

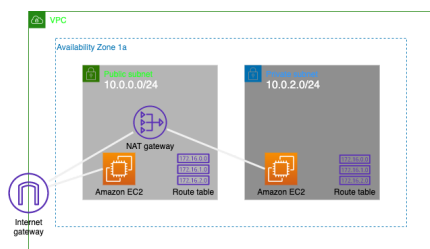
AWS】VPC～EC2試してみた①

2021.04.10に公開 5 min read

最終目標

AWS VPCを作成し、その中に二つのサブネット（片方はパブリック、もう片方はプライベート）を構築。そして各サブネットの中にAWS EC2を作成する。

※プライベートEC2にはパブリックEC2を踏み台にしてログインする事として、プライベートからのインターネット接続は、NAT gatewayを経由する事とする。



今回の目標

VPC、サブネットを構成図のように作成し、パブリックEC2を作成。ターミナルから

EC2にsshログインできることを確認する。

環境

端末:MacBook Pro(13-inch, 2020, Four Thunderbolt 3 ports)
OS :MacOS
Catalina(ver10.15.6)

VPCの作成

AWSマネジメントコンソールの上部検索でVPCを検索して開く



左メニューバーからVPCを選択してVPCの作成をクリック

名前を**test-vpc**としてIPv4 CIDR ブロックを以下のように設定する。



10.0.0.0/21について

「/21」IPアドレスを2進数表記したときにどこまで固定するかを示すもの。

(00000000 00000000 00000000 00000000)の32ビットで表現されたIPアドレスの

上から21番目までを固定していることになるので、今回の場合は以下の範囲である。

(10.0.0.0)～(10.0.7.255)

サブネットの作成

左メニューバーからサブネットを選択してサブネットの作成をクリック

先ほど作成したVPCを選択して関連付ける。



名前を**test-subnet-0**として
IPv4 CIDR ブロックを以下
のように設定する。



名前を**test-subnet-2**として
IPv4 CIDR ブロックを以下
のように設定する。



10.0.0.0/24,10.0.2.0/24 について

VPCで設定したIPアドレスの
範囲の中でそれぞれサブネッ
トを作成している。

- test-vpc :(10.0.0.0)～
(10.0.7.255)
- test-subnet-0:
(10.0.0.0)～(10.0.0.255)
- test-subnet-2:
(10.0.2.0)～(10.0.2.255)

「/24」は「/21」と比べて
1/8の範囲であることがわかる。

インターネット ゲートウェイの 作成

インターネットゲートウェイ
はVPC内部からインターネット
接続するためのコンポーネ
ントであり、VPCにアタッチ
することで可能となる。

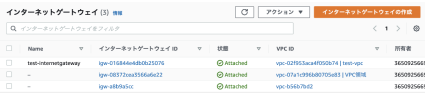
左メニューバーからイ ンターネットゲートウ エイを選択してインタ ーネットゲートウェイ の作成をクリック

名前をtest-
internetgatewayとして作
成する。



※作成してすぐは、どこにも
アタッチされていないので、
作成したインターネットゲー
トウェイを選択し、「アクシ
ョン」→「VPCにアタッチ」

より作成したVPCにアタッチする。成功すると、以下のよう
に状態が「Attached」になる。

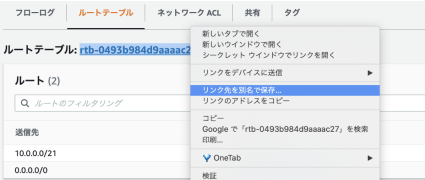


| Name | インターネットゲートウェイ ID | 状態 | VPC ID | 所有者 |
|----------------------|----------------------|----------|----------------------------------|------------|
| test-internetgateway | igw-01844a4b0d20276 | Attached | vpc-027955a4f0502b741 test-vpc | 3602925661 |
| - | igw-08172aa3556a6c22 | Attached | vpc-07a1c995680705a81 VPC接続 | 3602925661 |
| - | igw-48f695cc | Attached | vpc-b646b7b42 | 3602925661 |

ルートテーブルの編集

ローカルの通信はVPCにそれ
以外はインターネットゲート
ウェイにサブネットのルート
テーブルを編集する。

作成したサブネットを
クリックし、下部にあ
るルートテーブルを表
示させ、IDを右クリ
ックして新しいタブで
開く



画面下部のルートを選
択しルートの編集をク
リック

送信先を0.0.0.0/0としてタ
ーゲットを作成したインター

ネットゲートウェイに設定する。



0.0.0.0/0について

このIPアドレスは全てという意味があり、「デフォルトルート」と呼ばれる。流れとしては、デフォルトでは、ターゲットがインターネットゲートウェイになるが、VPC内部のIPアドレスのみターゲットがローカルになる。

EC2の作成

AWSマネジメントコンソールの上部検索でEC2を検索して開く



インスタンスを起動をクリックし作成するイ

インスタンスの設定を行う



今回は以下のAmazon Linux2 AMIを選択する。



ネットワークで作成したVPCを選択、サブネットは**test-subnet-0**を選択する。

※今回は自動割り当てパブリックIPを有効にしパブリックIPが割り当てられるようにする。

そしてストレージは起動確認を行うだけなので8GBのままを進める。



タグとしてNameに**test-ec2-1**と名前を付ける。

セキュリティグループは今回はデフォルトのままにする。



最後に起動ボタンをクリックするし、新しいキーペアを作成し、ダウンロードする。全て終了したらインスタンスを作成ボタンをクリックして作成を完了させる。

※作成に時間がかかる場合があるので、起動中になるのを待つ。



セキュリティグループを作成する

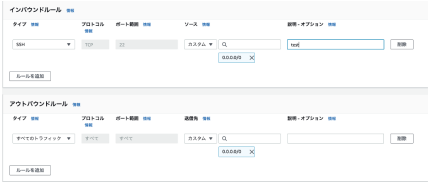
左メニューバーからセキュリティグループを選択してセキュリティグループの作成をクリック

名前をtest-sg-1とし、VPCを作成したVPCに設定する。



インバウンドとアウトバウンドのルールを設定する

今回はSSHログインすることが目的なので、SSHのインバウンドを全てに設定する。



インスタンスに割り当てられているセキュリティグループを変更する

インスタンスを選択し、「アクション」→「セキュリティ」→「セキュリティグループの変更」をクリックする。



デフォルトのセキュリティグループは削除し、作成したセキュリティグループを追加する。



EC2にログインする

ターミナルを開き、ダウンロードしたキーファイルの場所
に移動する。以下のコマンド
を打つと、yes/no?と聞かれる
るのでyesと打つ。

```
$ ssh -i test-keypair.pem ubuntu@ec2-3-11-10-10.ap-northeast-1.amazonaws.com
The authenticity of host 'ec2-3-11-10-10.ap-northeast-1.amazonaws.com' can't be established.
ECDSA key fingerprint is SHA256:D/7dRLRCptEnfW88.
Are you sure you want to continue connecting (yes/no)?
```

ec2-user

EC2インスタンスを作成した
ときにデフォルトで作成され
るユーザ。

ログインがうまくいかない時

キーファイルの権限の問題で
ログインできない場合があ

る。その場合は、キーファイルの権限を設定し直すことでログインができるようになる。

```
Warning: Permanently added 'ec2-54-92-164-123.compute-1.amazonaws.com' (SSH2-0.9.0).
Connection closed by 'パブリックIP' (192.168.1.100)
```

```
$ chmod 400 test-keypair.pem
$ ssh -i test-keypair.pem ec2-user@ec2-54-92-164-123.compute-1.amazonaws.com
```

```
_ | _ | _ )
_| (      /  Amaz
__|\__|__|
```

```
https://aws.amazon.com/answers/networking/
25 package(s) needed for
Run "sudo yum update" to
```

