AWSクラウド演習

AWSクラウド演習授業資料3

VPC(VIRTUAL PRIVATE CLOUD)

- VPC(Virtual Private Cloud)とは

  独自の仮想プライベートネットワークを構築できるサービス。VPCを使用することにより、他の仮想ネットワークから論理的に分離することができます。

  リージョンとAZ(アベイラビリティゾーン)に構築することができます。

- VPCで制御できるもの

  IPアドレスの範囲、サブネットの作成、ルートテーブル(ルーティングテーブル)の作成、

  ネットワークゲートウェイ、セキュリティ設定などを使用することができます。

VPCのコンポーネント

VPCに多くの用語やコンポーネントがあります。

- サブネット

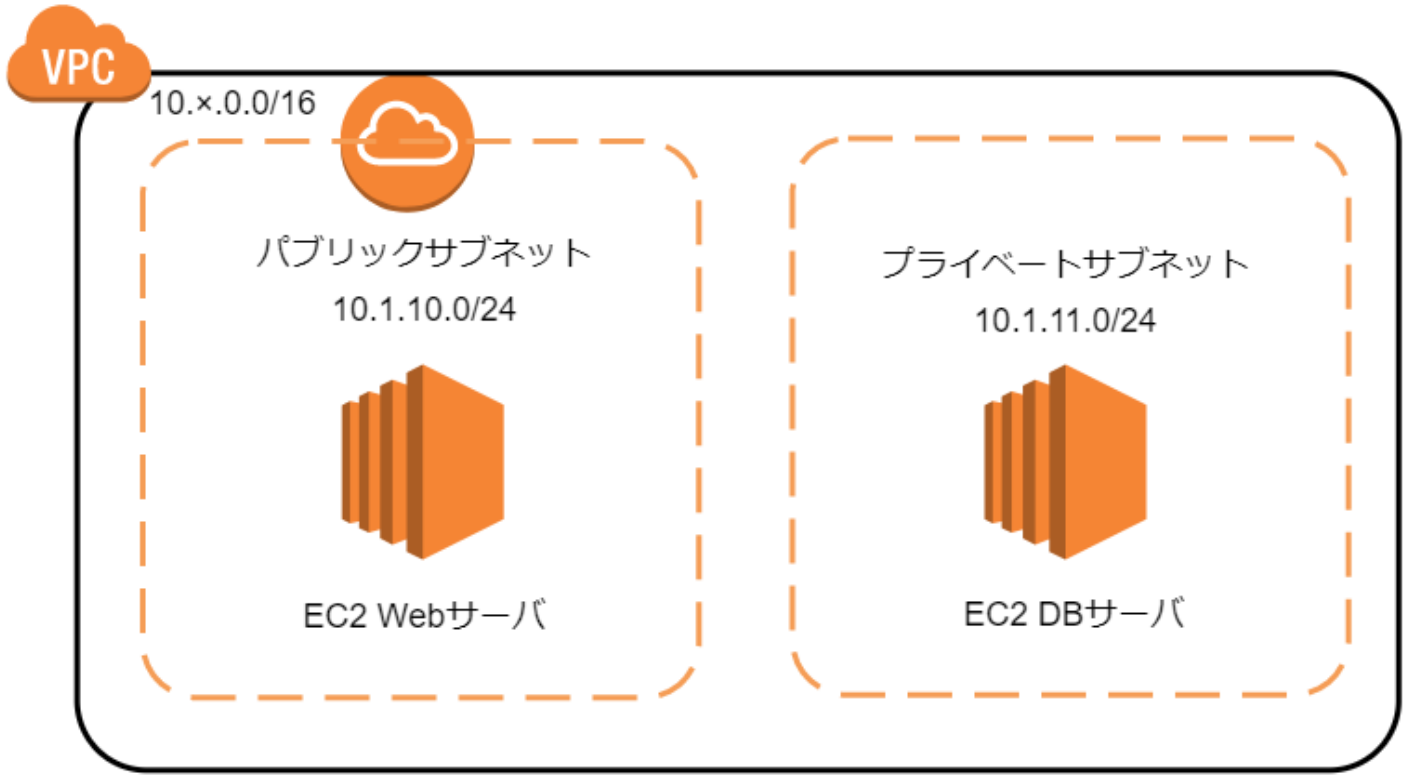
  VPCを分割したネットワークのこと。サブネットは1つのネットワークを意味し、VPC内に複数設定することができます。サブネットは役割に応じて次のように分けられます。

  パブリックサブネット　・・・　外部に公開するネットワーク
  プライベートサーブネット　・・・　外部に公開しない内部ネットワーク。

  ＊マルチサブネット　・・・　複数のAZに分けてサーバを構築すること。

サブネットのイメージ図

- Webサーバをパブリックサブネット、DBサーバをプライベートサブネットに配置した例



- CIDRとは

  IPアドレスのして方法の1つです。サブネットマスク(プレフィクス長)を使用してVPCをサブネットに分割する時に使用します。

  10.1.10.0/24　・・・　プレフィクス長、サブネットマスクを意味します。/8～/28

  ＊AWSの場合、基本情報処理の授業で習ったもの違う部分がありますの注意してください。

- インターネットゲートウェイ(Internet GateWay:IGW)

  サブネットからインターネット(外部)へ接続するための出入口です。

- エンドポイント

  他のサービスに接続するために直接接続するための出入口です。インターネットGWなど経由せずに接続できます。

- NATゲートウェイ(NATインスタンス)

  インターネットなど外部へプライベートサブネットからアクセスするためのものです。通信に料金がかかるので必要な時のみ使用します。

- ルートテーブル

  パケットの行き先を設定するためのテーブルです。一般にルーティングテーブルと呼ばれます。
  インターネットGWなどを指定します。

VPCのトラフィックの設定

VPCへアクセスできるサービスやプロトコルなどをしてします。指定方法は、セキュリティグループとネットワークACL(Access Control List)があります。

- セキュリティグループ
  ステートフルな仮想ファイアウォールのこと。アクセスを許可するサービスやプロトコルを指定します。＊インバウンド(受信)のみの設定を行います。

- ネットワークACL
  ステートレスな仮想ファイアウォールのこと。インバウンド(受信)とアウトバウンド(送信)の両方を設定する必要があります。

その他のコンポーネント

- EIP(Elastic IP)

  静的に割り当てられたパブリックアドレスのこと。インターネットにアクセスできる固定のIPアドレスですが、2つ以上割り当てた場合、料金がかかります。

- ENI(Elastic Network Interface)

  VPCに関連付けることができる仮想ネットワークインターフェースのことです。

- ピア接続

  VPC同士を接続した通信のことです。

VPCの設定手順

- VPCの設定手順は次の通りになります。

  ①CIDRでアドレスレンジの選択

  VPCに割り当てるネットワークを選択します。<例>10.1.0.0/16

  ②AZ(アベイラビリティゾーン)のサブネットを選択

  AZに割り当てるサブネットを選択します。<例>10.1.1.0/24

  ③インターネットの経路を選択

  IGW、ルートテーブルを設定して、外部へ接続できるようにします。

  ④VPCへのトラフィック許可の設定

  セキュリティグループまたはネットワークACLを選択します。<例>HTTPのみ許可など