Université de Tunis El Manar

Faculté des Sciences de Tunis
Département informatique

Rapport de Project cloud fin de semestre

Elaboré par :

Ben Kedim Mohamed

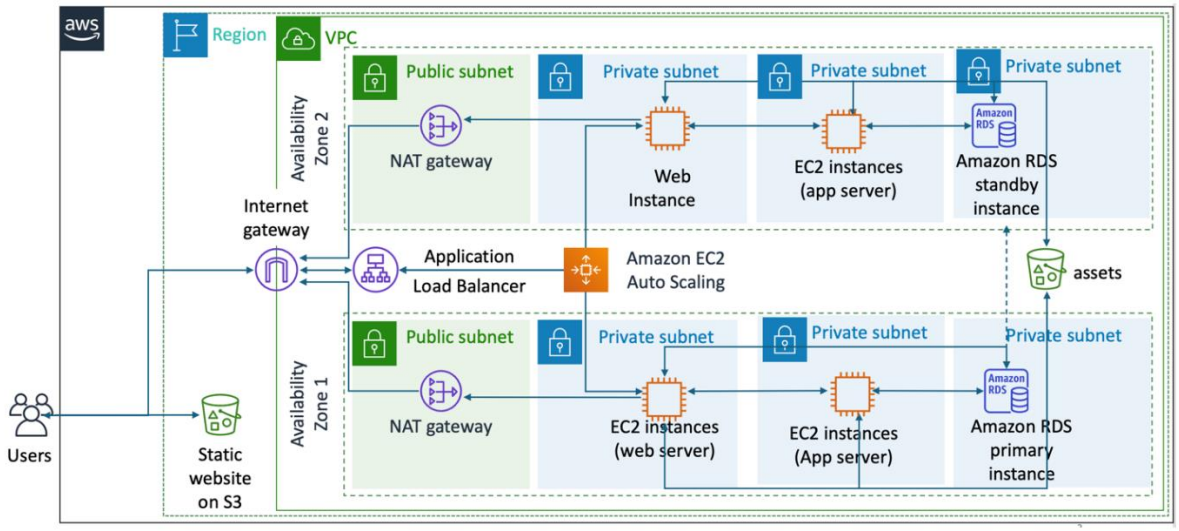
Sujet : Déploiement d'une application à 3 niveaux

Classe : IGL4

Table de matières

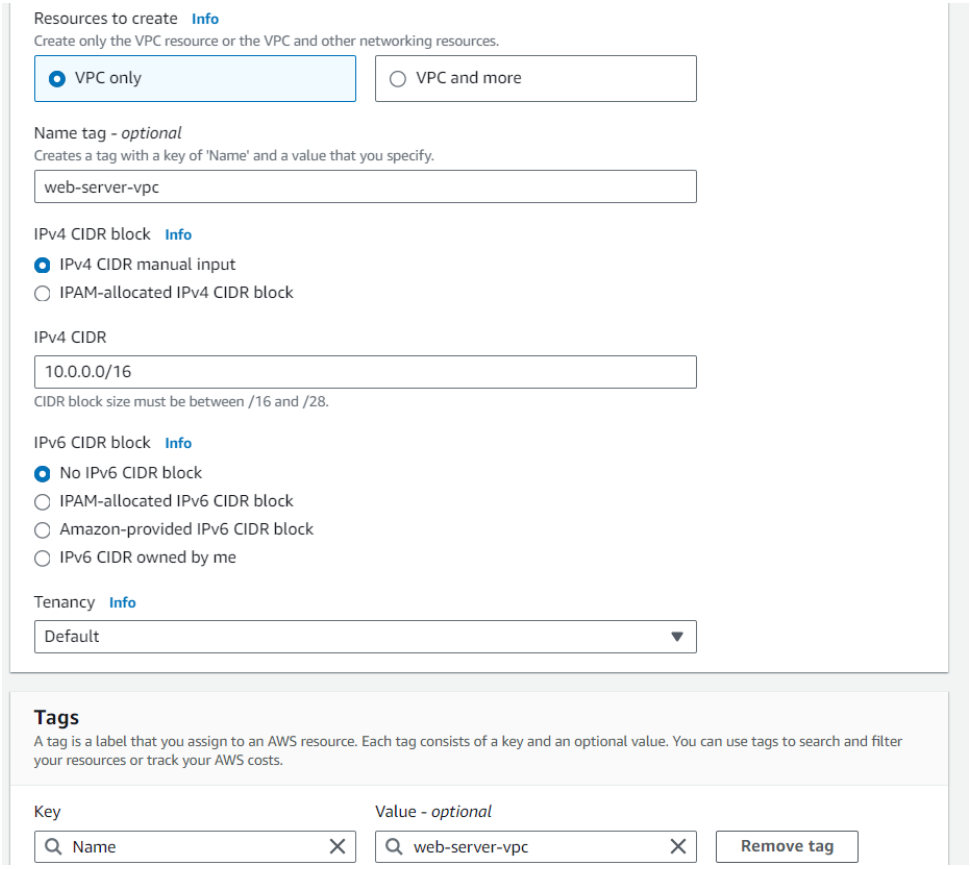
1- **Architecture à mettre en place**
2- **Etape 1 : Création du VPC (virtual private cloud)**
3- **Etape2 : Création des 6 sous-réseaux (2publiques, 4privés)**
    a. Réseaux Publiques
    b. Réseaux Privés
4- **Etape 3 : Création des Route tables**
    a. Création
    b. Ajouter des associations
5- **Etape 4 : Création des Internet Gateway**
6- **Etape 5 : Création des NAT Gateway**
7- **Etape 6 : Création des Security groups**
    a. Création du security group pour le SSH accessing
    b. Création du security group pour l'accès au base de données
    c. Création du security group pour l'accès au base de donnée
    d. Création du security group pour les instances EC2 privés
8- **Etape 7 : Création du machine Bastion**
9- **Etape 8 : Création de deux machine EC2**
    a. Machine EC2 1 : WebServer1
    b. Machine EC2 2 : Backend
10- **Etape 9 : Modification de quelques propriétés des machines EC2**
11- **Etape 10 : Création de l'Application load balancer**
12- **Etape 11 : création du target Group**
13- **Etape 12 : ouverture de session dans la machine Bastion**
14- **Etape 13 : Connection et déploiement du partie front dans la machine EC2 (WebServer1)**
15- **Etape 14 : Connection et déploiement du partie backend dans la machine EC2 (BackEndServer)**
16- **Etape 15 : Création et connexion avec le service RDS**
    a. Création d'un subnet Group
    b. Création de la base de donnés
    c. Installation de mysql dans la machine EC2 du backend et création de la base de données
    d. Connexion du base de données avec le backend
17- **Etape 16 : création de l'Auto Scaling Group**
    a. Création d'une Template
    b. Création de l'autoscaling group
18- **Etape 17 : Création de S3 et déploiement du site web statique**
    a. Upload du fichier statique
    b. Modification des permissions
19- **Teste de site web**
20- **Teste de site web statique**

Architecture à mettre en place :



Etape 1 : Création du VPC (virtual private cloud)

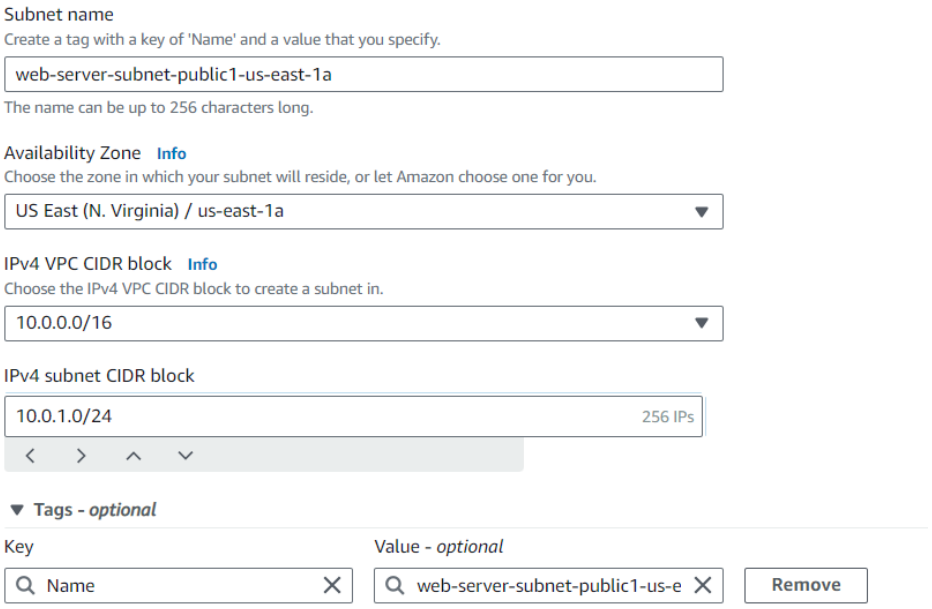
Comme il est bien montré dans l'architecture le VPC est étendu sur deux AV, et contiendra plusieurs sous-réseaux (subnets).



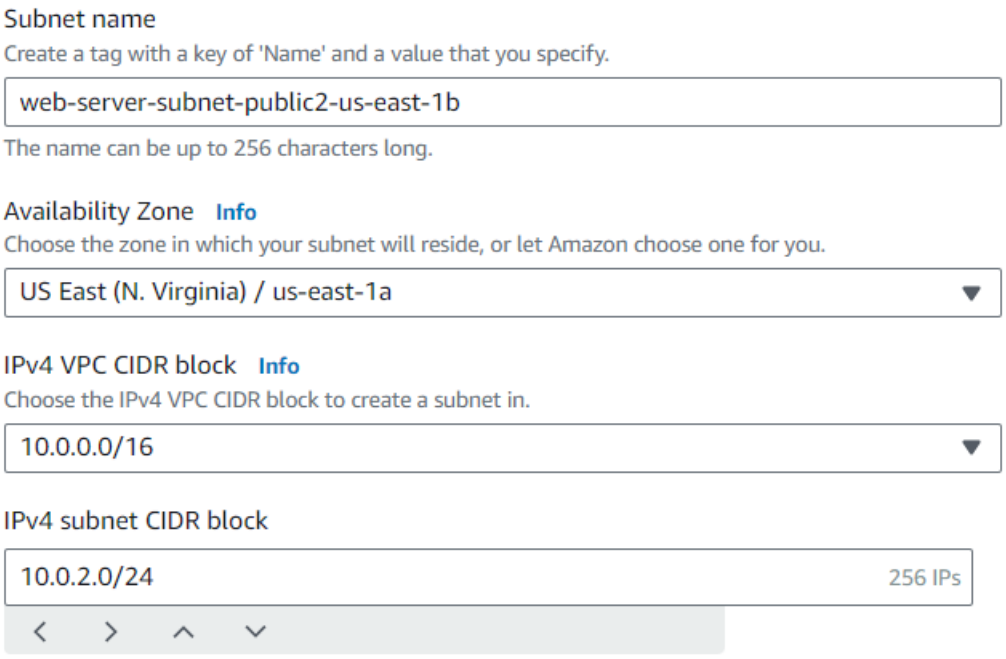
Etape2 : Création des 6 sous-réseaux (2publiques, 4privés) :

Réseaux Publiques :

Réseau publique 1 :

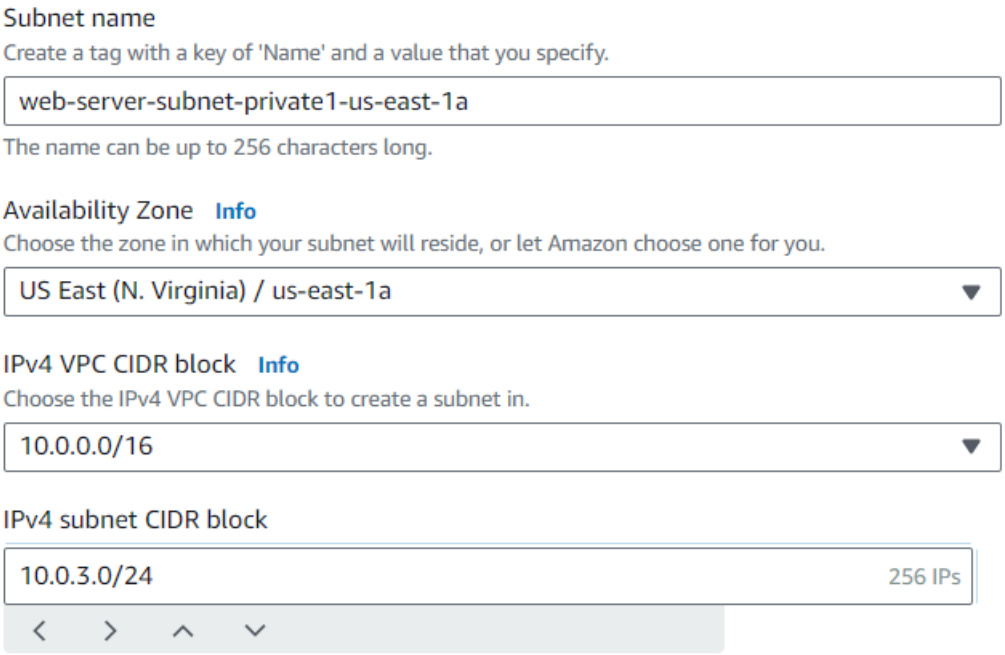


Réseau publique 2 :

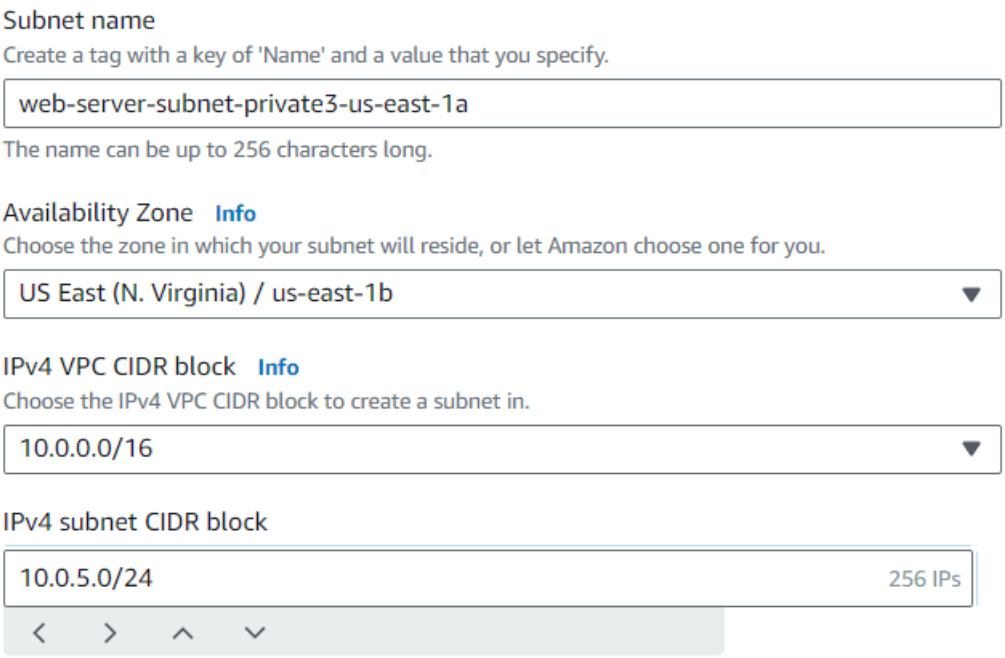


Réseaux Privés :

Réseau privé 1 :



Réseau privé 3 :



De même on crée 4 autre sous-réseaux suivant le tableau d'adressage ci-dessous :

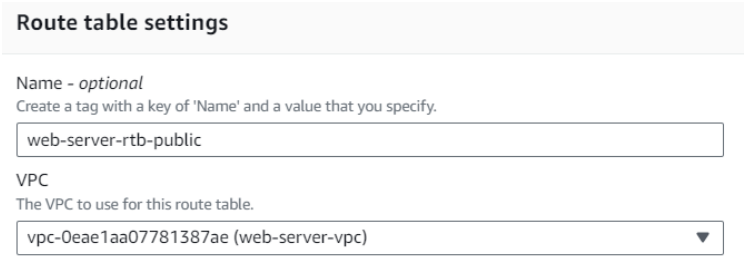
Type réseau	Subnet Name	A.V	IPv4 subnet
Publique	web-server-subnet-public1-us-east-1a	Us-east-1a	10.0.1.0/24
Publique	web-server-subnet-public1-us-east-1b	Us-east-1b	10.0.2.0/24
Privé	web-server-subnet-private1-us-east-1a	Us-east-1a	10.0.3.0/24
Privé	web-server-subnet-private2-us-east-1a	Us-east-1a	10.0.4.0/24
Privé	web-server-subnet-private3-us-east-1a	Us-east-1a	10.0.5.0/24
Privé	web-server-subnet-private4-us-east-1a	Us-east-1b	10.0.6.0/24
Privé	web-server-subnet-private5-us-east-1a	Us-east-1b	10.0.7.0/24
Privé	web-server-subnet-private6-us-east-1a	Us-east-1b	10.0.8.0/24

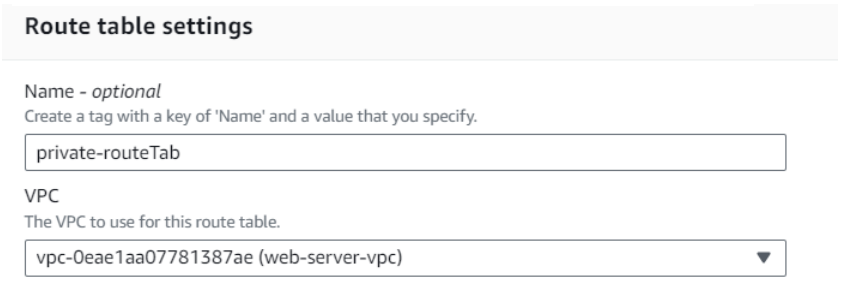
Remarque : tout réseau crée est pris comme réseau publique, donc pour les réseaux privés il faut sélectionner le réseau et modifier le paramètre « **Auto-assign public IPv4 adress** » et le rendre No.

Etape 3 : Création des Route tables

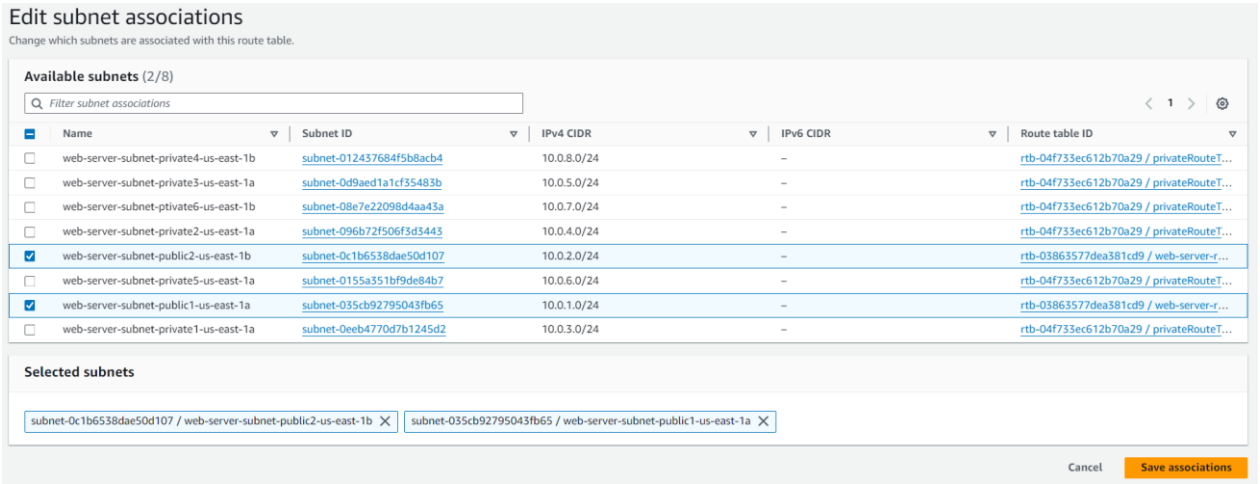
Création :

2 tables de routage vont être crée : une pour les subnets publiques et l'autre pour ceux qui sont privés





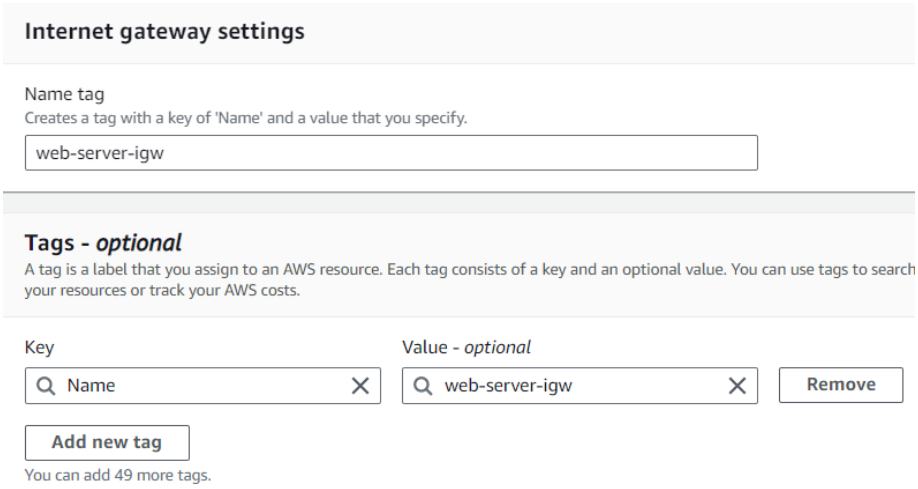
Ajouter des associations :



Les associations explicites on les supprime et après on choisit exactement les subnets qui doivent êtres incluent

Name	Route table ID	Explicit subnet associati...
web-server-rtb-public	rtb-03863577dea381cd9	2 subnets
privateRouteTable	rtb-04f733ec612b70a29	6 subnets

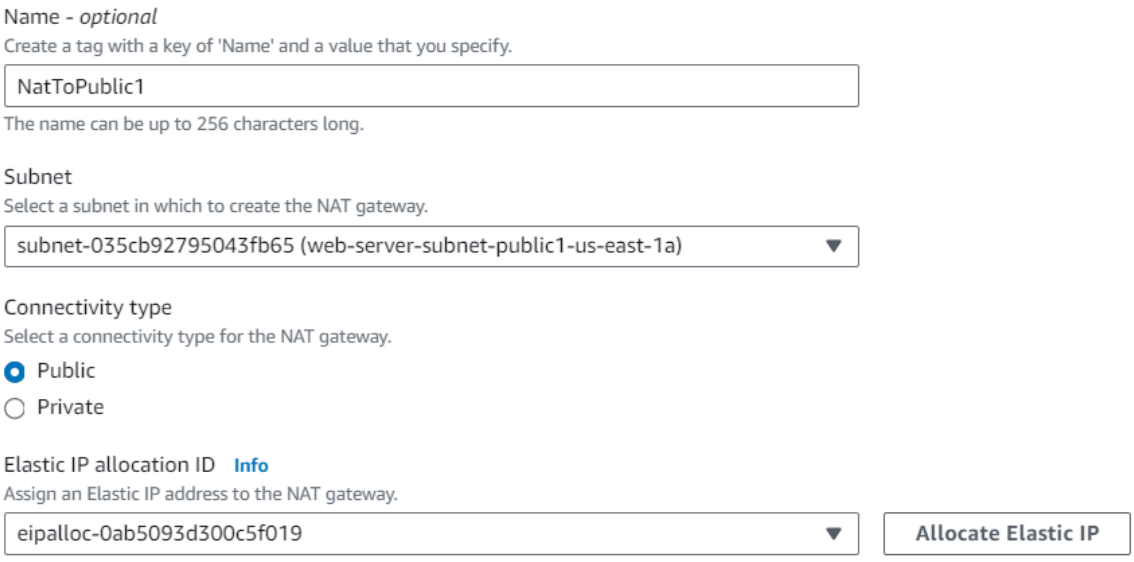
Etape 4 : Création des Internet Gateway :



Après la création du VPC on doit l'attacher à un VPC.

Etape 5 : Création des NAT Gateway :

On Devra crée deux Nat gateway chacun dans un réseau public en lui allouant une adresse up élastique :



Name	NAT gateway ID	Connectivity...	State
NatToPublic1	nat-0e2b15075c77d65d5	Public	Available
NatToPublic2	nat-0bb6c22b36fdc34a8	Public	Available

Etape 6 : Création des Security groups

1- Création du security group pour le SSH accessing

sg-07566aa15e1b5bc7d - SSH-accessing

Details | Inbound rules | Outbound rules | Tags

Inbound rules (1)

Manage tags | Edit inbound rules

Search

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
–	sgr-02b42d7fdd3103be5	IPv4	SSH	TCP	22	0.0.0.0/0

2- Création du security group pour l'accès au base de données

Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-0336bf20599341b0c	MYSQL/Aurora	TCP	3306	Custom	sg-04cfda9230cbd94d7		Delete
sgr-05ea0dc2d941d8fdc	All traffic	All	All	Custom	sg-04cfda9230cbd94d7		Delete
sgr-0962940b1f7baeebe	Custom TCP	TCP	0	Custom	sg-0a44b71ae4b2743c3		Delete
sgr-0c6f8d40eb85ead34	MYSQL/Aurora	TCP	3306	Custom	0.0.0.0/0		Delete

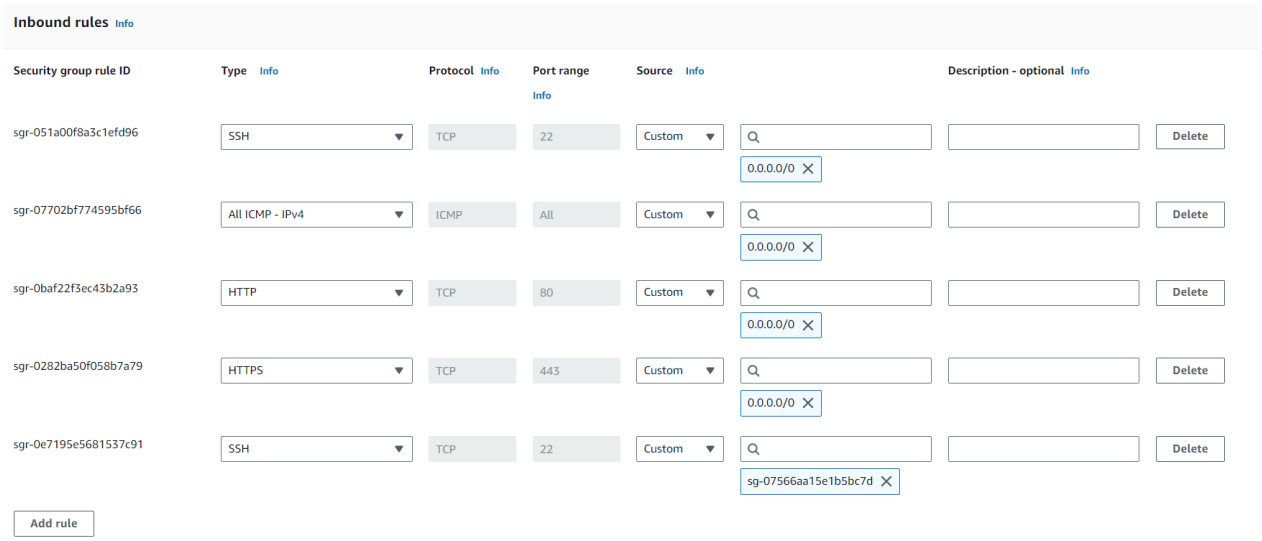
3- Création du security group pour l'accès au base de données

Inbound rules Info

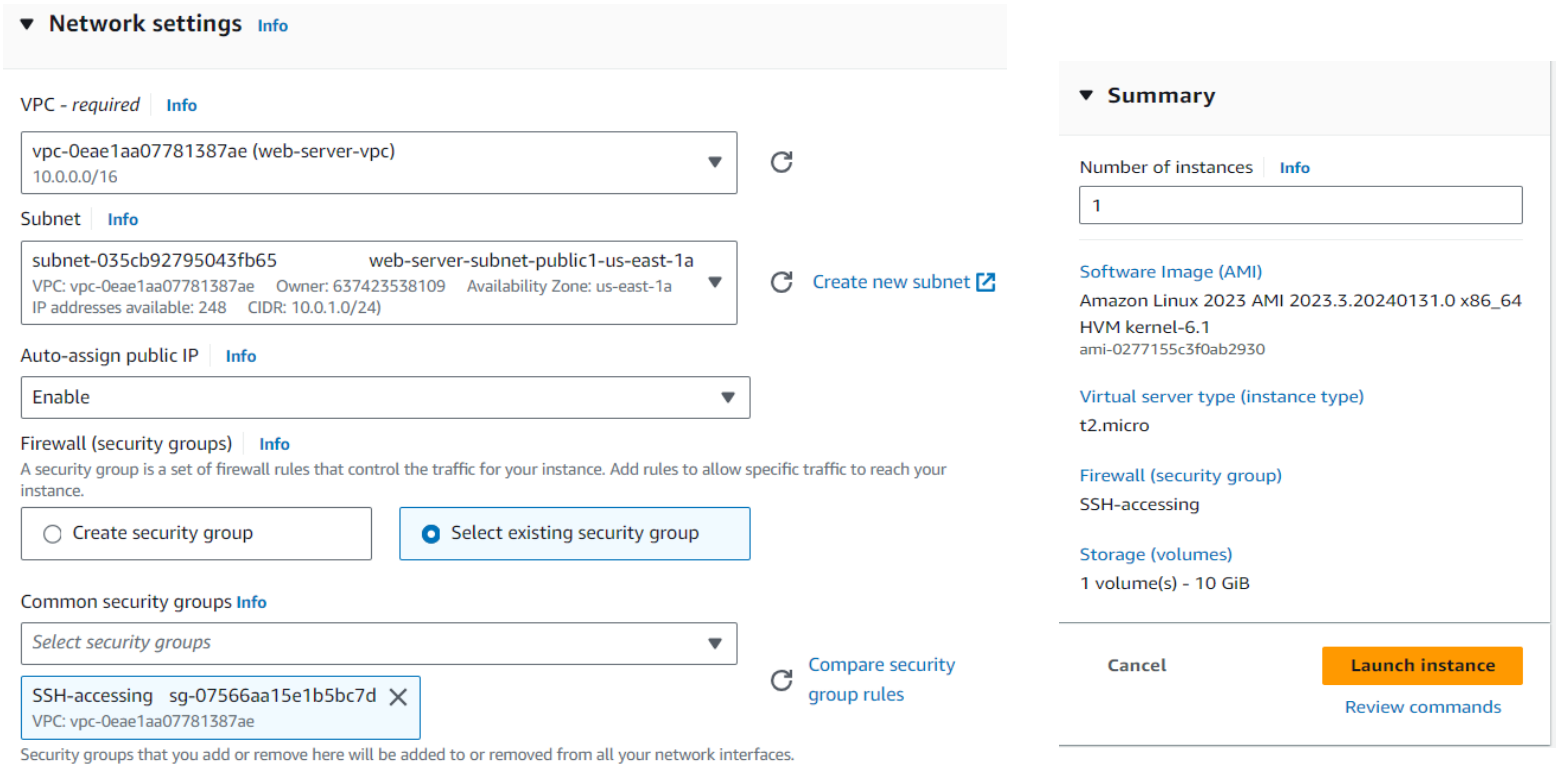
Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-0aaa04804cfbefd62	HTTPS	TCP	443	Custom	0.0.0.0/0		Delete
sgr-01bdc2fcd0acd9448	HTTP	TCP	80	Custom	0.0.0.0/0		Delete

Add rule

4- Création du security group pour les instances EC2 privés



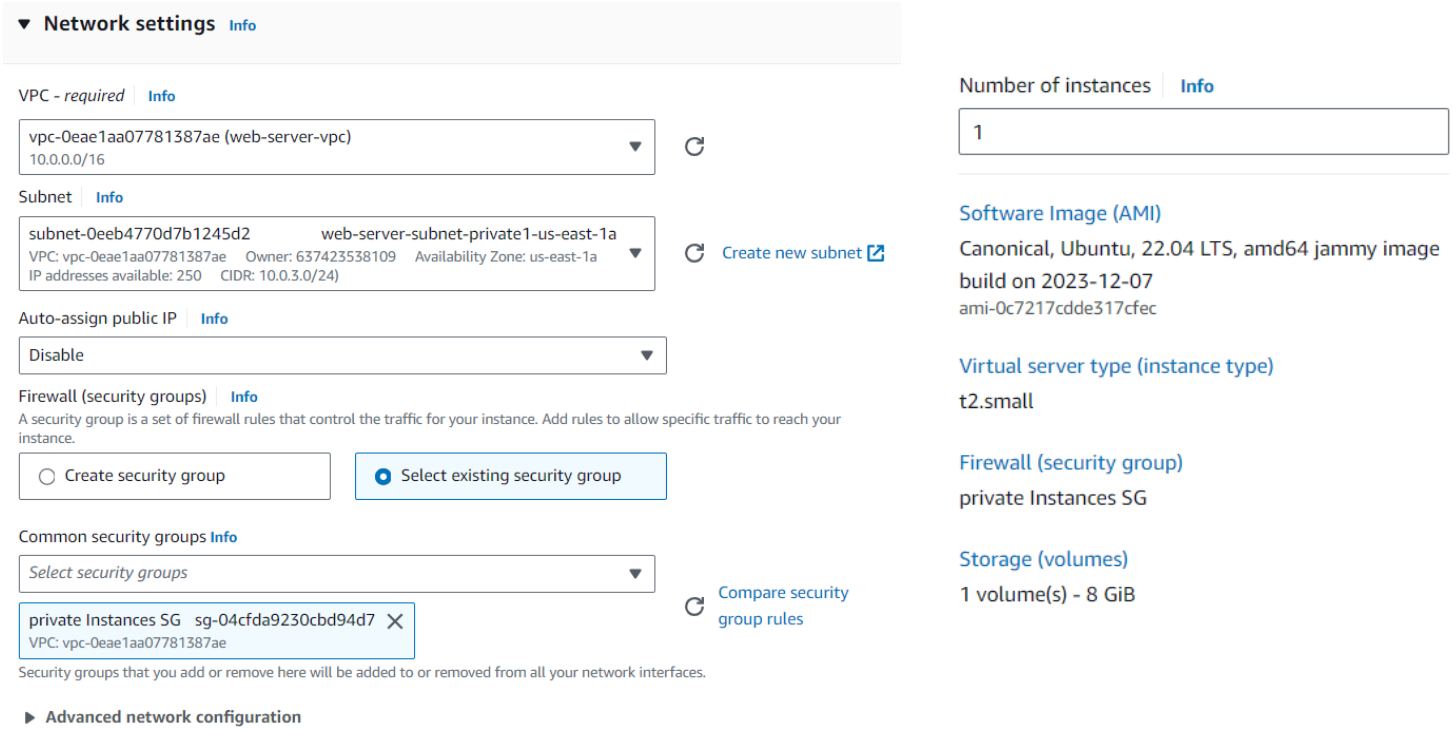
Etape 7 : Création du machine Bastion :



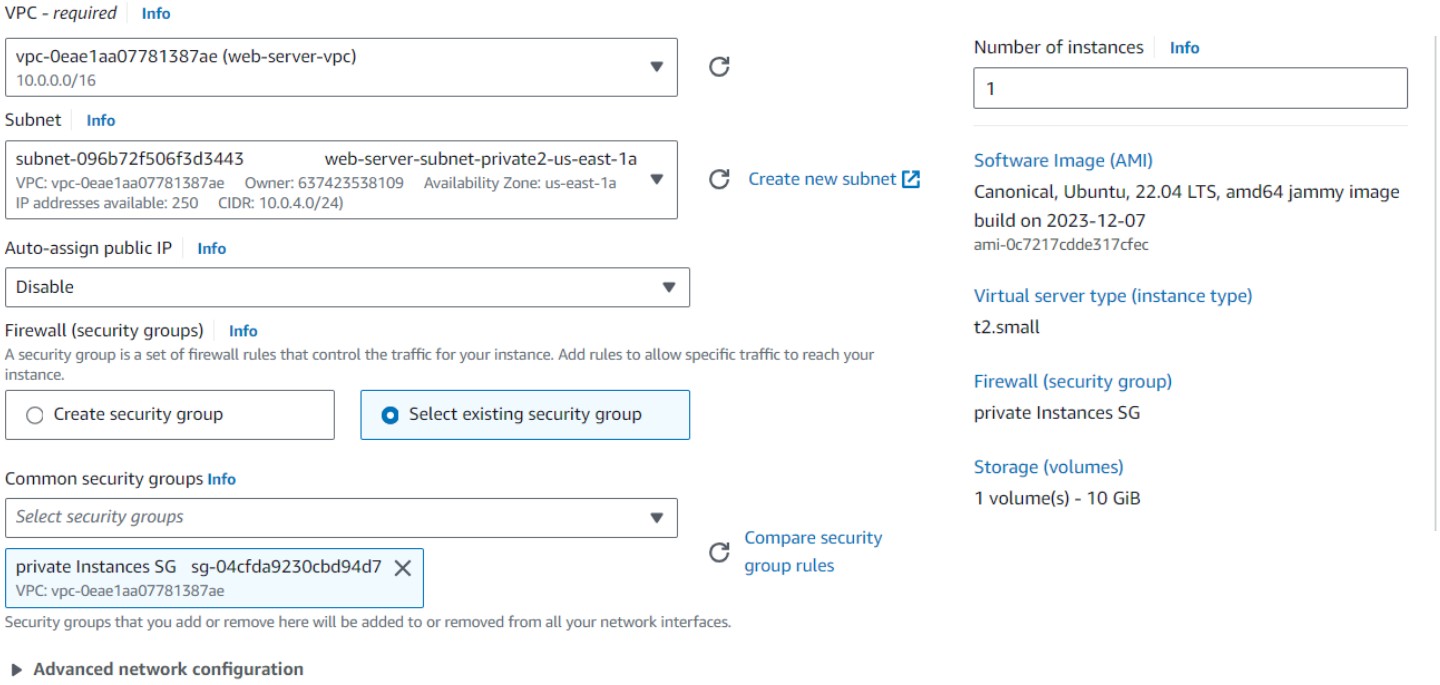
Cette machine doit être crée dans un sous réseau publique et aura un accès SSH.

Etape 8 : Création de deux machine EC2 :

Machine EC2 1 : WebServer1 : Hosting de front end de l'application :

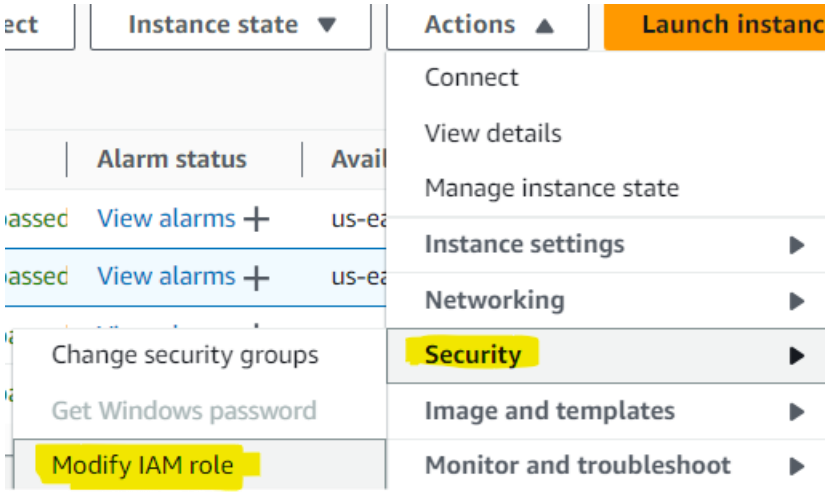


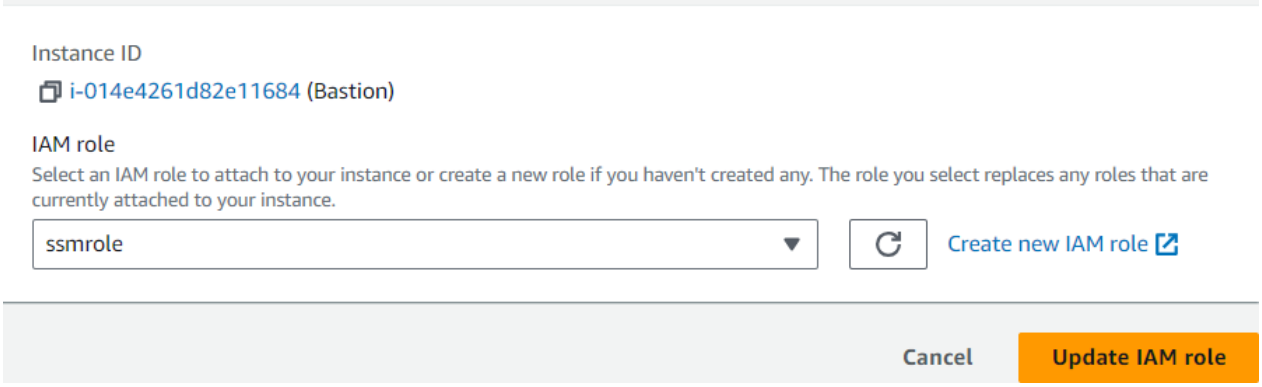
Machine EC2 2 : Backend : Hosting de Backend end de l'application :



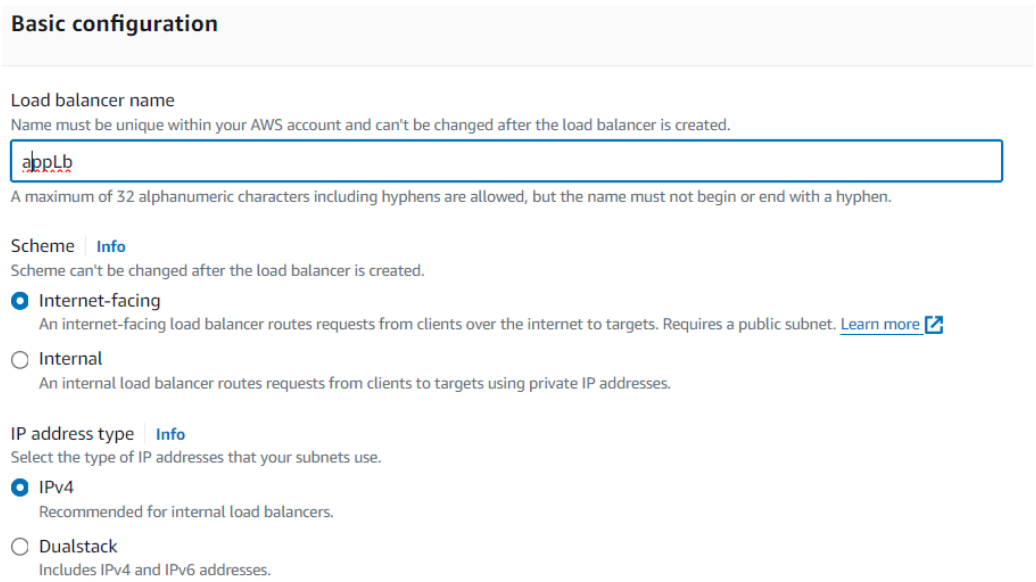
Etape 9 : Modification de quelques propriétés des machines EC2

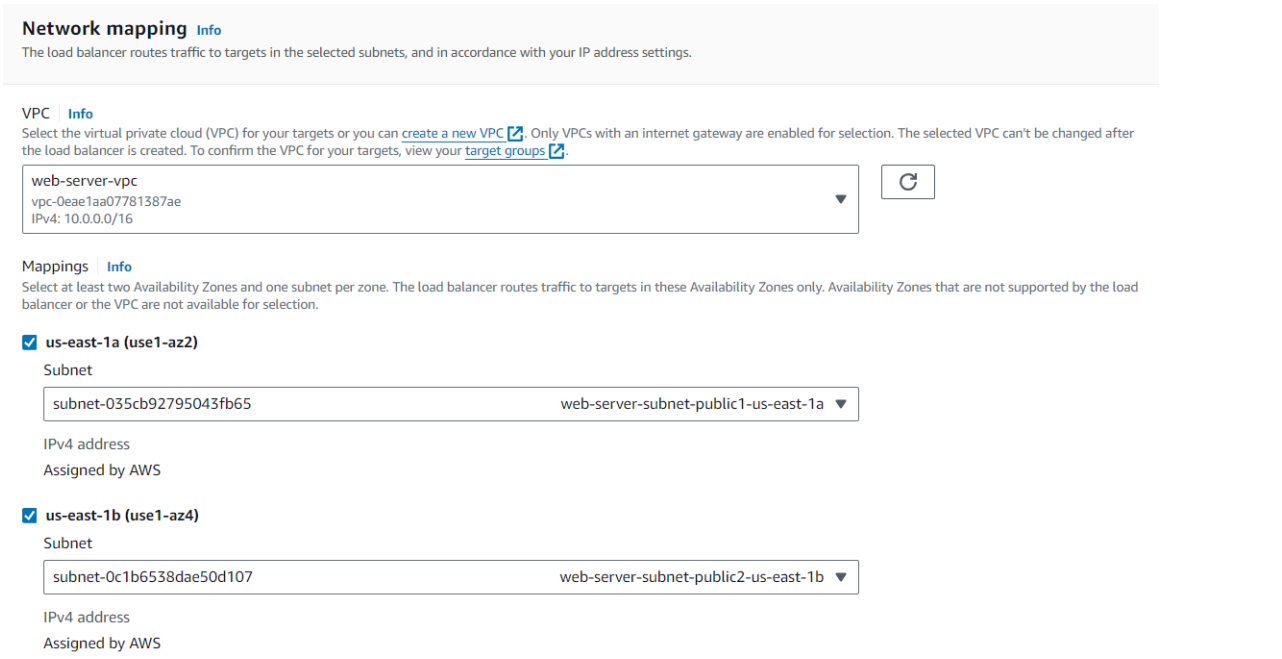
Pour la machine bastion il nous faut des privilèges pour ajouter un profile SSM

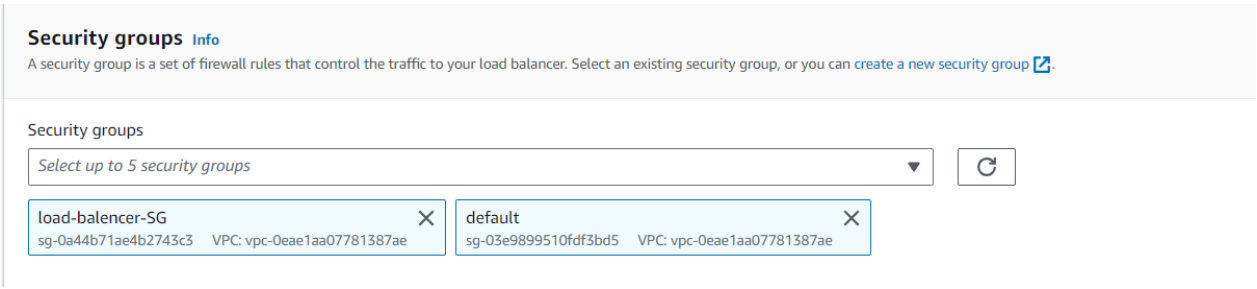




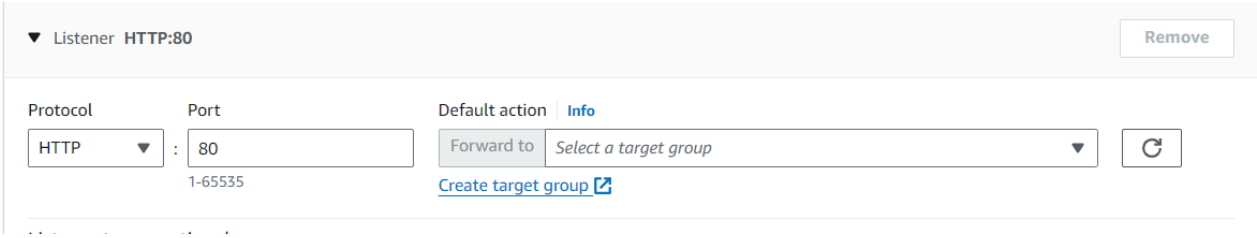
Etape 10 : Création de l'Application load balancer :







Il faut crée un Target group (expliqué dans la prochaine étape)



Etape 11 : création du target Group :

Basic configuration

Settings in this section can't be changed after the target group is created.

Choose a target type

- (•) Instances
  - Supports load balancing to instances within a specific VPC.
  - Facilitates the use of Amazon EC2 Auto Scaling to manage and scale your EC2 capacity.
- ( ) IP addresses
  - Supports load balancing to VPC and on-premises resources.
  - Facilitates routing to multiple IP addresses and network interfaces on the same instance.
  - Offers flexibility with microservice based architectures, simplifying inter-application communication.
  - Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.
- ( ) Lambda function
  - Facilitates routing to a single Lambda function.
  - Accessible to Application Load Balancers only.
- ( ) Application Load Balancer
  - Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
  - Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation

HTTP | 80

1-65535

IP address type

Only targets with the indicated IP address type can be registered to this target group.

- (•) IPv4
  Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.
- ( ) IPv6
  Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). Learn more

VPC

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

web-server-vpc
vpc-0eae1aa07781387ae
IPv4: 10.0.0.0/16

Protocol version

- (•) HTTP1
  Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

Sélection des instances EC2 front et backend :

Available instances (2/4)

Filter instances

1

Instance ID	Name	State	Security groups	Zone
i-02486622418367329	WebServer1	Running	private Instances SG	us-east-1a
i-014e4261d82e11684	Bastion	Running	SSH-accessing	us-east-1a
i-045a53cce42e71446	BackEndServer	Running	ec2-rds-1, private Instances SG	us-east-1a

Etape 12 : ouverture de session dans la machine Bastion :

1- On utilise le bastionkey déjà téléchargé dans notre machine :
user name : ec2-user
adresse ip publique : 44.201.236.127

```
MSI@Bnk-Msi MINGW64 ~/Downloads
$ ssh -A -i "bastionkey.pem" ec2-user@44.201.236.127
The authenticity of host '44.201.236.127 (44.201.236.127)' can't be established.
ED25519 key fingerprint is SHA256:sqFLugJOz7KkzIqgyLTSkTf5CVOjTLdYFjvhV/35g34.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:2: 54.164.111.204
    ~/.ssh/known_hosts:4: 18.234.164.201
    ~/.ssh/known_hosts:5: 3.89.111.183
    ~/.ssh/known_hosts:6: 3.86.146.143
    ~/.ssh/known_hosts:7: 44.205.251.112
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '44.201.236.127' (ED25519) to the list of known hosts.

A newer release of "Amazon Linux" is available.
  Version 2023.3.20240131:
Run "/usr/bin/dnf check-release-update" for full release and version update info
       #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Thu Feb  1 20:30:57 2024 from 196.176.79.63
[ec2-user@ip-10-0-1-175 ~]$
```

2- Copie du key qui sera utilisé dans la connexion au deux machine du front et de backend dans la machine bastion utilisant le même nom de la configuration déjà faite au cours de la création.

```
 GNU nano 5.8                                WebServer1Key.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAlMjdzD313GJOQneRcaZEAiAdTcmx6Xow71kAn7eVkZit/ohf
R6DVqceeJxKg/iuxsv/nwUmL2GbmUk/A5kONmafC3E7lNQZRPLpMkgQEDfOLSfrM
9KOIAGfvyHy/FBJLQEnNU7Hn751rcyLIMTGdNWOnr+cmUTd3KnTi38uuy+R9yfya
DZ+8PxavDCwKiN8fY51le1IFGCjpe+TCvrVbqY9AfIKyz9Tp3hvIc5+CAIf/C+dK
YDIHlT2xCjarq7LQKhwoER5L+N+gxcJw8QES5zuZWegJOuu1Bu6ipmTuiO0eY/ag
/WFDhDpH+a+BWWlrXgsksA4hbvNUMpsJmj5bEQIDAQABAoIBADcZ2MJ+I+KVaaRG
AdBUIhWjbRbU3pW4Eg1iKc/8vmCoaa+9M4QkdVymN9UCmirnZaOEBwFXSno/SYcs
UCU6XhIMxiau9UXY7BcQa7Eb2aCQmTCxuFvZBQCZfXODbgRx7fqGGoundFOSMKv4
Mqm9VRpnLW6ArXkgkHphxW/aUAbkK5a8h5P9oq9Cvu2BINUoDq9RJht7AvyqXCrg
KSgjRHffILWwmrAPfTCEpgmXoOFbqpFCPfywXm3iu3VYqaNl1/PoTOtAsw0vFzKO
E+LyBabfT5+D+lkGZKcDAuEwLhVa1zwU+UgSUamC+e/rpNLs19aDEnyI4wIp+Hsr
Kmc+xxOCgYEA2k4zTT1I1uwJioLyvyI4JnQlYKFEprBIJeZlqrGW8JfodpxtaEwI
sJOFBrrNRnyCV5sl9ZOyFqKO3phKliOWB/Zmu+e9kVV03/S/7sWlSIAlHbYXqVbY
z0lJrHeZZTw7wu/doEZeU0/zS1+6Es9ISEgCpWnFgLR2omt7f9E1N38CgYEArnmf
caladtxgSYYRylPQwMQDvPPx+3vJwvLZecgng699VJwBf/aALFbAf4Xb4ObWI1fw
VBZf4XCWNApzBPCSCR/4rqXGou270Vkk88GBDzdULlavDmZ/SaHtzeZHqEBEwNZo
ypLhNcGz8Dg6uLGJ5eKlegP05/Slhx87EmdSNW8CgYBBezdOMa/Jl998xq6dmlwR
XMFhbL406aeahrN0MfS+kjJOcbl3kWcB4B4E2L9+JxbJxGXseIxvsbpjEnc89cuo
88X5ExgPofx+uOFhc7OSPa3kbZxHVR+PfcI1k2JVtW2PmXd2/eSJRPALadlcjwR1
efQhPcraQkdbjLXsrwoxbQKBgHSGA6eMXD+PtLrFOHHZAkOLXBfAsDatmLUbLYU4
2LMI6+IrApFslnOGSK+iPZP5dsBKBdaSztwoLhh5dhGxfUac1KAHVR8ROON67sPg
OwnPgOglumoaqB4MCF7/OZGbwo8rYvcPm1skj8D6PLWG1Lr0YGGZ7OFRMY+JmxES
cgP/AoGBAIWrrCLIyCjyMHVI+oGe5rwQhEoKKNvZBvZ/qbhGJtdcH/hlEh5Dz4W+
fImR2K1Cf5oYLySvz7x3Xro3xiAgPwscH/8nci4SKKncZ3NuogRt/Qevqhm+MVYx
csDO7stxeUzK5WLjH8RwlWorRbEcJNNrDxvb8LvFjR1zka2YJcV6
-----END RSA PRIVATE KEY-----
```

Etape 13 : Connection et déploiement du partie front dans la machine EC2 (WebServer1) :

On installe apache avec les suites de commandes suivantes :
>>sudo apt update
>>sudo apt install apache2
>>sudo systemctl start apache2
>>sudo systemctl enable apache2

Déploiement du frontEnd :

>>cd /var/www/html
>>nano index.html //on ecrit le code html-js-css du front

```
 GNU nano 6.2                                        index.html
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>User Information Form</title>
    <style>
            body {
            font-family: Arial, sans-serif;
            background-color: #f4f4f4;
            margin: 0;
            padding: 0;
            display: flex;
            align-items: center;
            justify-content: center;
            height: 100vh;
        }

        .container {
            background-color: #fff;
            padding: 20px;
            border-radius: 8px;
            box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
            width: 300px;
            text-align: center;
        }

        input {
            width: 100%;
            padding: 10px;
            margin: 8px 0;
            box-sizing: border-box;
        }

        button {
            background-color: #4caf50;
            color: #fff;
            padding: 10px;
            border: none;
            border-radius: 4px;
            cursor: pointer;
```

Faire la connexion avec la partie backend :
on utilisera le lien de notre elastic load balancer pour pouvoir accéder à la ressource de backend.

```
// Create an AJAX request
var xhr = new XMLHttpRequest();
xhr.open("POST", "http://appLb-609149057.us-east-1.elb.amazonaws.com/backend.php", true);
xhr.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
```

Etape 14 : Connection et déploiement du partie backend dans la machine EC2 (BackEndServer) :

Etablir la connexion SSH avec la machine et installation de Apache de même que dans la machine webserver1

```
[ec2-user@ip-10-0-1-175 ~]$ ssh -i WebServer1Key.pem ubuntu@10.0.4.58
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1052-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Feb  2 21:42:03 UTC 2024

  System load:  0.0               Processes:             105
  Usage of /:   20.3% of 11.45GB  Users logged in:       0
  Memory usage: 21%               IPv4 address for eth0: 10.0.4.58
  Swap usage:   0%

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

26 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


Last login: Thu Feb  1 16:30:33 2024 from 10.0.1.175
```

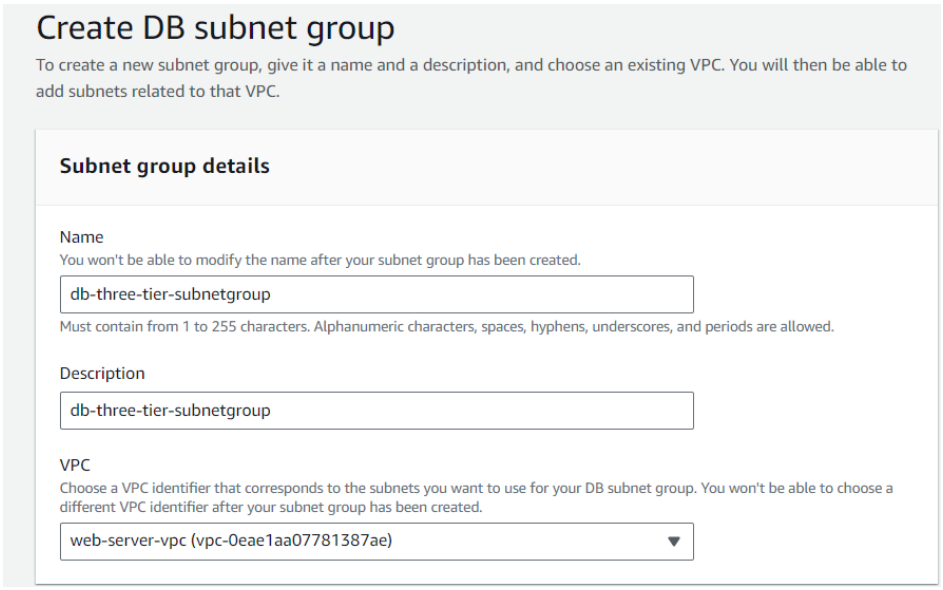
Création et déploiement de la partie backend php

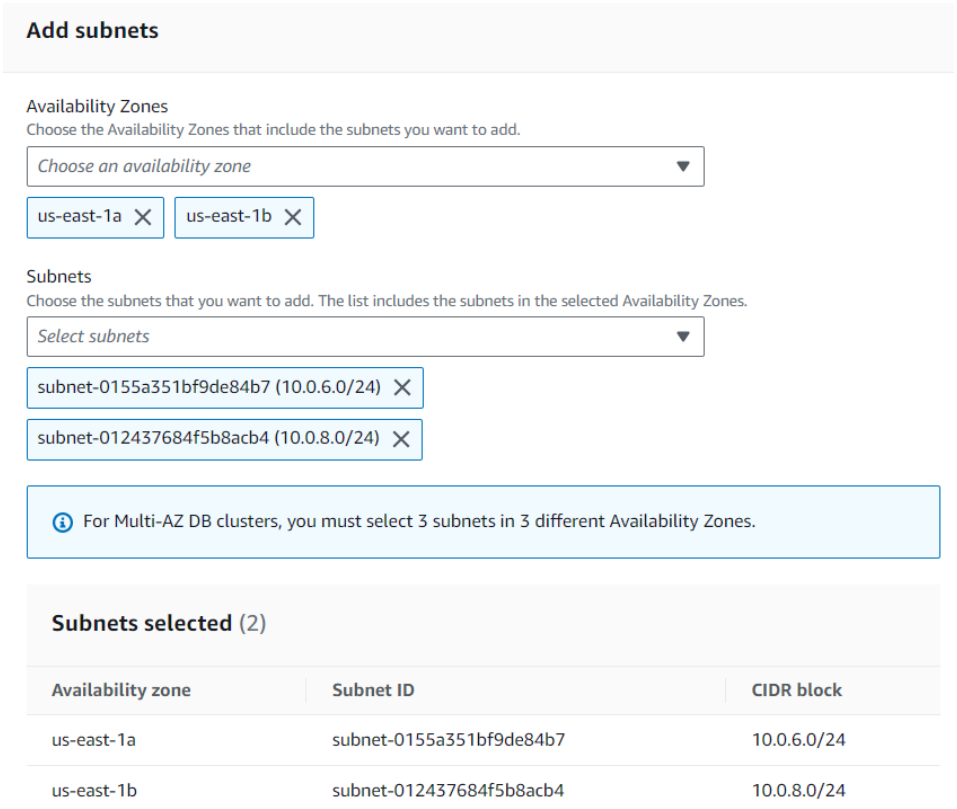
```php
<?php

define('DB_SERVER', 'rdsphpdb.cnq4000ie48g.us-east-1.rds.amazonaws.com');
define('DB_USERNAME', 'admin');
define('DB_PASSWORD', 'adminadmin');
define('DB_DATABASE', 'student');

// Allow requests from any origin
header("Access-Control-Allow-Origin: *");

// Allow requests with methods POST
header("Access-Control-Allow-Methods: POST");

// Retrieve user inputs from the POST request
$name = $_POST['name'];
$cin = $_POST['cin'];
$university = $_POST['university'];

// Create a PDO connection
try {
    $pdo = new PDO("mysql:host=" . DB_SERVER . ";dbname=" . DB_DATABASE, DB_USERNAME, DB_PASSWORD);
    $pdo->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);

    // Prepare and execute the SQL query to insert data
    $stmt = $pdo->prepare("INSERT INTO studentT (name, cin, university) VALUES (:name, :cin, :university)");
    $stmt->bindParam(':name', $name);
    $stmt->bindParam(':cin', $cin);
    $stmt->bindParam(':university', $university);
    $stmt->execute();

    // Print the inserted data
    $response = "Inserted data: Name - $name, CIN - $cin, University - $university";
    echo $response;
} catch (PDOException $e) {
    // Handle database connection or query errors
    $response = "Error: " . $e->getMessage();
    echo $response;
}

 // Fetch all data from the studentT table
    $stmt = $pdo->query("SELECT * FROM studentT");
    $data = $stmt->fetchAll(PDO::FETCH_ASSOC);

    // Print the inserted data in an HTML table
        echo '<style>
            table {
                font-family: Arial, sans-serif;
                border-collapse: collapse;
                width: 100%;
            }

            th, td {
                border: 1px solid #dddddd;
                text-align: left;
```

Notant bien : après chaque modification dans les fichiers déployés en apache il faut redémarrer le serveur apache dans la machine EC2.

Etape 15 : Création et connexion avec le service RDS

1- Création d'un subnet Group





2- Création de la base de donnés

Choose a database creation method Info

- (●) **Standard create**
  You set all of the configuration options, including ones for availability, security, backups, and maintenance.
- ( ) **Easy create**
  Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

- (●) **MySQL**

Availability and durability

Deployment options Info

The deployment options below are limited to those supported by the engine you selected above.

- ( ) **Multi-AZ DB Cluster**
  Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.
- (●) **Multi-AZ DB instance**
  Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.
- ( ) **Single DB instance**
  Creates a single DB instance with no standby DB instances.

Compute resource

Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

- (●) **Don't connect to an EC2 compute resource**
  Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.
- ( ) **Connect to an EC2 compute resource**
  Set up a connection to an EC2 compute resource for this database.

Virtual private cloud (VPC) Info

Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

web-server-vpc (vpc-0eae1aa07781387ae)
8 Subnets, 2 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change its VPC.

DB subnet group Info

Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

db-three-tier-subnetgroup
2 Subnets, 2 Availability Zones

Public access Info

- ( ) **Yes**
  RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.
- (●) **No**
  RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

3- Installation de mysql dans la machine EC2 du backend et création de la base de données

Installation :

>> sudo apt install mysql-server

Connection au service RDS :

>> **mysql -u admin -h rdsphpdb.cnq4000ie48g.us-east-1.rds.amazonaws.com –p**

>> //donner le mot de passe

```
ubuntu@ip-10-0-4-58:/var/www/html$ mysql -u admin -h rdsphpdb.cnq4000ie48g.us-east-1.rds.amazonaws.com -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 598
Server version: 8.0.35 Source distribution

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> Create database studennt;
Query OK, 1 row affected (0.04 sec)

mysql> Use studennt;
Database changed
mysql> create table studentT (cin varchar(10) primary key, name varchar(20), uni varchar(30));
Query OK, 0 rows affected (0.06 sec)

mysql>
```

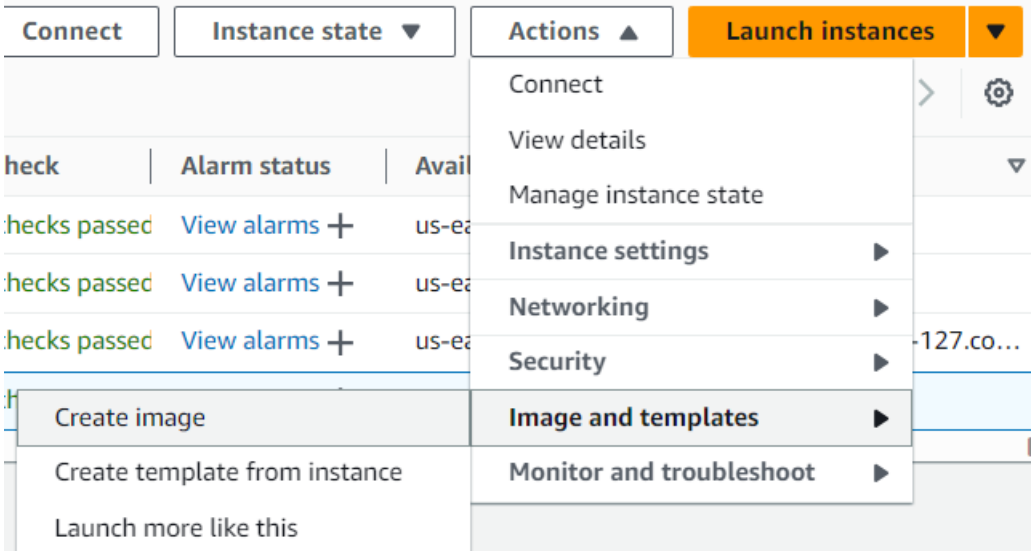
4- Connexion du base de données avec le backend :

utilisant le endpoint de la base de donnée crée dans RDS et les paramètres de configuration.

```
define('DB_SERVER', 'rdsphpdb.cnq4000ie48g.us-east-1.rds.amazonaws.com');
define('DB_USERNAME', 'admin');
define('DB_PASSWORD', 'adminadmin');
define('DB_DATABASE', 'student');
```

Etape 16 : création de l'Auto Scaling Group :

1- Création d'une Template :



AMI from catalog | Recents | My AMIs | Quick Start

Amazon Machine Image (AMI)

ubuntu/images/hvm-ssd/ubuntu-focal-20.04-amd64-server-20231025
ami-06aa3f7caf3a30282

Verified provider | Free tier eligible

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Published	Architecture	Virtualization	Root device type	ENA Enabled
2023-10-26T04:01:02.000Z	x86_64	hvm	ebs	Yes

Network settings Info

Subnet Info

subnet-012437684f5b8acb4 web-server-subnet-private4-us-east-1b
VPC: vpc-0eae1aa07781387ae Owner: 637423538109
Availability Zone: us-east-1b IP addresses available: 250 CIDR: 10.0.8.0/24)

Create new subnet

When you specify a subnet, a network interface is automatically added to your template.

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

(•) Select existing security group ( ) Create security group

Common security groups Info

Select security groups

private Instances SG sg-04cfda9230cbd94d7
VPC: vpc-0eae1aa07781387ae

Compare security group rules

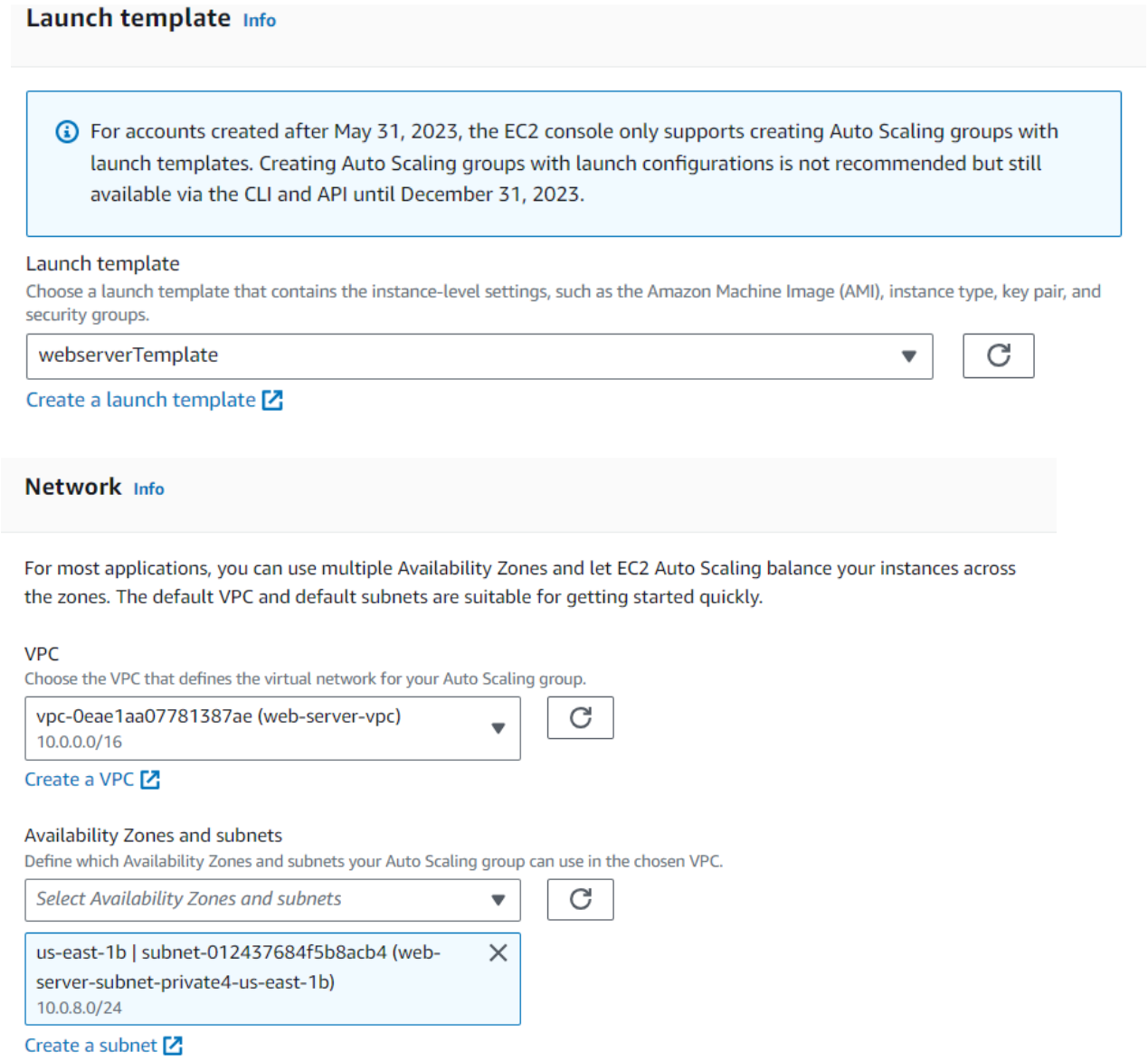
Show all selected (+1)

Security groups that you add or remove here will be added to or removed from all your network interfaces.

▶ Advanced network configuration

2- Création de l'autoscaling group

sélection de la Template



Load balancing Info

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

- ○ No load balancer
  Traffic to your Auto Scaling group will not be fronted by a load balancer.
- ◉ Attach to an existing load balancer
  Choose from your existing load balancers.
- ○ Attach to a new load balancer
  Quickly create a basic load balancer to attach to your Auto Scaling group.

Attach to an existing load balancer

Select the load balancers that you want to attach to your Auto Scaling group.

- ◉ Choose from your load balancer target groups
  This option allows you to attach Application, Network, or Gateway Load Balancers.
- ○ Choose from Classic Load Balancers

Existing load balancer target groups

Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

Select target groups ▼ 

TargetEc2Private | HTTP ✕
Application Load Balancer: appLb

Desired capacity

Specify your group size.

2

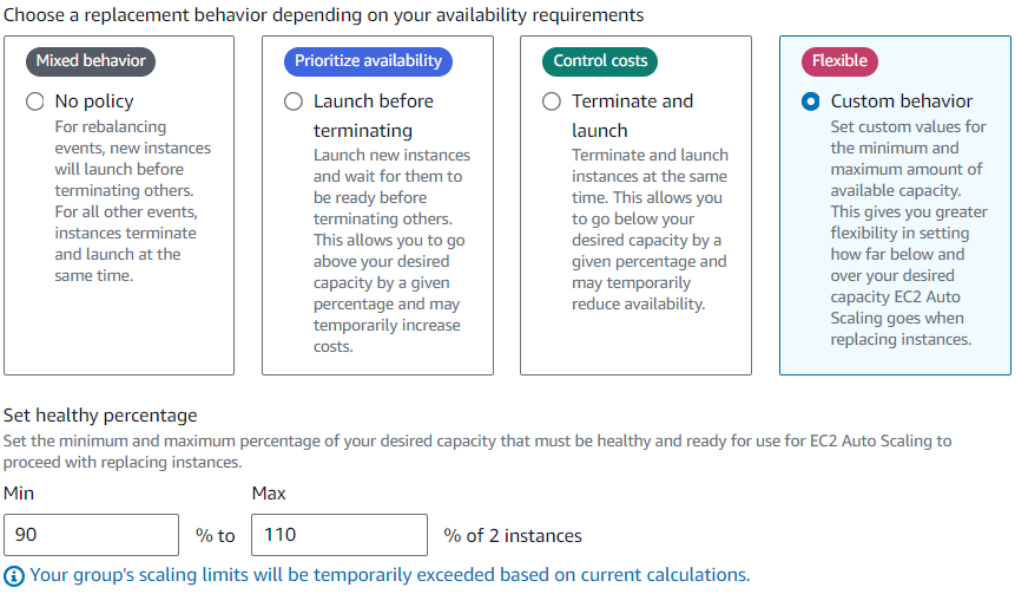
Scaling Info

You can resize your Auto Scaling group manually or automatically to meet changes in demand.

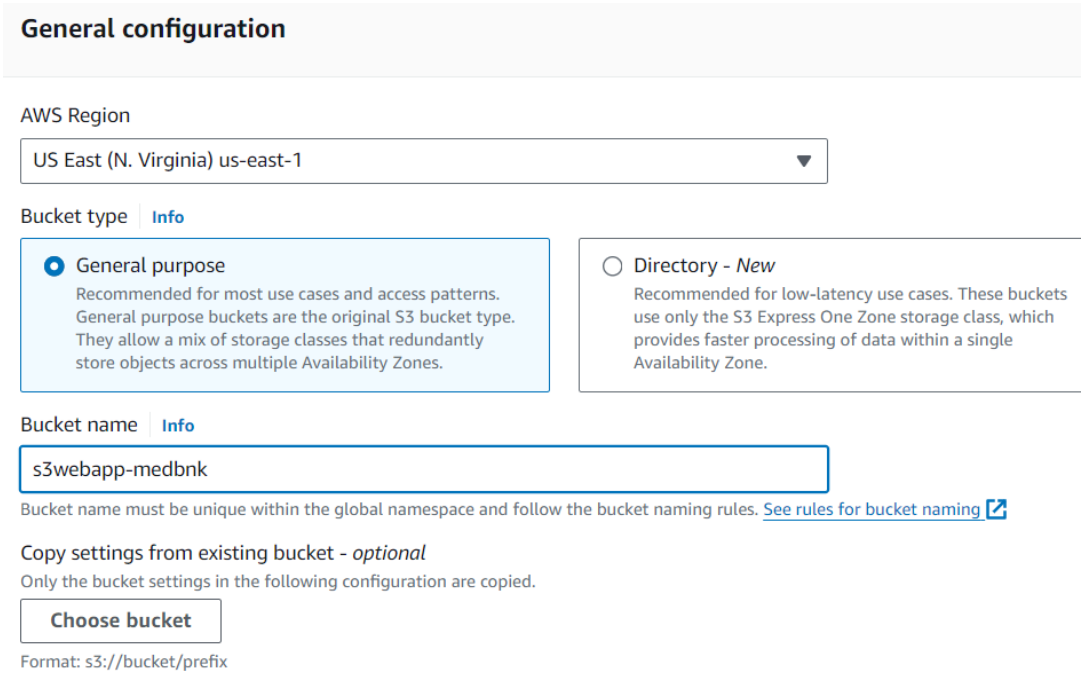
Scaling limits

Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity	Max desired capacity
1	2
Equal or less than desired capacity	Equal or greater than desired capacity



Etape 17 : Création de S3 et déploiement du site web statique :

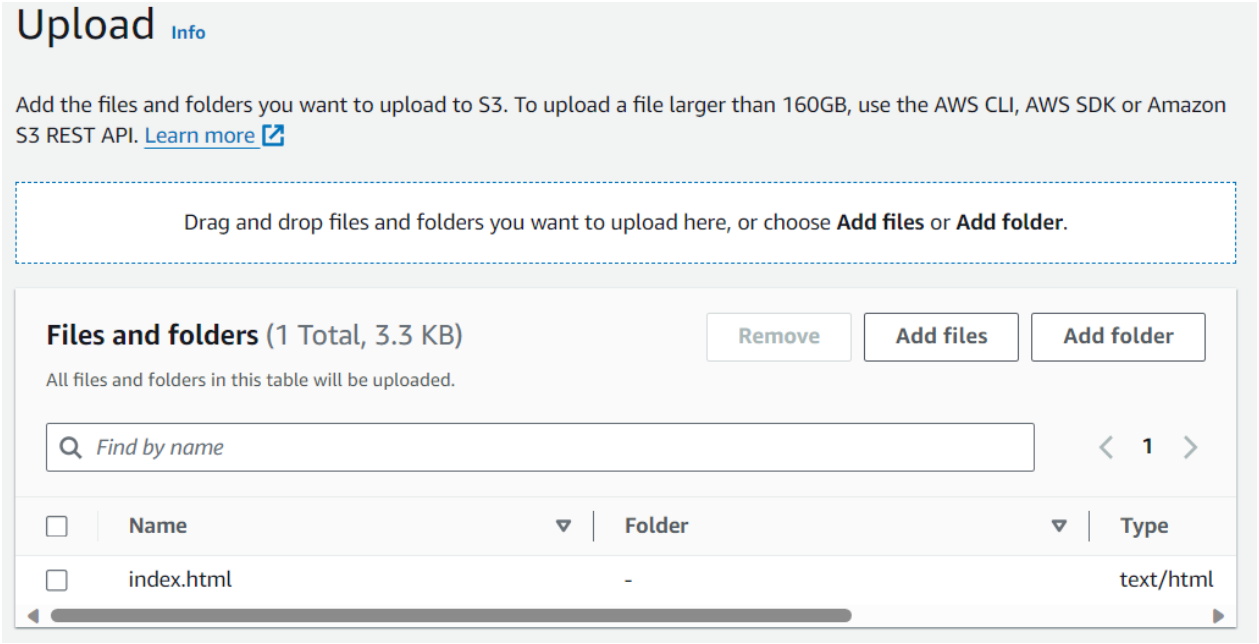


☐ **Block *all* public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  S3 will ignore all ACLs that grant public access to buckets and objects.
- ☐ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
  S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
  S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Upload du fichier statique :

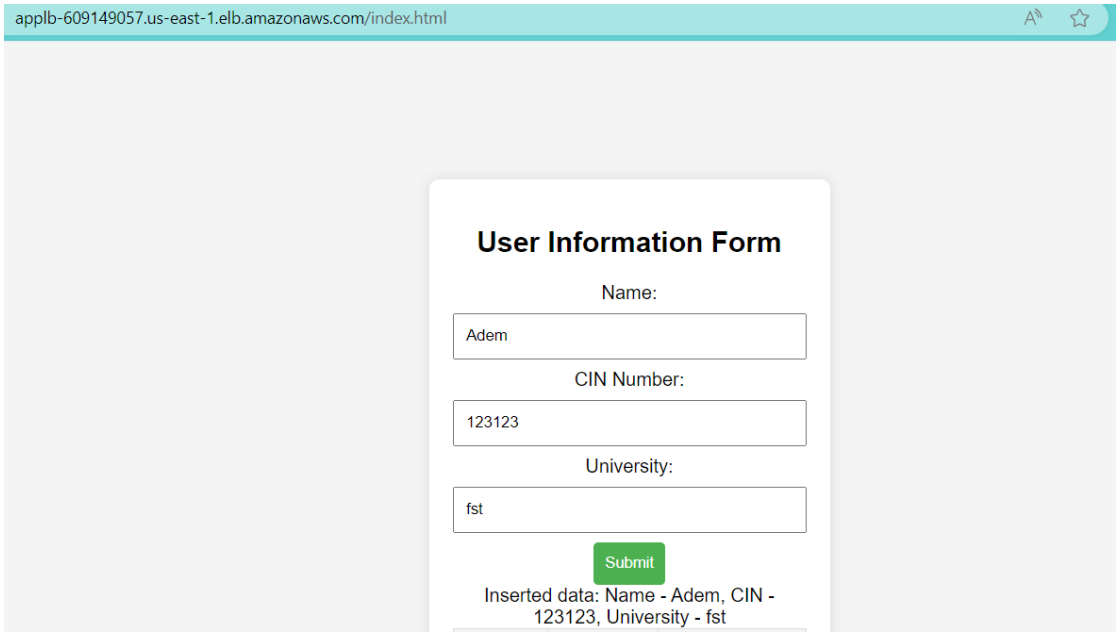


Modification des permissions :

On choisit permissions et on change les bucket policy pour que tout accès http soit accepté.


```
{
    "Version": "2012-10-17",
    "Id": "Policy1706821917218",
    "Statement": [
        {
            "Sid": "Stmt1706821913441",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::637423538109:root"
            },
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::s3webapp-medbnk"
        }
    ]
}
```

Teste de site web :



Teste de site web statique :