
Projet DevOps – Déploiement Automatisé d'une Application Java Multi-Tiers sur AWS

Objectif

Déployer l'application vProfile sur AWS à l'aide de services cloud tels qu'EC2, S3, IAM, Route 53, et le Load Balancer, tout en assurant l'automatisation des tâches d'infrastructure, la scalabilité de l'application et la haute disponibilité du service.

Prérequis

- Un compte AWS opérationnel
- Un utilisateur IAM doté des droits requis pour gérer les ressources AWS (EC2, S3, Route 53, etc.)
- Un terminal compatible (Git Bash ou équivalent) avec accès SSH configuré pour la connexion aux instances EC2

Architecture du projet

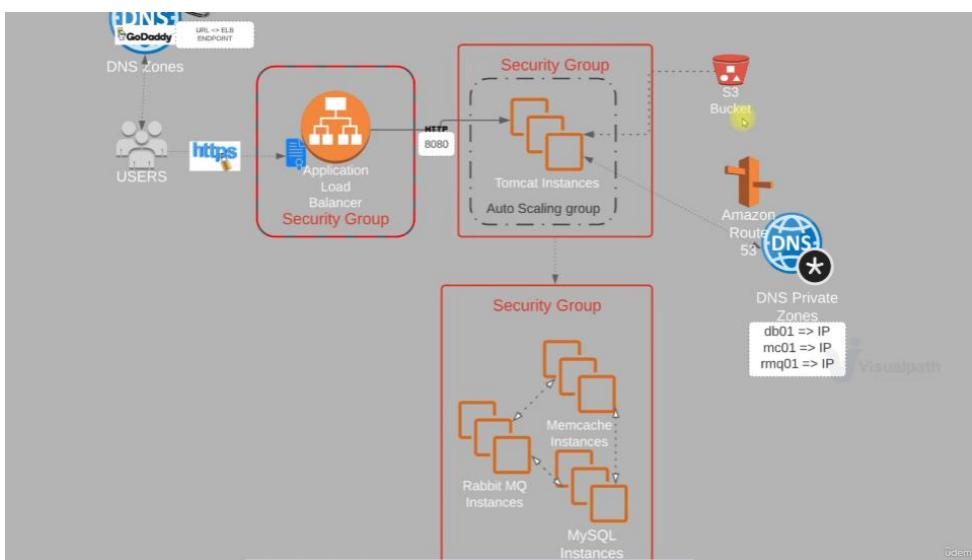


Figure de l'architecture du projet

Création d'une clé de sécurité

Créer une paire de clés Informations

Paire de clés

Une paire de clés, composée d'une clé privée et d'une clé publique, est un ensemble d'informations d'identification de sécurité que vous utilisez pour prouver votre identité lors de la connexion à une instance.

Nom

vprofile-key

Le nom peut avoir un maximum de 255 caractères ASCII. Il ne peut pas inclure d'espaces avant ou après.

Type de paire de clés Informations

RSA

ED25519

Format de fichier de clé privée

.pem

À utiliser avec OpenSSH

.ppk

À utiliser avec PuTTY

1. Générer une paire de clés SSH via AWS (ex : vprofile-key.pem).

- La clé privée est téléchargée localement, et la clé publique est utilisée pour l'accès à l'instance.

Configuration des groupes de sécurité

1. Groupe de sécurité Load Balancer

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

vprofile-ELB-SG

Le nom ne peut pas être modifié après sa création.

Description Informations

vprofile-ELB-SG

VPC Informations

vpc-0dfe9557a0c2a9db3

• Règles entrantes

Règles entrantes Informations

Type Informations

Informations

Protocole Informations

Informations

Plage de ports Informations

Informations

Source Informations

Informations

Description - facultatif Informations

HTTP	TCP	80	N <i>t...</i>	0.0.0.0/0		
HTTP	TCP	80	N <i>t...</i>	:/0		
HTTPS	TCP	443	N <i>t...</i>	0.0.0.0/0		
HTTPS	TCP	443	N <i>t...</i>	:/0		
Ajouter une règle						

HTTPS (port 443) : autorisé depuis n'importe quelle adresse IPv4 ou IPv6

HTTP (port 80) : autorisé depuis n'importe quelle adresse IPv4 ou IPv6

• Règles sortantes

Règles sortantes Informations

Type	Informations	Protocole	Informations	Plage de ports	Informations	Destination	Informations	Description - facultatif	Informations
Tout le trafic	Tous	Tous	Per...	0.0.0.0/0	X	N'i...	:/0	Ajouter une règle	
Tout le trafic	Tous	Tous	N'i...	:/0	X			Supprimer	

Tout le trafic est autorisé

2. Groupe de sécurité pour Tomcat

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
vprofile-app-sg
Le nom ne peut pas être modifié après sa création.

Description Informations
security group for tomcat app server

VPC Informations
vpc-0dfe9557a0c2a9db3

- *Règles entrantes*

Règles entrantes Informations

Type	Informations	Protocole	Informations	Plage de ports	Informations	Source	Informations	Description - facultatif	Informations
TCP personnalisé	TCP	8080	Per...	Q sg-0fbc1f5484b0 X	allow traffic from vprofile load balancer	sg-0fbc1f5484b0c88	f3	allow traffic from vprofile load balancer	Supprimer
TCP personnalisé	TCP	22	Mo...	37.170.255.4/32	X			Ajouter une règle	

- *Règles sortantes*

Règles sortantes Informations

Type	Informations	Protocole	Informations	Plage de ports	Informations	Destination	Informations	Description - facultatif	Informations
Tout le trafic	Tous	Tous	Per...	0.0.0.0/0	X	N'i...	:/0	Ajouter une règle	
Tout le trafic	Tous	Tous	N'i...	:/0	X			Supprimer	

Tout le trafic est autorisé

3. Groupe de sécurité pour le back-end

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](#)

vprofile-backend-sg

Le nom ne peut pas être modifié après sa création.

Description [Informations](#)

security group for mysql, memcache et rabbitmq allow from tomcat app server

VPC Informations

vpc-0dfe9557a0c2a9db3

● Règles entrantes

Règles entrantes [Informations](#)

Type	Informations	Protocole	Plage de ports	Source	Informations	Description - facultatif	Informations	
MySQL/Aurora	Informations	TCP	3306	Per...	<input type="text" value="sg-0641294fc0df62"/> X			Supprimer
TCP personnalisé	Informations	TCP	11211	Per...	<input type="text" value="sg-0641294fc0df62"/> X			Supprimer
TCP personnalisé	Informations	TCP	5672	Per...	<input type="text" value="sg-0641294fc0df62"/> X			Supprimer
TCP personnalisé	Informations	TCP	22	Mo...	<input type="text" value="37.170.255.4/32"/> X			Supprimer
Tout le trafic	Tous	Tous	Tous	Per...	<input type="text" value="sg-0641294fc0df62"/> X			Supprimer
-	Tous	Tous	Tous	Per...	<input type="text" value="sg-0cb0502bec5f"/> X			Supprimer
-	Tous	Tous	Tous	Per...	<input type="text" value="sg-0cb0502bec56b0"/> X			Supprimer
Ajouter une règle								

● Règles sortantes

Règles sortantes [Informations](#)

Type	Informations	Protocole	Plage de ports	Destination	Informations	Description - facultatif	Informations	
Tout le trafic	Tous	Tous	Tous	Per...	<input type="text" value="0.0.0.0/0"/> X			Supprimer
Tout le trafic	Tous	Tous	Tous	Nl...	<input type="text" value="::/0"/> X			Supprimer
Ajouter une règle								

Tout le trafic est autorisé

Création des instances EC2

1. Instance EC2 - MySQL

▼ Nom et balises [Informations](#)

Clé Informations	Valeur Informations	Types de ressources
Name <input type="text" value="vprofile-db01"/>	Informations	Instances <input type="button" value="Supprimer"/>
Sélectionner les ty...		Volumes <input type="button" value="Supprimer"/>
Project <input type="text" value="vprofile"/>	Informations	Instances <input type="button" value="Supprimer"/>
Sélectionner les ty...		Volumes <input type="button" value="Supprimer"/>
Ajouter une balise		

Vous pouvez ajouter jusqu'à 48 balises supplémentaires.

- Choix de la machine

Amazon Linux	macOS	Ubuntu	Windows	Red Hat	SUSE Linux	Explorer plus d'AMI
						Y compris les AMI d'AWS, de Marketplace et de la communauté
Amazon Machine Image (AMI)						Éligible à l'offre gratuite
AMI Amazon Linux 2023 ami-09e6f87aa47905347c (64 bits (x86), uefi-preferred) / ami-0db36bcbb6bf68b98 (64 bits (Arm), uefi) Virtualisation: hvm ENA activé: true Type de périphérique racine: ebs						
Description Amazon Linux 2023 est un système d'exploitation moderne basé sur Linux, à usage général et offrant cinq ans de support garanti. Optimisé pour AWS, il est conçu afin de fournir un environnement d'exécution sécurisé, stable et à hautes performances pour le développement et l'exécution de vos applications cloud.						
Amazon Linux 2023 AMI 2023.7.20250609.0 x86_64 HVM kernel-6.1						
Architecture	Mode de	ID AMI	Date de	Nom		

AMI choisie : AMI Amazon Linux 2023

Nom d'utilisateur SSH par défaut : ec2-user

- Choix de la clé

▼ Paire de clés (connexion) [Informations](#)

Vous pouvez utiliser une paire de clés pour vous connecter en toute sécurité à votre instance. Assurez-vous d'avoir accès à la paire de clés sélectionnée avant de lancer l'instance.

Nom de la paire de clés - obligatoire

vprofile-key

[Créer une paire de clés](#)

Clé SSH : vprofile-key

- Choix de la sécurité du groupe

Pare-feu (groupes de sécurité) [Informations](#)

Un groupe de sécurité est un ensemble de règles de pare-feu qui contrôlent le trafic de votre instance. Ajoutez des règles pour autoriser un trafic spécifique à atteindre votre instance.

[Créer un groupe de sécurité](#)

[Sélectionner un groupe de sécurité existant](#)

Groupes de sécurité courants [Informations](#)

[Sélectionner les groupes de sécurité](#)

vprofile-backend-sg sg-0cb0502bec56b05f9
VPC: vpc-0dfe9557a0c2a9db3

[Comparer les règles de groupe de sécurité](#)

Les groupes de sécurité que vous ajoutez ou supprimez ici seront ajoutés ou supprimés de toutes vos interfaces réseau.

Groupe de sécurité : vprofile-backend-sg

- Code d'automatisation

```

#!/bin/bash
DATABASE_PASS='admin123'
sudo dnf update -y
sudo dnf install git zip unzip -y
sudo dnf install mariadb105-server -y

sudo systemctl start mariadb
sudo systemctl enable mariadb
cd /tmp/
git clone -b main https://github.com/hkhcoder/vprofile-project.git

sudo mysqladmin -u root password "$DATABASE_PASS"
sudo mysql -u root -p"$DATABASE_PASS" -e "ALTER USER 'root'@'localhost'
IDENTIFIED BY '$DATABASE_PASS'"
sudo mysql -u root -p"$DATABASE_PASS" -e "DELETE FROM mysql.user"

```

Les données utilisateur ont déjà été codées en base64

L'integralite du code est disponible dans le fichier *mysql.sh*

2. Instance EC2 – Memcache

▼ Nom et balises [Informations](#)

Clé Informations <input type="text" value="Name"/> X	Valeur Informations <input type="text" value="vprofile-mc01"/> X	Type de ressources Informations Sélectionner les ty... Supprimer
		Instances X
		Volumes X

Clé Informations <input type="text" value="Project"/> X	Valeur Informations <input type="text" value="vprofile"/> X	Type de ressources Informations Sélectionner les ty... Supprimer
		Instances X
		Volumes X

[Ajouter une balise](#)

Vous pouvez ajouter jusqu'à 48 balises supplémentaires.

Pour le *Choix de la machine*, le *Choix de la clé*, et *Choix de la sécurité du groupe* la configuration est la même que celle de l'instance *vprofile-db01*

- Code d'automatisation

[↑ Choisir un fichier](#)

```
#!/bin/bash
sudo dnf install memcached -y
sudo systemctl start memcached
sudo systemctl enable memcached
sudo systemctl status memcached
sed -i 's/127.0.0.1/0.0.0.0/g' /etc/sysconfig/memcached
sudo systemctl restart memcached
sudo memcached -p 11211 -U 11111 -u memcached -d
```

Les données utilisateur ont déjà été codées en base64

L'integralite du code est disponible dans le fichier *memcache.sh*

3. Instance EC2 – RabbitMQ

▼ Nom et balises [Informations](#)

Clé Informations <input type="text"/> Name X	Valeur Informations <input type="text"/> vprofile-rmq01 X	Types de ressources Informations Sélectionner les ty... ▼
		Supprimer
		Instances X
		Volumes X

Clé Informations <input type="text"/> Project X	Valeur Informations <input type="text"/> vprofile X	Types de ressources Informations Sélectionner les ty... ▼
		Supprimer
		Instances X
		Volumes X

[Ajouter une balise](#)

Pour le *Choix de la machine*, le *Choix de la clé*, et *Choix de la sécurité du groupe* la configuration est la même que celle de l'instance *vprofile-db01*

- Code d'automatisation

```
#!/bin/bash

rpm --import 'https://github.com/rabbitmq/signing-keys/releases/
download/3.0/rabbitmq-release-signing-key.asc'

rpm --import 'https://github.com/rabbitmq/signing-keys/releases/
download/3.0/cloudsmith.rabbitmq-erlang.E495BB49CC4BBE5B.key'

rpm --import 'https://github.com/rabbitmq/signing-keys/releases/
download/3.0/cloudsmith.rabbitmq-server.9F4587F226208342.key'
curl -o /etc/yum.repos.d/rabbitmq.repo https://
raw.githubusercontent.com/hkhcoder/vprofile-project/refs/heads/
awsliftandshift/al2023rmq.repo
dnf update -y
```

Les données utilisateur ont déjà été codées en base64

L'integralite du code est disponible dans le fichier *rabbitmq.sh*

4. Instance EC2 – Tomcat

▼ Nom et balises [Informations](#)

Clé Informations	Valeur Informations	Types de ressources
Name	vprofile-app01	Informations
		Sélectionner les ty...
		Supprimer
		Instances X
		Volumes X

Clé Informations	Valeur Informations	Types de ressources
Project	vprofile	Informations
		Sélectionner les ty...
		Supprimer
		Instances X
		Volumes X

[Ajouter une balise](#)

Vous pouvez ajouter jusqu'à 48 balises supplémentaires.

- Choix de la machine

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
ami-020cba7c55df1f615 (64 bits (x86)) / ami-07041441b708acbd6 (64 bits (Arm))
Virtualisation: hvm ENA activé: true Type de périphérique racine: ebs

Éligible à l'offre gratuite ▾

Description

Ubuntu Server 24.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://>)

AMI choisie : Ubuntu Server (dernière LTS recommandée)

Nom d'utilisateur SSH par défaut : ubuntu

- Choix de la clé

▼ **Paire de clés (connexion)** Informations

Vous pouvez utiliser une paire de clés pour vous connecter en toute sécurité à votre instance. Assurez-vous d'avoir accès à la paire de clés sélectionnée avant de lancer l'instance.

Nom de la paire de clés - obligatoire

vprofile-key ▾

[Créer une paire de clés](#)

Clé SSH : vprofile-key

- Choix de la sécurité du groupe

Pare-feu (groupes de sécurité) Informations

Un groupe de sécurité est un ensemble de règles de pare-feu qui contrôlent le trafic de votre instance. Ajoutez des règles pour autoriser un trafic spécifique à atteindre votre instance.

Créer un groupe de sécurité Sélectionner un groupe de sécurité existant

Groupes de sécurité courants Informations

Sélectionner les groupes de sécurité ▾

vprofile-app-sg sg-0641294fc0df629ad X

VPC: vpc-0dfe9557a0c2a9db3

[Comparer les règles de groupe de sécurité](#)

Les groupes de sécurité que vous ajoutez ou supprimez ici seront ajoutés ou supprimés de toutes vos interfaces réseau.

Groupe de sécurité : vprofile-app-sg

- Code d'automatisation

```
#!/bin/bash
sudo apt update
sudo apt upgrade -y
sudo apt install openjdk-17-jdk -y
sudo apt install tomcat10 tomcat10-admin tomcat10-docs tomcat10-
common git -y
```

L'intégralité du code est disponible dans le fichier *tomcat.sh*

💡 État opérationnel des instances EC2

- Vprofile-db01

```
Administrator@DESKTOP-4UKNA42 MINGW64 / 
$ ssh -i ~/Downloads/vprofile-key.pem ec2-user@13.221.129.205
The authenticity of host '13.221.129.205 (13.221.129.205)' can't be established.
ED25519 key fingerprint is SHA256:oeF3ppJTW8IsIdic1T3JU4mYLqTvOjqRwGb/BMxFNHE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '13.221.129.205' (ED25519) to the list of known hosts.

   _#_
  ~\###
  ~\####
  ~\##|
  ~\#/ .__->
  ~\ V~ , _-->
  ~\ .-. . / \
  ~\ / , _/
[ec2-user@ip-172-31-23-34 ~]$ |
```

```
[ec2-user@ip-172-31-23-34 ~]$ sudo -i
[root@ip-172-31-23-34 ~]# systemctl status mariadb
● mariadb.service - MariaDB 10.5 database server
  Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; preset: disabled)
  Active: active (running) since Sat 2025-06-21 23:34:07 UTC; 19min ago
    Docs: man:mariadb(7)
          https://mariadb.com/kb/en/library/systemd/
Main PID: 27479 (mariadb)
  Status: "Taking your SQL requests now..."
      Tasks: 8 (limit: 1111)
     Memory: 67.3M
        CPU: 620ms
       CGroup: /system.slice/mariadb.service
              └─27479 /usr/libexec/mariadb --basedir=/usr

Jun 21 23:34:06 ip-172-31-23-34.ec2.internal mariadb-prepare-db-dir[27436]: The second is mysql@localhost, it has no password either, but
Jun 21 23:34:06 ip-172-31-23-34.ec2.internal mariadb-prepare-db-dir[27436]: you need to be the system 'mysql' user to connect.
Jun 21 23:34:06 ip-172-31-23-34.ec2.internal mariadb-prepare-db-dir[27436]: After connecting you can set the password, if you would need to be
Jun 21 23:34:06 ip-172-31-23-34.ec2.internal mariadb-prepare-db-dir[27436]: able to connect as any of these users with a password and without sudo
Jun 21 23:34:06 ip-172-31-23-34.ec2.internal mariadb-prepare-db-dir[27436]: See the MariaDB Knowledgebase at https://mariadb.com/kb
Jun 21 23:34:06 ip-172-31-23-34.ec2.internal mariadb-prepare-db-dir[27436]: Please report any problems at https://mariadb.org/jira
Jun 21 23:34:06 ip-172-31-23-34.ec2.internal mariadb-prepare-db-dir[27436]: The latest information about MariaDB is available at https://mariadb.org/.
Jun 21 23:34:06 ip-172-31-23-34.ec2.internal mariadb-prepare-db-dir[27436]: Consider joining MariaDB's strong and vibrant community:
Jun 21 23:34:07 ip-172-31-23-34.ec2.internal mariadb-prepare-db-dir[27436]: https://mariadb.org/get-involved/
Jun 21 23:34:07 ip-172-31-23-34.ec2.internal mariadb-prepare-db-dir[27436]: https://mariadb.org/
[root@ip-172-31-23-34 ~]# mysql -u admin -padmin123 accounts
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 14
Server version: 10.5.29-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [accounts]> show tables;
+-----+
| Tables_in_accounts |
+-----+
| role           |
| user           |
| user_role      |
+-----+
3 rows in set (0.000 sec)

MariaDB [accounts]> |
```

Le serveur de base de données MySQL est actif et prêt à recevoir des requêtes.

- Vprofile-mc01

```
Admin@DESKTOP-4UKNA42 MINGW64 /  
$ ssh -i ~/Downloads/vprofile-key.pem ec2-user@54.88.123.122  
The authenticity of host '54.88.123.122 (54.88.123.122)' can't be established.  
ED25519 key fingerprint is SHA256:9irT78g80br5/zMwhI4x0Awxbef98EOFw13r7M4j+tA.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '54.88.123.122' (ED25519) to the list of known hosts.  
      #  
  ~\_\ #####_          Amazon Linux 2023  
  ~~ \_\#####\_\_/  
  ~~  \'##\_\_/  
  ~~  \'#/  ____ https://aws.amazon.com/linux/amazon-linux-2023  
  ~~  V~-' '--->  
  ~~  /  
  ~~ .-. /  
  ~~ /` /  
  ~~ /m .  
[ec2-user@ip-172-31-20-144 ~]$ sudo -i  
[root@ip-172-31-20-144 ~]# systemctl status memcached  
● memcached.service - memcached daemon  
  Loaded: loaded (/usr/lib/systemd/system/memcached.service; enabled; preset: disabled)  
  Active: active (running) since Sat 2025-06-21 23:36:44 UTC; 22min ago  
    Main PID: 5065 (memcached)  
      Tasks: 10 (limit: 1111)  
     Memory: 1.8M  
       CPU: 330ms  
      CGroup: /system.slice/memcached.service  
              └─5065 /usr/bin/memcached -p 11211 -u memcached -m 64 -c 1024 -l 0.0.0.0,::1  
  
Jun 21 23:36:44 ip-172-31-20-144.ec2.internal systemd[1]: Started memcached.service - memcached daemon.  
[root@ip-172-31-20-144 ~]# |
```

Memcache a été correctement installé et répond aux vérifications de bon fonctionnement.

- Vprofile-rmq01

```
[ec2-user@ip-172-31-25-187 ~]$ ssh -i ~/Downloads/vprofile-key.pem ec2-user@44.222.210.222
The authenticity of host '44.222.210.222 (44.222.210.222)' can't be established.
ED25519 key fingerprint is SHA256:ogbvBEcX5YSGmJNxY9HkMDGfFJLACK7Y2ELyq6rve4w.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '44.222.210.222' (ED25519) to the list of known hosts.

[ec2-user@ip-172-31-25-187 ~]$ curl https://aws.amazon.com/linux/amazon-linux-2023
Amazon Linux 2023

[ec2-user@ip-172-31-25-187 ~]$ sudo -i
[root@ip-172-31-25-187 ~]# systemctl status rabbitmq-server
● rabbitmq-server.service - Open source RabbitMQ server
   Loaded: loaded (/usr/lib/systemd/system/rabbitmq-server.service; enabled; preset: disabled)
     Active: active (running) since Sat 2025-06-21 23:42:12 UTC; 19min ago
    Main PID: 26417 (beam.smp)
      Tasks: 23 (limit: 1111)
     Memory: 1.0M
        CPU: 4.445s
       CGroup: /system.slice/rabbitmq-server.service
           └─26417 /usr/lib64/erlang/erts-15.2.7/bin/beam.smp -W w -MBas ageffcbf -MHas ageffcbf -MB1mbcs 512 -Mh1mbcs 512 -MMmcbs 30 -pc unicode -P 1048576 -t 5000000 -z

[root@ip-172-31-25-187 ~]# rabbitmqctl status
  Loaded: loaded (/etc/rabbitmq/rabbitmq-server.config)
  Active: active (running) since Sat 2025-06-21 23:42:12 UTC; 19min ago
  Main PID: 26417 (beam.smp)
    Tasks: 23 (limit: 1111)
   Memory: 1.0M
      CPU: 4.445s
     CGroup: /system.slice/rabbitmq-server.service
         ├─26417 /usr/lib64/erlang/erts-15.2.7/bin/beam.smp -W w -MBas ageffcbf -MHas ageffcbf -MB1mbcs 512 -Mh1mbcs 512 -MMmcbs 30 -pc unicode -P 1048576 -t 5000000 -z
         ├─26420 erl_child_idc:sup 32768
         ├─26445 /usr/lib64/erlang/erts-15.2.7/bin/inet_gethost 4
         ├─26446 /usr/lib64/erlang/erts-15.2.7/bin/inet_gethost 4
         ├─26450 /usr/lib64/erlang/erts-15.2.7/bin/epmd -daemon
         └─26476 /bin/sh -s rabbit_disk_monitor

Jun 21 23:42:11 ip-172-31-25-187.ec2.internal rabbitmq-server[26417]: Doc guides: https://www.rabbitmq.com/docs
Jun 21 23:42:11 ip-172-31-25-187.ec2.internal rabbitmq-server[26417]: Support: https://www.rabbitmq.com/docs/contact
Jun 21 23:42:11 ip-172-31-25-187.ec2.internal rabbitmq-server[26417]: Tutorials: https://www.rabbitmq.com/tutorials
Jun 21 23:42:11 ip-172-31-25-187.ec2.internal rabbitmq-server[26417]: Monitoring: https://www.rabbitmq.com/docs/monitoring
Jun 21 23:42:11 ip-172-31-25-187.ec2.internal rabbitmq-server[26417]: Upgrading: https://www.rabbitmq.com/docs/upgrade
Jun 21 23:42:11 ip-172-31-25-187.ec2.internal rabbitmq-server[26417]: Logs: /var/log/rabbitmq/rabbit@ip-172-31-25-187.log
Jun 21 23:42:11 ip-172-31-25-187.ec2.internal rabbitmq-server[26417]: <stdout>
Jun 21 23:42:11 ip-172-31-25-187.ec2.internal rabbitmq-server[26417]: Config file(s): /etc/rabbitmq/rabbitmq.config
Jun 21 23:42:12 ip-172-31-25-187.ec2.internal rabbitmq-server[26417]: Starting broker... completed with 0 plugins.
Jun 21 23:42:12 ip-172-31-25-187.ec2.internal systemd[1]: Started rabbitmq-server.service - Open source RabbitMQ server.
[lines 1-25/25 (END)]
```

Le service RabbitMQ est opérationnel et fonctionne comme attendu.

Configuration DNS avec Route 53

• Creation de la zone d'hébergement

Configuration de la zone hébergée

Une zone hébergée est un conteneur qui contient des informations sur la façon dont vous souhaitez acheminer le trafic pour un domaine (tel que exemple.com) et ses sous-domaines.

Nom de domaine

Nom du domaine pour lequel vous souhaitez acheminer le trafic.

vprofile.in

Caractères valides : a-z, 0-9, !* # \$ % & ' { } * + , - / ; < = > ? @ [\] ^ _ ` { }) . -

Description - facultatif

Cette valeur vous permet de distinguer les zones hébergées portant le même nom.

La zone hébergée est utilisée pour...

La description ne peut pas comporter plus de 256 caractères. 0/256

Nom du domaine : vprofile.in

Type

Le type indique si vous souhaitez acheminer le trafic sur Internet ou dans un VPC Amazon.

Zone hébergée publique

Une zone hébergée publique détermine la façon dont le trafic est acheminé sur Internet.

Zone hébergée privée

Une zone hébergée privée détermine la façon dont le trafic est acheminé au sein d'un Amazon VPC.

Choix de la zone : Zone hébergée privée

VPC à associer à la zone hébergée

Pour utiliser cette zone hébergée et résoudre les requêtes DNS concernant un ou plusieurs VPC, sélectionnez les VPC. Pour associer un VPC à une zone hébergée lorsque le VPC a été créé à l'aide d'un autre compte AWS, vous devez utiliser une méthode de programmation telle que l'interface de ligne de commande AWS.

 Pour chaque VPC que vous associez à une zone hébergée privée, vous devez définir les paramètres du VPC Amazon [enableDnsHostnames](#) et [enableDnsSupport](#) sur true. 

Région

USA Est (Virginie du Nord)

ID de VPC

vpc-0dfe9557a0c2a9db3



[Supprimer un VPC](#)

[Ajouter un VPC](#)

Choisis une région et sélectionne l'id de vpc proposé

1. MySQL – db01

Créer un enregistrement [Infos](#)

Créer rapidement un enregistrement

▼ Enregistrement 1

Nom de l'enregistrement [Infos](#) db01 .vprofile.in
Laissez vide pour créer un enregistrement pour le domaine racine.

Type d'enregistrement [Infos](#) A - Achemine le trafic vers une adresse IPv4 et certaines ressources AWS.

Alias

Valeur [Infos](#) 172.31.23.34

Passer à l'assistant Supprimer

Récupérer IPv4 privé de l'instance vprofile-db01

2. Memcache – mc01

Créer rapidement un enregistrement

▼ Enregistrement 1

Nom de l'enregistrement [Infos](#) mc01 .vprofile.in
Laissez vide pour créer un enregistrement pour le domaine racine.

Type d'enregistrement [Infos](#) A - Achemine le trafic vers une adresse IPv4 et certaines ressources AWS.

Alias

Valeur [Infos](#) 172.31.20.144
Entrez plusieurs valeurs sur des lignes distinctes.

Durée de vie (secondes) [Infos](#) Stratégie de routage [Infos](#)

Passer à l'assistant Supprimer

Récupérer IPv4 privé de l'instance vprofile-mc01

3. Rabbit MQ – rmq01

Créer rapidement un enregistrement

▼ Enregistrement 1

Nom de l'enregistrement [Infos](#) rmq01 .vprofile.in
Laissez vide pour créer un enregistrement pour le domaine racine.

Type d'enregistrement [Infos](#) A - Achemine le trafic vers une adresse IPv4 et certaines ressources AWS.

Alias

Valeur [Infos](#) 172.31.25.187
Entrez plusieurs valeurs sur des lignes distinctes.

Passer à l'assistant Supprimer

Récupérer IPv4 privé de l'instance vprofile-rmq01

Build & Déploiement des artefacts vProfile sur S3

1. Création d'un bucket

Configuration générale

Région AWS

USA Est (Virginie du Nord) us-east-1

Type de compartiment | Infos

Usage général

Recommandé pour la plupart des cas d'utilisation et des modèles d'accès. Les compartiments à usage général sont du type de compartiment S3 d'origine. Ils permettent une combinaison de classes de stockage qui stockent de manière redondante des objets dans plusieurs zones de disponibilité.

Annuaire

Recommandé pour les cas d'utilisation à faible latence. Ces compartiments utilisent uniquement la classe de stockage S3 Express One Zone, qui permet un traitement plus rapide des données au sein d'une seule zone de disponibilité.

Nom du compartiment | Infos

vprofile-project-s3-buckets

Les noms de compartiment doivent comporter de 3 à 63 caractères et être uniques dans l'espace de noms global. Les noms des compartiments doivent également commencer et se terminer par une lettre ou un chiffre. Les caractères valides sont les suivants : a-z, 0-9, points (.) et tirets (-). [En savoir plus](#)

Copier les paramètres depuis un compartiment existant - facultatif

Seuls les paramètres de compartiment dans la configuration suivante sont copiés.

Sélectionner un compartiment

Format : s3://bucket/prefix

Type de compartiment : *Usage général*

Nom du compartiment : Choisis un nom (ex : *vprofile-project-s3-buckets*)

2. Création d'un utilisateur

Détails de l'utilisateur

Nom d'utilisateur

vprofile-s3-admin

Le nom d'utilisateur peut comporter jusqu'à 64 caractères. Caractères valides : A-Z, a-z, 0-9 et+=, @_ - (tiret)

Fournir aux utilisateurs l'accès à la console de gestion AWS - facultatif

Si vous fournissez à une personne l'accès à la console, c'est aux [bonne pratique](#) de gérer leur accès dans IAM Identity Center.

 En cas de création d'un accès par programmation à AWS CodeCommit ou Amazon Keyspaces via des clés d'accès ou des informations d'identification spécifiques à un service, vous pourrez les générer après avoir créé cet utilisateur IAM. [En savoir plus](#)

Annuler

Suivant

Nom d'utilisateur : vprofile-s3-admin

Options d'autorisations

Ajouter un utilisateur à un groupe

Ajouter un utilisateur à un groupe existant ou créer un nouveau groupe. Nous vous recommandons d'utiliser des groupes pour gérer les autorisations utilisateur par fonction de tâche.

Copier les autorisations

Copiez toutes les appartenances à un groupe, les politiques gérées attachées et les politiques en ligne à partir d'un utilisateur existant.

Attacher directement des politiques

Attacher une politique gérée directement à un utilisateur. La bonne pratique consiste à attacher des politiques à un groupe à la place. Ensuite, ajouter l'utilisateur au groupe approprié.

Politiques des autorisations (1/1364)



[Créer une politique](#)

Choisissez une ou plusieurs politiques à attacher à votre nouvel utilisateur.

Filtrer par Type			
	Nom de la politique	Type	Entités attachées
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	Gérées par AWS	0
<input checked="" type="checkbox"/>	AmazonS3FullAccess	Gérées par AWS	0
<input type="checkbox"/>	AmazonS3ObjectLambdaEx...	Gérées par AWS	0
<input type="checkbox"/>	AmazonS3OutpostsFullAcc...	Gérées par AWS	0
<input type="checkbox"/>	AmazonS3OutpostsReadO...	Gérées par AWS	0
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	Gérées par AWS	0
<input type="checkbox"/>	AmazonS3TablesFullAccess	Gérées par AWS	0

Accorder tous les accès à l'utilisateur

3. Création d'une clé de connexion

Cas d'utilisation

Interface de ligne de commande (CLI)

Vous prévoyez d'utiliser cette clé d'accès pour permettre à AWS CLI d'accéder à votre compte AWS.

Code local

Vous prévoyez d'utiliser cette clé d'accès pour permettre au code d'application dans un environnement de développement local d'accéder à votre compte AWS.

Application exécutée sur un service de calcul AWS

Vous prévoyez d'utiliser cette clé d'accès pour permettre au code d'application s'exécutant sur un service de calcul AWS comme Amazon EC2, Amazon ECS ou AWS Lambda d'accéder à votre compte AWS.

Service tiers

Créer une clé pour le CLI

4. Création d'un rôle

IAM > Rôles > Créer un rôle

- Étape 1
 Sélectionner une entité de confiance
 Étape 2
 Ajouter des autorisations
 Étape 3
 Nommer, vérifier et créer

Sélectionner une entité de confiance Infos

Type d'entité approuvée

Service AWS
Autorisez les services AWS tels qu'EC2, Lambda ou autre à effectuer des actions dans ce compte.

Identité Web
Permet aux utilisateurs fédérés par le fournisseur d'identité web externe spécifié d'assumer ce rôle pour effectuer des actions dans ce compte.

Compte AWS

Autorisez les entités d'autres comptes AWS qui appartiennent à vous à un tiers à effectuer des actions dans ce compte.

Fédération SAML 2.0

Autorisez les utilisateurs fédérés avec SAML 2.0 à partir d'un répertoire d'entreprise à effectuer des actions dans ce compte.

Cas d'utilisation

Autorisez un service AWS comme EC2, Lambda ou autres à effectuer des actions dans ce compte.

Service ou cas d'utilisation

EC2

Choisissez un cas d'utilisation pour le service spécifié.

Cas d'utilisation

EC2

Allows EC2 instances to call AWS services on your behalf.

EC2 Role for AWS Systems Manager

Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

EC2 Spot Fleet Role

Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

EC2 - Spot Fleet Auto Scaling

Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

EC2 - Spot Fleet Tagging

5. Association du rôle et de l'instance vprofile-app01

The screenshot shows the AWS EC2 Instances page. A dropdown menu is open over instance 'vprofile-app01' (ID: i-039c12c2d0a6ac830), with the option 'Modifier le rôle IAM' selected. Below the dropdown, the instance details are shown: ID i-039c12c2d0a6ac830, Public IP 107.20.40.185 (status: adresse ouverte), and Private IP 172.31.30.13. The 'Actions' tab is highlighted, and the 'Lancer des instances' button is visible at the top right.

Sélectionner l'instance vprofile-app01 pour modifier le rôle IAM

Modifier le rôle IAM

Attachez un rôle IAM à votre instance.

ID d'instance

i-039c12c2d0a6ac830 (vprofile-app01)

Rôle IAM

Sélectionner un rôle IAM à attacher à votre instance ou créer un rôle si vous n'en avez pas encore créé. Le rôle que vous sélectionnez remplace tous les rôles actuellement attachés à votre instance.

s3-admin

[Créer un nouveau rôle IAM](#)

Annulez

Mettre à jour le rôle IAM

Sélectionner votre rôle et mettre à jour le rôle IAM

6. Déploiement des artefacts vProfile sur S3

```
Admin@DESKTOP-4UKNA42 MINGW64 ~/Downloads/vprofile-project (awsliftandshift)
$ mvn install
```

Installation de maven

```
$ aws configure
AWS Access Key ID [*****MB3S]: AKIAWVDQTYB7NHNMGXP
AWS Secret Access Key [*****GwGJ]: JfCYD+4HKoe3cAJDREctrA9ciaTQbzb2WgqtX2Mp
Default region name [us-east-1]: us-east-1
Default output format [json]: json
```

Configuration d'AWS

```
Admin@DESKTOP-4UKNA42 MINGW64 ~/Downloads/vprofile-project (awsliftandshift)
● $ ls target/
  classes/           generated-test-sources/  maven-status/      test-classes/  vprofile-v2.war
  generated-sources/  maven-archiver/          surefire-reports/  vprofile-v2/
 
Admin@DESKTOP-4UKNA42 MINGW64 ~/Downloads/vprofile-project (awsliftandshift)
● $ aws s3 cp target/vprofile-v2.war s3://vprofile-project-s3-buckets/
  upload: target\vprofile-v2.war to s3://vprofile-project-s3-buckets/vprofile-v2.war

Admin@DESKTOP-4UKNA42 MINGW64 ~/Downloads/vprofile-project (awsliftandshift)
```

Mise à jour du bucket

```
Admin@DESKTOP-4UKNA42 MINGW64 /
$ ssh -i ~/Downloads/vprofile-key.pem ubuntu@107.20.40.185
The authenticity of host '107.20.40.185 (107.20.40.185)' can't be established.
ED25519 key fingerprint is SHA256:WIXsZIHfIJ5WPdmNYDoaPDpzK9P2ACaKrLrjraAcFBw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '107.20.40.185' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-1029-aws x86_64)

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

System information as of Sun Jun 22 02:05:45 UTC 2025

System load:  0.08           Processes:          106
Usage of /:   38.4% of 6.71GB  Users logged in:    0
Memory usage: 32%           IPv4 address for enX0: 172.31.30.13
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

5 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

```
ubuntu@ip-172-31-30-13:~$ sudo -i
root@ip-172-31-30-13:~# |
```

Lancement de la machine *vprofile-app01*

```
ubuntu@ip-172-31-30-13:~$ sudo -i
root@ip-172-31-30-13:~# snap install aws-cli --classic
aws-cli (v2/stable) 2.27.40 from Amazon Web Services (aws✓) installed
root@ip-172-31-30-13:~#
```

Installation d'aws-cli sur la machine *vprofile-app01*

Redirection du trafic via Load Balancer & Route 53

1. Configuration du groupe cible (Target Group)



Étape 1
 Spécifier les informations de groupe
 Étape 2
 Enregistrer les cibles

Spécifier les informations de groupe
 Votre équilibrEUR de charge achemine les demandes vers les cibles d'un groupe cible et effectUE des vErifications de l'Etat sur les cibles.

Configuration de base
 Les parametres de cette section ne peuvent pas tre modifiEs aprEs la crEation du groupe cible.

Choisir un type de cible

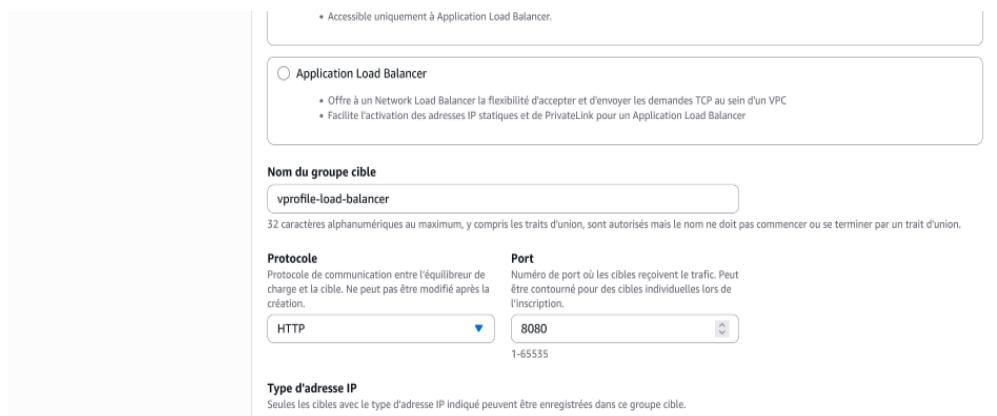
Instances

- Prend en charge l'quilibrEUR de charge dans les instances dans un VPC spEcifique.
- Facilite l'utilisation d'Amazon EC2 Auto Scaling pour gErer et mettre l'echelle votre capacite EC2.

Adresses IP

- Prend en charge l'quilibrEUR de charge sur les ressources VPC et sur site.
- Facilite le routage vers plusieurs adresses IP et interfaces rEseau sur la mEme instance.
- Offre une flexibilite avec les architectures basEes sur des microservices, ce qui simplifie la communication entre les applications.
- Prend en charge les cibles IPv6, ce qui permet la communication IPv6 de bout en bout et le protocole NAT IPv4-to-IPv6.

Choix type cible : Instances



* Accessible uniquement l'Application Load Balancer.

Application Load Balancer

- Offre un Network Load Balancer la flexibilite d'accepter et d'envoyer les demandes TCP au sein d'un VPC
- Facilite l'activation des adresses IP statiques et de PrivateLink pour un Application Load Balancer

Nom du groupe cible
 vprofile-load-balancer

32 caracteres alphanumEriques au maximum, y compris les traits d'union, sont autorisEs mais le nom ne doit pas commencer ou se terminer par un trait d'union.

Protocole
 Protocole de communication entre l'quilibrEUR de charge et la cible. Ne peut pas tre modifiE aprEs la crEation.

Port
 NumEro de port oU les cibles reoivent le trafic. Peut tre contournE pour des cibles individuelles lors de l'inscription.

HTTP 8080 1-65535

Type d'adresse IP
 Seules les cibles avec le type d'adresse IP indiquE peuvent tre enregistrEes dans ce groupe cible.
 ...

Choisir un nom de groupe cible et Mettre le port 8080

Paramètres avancés de vérification de l'état

Port de vérification de l'état
Le port utilisé par l'équilibrEUR de charge lors de l'exécution des surveillances de l'état sur les cibles. Par défaut, le port de surveillance de l'état est le même que le port de trafic du groupe cible. Cependant, vous pouvez spécifier un port différent pour le remplacer.

Port du trafic
 Remplacer
 8080
 1-65535

Seuil de bonne santé
Le nombre de vérifications consécutives réussies de l'état à partir duquel une cible défectueuse est considérée comme saine.

5
2-10

Seuil de défectuosité
Le nombre d'échecs consécutifs de vérification de l'état à partir duquel une cible est considérée comme défectueuse.

Dans les paramètres avancés, mettre le port de vérification de l'état à Remplacer et le mettre à 8080

2. Création du Load Balancer

Instances disponibles (1/4)

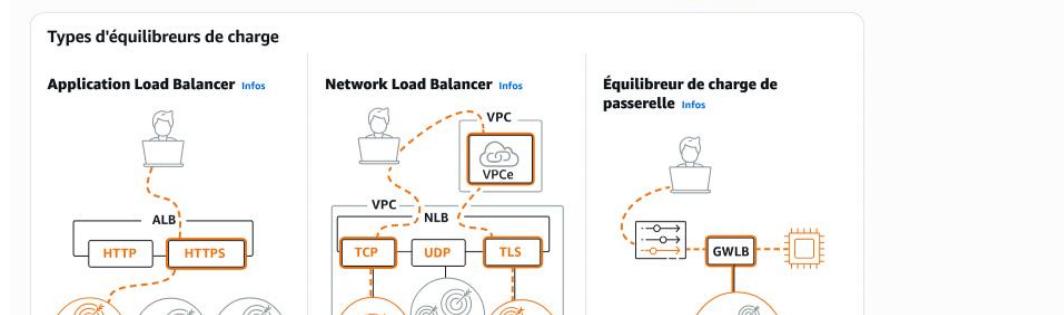
Filtrer instances	ID d'instance	Nom	État	Groupes de sécurité
<input checked="" type="checkbox"/>	i-039c12c2d0a6ac830	vprofile-app01	En cours d'exécution	vprofile-app-sg
<input type="checkbox"/>	i-0c651877f4341b97b	vprofile-rmq01	En cours d'exécution	vprofile-backend-sg
<input type="checkbox"/>	i-0858a02497ca3381d	vprofile-mc01	En cours d'exécution	vprofile-backend-sg
<input type="checkbox"/>	i-03ec7f1cc149b07ee	vprofile-db01	En cours d'exécution	vprofile-backend-sg

1 sélectionnés

Ports pour les instances sélectionnées
Ports de routage du trafic vers les instances

Comparer et sélectionner le type d'équilibrEUR de charge

Une comparaison complète fonction par fonction ainsi que les éléments principaux détaillés sont également disponibles. [En savoir plus](#)



Groupes d'adresses IP - nouveau [Infos](#)

Vous pouvez choisir de configurer un groupe IPAM comme source préférée pour les adresses IP de vos équilibreurs de charge. Créez ou consultez Groupes dans la [console du gestionnaire d'adresses IP d'Amazon VPC](#).

Utiliser le groupe IPAM pour les adresses IPv4 publiques

Le groupe IPAM que vous choisissez sera la source préférée d'adresses IPv4 publiques. Si le groupe est éprouvé, les adresses IPv4 seront attribuées par AWS.

Zones de disponibilité et sous-réseaux [Infos](#)

Selectionnez au moins deux zones de disponibilité et un sous-réseau pour chaque zone. Un nœud d'équilibrage de charge sera placé dans chaque zone sélectionnée et mettra automatiquement à l'échelle en fonction du trafic. L'équilibrleur de charge achemine le trafic vers les cibles situées dans les zones de disponibilité sélectionnées uniquement.

us-east-1a (use1-az1)

Sous-réseau
Seuls les blocs d'adresse CIDR correspondant au type d'adresse IP de l'équilibrleur de charge sont utilisés. Au moins 8 adresses IP disponibles sont nécessaires pour que votre équilibrleur de charge puisse être mis à l'échelle de manière efficace.

subnet-0b168ec76e0a6e726
CIDR du sous-réseau IPv4 : 172.31.0.0/20

us-east-1b (use1-az2)

Sous-réseau
Seuls les blocs d'adresse CIDR correspondant au type d'adresse IP de l'équilibrleur de charge sont utilisés. Au moins 8 adresses IP disponibles sont nécessaires pour que votre équilibrleur de charge puisse être mis à l'échelle de manière efficace.

subnet-01bf29210397a1e15

Groupes de sécurité [Infos](#)

Un groupe de sécurité est un ensemble de règles de pare-feu qui contrôlent le trafic vers votre équilibrleur de charge. Sélectionnez un groupe de sécurité existant ou vous pouvez [créer un nouveau groupe de sécurité](#).

Groupes de sécurité

Sélectionner jusqu'à 5 groupes de sécurité

vprofile-ELB-SG
sg-0fb1f5484b0c88f3 VPC: vpc-0dfe9557a0c2a9db3

Écouteurs et routage [Infos](#)

Un écouteur est un processus qui vérifie les demandes de connexion à l'aide du port et du protocole que vous configurez. Les règles que vous définissez pour un écouteur déterminent la façon dont l'équilibrleur de charge achemine les demandes vers ses cibles enregistrées.

▼ Écouteur HTTP:8080

Supprimer

Protocole	Port	Action par défaut
HTTP	8080	Réacheminer vers vprofile-load-balancer HTTP
		Type de cible: Instance, IPv4
		Créer un groupe cible

Balises d'écouteur - facultatif
Envisagez d'ajouter des balises à votre écouteur. Les balises permettent de classer vos ressources AWS afin de les gérer plus facilement.

Ajouter une balise d'écouteur
Vous pouvez ajouter jusqu'à 50 balises de plus.

Créer une image de l'instance vprofile-app01 et la choisir à ce niveau comme AMI

▼ Images d'applications et de systèmes d'exploitation (Amazon Machine Image) [Informations](#)

Une AMI est un modèle contenant la configuration logicielle (système d'exploitation, serveur d'applications et applications) requise pour lancer votre instance. Parcourez ou recherchez des AMI si vous ne trouvez pas ce que vous recherchez ci-dessous.

Effectuer une recherche dans notre catalogue complet, qui comprend des milliers d'images d'applications et de systèmes

Récentes **Mes AMI** **Démarrage rapide**

Ne pas inclure dans le modèle de lancement M'appartenant

Partagé avec moi

Explorer plus d'AMI
Y compris les AMI d'AWS, de Marketplace et de la communauté

Amazon Machine Image (AMI)
vprofile-app-img
ami-086f81d83e9f71524

▼ Type d'instance [Informations](#) | [Obtenez des conseils](#)

Avancé

Type d'instance

t2.micro

Famille: t2 1 vCPU 1 Gio Mémoire Génération actuelle: true
À la demande Windows base tarification: 0.0162 USD par heure
À la demande Ubuntu Pro base tarification: 0.0134 USD par heure
À la demande SUSE base tarification: 0.0116 USD par heure
À la demande RHEL base tarification: 0.026 USD par heure
À la demande Linux base tarification: 0.0116 USD par heure

Éligible à l'offre gratuite

Toutes les générations

[Comparer les types d'instance](#)

Des frais supplémentaires s'appliquent pour les AMI avec un logiciel préinstallé

▼ Paramètres réseau [Informations](#)

Sous-réseau | [Informations](#)

Ne pas inclure dans le modèle de lancement

[Créer un nouveau sous-réseau](#)

Lorsque vous indiquez un sous-réseau, une interface réseau est automatiquement ajoutée à votre modèle.

Pare-feu (groupes de sécurité) | [Informations](#)

Un groupe de sécurité est un ensemble de règles de pare-feu qui contrôlent le trafic de votre instance. Ajoutez des règles pour autoriser un trafic spécifique à atteindre votre instance.

Sélectionner un groupe de sécurité existant

Créer un groupe de sécurité

[Comparer les règles de groupe de sécurité](#)

Groupes de sécurité | [Informations](#)

[Sélectionner les groupes de sécurité](#)

vprofile-app-sg sg-0641294fc0df629ad [X](#)
VPC: vpc-0dfe9557a0c2a9db3

► Configuration réseau avancée

▼ Balises de ressource [Informations](#)

Clé | [Informations](#)

Name

[X](#)

Valeur | [Informations](#)

vprofile-app

Types de ressources

[Informations](#)

[Sélectionner les ty...](#)

[Supprimer](#)

[Instances](#)

[Volumes](#)

Clé | [Informations](#)

Project

[X](#)

Valeur | [Informations](#)

vprofile

Types de ressources

[Informations](#)

[Sélectionner les ty...](#)

[Supprimer](#)

[Instances](#)

[Ajouter une balise](#)

▼ Détails avancés [Informations](#)

Profil d'instance IAM | [Informations](#)

s3-admin

arn:aws:iam::457650192510:instance-profile/s3-admin

 [Créer un profil IAM](#) 

Type de nom d'hôte | [Informations](#)

Ne pas inclure dans le modèle de lancement

Nom d'hôte DNS | [Informations](#)

Activer les demandes DNS IPv4 (enregistrement A) basées sur les ressources

Activer les demandes DNS IPv6 (enregistrement AAAA) basées sur les ressources



Création de l'Auto Scaling Group – Scalabilité activée

 [EC2](#) > [Groupes Auto Scaling](#) > [Créer un groupe Auto Scaling](#)



Étape 1

Choisir un modèle de lancement

Étape 2

Choisir les options de lancement d'instance

Étape 3 - facultatif

Intégration avec d'autres services

Étape 4 - facultatif

Configurer la taille et la mise à l'échelle du groupe

Étape 5 - facultatif

Ajouter des notifications

Étape 6 - facultatif

Ajouter des identifications

Étape 7

Vérifier

Choisir un modèle de lancement [Info](#)

Spécifiez un modèle de lancement qui contient les paramètres communs à toutes les instances EC2 lancées par ce groupe Auto Scaling.

Nom

Nom du groupe Auto Scaling

Saisissez un nom pour identifier le groupe.

vprofile-app-asg

Doit être unique pour ce compte dans la région actuelle et ne doit pas dépasser 255 caractères.

Modèle de lancement [Info](#)

 Pour les comptes créés après le 31 mai 2023, la console EC2 prend uniquement en charge la création de groupes Auto Scaling avec des modèles de lancement. La création de groupes Auto Scaling avec des configurations de lancement n'est pas recommandée mais reste disponible via l'interface de ligne de commande et l'API jusqu'au 31 décembre 2023.

Nom : vprofile-app-asg

Créer un modèle de lancement – template avant de continuer

Nom : vprofile-app01-template

Modèle de lancement Info

💡 Pour les comptes créés après le 31 mai 2023, la console EC2 prend uniquement en charge la création de groupes Auto Scaling avec des modèles de lancement. La création de groupes Auto Scaling avec des configurations de lancement n'est pas recommandée mais reste disponible via l'interface de ligne de commande et l'API jusqu'au 31 décembre 2023.

Modèle de lancement

Choisissez un modèle de lancement qui contient les paramètres au niveau de l'instance, tels que l'Amazon Machine Image (AMI), le type d'instance, la paire de clés et les groupes de sécurité.

vprofile-app01-template



[Créer un modèle de lancement](#)

Version

Default (1)



[Créer une version de modèle de lancement](#)

Choix modèle de lancement : *vprofile-app01-template*

Zones de disponibilité et sous-réseaux

Définissez les zones de disponibilité et les sous-réseaux que votre groupe Auto Scaling peut utiliser dans le VPC choisi.

Sélectionner les zones de disponibilité et les sous-réseaux



- use1-az1 (us-east-1a) | subnet-0b168ec76e0a6e726
- 172.31.0.0/20 Default
- use1-az2 (us-east-1b) | subnet-01bf29210397a1e15
- 172.31.80.0/20 Default
- use1-az3 (us-east-1e) | subnet-05518597e56494b5d
- 172.31.48.0/20 Default
- use1-az4 (us-east-1c) | subnet-025f3fe388f828ae4
- 172.31.16.0/20 Default
- use1-az5 (us-east-1f) | subnet-0f26ef7c69899bebc
- 172.31.64.0/20 Default
- use1-az6 (us-east-1d) | subnet-0c624035c41ce0001
- 172.31.32.0/20 Default

[Créer un sous-réseau](#)

Choix de la Zone de disponibilité et sous-réseaux : Choisir toutes les zones proposées

Répartition de charge Info

Utilisez les options ci-dessous pour attacher votre groupe Auto Scaling à un équilibrEUR de charge existant ou à un nouvEL équilibrEUR de charge que vous définissez.

Aucun équilibrEUR de charge
Aucun équilibrEUR de charge ne se trouvera devant le trafic vers votre groupe Auto Scaling.

Attacher à un équilibrEUR de charge existant
Choisissez parmi vos équilibrEURS de charge existants.

Attacher à un nouvEL équilibrEUR de charge
Créez rapidement un équilibrEUR de charge de base à attacher à votre groupe Auto Scaling.

Repartition des charge : choisir Attacher a un Load Balancer

Attacher à un équilibrEUR de charge existant

Sélectionnez les équilibrEURS de charge que vous souhaitez attacher à votre groupe Auto Scaling.

- Choisir parmi les groupes cibles de votre équilibrEUR de charge

Cette option vous permet d'attacher des Application Load Balancers, des Network Load Balancers ou des Gateway Load Balancers.

- Choisir parmi les Classic Load Balancers

Groupes cibles d'équilibrEUR de charge existants

Seuls les groupes cibles d'instance qui appartiennent au même VPC que votre groupe Auto Scaling sont disponibles pour la sélection.

Selectionner des groupes cibles



vprofile-load-balancer | HTTP

Application Load Balancer: vprofile-load-balancer1

Choisir le load balancer créé précédemment

Surveillances de l'état

Les surveillances de l'état augmentent la disponibilité en remplaçant les instances défectueuses. Lorsque vous procédez à plusieurs surveillances de l'état, toutes sont évaluées et, si au moins une échoue, le remplacement d'instance a lieu.

Surveillances de l'état EC2

Toujours activé

Autres types de surveillance de l'état - facultatif | Info

- Activer les surveillances de l'état Elastic Load Balancing Recommandé

Elastic Load Balancing surveille si les instances sont disponibles pour traiter les demandes. Lorsqu'il signale une instance défectueuse, EC2 Auto Scaling la remplace lors de sa prochaine surveillance périodique.

- EC2 Auto Scaling commencera à détecter et à agir sur les surveillances de l'état effectuées par Elastic Load Balancing. X

Pour éviter les résiliations inattendues, commencez par vérifier les paramètres de ces surveillances de l'état dans la

[Console de l'équilibrEUR de charge](#)

- Activer les surveillances de l'état du réseau VPC

VPC Lattice peut surveiller si les instances sont disponibles pour traiter les demandes. S'il considère qu'une cible a échoué à une surveillance d'état, EC2 Auto Scaling la remplace après sa prochaine vérification périodique.

- Activer les surveillances de l'état Amazon FRS

Étape 4 - facultatif Configurer la taille et la mise à l'échelle du groupe

Étape 5 - facultatif

Ajouter des notifications

Étape 6 - facultatif

Ajouter des identifications

Étape 7

Vérifier

Type de capacité souhaitée
Choisissez l'unité de mesure pour la valeur de capacité souhaitée. Les vCPU et la mémoire (GiB) ne sont pris en charge que pour les groupes d'instances mixtes configurés avec un ensemble d'attributs d'instances.

Unités (nombre d'instances)

Capacité souhaitée
Spécifiez la taille de votre groupe.

1

Mise à l'échelle

Vous pouvez redimensionner votre groupe Auto Scaling manuellement ou automatiquement en fonction de l'évolution de la demande.

Limites de mise à l'échelle
Fixez des limites relatives à l'augmentation ou à la diminution de la capacité souhaitée.

Capacité minimale souhaitée

1

Inférieure ou égale à la capacité souhaitée

Capacité maximale souhaitée

4

Supérieure ou égale à la capacité souhaitée

<p>Intérieure ou égale à la capacité souhaitée</p> <p>Mise à l'échelle automatique - facultatif</p> <p>Choisir d'utiliser ou non une politique de suivi de cible Info</p> <p>Vous pouvez configurer d'autres politiques de mise à l'échelle basées sur les métriques et une mise à l'échelle planifiée après avoir créé votre groupe Auto Scaling.</p> <p><input type="radio"/> Aucune politique de mise à l'échelle Votre groupe Auto Scaling conservera sa taille initiale et ne sera pas redimensionné de manière dynamique en fonction de la demande.</p>	<p>Supérieure ou égale à la capacité souhaitée</p> <p><input checked="" type="radio"/> Politique de suivi des objectifs et d'échélonnement Choisissez une valeur cible et de métrique CloudWatch et laissez la politique de mise à l'échelle ajuster la capacité souhaitée proportionnellement à la valeur de la métrique.</p>
<p>Nom de politique de mise à l'échelle</p> <p>Target Tracking Policy</p>	
<p>Type de métrique Info</p> <p>Métrique surveillée qui permet de déterminer si l'utilisation des ressources est trop faible ou trop élevée. Si vous utilisez des métriques EC2, envisagez d'activer la surveillance détaillée afin d'améliorer les performances de mise à l'échelle.</p> <p>Utilisation moyenne du processeur</p>	
<p>Valeur cible</p>	

<p>Étape 1</p> <p>Choisir un modèle de lancement</p> <p>Étape 2</p> <p>Choisir les options de lancement d'instance</p> <p>Étape 3 - facultatif</p> <p>Intégration avec d'autres services</p> <p>Étape 4 - facultatif</p> <p>Configurer la taille et la mise à l'échelle du groupe</p> <p>Étape 5 - facultatif</p> <p><input checked="" type="radio"/> Ajouter des notifications</p> <p>Étape 6 - facultatif</p> <p>Ajouter des identifications</p> <p>Étape 7</p> <p>Vérifier</p>	<p>Ajouter des notifications - facultatif Info</p> <p>Envoyez des notifications aux rubriques SNS chaque fois qu'Amazon EC2 Auto Scaling lance ou résilie les instances EC2 de votre groupe Auto Scaling.</p> <p>Notification 1</p> <p>Rubrique SNS</p> <p>Choisir une rubrique SNS à utiliser pour envoyer des notifications</p> <p>AWS_CloudWatch_Alarms</p> <p>Créer une rubrique</p> <p>Types d'événements</p> <p>Avertir les abonnés chaque fois que des instances</p> <p><input checked="" type="checkbox"/> sont lancées</p> <p><input checked="" type="checkbox"/> sont résiliées</p> <p><input checked="" type="checkbox"/> échouent leur lancement</p> <p><input checked="" type="checkbox"/> échouent leur résiliation</p>
--	--

Ajouter une alarme – pas obligatoire

<p>C2 > Groupes Auto Scaling > Créer un groupe Auto Scaling</p> <p>Étape 1</p> <p>Choisir un modèle de lancement</p> <p>Étape 2</p> <p>Choisir les options de lancement d'instance</p> <p>Étape 3 - facultatif</p> <p>Intégration avec d'autres services</p> <p>Étape 4 - facultatif</p> <p>Configurer la taille et la mise à l'échelle du groupe</p> <p>Étape 5 - facultatif</p> <p>Ajouter des notifications</p> <p>Étape 6 - facultatif</p> <p><input checked="" type="radio"/> Ajouter des identifications</p> <p>Étape 7</p> <p>Vérifier</p>	<p>Ajouter des identifications - facultatif Info</p> <p>Ajoutez des identifications pour vous aider à rechercher, filtrer et suivre votre groupe Auto Scaling sur AWS. Vous pouvez également choisir d'ajouter automatiquement ces identifications aux instances lorsqu'elles sont lancées.</p> <p>Identifications (0)</p> <p>Ajouter une identification</p> <p>50 restant</p>
--	---

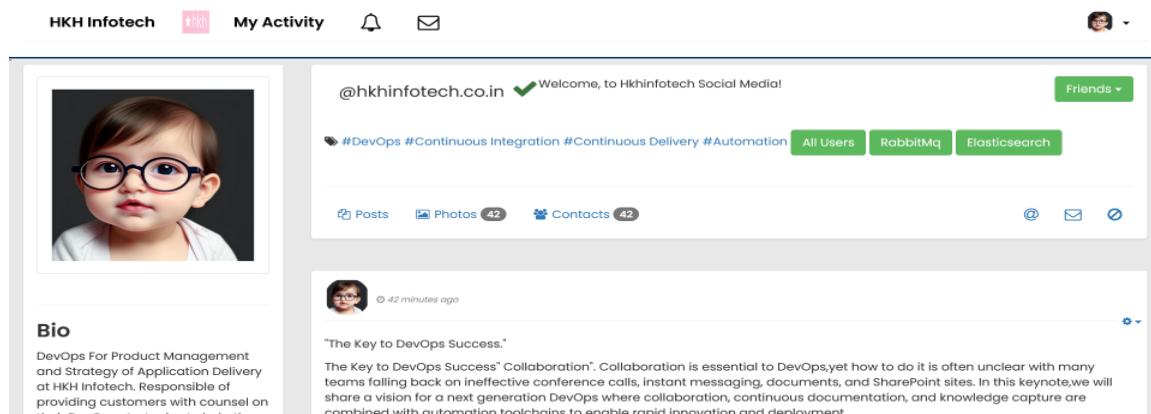
Création de vprofile-app01-asg terminée.

Résultat attendu

Accéder à la page web depuis un navigateur via : url propose par le load balancer ou sur <http://107.20.40.185:8080/>

User : admin_vp

Password : admin_vp



The screenshot shows the homepage of a social media platform for HKH Infotech. At the top, there's a navigation bar with links for 'HKH Infotech', 'My Activity', a bell icon, and an envelope icon. On the right, there's a user profile picture and a 'Friends' button. The main content area features a profile picture of a baby wearing glasses. Below it, a bio section reads: 'Bio DevOps For Product Management and Strategy of Application Delivery at HKH Infotech. Responsible of providing customers with counsel on their DevOps strategies to help them'. A post from the same user says: 'The Key to DevOps Success.' followed by a detailed description about collaboration in DevOps. Below this, there's a horizontal banner with images of a keyboard and some flowers. The bottom part of the screenshot shows a 'Users List' table with the following data:

User Name	Action
Hiboo Prince	4
Aejaz Habeeb	5
Jackie	6
admin_vp	7
Abrar Nirban	8
Amayra Fatima	9

On the right side of the table, there are 'Login' and 'Sign up' buttons, and a small decorative image of a rose.

RabbitMQ Initiated

Generated 7 Connections

8 Channels, 6 Exchange, and 7 Queues

 **Technologies utilisées**

- AWS EC2 / S3 / Route 53 / IAM / ELB
- Ubuntu Server / Amazon Linux
- Shell Script (bash)
- Maven
- Java Web Application
- HTML/CSS (template statique)

 **Nettoyage**

⚠ Pensez à supprimer toutes les ressources AWS (instances EC2, buckets S3, groupes de sécurité, Load Balancer, etc.) une fois le projet terminé pour éviter des frais supplémentaires.

 **Auteur**

Projet réalisé par **Badaoudou BARRO**