

# Capstone project

PERIN LEA



# **Sommaire**

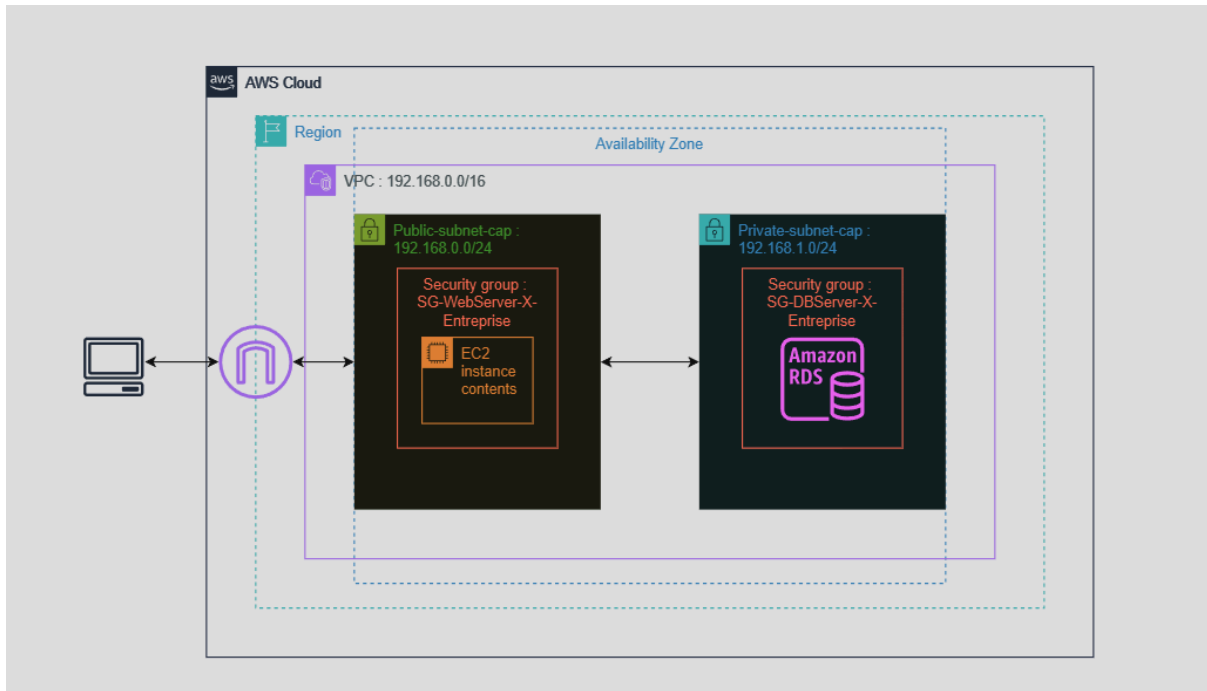
- 1. Introduction**
- 2. Architectural Diagram**
- 3. Design Rationale**
  - 3.1 Virtual Private Cloud (VPC)**
  - 3.2 Subnets and Routing**
  - 3.3 Internet Gateway**
  - 3.4 EC2 Instances**
  - 3.5 AWS RDS (Relational Database Service)**
- 4. Deploying Cloud Architecture**
  - 4.1 Creating Virtual Private Cloud (VPC)**
  - 4.2 Adding Internet Gateway**
  - 4.3 Creating EC2 Instances**
  - 4.4 Configuring PostgreSQL Database on RDS**
- 5. Database Management**
  - 5.1 Database Creation**
  - 5.2 Postbird Usage**
  - 5.3 Database Connection**
- 6. Conclusion**

## 1. Introduction

This document outlines the architectural design and deployment strategy for hosting the X Company's website on the AWS cloud infrastructure.

## 2. Architectural Diagram

The diagram below illustrates the cloud deployment architecture :

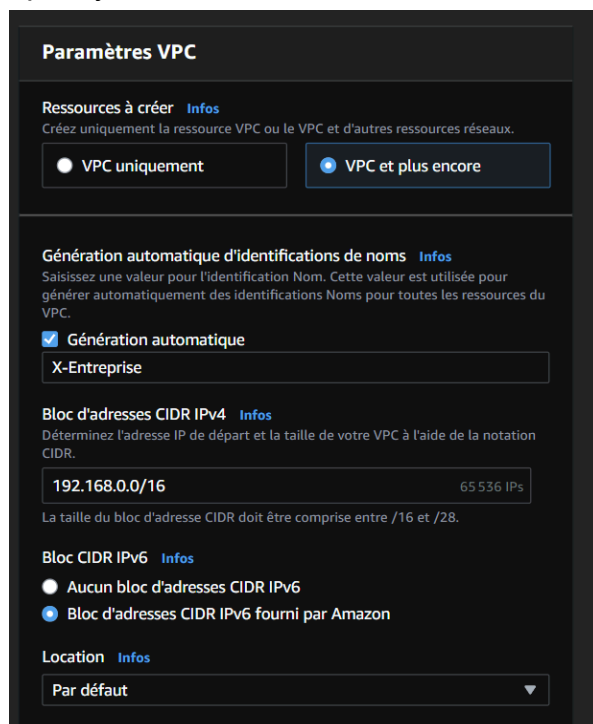


## 3. Deploying Cloud Architecture

### 3.1 Creating Virtual Private Cloud (VPC)

- Log in to the AWS console.
- Go to the VPC service and click on "Create VPC".

→ Specify VPC details such as name, CIDR block



**Paramètres VPC**

**Ressources à créer** [Infos](#)  
Créez uniquement la ressource VPC ou le VPC et d'autres ressources réseaux.

☐ VPC uniquement ☒ VPC et plus encore

**Génération automatique d'identifications de noms** [Infos](#)  
Saisissez une valeur pour l'identification Nom. Cette valeur est utilisée pour générer automatiquement des identifications Noms pour toutes les ressources du VPC.

☒ Génération automatique  
X-Entreprise

**Bloc d'adresses CIDR IPv4** [Infos](#)  
Déterminez l'adresse IP de départ et la taille de votre VPC à l'aide de la notation CIDR.

192.168.0.0/16 65 536 IPs

La taille du bloc d'adresse CIDR doit être comprise entre /16 et /28.

**Bloc CIDR IPv6** [Infos](#)

☐ Aucun bloc d'adresses CIDR IPv6 ☒ Bloc d'adresses CIDR IPv6 fourni par Amazon

**Location** [Infos](#)  
Par défaut ▼

→ Next, create two subnets: one public subnet and one private subnet, specifying appropriate CIDR ranges.



**Nombre de sous-réseaux publics** [Infos](#)  
Nombre de sous-réseaux publics à ajouter à votre VPC. Utilisez des sous-réseaux publics pour les applications web qui doivent être publiquement accessibles via Internet.

0 1

**Nombre de sous-réseaux privés** [Infos](#)  
Nombre de sous-réseaux privés à ajouter à votre VPC. Utilisez des sous-réseaux privés pour sécuriser les ressources backend qui n'ont pas besoin d'un accès public.

0 1 2

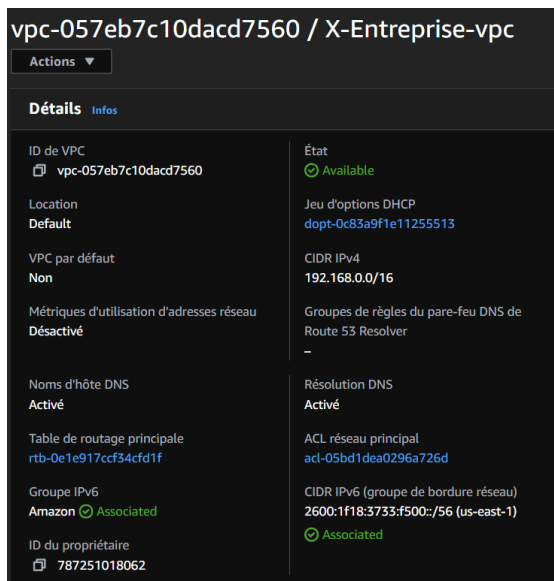
▼ **Personnaliser les blocs d'adresse CIDR des sous-réseaux**

**Bloc d'adresse CIDR de sous-réseau public dans us-east-1a**

192.168.0.0/24 256 IPs

**Bloc d'adresse CIDR de sous-réseau privé dans us-east-1a**

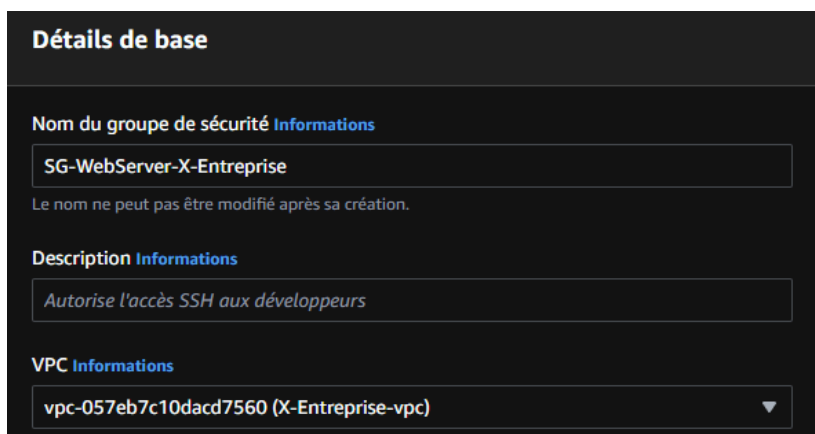
192.168.1.0/24 256 IPs



→ Create security groups to regulate inbound and outbound traffic for EC2 instances. There are two security groups created for this purpose:

→ SG-WebServer-X-Enterprise (for EC2 instances in the public subnet):

- Inbound Rules :  
Allow HTTP (port 80) traffic from anywhere.  
Allow HTTPS (port 443) traffic from anywhere.  
Allow SSH (port 22) traffic from anywhere.
- Outbound Rules :  
All outbound traffic is allowed by default.



### Règles entrantes Informations

Règle entrante 1 Supprimer

Type Informations

HTTP ▼

Protocole Informations

TCP

Plage de ports Informations

80

Type de source Informations

N'importe où - IPv4 ▼

Source Informations

Q

0.0.0.0/0 ✕

Description - facultatif Informations

---

Règle entrante 2 Supprimer

Type Informations

HTTPS ▼

Protocole Informations

TCP

Plage de ports Informations

443

Type de source Informations

N'importe où - IPv4 ▼

Source Informations

Q

0.0.0.0/0 ✕

Description - facultatif Informations

Ajouter une règle

Règle entrante 3 Supprimer

ID de règle de groupe de sécurité

–

Type Informations

SSH ▼

Protocole Informations

TCP

Plage de ports Informations

22

Type de source Informations

N'importe où - IPv4 ▼

Source Informations

Q

0.0.0.0/0 ✕

Description - facultatif Informations

Ajouter une règle

→ SG-DBServer-X-Enterprise (for RDS database instances in the private subnet) :

- Inbound Rules:  
Allow PostgreSQL (port 5432) traffic from SG-WebServer-X-Enterprise.
- Outbound Rules:  
All outbound traffic is allowed by default

## Détails de base

Nom du groupe de sécurité [Informations](#)

SG-DBServer-X-Entreprise

Le nom ne peut pas être modifié après sa création.

Description [Informations](#)

Autorise l'accès SSH aux développeurs

VPC [Informations](#)

vpc-057eb7c10dacd7560 (X-Entreprise-vpc) ▼

## Règles entrantes [Informations](#)

Règle entrante 1

Supprimer

Type [Informations](#)

PostgreSQL ▼

Protocole [Informations](#)

TCP

Plage de ports [Informations](#)

5432

Type de source [Informations](#)

Personnalisé(e) ▼

Source [Informations](#)

🔍 sg-0e3ee78c3d9692771 ✕

sg-0e3ee78c3d9692771 ✕

Description - facultatif [Informations](#)

Ajouter une règle

Règles sortantes Informations

Règle sortante 1

Supprimer

Type Informations

Protocole Informations

Plage de ports Informations

Tout le trafic

Tous

Tous

Type de destination Informations

Destination Informations

Description - facultatif Informations

N'importe où - IPv4

0.0.0.0/0

×

Règle sortante 2

Supprimer

Type Informations

Protocole Informations

Plage de ports Informations

Tout le trafic

Tous

Tous

Type de destination Informations

Destination Informations

Description - facultatif Informations

N'importe où - IPv6

::/0

×

Ajouter une règle

Result :

	Name	ID du groupe de sécurité	Nom du groupe de sécurité	ID de VPC	Description
	-	<a href="#">sg-0e3ee78c3d9692771</a>	SG-WebServer-X-Entreprise	<a href="#">vpc-057eb7c10d9cd7560</a>	SG-webserver
	-	<a href="#">sg-09645734465d5e4ed</a>	default	<a href="#">vpc-057eb7c10d9cd7560</a>	default VPC security group
	-	<a href="#">sg-09bce223e7fcb8c9</a>	default	<a href="#">vpc-0e9ce8e9b175e27be5</a>	default VPC security group
	-	<a href="#">sg-06c140100f0409a42</a>	SG-DBServer-X-Entreprise	<a href="#">vpc-057eb7c10d9cd7560</a>	SG-DBServer
	-	<a href="#">sg-0e33f6425e9a844f3</a>	default	<a href="#">vpc-0518753564195588c</a>	default VPC security group
	-	<a href="#">sg-03065471518afdf03</a>	Ec2SecurityGroup	<a href="#">vpc-0e9ce8e9b175e27be5</a>	VPC Security Group

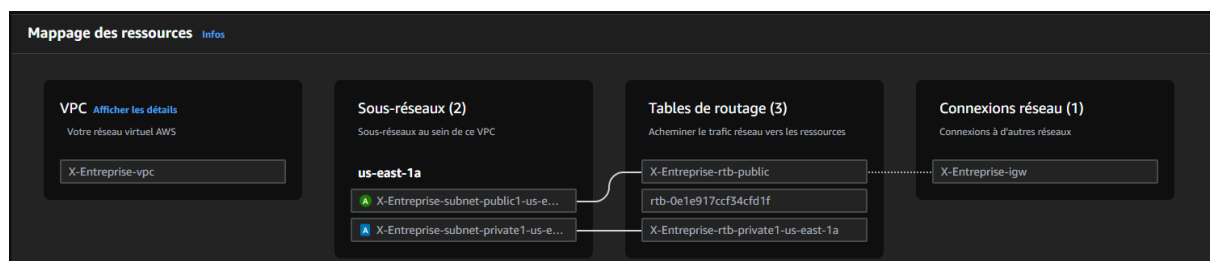
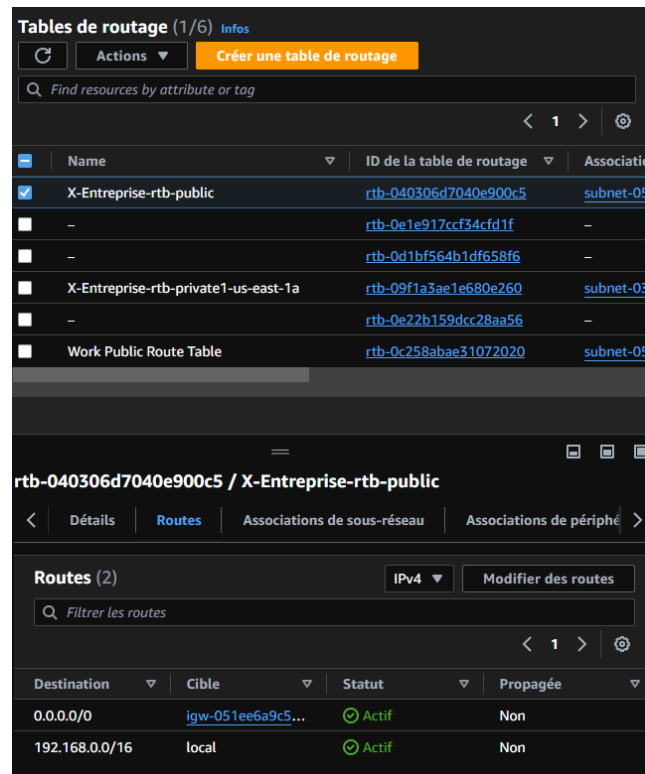
## 3.2 Adding Internet Gateway

- In the VPC console, select "Internet Gateways" and click on "Create Internet Gateway".
- Attach the Internet Gateway to the VPC created earlier.  
Select the Internet Gateway you just created and click on "Actions" -> "Attach to VPC".  
Select your VPC-X-Enterprise and click on "Attach Internet Gateway".

7

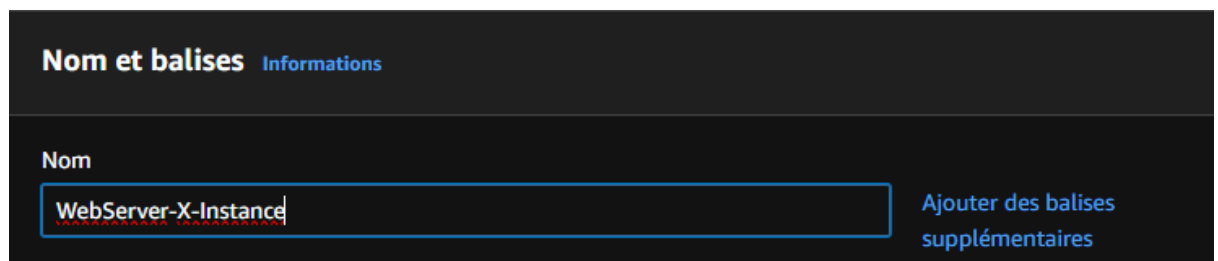


- Modify the public route table to include a route to the Internet Gateway.  
Click on "Add route" and enter "0.0.0.0/0" as the destination (which means all traffic) and select the Internet Gateway you attached to your VPC as the target.

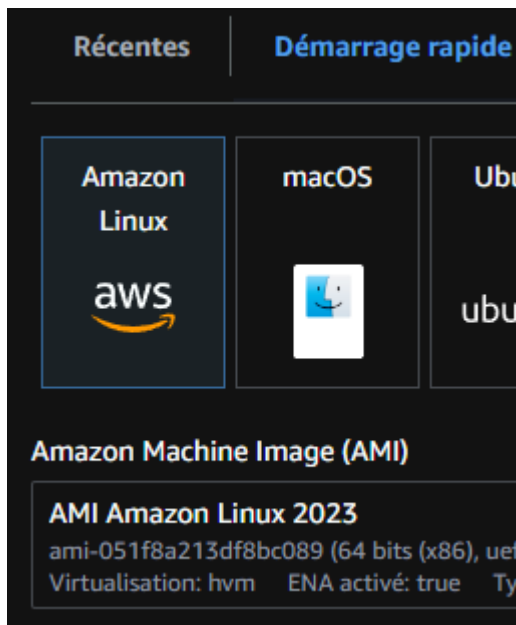


### 3.3 Creating EC2 Instances

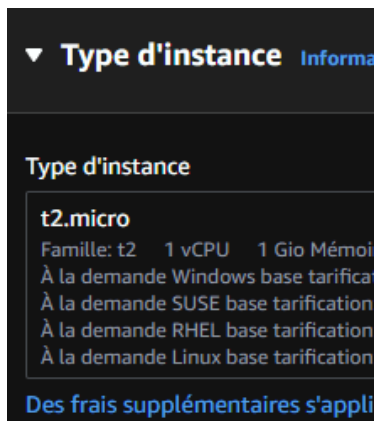
- Go to the EC2 console and click on "Launch Instance".



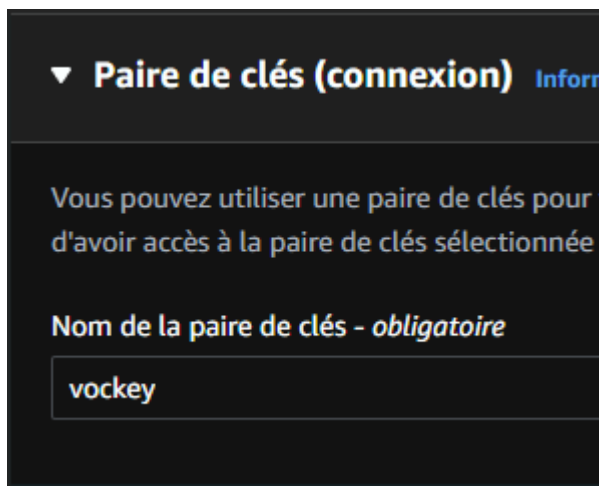
- Select the Amazon Linux 2 (version 2023) image.



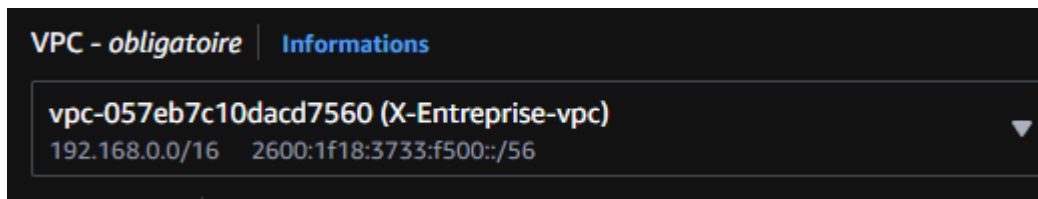
→ Choose the instance type "t2.micro".



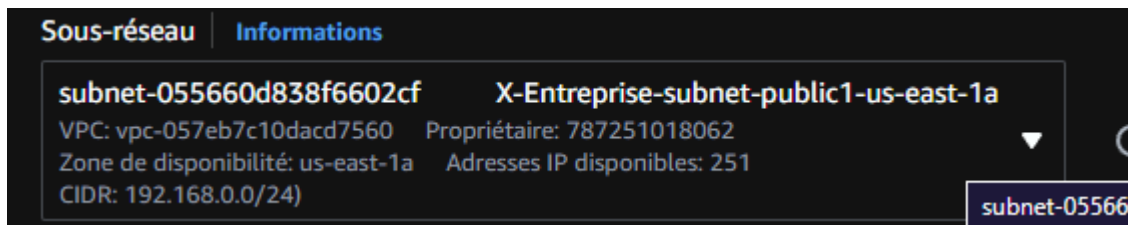
→ Select the key pair "vockey".



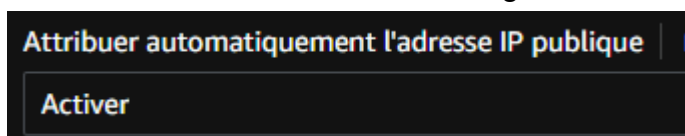
→ In the network settings, choose your VPC "x-enterprise-vpc".



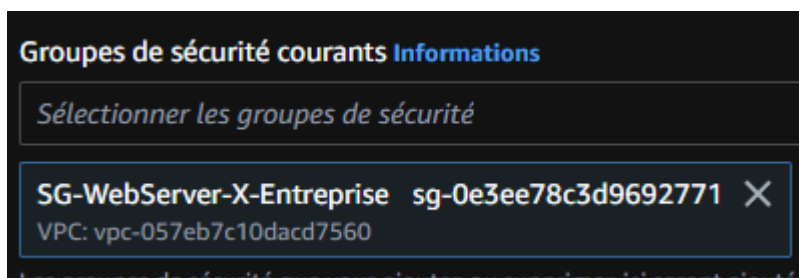
→ Select your public subnet: "x-enterprise-subnet-public-us-east-1a".



→ Check the box to enable "Auto-assign Public IP".



→ Select the existing security group "sg-webserver-x-enterprise" to allow HTTP and HTTPS traffic.



→ Copy this script to my EC2 instance, and then execute it to install and start Apache.

```
#!/bin/bash

# Installation d'Apache
echo "Installation d'Apache..."
sudo yum update -y
sudo yum install -y httpd
sudo systemctl start httpd
sudo systemctl enable httpd

# Clonage du dépôt Git
echo "Clonage du dépôt Git..."
git clone https://github.com/Nerlyss1/CAPSTONE-PROJECT.git

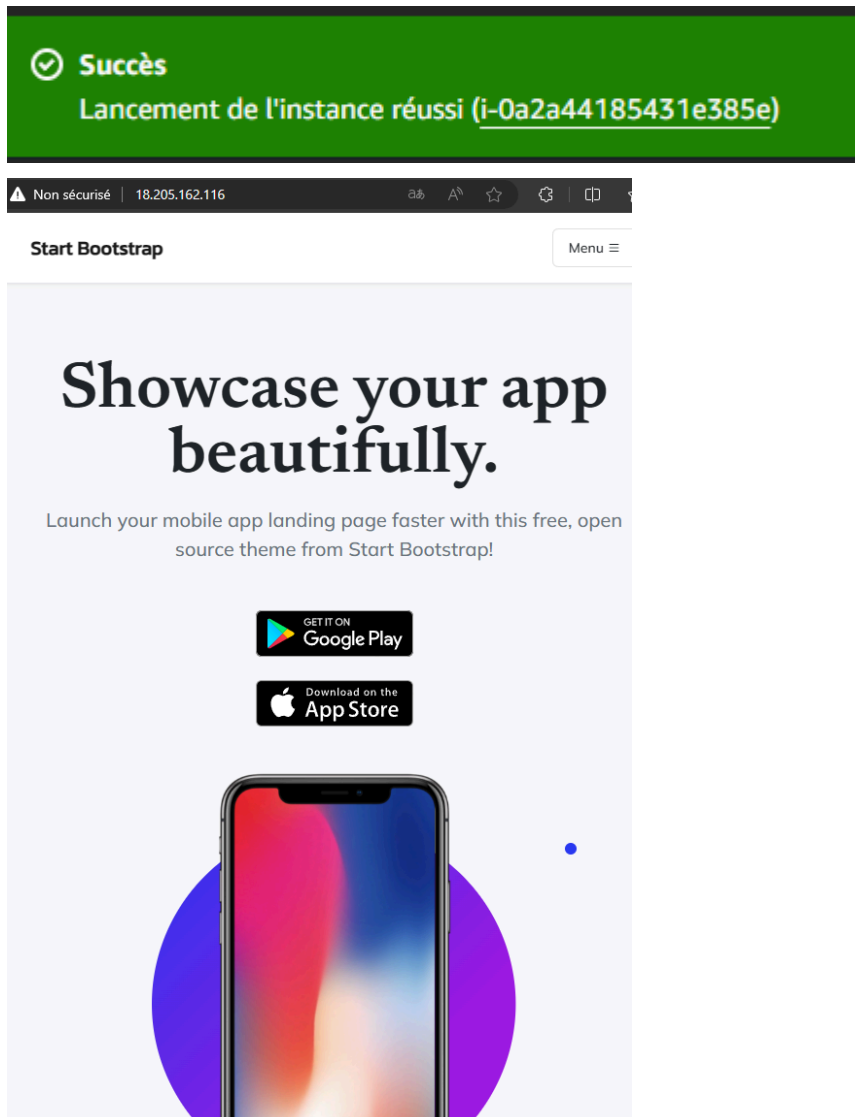
# Copie des fichiers vers /var/www/html
echo "Copie des fichiers vers /var/www/html..."
cd CAPSTONE-PROJECT/2024/b3/cloud/sample-app
sudo cp -r * /var/www/html/

# Attribution des permissions
echo "Attribution des permissions..."
sudo chown -R apache:apache /var/www/html
sudo chmod -R 755 /var/www/html

# Redémarrage d'Apache
echo "Redémarrage d'Apache..."
sudo systemctl restart httpd

echo "Installation et déploiement terminés avec succès."
```

→ Finally, launch the instance.



## 4. Database Creation

### 4.1. Creating PostgreSQL Database on AWS RDS

→ Go to the RDS service.

→ Create a database subnet group

## Créer un groupe de sous-réseaux de base de données

Pour créer un nouveau groupe de sous-réseaux, attribuez-lui un nom et une description, puis choisissez un VPC existant. Vous pourrez ensuite ajouter des sous-réseaux associés à ce VPC.

### Détails du groupe de sous-réseaux

**Nom**  
Vous ne pouvez pas modifier le nom une fois que le groupe de sous-réseaux a été créé.

Db-Subnet-Group

Celui-ci doit contenir entre 1 et 255 caractères. Les caractères alphanumériques, les espaces, les tirets, les traits de soulignement et les points sont autorisés.

**Description**

Db-Subnet-Group

**VPC**  
Choisissez un identifiant de VPC qui correspond aux sous-réseaux que vous souhaitez utiliser avec votre groupe de sous-réseaux de base de données. Vous ne pouvez pas choisir un autre identifiant après la création de votre groupe de sous-réseaux.

X-Entreprise-vpc (vpc-057eb7c10dacd7560)

X-Entreprise-vpc (vpc-057eb7c10dacd7560)

→ Click on "Create database".

→ Choose PostgreSQL as the database engine.

### Choisir une méthode de création de bases de données

**Création standard**  
Vous définissez toutes les options de configuration, y compris celles relatives à la disponibilité, la sécurité, aux sauvegardes et à la maintenance.

**Création facile**  
Utilisez les configurations recommandées selon les bonnes pratiques. Certaines options de configuration peuvent être modifiées après la création de la base de données.

### Options de moteur

Type de moteur

**Aurora (MySQL Compatible)**

**Aurora (PostgreSQL Compatible)**

→ Configure database instance details such as instance type

→ Connection of instance EC2

### Connectivité

**Ressource de calcul**  
Choisissez si vous souhaitez configurer une connexion à une ressource de calcul pour cette base de données. La configuration d'une connexion modifiera automatiquement les paramètres de connectivité afin que la ressource de calcul puisse se connecter à cette base de données.

**Ne pas se connecter à une ressource de calcul EC2**  
Ne configurez pas de connexion à une ressource de calcul pour cette base de données. Vous pouvez configurer manuellement une connexion à une ressource de calcul ultérieurement.

**Se connecter à une ressource de calcul EC2**  
Configurez une connexion à une ressource de calcul EC2 pour cette base de données.

**Instance EC2**  
Choisissez l'instance EC2 à ajouter en tant que ressource de calcul pour cette base de données. Un groupe de sécurité VPC est ajouté à cette instance EC2. Un groupe de sécurité VPC est également ajouté à la base de données avec une règle entrante qui autorise l'instance EC2 à accéder à la base de données.

i-0a2a44185431e385e  
WebServer-X-Instance

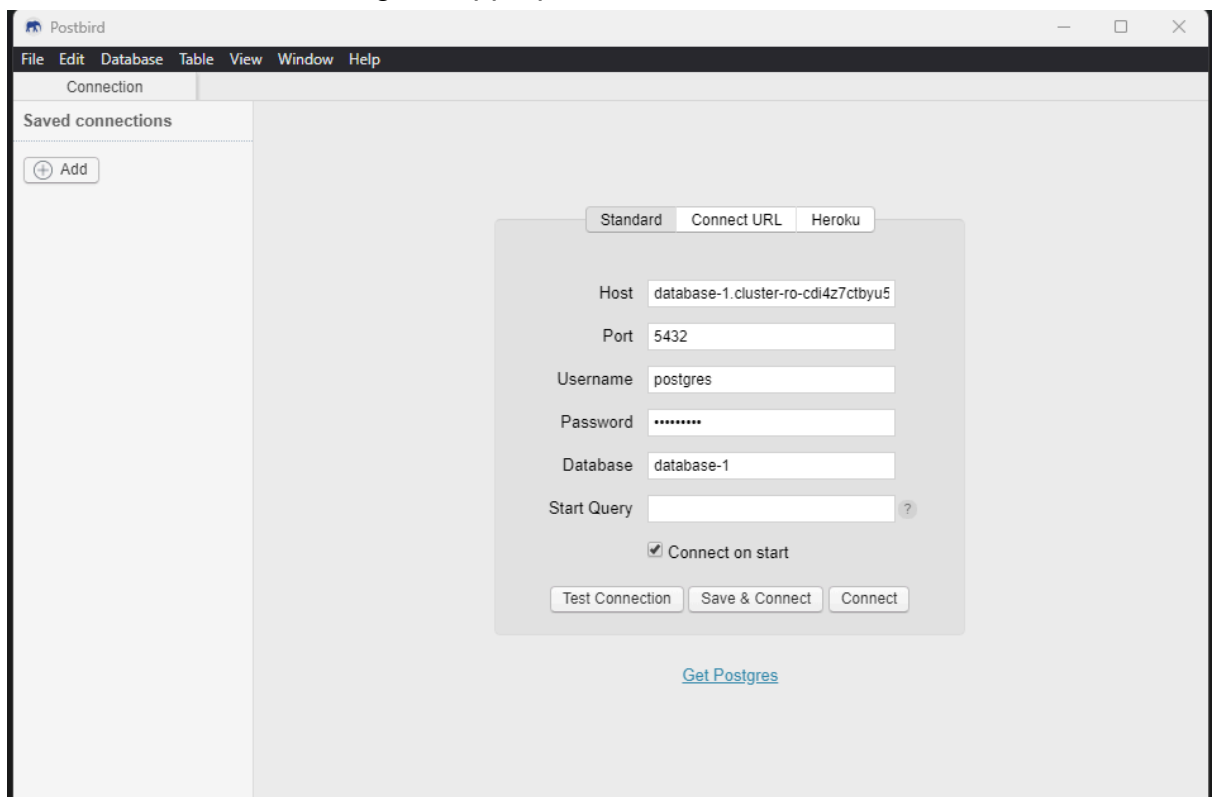
- Select security group options to allow access to the database from your EC2 instance.



- Launch the database creation process.

## 4.2. Installation and Configuration of Postbird

- Install Postbird
- Once Postbird is installed, launch the application and connect to your RDS database using the appropriate credentials.



## 5. Database Connection

- An SSH connection is established with the EC2 web server.
- A PostgreSQL client is installed on the web server.
- A connection to the database is established from the command line to verify connectivity and functionality.