設計パターン(Webサイト・ネットワーク/踏み台サーバ)演習1-1

クラス名　　　　No. 氏名

今回の演習ではWebサーバをプライベートサブネット配置して、よりセキュリティを強化した設計パターンを構築する。パブリックサブネットには踏み台サーバを設定して、プライベートサブネットのWebサーバ(EC２)を設定します。

＊設定情報はWebサイト設定シートファイルに入力していくこと。

グラフィカル ユーザー インターフェイス

自動的に生成された説明

■キーペアの作成

1.キーペアがない場合、クラス名-key.pemで作成しておくこと。

■ネットワークの構築

VPC、サブネットなどネットワークの構築を行いなさい。

1.VPCを作成しなさい。

　VPC名：クラス名番号\_vpc CIDR: 10.10.0.0/16

2.次のサブネットを作成しなさい(VPC：クラス名番号\_vpc)。

①パブリックサブネット用・・・サブネット名：public\_sub\_a　AZ：us-east-1a　CIDR：10.10.1.0/24  
②パブリックサブネット用・・・サブネット名：public\_sub\_b　AZ：us-east-1b　CIDR：10.10.3.0/24  
③プライベートサブネット用・・・サブネット名：private\_sub\_a　AZ：us-east-1a　CIDR：10.10.2.0/24

④プライベートサブネット用・・・サブネット名：private\_sub\_b　AZ：us-east-1b　CIDR：10.10.4.0/24

⑤プライベートサブネット用・・・サブネット名：private\_rds\_sub　AZ：us-east-1c　CIDR：10.10.5.0/24

3.インターネットゲートウェイを作成しなさい。

　名前：クラス名番号\_igw　アタッチ：クラス名番号\_vpc

4.NATゲートウェイを作成しなさい。

　名前：クラス名番号\_natgw\_a　サブネット：public\_sub\_a　 EIPの割り当てを行う

名前：クラス名番号\_natgw\_b　サブネット：public\_sub\_b　EIPの割り当てを行う

5.次のルートテーブルを作成しなさい。VPC:クラス名番号\_vpc

　①public\_sub\_a、public\_sub\_b用・・・ルートテーブル名：クラス名番号\_pub\_route

　②pri\_sub\_a用・・・ルートテーブル名：クラス名番号\_pri\_a\_route

　③pri\_sub\_a用・・・ルートテーブル名：クラス名番号\_pri\_b\_route

6.次のようにサブネットのルートテーブルの関連付けを行いなさい。

　①クラス名番号\_pub\_route・・・public\_sub\_a、public\_sub\_ｂ

　②クラス名番号\_pri\_a\_route・・・private\_sub\_a

　③クラス名番号\_pri\_b\_route・・・private\_sub\_b

7.次のセキュリティグループを作成しなさい。

　①踏み台サーバ用(クラス名番号\_bastion)

グループ名：クラス名番号\_bst\_sg　説明：クラス名番号\_bst\_sg 　VPC：クラス名番号\_vpc

タイプ：SSH ソース：0.0.0.0

　②Webサーバ用(クラス名番号\_ websv\_sg)

グループ名：クラス名番号\_websv\_sg 説明：クラス名番号\_websv\_sg VPC：クラス名番号\_vpc

タイプ：SSH ソース：クラス名番号\_bst\_sg、タイプ：HTTP ソース：0.0.0.0)

　③RDS用(クラス名番号\_rds\_sg)

グループ名：クラス名番号\_rds\_sg 説明：クラス名番号\_rds\_sg VPC：クラス名番号\_vpc

タイプ：MySQL/Aurora ソース：10.10.0.0/16)

④ELB用(クラス名番号\_elb\_sg)

グループ名：クラス名番号\_elb\_sg 説明：クラス名番号\_elb\_sg VPC：クラス名番号\_vpc

タイプ：HTTP ソース：0.0.0.0/0)

8.ルートテーブル(クラス名番号\_pub\_route)にルートを追加しなさい。

　送信先：0.0.0.0 ターゲット：インターネットゲートウェイ(クラス名番号\_igw)

■EC２の設定１(踏み台サーバ)

1.次の仕様でインスタンスを起動しなさい。

・キーペア　・・・　クラス名-key.pem

・VPC：クラス名番号\_vpc　サブネット：public\_sub\_a AZ：us-east-1a　名前：クラス名番号\_bastion

パブリックIPの自動割り当て：有効化　 セキュリティグループ：クラス名番号\_bst\_sg

■接続確認

1.Tera termで踏み台サーバ(クラス名番号\_bastion)に接続しなさい。＊パブリックアドレスでアクセスする

2.RDSに接続できるように次のコマンドMySQLのツールをインストールしなさい。

|  |
| --- |
| sudo yum install -y mysql |

3.踏み台サーバから他のサーバ(EC2)に接続するために、キー(クラス名-key.pem)をアップロードしなさい。

設計パターン(Webサイト・Webサーバ)演習1-2

クラス名　　　　No. 氏名

■Webサーバの構築１

1.次の仕様でEC2インスタンスを起動しなさい。

・キーペア　・・・　クラス名-key.pem

・VPC：クラス名番号\_vpc　サブネット：private\_sub\_a AZ：us-east-1a　名前：クラス名番号\_web\_sv1a

パブリックIPの自動割り当て：無効化　 セキュリティグループ：クラス名番号\_websv\_sg

2.ルートテーブル(クラス名番号\_pri\_a\_route)に次のルートを追加しなさい。

　 ルートの追加・・・0.0.0.0 NATゲートウェイ(クラス名番号\_natgw\_a)

3.次のコマンドを使用して作成したインスタンスに接続しなさい(クラス名番号\_bastionから接続する)。

|  |
| --- |
| ssh -i クラス名-key.pem ec2-user@IPアドレス(クラス名番号\_web\_sv1a) |

4.Webサーバ(Apache)とPHPをインストールしなさい。

|  |
| --- |
| sudo yum install -y httpd  sudo amazon-linux-extras install -y php8.0  sudo systemctl start httpd  sudo systemctl enable httpd |

■外部からの設定準備(ELB)

プライベートサブネットへ外部からアクセスするためにELB (ロードバランサー)を設定しなさい。

1.次の仕様に従いロードバランサーを設定しなさい。

　①ターゲットグループを作成しなさい。

　　ターゲットグループ名：クラス名番号-elb-tg VPC：クラス名番号\_vpc

登録ターゲット：クラス名番号\_web\_sv1a

　②ロードバランサー(ALB)を作成しなさい。

　　名前：クラス名番号-elb VPC：クラス名番号\_vpc

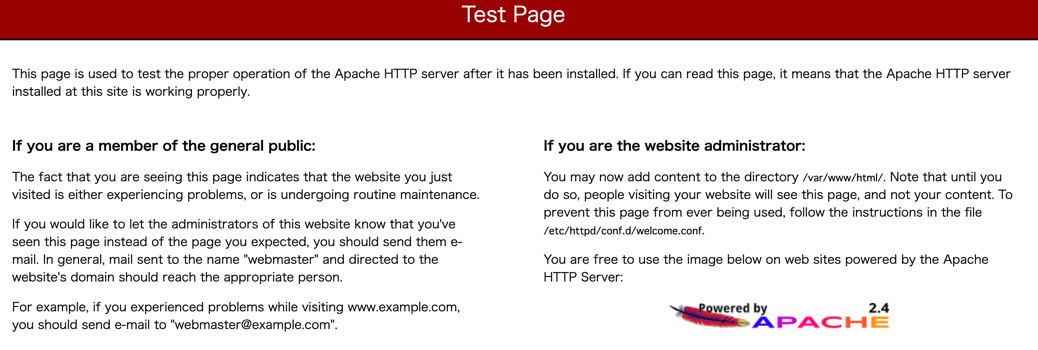
Mapping：us-east-1a(クラス名番号\_pub\_a)、us-east-1b(クラス名番号\_pub\_b)

セキュリティグループ：クラス名番号\_elb\_sg ターゲットグループ：クラス名番号-elb-tg

■接続確認

1.作成したELBのDNS名で接続し次のようなページが表示されるか確認しなさい。

　http://DNS名



■Webページの作成1

1.次のようなWebページを作成し、ドキュメントルートへ移動しなさい(クラス名番号\_web\_sv1aで行う。)。

　①次のコマンドでエディタを開きなさい。

|  |
| --- |
| vi hello.php |

　②作成するページ(hello.php)

|  |
| --- |
| <?php  print ‘<h1>Hello SV1A</h1>’;  ?> |

③ドキュメントルートへファイルを移動させる

|  |
| --- |
| sudo mv hello.php /var/www/html/ |

2.ブラウザで確認しなさい。

　　http://DNS名/hello.php



■AMIの作成

１台のWebサーバが構築できたのでクラス名番号\_web\_1aのAMIを次のように作成しなさい。

イメージ名：クラス名番号\_web\_sv\_ami　説明：クラス名番号\_web\_sv\_ami

■Webサーバの構築２

1.次の仕様でEC2インスタンスを起動しなさい。

・キーペア　・・・　クラス名-key.pem

・VPC：クラス名番号\_vpc　サブネット：private\_sub\_b AZ：us-east-1b　名前：クラス名番号\_web\_sv1b

　イメージ：自分のAMI (クラス名番号\_web\_sv\_ami)

パブリックIPの自動割り当て：無効化　 セキュリティグループ：クラス名番号\_websv\_sg

2.ルートテーブル(クラス名番号\_pri\_b\_route)に次のルートを修正しなさい。

　 ルートの追加・・・0.0.0.0 NATゲートウェイ(クラス名番号\_natgw\_b)

　＊いったん「0.0.0.0」を削除して、追加すること。

3.次のコマンドを使用して作成したインスタンスに接続しなさい(クラス名番号\_bastionから接続する)。

＊いったんexitしておき、クラス名番号\_bastion(10.10.1.0/24)でコマンドを実行すること。

|  |
| --- |
| ssh -i クラス名-key.pem ec2-user@IPアドレス(クラス名番号\_web\_sv1b) |

■Webページの作成2

1.次のようなWebページを作成し、ドキュメントルートへ移動しなさい(クラス名番号\_web\_sv1bで行う。)。

　①作成するページ(hello.php) ＊AMIで作成したのでhello.phpはすでにあるので変更のみ。

|  |
| --- |
| sudo vi /var/www/html/hello.php |

変更箇所(1Aを１Bに変更)

|  |
| --- |
| print ‘<h1>Hello SV1B</h1>’; |

　②変更後保存しなさい。

設計パターン(Webサイト・ロードバランサー/クラウドフロント/RDS)演習1-3

クラス名　　　　No. 氏名

■ELB (ロードバランサー)の設定と確認

1.ターゲットグループ(クラス名番号\_elb\_tg)に「クラス名番号\_web\_sv1b」を追加しなさい。

2.２台のEC2でWebサーバが動作して、交互に「Hello SV1A」、「Hello SV1B」が表示されるか確認しなさい。

　http://DNS名/hello.php



■CloudFrontの設定

1.ディストリビューションの作成を次の仕様に従い設定しなさい。

オリジンドメインの作成：クラス名番号-elb(Elastic LoadBlancer)

料金クラス：北米、欧州、アジア、中東、アフリカを使用

2.CloudFrontに接続できるか確認しなさい。

　http://ディストリビューションドメイン名/hello.php

挿絵, 抽象 が含まれている画像

自動的に生成された説明

　＊表示はSV1AまたはSV1Bのどちらかのみ表示される。

■RDS(Aurora/MySQL)の設定(すでにあればそれを使いますので省略)

1.次の仕様に従いサブネットグループを作成しなさい。

名前：クラス名番号\_rds\_subnet VPC：クラス名番号\_vpc　AZ：us-east-1a〜c

サブネット：10.10.2.0/24,10.10.4.0/24

2.次の仕様に従いデータベースを作成しなさい。

エンジンタイプ：Amazon Aurora (MySQL互換エディション)　テンプレート：開発/テスト

DBクラスター識別子：クラス名番号-aurora-db　　ユーザー名：root パスワード：123qwecc

インスタンスクラス：バースト可能クラス(tクラスを含む)　db.t2.small ＊以前の世代のクラスを含める

可用性と耐久性：Auroraレプリカを作成しない。

　 VPC：クラス名番号\_vpc　DBサブネットグループ：クラス名番号\_rds\_subnet

セキュリティグループ：クラス名番号\_rds\_sg 拡張モニタリングの有効化：チェックをはずす

■接続確認

1.踏み台用のサーバ(クラス名番号\_bastion)から次のコマンドを使用して、データベースにアクセスしなさい。

|  |
| --- |
| mysql -u root -p -h ライターインスタンスのエンドポイント |

2.データベースの作成とテーブルの作成をしなさい。テーブルの作成、データの追加は、DB.txtを使用すること。

|  |
| --- |
| create database クラス名\_db;　　・・・　すでにある場合は不要  use クラス名\_db;  show tables;  ＊もし「shohins」がある場合、次のコマンドを実行していったんテーブルを削除する。  drop table shohins; |

3.データが挿入されたか確認しなさい。

|  |
| --- |
| select \* from shohins; |

■Webページのアップロード

1.part1-db.phpファイルの「データベース名」、「エンドポイント」を変更してTera termで「クラス名番号\_bastion」にアップロードしなさい。

2.次のコマンドを使用して「クラス名番号\_web\_sv1a」と「クラス名番号\_web\_sv1b」にアップロードしなさい。

|  |
| --- |
| scp -i ｸﾗｽ名-key.pem part-db.php ec2-user@ｸﾗｽ名番号\_web\_1aのIPｱﾄﾞﾚｽ:/home/ec2-user/ ・・・　クラス名番号\_web\_1aへのアップロード  scp -i ｸﾗｽ名-key.pem part-db.php ec2-user@ｸﾗｽ名番号\_web\_1bのIPｱﾄﾞﾚｽ:/home/ec2-user/　　　　　・・・　クラス名番号\_web\_1aへのアップロード |

3.各サーバのドキュメントルートへpart-db.phpを次のコマンドを利用して移動させなさい。

・クラス名番号\_web\_sv1a

|  |
| --- |
| ssh -i クラス名-key ec2-user@クラス名番号\_web\_sv1aのIPアドレス  sudo mv part-db.php /var/www/html/  sudo chmod 644 /var/www/html/part-db.php |

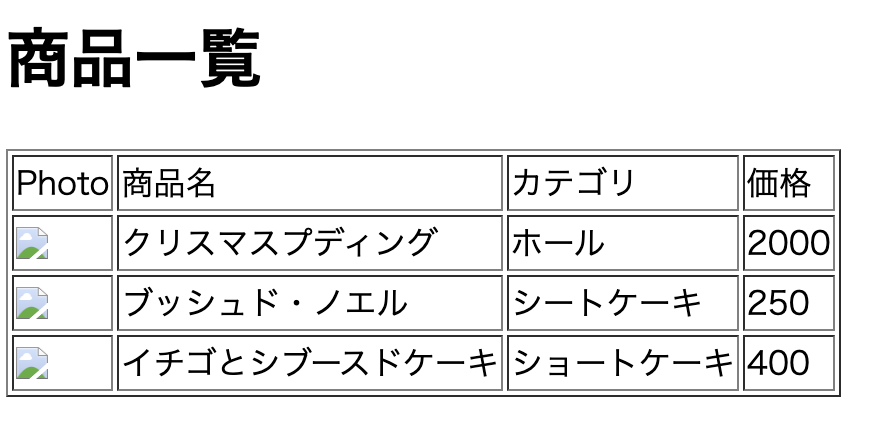
・クラス名番号\_web\_sv1b

|  |
| --- |
| ssh -i クラス名-key ec2-user@クラス名番号\_web\_sv1bのIPアドレス  sudo mv part-db.php /var/www/html/  sudo chmod 644 /var/www/html/part-db.php |

■確認

1.次のURLでアクセスし、下のような表示されるか確認しなさい。

　http://ディストリビューションドメイン名/part-db.php

 ＊この段階ではイメージファイルは表示されません。

■提出

part-db.phpを番号名前\_part-db.phpに変更してsv23へ提出しなさい。

また設定シート\_web\_siteを番号名前\_設定シート\_web\_siteで提出しなさい。