

CAPSTONE PROJECT DOCUMENTATION

Cloud - AWS

Date : 08/04/2024

Zitouni Iptissem

I. Introduction

II. Diagram architecture

III. Deploying Architecture

1. Virtual Private Cloud VPC

IV. Deploying Database

V. Conclusion

I. Introduction

Through this project, we will deploy our website named capstone on the cloud and create a database.

To do this, we will go through several steps: an architecture diagram, a virtual private network and site hosting.

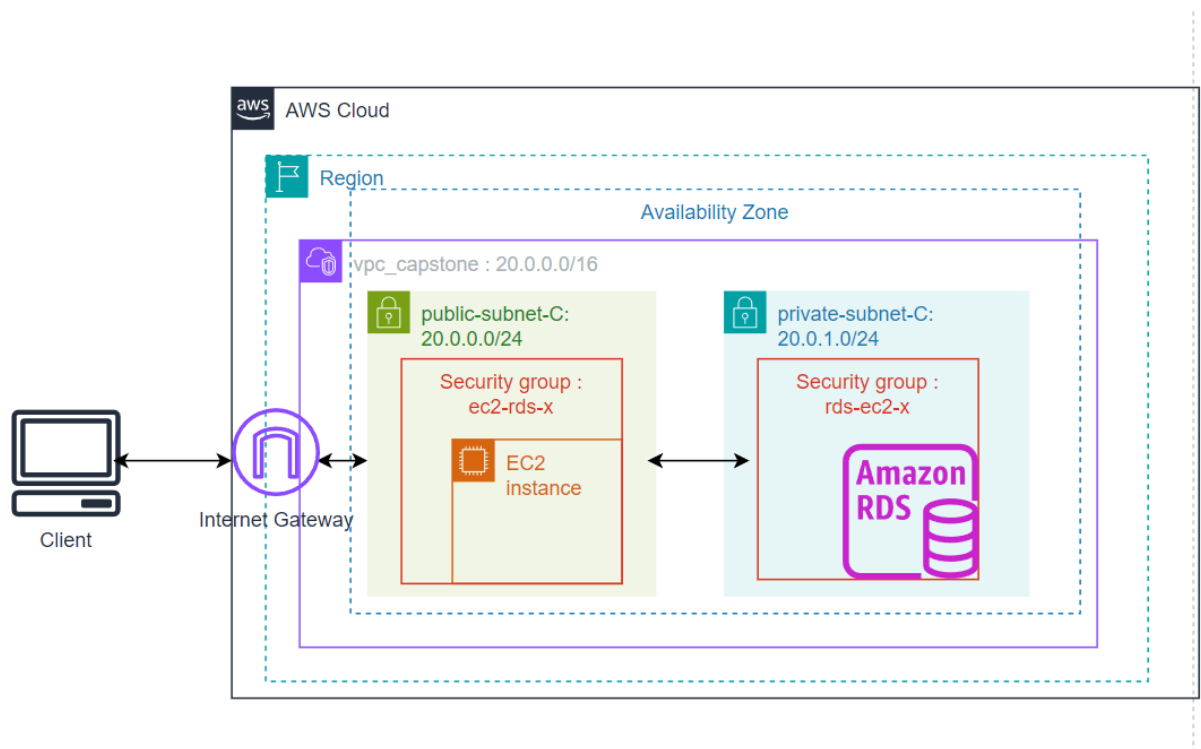
Then, creating a database and we will establish an SSH connection.

The technologies used to carry out this project: AWS cloud, like EC2, VPC, RDS.. To carry out this project, we use the sandbox functionality of our AWS sessions.

II. Diagram architecture

We have in our architecture a VPC with two subnets: a public in which will be our web server and the other private for the database.

We also have a client who will allow us to test our architecture.



III. Deploying Architecture

1. Virtual Private Cloud VPC

We configure our VPC to respect the scheme







The screenshot shows the AWS Management Console interface for creating a new VPC. The top navigation bar includes the AWS logo, 'Services', a search icon, a home icon, a notifications bell, a help icon, a settings gear, the user name 'Virginie', and the account ID 'voclabs/user3035602=Iptissem_ZITOU'.

The breadcrumb trail is 'VPC > Vos VPC > Créer un VPC'. The main heading is 'Créer un VPC' with an 'Infos' link. Below the heading is a descriptive paragraph: 'Un VPC est une partie isolée du Cloud AWS remplie d'objets AWS, tels que des instances Amazon EC2. Passez la souris sur une ressource pour mettre en évidence les ressources connexes.'

The 'Paramètres VPC' section contains the following options:

- Ressources à créer** (with an 'Infos' link): 'Créez uniquement la ressource VPC ou le VPC et d'autres ressources réseaux.' There are two radio buttons: 'VPC uniquement' (unselected) and 'VPC et plus encore' (selected).
- Génération automatique d'identifications de noms** (with an 'Infos' link): 'Saisissez une valeur pour l'identification Nom. Cette valeur est utilisée pour générer automatiquement des identifications Noms pour toutes les ressources du VPC.' A checkbox labeled 'Génération automatique' is checked. Below it is a text input field containing 'capstone'.
- Bloc d'adresses CIDR IPv4** (with an 'Infos' link): 'Déterminez l'adresse IP de départ et la taille de votre VPC à l'aide de la notation CIDR.' Below this is a text input field containing '10.0.0.0/16' and a secondary field showing '65 536 IPs'. A note below states: 'La taille du bloc d'adresse CIDR doit être comprise entre /16 et /28.'
- Bloc CIDR IPv6** (with an 'Infos' link): This section is partially visible at the bottom.

The 'Aperçu' (Preview) section on the right shows a preview of the VPC configuration, including the name 'capstone-vpc'.

 Services      Virginie ▼ voclabs/us

Nombre de zones de disponibilité (AZ) [Infos](#)

Choisissez le nombre de zones de disponibilité dans lesquelles mettre en service des sous-réseaux. Nous vous recommandons d'utiliser au moins deux zones de disponibilité pour avoir une haute disponibilité.

☒ 1 ☐ 2 ☐ 3

► Personnalisez les zones de disponibilité

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

256 IPs

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

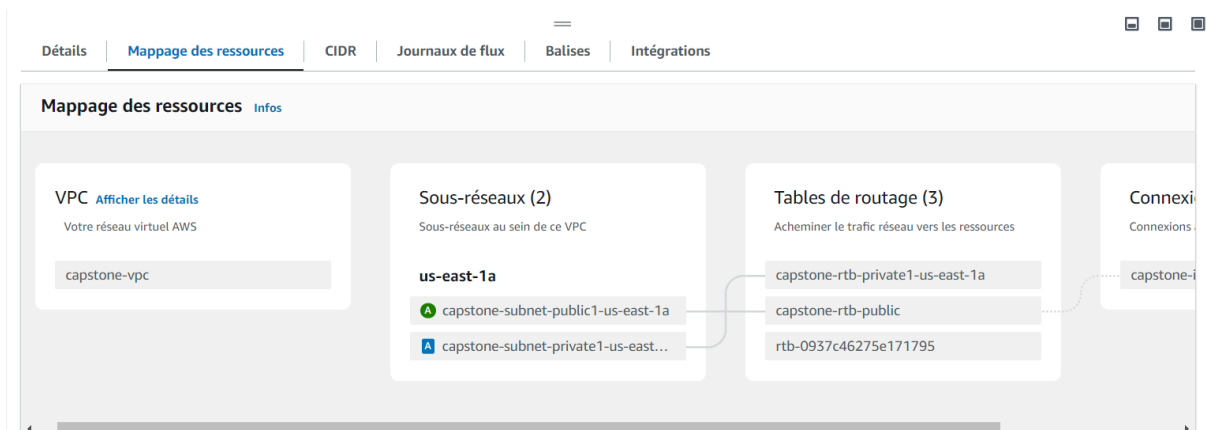
256 IPs

CAPSTONE PROJECT DOCUMENTATION



The description matches well: our vpc is created.

Here, the resource mapping section allows us to check that everything is good, it is.



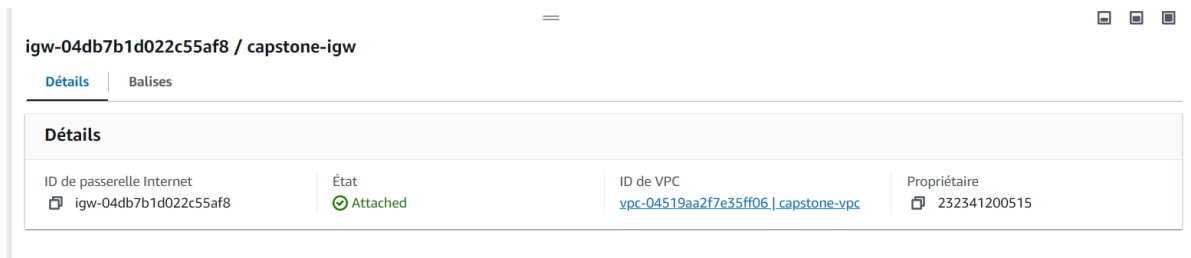
2. Routing and internet gateway

The VPC was created, it configured two very important steps: **the routing table** and the **internet gateway**.

Indeed, during the configuration of our VPC, we specified our subnetworks, so it deduces its parameters

Internet gateway allows communication between resources within a virtual private cloud (VPC) and the Internet, enabling inbound and outbound traffic to and from the Internet.

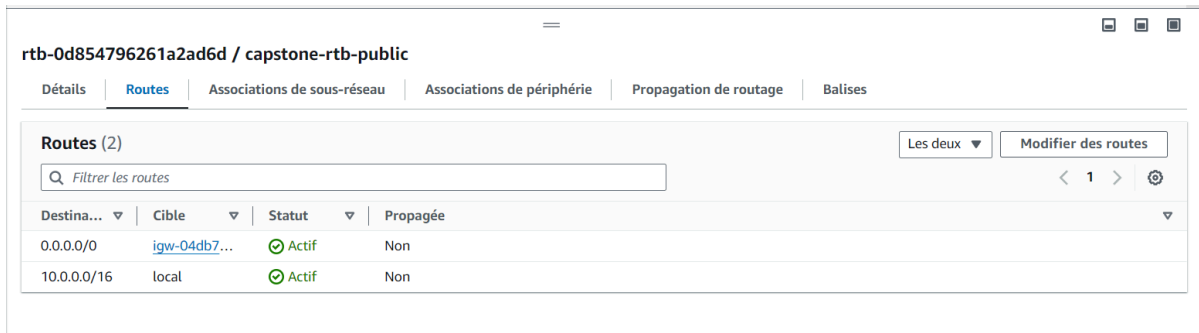
CAPSTONE PROJECT DOCUMENTATION



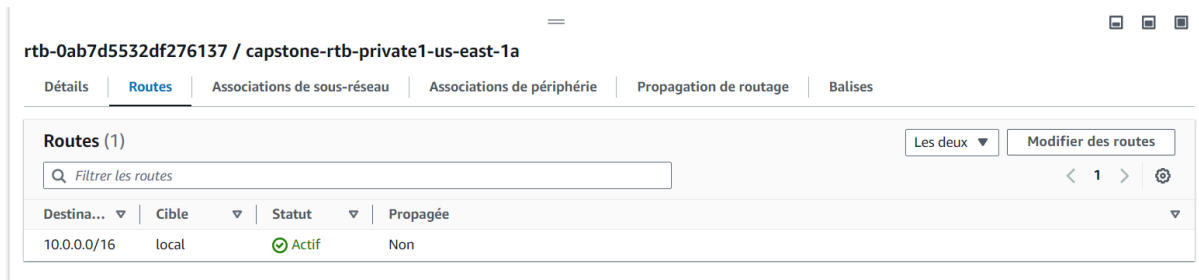
Routing table : set of rules that guides network traffic between different resources in an AWS virtual network, indicating where to send traffic based on its destination.

Public routing table : routes traffic to resources accessible from the Internet

Here, the 0.0.0.0/0 means internet.



Private routing table : directs traffic to resources internal to the virtual network



The 10.0.0.0/16 is the local route.

3. Creating security group

After configuring our environment, we will create security groups for our 2 subnets.
création groupe de sécurité.

They acts as a virtual **firewall** for instances, controlling inbound and outbound traffic based on defined rules, thus helping to enhance network security within the AWS environment.

- **Group security for web equip** :

The screenshot shows the AWS Management Console interface for creating a security group. The breadcrumb navigation is 'VPC > Groupes de sécurité > Créer un groupe de sécurité'. The main heading is 'Créer un groupe de sécurité' with an 'Informations' link. Below the heading is a descriptive paragraph: 'Un groupe de sécurité agit comme un pare-feu virtuel pour votre instance afin de contrôler le trafic entrant et sortant. Pour créer un groupe de sécurité, complétez les champs ci-dessous.' The 'Détails de base' section contains three fields: 'Nom du groupe de sécurité' (Web Security Group), 'Description' (Enable HTTP access), and 'VPC' (vpc-04519aa2f7e35ff06 (capstone-vpc)).

aws Services [Search] [Home] [Alerts] [Help] [Settings] Virgini voclabs/user3035602=Iptissem_ZIT

VPC > Groupes de sécurité > Créer un groupe de sécurité

Créer un groupe de sécurité [Informations](#)

Un groupe de sécurité agit comme un pare-feu virtuel pour votre instance afin de contrôler le trafic entrant et sortant. Pour créer un groupe de sécurité, complétez les champs ci-dessous.

Détails de base

Nom du groupe de sécurité [Informations](#)

Web Security Group

Le nom ne peut pas être modifié après sa création.

Description [Informations](#)

Enable HTTP access

VPC [Informations](#)

vpc-04519aa2f7e35ff06 (capstone-vpc)

- Rules we added : HTTPS, HTTP

The screenshot shows the 'Règles entrantes' (Inbound rules) section of the AWS Management Console. It features a table with columns: Type, Protocole, Plage de ports, Source, and Description - facultatif. Two rules are listed: HTTP (port 80) and HTTPS (port 443), both with source 0.0.0.0/0. Each rule has a 'Supprimer' (Delete) button. An 'Ajouter une règle' (Add rule) button is at the bottom left.

VPC [Informations](#)

vpc-04519aa2f7e35ff06 (capstone-vpc)

Règles entrantes [Informations](#)

Type Informations	Protocole Informations	Plage de ports Informations	Source Informations	Description - facultatif Informations	
HTTP	TCP	80	N'imp... 0.0.0.0/0 X	Permit web requests	Supprimer
HTTPS	TCP	443	N'imp... 0.0.0.0/0 X	Permit web requests	Supprimer

Ajouter une règle

We will add the incoming **SSH** rule to be able to access our virtual machine

CAPSTONE PROJECT DOCUMENTATION

✓ Le groupe de sécurité (sg-0d07bb00c0caad322 | Web Security Group) a été créé avec succès.

► Détails

VPC > Groupes de sécurité > sg-0d07bb00c0caad322 - Web Security Group

sg-0d07bb00c0caad322 - Web Security Group

Actions ▼

Détails

Nom du groupe de sécurité Web Security Group	ID du groupe de sécurité sg-0d07bb00c0caad322	Description Enable HTTP access	ID de VPC vpc-04519aa2f7e35ff06
Propriétaire 232341200515	Nombre de règles entrantes 2 Entrées d'autorisation	Nombre de règles sortantes 1 Entrée d'autorisation	

Well !

- Db server group : Permit access from Web Security Group

sg-08951da71f5ce92fb - DB Server Group

Actions ▼

Détails

Nom du groupe de sécurité DB Server Group	ID du groupe de sécurité sg-08951da71f5ce92fb	Description Enable access to DB	ID de VPC vpc-04519aa2f7e35ff06
Propriétaire 232341200515	Nombre de règles entrantes 1 Entrée d'autorisation	Nombre de règles sortantes 1 Entrée d'autorisation	

Règles entrantes Règles sortantes Balises

Règles entrantes (1)

Recherche

	Name	ID de règle de grou...	Version IP	Type	Protocole	Plage de port
<input type="checkbox"/>	-	sgr-08ba30ac15b76dd...	-	PostgreSQL	TCP	5432

- Rules : We specify the web security group

aws Services Rechercher [Alt+S] Virginie du Nord voclabs/user3035602=iptissem_ZITOUNI @ 2323-4120-05

VPC > Groupes de sécurité > sg-08951da71f5ce92fb - DB Server Group > Modifier les règles entrantes

Modifier les règles entrantes

Les règles entrantes contrôlent le trafic entrant qui est autorisé à atteindre l'instance.

Règles entrantes

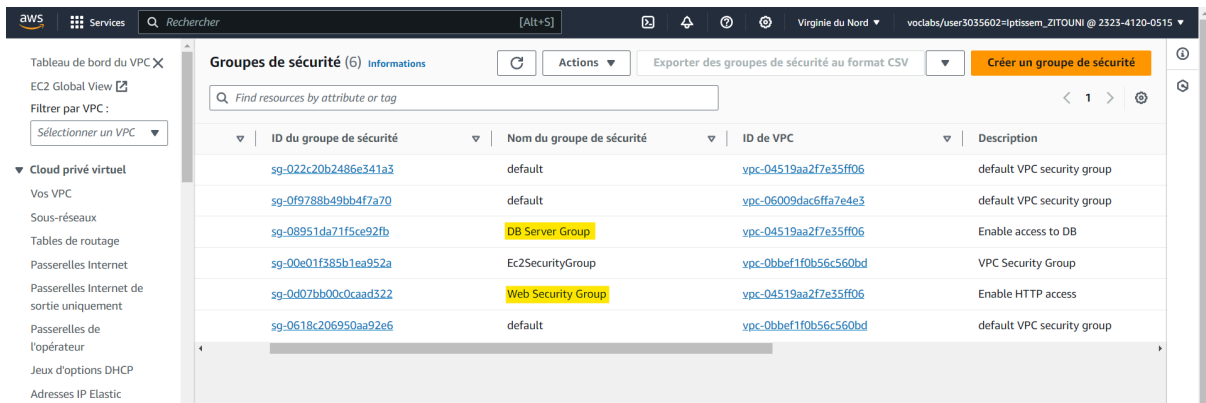
ID de règle de groupe de sécurité	Type	Protocole	Plage de ports	Source	Description - facultatif
sgr-08ba30ac15b76dd48	PostgreSQL	TCP	5432	Perso... sg-0d07bb00c0caad322	

Ajouter une règle

Annuler Aperçu des modifications Enregistrer les règles

CAPSTONE PROJECT DOCUMENTATION

Our security groups are well created and active :



The screenshot shows the AWS IAM console 'Groupes de sécurité' page. It lists six security groups with their IDs, names, VPC IDs, and descriptions. The 'DB Server Group' and 'Web Security Group' are highlighted in yellow.

ID du groupe de sécurité	Nom du groupe de sécurité	ID de VPC	Description
sg-022c20b2486e341a3	default	vpc-04519aa2f7e35ff06	default VPC security group
sg-0f9788b49bb4f7a70	default	vpc-06009dac6ffa7e4e3	default VPC security group
sg-08951da71f5ce92fb	DB Server Group	vpc-04519aa2f7e35ff06	Enable access to DB
sg-00e01f385b1ea952a	Ec2SecurityGroup	vpc-0bbe1f0b56c560bd	VPC Security Group
sg-0d07bb00c0caad322	Web Security Group	vpc-04519aa2f7e35ff06	Enable HTTP access
sg-0618c206950aa92e6	default	vpc-0bbe1f0b56c560bd	default VPC security group

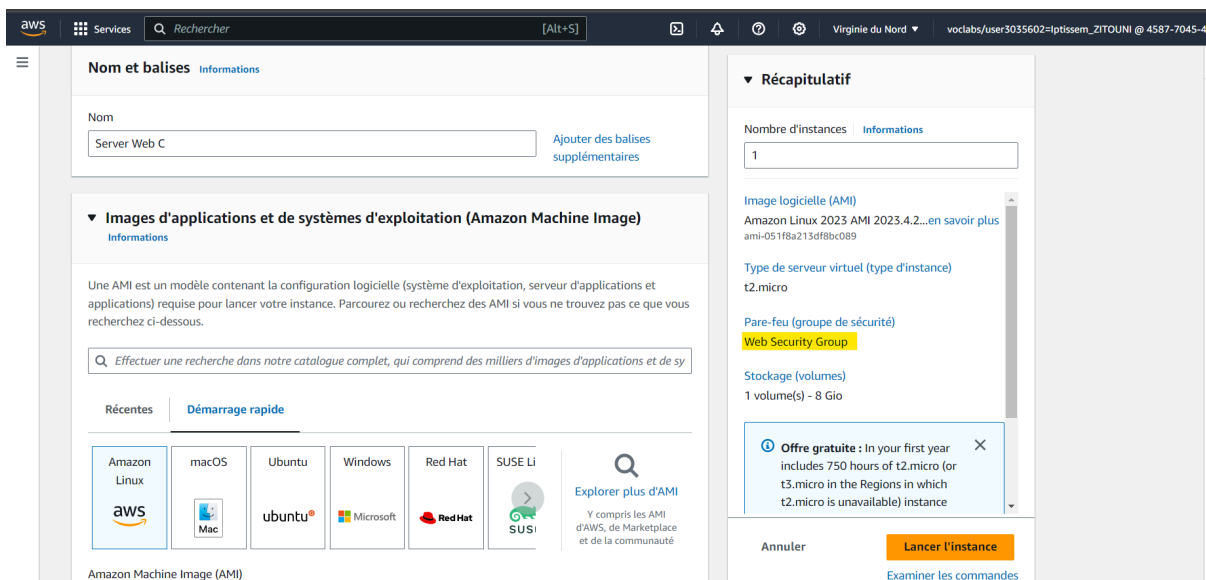
IV. Launch a Web Server Instance

Our instance is virtual machine configured to host websites or web applications, serving content to users accessing it through their web browsers over the Internet.

Here, we are going to deploy a website.

In our AWS console, we go to Instance/Launch Instance: there is more information to complete.

We assign to our server the web security group create earlier



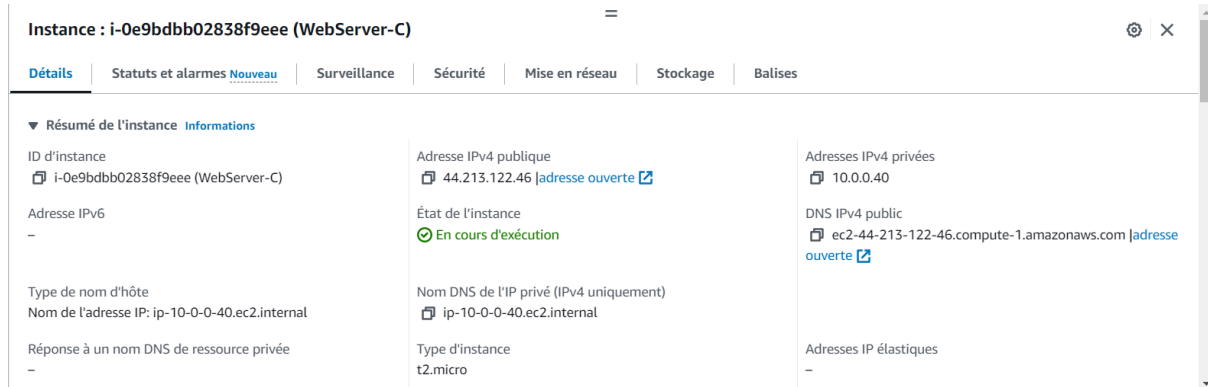
The screenshot shows the 'Launch Instance' wizard in the AWS console. The 'Nom et balises' section has 'Server Web C' as the name. The 'Images d'applications et de systèmes d'exploitation' section shows 'Amazon Linux 2023.4.2' as the selected AMI. The 'Type de serveur virtuel' is 't2.micro'. The 'Pare-feu (groupe de sécurité)' is 'Web Security Group'. The 'Stockage (volumes)' section shows '1 volume(s) - 8 Gio'. A 'Récapitulatif' section on the right summarizes these choices. A 'Lancer l'instance' button is visible at the bottom right.

CAPSTONE PROJECT DOCUMENTATION

Our server has been created.

A public IP address is assigned to enable users to access it over the Internet, facilitating the routing of requests from internet users to the server for web content delivery.

It is with this one that we will access our site



To deploy our site, we had two solutions: either with a script, or with hands. We chose the second solution here.

We first install git to retrieve our files and httpd which is the apache server.

```
[ec2-user@ip-20-0-0-62 ~]$ sudo yum install git
Last metadata expiration check: 0:12:37 ago on Mon Apr  8 14:10:52 2024.
Dependencies resolved.
```

```
[ec2-user@ip-20-0-0-62 ~]$ sudo yum install httpd
Last metadata expiration check: 0:12:49 ago on Mon Apr  8 14:10:52 2024.
Dependencies resolved.
```

Package	Arch	Version	Repository	Size
---------	------	---------	------------	------

Then, we git clone our project and copy our site in /var/www/html/

```
[ec2-user@ip-20-0-0-62 ~]$ git clone https://github.com/iptissem/capstone.git
Cloning into 'capstone'...
[ec2-user@ip-10-0-0-40 capstone]$ ls
sample-app
[ec2-user@ip-10-0-0-40 capstone]$ cd sample-app/
[ec2-user@ip-10-0-0-40 sample-app]$ ls
assets  css  index.html  js
[ec2-user@ip-10-0-0-40 sample-app]$ sudo cp -r * /var/www/html/
[ec2-user@ip-10-0-0-40 sample-app]$ sudo systemctl start httpd
[ec2-user@ip-10-0-0-40 sample-app]$
```

We restart our httpd service and our web server is configured.

You can also check the server status by doing a `systemctl status httpd`: it is running.

We refresh our instance.

Résumé de l'instance pour i-0e9bdbb02838f9eee
(WebServer-C) [Informations](#)

 Se connecter État de l'instance ▼



Actions ▼

Mis à jour il y a 1 minute

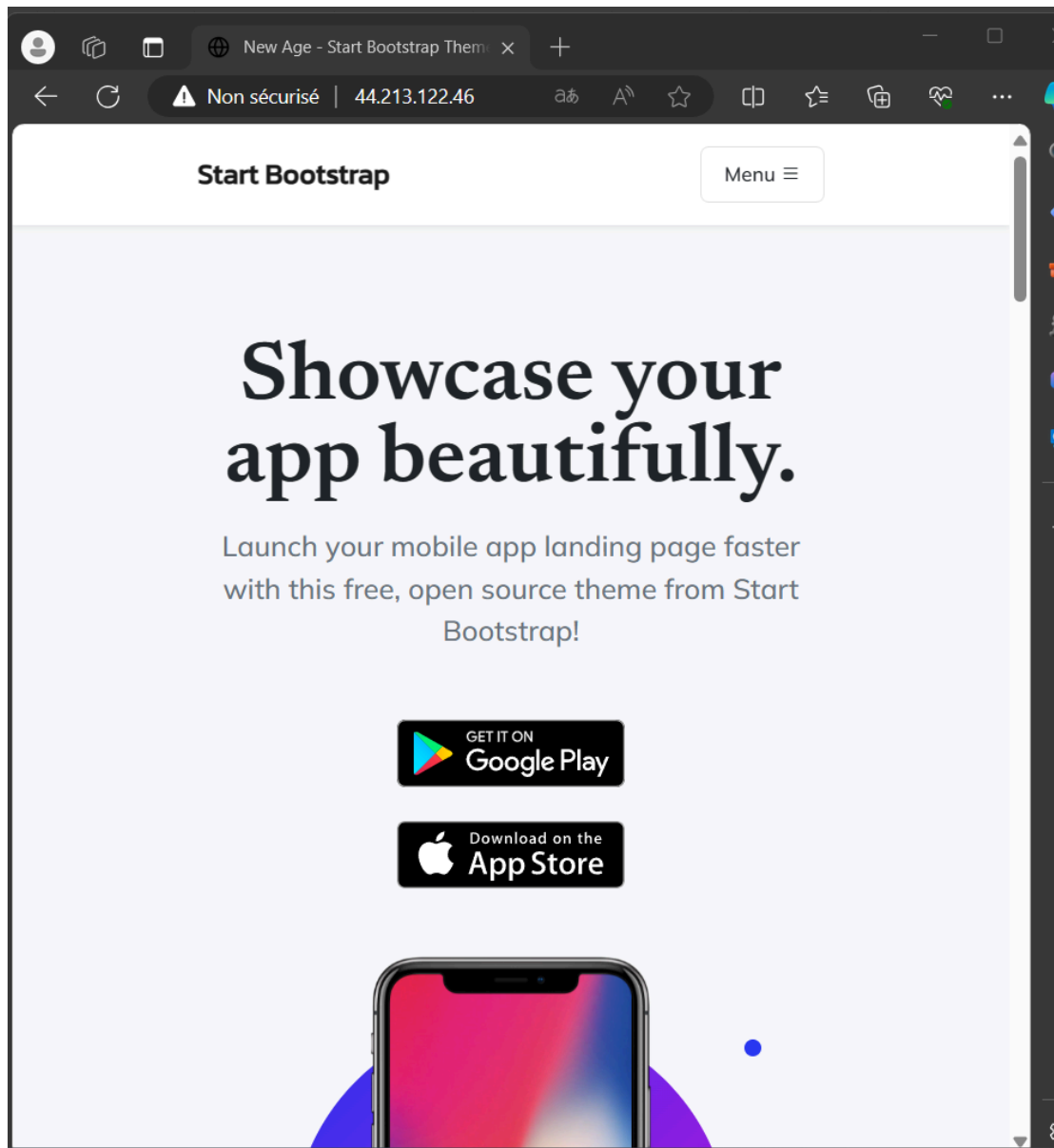
ID d'instance

 i-0e9bdbb02838f9eee (WebServer-C)

Adresse IPv4 publique

 44.213.122.46 [adresse ouverte](#) 

We put our IP in browser : succes !

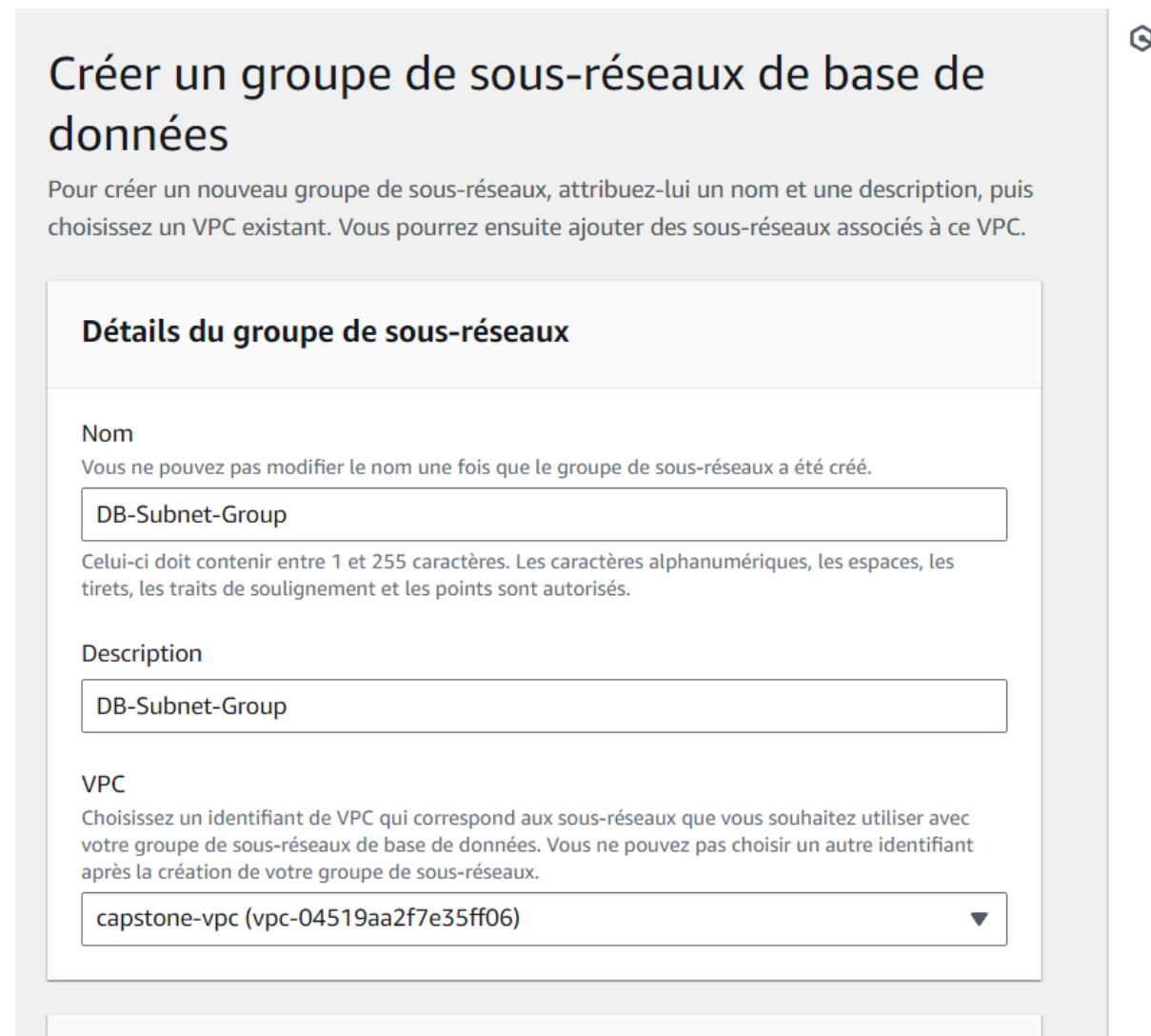


IV. Build our Database

Amazon RDS (Relational Database Service) is a managed database service that simplifies database setup, operation, and scaling in the cloud, offering support for various relational database engines.

We will use postgresSQL.

4. Create a DB 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.

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

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.

We select the subnets associated with the CIDR ranges **10.0.1.0/24**

5. Create an Amazon RDS DB Instance

database creation :

[RDS](#) > Créer une base de données

Créer une base de données


Choisir une méthode de création de bases de données [Infos](#)


☒ **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 [Infos](#)

☐ Aurora (MySQL Compatible)


☒ Aurora (PostgreSQL Compatible)


We then configured our fields, the most important :

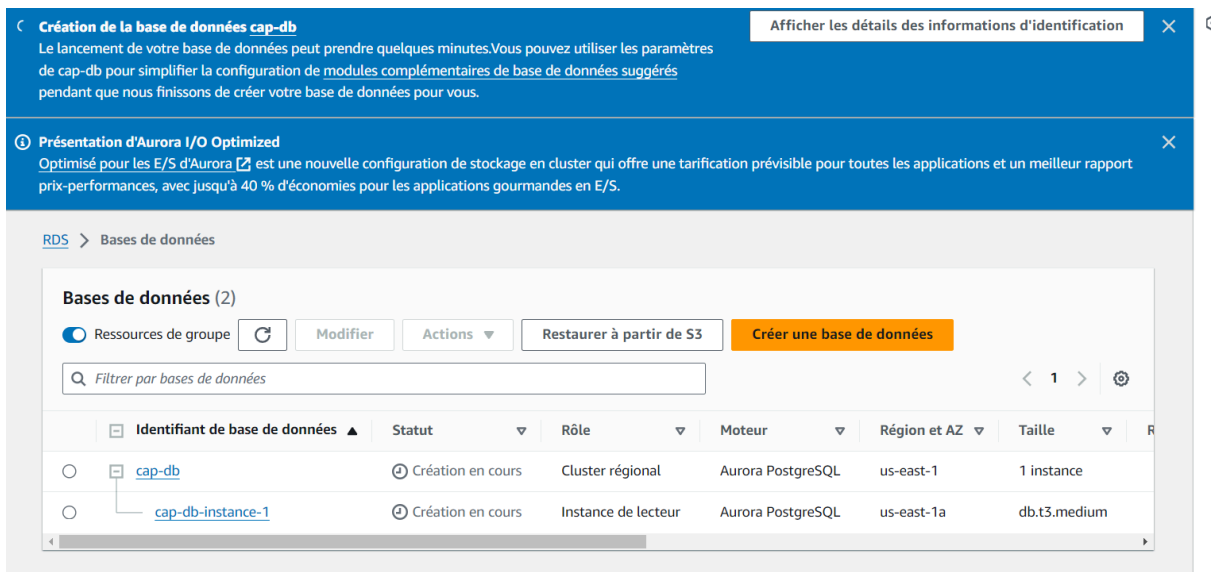
DB instance identifier: cap-db

Initial database name: cap

password

VPC

Make sure your database is public.



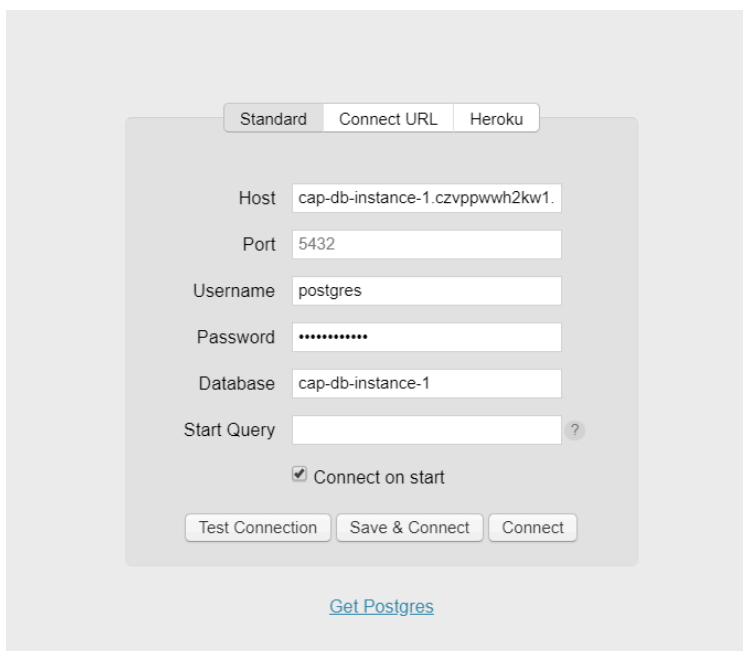
Our database has been created.

V. Testing Database

For testing our job we are going to use postbird : a PostgreSQL client application that provides a user-friendly interface for managing PostgreSQL databases and executing queries.

For these we have to find our endpoint in cap-db-instance-1. :

cap-db.cluster-czvppwwh2kw1.us-east-1.rds.amazonaws.com



VI. Conclusion

After several tests, we can not reach our two hosts

Here are the tests done to try debug:

Check our VPCs,

that the database is public,

We have carefully selected our networks and security group.