。このページの他のデフォルトの設定はそのままにして、[Continue] をクリックします。



4. 次に表示される [INSTANCE DETAILS] 数ページでデフォルトの設定を使用するには、各ページで [Continue] をクリックします。
5. [CREATE A KEY PAIR] ページで、作成済みの既存のキーペアから選択するか、ウィザードの指示にしたがって新しいキーペアを作成します。

6. [Configure Firewall] ページで、所有する既存のセキュリティグループから選択するか、ウィザードの指示にしたがって新しいセキュリティグループを作成します。
7. 設定を確認します。選択した内容でよければ、[Launch] をクリックします。

サブネットを削除する

サブネット内にインスタンスが存在する場合はそれをまず終了する必要があります。

サブネットを削除するには

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. サブネットのすべてのインスタンスを終了します。
3. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
4. ナビゲーションペインで [Subnets] をクリックします。
5. 削除するサブネットを選択し、[Delete] をクリックします。
6. [Delete Subnet] ダイアログボックスで、[Yes, Delete] をクリックします。

デフォルトの VPC とサブネット

デフォルトの VPC は、EC2-VPC プラットフォームの高度なネットワーキング機能と EC2-Classic プラットフォームの使いやすさのメリットを兼ね備えています。

EC2-Classic プラットフォームと EC2-VPC プラットフォームの詳細については、「サポートされているプラットフォーム」を参照してください。

Topics

デフォルトの VPC の基本

このセクションでは、デフォルトの Virtual Private Cloud (VPC) とそのデフォルトのサブネットについて説明します。

可用性

AWS アカウントの各リージョンがサポートするプラットフォームを確認する場合は、「サポートされているプラットフォームとデフォルト VPC があるかどうかを確認する (p. 63)」を参照してください。

AWS アカウントが EC2-VPC しかサポートされていない場合は、その AWS アカウントに関連付けられている IAM アカウントも EC2-VPC しかサポートされません。また、この IAM アカウントでは、AWS アカウントと同じデフォルトの VPC が使用されます。

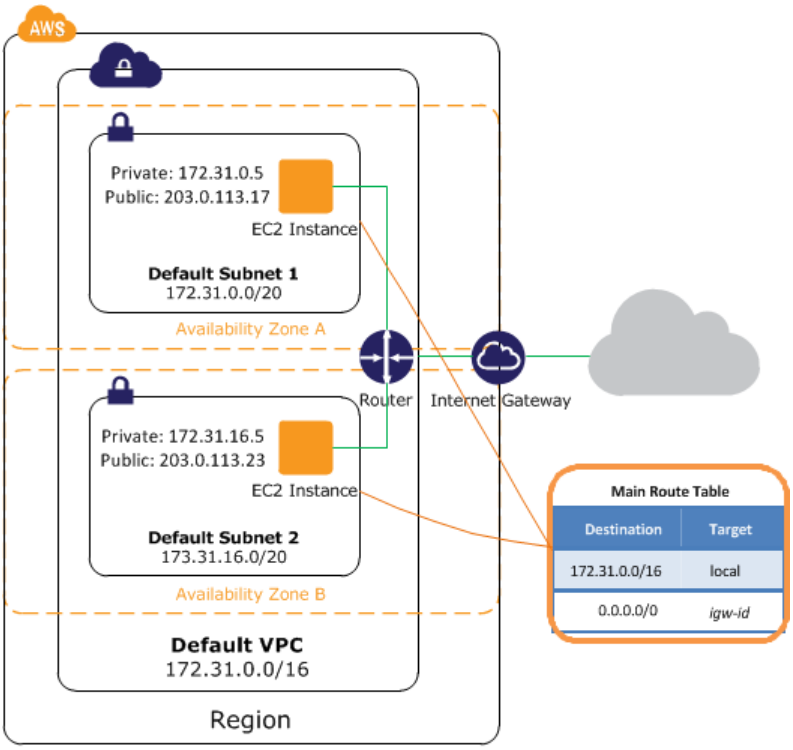
コンポーネント

デフォルトの VPC を作成するとき、Amazon 側で次の設定を行います。

- 各アベイラビリティーゾーンにデフォルトのサブネットを作成する。
- インターネットゲートウェイを作成して、デフォルトの VPC に接続する。
- デフォルトの VPC に対して、インターネット用のすべてのトラフィックをインターネットゲートウェイに送信するルールを持つメインルートテーブルを作成する。

- デフォルトのセキュリティグループを作成し、デフォルトの VPC に関連付ける。
- デフォルトのネットワークアクセスコントロールリスト（ACL）を作成し、デフォルトの VPC に関連付ける。
- デフォルトの VPC を備えた AWS アカウントに、デフォルトの DHCP オプションセットを関連付ける。

次の図は、デフォルトの VPC に対して設定する重要なコンポーネントを示します。



デフォルトの VPC 内に起動する各インスタンスは、プライベート IP アドレスとパブリック IP アドレスの両方を受け取ります。インスタンスはそれぞれ、パブリック DNS ホスト名とプライベート DNS ホスト名の両方も受け取ります。

デフォルトの VPC は、他の VPC; と同じように動作します。例えば、サブネットの追加、メインルートテーブルの変更、ルートテーブルの追加、追加のセキュリティグループの関連付け、デフォルトのセキュリティグループルールの更新、および VPN 接続の追加が可能です。また、追加の VPC を作成することもできます。

デフォルトのサブネットは、他のサブネット; と同じように動作します。例えば、カスタムルートテーブルを追加したり、ネットワーク ACL を設定したりできます。また、EC2 インスタンスを起動するときに、デフォルトのサブネットを指定することもできます。

デフォルトのサブネット

デフォルト VPC の CIDR ブロックは常に 172.31.0.0/16 です。これは、最大 65,536 個のプライベート IP アドレスを提供します。デフォルトサブネットのネットマスクは常に /20 です。これは、サブネットあたり最大 4,096 個のアドレスを提供します。この中のいくつかは、Amazon が使用するように予約されています。

デフォルトでは、デフォルトのサブネットはパブリックサブネットです。メインルートテーブルがインターネット用のサブネットのトラフィックをインターネットゲートウェイに送信するためです。デフォルトのサブネットをプライベートサブネットにするには、送信元 0.0.0.0/0 からインターネットゲートウェイへのルートを削除します。ただし、この操作を行った場合、そのサブネットで実行されている EC2 インスタンスすべてが、インターネットや、Amazon Simple Storage Service (Amazon S3) などの他の AWS 製品にアクセスできなくなります。

サポートされているプラットフォームとデフォルト VPC があるかどうかを確認する

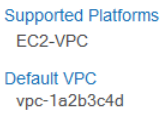
Amazon VPC に関する知識がなくても、デフォルトの VPC に EC2 インスタンスを起動し、Elastic Load Balancing、Amazon Relational Database Service (Amazon RDS) や Amazon Elastic MapReduce (Amazon EMR) などのサービスを使用できます。これらのサービスは、デフォルトの VPC または EC2-Classic のどちらを使っていても同じように利用できます。ただし、お使いの AWS アカウントが両方のプラットフォームをサポートしているかどうか、またデフォルトの VPC を備えているかどうかがわかります。次のセクションでは、Amazon EC2 コンソール、Amazon EC2 コマンドラインインターフェイス、および Amazon EC2 API アクションを使用して、その方法について説明します。

AWS マネジメントコンソール

Amazon EC2 コンソールは、EC2 インスタンスを起動できるプラットフォームと、デフォルトの VPC があるかどうかを示しています。

Verify that the region you'll use is selected in the navigation bar. On the Amazon EC2 console dashboard, look for Supported Platforms under Account Attributes. If there are two values, `EC2-Classic` and `EC2-VPC`, you can launch instances into either platform. If there is one value, `EC2-VPC`, you can launch instances only into EC2-VPC.

例えば、次の図は、アカウントが EC2-VPC プラットフォームのみをサポートしていること、および識別子 `vpc-1a2b3c4d` を持つデフォルトの VPC があることを示しています。



デフォルトの VPC を削除すると、[Default VPC] 値として `None` が表示されます。詳細については、「デフォルトの VPC を削除する (p. 66)」を参照してください。

コマンドラインインターフェイス

`supported-platforms` 属性は、EC2 インスタンスを起動できるプラットフォームを示します。アカウントのこの属性の値を取得するには、次のように `ec2-describe-account-attributes` コマンドを使用します。

```
ec2-describe-account-attributes supported-platforms
```

この属性に 2 つの値 `EC2-Classic` と `EC2-VPC` がある場合、アカウントはいずれかのプラットフォーム内に EC2 インスタンスを起動できます。インスタンスの起動時に VPC を指定しないと、インスタンスは EC2-Classic 内に起動されます。

この属性の値が EC2-VPC の場合、アカウントは EC2-VPC 内にのみインスタンスを起動できます。インスタンスの起動時に VPC を指定しないと、インスタンスはデフォルトの VPC 内に起動されます。

次のサンプル出力は、インスタンスを常に EC-VPC 内に起動することを示しています。

```
ACCOUNTATTRIBUTE    supported-platforms
VALUE     EC2-VPC
```

default-vpc 属性は、デフォルトの VPC があるかどうかを示します。デフォルトの VPC がある場合は、その識別子も一緒に表示します。この属性の値を取得するには、ec2-describe-account-attributes コマンドを使用します。supported-platforms と default-vpc の両方の属性を同じコマンドラインで指定できます。また、ここで示すように、個別に使用することもできます。

```
ec2-describe-account-attributes default-vpc
```

次のサンプル出力は、ID が vpc-1a2b3c4d のデフォルトの VPC があることを示しています。

```
ACCOUNTATTRIBUTE    default-vpc
VALUE     vpc-1a2b3c4d
```

また、ec2-describe-vpcs コマンドを使用して VPC を表示するときも、デフォルトの VPC が出力に表示されます。ec2-describe-subnets コマンドを使用してサブネットを表示すると、アベイラビリティーゾーンごとにデフォルトのサブネットが出力に示されます。

詳細については、「*Amazon Elastic Compute Cloud Command Line Reference*」の「ec2-describe-account-attributes」、「ec2-describe-vpcs」、および「ec2-describe-subnets」を参照してください。

API

supported-platforms 属性は、EC2 インスタンスを起動できるプラットフォームを示します。default-vpc 属性は、デフォルトの VPC があるかどうかを示します。デフォルトの VPC がある場合は、その識別子も一緒に表示します。アカウントのこのような属性の値を取得するには、DescribeAccountAttributes API アクションを使用します。

また、DescribeVpcs API アクションを使用して VPC を表示するときも、デフォルトの VPC が応答に表示されます。DescribeSubnets API アクションを使用してサブネットを表示すると、アベイラビリティーゾーンごとにデフォルトのサブネットが応答に示されます。

詳細については、「*Amazon Elastic Compute Cloud API Reference*」の「DescribeAccountAttributes」、「DescribeVpcs」および「DescribeSubnets」を参照してください。

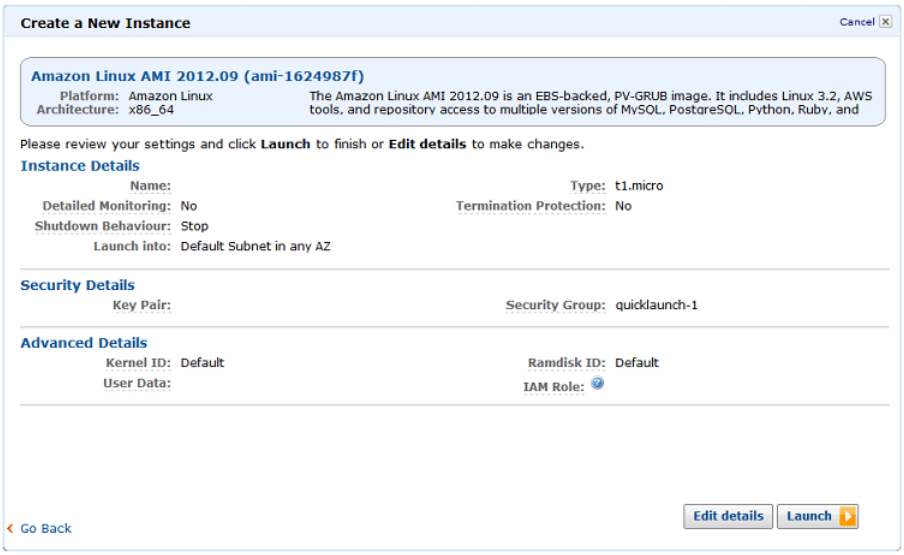
EC2 インスタンスをデフォルトの VPC 内に起動する

サブネットを指定せずに EC2 インスタンスを起動すると、そのインスタンスはデフォルトの VPC のデフォルトのサブネット内に自動的に起動されます。デフォルトでは、アベイラビリティーゾーンが選択され、インスタンスは、そのアベイラビリティーゾーンに対応するサブネット内に起動されます。また、インスタンスのアベイラビリティーゾーンを選択することもできます。それには、対応するデフォルトのサブネットをコンソールで選択するか、サブネットまたはアベイラビリティーゾーンを CLI で指定します。

AWS マネジメントコンソール

EC2 インスタンスをデフォルトの VPC 内に起動するには

1. Sign in to the AWS Management Console and open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. Amazon EC2 コンソールのダッシュボードで、[Launch Instance] をクリックします。
3. [Create a New Instance] ページで、[Quick Launch Wizard] をクリックします。ウィザードの指示にしたがって操作します。インスタンス名を指定し、キーペアを作成して、AMI を選択します。デフォルトのセキュリティグループを使用します。
4. 設定を確認します。[Launch into] のデフォルトは [Default Subnet in any AZ] です。つまり、インスタンスは、選択したアベイラビリティーゾーンのデフォルトのサブネット内に起動されていることを意味します。また、[Edit details] をクリックし、特定のアベイラビリティーゾーンのデフォルトのサブネットを選択することもできます。



5. [Launch] をクリックして、インスタンスを起動します。

コマンドラインインターフェイス

EC2 インスタンスをデフォルトの VPC 内に起動するには、`ec2-run-instances` コマンドを使用して、サブネットまたはアベイラビリティーゾーンを指定せずにインスタンスを起動します。次に例を示します。

```
ec2-run-instances ami-b232d0db
```

EC2 インスタンスをデフォルトの VPC の特定のサブネット内に起動するには、アベイラビリティーゾーンを指定します。

```
ec2-run-instances ami-b232d0db --availability-zone us-east-1a
```

または、`ec2-describe-subnets` コマンドを使用してサブネットのリストを表示するか、アベイラビリティーゾーンのデフォルトのサブネットを表示します。

```
ec2-describe-subnets
SUBNET  subnet-9d4a7b6c   available   vpc-1a2b3c4d  10.0.1.0/24   250   us-east-
1a  true true
```

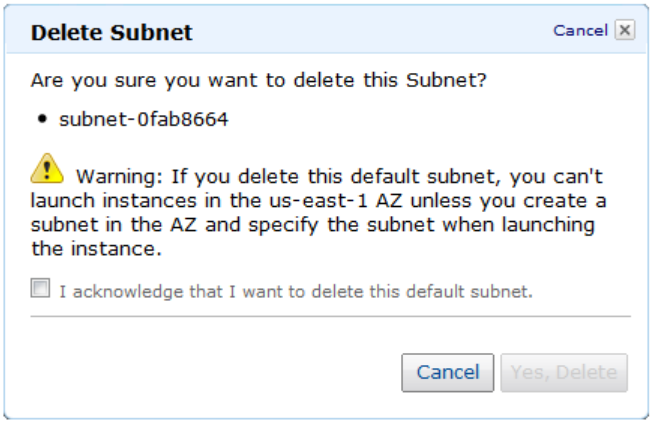
次に、ec2-run-instances を使用して、アベイラビリティーゾーンのデフォルトのサブネット内にインスタンスを起動します。次に例を示します。

```
ec2-run-instances ami-b232d0db -s subnet-9d4a7b6c
```

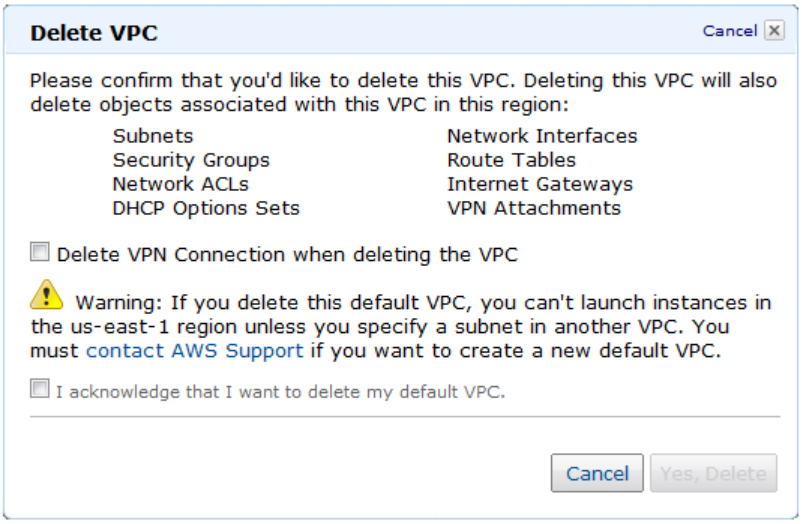
デフォルトの VPC を削除する

1 つ以上のデフォルトのサブネットを、他のサブネットと同じように削除できます。ただし、デフォルトのサブネットを削除したら、そのサブネットは消失します。この場合、EC2 インスタンスを、デフォルトの VPC のそのアベイラビリティーゾーン内に起動することはできません。これを行うには、そのアベイラビリティーゾーンにサブネットを作成し、インスタンスをそのサブネット内に明示的に起動する必要があります。デフォルトの VPC のすべてのデフォルトのサブネットを削除したら、EC2 インスタンスを起動するときに、他の VPC のサブネットを指定する必要があります。これは、EC2-Classic 内にはインスタンスを起動できないからです。

デフォルトのサブネットを削除しようとすると、[Delete Subnet] ダイアログボックスに警告メッセージが表示されます。このダイアログボックスで、デフォルトの VPC を削除することを確認する必要があります。



デフォルトの VPC は、他の VPC と同じように削除できます。ただし、デフォルトの VPC を削除したら、その VPC は消失します。つまり、EC2 インスタンスを起動するときに、他の VPC のサブネットを指定する必要があります。これは、EC2-Classic 内にはインスタンスを起動できないからです。デフォルトの VPC を削除しようとすると、[Delete VPC] ダイアログボックスに警告メッセージが表示されます。このダイアログボックスで、デフォルトの VPC を削除することを確認する必要があります。



デフォルトの VPC を削除した後、その VPC を復元する必要がある場合は、AWS Support に連絡して、新しいデフォルトの VPC を作成できるようアカウントをリセットしてください。

VPC のセキュリティ

Amazon VPC では、次の 2 つの機能を使用して、VPC のセキュリティを強化できます。

- セキュリティグループ – 関連付けられた Amazon EC2 インスタンスのファイアウォールとして動作し、インバウンドトラフィックとアウトバウンドトラフィックの両方をインスタンスレベルでコントロールします
- ネットワークアクセスコントロールリスト（ACL）– 関連付けられたサブネットのファイアウォールとして動作し、インバウンドトラフィックとアウトバウンドトラフィックの両方をサブネットレベルでコントロールします

VPC 内にインスタンスを起動するときに、作成した 1 つ以上のセキュリティグループを関連付けることができます。VPC 内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。インスタンスを起動するときにセキュリティグループを指定しないと、そのインスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。セキュリティグループの詳細については、「VPC のセキュリティグループ (p. 70)」を参照してください。

VPC インスタンスはセキュリティグループでのみ保護できます。ただし、第 2 保護レイヤーとしてネットワーク ACL を追加することができます。ネットワーク ACL の詳細については、「ネットワーク ACL (p. 77)」を参照してください。

AWS Identity and Access Management を使用すると、組織内の誰がセキュリティグループやネットワーク ACL を作成/管理できるようにするかをコントロールできます。例えば、ネットワーク管理者にだけその許可を付与し、インスタンスの起動のみが必要な作業員には付与しないようにできます。詳細については、「Amazon VPC のリソースに対するアクセスの制御 (p. 98)」を参照してください。

Note

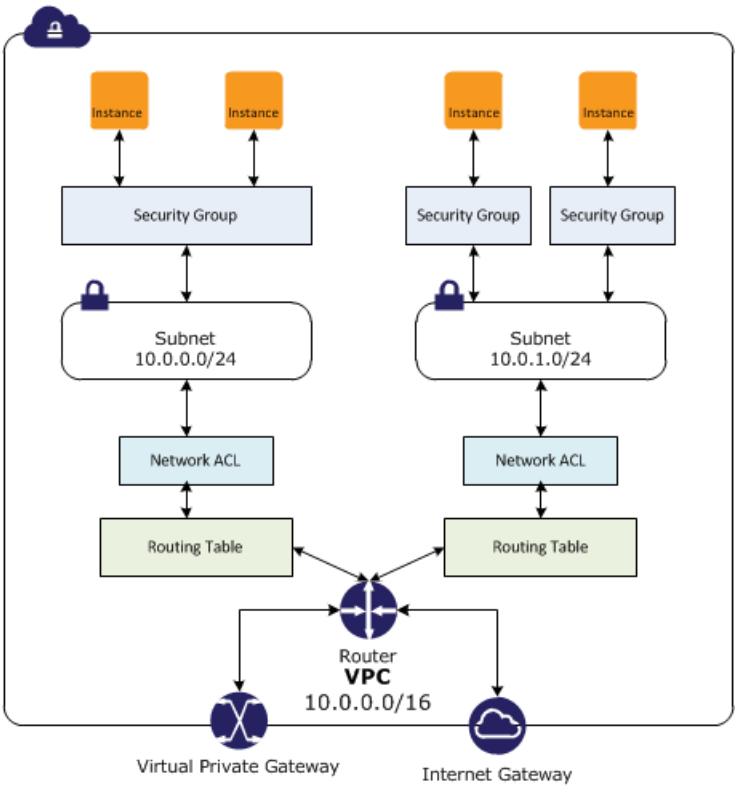
Amazon セキュリティグループとネットワーク ACL では、リンクローカルアドレス（169.254.0.0/16）へのトラフィック、またはそのアドレスからのトラフィックはフィルタされません。VPC のリンクローカルアドレスでは、ドメインネームサービス（DNS）、動的ホスト構成プロトコル（DHCP）、Amazon EC2 インスタンス固有のメタデータ、および Key Management Server（KMS – Windows インスタンスのライセンス管理）がサポートされます。追加のファイアウォールソリューションをインスタンスで実装すれば、リンクローカルアドレスとのネットワーク通信をブロックできます。

セキュリティグループとネットワーク ACL の比較

次の表は、セキュリティグループとネットワーク ACL の基本的な違いをまとめたものです。

セキュリティグループ	ネットワーク ACL
インスタンスレベルで動作します (第 1 保護レイヤー)	サブネットレベルで動作します (第 2 保護レイヤー)
ルールの許可のみがサポートされます	ルールの許可と拒否がサポートされます
ステートフル: ルールに関係なく、返されたトラフィックが自動的に許可されます	ステートレス: 返されたトラフィックがルールによって明示的に許可されます
トラフィックを許可するかどうかを決める前に、すべてのルールを評価します	トラフィックを許可するかどうかを決めるときに、順番にルールを処理します
インスタンスの起動時に誰かがセキュリティグループを指定した場合、または後でセキュリティグループをインスタンスに関連付けた場合にのみ、インスタンスに適用されます。	関連付けられたサブネット内のすべてのインスタンスに自動的に適用されます (バックアップの保護レイヤーなので、セキュリティグループを指定する人物に依存する必要はありません)

次の図は、セキュリティグループおよびネットワーク ACL が提供するセキュリティレイヤーを示しています。例えば、インターネットゲートウェイからのトラフィックは、ルーティングテーブルのルートを使用して適切なサブネットにルーティングされます。サブネットに対してどのトラフィックが許可されるかは、そのサブネットに関連付けられているネットワーク ACL のルールによってコントロールされます。インスタンスに対してどのトラフィックが許可されるかは、そのインスタンスに関連付けられているセキュリティグループのルールによってコントロールされます。



VPC のセキュリティグループ

*セキュリティグループ*は、仮想ファイアウォールとして動作し、そのグループに関連付けられたインスタンスを出入りするトラフィックをコントロールします。VPC 内でインスタンスを起動した場合、そのインスタンスは最大 5 つのセキュリティグループに割り当てることができます。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。このため、VPC 内のサブネット内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。起動時に特定のグループを指定しないと、インスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。

セキュリティグループごとに、インスタンスへのインバウンドトラフィックをコントロールする*ルール*と、アウトバウンドトラフィックをコントロールする一連のルールを個別に追加します。このセクションでは、VPC のセキュリティグループとそのルールについて、知っておく必要がある基本事項について説明します。

セキュリティの追加レイヤーを VPC に追加するには、セキュリティグループと同様のルールを指定したネットワーク ACL をセットアップできます。セキュリティグループとネットワーク ACL の違いの詳細については、「セキュリティグループとネットワーク ACL の比較 (p. 69)」を参照してください。

Topics

セキュリティグループの基本

VPC のセキュリティグループの基本的な特性を次に示します。

- VPC ごとに最大 100 のセキュリティグループを作成できます。最大 50 のルールを各セキュリティグループに追加できます。1 つのインスタンスに 50 を超えるルールを適用する必要がある場合は、各インスタンスにつき最大 5 つのセキュリティを指定できます。
- 許可ルールを指定できます。拒否ルールは指定できません。
- インバウンドトラフィックとアウトバウンドトラフィックのルールを個別に指定できます。
- デフォルトでは、インバウンドトラフィックは、インバウンドルールをセキュリティグループに追加するまで許可されません。
- デフォルトでは、アウトバウンドルールをグループに追加するまで、すべてのアウトバウンドトラフィックが許可されます (その後、許可しないアウトバウンドトラフィックを指定します)。
- 許可されたインバウンドトラフィックに対する応答は、アウトバウンドルールにかかわらずアウトバウンドに流れることができます。また、その逆も当てはまります (したがって、セキュリティグループはステートフルです)。
- セキュリティグループに関連付けられたインスタンスの相互通信は、それを許可するルールを追加するまで許可されません (例外: デフォルトのセキュリティグループについては、このルールがデフォルトで指定されています)。
- インスタンスを起動したら、インスタンスが関連付けられているセキュリティグループを変更できます。

VPC のデフォルトセキュリティグループ

VPC ではデフォルトのセキュリティグループが自動的に使用されます。VPC で起動する EC2 インスタンスは、そのインスタンスの起動時に別のセキュリティグループを指定しない限り、それぞれがデフォルトのセキュリティグループに自動的に関連付けられます。

次の表では、デフォルトのセキュリティグループ用のデフォルトルールについて説明します。

インバウンド			
送信元	プロトコル	ポート範囲	コメント
セキュリティグループ ID（sg-*xxxxxxxx*）	すべて	すべて	同じセキュリティグループに割り当てられたインスタンスからのインバウンドトラフィックを許可する
アウトバウンド			
送信先	プロトコル	ポート範囲	コメント
0.0.0.0/0	すべて	すべて	すべてのアウトバウンドトラフィックを許可する

デフォルトのセキュリティグループのルールは変更できます。

セキュリティグループのルール

セキュリティグループのルールは追加または削除できます（インバウンドまたはアウトバウンドアクセスの*許可*または*取り消し*とも呼ばれます）。ルールが適用されるのは、インバウンドトラフィック（受信）またはアウトバウンドトラフィック（送信）のいずれかです。特定の CIDR 範囲へのアクセス、または VPC 内の他のセキュリティグループへのアクセスを許可できます。

セキュリティグループのルールの基本要素を次に示します。

- （インバウンドルールのみ）トラフィックの送信元（CIDR 範囲またはセキュリティグループ）と、送信先ポートまたはポート範囲
- （アウトバウンドルールのみ）トラフィックの送信先（CIDR 範囲またはセキュリティグループ）と、送信先ポートまたはポート範囲
- 標準のプロトコル番号を持つ任意のプロトコル（リストについては、「Protocol Numbers」を参照）。

  ICMP をプロトコルとして指定すると、ICMP の種類とコードの一部またはすべてを指定できます。

ルールを追加または削除すると、セキュリティグループに関連付けられたすべてのインスタンスにこの操作が自動的に適用されます。

Note

ファイアウォールを設定するためのシステムの一部を使用すると、送信元ポートでフィルタを適用できます。セキュリティグループを使用すると、送信先ポートでのみフィルタを適用できます。

次の表では、ウェブサーバーのセキュリティグループに対するルールの例を説明します。ウェブサーバーは HTTP および HTTPS トラフィックを受信し、SQL または MySQL トラフィックをデータベースサーバーに送信することができます。

インバウンド			
送信元	プロトコル	ポート範囲	コメント
0.0.0.0/0	TCP	80	すべての場所からのインバウンド HTTP アクセスを許可する
0.0.0.0/0	TCP	443	すべての場所からのインバウンド HTTPS アクセスを許可する
ネットワークのパブリック IP アドレス範囲	TCP	22	ネットワークから Linux インスタンスへのインバウンド SSH アクセス（インターネットゲートウェイ経由）を許可する
ネットワークのパブリック IP アドレス範囲	TCP	3389	ネットワークから Windows インスタンスへのインバウンド RDP アクセス（インターネットゲートウェイ経由）を許可する
アウトバウンド			
送信先	プロトコル	ポート範囲	コメント
データベースサーバーのセキュリティグループの ID	TCP	1433	アウトバウンド Microsoft SQL Server が指定されたセキュリティグループ内のインスタンスにアクセスするのを許可する
MySQL データベースサーバーのセキュリティグループの ID	TCP	3306	アウトバウンド MySQL が指定されたセキュリティグループ内のインスタンスにアクセスするのを許可する

ウェブサーバーとデータベースサーバー用にセキュリティグループを作成するための段階的な手順については、「推奨セキュリティグループ (p. 32)」を参照してください。

EC2-Classic と EC2-VPC のセキュリティグループの違い

既に Amazon EC2 を使用しているのであれば、セキュリティグループについてはご存知でしょう。ただし、EC2-Classic で使用するために作成したセキュリティグループは、VPC のインスタンスで使用することはできません。VPC のインスタンスで使用するためのセキュリティグループを特別に作成する必要があります。VPC のセキュリティグループで使用するために作成したルールは、EC2-Classic のセキュリティグループを参照できません。その逆も同様です。

次の表は、EC2-Classic で使用するセキュリティグループと EC2-VPC で使用するセキュリティグループの違いをまとめたものです。

EC2-Classic	EC2-VPC
リージョンごとに最大 500 のセキュリティグループを作成できます。	VPC ごとに最大 100 のセキュリティグループを作成できます。
最大 100 のルールをセキュリティグループに追加できます。	最大 50 のルールをセキュリティグループに追加できます。

EC2-Classic	EC2-VPC
インバウンドトラフィックのみにルールを追加できます。	インバウンドトラフィックとアウトバウンドトラフィックのルールを追加できます。
無制限の数のセキュリティグループを 1 つのインスタンスに割り当てることができます。	最大 5 つのセキュリティグループを 1 つのインスタンスに割り当てることができます。
他の AWS アカウントからセキュリティグループを参照できます。	VPC のセキュリティグループのみ参照できます。
インスタンスを起動すると、インスタンスに関連付けられているセキュリティグループは変更できません。	インスタンスの起動後でも、インスタンスに関連付けられているセキュリティグループは変更できます。
ルールをセキュリティグループに追加するとき、プロトコルを指定する必要はありません。TCP、UDP、または ICMP のみを使用できます。	ルールをセキュリティグループに追加するときは、プロトコルを指定する必要があります。標準のプロトコル番号を持つ任意のプロトコル、またはすべてのプロトコル (Protocol Numbers を参照) を使用できます。
ルールをセキュリティグループに追加するときは、ポート番号を指定する必要があります (TCP または UDP 用) 。	ルールをセキュリティグループに追加するときは、そのルールが TCP または UDP 用の場合にのみポート番号を指定できます。すべてのポート番号を指定できます。

セキュリティグループを操作する

このセクションでは、AWS マネジメントコンソールを使用してセキュリティグループを操作する方法について説明します。

Topics

デフォルトのセキュリティグループを変更する

VPC に用意されているデフォルトのセキュリティグループの初期ルールでは、すべてのインバウンドトラフィックが拒否され、すべてのアウトバウンドトラフィックと、そのグループのインスタンス間のすべてのトラフィックが許可されます。このグループは削除できませんが、グループのルールは変更できます。その手順は、他のセキュリティグループを変更する手順と同じです。詳細については、「ルールを追加および削除する (p. 74)」を参照してください。

セキュリティグループを作成する

インスタンスのデフォルトのセキュリティグループを使用できますが、お客様独自のグループを作成し、システムにおけるインスタンスの様々な役割を反映させたい場合があります。

セキュリティグループを作成するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Security Groups] をクリックします。
3. [Create Security Group] ボタンをクリックします。
4. セキュリティグループ名 (例えば、`my-security-group`) と説明を入力します。[VPC] メニューで VPC の ID を選択し、[Yes, Create] をクリックします。

デフォルトでは、新しいセキュリティグループには、すべてのトラフィックがインスタンスを出ることを許可するアウトバウンドルールのみが設定されています。任意のインバウンドトラフィックを許可するには、またはアウトバウンドトラフィックを制限するには、ルールを追加する必要があります。

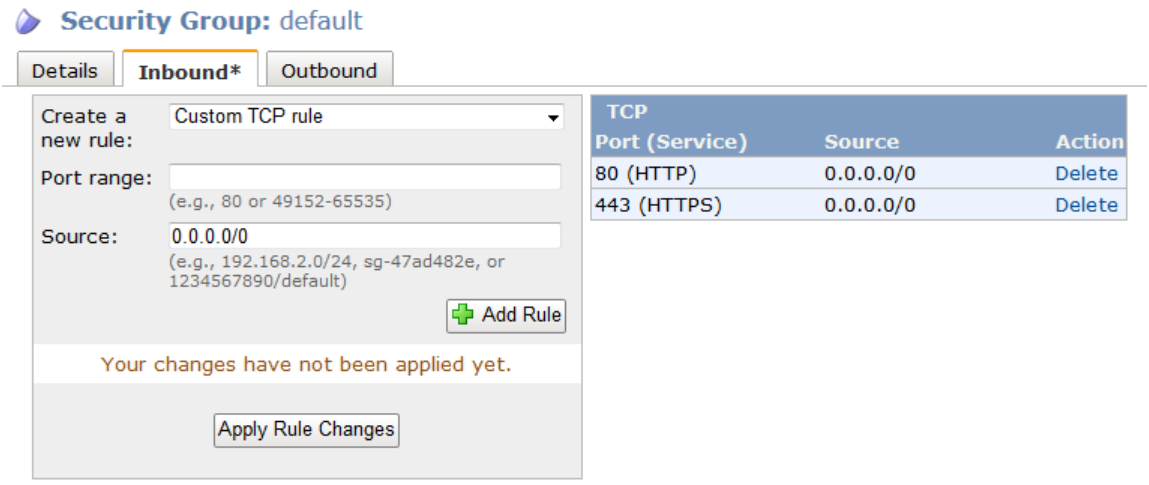
ルールを追加および削除する

ルールを追加または削除すると、セキュリティグループに既に割り当てられているすべてのインスタンスが変更される可能性があります。ルールは変更できません。ルールの追加と削除のみを行うことができます。

このガイドで示すシナリオのいくつかは、ルールをセキュリティグループに追加する手順を示しています。例については、「推奨セキュリティグループ (p. 32)」を参照してください。

ルールを追加するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Security Groups] をクリックします。
3. 更新するセキュリティグループを選択します。詳細ペインには、セキュリティグループの詳細と、インバウンドルールとアウトバンドルールを操作するタブが表示されます。
4. [Inbound] タブを使用して、[Create a new rule] からインバウンドトラフィックのルールに関するオプションを選択し、必要な情報を入力してから、[Add Rule] をクリックします。例えば、`HTTP` または `HTTPS` を選択し、[Source] を `0.0.0.0/0` のままにします。[Apply Rule Changes] ボタンが有効で、ボタンの上には "Your changes have not been applied yet" というテキストが表示されています。必要なインバウンドトラフィックのすべてのルールを追加したら、[Apply Rule Changes] をクリックしてルールを追加します。



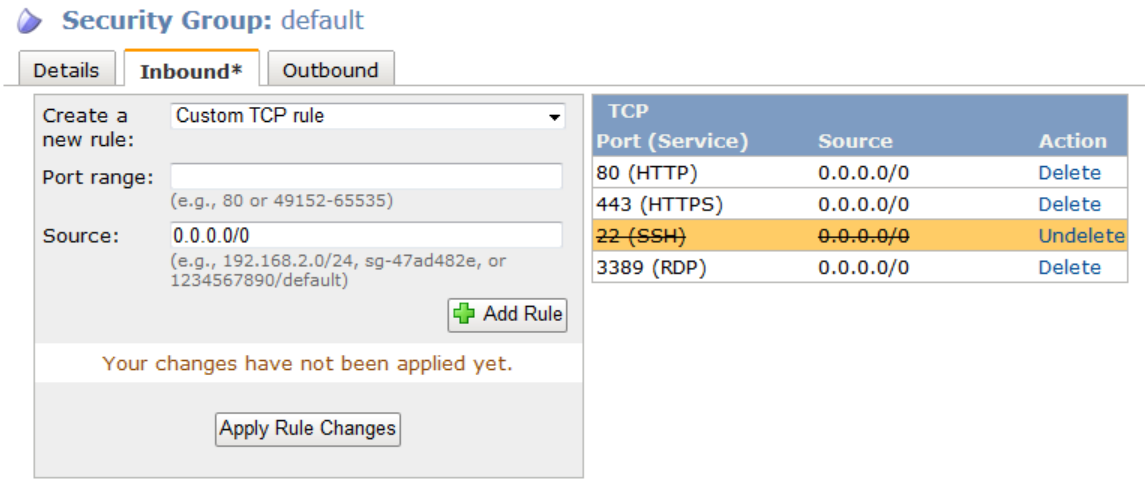
5. このセキュリティグループに関連付けられたすべてのインスタンス間での通信を許可することもできます。[Inbound] タブを使用して、[Create a new rule] から `All Traffic` を選択します。[Source] でセキュリティグループの ID の入力を開始します。すると、セキュリティグループのリストが表

示されます。このリストからセキュリティグループを選択し、[Add Rule] をクリックし、[Apply Rule Changes] をクリックします。

6. 必要に応じて、[Outbound] タブを使用し、アウトバウンドトラフィックのルールを追加できます。

ルールを削除するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Security Groups] をクリックします。
3. 更新するセキュリティグループを選択します。詳細ペインには、セキュリティグループの詳細と、インバウンドルールとアウトバンドルールを操作するタブが表示されます。
4. 削除するルールで [Delete] をクリックします。[Apply Rule Changes] ボタンが有効で、ボタンの上には "Your changes have not been applied yet" というテキストが表示されています。
5. [Apply Rule Changes] をクリックし、そのルールを削除します。

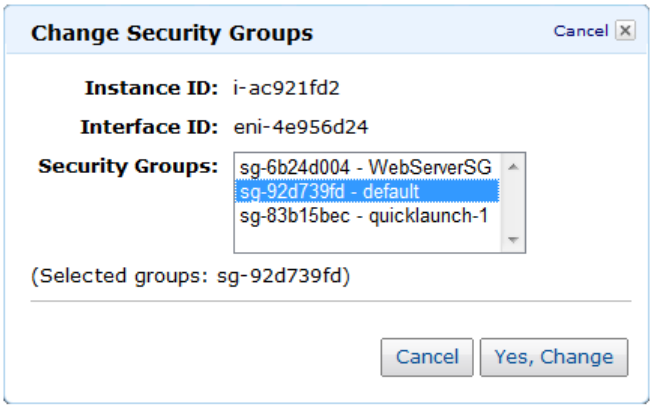


インスタンスのセキュリティグループを変更する

VPC のインスタンスが割り当てられているセキュリティグループは、そのインスタンスの起動後に変更できます。変更した場合、インスタンスは実行または停止します。

インスタンスのセキュリティグループを変更するには

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. ナビゲーションペインで [Instances] をクリックします。
3. インスタンスを右クリックし、[Change Security Groups] を選択します。
4. [Change Security Groups] ダイアログボックスで、1 つ以上のセキュリティグループを [Security Groups] から選択し、[Yes, Change] をクリックします。



セキュリティグループを削除する

セキュリティグループは、インスタンスが実行されているかどうかにかかわらず、そのグループに割り当てられていない場合にのみ削除できます。インスタンスは、セキュリティグループを削除する前に他のセキュリティグループに割り当てることができます (「インスタンスのセキュリティグループを変更する (p. 75)」を参照) 。

セキュリティグループを削除するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Security Groups] をクリックします。
3. セキュリティグループを選択し、[Delete] をクリックします。
4. [Delete Security Group] ダイアログボックスで、[Yes, Delete] をクリックします。

2009 年 7 月 15 日デフォルトのセキュリティグループを削除する

2011 年 1 月 1 日より前の API バージョンを使用して作成された VPC には、`2009-07-15-default` セキュリティグループが含まれます。すべての VPC に含まれる通常の `default` セキュリティグループの他に、このセキュリティグループが存在します。インターネットゲートウェイは、`2009-07-15-default` セキュリティグループを含む VPC にアタッチすることはできません。したがって、VPC にインターネットゲートウェイをアタッチする前に、このセキュリティグループを削除する必要があります。

Note

このセキュリティグループを任意のインスタンスに割り当てている場合、そのセキュリティグループは、該当するインスタンスを別のセキュリティグループに割り当ててからでなければ、削除できません。

`2009-07-15-default` セキュリティグループを削除するには

1. このセキュリティグループがどのインスタンスにも割り当てられていないことを確認します。
   a. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
   b. ナビゲーションペインで [Network Interfaces] をクリックします。

c. リストからインスタンスのネットワークインターフェイスを選択し、[Actions] リストで [Change Security Groups] を選択します。
d. [Change Security Groups] ダイアログボックスで、[Security Groups] リストから新しいセキュリティグループを選択し、[Save] をクリックします。

Tip

インスタンスのセキュリティグループを変更するときに、複数のグループをリストから選択できます。選択したセキュリティグループによって、インスタンスの現在のセキュリティグループが置き換えられます。

e. 各インスタンスごとに前述の手順を繰り返します。

2. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
3. ナビゲーションペインで [Security Groups] をクリックします。
4. `2009-07-15-default` セキュリティグループを選択し、[Delete] ボタンをクリックします。
5. [Delete Security Group] ダイアログボックスで、[Yes, Delete] をクリックします。

API とコマンドの概要

次の表は、使用可能なセキュリティグループコマンドと対応する API アクションをまとめたものです。

説明	コマンド	API アクション
セキュリティグループを作成します。	ec2-create-group	CreateSecurityGroup
ルールをセキュリティグループに追加します。	ec2-authorize	AuthorizeSecurityGroupIngress AuthorizeSecurityGroupEgress
1 つ以上のセキュリティグループについて説明します。	ec2-describe-group	DescribeSecurityGroups
インスタンスが関連付けられているセキュリティグループを変更します。	ec2-modify-instance-attribute	ModifyInstanceAttribute
ルールをセキュリティグループから削除します。	ec2-revoke	RevokeSecurityGroupIngress RevokeSecurityGroupEgress
セキュリティグループを削除します。	ec2-delete-group	DeleteSecurityGroup

ネットワーク ACL

ネットワークアクセスコントロールリスト (ACL) は、サブネットのインバウンドトラフィックとアウトバウンドトラフィックを制御するファイアウォールとして動作するセキュリティのオプションレイヤーです。セキュリティの追加レイヤーを VPC に追加するには、セキュリティグループと同様のルールを指定したネットワーク ACL をセットアップできます。セキュリティグループとネットワーク ACL の違いの詳細については、「セキュリティグループとネットワーク ACL の比較 (p. 69)」を参照してください。

Topics

ネットワーク ACL の基本

ネットワーク ACL について知っておく必要がある基本的な情報を以下に示します。

- ネットワーク ACL は、低い番号から順に評価される番号付きのルールリストであり、ネットワーク ACL に関連付けられたサブネットのインバウンドトラフィックまたはアウトバウンドトラフィックが許可されるかどうかを指定します。ルールに使用できる最も高い番号は 32766 です。まずは 100 の倍数のルール番号を付けたルールを作成することをお勧めします。こうすると、後で必要になったときに新しいルールを挿入できます。
- ネットワーク ACL には個別のインバウンドルールとアウトバウンドルールがあり、各ルールでトラフィックを許可または拒否できます。
- VPC には、変更可能なデフォルトのネットワーク ACL が自動的に設定されます。デフォルトでは、この ACL はすべてのインバウンドトラフィックとアウトバウンドトラフィックを許可します。
- カスタムネットワーク ACL を作成できます。各カスタムネットワーク ACL の初期状態は、ルールを追加するまで閉じられています (一切のトラフィックを許可していません) 。
- 各サブネットはネットワーク ACL に関連付ける必要があります。サブネットをネットワーク ACL に明示的に関連付けない場合、サブネットはデフォルトのネットワーク ACL に自動的に関連付けられます。
- ネットワーク ACL はステートレスです。許可されているインバウンドトラフィックに対する応答は、アウトバウンドトラフィックのルールに従います (その逆の場合も同様です) 。

作成できるネットワーク ACL の数の詳細については、「Amazon VPC 制限 (p. 159)」を参照してください。

ネットワーク ACL ルール

デフォルトのネットワーク ACL に対してルールの追加または削除を行うことができます。また、VPC に合わせて追加のネットワーク ACL を作成することができます。ネットワーク ACL に対してルールの追加または削除を行うと、変更内容は、その ACL に関連付けられているサブネットに自動的に適用されます。

次に、ネットワーク ACL ルールの一部を示します。

- ルール番号。ルールは、最も低い番号のルールから評価されます。
- プロトコル。標準のプロトコル番号を持つ任意のプロトコルを指定できます。詳細については、「プロトコル番号」を参照してください。プロトコルとして ICMP を指定する場合、任意またはすべての ICMP タイプとコードを指定できます。
- [インバウンドルールのみ] トラフィックの送信元 (CIDR の範囲) と送信先 (リッスン) ポートまたはポートの範囲。
- [アウトバウンドルールのみ] トラフィックの送信先 (CIDR の範囲) と送信先ポートまたはポートの範囲。
- 許可または拒否の選択。

デフォルトのネットワーク ACL

ACL ルールの概要を理解できるように、ここでは、デフォルトのネットワーク ACL は次のような初期状態です。デフォルトのネットワーク ACL は、各サブネットを出入りするすべてのトラフィックを許可するように設定されています。各ネットワーク ACL には、ルール番号がアスタリスクのルールが含まれます。このルールによって、パケットが他のいずれのルールとも一致しない場合は、確実に拒否されます。このルールを変更または削除することはできません。

インバウンド				
ルール番号	送信元 IP	プロトコル	ポート	許可/拒否
100	0.0.0.0/0	すべて	すべて	許可
*	0.0.0.0/0	すべて	すべて	拒否
アウトバウンド				
ルール番号	送信先 IP	プロトコル	ポート	許可/拒否
100	0.0.0.0/0	すべて	すべて	許可
*	0.0.0.0/0	すべて	すべて	拒否

カスタムネットワーク ACL の例

次の表に、カスタムネットワーク ACL の例を示します。この ACL には、HTTP および HTTPS のインバウンドトラフィック (インバウンドルール 100 および 110) を許可するルールが含まれます。そのインバウンドトラフィックに対する応答を可能にする、対応するアウトバウンドルールがあります (一時ポート 49152 ~ 65535 を対象とするアウトバウンドルール 120) 。適切な一時ポートの範囲を選択する方法の詳細については、「一時ポート (p. 81)」を参照してください。

ネットワーク ACL には、SSH および RDP からサブネットに対するトラフィックを許可するインバウンドルールも含まれます。アウトバウンドルール 120 は、サブネットに送信される応答を可能にします。

ネットワーク ACL には、サブネットからの HTTP および HTTPS のアウトバウンドトラフィックを許可するアウトバウンドルール (100 および 110) があります。そのアウトバウンドトラフィックに対する応答を可能にする、対応するインバウンドルールがあります (一時ポート 49152 ~ 65535 を対象とするインバウンドルール 140) 。

インバウンド					
ルール番号	送信元 IP	プロトコル	ポート	許可/拒否	コメント
100	0.0.0.0/0	TCP	80	許可	すべての場所からのインバウンド HTTP トラフィックを許可します。
110	0.0.0.0/0	TCP	443	許可	すべての場所からのインバウンド HTTPS トラフィックを許可します。

120	192.0.2.0/24	TCP	22	許可	（インターネットゲートウェイを介した）ホームネットワークのパブリック IP アドレスの範囲からのインバウンド SSH トラフィックを許可します。
130	192.0.2.0/24	TCP	3389	許可	（インターネットゲートウェイを介した）ホームネットワークのパブリック IP アドレスの範囲からウェブサーバーに対するインバウンド RDP トラフィックを許可します。
140	0.0.0.0/0	TCP	49152 ~ 65535	許可	（送信元がサブネットであるリクエストに対する）インターネットからのインバウンドリターントラフィックを許可します。 適切な一時ポートの範囲を選択する方法の詳細については、「一時ポート (p. 81)」を参照してください。
150	0.0.0.0/0	UDP	32768-61000	許可	インバウンドリターン UDP トラフィックを許可します。 適切な一時ポートの範囲を選択する方法の詳細については、「一時ポート (p. 81)」を参照してください。
*	0.0.0.0/0	すべて	すべて	拒否	前のルールでまだ処理されていないすべてのインバウンドトラフィックを拒否します（変更不可能）。
アウトバウンド					
ルール番号	送信先 IP	プロトコル	ポート	許可/拒否	コメント
100	0.0.0.0/0	TCP	80	許可	サブネットからインターネットへのアウトバウンド HTTP トラフィックを許可します。
110	0.0.0.0/0	TCP	443	許可	サブネットからインターネットへのアウトバウンド HTTPS トラフィックを許可します。

120	0.0.0.0/0	TCP	49152 ~ 65535	許可	インターネット上のクライアントに対するアウトバウンド応答を許可します (例えば、サブネット内のウェブサーバーを訪問するユーザーに対するウェブページの提供など)。 適切な一時ポートの範囲を選択する方法の詳細については、「一時ポート (p. 81)」を参照してください。
*	0.0.0.0/0	すべて	すべて	拒否	前のルールでまだ処理されていないすべてのアウトバウンドトラフィックを拒否します (変更不可能)。

パケットがサブネットに送信されると、サブネットが関連付けられている ACL の進入ルールと照合して評価されます (ルールリストの一番上から順に一番下まで評価されます)。例えば、パケットが SSL ポート (443) あてだとします。パケットは最初に評価されるルール (ルール 100) と一致しません。また、2 番目のルール (110) とは一致します。このルールでは、サブネットに送信されるパケットを許可します。パケットがポート 139 (NetBIOS) あての場合、先頭の 2 つのルールは一致しませんが、最終的に * ルールによってパケットが拒否されます。

正当に幅広い範囲のポートを開く必要があり、その範囲内の特定のポートは拒否したい場合は、拒否ルールを追加します。このとき、テーブル内で、幅広い範囲のポートトラフィックを許可するルールよりも先に拒否ルールを配置します。

一時ポート

前のセクションでは、ネットワーク ACL の例に 49152 ~ 65535 という一時ポートの範囲を使用しています。ただし、ネットワーク ACL には別の範囲を使用することができます。ここではその理由について説明します。

リクエストを開始するクライアントは、一時ポートの範囲を選択します。範囲は、クライアントのオペレーティングシステムによって変わります。多くの Linux カーネル (Amazon Linux カーネルを含む) は、ポート 32768 ~ 61000 を使用します。Elastic Load Balancing が送信元のリクエストは、ポート 1024 ~ 65535 を使用します。Windows Server 2003 を介する Windows オペレーティングシステムは、ポート 1025 ~ 5000 を使用します。Windows Server 2008 は、ポート 49152 ~ 65535 を使用します。そのため、インターネット上の Windows XP クライアントから、お使いの VPC のウェブサーバーにリクエストが送信される場合、ネットワーク ACL には、ポート 1025 ~ 5000 あてのトラフィックを可能にするアウトバウンドルールを用意する必要があります。

VPC 内の EC2 インスタンスが、リクエストを開始するクライアントの場合、ネットワーク ACL には、インスタンス (Amazon Linux, Windows Server 2008 など) の種類に固有の一時ポートあてのトラフィックを可能にするインバウンドルールを用意する必要があります。

実際に、VPC 内のパブリックに面したインスタンスに対して、トラフィックを開始することができる多様なクライアントを対象にするには、一時ポート 1024 ~ 65535 を開く必要があります。ただし、その範囲内で悪意のあるポートのトラフィックを拒否するルールを ACL を追加することもできます。このとき、テーブル内で、幅広い範囲の一時ポートを開くルールよりも先に拒否ルールを配置します。

ネットワーク ACL の操作

ここでは、Amazon VPC コンソールを使用してネットワーク ACL を操作する方法について説明します。

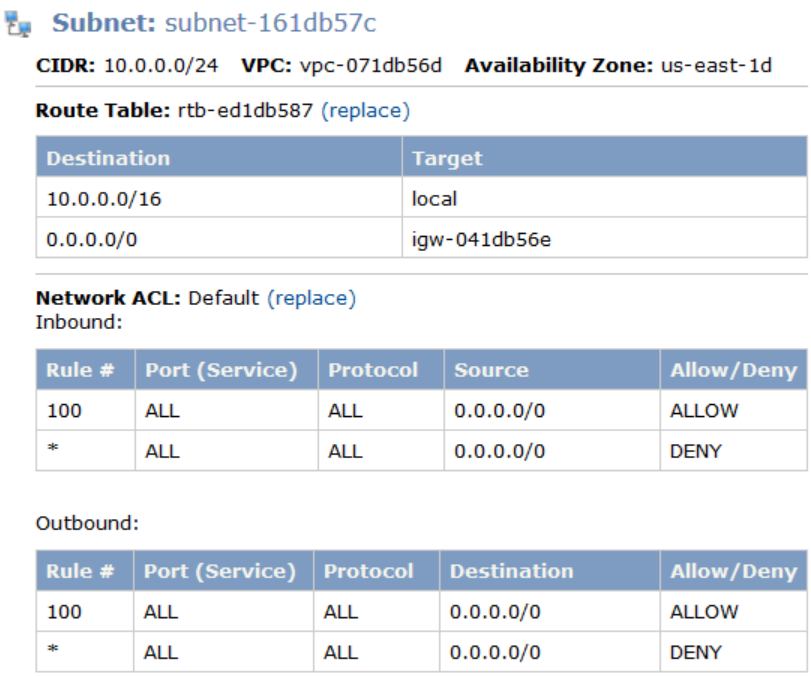
Topics

サブネットを関連付けるネットワーク ACL の決定

サブネットを関連付けるネットワーク ACL を決定するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Subnets] をクリックし、サブネットを選択します。

   サブネットに関連付けられているネットワーク ACL は、ネットワーク ACL のルールと共に詳細ペインに表示されます。



Subnet: subnet-161db57c

CIDR: 10.0.0.0/24 **VPC:** vpc-071db56d **Availability Zone:** us-east-1d

Route Table: rtb-ed1db587 (replace)

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-041db56e

Network ACL: Default (replace)
Inbound:

Rule #	Port (Service)	Protocol	Source	Allow/Deny
100	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL	ALL	0.0.0.0/0	DENY

Outbound:

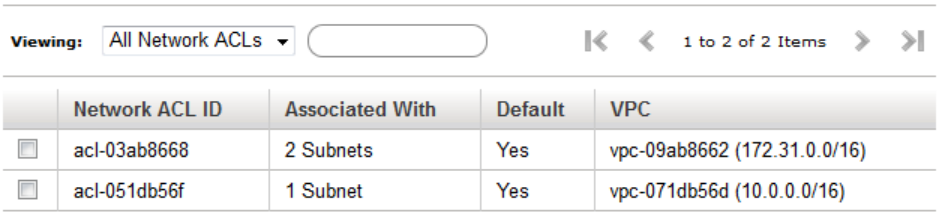
Rule #	Port (Service)	Protocol	Destination	Allow/Deny
100	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL	ALL	0.0.0.0/0	DENY

ネットワーク ACL に関連付けられたサブネットの決定

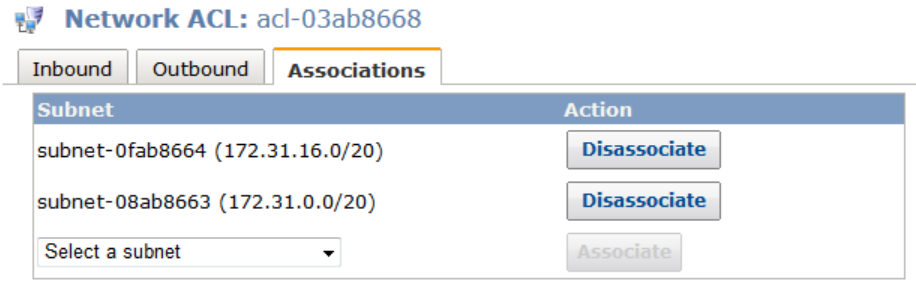
ネットワーク ACL に関連付けられたサブネットを決定するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Network ACLs] をクリックします。

   コンソールにネットワーク ACL が表示されます。[Associated With] 列には、関連付けられているサブネットの数が表示されます。



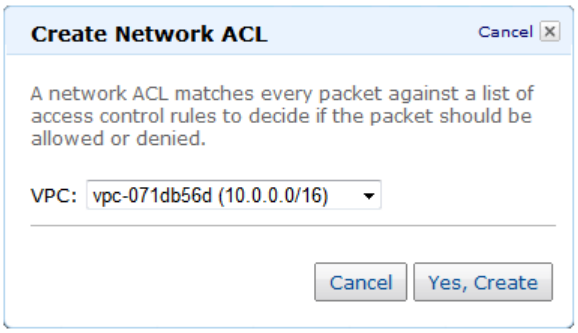
3. ネットワーク ACL を選択します。
4. 詳細ペインで [Associations] タブをクリックして、ネットワーク ACL に関連付けられているサブネットを表示します。



ネットワーク ACL を作成する

ネットワーク ACL を作成するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Network ACLs] をクリックします。
3. [Create Network ACL] ボタンをクリックします。
4. [Create Network ACL] ダイアログボックスで [VPC] リストから VPC の ID を選択してから、[Yes, Create] をクリックします。



ネットワーク ACL の初期設定では、すべてのインバウンドトラフィックとアウトバウンドトラフィックをブロックします。このネットワーク ACL には、すべての ACL にある * ルール以外にルールがありません。

新しい ACL に関連付けられたサブネットはありません。

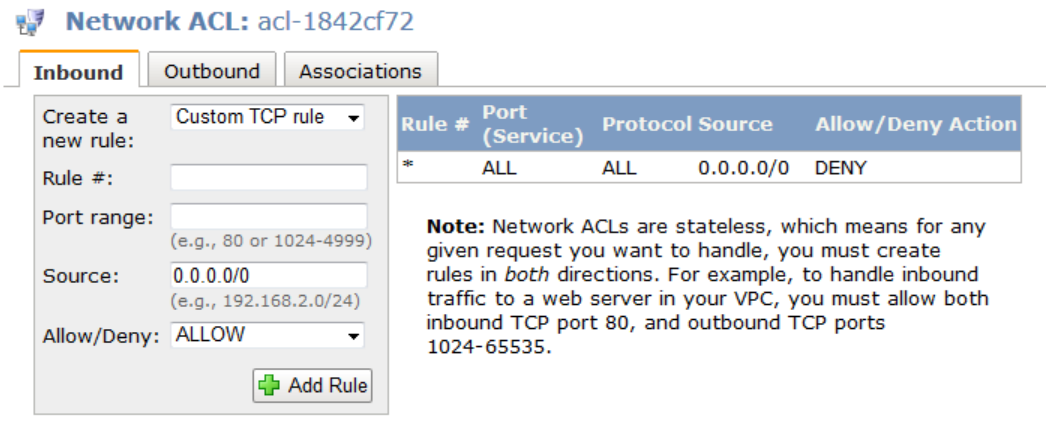
ルールの追加と削除

ACL のルールの追加または削除を行うと、その ACL に関連付けられたすべてのサブネットに変更が反映されます。サブネット内のインスタンスを終了して再起動する必要はありません。短時間で変更が反映されます。

ルールは変更できません。ルールの追加と削除のみを行うことができます。ACL のルールの順序を変更する必要がある場合は、新しいルール番号を指定した新しいルールを追加してから、元のルールを削除します。

ルールをネットワーク ACL に追加するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Network ACLs] をクリックしてから、ネットワーク ACL を選択します。
3. 詳細ペインで、追加する必要があるルールの種類に応じて、[Inbound] タブまたは [Outbound] タブを選択します。



4. [Create a new rule] ドロップダウンリストからオプションを選択します。例えば、HTTP のルールを追加するには、[HTTP] オプションを選択します。すべての TCP トラフィックを許可するルールを追加するには、[All TCP] を選択します。これらのオプションの一部 (HTTP など) については、

ポートが自動入力されます。表示されていないプロトコルを使用するには、[Custom protocol rule] を選択します。

5. ルールの詳細を指定します。

   a. [Rule #] にルール番号（100 など）を入力します。ネットワーク ACL にすでに使用されているルール番号は使用できません。ルールは、最も低い番号から順に処理されます。

      Tip

      ルール番号は、連続番号（101、102、103 など）を使用せずに、間を空けておくことをお勧めします（100、200、300 など）。こうすることで、既存のルールに番号を振り直さなくても、所属する新しいルールを簡単に追加できるようになります。

   b. （オプション）カスタムプロトコルルールを作成する場合、プロトコルの番号（47）または名前（GRE）を [Protocol] ボックスに入力します。詳細については、「プロトコル番号の IANA リスト」を参照してください。

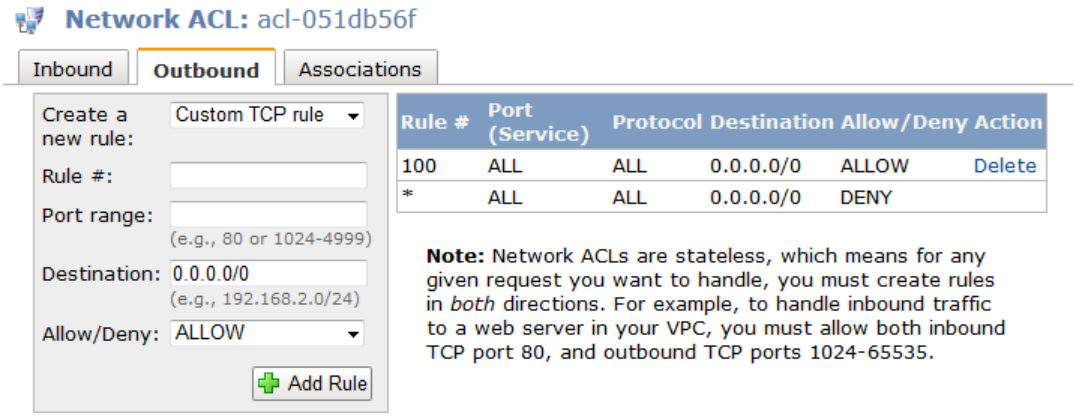
   c. （オプション）選択したプロトコルにポート番号が必要な場合、ポート番号またはハイフンで区切ったポート番号の範囲（49152-65535 など）を入力します。

   d. インバウンドルールかアウトバウンドルールかに応じて、[Source] または [Destination] ボックスに、ルールを適用する CIDR の範囲を入力します。

6. [Allow/Deny] リストから、指定したトラフィックを許可するには [ALLOW]、指定したトラフィックを拒否するには [DENY] を選択します。
7. [Add Rule] をクリックします。

ネットワーク ACL からルールを削除するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Network ACLs] をクリックしてから、ネットワーク ACL を選択します。
3. 詳細ペインで、[Inbound] タブまたは [Outbound] タブを選択してから、[Delete] をクリックします。



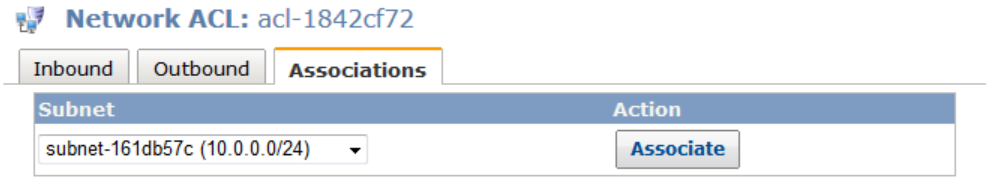
4. [Delete Network ACL Rule] ダイアログボックスで [Yes, Delete] をクリックします。

サブネットをネットワーク ACL と関連付ける

ネットワーク ACL のルールを特定のサブネットに適用するには、サブネットをネットワーク ACL と関連付ける必要があります。1 つのネットワーク ACL を複数のサブネットに関連付けることができます。ただし、1 つのサブネットは 1 つのネットワーク ACL にのみ関連付けることができます。特定の ACL に関連付けられていないサブネットは、デフォルトでデフォルトのネットワーク ACL と関連付けられます。

サブネットをネットワーク ACL と関連付けるには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Network ACLs] をクリックしてから、ネットワーク ACL を選択します。
3. 詳細ペインの [Associations] タブで、テーブルに関連付けるサブネットを選択してから、[Associate] をクリックします。



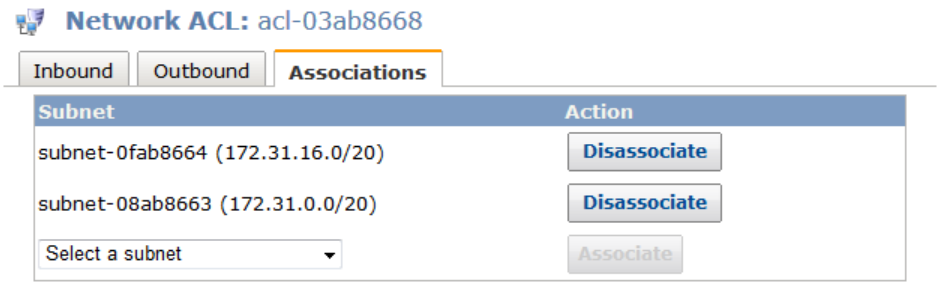
4. [Associate Network ACL] ダイアログボックスで [Yes, Associate] をクリックします。

ネットワーク ACL とサブネットの関連付けの解除

サブネットとネットワーク ACL の関連付けを解除することができます。例えば、カスタムネットワーク ACL と関連付けられているサブネットがあり、そのサブネットをデフォルトのネットワーク ACL と関連付ける場合があります。サブネットとカスタムネットワーク ACL の関連付けを解除すると、そのサブネットはデフォルトのネットワーク ACL と関連付けられます。

サブネットとネットワーク ACL の関連付けを解除するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Network ACLs] をクリックしてから、ネットワーク ACL を選択します。
3. 詳細ペインで [Associations] タブをクリックします。
4. [Disassociate] をクリックします。



5. [Disassociate Network ACL] ダイアログボックスで [Yes, Disassociate] をクリックします。

サブネットのネットワーク ACL の変更

サブネットが関連付けられているネットワーク ACL を変更できます。例えば、サブネットを作成すると、初期状態で、そのサブネットにはデフォルトのネットワーク ACL が関連付けられます。このサブネットには、作成したカスタムネットワーク ACL を関連付けることができます。

サブネットのネットワーク ACL を変更した後は、サブネット内のインスタンスを終了して再起動する必要はありません。短時間で変更が反映されます。

サブネットのネットワーク ACL の関連付けを変更するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Subnets] をクリックし、サブネットを選択します。
3. 詳細ペインで、サブネットに関連付けられたネットワーク ACL の ID の横に表示される [Replace] をクリックします。

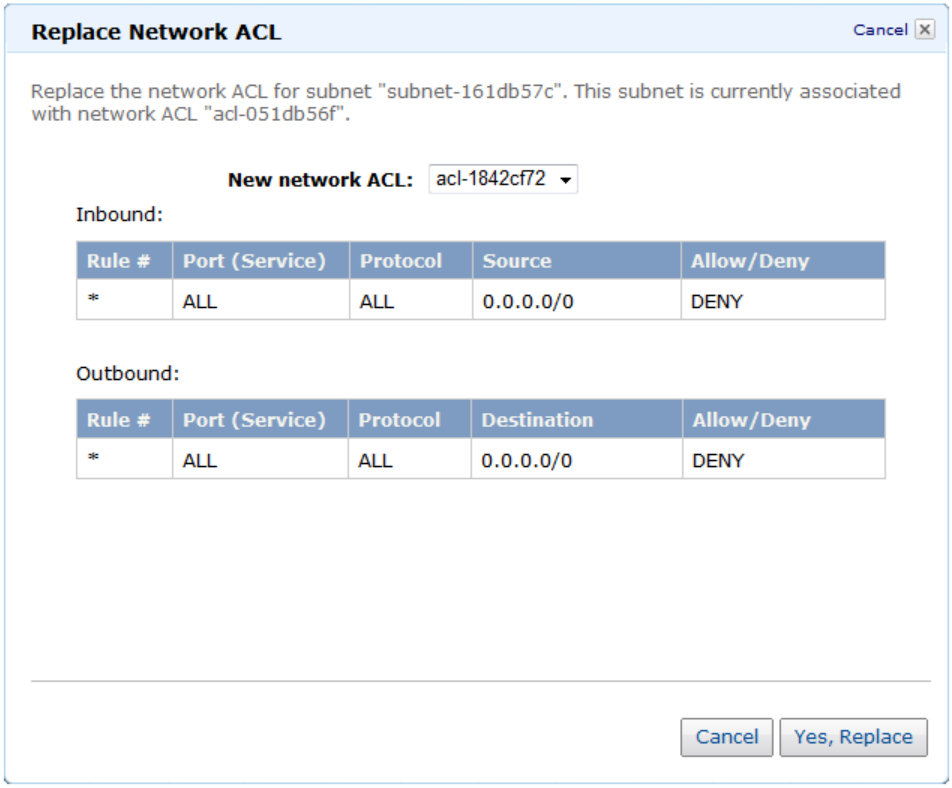
Network ACL: Default (replace)
Inbound:

Rule #	Port (Service)	Protocol	Source	Allow/Deny
100	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL	ALL	0.0.0.0/0	DENY

Outbound:

Rule #	Port (Service)	Protocol	Destination	Allow/Deny
100	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL	ALL	0.0.0.0/0	DENY

4. [Replace Network ACL] ダイアログボックスのドロップダウンリストで、サブネットを関連付けるネットワーク ACL を選択し、[Yes, Replace] をクリックします。



ネットワーク ACL の削除

ネットワーク ACL に関連付けられているサブネットがない場合にのみ、そのネットワーク ACL を削除できます。デフォルトのネットワーク ACL は削除できません。

ネットワーク ACL を削除するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Network ACLs] をクリックします。
3. ネットワーク ACL を選択してから、[Delete] ボタンをクリックします。
4. [Delete Network ACL] ダイアログボックスで [Yes, Delete] をクリックします。

API とコマンドの概要

次の表は、使用できるネットワーク ACL コマンドと、それに対応する API アクションの概要です。

説明	コマンド	API アクション
VPC のネットワーク ACL を作成します。	ec2-create-network-acl	CreateNetworkAcl
1 つまたは複数のネットワーク ACL について説明します。	ec2-describe-network-acls	DescribeNetworkAcls
ネットワーク ACL を削除します。	ec2-delete-network-acl	DeleteNetworkAcl

説明	コマンド	API アクション
ルールをネットワーク ACL に追加します。	ec2-create-network-acl-entry	CreateNetworkAclEntry
ネットワーク ACL からルールを削除します。	ec2-delete-network-acl-entry	DeleteNetworkAclEntry
ネットワーク ACL の既存のルールを置換します。	ec2-replace-network-acl-entry	ReplaceNetworkAclEntry
サブネットを関連付けるネットワーク ACL を変更します。	ec2-replace-network-acl-association	ReplaceNetworkAclAssociation

VPC に推奨されるネットワーク ACL ルール

Topics

このガイドで前述したシナリオでは、デフォルトのネットワーク ACL をデフォルトのルールで使用しています。デフォルトのルールでは、サブネットのインバウンドトラフィックとアウトバンドトラフィックのすべてを許可しています。つまり実質的には、VPC のセキュリティを向上するための ACL を使用していません。

この付録では、このガイドで使用しているシナリオで、セキュリティの追加レイヤーが必要な場合に推奨するネットワーク ACL ルールについて説明します。ネットワーク ACL とその使用方法の詳細については、「ネットワーク ACL (p. 77)」を参照してください。

Important

次の ACL 例では、49152 ~ 65535 という一時ポートの範囲を使用しています。この範囲は変更できます。詳細については、「一時ポート (p. 81)」を参照してください。

シナリオ 1 に推奨されるルール

シナリオ1には、インターネットトラフィックを送受信できるインスタンスを含む単一のサブネットがあります。シナリオ 1 の詳細については、「シナリオ 1: 1 つのパブリックサブネットのみを持つ VPC (p. 9)」を参照してください。

次の表は、推奨されるルールを示します。これらのルールでは、明示的に必要なトラフィックを除き、すべてのトラフィックをブロックします。

インバウンド					
ルール番号	送信元 IP	プロトコル	ポート	許可/拒否	コメント
100	0.0.0.0/0	TCP	80	許可	すべての場所からのインバウンド HTTP トラフィックを許可します

110	0.0.0.0/0	TCP	443	許可	すべての場所からのインバウンド HTTPS トラフィックを許可します
120	ホームネットワークのパブリック IP アドレスの範囲	TCP	22	許可	(インターネットゲートウェイを介した) ホームネットワークからのインバウンド SSH トラフィックを許可します
130	ホームネットワークのパブリック IP アドレスの範囲	TCP	3389	許可	(インターネットゲートウェイを介した) ホームネットワークからのインバウンド RDP トラフィックを許可します
140	0.0.0.0/0	TCP	49152 ~ 65535	許可	送信元がサブネットであるリクエストからのインバウンドリターントラフィックを許可します 正しい一時ポートの指定については、このトピックの冒頭にある「重要」を参照してください。
*	0.0.0.0/0	すべて	すべて	拒否	前のルールでまだ処理されていないすべてのインバウンドトラフィックを拒否します (変更不可能)
アウトバウンド					
ルール番号	送信先 IP	プロトコル	ポート	許可/拒否	コメント
100	0.0.0.0/0	TCP	80	許可	サブネットからインターネットへのアウトバウンド HTTP トラフィックを許可します
110	0.0.0.0/0	TCP	443	許可	サブネットからインターネットへのアウトバウンド HTTPS トラフィックを許可します
120	0.0.0.0/0	TCP	49152 ~ 65535	許可	インターネット上のクライアントに対するアウトバウンド応答を許可します (サブネットのウェブサーバーに訪問するユーザーにウェブページを提供するなどの処理) 正しい一時ポートの指定については、このトピックの冒頭にある「重要」を参照してください。

*	0.0.0.0/0	すべて	すべて	拒否	前のルールでまだ処理されていないすべてのアウトバウンドトラフィックを拒否します（変更不可能）

シナリオ 2 に推奨されるルール

シナリオ2では、インターネットトラフィックを送受信できるインスタンスを含むパブリックサブネットと、インターネットからのトラフィックを直接受信できないプライベートサブネットがあります。ただし、プライベートサブネットは、パブリックサブネットの NAT インスタンスを介して、インターネットに対するアウトバウンドトラフィックを開始すること（および応答を受信すること）はできます。シナリオ 2 の詳細については、「シナリオ 2: パブリックサブネットとプライベートサブネットを持つ VPC (p. 16)」を参照してください。

このシナリオの場合、パブリックサブネット用のネットワーク ACL とは別に、プライベートサブネット用のネットワーク ACL があります。次の表に、各 ACL に推奨されるルールを示します。これらのルールでは、明示的に必要なトラフィックを除き、すべてのトラフィックをブロックします。これらのルールは、このシナリオのセキュリティグループルールとほとんど同じです。

パブリックサブネット用の ACL ルール

インバウンド					
ルール番号	送信元 IP	プロトコル	ポート	許可/拒否	コメント
100	0.0.0.0/0	TCP	80	許可	すべての場所からのインバウンド HTTP トラフィックを許可します
110	0.0.0.0/0	TCP	443	許可	すべての場所からのインバウンドHTTPSトラフィックを許可します
120	ホームネットワークのパブリック IP アドレスの範囲	TCP	22	許可	（インターネットゲートウェイを介した）ホームネットワークからのインバウンドSSHトラフィックを許可します
130	ホームネットワークのパブリック IP アドレスの範囲	TCP	3389	許可	（インターネットゲートウェイを介した）ホームネットワークからのインバウンドRDPトラフィックを許可します
140	0.0.0.0/0	TCP	49152 ~ 65535	許可	送信元がサブネットであるリクエストからのインバウンドリターントラフィックを許可します 正しい一時ポートの指定については、このトピックの冒頭にある「重要」を参照してください。

*	0.0.0.0/0	すべて	すべて	拒否	前のルールでまだ処理されていないすべてのインバウンドトラフィックを拒否します（変更不可能）
アウトバウンド					
ルール番号	送信先 IP	プロトコル	ポート	許可/拒否	コメント
100	0.0.0.0/0	TCP	80	許可	サブネットからインターネットへのアウトバウンド HTTP トラフィックを許可します
110	0.0.0.0/0	TCP	443	許可	サブネットからインターネットへのアウトバウンド HTTPS トラフィックを許可します
120	10.0.1.0/24	TCP	1433	許可	プライベートサブネット内のデータベースサーバーに対するアウトバウンド MS SQL アクセスを許可します
130	10.0.1.0/24	TCP	3306	許可	プライベートサブネット内のデータベースサーバーに対するアウトバウンド MySQL アクセスを許可します
140	0.0.0.0/0	TCP	49152 ~ 65535	許可	インターネット上のクライアントに対するアウトバウンド応答を許可します（サブネットのウェブサーバーに訪問するユーザーにウェブページを提供するなどの処理） 正しい一時ポートの指定については、このトピックの冒頭にある「重要」を参照してください。
*	0.0.0.0/0	すべて	すべて	拒否	前のルールでまだ処理されていないすべてのアウトバウンドトラフィックを拒否します（変更不可能）

プライベートサブネット用の ACL ルール

インバウンド					
ルール番号	送信元 IP	プロトコル	ポート	許可/拒否	コメント

100	10.0.0.0/24	TCP	1433	許可	パブリックサブネット内のウェブサーバーから、プライベートサブネット内の MS SQL サーバーに対する読み取りと書き込みを許可します
110	10.0.0.0/24	TCP	3306	許可	パブリックサブネット内のウェブサーバーから、プライベートサブネット内の MySQL サーバーに対する読み取りと書き込みを許可します
120	10.0.0.0/24	TCP	22	許可	パブリックサブネット内の SSH 拠点からのインバウンド SSH トラフィックを許可します
130	10.0.0.0/24	TCP	3389	許可	パブリックサブネット内の Microsoft Terminal Services ゲートウェイからのインバウンド TDP トラフィックを許可します
140	10.0.0.0/24	TCP	49152 ~ 65535	許可	送信元がプライベートサブネットであるリクエストについて、パブリックサブネットの NAT インスタンスからのインバウンドリターントラフィックを許可します 正しい一時ポートの指定については、このトピックの冒頭にある「重要」を参照してください。
*	0.0.0.0/0	すべて	すべて	拒否	前のルールでまだ処理されていないすべてのインバウンドトラフィックを拒否します（変更不可能）
アウトバウンド					
ルール番号	送信先 IP	プロトコル	ポート	許可/拒否	コメント
100	0.0.0.0/0	TCP	80	許可	サブネットからインターネットへのアウトバウンド HTTP トラフィックを許可します
110	0.0.0.0/0	TCP	443	許可	サブネットからインターネットへのアウトバウンド HTTPS トラフィックを許可します

120	10.0.0.0/24	TCP	49152 ~ 65535	許可	パブリックサブネットに対するアウトバウンド応答を許可します (例えば、プライベートサブネット内の DB サーバーと通信している、パブリックサブネット内のウェブサーバーに対する応答) 正しい一時ポートの指定については、このトピックの冒頭にある「重要」を参照してください。
*	0.0.0.0/0	すべて	すべて	拒否	前のルールでまだ処理されていないすべてのアウトバウンドトラフィックを拒否します (変更不可能)

シナリオ 3 に推奨されるルール

シナリオ3では、インターネットトラフィックを送受信できるインスタンスを含むパブリックサブネットと、VPN 接続でホームネットワークとのみ通信できるインスタンスを含む VPN のみのサブネットがあります。シナリオ3の詳細については、「シナリオ3: パブリックサブネットとプライベートサブネット、およびハードウェア VPN アクセスを持つ VPC (p. 28)」を参照してください。

このシナリオの場合、パブリックサブネット用のネットワーク ACL とは別に、VPN のみのサブネット用のネットワーク ACL があります。次の表に、各 ACL に推奨されるルールを示します。これらのルールでは、明示的に必要なトラフィックを除き、すべてのトラフィックをブロックします。

パブリックサブネット用の ACL ルール

インバウンド					
ルール番号	送信元 IP	プロトコル	ポート	許可/拒否	コメント
100	0.0.0.0/0	TCP	80	許可	任意の場所からウェブサーバーへのインバウンド HTTP トラフィックを許可します
110	0.0.0.0/0	TCP	443	許可	任意の場所からウェブサーバーへのインバウンド HTTPS トラフィックを許可します
120	ホームネットワークのパブリック IP アドレスの範囲	TCP	22	許可	(インターネットゲートウェイを介した) ホームネットワークからウェブサーバーへのインバウンド SSH トラフィックを許可します

130	ホームネットワークのパブリック IP アドレスの範囲	TCP	3389	許可	（インターネットゲートウェイを介した）ホームネットワークからウェブサーバーへのインバウンド RDP トラフィックを許可します
140	0.0.0.0/0	TCP	49152 ~ 65535	許可	送信元がサブネットであるリクエストからのインバウンドリターントラフィックを許可します 正しい一時ポートの指定については、このトピックの冒頭にある「重要」を参照してください。
*	0.0.0.0/0	すべて	すべて	拒否	前のルールでまだ処理されていないすべてのインバウンドトラフィックを拒否します（変更不可能）
アウトバウンド					
ルール番号	送信先 IP	プロトコル	ポート	許可/拒否	コメント
100	0.0.0.0/0	TCP	80	許可	サブネットからインターネットへのアウトバウンド HTTP トラフィックを許可します
110	0.0.0.0/0	TCP	443	許可	サブネットからインターネットへのアウトバウンド HTTPS トラフィックを許可します
120	10.0.1.0/24	TCP	1433	許可	VPN のみのサブネット内のデータベースサーバーに対するアウトバウンド MS SQL アクセスを許可します
130	10.0.1.0/24	TCP	3306	許可	VPN のみのサブネット内のデータベースサーバーに対するアウトバウンド MySQL アクセスを許可します
140	0.0.0.0/0	TCP	49152 ~ 65535	許可	インターネット上のクライアントに対するアウトバウンド応答を許可します（サブネットのウェブサーバーに訪問するユーザーにウェブページを提供するなどの処理） 正しい一時ポートの指定については、このトピックの冒頭にある「重要」を参照してください。

*	0.0.0.0/0	すべて	すべて	拒否	前のルールでまだ処理されていないすべてのアウトバウンドトラフィックを拒否します（変更不可能）

VPN のみのサブネットの ACL 設定

インバウンド					
ルール番号	送信元 IP	プロトコル	ポート	許可/拒否	コメント
100	10.0.0.0/24	TCP	1433	許可	パブリックサブネット内のウェブサーバーから、VPN のみのサブネット内の MS SQL サーバーに対する読み取りと書き込みを許可します
110	10.0.0.0/24	TCP	3306	許可	パブリックサブネット内のウェブサーバーから、VPN のみのサブネット内の MySQL サーバーに対する読み取りと書き込みを許可します
120	ホームネットワークのプライベート IP アドレスの範囲	TCP	22	許可	（仮想プライベートゲートウェイを介した）ホームネットワークからのインバウンド SSH トラフィックを許可します
130	ホームネットワークのプライベート IP アドレスの範囲	TCP	3389	許可	（仮想プライベートゲートウェイを介した）ホームネットワークからのインバウンド RDP トラフィックを許可します
140	ホームネットワークのプライベート IP アドレスの範囲	TCP	49152 ~ 65535	許可	（仮想プライベートゲートウェイを介した）ホームネットワークのクライアントからのインバウンドリターントラフィックを拒否します 正しい一時ポートの指定については、このトピックの冒頭にある「重要」を参照してください。
*	0.0.0.0/0	すべて	すべて	拒否	前のルールでまだ処理されていないすべてのインバウンドトラフィックを拒否します（変更不可能）
アウトバウンド					
ルール番号	送信先 IP	プロトコル	ポート	許可/拒否	コメント

100	ホームネットワークのプライベート IP アドレスの範囲	すべて	すべて	許可	（仮想プライベートゲートウェイを介した）サブネットからホームネットワークに対するすべてのアウトバウンドトラフィックを許可します
110	10.0.0.0/24	TCP	49152 ~ 65535	許可	パブリックサブネット内のウェブサーバーに対するアウトバウンド応答を許可します 正しい一時ポートの指定については、このトピックの冒頭にある「重要」を参照してください。
120	ホームネットワークのプライベート IP アドレスの範囲	TCP	49152 ~ 65535	許可	（仮想プライベートゲートウェイを介した）ホームネットワークのクライアントに対するアウトバウンド応答を拒否します 正しい一時ポートの指定については、このトピックの冒頭にある「重要」を参照してください。
*	0.0.0.0/0	すべて	すべて	拒否	前のルールでまだ処理されていないすべてのアウトバウンドトラフィックを拒否します（変更不可能）

シナリオ 4 に推奨されるルール

シナリオ4では、VPN 接続でホームネットワークとのみ通信できるインスタンスを含む単一のサブネットがあります。シナリオ 4 の詳細については、「シナリオ 4: 1 つのプライベートサブネットのみ、およびハードウェア VPN アクセスを持つ VPC (p. 42)」を参照してください。

次の表は、推奨されるルールを示します。これらのルールでは、明示的に必要なトラフィックを除き、すべてのトラフィックをブロックします。

インバウンド					
ルール番号	送信元 IP	プロトコル	ポート	許可/拒否	コメント
100	ホームネットワークのプライベート IP アドレスの範囲	TCP	22	許可	ホームネットワークからサブネットに対するインバウンド SSH トラフィックを許可します
110	ホームネットワークのプライベート IP アドレスの範囲	TCP	3389	許可	ホームネットワークからサブネットに対するインバウンド RDP トラフィックを許可します

120	ホームネットワークのプライベート IP アドレスの範囲	TCP	49152 ~ 65535	許可	送信元がサブネットであるリクエストからのインバウンドリターントラフィックを許可します 正しい一時ポートの指定については、このトピックの冒頭にある「重要」を参照してください。
*	0.0.0.0/0	すべて	すべて	拒否	前のルールでまだ処理されていないすべてのインバウンドトラフィックを拒否します（変更不可能）
アウトバウンド					
ルール番号	送信先 IP	プロトコル	ポート	許可/拒否	コメント
100	ホームネットワークのプライベート IP アドレスの範囲	すべて	すべて	許可	サブネットからホームネットワークに対するすべてのアウトバンドトラフィックを許可します
120	ホームネットワークのプライベート IP アドレスの範囲	TCP	49152 ~ 65535	許可	ホームネットワークのクライアントに対するアウトバウンド応答を拒否します 正しい一時ポートの指定については、このトピックの冒頭にある「重要」を参照してください。
*	0.0.0.0/0	すべて	すべて	拒否	前のルールでまだ処理されていないすべてのアウトバウンドトラフィックを拒否します（変更不可能）

Amazon VPC のリソースに対するアクセスの制御

仮想プライベートクラウド（VPC）を設定および管理できるユーザーを制御する必要がありますか？インターネットゲートウェイをアタッチできるユーザーや、セキュリティグループとネットワーク ACL を定義できるユーザーを制御する必要がありますか？AWS Identity and Access Management（IAM）を使用して、アカウント内でユーザーとグループを作成および管理し、各ユーザーとグループが使用できる API アクションと Amazon VPC リソースを制御できます。これにより、組織の全員が VPC のレイアウト、ルーティング、セキュリティを変更しないようにできます。

ユーザー、グループ、ポリシーの作成の詳細については、「*Amazon Elastic Compute Cloud User Guide*」の Amazon EC2 リソースへのアクセスの制御を参照してください。

Amazon VPC 用のポリシー例

Example 1. VPC を管理する

以下のポリシーは、VPC を作成および管理する許可をユーザーに与えます。このポリシーはネットワーク管理者のグループに割り当てることができます。[Action] エレメントは、VPC、サブネット、インターネットゲートウェイ、カスタマーゲートウェイ、仮想プライベートゲートウェイ、VPN 接続、ルートテーブル、Elastic IP アドレス、セキュリティグループ、ネットワーク ACL、および DHCP オプションセットに関連した API アクションを指定します。また、このポリシーにより、グループはインスタンスを実行、停止、開始、および終了することを許可されます。さらに、グループは Amazon EC2 のリソースを一覧表示することもできます。

```
{
    "Statement":[{
    "Effect":"Allow",
    "Action":["ec2:*Vpc*",
              "ec2:*Subnet*",
              "ec2:*Gateway*",
              "ec2:*Vpn*",
              "ec2:*Route*",
              "ec2:*Address*",
              "ec2:*SecurityGroup*",
              "ec2:*NetworkAcl*",
              "ec2:*DhcpOptions*",
              "ec2:RunInstances",
              "ec2:StopInstances",
              "ec2:StartInstances",
              "ec2:TerminateInstances",
              "ec2:Describe*"],
    "Resource":"*"
    }
  ]
  }
```

ポリシーでは、ワイルドカードを使用して、各オブジェクトタイプに許可されるアクションをすべて指定します (例: `*SecurityGroup*`)。または、各アクションを明示的にリストすることもできます。ワイルドカードを使用する場合は、名前にワイルドカード文字列を含む新しいアクションをポリシーに追加すると、そのポリシーによってグループには自動的に新しいアクションへのアクセスが許可されることにご留意ください。

Example 2. Amazon VPC 用の読み取り専用ポリシー

次のポリシーは、VPC とそのコンポーネントをリストする許可をユーザーに与えます。ユーザーは、VPC を作成、更新、または削除することはできません。

```
{
    "Statement":[{
    "Effect":"Allow",
    "Action":["ec2:DescribeVpcs",
              "ec2:DescribeSubnets",
              "ec2:DescribeInternetGateways",
              "ec2:DescribeCustomerGateways",
              "ec2:DescribeVpnGateways",
              "ec2:DescribeVpnConnections",
              "ec2:DescribeRouteTables",
              "ec2:DescribeAddresses",
              "ec2:DescribeSecurityGroups",
              "ec2:DescribeNetworkAcls",
              "ec2:DescribeDhcpOptions",
              "ec2:DescribeTags",
              "ec2:DescribeInstances"],
    "Resource":"*"
    }
  ]
}
```

Example 3. Amazon VPC 用のカスタムポリシー

次のポリシーは、インスタンスの起動、インスタンスの停止、インスタンスの開始、インスタンスの終了の許可をユーザーに与え、Amazon EC2 および Amazon VPC で利用できるリソースについて説明します。

ポリシーの 2 番目の定義文は、その他のポリシーで明示的に許可を否定することにより、ユーザーに許可される可能性がある広範囲の API アクションへのアクセスを否定しています。

```
{
  "Statement":[{
    "Effect":"Allow",
    "Action":["ec2:RunInstances",
              "ec2:StopInstances",
              "ec2:StartInstances",
              "ec2:TerminateInstances",
              "ec2:Describe*"],
     "Resource":"*"
     },
     {
     "Effect":"Deny",
     "NotAction":["ec2:RunInstances",
                  "ec2:StopInstances",
                  "ec2:StartInstances",
                  "ec2:TerminateInstances",
                  "ec2:Describe*"],
     "Resource":"*"
     }
  ]
}
```

VPC でのネットワーキング

次のコンポーネントを使用して VPC にネットワーキングを設定できます。

- IP アドレス (p. 101)
- ネットワークインターフェイス (p. 105)
- ルートテーブル (p. 106)
- インターネットゲートウェイ (p. 117)
- NAT インスタンス (p. 122)
- DHCP オプションセット (p. 127)
- DNS (p. 133)

VPC の IP アドレス指定

ここでは、VPC の Amazon EC2 インスタンスに使用できる IP アドレスについて説明します。

パブリック IP アドレスとプライベート IP アドレス

VPC 内のインスタンス間で通信するには、プライベート IP アドレスを使用できます。インスタンスとインターネット間で通信するには、パブリック IP アドレスを使用できます。

VPC 内の各インスタンスには、デフォルトのネットワークインターフェイスがあり、そのインターフェイスには、サブネットのアドレス範囲内のプライマリプライベート IP アドレスが割り当てられています。プライマリプライベート IP アドレスを指定しない場合、サブネットの範囲内で使用可能な IP アドレスが選択されます。ネットワークインターフェイスの詳細については、「*Amazon Elastic Compute Cloud User Guide*」の Elastic Network Interfaces を参照してください。

デフォルトのサブネットの場合、インスタンスの起動時に、ネットワークインターフェイスに 2 つの IP アドレスが自動的に割り当てられます。プライマリプライベート IP アドレスとパブリック IP アドレスです。パブリック IP アドレスは、ネットワークアドレス変換 (NAT) を介してプライマリプライベート IP アドレスにマップされます。

デフォルトではないサブネットの場合、ネットワークインターフェイスにはデフォルトでプライベート IP アドレスのみが自動的に割り当てられます。ネットワークインターフェイスにパブリック IP アドレスが割り当てられるのは、起動中にこれを指定する場合のみです。詳細については、「起動中のパブリック IP アドレスの割り当て (p. 102)」を参照してください。デフォルトではないサブネットのインス

タンスがインターネットと通信できるようにするには、VPC に使用する Elastic IP アドレスを割り当て、そのEIPを、インスタンスにアタッチされたネットワークインターフェイスが指定するプライベート IP アドレスに割り当てる必要があります。詳細については、「Elastic IP アドレス (p. 103)」を参照してください。

VPC で実行されているインスタンスに、セカンダリプライベート IP アドレスと呼ばれる、追加の IP アドレスを割り当てることができます。プライマリプライベート IP アドレスとは異なり、セカンダリプライベート IP アドレスを 1 つのネットワークインターフェイスから他のネットワークインターフェイスへ、または1つのインスタンスから他のインスタンスへ再割り当てすることができます。プライマリ IP アドレスとセカンダリ IP アドレスの詳細については、「*Amazon Elastic Compute Cloud User Guide*」の複数の IP アドレスを参照してください。

起動中のパブリック IP アドレスの割り当て

デフォルトでは、デフォルトのサブネット内に起動されたインスタンスのみにパブリック IP アドレスが割り当てられます。ただし、インスタンスにパブリック IP アドレスが割り当てられるかどうかを制御するために、起動時にパブリック IP アドレス指定機能を利用できます。

インスタンスの起動時にパブリック IP アドレス指定機能にアクセスするには

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. [Launch Instance] をクリックします。
3. [Create a New Instance] ページで、[Classic Wizard] を選択してから [Continue] をクリックします。
4. [CHOOSE AN AMI] ページで、AMI を選択し、その [Select] ボタンを選択します。
5. [INSTANCE DETAILS] ページで、起動するインスタンスの数とタイプを設定します。サブネットを選択し、[Continue] をクリックします。
6. 次の [INSTANCE DETAILS] ページの [Number of Network Interfaces] セクションで、[Assign Public IP] チェックボックスをオンにすると、インスタンスにパブリック IP アドレスが割り当てられます。デフォルトのサブネットを選択するか、サブネットに対して [No Preference] を指定した場合、[Assign Public IP] チェックボックスがデフォルトでオンになります。

   Note

   アカウントで EC2-VPC のみをサポートしていて、サブネットに対して [No Preference] を選択した場合、[Number of Network Interfaces] セクションは表示されません。代わりに、[Assign Public IP] チェックボックスのみが表示されます。

   スポットインスタンスをリクエストしている場合は、[Number of Network Interfaces] セクションは表示されません。[Public IP] チェックボックスのみが表示されます。スポットインスタンスのリクエストの詳細については、「*Amazon Elastic Compute Cloud User Guide*」の Creating a Spot Instance Request を参照してください。

次のルールが適用されます。

- パブリック IP アドレスは、デバイスインデックスが eth0 の単一のネットワークインターフェイスのみに関連付けることができます。複数のネットワークインターフェイスを起動する場合、[Assign Public IP] チェックボックスは使用できず、eth1 ネットワークインターフェイスでは使用できません。
- パブリック IP アドレスは、既存のインターフェイスではなく、新しいネットワークインターフェイスのみに割り当てることができます。

この機能は起動中のみ使用できます。ただし、起動中にパブリック IP アドレスをインスタンスに割り当てるかどうかにかかわらず、起動後にインスタンスに Elastic IP アドレスを関連付けることができます。詳細については、「Elastic IP アドレス (p. 103)」を参照してください。

パブリック IP アドレス指定の API とコマンドラインツール

パブリックアドレス指定機能を有効または無効にするには、`NetworkInterface.n.AssociatePublicIpAddress` パラメーターを RunInstances リクエストに使用するか、`--associate-public-ip-address` オプションを ec2-run-instances コマンドに使用します。

Elastic IP アドレス

*Elastic IP アドレス*は、動的なクラウドコンピューティングのために設計された静的なパブリック IP アドレスです。Elastic IP アドレスは、VPC の任意のインスタンスまたはネットワークインターフェイスに関連付けることができます。EIP を使用すると、アドレスを VPC 内の別のインスタンスへ迅速に再マップすることで、インスタンスのエラーを隠すことができます。Elastic IP アドレスを直接インスタンスに関連付けずにネットワークインターフェイスに関連付ける利点は、1 つのステップでネットワークインターフェイスの全属性を 1 つのインスタンスから別のインスタンスに移動できることです。

Topics

Elastic IP アドレスの基本

Elastic IP アドレスについて知っておく必要がある基本的な情報を以下に示します。

- まず VPC で使用するために EIP を割り当ててから、それを VPC 内のインスタンスに関連付けます（同時に割り当てることができるのは 1 つのインスタンスのみです）。
- EIP はネットワークインターフェイスのプロパティです。EIP をインスタンスに割り当てるには、インスタンスにアタッチされているネットワークインターフェイスを更新します。
- パブリック IP アドレスは、起動中にインスタンスの eth0 ネットワークインターフェイスに割り当てることができます。詳細については、「起動中のパブリック IP アドレスの割り当て (p. 102)」を参照してください。起動後に EIP を eth0 ネットワークインターフェイスに関連付ける場合、現在のパブリック IP アドレスが EC2-VPC パブリック IP アドレスプールに解放されます。EIP の関連付けを解除すると、数分内に新しいパブリック IP アドレスが eth0 ネットワークインターフェイスに自動的に割り当てられます。2 番目のネットワークインターフェイスをインスタンスにアタッチした場合、これは該当しません。その場合は、EIP を手動で eth0 ネットワークインターフェイスに手動で関連付ける必要があります。
- VPC で使用する EIP と、EC2-Classic で使用する EIP には違いがあります。詳細については、「*Amazon Elastic Compute Cloud User Guide*」の EC2-Classic と Amazon EC2-VPC の違い を参照してください。
- EIP は別のインスタンスに移動できます。同じ VPC 内または別の VPC 内のインスタンスに移動することはできますが、EC2-Classic 内のインスタンスに移動することはできません。
- EIP と AWS アカウントの関連付けは、明示的に関連付けを解放するまで維持されます。
- EIP を効率的に使用するため、EIP が実行中のインスタンスに関連付けられていない場合や、停止しているインスタンスやアタッチされていないネットワークインターフェイスに関連付けられている場合は、時間毎に小額の料金が請求されます。インスタンスを実行しているときは、インスタンスに関連付けられた 1 つの EIP については課金されませんが、インスタンスに関連付けられた追加の EIP がある場合、追加分には課金されます。

- Elastic IP アドレスは、枯渇しないようにユーザー 1 人に対して最大 5 個に制限されています。また、NAT インスタンスを使用することができます (「NAT インスタンス (p. 122)」を参照してください) 。

Elastic IP アドレスの操作

Elastic IP アドレスを割り当ててから、VPC 内のインスタンスと関連付けることができます。

VPC で使用するための Elastic IP アドレスを割り当てるには

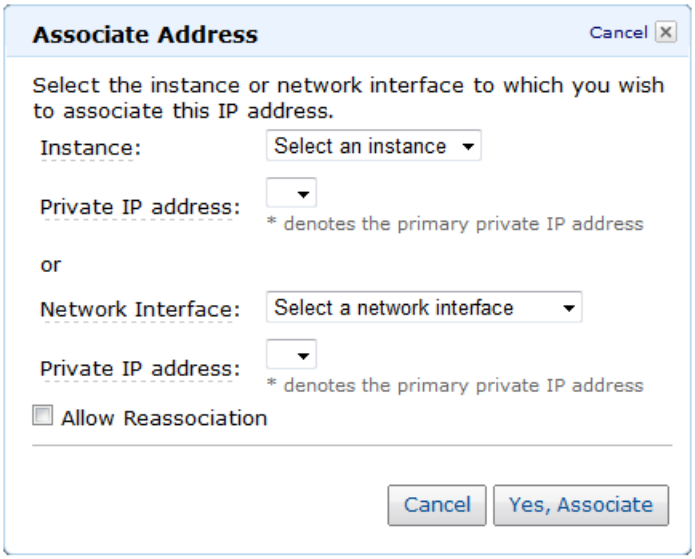
1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Elastic IPs] をクリックします。
3. [Allocate New Address] ボタンをクリックします。
4. [EIP used in] リストで VPC を選択し、[Yes, Allocate] をクリックします。

EIP を表示するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Elastic IPs] をクリックします。
3. 表示されているリストをフィルタするには、割り当てられているインスタンスの EIP または ID の一部を検索ボックスに入力します。

Elastic IP アドレスを VPC 内で実行されているインスタンスと関連付けるには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Elastic IPs] をクリックします。
3. この Elastic IP アドレスを選択してから、[Associate Address] ボタンをクリックします。
4. [Associate Address] ダイアログボックスで [Network Interface] リストからネットワークインターフェイスを選択するか、[Instance] リストからインスタンスを選択します。対応する [Private IP Address] リストから EIP を関連付けるアドレスを選択して、[Yes, Associate] をクリックします。



5. （オプション）Elastic IP アドレスをインスタンスに関連付けると、DNS ホスト名が有効な場合は DNS ホスト名を受け取ります。詳細については、「VPC での DNS の使用 (p. 133)」を参照してください。

Elastic IP アドレスと関連付けるインスタンスを変更するには、現在関連付けられているインスタンスから関連付けを解除してから、VPC 内の新しいインスタンスと関連付けます。

Elastic IP アドレスの関連付けを解除するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Elastic IPs] をクリックします。
3. Elastic IP アドレスを選択してから、[Disassociate Address] ボタンをクリックします。
4. プロンプトが表示されたら、[Yes, Disassociate] をクリックします。

Elastic IP アドレスが不要になった場合は、解放することをお勧めします（この Elastic IP アドレスをインスタンスに関連付けることはできません）。VPC で使用するために割り当てられ、インスタンスに関連付けられていない EIP には料金が発生します。

Elastic IP アドレスを解放するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Elastic IPs] をクリックします。
3. Elastic IP アドレスを選択してから、[Release Address] をクリックします。
4. プロンプトが表示されたら、[Yes, Release] をクリックします。

API とコマンドの概要

次の表は、Elastic IP アドレスのコマンドと API アクションの概要です。

説明	コマンド	API アクション
インスタンスで使用する Elastic IP アドレスを取得します。	ec2-allocate-address	AllocateAddress
Elastic IP アドレスをインスタンスまたはネットワークインターフェイスに関連付けます。	ec2-associate-address	AssociateAddress
1 つまたは複数の Elastic IP アドレスの一覧と説明を表示します。	ec2-describe-addresses	DescribeAddresses
インスタンスまたはネットワークインターフェイスから Elastic IP アドレスの関連付けを解除します。	ec2-disassociate-address	DisassociateAddress
AWS アカウントに割り当てられている Elastic IP アドレスを解放します。	ec2-release-address	ReleaseAddress

VPC で Elastic Network Interface を使用する

VPC の各インスタンスには、VPC 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た、デフォルトのネットワークインターフェイスがあります。また、Elastic Network Interface（ENI）と呼ばれる追加のネットワークインターフェイスを作成し、この VPC 内のインスタンスにアタッチす

ることもできます。アタッチできる ENI の数はインスタンスタイプによって異なります。詳細については、「*Amazon Elastic Compute Cloud User Guide*」の「Private IP Addresses Per ENI Per Instance Type」を参照してください。

ENI は、次の属性を指定できる仮想ネットワークインターフェイスです。

- プライマリプライベート IP アドレス
- 1 つ以上のセカンダリプライベート IP アドレス
- プライベート IP アドレスごとに 1 つの Elastic IP アドレス
- MAC アドレス
- 1 つまたは複数のセキュリティグループ
- 送信元/送信先チェックフラグ
- 説明

ENI を作成して、インスタンスへのアタッチ、インスタンスからのデタッチ、および別のインスタンスへのアタッチを行うことができます。ENI の属性は、ENI がインスタンスにアタッチまたはデタッチされたときや、別のインスタンスに再アタッチされたときに、ENI に付随します。インスタンス間で ENI を移動すると、ネットワークトラフィックは、新しいインスタンスにリダイレクトされます。

次の作業を行う場合、複数の ENI をインスタンスにアタッチすると便利です。

- 管理用ネットワークを作成する。
- VPC 内でネットワークアプライアンスやセキュリティアプライアンスを使用する。
- 別個のサブネット上のワークロード/ロールを使用するデュアルホーム接続インスタンスを作成する。
- 低予算で可用性の高いソリューションを作成する。

ENI の詳細、および Amazon EC2 コンソールを使用して ENI を操作する手順については、「*Amazon Elastic Compute Cloud User Guide*」の「Elastic Network Interfaces」を参照してください。

ルートテーブル

*ルートテーブル*には、ネットワークトラフィックの経路を判断する際に使用される、*ルート*と呼ばれる一連のルールが含まれます。

VPC の各サブネットをルートテーブルに関連付ける必要があります。サブネットのルーティングは、このテーブルによってコントロールされます。複数のサブネットを同じルートテーブルに関連付けることができますが、サブネットを関連付けられるのは 1 つのルートテーブルだけです。

Topics

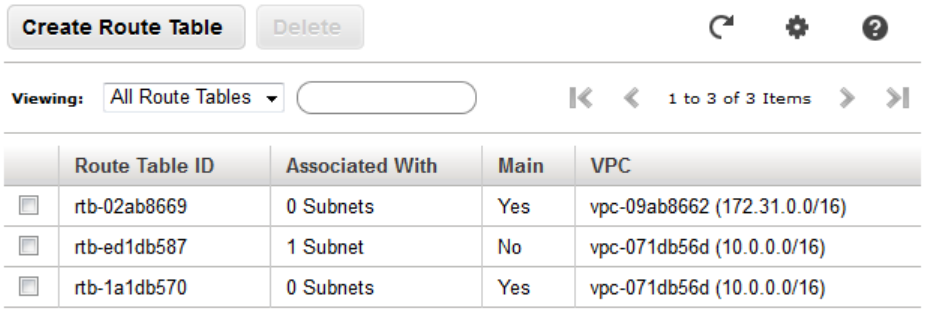
ルートテーブルの基本

ルートテーブルに関して覚えておく必要がある基本事項を次に示します。

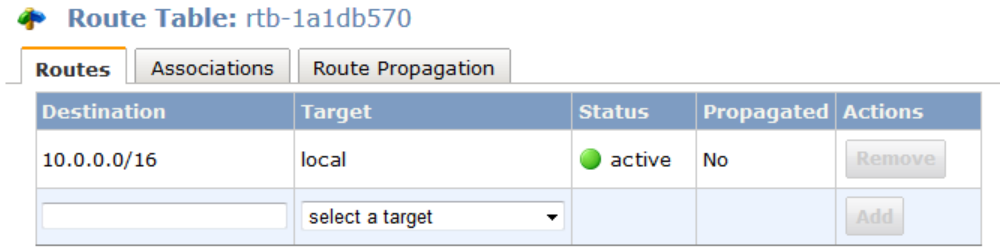
- VPC には暗示的なルーターがあります。
- VPC には、変更できるメインルートテーブルが自動的に割り当てられます。
- VPC に対して追加のカスタムルートテーブルを作成できます。
- 各サブネットをルートテーブルに関連付ける必要があります。サブネットのルーティングは、このテーブルによってコントロールされます。サブネットを特定のルートテーブルに明示的に関連付けないと、そのサブネットでは、メインルートテーブルが使用されます。
- メインルートテーブルは、作成したカスタムテーブルに置き換えることができます (この場合、カスタムテーブルは、新しい各サブネットが関連付けられるデフォルトのテーブルになります)。
- テーブルの各ルートが送信先 CIDR とターゲットを指定します (例えば、送信先が 172.16.0.0/12 のトラフィックのターゲットは仮想プライベートゲートウェイです)。トラフィックに最も合ったルートを使用し、トラフィックのルーティング方法を決定します。

メインルートテーブル

VPC を作成するときに、メインルートテーブルが自動的に割り当てられます。VPC コンソールの次の図は、各 VPC のメインルートテーブルを示しています ([Main] 列は Yes です)。



最初、メインルートテーブル (および VPC 内のすべてのルートテーブル) には、1 つのルート (VPC 内の通信を有効にするローカルルート) しか含まれません。

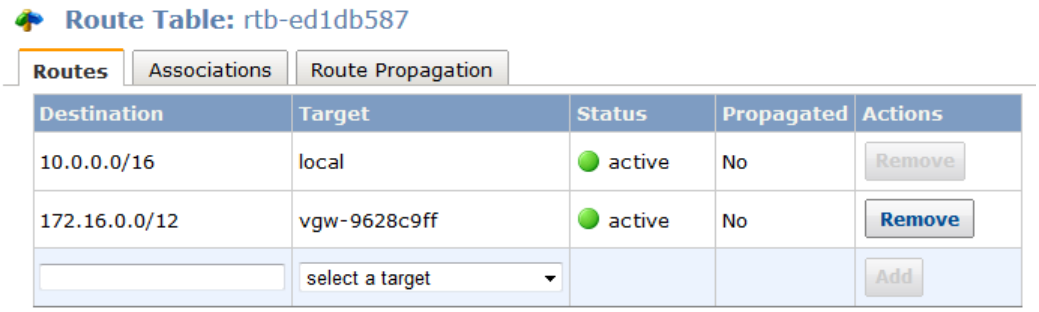


ルートテーブルでは、ローカルルートを変更できません。VPC のインスタンスを起動すると必ず、そのインスタンスは、ローカルルートに自動的に含められます。新しいインスタンスをルートテーブルに追加する必要はありません。

サブネットを特定のルートテーブルに明示的に関連付けないと、そのサブネットは、メインルートテーブルに暗示的に関連付けられます。ただし、そのメインルートテーブルには、引き続きサブネットを明示的に関連付けることができます。この作業は、メインルートテーブルにするテーブルを変更するときに行います (「メインルートテーブルを置き換える (p. 116)」を参照)。

コンソールには、各テーブルに関連付けられているサブネットの数が表示されます。この数には、明示的な関連付けのみが含まれます (「テーブルに明示的に関連付けられているサブネットを特定する (p. 112)」を参照)。

ゲートウェイ (インターネットゲートウェイまたは仮想プライベートゲートウェイのいずれか) を VPC に追加するときに、そのゲートウェイを使用する任意のサブネットのルートテーブルを更新する必要があります。例えば、次の図は、トラフィックを仮想プライベートゲートウェイにルーティングするメインルートテーブルに対する更新を示しています。



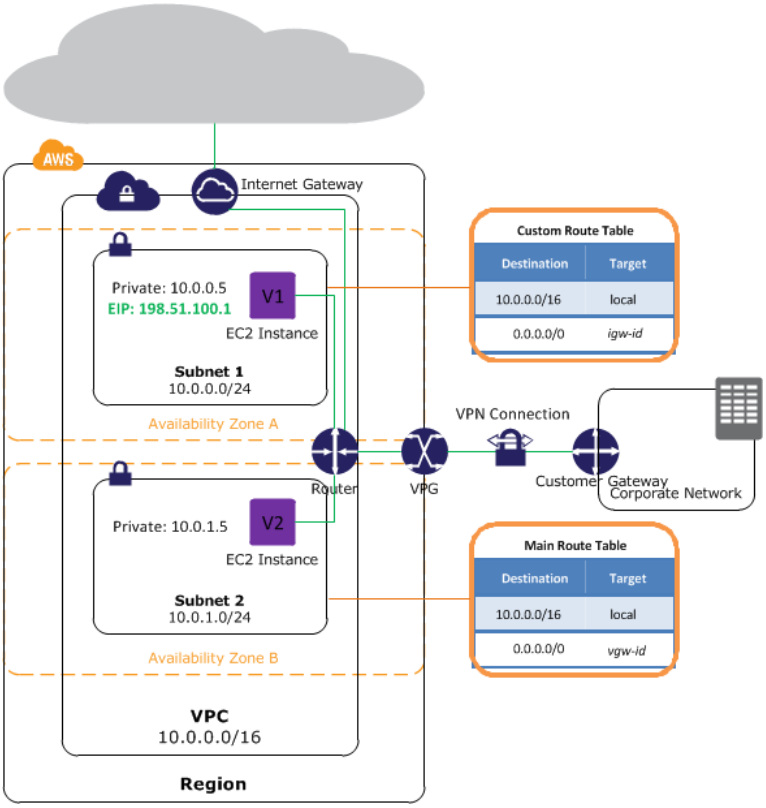
仮想プライベートゲートウェイを VPC にアタッチし、ルートテーブルでルート伝達を有効にした場合は、VPN 接続を表すルートが、伝達されたルートとして、ルートテーブルのルートのリストに自動的に表示されます。

カスタムルートテーブル

VPC は、デフォルトテーブル以外のルートテーブルを持つことができます。VPC を保護するには、メインルートテーブルをローカルルートが 1 つしか含まれない元のデフォルトの状態のままにして、新しいサブネットを作成し、その各サブネットを作成したカスタムルートテーブルの 1 つに明示的に関連付ける方法があります。これにより、各サブネットのアウトバウンドトラフィックのルーティング方法を、明示的にコントロールしなければなりません。

作成できるルートテーブルの数の制限については、「Amazon VPC 制限 (p. 159)」を参照してください。

次の図は、インターネットゲートウェイと仮想プライベートゲートウェイ、およびパブリックサブネットと VPN のみのサブネットを持つ VPC のルーティングを示しています。メインルートテーブルには VPC が割り当てられます。また、VPN のみのサブネットのルートも含まれます。カスタムルートテーブルもあり、これはパブリックサブネット (サブネット 1) に関連付けられています。カスタムルートテーブルには、インターネットゲートウェイ経由のパブリックサブネットのルートが含まれます (送信先は 0.0.0.0/0 で、ターゲットはインターネットゲートウェイです) 。



この VPC で新しいサブネットを作成すると、そのサブネットはメインルートテーブルに自動的に関連付けられ、メインルートテーブルは、そのトラフィックを仮想プライベートゲートウェイにルーティングします。逆の設定 (インターネットゲートウェイへのルートが含まれるメインルートテーブルと、仮想プライベートゲートウェイへのルートが含まれるカスタムルートテーブル) を行い、新しいサブネットを作成すると、そのサブネットには自動的に、インターネットゲートウェイへのルートが含まれるようになります。

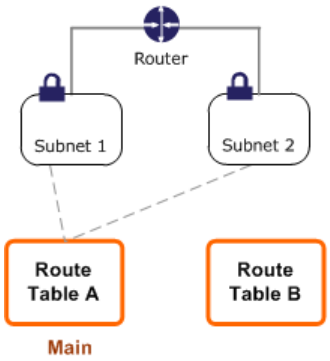
ルートテーブルの関連付け

メインルートテーブルは、サブネットが他のテーブルに明示的に関連付けられていない場合に、サブネットが使用するデフォルトのテーブルです。新しいサブネットを追加すると、そのサブネットでは、メインルートテーブルで指定されているルートが自動的に使用されます。メインルートテーブルにするテーブルは変更できるので、新しい追加サブネットのデフォルトも変更できます。

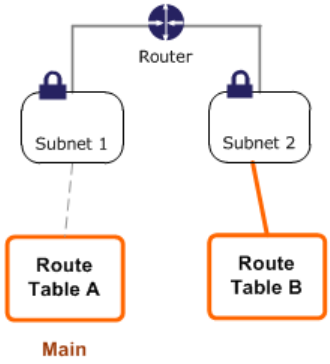
メインルートテーブルには、暗示的または明示的にサブネットを関連付けることができます。サブネットとメインルートテーブルとの間には、通常、明示的な関連付けはありません。ただし、この明示的な関連付けは、メインルートテーブルを置き換えるときに一時的に発生する可能性があります。

トラフィックを中断せずに、メインルートテーブルを変更する必要がある場合は、まず、カスタムルートテーブルを使用して、ルートの変更をテストします。テストの結果に満足したら、メインルートテーブルを新しいカスタムテーブルに置き換えます。

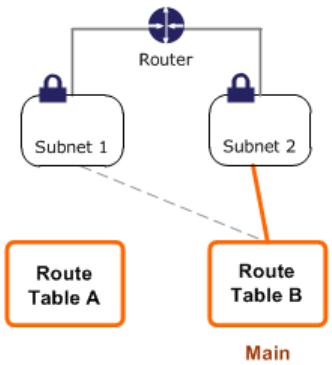
次の図は、メインルートテーブル (ルートテーブル A) に暗示的に関連付けられている 2 つのサブネットを持つ VPC を示しています。カスタムルートテーブル (ルートテーブル B) は、どのサブネットにも関連付けられていません。



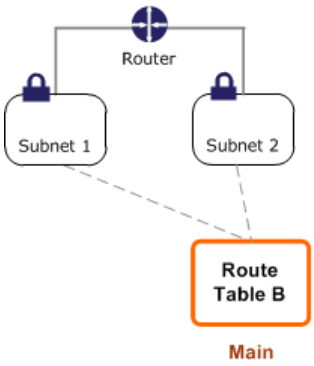
サブネット 2 とルートテーブル B の間には明示的な関連付けを作成できます。



ルートテーブル B をテストしたら、そのテーブルをメインルートテーブルにできます。サブネット 2 とルートテーブル B との間に、まだ明示的な関連付けがあることに注意してください。また、ルートテーブル B は新しいメインルートテーブルなので、サブネット 1 とルートテーブル B の間には暗示的な関連付けがあります。ルートテーブル A はもう使用されていません。



サブネット 2 とルートテーブル B の関連付けを解除しても、サブネット 2 とルートテーブル B との間の暗示的な関連付けは残ります。不要になったルートテーブル A は削除できます。



ルートテーブルを操作する

このセクションでは、ルートテーブルを操作する方法について説明します。

Note

コンソールでウィザードを使用して、ゲートウェイが含まれる VPC を作成すると、そのゲートウェイを使用するようにルートテーブルが自動的に更新されます。コマンドラインツールまたは API を使用して VPC をセットアップする場合、ルートテーブルはご自身で更新する必要があります。

Topics

サブネットが関連付けられているルートテーブルを特定する

サブネットが関連付けられているルートテーブルを特定するには、Amazon VPC コンソールでサブネットの詳細を確認します。

サブネットが関連付けられているルートテーブルを特定するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Subnets] をクリックし、サブネットを選択します。

   サブネットの詳細が詳細ペインに表示されます。詳細には、サブネットが関連付けられているルートテーブルの ID が含まれます (次の画像を参照) 。メインルートテーブルの場合、関連付けが暗示的か明示的かはコンソールに表示されません。メインルートテーブルとの関連付けが明示的かどうかを特定する方法については、「テーブルに明示的に関連付けられているサブネットを特定する (p. 112)」を参照してください。

テーブルに明示的に関連付けられているサブネットを特定する

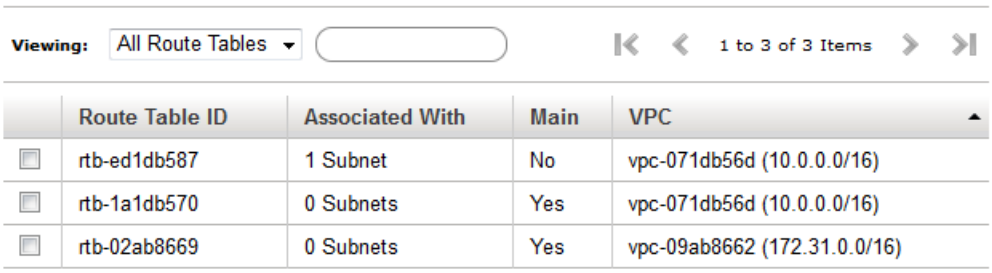
ルートテーブルに明示的に関連付けられているサブネットと、そのサブネットの数を特定できます。

メインルートテーブルは、明示的な関連付けと暗示的な関連付けを持つことができます。カスタムルートテーブルは、明示的な関連付けしか持つことができません。

どのルートテーブルにも明示的に関連付けられていないサブネットは、メインルートテーブルに暗示的に関連付けられています。サブネットをメインルートテーブルに明示的に関連付けることもできます（これを行う理由を示す例については、「メインルートテーブルを置き換える (p. 116)」を参照してください）。

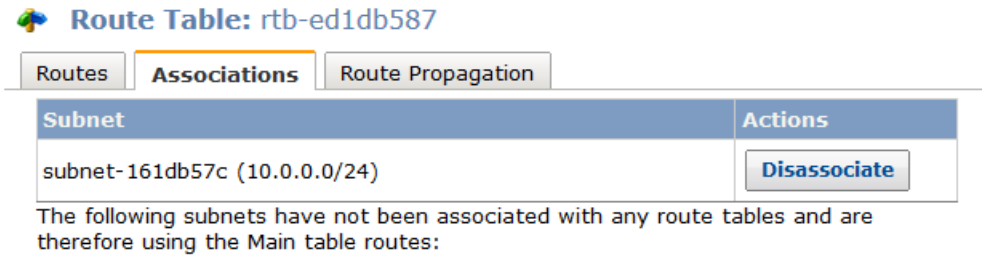
明示的に関連付けられているサブネットの数を特定するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Route Tables] をクリックします。
   [Associated With] 列で、明示的に関連付けられたサブネットの数を確認します。



明示的に関連付けられているサブネットを特定するには

1. 該当するルートテーブルを選択します。
2. 詳細ペインの [Associations] タブをクリックします。このタブには、テーブルに明示的に関連付けられているサブネットが表示されています。また、どのルートテーブルにも関連付けられていない（つまり、メインルートテーブルに暗示的に関連付けられている）サブネットも表示されます。



カスタムルートテーブルを作成する

状況によっては、独自のルートテーブルを作成しなければならないことがあります。

カスタムルートテーブルを作成するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Route Tables] をクリックします。
3. [Create Route Table] ボタンをクリックします。
4. [Create Route Table] ダイアログボックスの [VPC] ドロップダウンリストで、ご利用の VPC を選択し、[Yes, Create] をクリックします。

ルートテーブルでルートを追加および削除する

テーブルのルートは変更できません。追加と削除のみが可能です。

ルートをルートテーブルに追加するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Route Tables] をクリックし、ルートテーブルを選択します。
3. 詳細ペインの [Routes] タブで、ルートの送信先とターゲットを入力し、[Add] をクリックします。
4. [Create Route] ダイアログボックスで、[Yes, Create] をクリックします。

ルートをルートテーブルから削除するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Route Tables] をクリックし、ルートテーブルを選択します。
3. 削除するルートを右クリックし、[Delete] ボタンをクリックします。
4. [Delete Route] ダイアログボックスで、[Yes, Delete] をクリックします。

ルート伝達を有効および無効にする

ルート伝達を使用すると、仮想プライベートゲートウェイが、ルートをルートテーブルに自動的に伝達できます。したがって、ルートテーブルへの VPN ルートを手動で入力する必要はありません。ルートの伝播は有効または無効にできます。

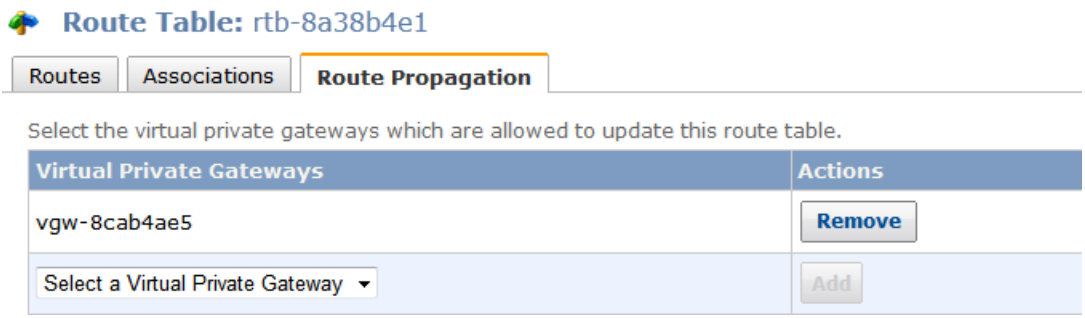
VPN ルートオプションの詳細については、「VPN のルーティングオプション (p. 140)」を参照してください。

ルート伝達を有効にするには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Route Tables] をクリックし、ルートテーブルを選択します。
3. 詳細ペインで、[Route Propagation] タブをクリックします。
4. ドロップダウンリストで仮想プライベートゲートウェイを選択し、[Add] をクリックします。

ルート伝達を無効にするには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Route Tables] をクリックし、ルートテーブルを選択します。
3. 詳細ペインの [Route Propagation] タブで、VGW の ID の横にある [Remove] をクリックします。



4. [Remove Virtual Private Gateway] ダイアログボックスで、[Yes, Disable] をクリックします。

サブネットをルートテーブルに関連付ける

ルートテーブルのルートを特定のサブネットに適用するには、ルートテーブルをサブネットに関連付ける必要があります。ルートテーブルは複数のサブネットに関連付けることができますが、サブネットには 1 つのルートテーブルしか関連付けることができません。どのテーブルにも明示的に関連付けられていないサブネットは、デフォルトでメインルートテーブルに暗示的に関連付けられています。

テーブルをサブネットに関連付けるには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Route Tables] をクリックし、ルートテーブルを選択します。
3. 詳細ペインの [Associations] タブで、テーブルに関連付けるサブネットを選択し、[Associate] をクリックします。
4. [Associate Route Table] ダイアログボックスで、[Yes, Associate] をクリックします。

サブネットのルートテーブルを変更する

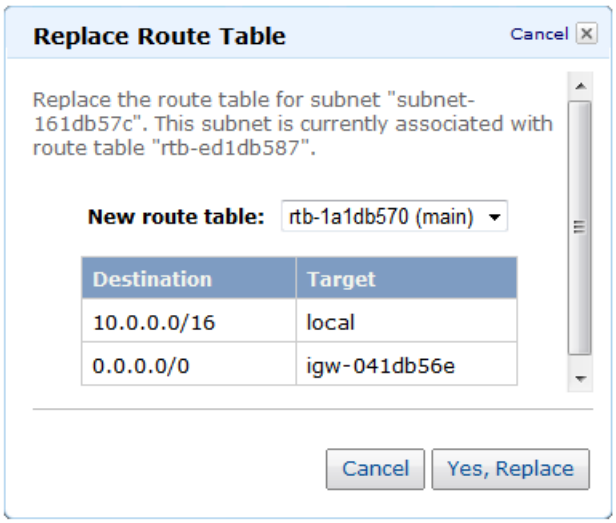
サブネットに関連付けるルートテーブルは変更できます。例えば、サブネットを作成すると、そのサブネットはメインルートテーブルに暗示的に関連付けられます。このサブネットを、メインルートテーブルではなく、作成したカスタムルートテーブルに関連付けることができます。

サブネットとルートテーブルの関連付けを変更するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Subnets] をクリックし、サブネットを選択します。

3. 詳細ペインで、サブネットに関連付けられたルートテーブルの ID の横にある [Replace] をクリックします。

4. [Replace Route Table] ダイアログボックスの [New Route Table] で、サブネットを関連付けるルートテーブルを選択し、[Yes, Replace] をクリックします。



サブネットとルートテーブルの関連付けを解除する

サブネットとルートテーブルの関連付けを解除したい場合。例えば、カスタムルートテーブルに関連付けられたサブネットを、メインルートテーブルに関連付けるとします。サブネットとカスタムルートテーブルの関連付けを解除すると、そのサブネットは、暗示的にメインルートテーブルに関連付けられます。

サブネットとルートテーブルの関連付けを解除するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Route Tables] をクリックし、ルートテーブルを選択します。
3. 詳細ペインの [Associations] で、サブネットが現在ルートテーブルに関連付けられていることを確認します。
4. [Disassociate] をクリックします。
5. [Disassociate Route Table] ダイアログボックスで、[Yes, Disassociate] をクリックします。

メインルートテーブルを置き換える

次の手順では、VPC でメインルートテーブルとして使用するルートテーブルを変更する方法について説明します。

メインルートテーブルを置き換えるには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Route Tables] をクリックします。
3. 新しいメインルートテーブルにするルートテーブルを特定し、そのテーブルを右クリックして、[Set as Main Table] を選択します。
4. [Set Main Route Table] ダイアログボックスで、[Yes, Set] をクリックします。

次の手順では、サブネットとメインルートテーブルの間の明示的な関連付けを解除する方法について説明します。これにより、サブネットとメインルートテーブルが暗示的に関連付けられます。そのプロセスは、サブネットと任意のルートテーブルの関連付け解除と同じです。

メインルートテーブルとの明示的な関連付けを解除するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Route Tables] をクリックします。
3. メインルートテーブルを選択し、その [Associations] タブをクリックします。
4. [Disassociate] をクリックします。
5. [Disassociate Route Table] ダイアログボックスで、[Yes, Disassociate] をクリックします。

ルートテーブルを削除する

ルートテーブルは、サブネットが関連付けられていない場合にのみ削除できます。メインルートテーブルを削除することはできません。

ルートテーブルを削除するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Route Tables] をクリックします。
3. ルートテーブルを選択し、[Delete] ボタンをクリックします。
4. [Delete Route Table] ダイアログボックスで、[Yes, Delete] をクリックします。

API とコマンドの概要

次の表は、使用可能なルートテーブルコマンドと対応する API アクションをまとめたものです。

説明	コマンド	API アクション
VPC に対してカスタムルートテーブルを作成します。	ec2-create-route-table	CreateRouteTable
1 つ以上のルートテーブルについて説明します。	ec2-describe-route-tables	DescribeRouteTables
ルートテーブルを VPC から削除します。	ec2-delete-route-table	DeleteRouteTable
新しいルートをルートテーブルに追加します。	ec2-create-route	CreateRoute

説明	コマンド	API アクション
ルートをルートテーブルから削除します。	ec2-delete-route	DeleteRoute
ルートテーブルの既存のルートを置き換えます。	ec2-replace-route	ReplaceRoute
サブネットをルートテーブルに関連付けます。	ec2-associate-route-table	AssociateRouteTable
サブネットとルートテーブルの関連付けを解除します。	ec2-disassociate-route-table	DisassociateRouteTable
サブネットに関連付けられているルートテーブルを変更します。また、メインルートテーブルにするルートテーブルを変更します。	ec2-replace-route-table-association	ReplaceRouteTableAssociation
仮想プライベートゲートウェイ (VGW) による VPC のルーティングテーブルへのルートの伝達を有効にします。	ec2-enable-vgw-route-propagation	EnableVgwRoutePropagation
VGW による VPC のルーティングテーブルへのルートの伝達を無効にします。ルート伝達を無効にしたら、ルートテーブルへの VPN 接続に関連付けられたルートを手動で入力する必要があります。	ec2-disable-vgw-route-propagation	DisableVgwRoutePropagation
VPN 接続に関連付けられた静的ルートを作成します。	ec2-create-vpn-connection-route	CreateVPNConnectionRoute
VPN 接続に関連付けられた静的ルートを削除します。	ec2-delete-vpn-connection-route	DeleteVPNConnectionRoute

インターネットゲートウェイを VPC に追加する

デフォルトの VPC にはインターネットゲートウェイがあり、デフォルトのサブネットで起動されたインスタンスは、起動中に指定しない限り、デフォルトでパブリック IP アドレスを受け取ります。そのため、デフォルトのサブネットで起動したインスタンスは、インターネットと自動的に通信できるようになります。詳細については、「デフォルトの VPC とサブネット (p. 61)」を参照してください。

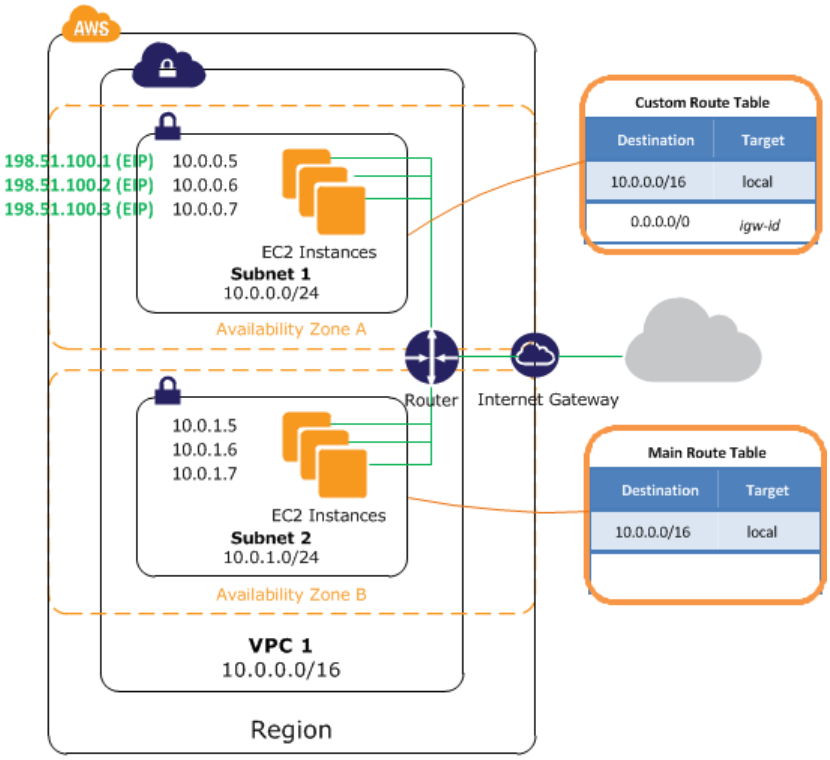
デフォルトではないサブネットで起動するインスタンスは、起動中に特に割り当てない限り、デフォルトではパブリック IP アドレスを受け取りません。したがって、インターネットと通信することはできません。起動時のパブリック IP アドレスの割り当ての詳細については、「起動中のパブリック IP アドレスの割り当て (p. 102)」を参照してください。また、デフォルトではないサブネットで起動するインスタンスのインターネットアクセスを有効にするには、インターネットゲートウェイを VPC にアタッチし、カスタムルートテーブルを作成して、セキュリティグループルールを更新し、Elastic IP アドレスを各インスタンスと関連付けます。

新しいサブネットを VPC に追加するとき、サブネットに必要なルーティングとセキュリティを設定する必要があります。セットアップはこのページの説明にしたがって手動で行うことができますが、VPC ウィザードを使用すると簡単に設定できます。例えば、VPC ウィザードでは、選択したオプションに応じて、インスタンスがインターネットと通信できるように、インターネットゲートウェイが VPC に追加され、ルートテーブルが更新されます。VPC ウィザードを使用して、インターネットゲートウェイを使うサブネットを作成する方法について詳しくは、「シナリオ 1: 1 つのパブリックサブネットのみを持つ VPC (p. 9)」または「シナリオ 2: パブリックサブネットとプライベートサブネットを持つ VPC (p. 16)」を参照してください。

以降のセクションでは、インターネットアクセスをサポートするサブネットを手動でセットアップする方法について説明します。

Topics

サブネットのセットアップを完了すると、VPC は次の図のように設定されます。



サブネットを作成する

サブネットを VPC に追加するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Subnets] をクリックし、続いて [Create Subnet] をクリックします。
3. [Create Subnet] ダイアログボックスで [VPC] を選択し、[アベイラビリティーゾーン] を選択し、サブネットの CIDR 範囲を指定してから、[Yes, Create] をクリックします。

サブネットの詳細については、「VPC とサブネット (p. 52)」を参照してください。

インターネットゲートウェイをアタッチする

インターネットゲートウェイを作成して VPC にアタッチするには

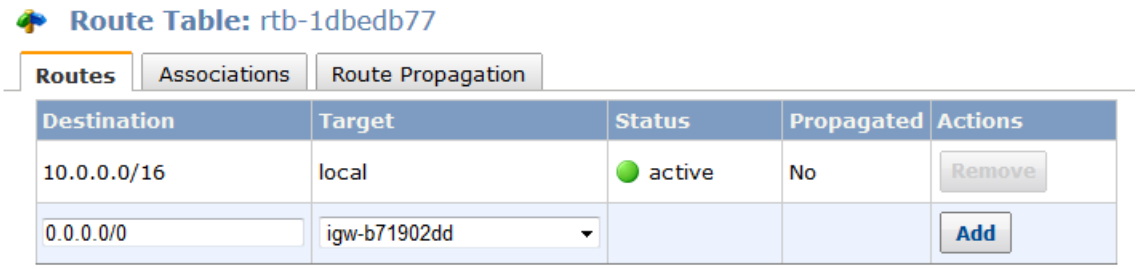
1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Internet Gateways] をクリックしてから、[Create Internet Gateway] をクリックします。
3. [Create Internet Gateway] ダイアログボックスで [Yes, Create] をクリックします。
4. 作成したインターネットゲートウェイを選択して、[Attach to VPC] をクリックします。
5. [Attach to VPC] ダイアログボックスのリストから VPC を選択してから、[Yes, Attach] をクリックします。

カスタムルートテーブルを作成する

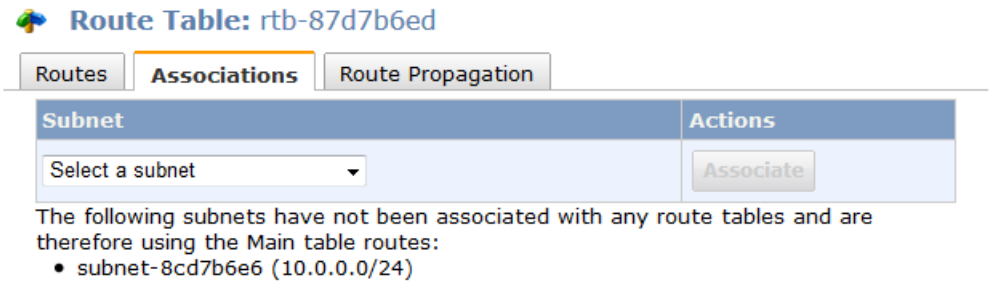
サブネットを作成すると、VPC のメインルートテーブルと自動的に関連付けられます。デフォルトでは、メインルートテーブルにインターネットゲートウェイへのルートは含まれません。次の手順では、VPC の外部あてのトラフィックをインターネットゲートウェイに送信するルートを含むカスタムルートテーブルを作成してから、それをサブネットに関連付けます。

カスタムルートテーブルを作成するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Route Tables] をクリックして、[Create Route Table] をクリックします。
3. [Create Route Table] ダイアログボックスで VPC を選択してから、[Yes, Create] をクリックします。
4. 作成したカスタムルートテーブルを選択します。詳細ペインには、ルート、関連付け、ルートのプロパゲーションを操作するタブが表示されます。
5. [Routes] タブの [Destination] ボックスに `0.0.0.0/0` を指定し、[Target] リストでインターネットゲートウェイ ID を選択してから、[Add] をクリックします。



6. [Associations] タブでサブネットの ID を選択してから、[Associate] をクリックします。



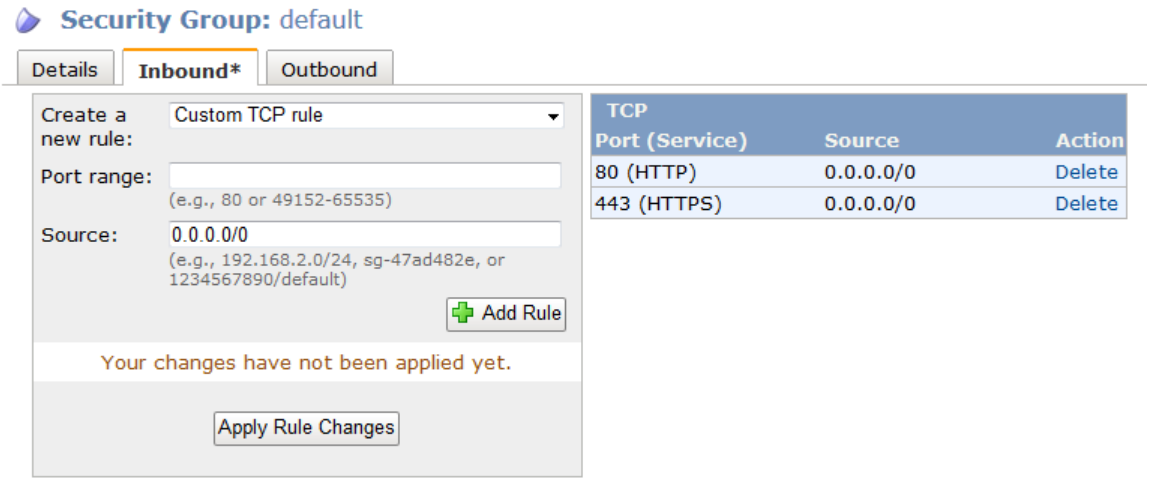
ルートテーブルの詳細については、「ルートテーブル (p. 106)」を参照してください。

セキュリティグループルールを更新する

VPC にはデフォルトのセキュリティグループが用意されています。VPC で起動する各インスタンスは、自動的にそのデフォルトのセキュリティグループに関連付けられます。デフォルトのセキュリティグループのデフォルトの設定では、インターネットからのインバウンドトラフィックを許可せず、インターネットに対するすべてのアウトバンドトラフィックを許可します。そのため、インスタンスがインターネットと通信できるようにするには、パブリックインスタンスがインターネットにアクセスすることを許可する新しいセキュリティグループを作成する必要があります。

新しいセキュリティグループを作成し、インスタンスに関連付けるには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Security Groups] をクリックして、[Create Security Group] をクリックします。
3. [Create Security Group] ダイアログボックスに、セキュリティグループの名前と説明を入力します。[VPC] リストで VPC の ID を選択し、[Yes, Create] をクリックします。
4. セキュリティグループを選択します。詳細ペインには、セキュリティグループの詳細と、インバウンドルールとアウトバンドルールを操作するタブが表示されます。
5. [Inbound] タブで、[Create a new rule] リストからルールのタイプを選択し、必要な情報を入力してから、[Add Rule] をクリックします。例えば、[HTTP] または [HTTPS] を選択し、[Source] を `0.0.0.0/0` のままにします。[Apply Rule Changes] ボタンが有効で、ボタンの上には "Your changes have not been applied yet" というテキストが表示されています。必要なインバウンドトラフィックのすべてのルールを追加したら、[Apply Rule Changes] をクリックしてルールを追加します。



6. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
7. ナビゲーションペインで [Instances] をクリックします。
8. インスタンスを右クリックし、[Change Security Groups] を選択します。
9. [Change Security Groups] ダイアログボックスで、[Security Groups] のリストから新しいセキュリティグループを選択してから、[Yes, Change] をクリックします。

セキュリティグループの詳細については、「VPC のセキュリティグループ (p. 70)」を参照してください。

Elastic IP アドレスを追加する

インターネットからインスタンスに到達できるようにするには、サブネットでインスタンスを起動した後に、そのインスタンスに Elastic IP アドレスを割り当てる必要があります。

To allocate an Elastic IP address and assign it to an instance

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. Click Elastic IPs in the navigation pane.
3. Click the Allocate New Address button.
4. In the Allocate New Address dialog box, in the EIP used in list, select VPC, and then click Yes, Allocate.
5. Select the Elastic IP address from the list, and then click the Associate Address button.
6. In the Associate Address dialog box, select the network interface or instance. Select the address to associate the Elastic IP address with from the corresponding Private IP Address list, and then click Yes, Associate.

Elastic IP アドレスについては、「Elastic IP アドレス (p. 103)」を参照してください。

VPC からのインターネットゲートウェイのアタッチ解除

デフォルトではない VPC 内に起動するインスタンスでインターネットアクセスが不要になった場合には、VPC からインターネットゲートウェイをアタッチ解除できます。VPC に関連付けられた Elastic IP アドレスを持つインスタンスがある場合、インターネットゲートウェイをアタッチ解除することはできません。

インターネットゲートウェイをアタッチ解除するには

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. ナビゲーションペインで [Elastic IPs] をクリックします。
3. IP アドレスを選択し、[Disassociate Address] ボタンをクリックして、[Yes, Disassociate] をクリックします。
4. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
5. ナビゲーションペインで [Internet Gateways] をクリックします。
6. インターネットゲートウェイを選択し、[Detach from VPC] をクリックします。
7. [Detach from VPC] ダイアログボックスの [VPC] リストで、アタッチ解除する VPC を選択して、[Yes, Detach] をクリックします。

インターネットゲートウェイを削除する

インターネットゲートウェイ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。VPC にアタッチされているインターネットゲートウェイを削除することはできません。

インターネットゲートウェイを削除するには

1. インターネットゲートウェイを選択し、[Delete] をクリックします。
2. [Delete Internet Gateway] ダイアログボックスで、[Yes, Delete] をクリックします。

API とコマンドの概要

次の表は、使用できるインターネットゲートウェイコマンドと対応する API アクションをまとめたものです。

説明	コマンド	API アクション
指定された VPC にインターネットゲートウェイを設置します。	ec2-attach-internet-gateway	AttachInternetGateway
VPC で使用する新しいインターネットゲートウェイを作成します。	ec2-create-internet-gateway	CreateInternetGateway
AWS アカウントからインターネットゲートウェイを削除します。	ec2-delete-internet-gateway	DeleteInternetGateway
1 つまたは複数のインターネットゲートウェイについて説明します。	ec2-describe-internet-gateways	DescribeInternetGateways
指定された VPC からインターネットゲートウェイをアタッチ解除します。	ec2-detach-internet-gateway	DetachInternetGateway

NAT インスタンス

Virtual Private Cloud (VPC) のプライベートサブネット内に起動するインスタンスは、インターネットとは通信できません。オプションとして、VPC のパブリックサブネットでネットワークアドレス変換 (NAT) インスタンスを使用し、プライベートサブネットのインスタンスを有効にすれば、インターネットへのアウトバウンドトラフィックを開始することができます。ただし、インターネット上で他の人が開始したインバウンドトラフィックは受信できません。

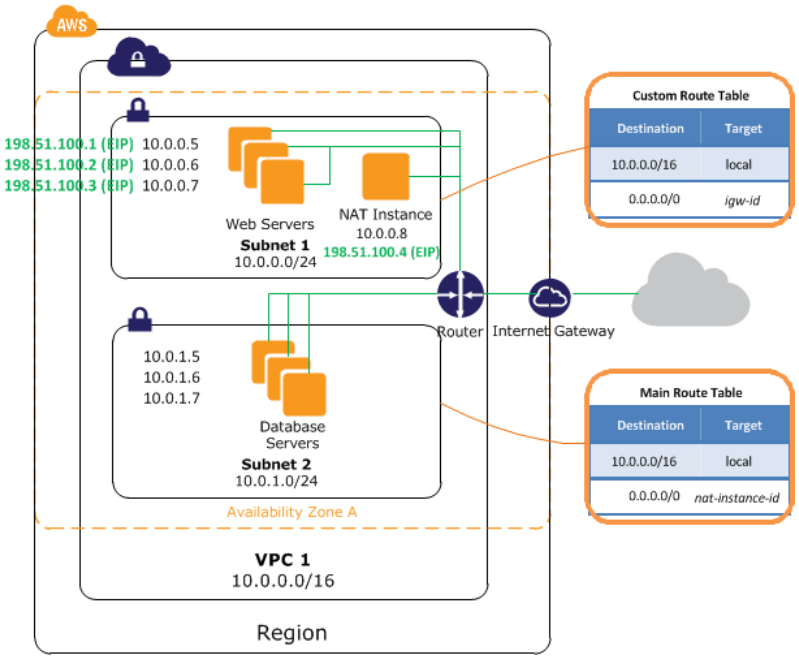
Note

*NAT インスタンス*という用語を使っていますが、実際のところ、NAT インスタンスは主にポートアドレス変換 (PAT) の役割を果たします。ここでは、よく知られている NAT という用語を選びました。NAT および PAT の詳細については、ネットワークアドレス変換に関する Wikipedia の記事を参照してください。

Topics

NAT インスタンスの基本

次の図は、NAT インスタンスの基本を示しています。メインルートテーブルは、プライベートサブネット内のインスタンスからパブリックサブネット内の NAT インスタンスにトラフィックを送信します。NAT インスタンスは、そのトラフィックを VPC のインターネットゲートウェイに送信します。トラフィックは NAT インスタンスの Elastic IP アドレスによってもたらされます。NAT インスタンスは応答用に大きなポート番号を指定します。応答が戻ってきた場合、NAT インスタンスはそれをプライベートサブネット内のインスタンスに、応答用のポート番号に基づいて送信します。



VPC とサブネットの概要については、「Amazon VPC とは (p. 1)」を参照してください。

NAT インスタンスを設定する

VPC ウィザードを使用すると、NAT インスタンスで VPC を設定できます。詳細については、「シナリオ 2: パブリックサブネットとプライベートサブネットを持つ VPC (p. 16)」を参照してください。また、次の手順で NAT インスタンスを手動で設定することもできます。

1. 2 つのサブネットを持つ VPC を作成します。
   a. VPC を作成する (「VPC を作成する (p. 54)」を参照)
   b. 2 つのサブネットを作成する (「サブネットを作成する (p. 118)」を参照)
   c. インターネットゲートウェイを 1 つのサブネットにアタッチし (「インターネットゲートウェイをアタッチする (p. 119)」を参照)、それをパブリックサブネットにする
   d. パブリックサブネットのカスタムメインルートテーブルを作成する (「カスタムルートテーブルを作成する (p. 119)」を参照)
2. NATSG セキュリティグループを作成します (「NATSG セキュリティグループを作成する (p. 125)」を参照)。このセキュリティグループは、NAT インスタンスの起動時に指定します。
3. NAT インスタンスとして実行されるように設定された AMI からパブリックサブネット内にインスタンスを起動します。Amazon では、NAT インスタンスとして実行されるように設定された Amazon Linux AMI を提供しています。これらの AMI の名前には文字列 `ami-vpc-nat` が含まれているので、AWS マネジメントコンソールで検索できます。
   a. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
   b. ナビゲーションペインで [Instances] をクリックします。
   c. [Launch Instance] ボタンをクリックします。
   d. [Create a New Instance] ページで、[Quick Launch Wizard] をクリックします。以下の手順にしたがってウィザードの設定を完了します。
      i. NAT インスタンスの名前を指定します。
      ii. キーペアを選択または作成します。
      iii. [Choose a Launch Configuration] で [More Amazon Machine Images] を選択し、[Continue] をクリックします。
      iv. [Public AMIs] タブで、`ami-vpc-nat` を検索します。結果リストから NAT AMI を選択し、[Continue] をクリックします。
      v. [Edit Details] をクリックします。
      vi. [Instance Details] で [Launch into a VPC] を選択し、パブリックサブネットを指定します。
      vii. [Security Settings] で、作成した NATSG セキュリティグループを選択し、[Save Details] をクリックします。
      viii. 選択した設定を確認します。必要に応じて設定を変更し、[Launch] をクリックします。
4. (オプション) NAT インスタンスにログオンし、必要に応じて修正を加え、NAT インスタンスとして実行されるように設定された独自の AMI を作成します。この AMI は、次回 NAT インスタンスを起動する必要があるときに使用できます。独自の AMI の作成の詳細については、「*Amazon Elastic Compute Cloud User Guide*」の「Amazon EBS-Backed AMI の作成」を参照してください。

Note

Amazon Linux AMI のログインは `ec2-user` です。`root` ではありません。

5. NAT インスタンスの SrcDestCheck 属性を無効にします (「送信元/送信先チェックを無効にする (p. 126)」を参照) 。
6. Elastic IP アドレスと NAT インスタンスを関連付けます。
   a. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
   b. ナビゲーションペインで [Elastic IPs] をクリックします。
   c. [Allocate New Address] ボタンをクリックします。
   d. [Allocate New Address] ダイアログボックスの [EIP used in] リストで VPC を選択し、[Yes, Allocate] をクリックします。
   e. リストで Elastic IP アドレスを選択し、[Associate Address] ボタンをクリックします。
   f. [Associate Address] ダイアログボックスで、NAT インスタンスのネットワークインターフェイスを選択します。[Private IP Address] リストから、EIP を関連付けるアドレスを選択し、[Yes, Associate] をクリックします。
7. メインルートテーブルを更新して、NAT インスタンスにトラフィックを送信します。詳細については、「メインルートテーブルを更新する (p. 127)」を参照してください。

NATSG セキュリティグループを作成する

次の表に示すように NATSG セキュリティグループを定義し、NAT インスタンスを有効にして、インターネットに接続されたトラフィックを、プライベートサブネットのインスタンスから受け取ります。また、SSH トラフィックをネットワークから受け取ります。また、NAT インスタンスは、ネットワークにトラフィックを送信することもできます。これにより、プライベートサブネットのインスタンスがソフトウェア更新を取得できます。

NATSG: 推奨ルール

インバウンド			
送信元	プロトコル	ポート範囲	コメント
10.0.1.0/24	TCP	80	プライベートサブネットのサーバーからのインバウンド HTTP トラフィックを許可する
10.0.1.0/24	TCP	443	プライベートサブネットのサーバーからのインバウンド HTTPS トラフィックを許可する
ネットワークのパブリック IP アドレスの範囲	TCP	22	ネットワークから NAT インスタンスへのインバウンド SSH アクセス (インターネットゲートウェイ経由) を許可する
アウトバウンド			
送信先	プロトコル	ポート範囲	コメント
0.0.0.0/0	TCP	80	インターネットへのアウトバウンド HTTP アクセスを許可する
0.0.0.0/0	TCP	443	インターネットへのアウトバウンド HTTPS アクセスを許可する

NATSG セキュリティグループを作成するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Security Groups] をクリックします。
3. [Create Security Group] ボタンをクリックします。
4. [Create Security Group] ダイアログボックスで、セキュリティグループ名として NATSG を指定し、説明を入力します。[VPC] リストで VPC の ID を選択し、[Yes, Create] をクリックします。
5. 先ほど作成した NATSG セキュリティグループを選択します。詳細ペインに、セキュリティグループの詳細と、インバウンドルールおよびアウトバウンドルールを操作するためのタブが表示されます。
6. 次に示すように、[Inbound] タブを使用して、インバウンドトラフィックのルールを追加します。
   a. [Create a new rule] リストで HTTP を選択します。[Source] ボックスで、プライベートサブネットの IP アドレス範囲を指定し、[Add Rule] をクリックします。
   b. [Create a new rule] リストで HTTPS を選択します。[Source] ボックスで、プライベートサブネットの IP アドレス範囲を指定し、[Add Rule] をクリックします。
   c. [Create a new rule] リストで SSH を選択します。[Source] ボックスで、ネットワークのパブリック IP アドレス範囲を指定し、[Add Rule] をクリックします。
   d. [Apply Rule Changes] をクリックします。
7. 次に示すように、[Outbound] タブを使用して、アウトバウンドトラフィックのルールを追加します。
   a. [Create a new rule] リストから HTTP を選択します。[Destination] が `0.0.0.0/0` であることを確認し、[Add Rule] をクリックします。
   b. [Create a new rule] リストで HTTPS を選択します。[Destination] が `0.0.0.0/0` であることを確認し、[Add Rule] をクリックします。
   c. [Apply Rule Changes] をクリックします。

セキュリティグループの詳細については、「VPC のセキュリティグループ (p. 70)」を参照してください。

送信元/送信先チェックを無効にする

EC2 インスタンスは、送信元/送信先チェックをデフォルトで実行します。つまり、そのインスタンスは、そのインスタンスが送受信する任意のトラフィックの送信元または送信先である必要があります。しかし、NAT インスタンスは、送信元または送信先がそのインスタンスでないときにも、トラフィックを送受信できなければなりません。したがって、NAT インスタンスでは送信元/送信先チェックを無効にする必要があります。

実行または停止する NAT インスタンスの `SrcDestCheck` 属性を無効にするには、次の手順を行います。

To disable source/destination checking on a NAT instance

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. Click Instances in the navigation pane.
3. Right-click the NAT instance, and then select Change Source / Dest Check.
4. For a NAT instance, this attribute should be disabled. Click Yes, Disable.

メインルートテーブルを更新する

メインルートテーブルを以下の手順にしたがって更新します。デフォルトでは、メインルートテーブルによって、VPC 内のインスタンスはお互いに通信することができます。その他のすべてのサブネットトラフィックを NAT インスタンスに送信するルートが追加されます。

メインルートテーブルを更新するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. VPC 用のメインルートテーブルを選択します。詳細ペインには、ルート、関連付け、ルートの伝播を操作するタブが表示されます。
3. [Routes] タブで、[Destination] ボックスに `0.0.0.0/0` を指定し、[Target] ボックスに NAT インスタンスのインスタンス ID を指定して、[Add] をクリックします。
4. [Associations] タブでサブネットの ID を選択して、[Associate] をクリックします。

ルートテーブルの詳細については、「ルートテーブル (p. 106)」を参照してください。

API とコマンドの概要

次の表は、NAT インスタンスに関連する使用可能な EC2 コマンドと API アクションをまとめたものです。

説明	コマンド	API アクション
EC2 インスタンスの `SrcDestCheck` 属性を有効または無効にします。これにより、ネットワークアドレス変換 (NAT) を実行できるかどうかが決まります。	ec2-modify-instance-attribute	ModifyInstanceAttribute

DHCP オプションセット

このトピックでは、DHCP オプションセットと、VPC の DHCP オプションを指定する方法について説明します。

Topics

DHCP オプションセットの概要

DHCP (Dynamic Host Configuration Protocol) は、TCP/IP ネットワークのホストに設定情報を渡すための規格です。DHCP メッセージの *`options`* フィールドの内容は設定パラメータです。パラメータには、ドメイン名、ドメインネームサーバー、netbios-node-type などがあります。

DHCP オプションセットは AWS アカウントに関連付けられ、すべての Virtual Private Cloud (VPC) で使用できます。

デフォルトではない VPC 内に起動する Amazon EC2 インスタンスは、デフォルトでプライベートになり、起動中に特別に割り当てない限り、パブリック IP アドレスは割り当てられません。デフォルトでは、デフォルトではない VPC 内のすべてのインスタンスが、AWS によって割り当てられた解決できないホスト名を受け取ります (ip-10-0-0-202 など) 。インスタンスに独自のドメイン名を割り当て、独自の DNS サーバーのうち 4 台までを使用できます。そのためには、特別な DHCP オプションセットを指定する必要があります。このセットの内容は、よく使われる他の DHCP オプションです (サポートされているオプションの詳細については、次の表を参照してください) 。オプションの詳細については、RFC 2132 を参照してください。

DHCP Option Name	Description
domain-name-servers	The IP addresses of up to four domain name servers, or AmazonProvidedDNS. The default DHCP option set specifies AmazonProvidedDNS.
domain-name	If you're using AmazonProvidedDNS in US East (Northern Virginia) Region, specify compute-1.amazonaws.com. If you're using AmazonProvidedDNS in another region, specify *region*.compute.amazonaws.com. Otherwise, specify a domain name (for example, `MyCompany.com`).
ntp-servers	The IP addresses of up to four Network Time Protocol (NTP) servers.
netbios-name-servers	The IP addresses of up to four NetBIOS name servers.
netbios-node-type	The NetBIOS node type (1, 2, 4, or 8). We recommend that you specify 2 (broadcast and multicast are not currently supported). For more information about these node types, see RFC 2132.

Amazon DNS サーバー

VPC を作成する際、DHCP オプションのセットを自動的に作成し、VPC に関連付けます。このセットに含まれるのは、`domain-name-servers=AmazonProvidedDNS` という 1 つのオプションだけです。これは Amazon DNS サーバーです。このオプションは、VPC のインターネットゲートウェイを介して通信する必要があるインスタンスに対して DNS を有効にします。文字列 `AmazonProvidedDNS` は、リザーブド IP アドレスで実行中の DNS サーバーにマップされ、VPC ネットワークの範囲に "2" をプラスした値です。例えば、10.0.0.0/16 ネットワークの DNS サーバーの位置は 10.0.0.2 となります。

Note

Amazon DNS サーバーの IP アドレス 169.254.169.253 を使用することも可能ですが、このアドレスを使用できないサーバーもあります。例えば、Windows Server 2008 では、ネットワーク範囲 169.254.x.x にある DNS サーバーは使用できません。

DHCP オプションを変更する

DHCP オプションセットを作成後に変更することはできません。VPC で異なる DHCP オプションセットを使用するには、新しいセットを作成して VPC に関連付ける必要があります。DHCP オプションを使用しないように VPC を設定することもできます。

複数セットの DHCP オプションを使用できますが、一度に VPC に関連付けることができる DHCP オプションセットは 1 つだけです。VPC を削除すると、その VPC に関連付けられている DHCP オプションセットも削除されます。

新しい DHCP オプションセットを VPC に関連付けた後に VPC 内で起動する既存のインスタンスとすべての新しいインスタンスに、それらのオプションが使用されます。 You don't need to restart or relaunch

the instances. They automatically pick up the changes within a few hours, depending on how frequently the instance renews its DHCP lease. If you want, you can explicitly renew the lease using the operating system on the instance.

DHCP オプションセットを使用する

このセクションでは、DHCP オプションセットの使用方法を示します。

Topics

DHCP オプションセットを作成する

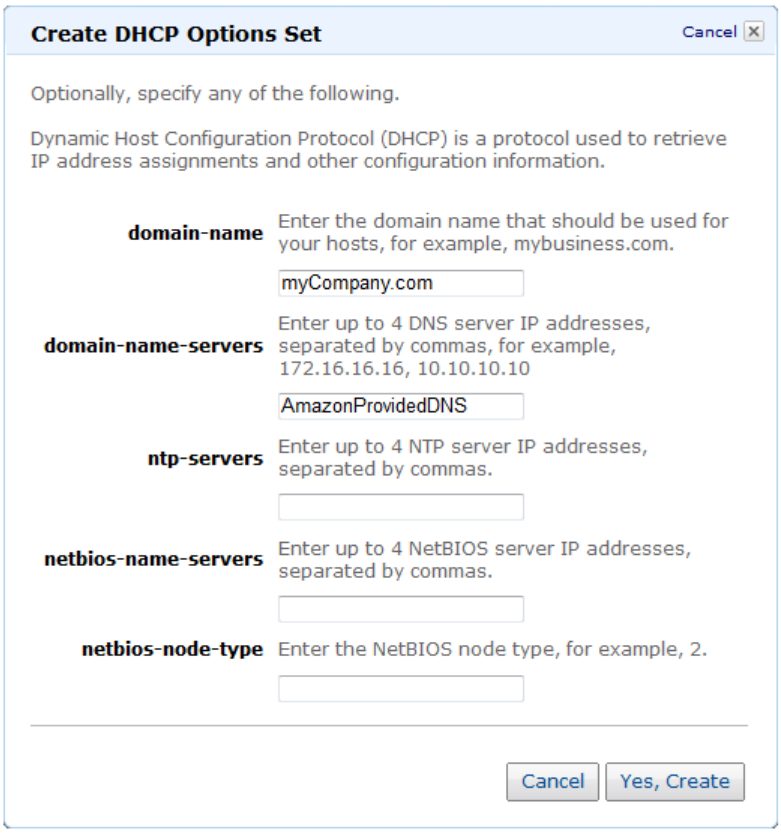
必要な数だけ追加の DHCP オプションセットを作成できます。ただし、一度に VPC に関連付けることができる DHCP オプションセットは 1 つだけです。DHCP オプションセットを作成した後、そのセットを使用するように VPC を設定する必要があります。詳細については、「VPC で使用する DHCP オプションセットを変更する (p. 131)」を参照してください。

DHCP オプションセットを作成するには

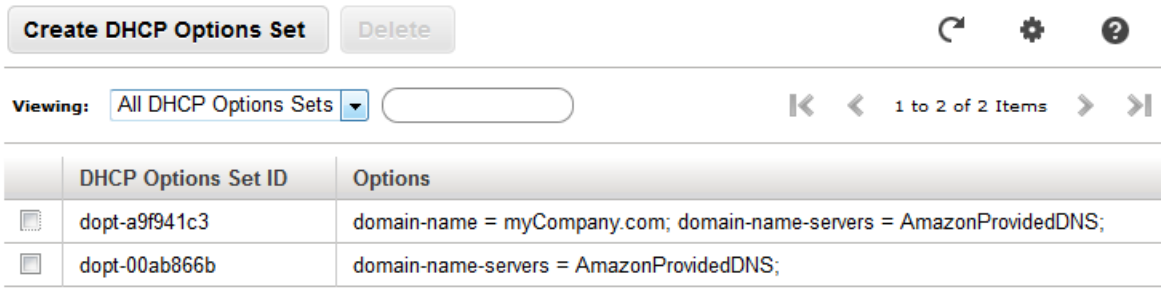
1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [DHCP Options Sets] をクリックし、[Create DHCP Options Set] ボタンをクリックします。
3. [Create DHCP Options Set] ダイアログボックスで、使用するオプションの値を入力し、[Yes, Create] をクリックします。

Important

VPC にインターネットゲートウェイがある場合は、独自の DNS サーバーまたは Amazon の DNS サーバー (AmazonProvidedDNS) を domain-name-servers 値として指定してください。そうしないと、インターネットと通信する必要があるインスタンスが DNS にアクセスできません。



新しい DHCP オプションのセットが DHCP オプションの一覧に表示されます。次の画像は一覧の例を示しています。さきほど作成した DHCP オプションのセットと、VPC に自動的に付属しているセット (domain-name-servers=AmazonProvidedDNS が唯一のオプション) の両方が表示されています。



4. 新しい DHCP オプションセットの ID を書き留めておいてください (dopt-*xxxxxxxx*) 。新しいオプションセットを VPC に関連付けるときに必要です。

DHCP オプションセットを作成しても、オプションを有効に機能させるには、オプションを VPC に関連付ける必要があります。複数の DHCP オプションセットを作成できますが、一度に VPC に関連付けることができる DHCP オプションセットは 1 つだけです。

VPC で使用する DHCP オプションセットを変更する

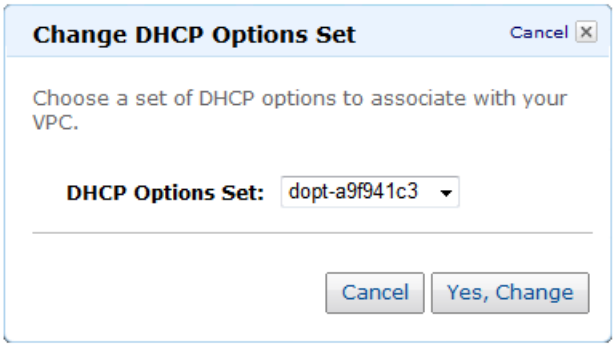
VPC でどの DHCP オプションセットを使用するかを変更できます。VPC で DHCP オプションを使用しない場合は、DHCP オプションを使用しないように VPC を変更する (p. 131) を参照してください。

Note

次の手順では、変更したい DHCP オプションセットはすでに作成済みであることを想定しています。まだ作成していない場合は、この時点でオプションセットを作成してください。詳細については、「DHCP オプションセットを作成する (p. 129)」を参照してください。

VPC に関連付けられた DHCP オプションセットを変更するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Your VPCs] をクリックします。
3. VPC を選択し、[Change DHCP Options Set] ボタンをクリックします。
4. [Change DHCP Options Set] ダイアログボックスで、ドロップダウンリストからオプションセットを選択し、[Yes, Change] をクリックします。

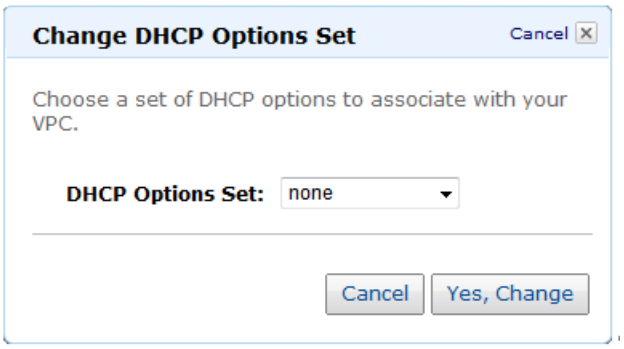


新しい DHCP オプションセットを VPC に関連付けた後、VPC 内で起動する既存のインスタンスおよび新しいインスタンスのすべてで、それらのオプションが使用されます。インスタンスを再起動する必要はありません。インスタンスで DHCP リースが更新される頻度に応じて、数時間以内に自動的に変更が反映されます。インスタンスのオペレーティングシステムを使用してリースを明示的に更新することもできます。

DHCP オプションを使用しないように VPC を変更する

DHCP オプションを使用しないように VPC を設定できます。

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Your VPCs] をクリックします。
3. VPC を選択し、[Change DHCP Options Set] ボタンをクリックします。
4. [Change DHCP Options Set] ダイアログボックスで、ドロップダウンリストから [none] を選択し、[Yes, Change] をクリックします。



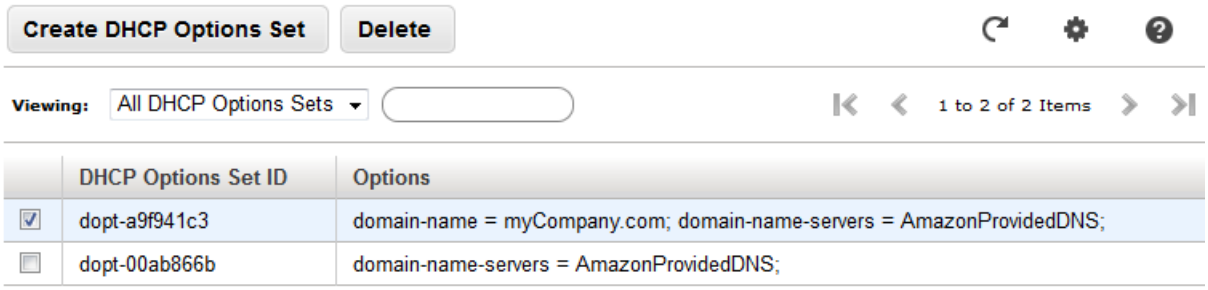
You don't need to restart or relaunch the instances. They automatically pick up the changes within a few hours, depending on how frequently the instance renews its DHCP lease. If you want, you can explicitly renew the lease using the operating system on the instance.

DHCP オプションセットを削除する

DHCP オプションセットが不要になった場合は、次の手順にしたがって削除します。VPC でオプションセットを使用していないことが必要です。

DHCP オプションセットを削除するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [DHCP Options Set] をクリックします。
3. 削除する DHCP オプションセットを選択し、[Delete] をクリックします。



4. [Delete DHCP Options Set] ダイアログボックスで、[Yes, Delete] をクリックします。

API とコマンドの概要

次の表は、使用できる DHCP オプションセット用コマンドおよび対応する API アクションをまとめて示します。

説明	コマンド	API アクション
VPC 用の DHCP オプションセットを作成します。	ec2-create-dhcp-options	CreateDhcpOptions

説明	コマンド	API アクション
DHCP オプションセットを指定した VPC に関連付けるか、DHCP オプションを使用するように VPC を変更します。	ec2-associate-dhcp-options	AssociateDhcpOptions
1 つ以上の DHCP オプションセットを定義します。	ec2-describe-dhcp-options	DescribeDhcpOptions
DHCP オプションセットを削除します。	ec2-delete-dhcp-options	DeleteDhcpOptions

VPC での DNS の使用

Amazon EC2 インスタンスの通信には IP アドレスが必要です。パブリック IP アドレスによってインターネットでの通信が可能になり、プライベート IP アドレスによってインスタンス (EC2-Classic または VPC) のネットワーク内部での通信が可能になります。

インターネットで使用される名前を対応する IP アドレスに解決するには、ドメインネームシステム (DNS) が標準的です。DNS ホスト名はコンピュータを一意に識別する絶対名で、ホスト名とドメイン名で構成されます。DNS サーバーは DNS ホスト名を対応する IP アドレスに解決します。

Amazon では Amazon DNS サーバーを提供しています。独自の DNS サーバーを使用するには、VPC の DHCP オプションセットを更新します。詳細については、「DHCP オプションセット (p. 127)」を参照してください。

EC2 インスタンスをパブリックにアクセス可能にするには、パブリック IP アドレス、DNS ホスト名、DNS 解決が必要です。

EC2 インスタンスの DNS ホスト名を確認する

EC2-Classic プラットフォームまたはデフォルトの VPC 内にインスタンスを起動すると、パブリック DNS ホスト名およびプライベート DNS ホスト名がインスタンスに割り当てられます。デフォルト以外の VPC 内にインスタンスを起動した場合、AWS アカウントでサポートされているプラットフォームによって、パブリック DNS ホスト名およびプライベート DNS ホスト名が割り当てられる場合と、割り当てられない場合があります。

Amazon EC2 コンソールまたは Amazon EC2 コマンドラインインターフェイスを使用して、実行中のインスタンスまたはネットワークインターフェイスの DNS ホスト名を確認できます。

AWS マネジメントコンソール

コンソールを使用してインスタンスの DNS ホスト名を確認するには

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. [Navigation] ペインの [Instances] をクリックします。
3. リストからインスタンスを選択します。
4. 詳細ペインの [Description] タブで、[Public DNS] および [Private DNS] フィールドの値を確認します。

コンソールを使用してネットワークインターフェイスの DNS ホスト名を確認するには

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. ナビゲーションペインの [Network Interfaces] をクリックします。
3. リストからネットワークインターフェイスを選択します。
4. ネットワークインターフェイスの [Details] タブで、[Public DNS] および [Private DNS] フィールドの値を確認します。

コマンドラインインターフェイス

コマンドラインインターフェイスを使用してインスタンスの DNS ホスト名を確認するには、ec2-describe-instances コマンドを使用します。例えば次のコマンドは、ID `i-1a2b3c4d` のインスタンスについて、DNS ホスト名などの情報を表示します。

```
ec2-describe-instances i-1a2b3c4d
```

このコマンドの出力の抜粋を次に示します。この例ではパブリック DNS ホスト名が `ec2-203-0-113-12.compute-1.amazonaws.com` で、プライベート DNS ホスト名が `ip-172-31-14-29.ec2.internal` です。これらの名前はサンプルです。ご使用のインスタンスの DNS ホスト名は、インスタンスが起動された場所と方法によって、形式が異なる場合があります。

```
RESERVATION     r-6482711d      880185128111    quicklaunch-2
INSTANCE  i-1a2b3c4d  ami-1624987f  ec2-203-0-113-12.compute-1.amazonaws.com

ip-172-31-14-29.ec2.internal  running
```

コマンドラインインターフェイスを使用してネットワークインターフェイスの DNS ホスト名を確認するには、ec2-describe-network-interfaces コマンドを使用して、指定したネットワークインターフェイスの DNS ホスト名を表示します。例えば、次のコマンドは、ID `eni-1a2b3c4d` のネットワークインターフェイスについて、DNS ホスト名などの情報を表示します。

```
ec2-describe-network-interfaces eni-1a2b3c4d
```

このコマンドの出力の抜粋を次に示します。この例ではパブリック DNS ホスト名が `ec2-203-0-113-12.compute-1.amazonaws.com` で、プライベート DNS ホスト名が `ip-172-31-14-29.ec2.internal` です。これらの名前はサンプルです。ご使用のインスタンスの DNS ホスト名は、インスタンスが起動された場所と方法によって、形式が異なる場合があります。

```
NETWORKINTERFACE    eni-1a2b3c4d    subnet-73ba071a vpc-1a2b3c4d  us-east-1b
 false   in-use
172-31-14-29 ip-172-31-14-29.ec2.internal   true
...
ASSOCIATION    203-0-113-12   amazon  172-31-14-29   ec2-203-0-113-12.compute-
1.amazonaws.com
PRIVATEIPADDRESS 172-31-14-29   ip-172-31-14-29.ec2.internal
```

VPC の DNS サポートを更新する

VPC 内にインスタンスを起動したとき、VPC で DNS ホスト名が有効になっている場合にのみ、パブリック DNS ホスト名とプライベート DNS ホスト名がインスタンスに割り当てられます。デフォルトでは、DNS ホスト名はデフォルトの VPC と、VPC コンソールを使用して作成した VPC でのみ有効に

なります。VPC 内のインスタンスに DNS ホスト名と DNS 解決がない場合、インターネットからインスタンスにアクセスすることはできません。

DNS サポートを制御する次の VPC 属性がサポートされています。パブリック IP アドレスを持つインスタンスをインターネットからアクセス可能にする場合は、必ず両方の属性を `true` に設定します。

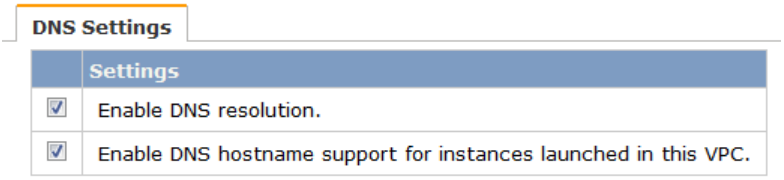
属性	説明
`enableDnsHostnames`	VPC 内に起動されるインスタンスが DNS ホスト名を取得するかどうかを示します。この属性が `true` の場合、VPC 内のインスタンスは DNS ホスト名を取得します。それ以外の場合は取得しません。この属性を `true`に設定するには、`enableDnsSupport` が `true` でなければなりません。
`enableDnsSupport`	VPC に対して DNS 解決がサポートされているかどうかを示します。この属性が `true` の場合、Amazon DNS サーバーはインスタンスの DNS ホスト名を対応する IP アドレスに解決します。それ以外の場合は解決しません。

以前は DNS ホスト名をサポートしていなかった VPC で DNS ホスト名を有効にすると、その VPC 内に既に起動されているインスタンスは DNS ホスト名を受け取ります。ただし、そのためには、インスタンスにパブリック IP アドレスまたは Elastic IP アドレスが割り当てられている必要があります。

AWS マネジメントコンソール

Amazon VPC コンソールを使用して VPC の DNS サポートを更新するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Your VPCs] をクリックします。
3. 一覧から VPC を選択します。
4. [DNS Settings] タブの情報を確認します。この例では、両方の設定が有効になっています。



5. 必要に応じて設定を更新します。

コマンドラインインターフェイス

DNS による解決と DNS ホスト名が指定した VPC でサポートされているかどうかを判断するには、ec2-describe-vpc-attribute コマンドを使用します。

```
ec2-describe-vpc-attribute -H vpc-id
```

次の出力例は、DNS による解決と DNS ホスト名が指定した VPC でサポートされていることを示しています。

```
TYPE            EnableDnsSupport   EnableDnsHostnames
VPCATTRIBUTES   true               true
```

必要に応じて設定を更新する場合は、ec2-modify-vpc-attribute コマンドを使用します。例えば、次のコマンドは DNS ホスト名のサポートを無効にします。

```
ec2-modify-vpc-attribute vpc-id --dns-hostnames false
```

VPC へのハードウェア仮想プライベートゲートウェイの追加

デフォルトでは、Virtual Private Cloud (VPC) 内に起動されるインスタンスとユーザー独自のネットワークとの通信はできません。VPC から独自のネットワークへのアクセスを可能にするには、仮想プライベートゲートウェイを VPC に関連付け、カスタムルートテーブルを作成して、セキュリティグループ規則を更新します。

このプロセスは、このページの説明にしたがって手動で実行することも、VPC 作成ウィザードを使用して多くのステップを自動的に実行することもできます。VPC 作成ウィザードを使用して仮想プライベートゲートウェイを設定する方法の詳細については、「シナリオ 3: パブリックサブネットとプライベートサブネット、およびハードウェア VPN アクセスを持つ VPC (p. 28)」または「シナリオ 4: 1 つのプライベートサブネットのみ、およびハードウェア VPN アクセスを持つ VPC (p. 42)」を参照してください。

*VPN 接続*という用語は一般的な用語ですが、VPC のドキュメントにおいては、VPN 接続は VPC とユーザー独自のネットワーク間の接続を指します。

Topics

お客様の VPC で VPN 接続を使用する場合の料金について詳しくは、「Amazon VPC 製品のページ」を参照してください。

VPN のコンポーネント

VPN 接続は次のコンポーネントで構成されます。

仮想プライベートゲートウェイ

*仮想プライベートゲートウェイ*は、VPN 接続の Amazon 側にある VPN コンセントレータです。

リージョン当たりの仮想プライベートゲートウェイの最大数や、VPC 内の他のコンポーネントに適用される制限については、「Amazon VPC 制限 (p. 159)」を参照してください。

カスタマーゲートウェイ

*カスタマーゲートウェイ*は、VPN 接続のユーザー側にある物理的なデバイスまたはソフトウェアアプリケーションです。

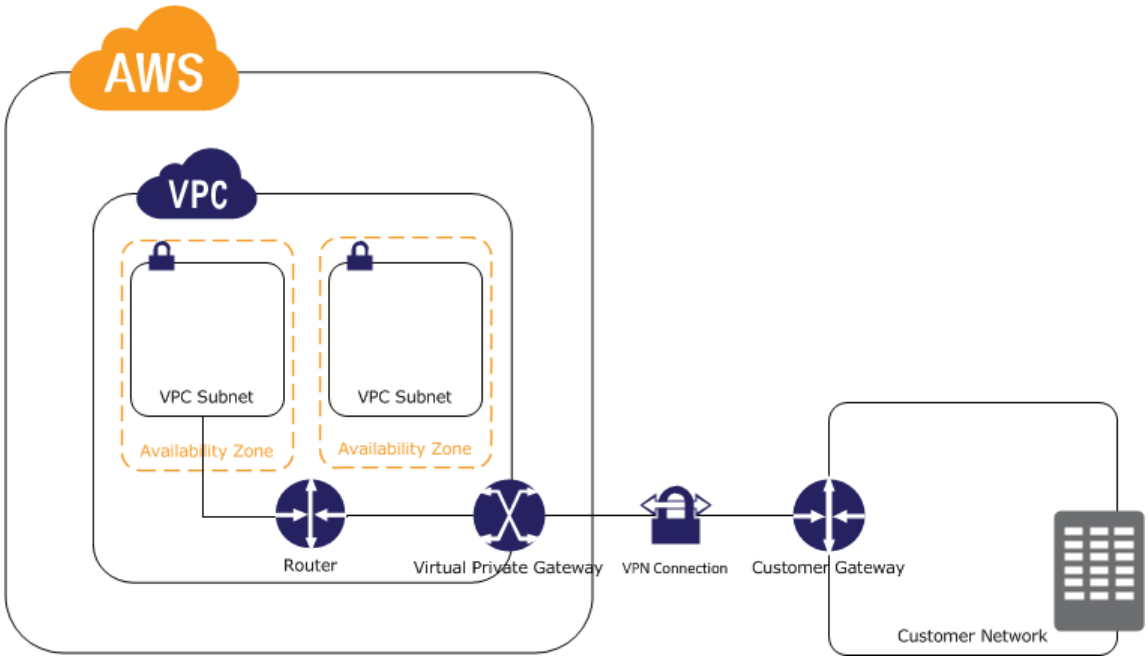
Amazon VPC でテスト済みのカスタマーゲートウェイの一覧を確認するには、「Amazon Virtual Private Cloud のよくある質問」を参照してください。

VPN の設定例

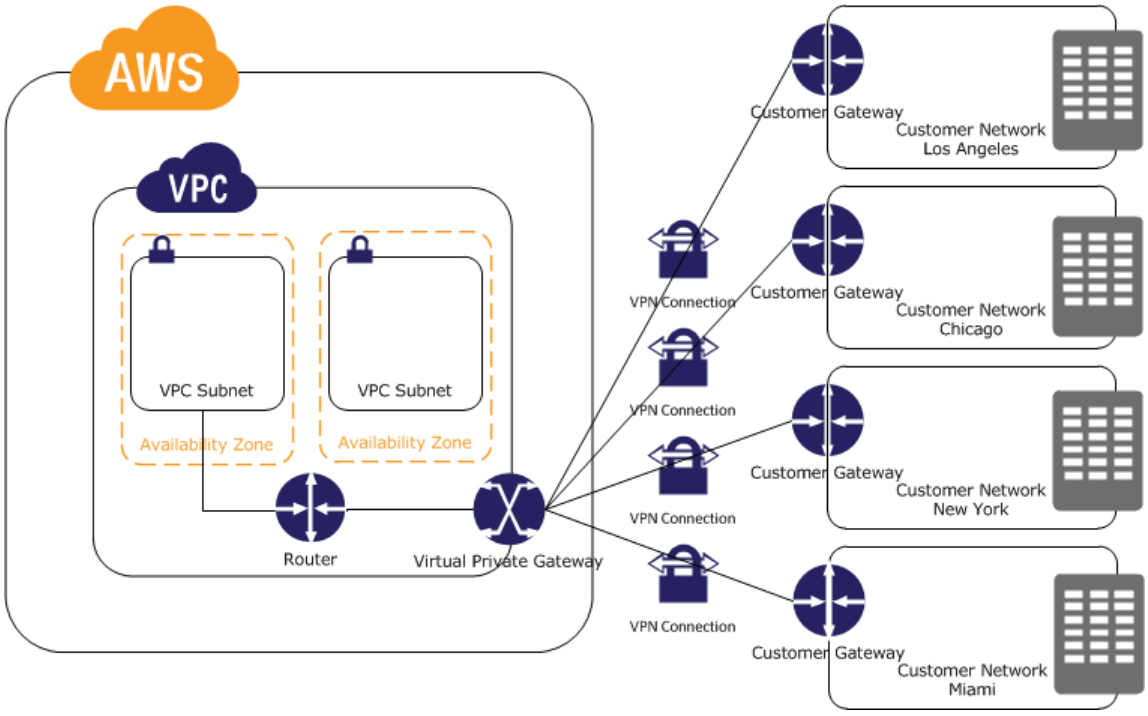
次の図に単一および複数の VPN 接続を示します。VPC には仮想プライベートゲートウェイが関連付けられていて、ネットワークにはカスタマーゲートウェイが使用されています。カスタマーゲートウェイは、VPN 接続を有効にするように設定する必要があります。ルーティングを設定して、VPC からユーザーネットワークに向けてのトラフィックが仮想プライベートゲートウェイにルーティングされるようにします。

単一の VPC に対して複数の VPN 接続を作成する場合、2 番目のカスタマーゲートウェイを設定して、外部にある同一の場所への冗長な接続を作成できます。また、複数の地理的な場所への VPN 接続を作成することもできます。

単一の VPN 接続



複数の VPN 接続



VPN のルーティングオプション

VPN 接続を作成する場合、使用するルーティングのタイプを指定する必要があります。選択するルーティングのタイプは、VPN デバイスの構成とモデルによって異なります。VPN デバイスがボーダーゲートウェイプロトコル (BGP) をサポートしている場合は、VPN 接続を設定するときに動的ルーティングを指定します。デバイスが BGP をサポートしていない場合は、静的ルーティングを指定します。Amazon VPC でテスト済みの静的ルーティングデバイスと動的ルーティングデバイスの一覧を確認するには、「Amazon Virtual Private Cloud のよくある質問」を参照してください。

BGP デバイスを使用する場合は、BGP を使用してデバイスから仮想プライベートゲートウェイにルートがアドバタイズされるので、VPN 接続への静的ルートを指定する必要はありません。BGP をサポートしていないデバイスを使用する場合は、静的ルーティングを選択し、仮想プライベートゲートウェイに通知するネットワークのルート (IP プレフィックス) を入力する必要があります。BGP アドバタイズを使用するか静的ルートエントリを使用するかにかかわらず、VPC からのトラフィックを受信できるのは、仮想プライベートゲートウェイに対して既知の IP プレフィックスのみです。

使用可能な場合は BGP に対応したデバイスを使用することをお勧めします。BGP プロトコルは安定したライブ状態検出チェックが可能であり、1 番目のトンネル停止時の 2 番目の VPN トンネルへのフェイルオーバーに役立ちます。BGP をサポートしていないデバイスでも、ヘルスチェックを実行することによって、必要時に 2 番目のトンネルへのフェイルオーバーを支援できます。

VPN 接続に必要なもの

VPN 接続で Amazon VPC を使用するには、ユーザー自身またはネットワーク管理者が物理的なアプライアンスをカスタマーゲートウェイとして指定し、設定する必要があります。VPN 事前共有キーおよび VPN 接続の設定に関連したその他のパラメータを含む必須の設定情報は、Amazon から提供されます。この設定はネットワーク管理者が行うのが一般的です。カスタマーゲートウェイの要件および設定については、「Amazon Virtual Private Cloud Network Administrator Guide」を参照してください。

次の表は、VPN 接続を確立するために必要な情報の一覧です。

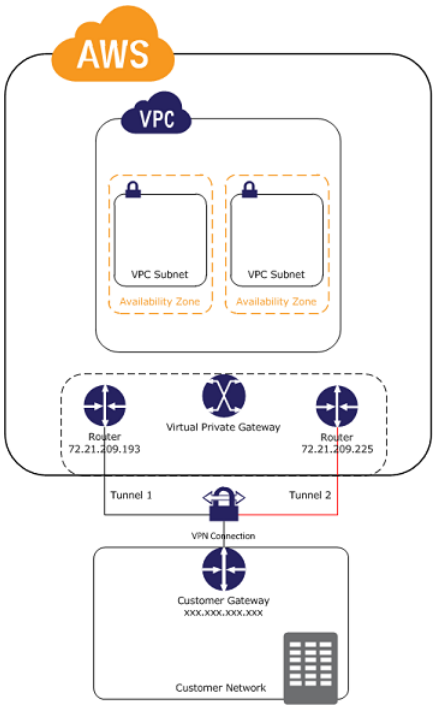
項目	用途	コメント	
カスタマーゲートウェイのタイプ (例: Cisco ASA、Juniper J-Series、Juniper SSG、Yamaha)	返される情報 (カスタマーゲートウェイの設定に使用する) の形式を指定します。		
カスタマーゲートウェイの外部インターフェイスの、インターネットでルーティング可能な IP アドレス (静的)	カスタマーゲートウェイを作成して設定するために使用されます。YOUR_UPLINK_ADDRESS と呼ばれます。	値が静的な値であること、および、ネットワークアドレス変換 (NAT) を実行するデバイスの背後ではないことが必要です。	

項目	用途	コメント	
（オプション）動的にルーティングされる VPN 接続を作成する場合は、カスタマーゲートウェイのボーダーゲートウェイプロトコル（BGP）自律システム番号（ASN）。	カスタマーゲートウェイを作成して設定するために使用されます。YOUR_BGP_ASN と呼ばれます。 コンソールでウィザードを使用して VPC を設定すると、ASN として自動的に 65000 が使用されます。	ネットワークに割り当てられている既存の ASN を使用できます。既存の ASN がない場合は、プライベート ASN（64512 から 65534 までの範囲）を使用できます。ASN の詳細については、「Wikipedia の記事」を参照してください。 Amazon VPC は 2 バイトの ASN 番号をサポートしています。	
VPC への VPN 接続を通してアドバタイズする内部ネッ ワーク IP の範囲。	静的ルーターを指定するために使用されます。		

VPN 接続用に 2 つの VPN トンネルを設定する

ネットワークを VPC に接続するには、VPN 接続を使用します。各 VPN 接続には 2 つのトンネルがあり、それぞれのトンネルが固有の仮想プライベートゲートウェイのパブリック IP アドレスを使用します。冗長性を確保するために両方のトンネルを設定することが重要です。1 つのトンネルが使用できなくなったとき（例えばメンテナンスのために停止）、ネットワークトラフィックはその特定の VPN 接続用に使用可能なトンネルへ自動的にルーティングされます。

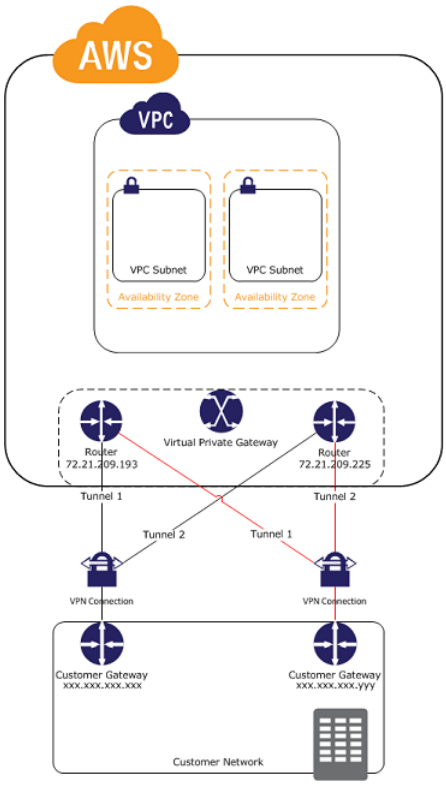
次の図は、VPN 接続の 2 つのトンネルを示しています。



冗長な VPN 接続を使用してフェイルオーバーを提供する

前述のように、VPN 接続では、接続の 1 つが使用できなくなった場合に備えて 2 つのトンネルを設定します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 番目のカスタマーゲートウェイを使用して、VPC への 2 番目の VPN 接続を設定できます。冗長な VPN 接続とカスタマーゲートウェイを使用すれば、1 つのカスタマーゲートウェイでメンテナンスを実行しながら、2 番目のカスタマーゲートウェイの VPN 接続を通してトラフィックの送信を継続することができます。冗長な VPN 接続とカスタマーゲートウェイをネットワークに確立するには、2 番目の VPN 接続を設定する必要があります。2 番目の VPN 接続のカスタマーゲートウェイの IP アドレスはパブリックにアクセス可能である必要があり、1 番目の VPN 接続に使用しているパブリック IP アドレスと同じアドレスにすることはできません。

次の図は、VPN 接続の 2 つのトンネルと 2 つのカスタマーゲートウェイを示しています。



動的にルーティングされる VPN 接続では、ボーダーゲートウェイプロトコル (BGP) を使用して、カスタマーゲートウェイと仮想プライベートゲートウェイ間で情報をルーティングします。静的にルーティングされる VPN 接続では、カスタマーゲートウェイのユーザー側でネットワークの静的ルートを入力する必要があります。BGP でアドバタイズされる静的に入力されたルート情報によって、双方のゲートウェイで使用可能なトンネルを判別し、障害発生時にトラフィックを再ルーティングすることができます。BGP (使用可能な場合) で提供されるルーティング情報を使用して使用可能なパスを選択するようネットワークを設定することをお勧めします。正確な設定はネットワークのアーキテクチャーによって異なります。

VPN 接続を設定する

VPN 接続を手動で設定するには、次の手順を実行します。別の方法として、VPC およびサブネットを作成してから、VPC ウィザードを使用してこの手順の最初の 4 つのステップを実行する方法もあります。詳細については、「シナリオ 3 を実装する (p. 37)」または「シナリオ 4 を実装する (p. 45)」を参照してください。

この 手順 では、1 つ以上のサブネットがある VPC を使用し、必要なネットワーク情報 (VPN 接続に必要なもの (p. 140) を参照) を所有していることを前提にしています。

1. カスタマーゲートウェイを作成する。

   a. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
   b. ナビゲーションペインで [Customer Gateways] をクリックしてから、[Create Customer Gateway] をクリックします。
   c. ルーティングのタイプとカスタマーゲートウェイデバイスの静的 IP アドレスを指定し、[Yes, Create] をクリックします。

2. 仮想プライベートゲートウェイを作成して VPC に関連付ける。

   a. ナビゲーションペインで [Virtual Private Gateways] をクリックしてから、[Create Virtual Private Gateway] をクリックします。
   b. プロンプトが表示されたら、[Yes, Create] をクリックします。
   c. 作成した仮想プライベートゲートウェイを選択して、[Attach to VPC] をクリックします。
   d. [Attach to VPC] ダイアログボックスで、一覧から VPC を選択し、[Yes, Attach] をクリックします。

3. ルートテーブルにルートを追加し、ルートの伝播を有効にします。。

   a. ナビゲーションペインで [Route Tables] をクリックして、サブネットと関連付けられたルートテーブルを選択します。デフォルトでは、これは VPC のメインルートテーブルです。
   b. 詳細ペインの [Routes] タブで、以下のいずれかの操作を実行してから、[Add] をクリックします。

      - VPN 接続の静的ルーティングを使用している場合は、VPN 接続で使用される静的ルートを [Destination] ボックスに追加し、[Target] リストから仮想プライベートゲートウェイ ID を選択します。
      - VPN 接続に動的ルーティングを使用している場合は、カスタマーネットワークの IP プレフィックスを [Destination] ボックスに入力し、仮想プライベートゲートウェイ ID を [Target] リストで選択します。

   c. 詳細ペインの [Route Propagation] タブで、VPC に関連付けられた仮想プライベートゲートウェイを一覧から選択し、[Add] をクリックします。

      Note

      VPN 接続で動的ルーティングを使用するように設定し、ルートの伝播を有効にした場合、カスタマーゲートウェイから BGP でアドバタイズされたルートがルートテーブルに表示されるには、VPN 接続のステータスが UP である必要があります。

4. セキュリティグループにルールを追加し、ネットワークからの SSH および RDP アクセスを有効にします。インバウンドルールの追加の詳細については、「ルールを追加および削除する (p. 74)」を参照してください。

   a. ナビゲーションペインで [Security Groups] をクリックして、VPC のデフォルトのセキュリティグループを選択します。
   b. 詳細ペインの [Inbound] タブで、インバウンド SSH アクセスのルールと、ネットワークからグループへのインバウンド RDP アクセスのルールを追加してから、[Apply Rule Changes] をクリックします。

5. VPN 接続を作成する。

   a. ナビゲーションペインで [VPN Connections] をクリックします。
   b. [Create VPN Connection] をクリックします。
   c. [Add VPN Connection] ダイアログボックスで、次の操作を行い、[Yes, Create] をクリックします。

      - カスタマーゲートウェイの IP アドレスを指定します。

- VPN ルートがボーダーゲートウェイプロトコル (BGP) をサポートしているかどうかに基づいて、いずれかのルーティングオプションを選択します。
  - VPN ルーターが BGP をサポートしている場合は、[Use dynamic routing (requires BGP)] を選択します。
  - VPN ルーターが BGP をサポートしていない場合は、[Use static routing] を選択します。[IP Prefix] ボックスで、VPN 接続のプライベートネットワークの各 IP プレフィックスを指定し、[Add] をクリックします。

6. カスタマーゲートウェイを設定する。
   a. ナビゲーションペインで [VPN Connections] をクリックします。
   b. VPN 接続を選択し、[Download Configuration] をクリックします。
   c. このガイド (Amazon Virtual Private Cloud Network Administrator Guide) とともに、ネットワーク管理者に設定情報を連絡します。ネットワーク管理者がカスタマーゲートウェイを設定した後、VPN 接続が機能するようになります。

7. サブネット内にインスタンスを起動する。
   a. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
   b. [Navigation] ペインの [Instances] をクリックします。
   c. [Launch Instance] をクリックします。
   d. [Create a New Instance] ページで [Quick Launch Wizard] をクリックし、指示にしたがって操作します。インスタンスの名前を指定し、キーペア、AMI の順に選択し、[Continue] をクリックします。
   e. [Edit Details] をクリックし、[Instance Details] の [Launch into a VPC] を選択し、サブネットを指定してから、[Save Details] をクリックします。
   f. 選択した設定を確認します。必要に応じて設定を変更し、[Launch] をクリックします。

インスタンスのエンドツーエンド接続のテスト

VPN 接続を設定してインスタンスを起動した後、インスタンスへの ping を実行して接続をテストします。ping リクエストに応答する AMI を使用する必要があります。Amazon Linux AMI のいずれかを使用することをお勧めします。ご使用のインスタンスで Windows Server を実行している場合、インスタンスへの ping を実行するには、インスタンスにログインし、Windows ファイアウォールでインバウンド ICMPv4 を有効にする必要があります。

Important

インバウンドおよびアウトバウンドの ICMP トラフィックを許可するために、インスタンスへのトラフィックをフィルタするセキュリティグループまたはネットワーク ACL を VPC 内に設定する必要があります。

Amazon VPC コンソールまたは Amazon EC2 API/CLI を使用して、VPN 接続のステータスをモニタリングできます。VPN 接続について、接続の状態、最後の状態変化からの経過時間、エラー説明のテキストなどの情報を確認できます。

エンドツーエンド接続をテストするには

1. インスタンスが実行中になった後、そのプライベート IP アドレス (例えば `10.0.0.4`) を取得します。Amazon EC2 コンソールにインスタンスの詳細の一部としてアドレスが表示されます。
2. ネットワークでカスタマーゲートウェイの背後にあるコンピュータから、インスタンスのプライベート IP アドレスを指定した ping コマンドを実行します。正常な応答は次のようになります。

```
PROMPT> ping 10.0.0.4
Pinging 10.0.0.4 with 32 bytes of data:

Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.4:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

これで SSH または RDP を使用して、VPC のインスタンスに接続できるようになりました。Linux インスタンスに接続する方法については、「*Amazon Elastic Compute Cloud User Guide*」の Connect to Your Linux Instance を参照してください。Windows インスタンスに接続する方法については、「*Amazon Elastic Compute Cloud Microsoft Windows Guide*」の Connect to Your Windows Instance を参照してください。

漏洩した認証情報の置き換え

VPN 接続のトンネル認証情報が漏洩したと思われる場合は、IKE 事前共有キーを変更できます。そのためには、VPN 接続を削除し、同じ仮想プライベートゲートウェイを使用して新しい接続を作成して、カスタマーゲートウェイに新しいキーを設定します。また、トンネルの内部のアドレスと外部のアドレスが一致することを確認することも必要です。VPN 接続を再作成するとアドレスが変更されることがあるためです。この手順を実行する間、VPC 内のインスタンスとの通信は停止しますが、インスタンスは中断されずに実行を継続します。ネットワーク管理者が新しい設定情報を実装した後、VPN 接続に新しい認証情報が使用されるようになり、VPC 内のインスタンスへのネットワーク接続が再開されます。

Important

この手順にはネットワーク管理者グループの助けが必要です。

IKE 事前共有キーを変更するには

1. VPN 接続を削除します。VPC または仮想プライベートゲートウェイを削除する必要はありません。
   a. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
   b. ナビゲーションペインで [VPN Connections] をクリックします。
   c. VPN 接続を選択し、[Delete] をクリックします。
   d. [Delete VPN Connection] ダイアログボックスの [Yes, Delete] をクリックします。

2. 新しい VPN 接続を作成します。

   a. 同じ [VPN Connections] ページで、[Create VPN Connection] をクリックします。仮想プライベートゲートウェイとカスタマーゲートウェイが既に選択されています。

   b. VPN ルーターがボーダーゲートウェイプロトコル (BGP) をサポートしているかどうかに基づいて、ルーティングオプションの 1 つを選択します。不明な場合は、「Amazon Virtual Private Cloud のよくある質問」を参照してください。

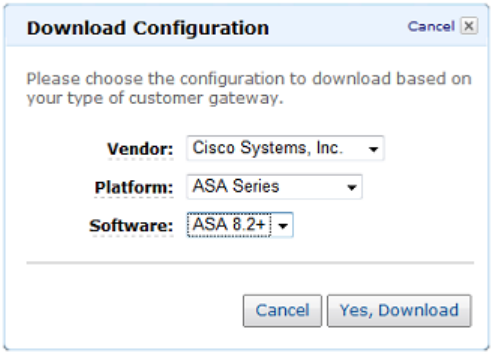
      - VPN ルーターがボーダーゲートウェイプロトコル (BGP) をサポートしている場合は、[Use dynamic routing (requires BGP)] をクリックします。
      - VPN ルーターが BGP をサポートしていない場合は、[Use static routing] をクリックします。[IP Prefix] ボックスにネットワークの各 IP プレフィックスを入力し、[Add] をクリックします。

   c. [Yes, Create] をクリックします。

3. 新しいカスタマーゲートウェイ設定をダウンロードします。この設定はネットワーク管理者が実装する必要があります。この新しい設定は、古い IKE 事前共有キーを使用する以前のゲートウェイ構成に置き換わります。

   a. 作成した VPN 接続を選択し、[Download Configuration] をクリックします。

   b. カスタマーゲートウェイのベンダー、プラットフォーム、およびソフトウェアバージョンを選択し、[Yes, Download] をクリックします。



   c. テキストファイルを保存し、Amazon Virtual Private Cloud Network Administrator Guide とともにネットワーク管理者に渡します。

VPN 接続を削除する

VPN 接続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。

Important

VPN 接続を削除し、新しい VPN 接続を作成する場合は、新しい設定情報をダウンロードし、ネットワーク管理者にカスタマーゲートウェイを再設定してもらう必要があります。

VPN 接続を削除するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [VPN Connections] をクリックします。
3. VPN 接続を選択し、[Delete] をクリックします。
4. [Delete VPN Connection] ダイアログボックスの [Yes, Delete] をクリックします。

カスタマーゲートウェイ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。VPN 接続で使用中のカスタマーゲートウェイを削除することはできません。

カスタマーゲートウェイを削除するには

1. ナビゲーションペインで [Customer Gateways] をクリックします。
2. 削除するカスタマーゲートウェイを選択し、[Delete] をクリックします。
3. [Delete Customer Gateway] ダイアログボックスで、[Yes, Delete] をクリックします。

VPC 用の仮想プライベートゲートウェイが不要になった場合には、それをアタッチ解除することができます。

仮想プライベートゲートウェイをアタッチ解除するには

1. ナビゲーションペインで [Virtual Private Gateways] をクリックします。
2. 仮想プライベートゲートウェイを選択し、[Detach from VPC] をクリックします。
3. [Detach from VPC] ダイアログボックスで、[VPC] リストをクリックし、アタッチ解除する VPC を選択してから、[Yes, Detach] をクリックします。

仮想プライベートゲートウェイ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。VPC にアタッチされている仮想プライベートゲートウェイを削除することはできません。

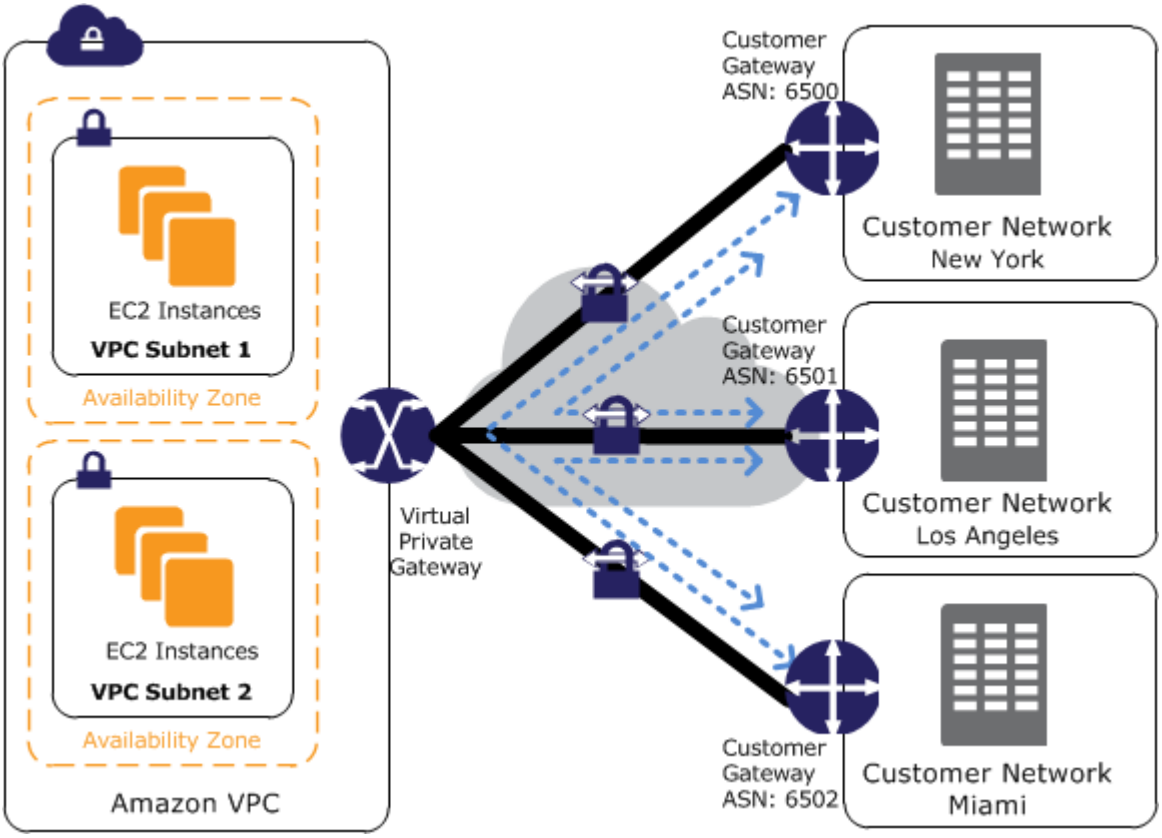
仮想プライベートゲートウェイを削除するには

1. 削除する仮想プライベートゲートウェイを選択し、[Delete] をクリックします。
2. [Delete Virtual Gateway] ダイアログボックスで、[Yes, Delete] をクリックします。

VPN CloudHub を使用して安全なサイト間通信を提供する

複数の VPN 接続がある場合は、AWS VPN CloudHub を使用して、安全なサイト間通信を提供することができます。VPN CloudHub は、VPC の有無にかかわらず使用できるシンプルなハブアンドスポークモデルで動作します。この設計は、複数のブランチオフィスと既存のインターネット接続を持つ顧客が、リモートオフィス間でプライマリ接続またはバックアップ接続を実現するために、便利でコストを抑えられる可能性のあるハブアンドスポークモデルを実装したいと考えている場合に適しています。

次の図は VPN CloudHub アーキテクチャーです。青色の点線は、VPN 接続を介してルーティングされているリモートサイト間のネットワークトラフィックを示しています。



AWS VPN CloudHub を使用するには、仮想プライベートゲートウェイと、複数のカスタマーゲートウェイを作成する必要があり、それぞれに固有のボーダーゲートウェイプロトコル（BGP）自律システム番号（ASN）があります。カスタマーゲートウェイは、適切なルート（BGP プレフィックス）をその VPN 接続にアドバタイズします。これらのルーティングアドバタイズメントが受信され、各 BGP ピアに再アドバタイズされることで、サイト間でのデータの送受信が可能になります。各スポークのルートに固有の ASN があるので、サイトの IP 範囲が重なることはありません。各サイトが、標準の VPN 接続を使用しているように、VPC とデータを送受信することもできます。

仮想プライベートゲートウェイへの AWS Direct Connect 接続を使用するサイトを、AWS VPN CloudHub に含めることもできます。例えば、ニューヨーク本社で VPC への AWS Direct Connect 接続を確立しながら、ブランチオフィスで VPC への VPN 接続を使用できます。ロサンゼルスとマイアミのブランチオフィスは、AWS VPN CloudHub を使用して、相互にデータを送受信したり、本社とデータを送受信したりできます。

AWS VPN CloudHub を設定するには、AWS マネジメントコンソールを使用して、複数のカスタマーゲートウェイを作成します。このそれぞれに、ゲートウェイの固有のパブリック IP アドレスと固有の ASN があります。次に、各カスタマーゲートウェイから一般的な仮想プライベートゲートウェイへの VPN 接続を作成します。各 VPN 接続が、その特定の BGP ルートをアドバタイズする必要があります。これを行うには、VPN 接続の VPN 設定ファイルでネットワークステートメントを使用します。ネットワークステートメントは、使用するルーターの種類によって少し違いがあります。

AWS VPN CloudHub を使用する場合は、通常の Amazon VPC VPN 接続料金を支払います。各 VPN が仮想プライベートゲートウェイに接続されている間は、1 時間ごとに接続料金が発生します。AWS VPN CloudHub を使用してサイト間でデータを送信する場合、サイトから仮想プライベートゲートウェイへのデータ送信にはコストがかかりません。仮想プライベートゲートウェイからエンドポイントに中継されるデータに対しては、標準の AWS データ転送料金のみがかかります。例えば、ロサンゼルスとニューヨークそれぞれにサイトがあり、両方のサイトに、仮想プライベートゲートウェイへの VPN 接続が存在する場合は、VPN 接続ごとに 0.05 USD/時間（合計 0.10 USD/時間）の支払いが発生します。また、ロサンゼルスからニューヨーク（およびその逆）に VPN 接続経由でデータを送信すると、そのデータ

すべてに対して標準の AWS データ転送料金が発生します。VPN 接続経由で仮想プライベートゲートウェイに送信されるネットワークトラフィックは無料ですが、VPN 接続経由で仮想プライベートゲートウェイからエンドポイントに送信されるネットワークトラフィックには、標準の AWS データ転送料金がかかります。詳細については、「VPN 接続料金表」を参照してください。

EC2 ハードウェア専有インスタンスの使用

Amazon EC2 ハードウェア専有インスタンスは、シングルテナントのハードウェアで実行されます。このようなインスタンスは、お使いになっているその他のインスタンスや、他の AWS アカウントに属するインスタンスとは、ホストハードウェアのレベルで物理的に分離されます。ハードウェア専有インスタンスは Virtual Private Cloud (VPC) 内に起動する必要があります。

このトピックでは、ハードウェア専有インスタンスの基礎を説明し、その実装方法を示します。

Topics

ハードウェア専有インスタンスの基礎

VPC 内に起動する各インスタンスにはテナント属性があります。この属性の値を次に示します。

値	説明
`default`	インスタンスは共有するハードウェアで実行されます。
`dedicated`	インスタンスはシングルテナントのハードウェアで実行されます。

インスタンスの起動後にテナント属性を変更することはできません。インスタンス起動時にテナント属性を `dedicated` に設定しなかった場合は、インスタンスの実行を停止し、テナント属性を設定してから、インスタンスを再起動する必要があります。

各 VPC には関連したインスタンスのテナント属性があります。この属性の値を次に示します。

値	説明
`default`	VPC 内に起動されたインスタンスは、インスタンスのテナント属性が `dedicated` である場合、ハードウェア専有インスタンスです。
`dedicated`	VPC 内に起動されたすべてのインスタンスは専有インスタンスであり、インスタンスのテナント属性の値は関係ありません。

VPC の作成後に VPC インスタンスのテナント属性を変更することはできません。変更するには、VPC 内のインスタンスを終了し、VPC を削除してから、インスタンスのテナント属性に新しい値を指定して VPC を再作成し、インスタンスを再起動する必要があります。

ハードウェア専有インスタンスを使用する場合は、次のいずれかの方法でインスタンスを実装できます。

- インスタンスのテナント属性を `dedicated` (この VPC 内に起動されたすべてのインスタンスはハードウェア専有インスタンス) に設定して VPC を作成します。
- インスタンスのテナント属性を `default` に設定して VPC を作成し、起動時にハードウェア専有インスタンスとするインスタンスの専有テナント属性を指定します。

Amazon EBS とハードウェア専有インスタンス

Amazon EBS バックト専有インスタンスを起動した場合、シングルテナントのハードウェアで EBS ボリュームは実行できません。

専有テナント属性を所有するリザーブドインスタンス

専有インスタンスを起動するうえで十分な空き容量を確保するために、専有リザーブドインスタンスを購入できます。リザーブドインスタンスの詳細については、「オンデマンドとリザーブドインスタンス」を参照してください。

ハードウェア専有リザーブドインスタンスを購入すると、VPC 内にハードウェア専有インスタンスを起動するための容量を格安の使用料金で購入することになります。時間単位での料金引き下げは、専有テナント属性が指定されたインスタンスを起動した場合にのみ適用されるためです。ただし、デフォルトのテナント属性値でリザーブドインスタンスを購入する場合は、`dedicated` インスタンステナント属性でインスタンスを起動するときに、ハードウェア専有リザーブドインスタンスは取得されません。

さらに、リザーブドインスタンスの購入後にそのインスタンスのテナント属性を変更することはできません。

ハードウェア専有インスタンスの Auto Scaling

ハードウェア専有インスタンスの Auto Scaling を使用する場合、インスタンスのテナント属性を `dedicated` に設定した VPC 内に起動する必要があります。

ハードウェア専有インスタンスの価格設定

ハードウェア専有インスタンスには個別の価格設定モデルがあります。詳細については、Amazon EC2 ハードウェア専有インスタンスの製品ページを参照してください。

ハードウェア専有インスタンスの使用

このセクションでは、次のタスクの実行方法を説明します。

Topics

インスタンスのテナント属性が専有である VPC を作成する

VPC を作成するときにインスタンスのテナント属性を指定できます。デフォルト設定のまま使用することも、使用する VPC にインスタンスのテナント属性として `dedicated` を指定することもできます。このセクションでは、インスタンスのテナント属性を `dedicated` に設定した VPC を作成する方法を示します。

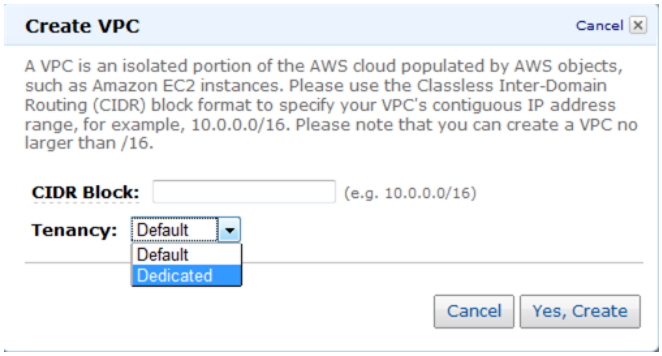
インスタンスのテナント属性がハードウェア専有である VPC を作成するには (VPC ウィザード)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ダッシュボードで [Start VPC Wizard] ボタンをクリックします。
3. VPC 設定を選択し、[Continue] をクリックします。
4. 確認ページで、[Edit Hardware Tenancy] をクリックし、[Dedicated] を選択します。

5. [Create VPC] ボタンをクリックして VPC を作成します。

インスタンスのテナント属性がハードウェア専有である VPC を作成するには (VPC ダイアログボックスの作成)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Your VPCs] をクリックし、[Create VPC] ボタンをクリックします。
3. [Create VPC] ダイアログボックスで、[Tenancy] ドロップダウンリストから [Dedicated] を選択します。[CIDR Block] を指定し、[Yes, Create] をクリックします。

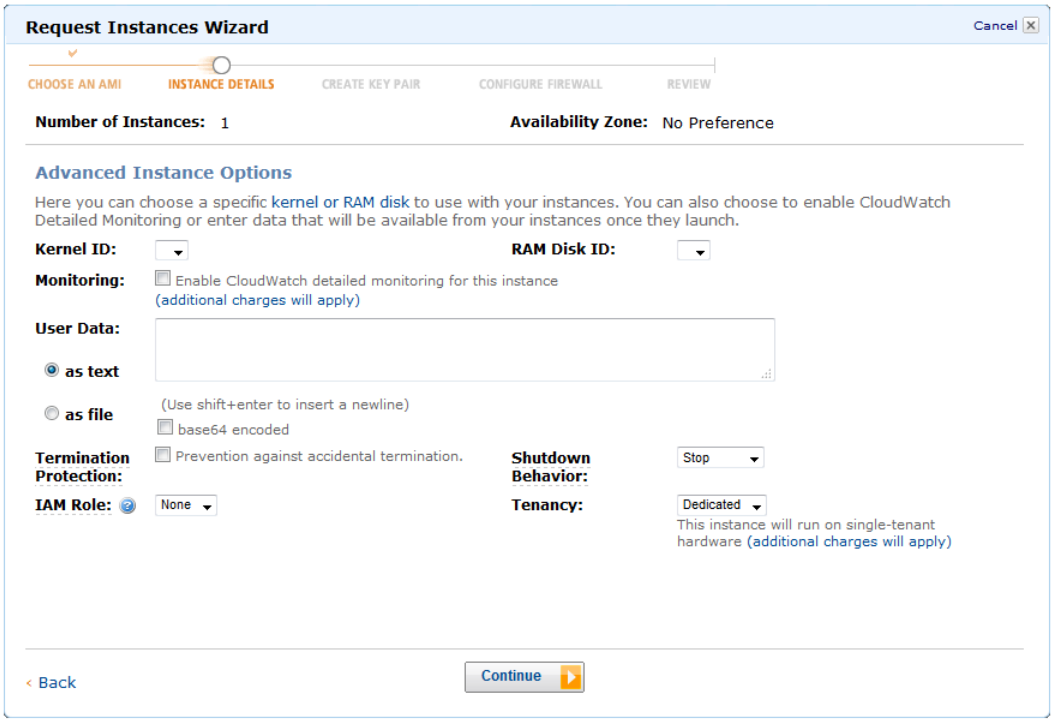


ハードウェア専有インスタンスを VPC 内に起動する

インスタンスのテナント属性が `dedicated` である VPC 内にインスタンスを起動すると、インスタンスのテナント属性とは関係なく、インスタンスは自動的にハードウェア専有インスタンスとなります。次の手順は、デフォルトのインスタンスのテナント属性が指定された VPC 内にハードウェア専有インスタンスを起動する方法を示しています。

デフォルトのインスタンスのテナント属性が指定されたハードウェア専有インスタンスを VPC 内に起動するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. VPC を作成するか、既存の VPC を使用します。
3. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
4. [Launch Instance] ボタンをクリックし、[Classic Wizard] を選択して、[Continue] をクリックします。
5. [CHOOSE AN AMI] ページで、AMI を選択します。
6. [INSTANCE DETAILS] ページで、[Instance Type] リストから [M1 small (m1.small)] を選択します。[Launch Instances] で、インスタンスを起動する VPC のサブネットを選択します。[Continue] をクリックします。
7. [Advanced Instance Options] で、[Tenancy] ドロップダウンリストから [Dedicated] を選択し、[Continue] をクリックします。

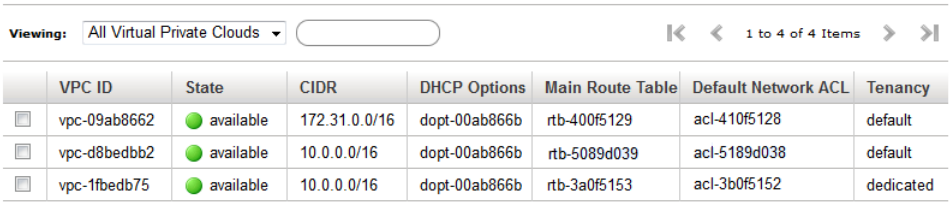


8. VPC ウィザードにしたがって続行します。[REVIEW] ページでオプションを確認し終わったら、[Launch] ボタンをクリックしてハードウェア専有インスタンスを起動します。

テナント属性情報を表示する

VPC のテナント属性情報を表示するには

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. ナビゲーションペインで [Your VPCs] をクリックします。
3. [Tenancy] 列で、VPC のインスタンスのテナント属性を確認します。

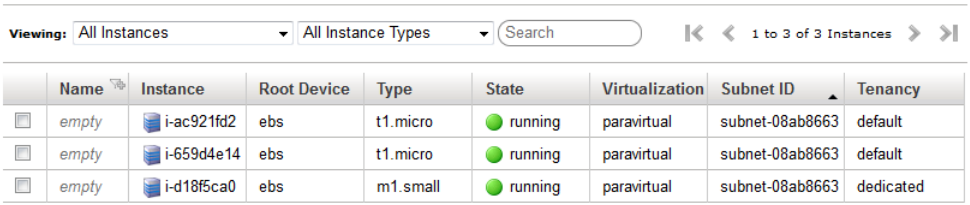


	VPC ID	State	CIDR	DHCP Options	Main Route Table	Default Network ACL	Tenancy
☐	vpc-09ab8662	available	172.31.0.0/16	dopt-00ab866b	rtb-400f5129	acl-410f5128	default
☐	vpc-d8bedbb2	available	10.0.0.0/16	dopt-00ab866b	rtb-5089d039	acl-5189d038	default
☐	vpc-1fbedb75	available	10.0.0.0/16	dopt-00ab866b	rtb-3a0f5153	acl-3b0f5152	dedicated

4. [Tenancy] 列が表示されていない場合は、[Show/Hide] ボタンをクリックし、[Show/Hide Columns] ダイアログボックスで [Tenancy] を選択して、[Close] をクリックします。

インスタンスのテナント属性情報を表示するには

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. ナビゲーションペインで [Instances] をクリックします。
3. [Tenancy] 列でインスタンスのテナント属性を確認します。



4. [Tenancy] 列が表示されていない場合は、次のいずれかを行います。

   - [Show/Hide] ボタンをクリックし、[Show/Hide Columns] ダイアログボックスで [Tenancy] を選択して、[Close] をクリックします。
   - インスタンスを選択します。詳細ペインの [Description] タブに、テナント属性を含めてインスタンスに関する情報が表示されます。次に例を示します。

API とコマンドの概要

次の表は、ハードウェア専有インスタンスに使用できるコマンドと API アクションの一覧です。

説明	コマンド	API アクション
VPC 内に起動するインスタンスに対して、サポートされているテナント属性オプションを指定できます。`default` の値は、任意のテナント属性が指定されたインスタンスを VPC 内に起動できることを意味します。`dedicated` の値は、すべてのインスタンスをハードウェア専有インスタンスとして VPC 内に起動する必要があることを意味します。	ec2-create-vpc	CreateVpc
VPC 内に起動するインスタンスに対してサポートされているテナント属性オプション (`default` または `dedicated`) を定義します。	ec2-describe-vpcs	DescribeVpcs
VPC 内に起動するインスタンスのテナント属性オプション (`default` または `dedicated`) を指定できます。	ec2-run-instances	RunInstances
インスタンスのテナント属性値 (`default` または `dedicated`) を定義します。	ec2-describe-instances	DescribeInstances
リザーブドインスタンスのテナント属性値 (`default` または `dedicated`) を定義します。	ec2-describe-reserved-instances	DescribeReservedInstances

説明	コマンド	API アクション
リザーブドインスタンスサービスのテナント属性値 (`default` または `dedicated`) を定義します。	ec2-describe-reserved-instances-offerings	DescribeReservedInstancesOfferings

Amazon VPC 制限

次の表は、Amazon VPC に関連する制限数を表示しています。この制限数を増やすよう要請するには、Amazon VPC 制限フォームを参照してください。

コンポーネント	制限	コメント
リージョン当たりの VPC の数	5	
VPC 当たりのサブネットの数	200	
リージョン当たりのインターネットゲートウェイの数	5	VPC 当たり 1
リージョン当たりの仮想プライベートゲートウェイの数	5	VPC 当たり 1
リージョン当たりのカスタマーゲートウェイの数	50	
リージョン当たりの VPN 接続の数	50	仮想プライベートゲートウェイ当たり 10
VPC 当たりのルートテーブルの数	10	メインルートテーブルを含む
ルートテーブル当たりのエントリの数	20	
AWS アカウント当たり、1 リージョン内の Elastic IP アドレスの数	5	Amazon EC2 には、AWS アカウント当たり 1 リージョン内の Elastic IP アドレスの数について独自の制限があります。
VPC 当たりのセキュリティグループの数	100	
セキュリティグループ当たりのルールの数	50	
VPC 内のインスタンスに割り当てることができるセキュリティグループの数	5	
VPC 当たりのネットワーク ACL の数	50	
ネットワーク ACL 当たりのルールの数	20	

コンポーネント	制限	コメント
VPN 接続当たりの BGP アドバタイズドルートの数	100	

ドキュメントの履歴

次の表に、この Amazon VPC ガイドの各リリースにおける重要な変更点を示します。

機能	API バージョン	説明	リリース日
パブリック IP アドレスの割り当て	2013-07-15	VPC 内に起動されたインスタンス用の新しいパブリック IP アドレス指定機能に関する情報を追加しました。詳細については、「起動中のパブリック IP アドレスの割り当て (p. 102)」を参照してください。	2013 年 8 月 20 日
DNS ホスト名の有効化と DNS 解決の無効化	2013-02-01	デフォルトでは、DNS 解決は有効になっています。DNS 解決は、Amazon VPC コンソール、Amazon EC2 コマンドラインインターフェイス、または Amazon EC2 API アクションを使用して無効にできます。 デフォルトでは、デフォルトではない VPC に対して DNS ホスト名は無効になっています。DNS ホスト名は、Amazon VPC コンソール、Amazon EC2 コマンドラインインターフェイス、または Amazon EC2 API アクションを使用して有効にできます。 詳細については、「VPC での DNS の使用 (p. 133)」を参照してください。	2013 年 3 月 11 日
静的なルーティング設定を使用した VPN 接続	2012-08-15	静的なルーティング設定を使用して Amazon VPC への IPsec VPN 接続を作成できます。以前は、VPN 接続にはボーダーゲートウェイプロトコル（BGP）を使用する必要がありました。現在では両方のタイプの接続をサポートしており、Cisco ASA や Microsoft Windows Server 2008 R2 など、BGP をサポートしていないデバイスからの接続も可能です。	2012 年 9 月 13 日

機能	API バージョン	説明	リリース日
ルートの自動伝播	2012-08-15	VPN および Direct Connect リンクから VPC ルーティングテーブルへのルートの自動伝播を設定できるようになりました。この機能により、Amazon VPC への接続を作成して維持する手間が簡略化されます。	2012 年 9 月 13 日
AWS VPN CloudHub と冗長な VPN 接続		VPC の有無にかかわらず、1 つのサイトから別のサイトに安全に通信できます。冗長な VPN 接続を使用して、VPC へのフォールトトレラントな接続ができます。	2011 年 9 月 29 日
VPC Everywhere	2011-07-15	5 つの AWS リージョンでのサポート、複数のアベイラビリティーゾーンでの VPC、AWS アカウント当たり複数の VPC、VPC 当たり複数の VPN 接続、Microsoft Windows Server 2008 R2 および Microsoft SQL Server リザーブドインスタンス。	2011 年 8 月 3 日
ハードウェア専有インスタンス	2011-02-28	ハードウェア専有インスタンスとは、単一のお客様専用のハードウェアを実行する VPC 内で起動される Amazon EC2 インスタンスのことです。ハードウェア専有インスタンスを使用すれば、インスタンスをハードウェアレベルで確実に分離しながら、従量課金制、プライベートの独立した仮想ネットワークといった、Amazon VPC と AWS 伸縮自在なプロビジョニングの利点を十分にご活用いただけます。	2011 年 3 月 27 日