



UNIVERSITÉ HASSAN II DE CASABLANCA
ECOLE NORMALE SUPERIEURE D'ENSEIGNEMENT
TECHNIQUE DE MOHAMMEDA

INGÉNIERIE INFORMATIQUE - BIG DATA ET CLOUD COMPUTING

RAPPORT DE PROJET DE FIN DE MODULE

Déploiement d'une architecture de supervision Cloud distribuée avec Zabbix sur AWS



Réalisé par :
Elbatir Elmahdi (II-BDCC)

Sous l'encadrement de :
Pr. Azeddine KHIAT

Table des matières

1	Introduction	2
2	Architecture Réseau	2
2.1	Création du VPC	2
2.2	Configuration de l'accès Internet (Internet Gateway)	3
2.3	Création du Sous-réseau Public (Subnet)	3
2.4	Table de Routage (Routing Table)	4
2.5	Sécurité et Filtrage (Security Groups)	4
3	Architecture des Instances EC2	5
3.1	Création de la Paire de Clés (Key Pair)	5
3.2	Procédure de Lancement : Serveur Zabbix	6
3.3	Procédure de Lancement : Clients de Supervision	6
4	Déploiement du Serveur Zabbix	7
4.1	Connexion et Préparation	7
4.2	Installation de Docker	8
4.3	Déploiement des Services	9
5	Configuration des Clients (Agents)	12
5.1	Client Linux (Ubuntu)	12
5.2	Client Windows	13
6	Monitoring et Analyse des Métriques	14
6.1	Visualisation des Graphiques	14
7	Conclusion	15

1 Introduction

Ce projet vise à déployer une solution de supervision robuste et distribuée dans un environnement Cloud. L'objectif est de moniter en temps réel la disponibilité et les performances d'un parc de serveurs hétérogène (Linux et Windows) hébergé sur Amazon Web Services (AWS).

Pour répondre à ce besoin, nous avons choisi **Zabbix 6.0 LTS**, une solution open-source leader sur le marché, couplée à **Docker** pour faciliter le déploiement et la maintenance du serveur de supervision. L'infrastructure repose sur des instances EC2 interconnectées au sein d'un VPC sécurisé.

Lien Repo Git : https://github.com/MAHDIBATIR/Projet_CyberOps.git

2 Architecture Réseau

La première étape de notre projet a consisté à construire le socle réseau (Network Layer) sur AWS. Nous avons mis en place un **VPC (Virtual Private Cloud)** personnalisé pour isoler nos ressources et maîtriser l'adressage IP.

L'architecture réseau a été configurée étape par étape via la console AWS VPC.

2.1 Création du VPC

Nous avons défini un espace d'adressage privé pour notre projet.

1. Dans la console AWS, service **VPC > Your VPCs > Create VPC**.
2. **Name tag** : Zabbix-VPC.
3. **IPv4 CIDR block** : 10.0.0.0/16 (Ce qui nous offre 65 536 adresses IP privées potentielles).
4. **Tenancy** : Default.

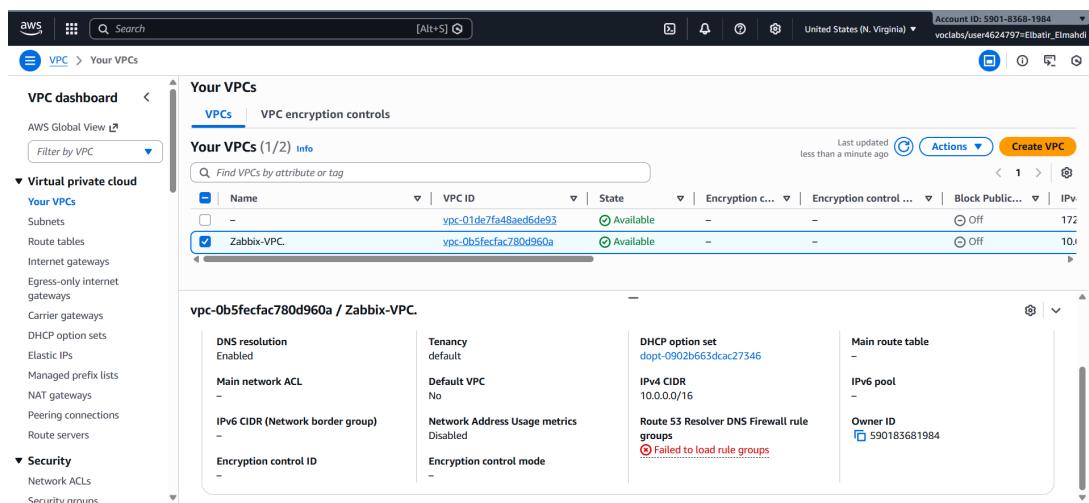


FIGURE 1 – Crédit de la capture d'écran

2.2 Configuration de l'accès Internet (Internet Gateway)

Pour que notre serveur Zabbix puisse télécharger les paquets Docker et que nous puissions y accéder à distance, une connexion internet est indispensable.

1. Menu **Internet Gateways > Create internet gateway**.
2. **Name** : IGW-Zabbix.
3. **Action** : Une fois créée, nous avons cliqué sur **Attach to VPC** et sélectionné notre Zabbix-VPC.

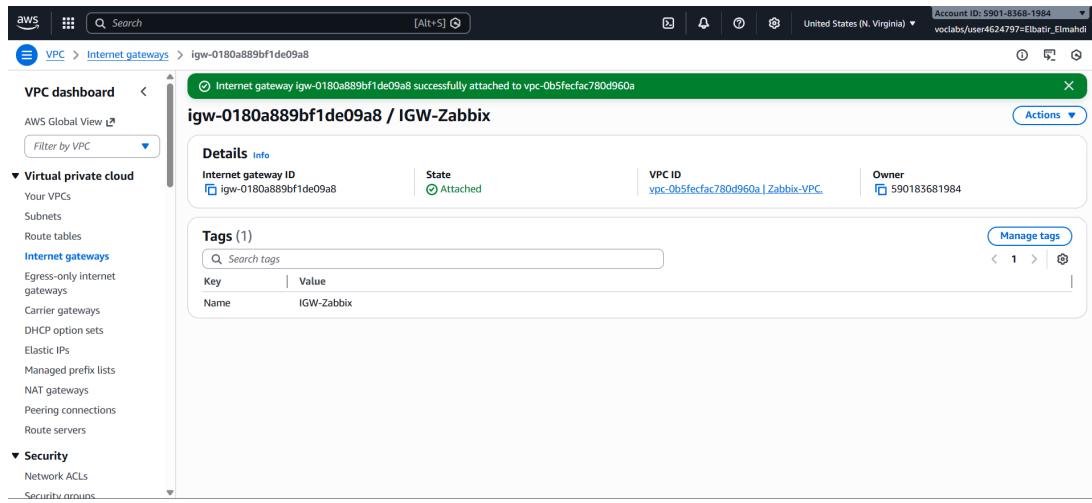


FIGURE 2 – Configuration de Gateway

2.3 Crédation du Sous-réseau Public (Subnet)

Nous avons segmenté le VPC pour placer nos instances.

1. Menu **Subnets > Create subnet**.
2. **VPC ID** : Sélection de Zabbix-VPC.
3. **Subnet name** : Public-Subnet-1.
4. **Availability Zone** : us-east-1a (pour garantir la haute disponibilité dans une zone précise).
5. **IPv4 CIDR block** : 10.0.1.0/24 (256 adresses IP).
6. **Configuration IP** : Nous avons activé l'option "*Enable auto-assign public IPv4 address*" pour que chaque instance reçoive automatiquement une IP publique.

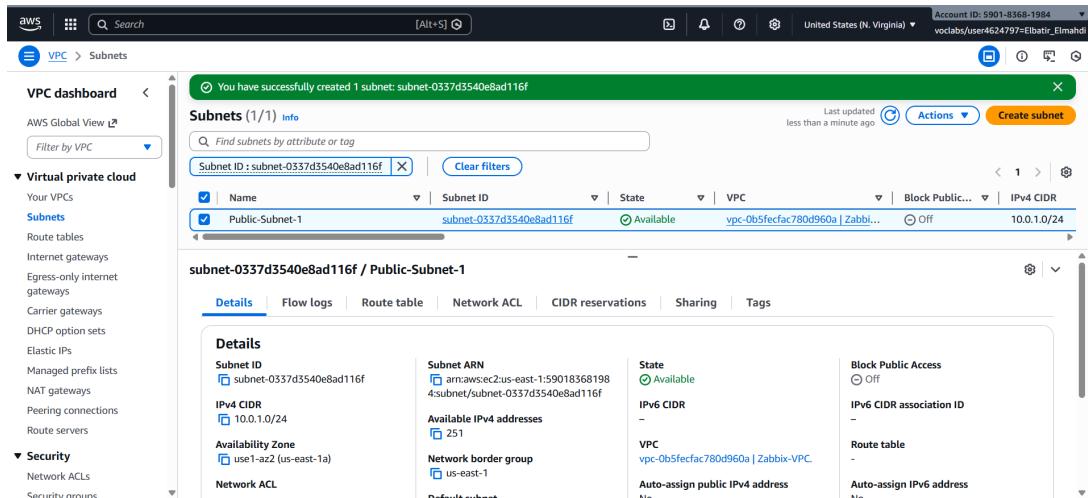


FIGURE 3 – Crédation de sous-réseau Public

2.4 Table de Routage (Routing Table)

C'est l'étape qui rend le sous-réseau véritablement "public".

1. Menu **Route Tables**.
2. Sélection de la table de routage associée à notre VPC.
3. Onglet **Routes** > **Edit routes** > **Add route**.
4. **Destination** : 0.0.0.0/0 (Tout le trafic internet).
5. **Target** : Sélection de l'Internet Gateway créé (Zabbix-IGW).
6. **Association** : Dans l'onglet *Subnet associations*, nous avons lié cette table à notre Public-Subnet-1.

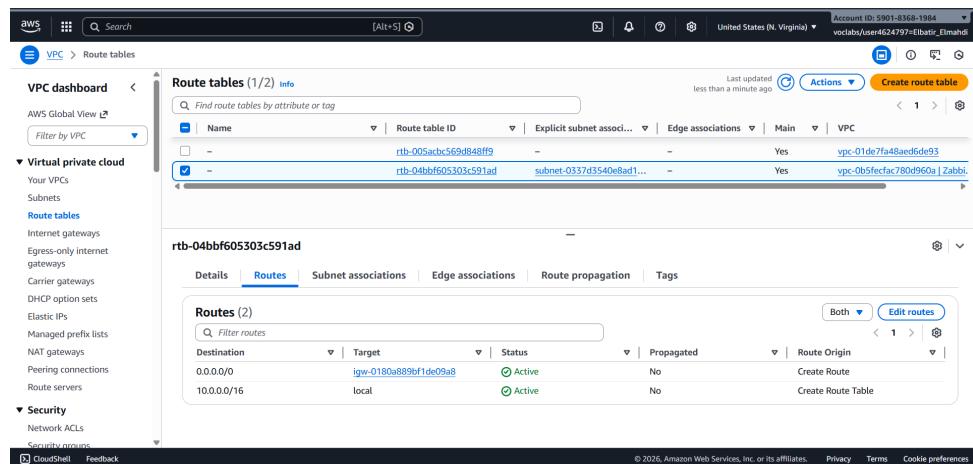


FIGURE 4 – Table de Routage

2.5 Sécurité et Filtrage (Security Groups)

Enfin, nous avons créé un pare-feu virtuel (**Security Group**) appliqué à nos instances pour filtrer les connexions entrantes.

Configuration via le menu "EC2 > Security Groups" : Nous avons créé le groupe Zabbix-SG avec les règles entrantes (Inbound Rules) suivantes :

1. **Administration (SSH/RDP)** : Ports 22 et 3389 ouvert sur 0.0.0.0/0.
2. **Interface Web** : Port 80 ouvert sur 0.0.0.0/0 pour l'accès HTTP.
3. **Communication Zabbix (Critique) :**
 - **Port 10050 (TCP)** : Autorisé pour permettre au serveur de contacter les agents. Sans cette règle explicite, nous avions rencontré une erreur "Connection Refused".
 - **Port 10051 (TCP)** : Autorisé pour les remontées d'alertes actives.

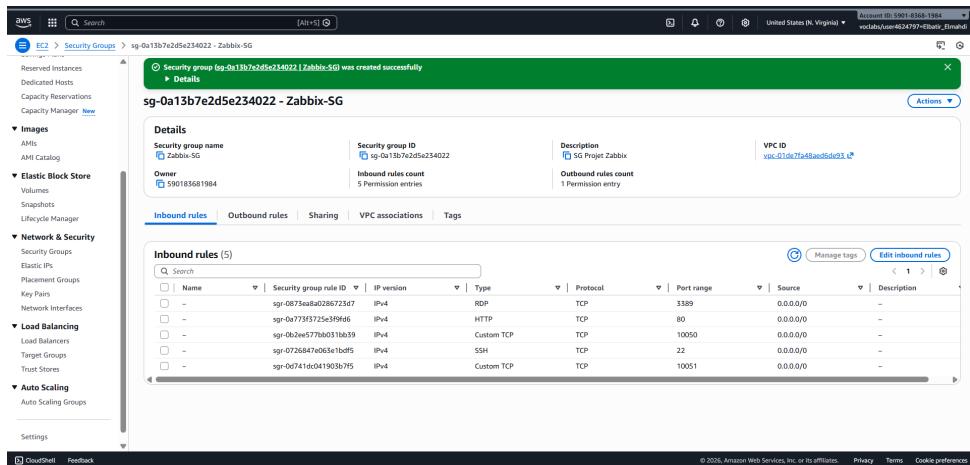


FIGURE 5 – Configuration des règles de sécurité (Inbound Rules)

3 Architecture des Instances EC2

Une fois le réseau configuré, nous avons procédé au déploiement des serveurs virtuels. Cette étape a nécessité la création préalable d'une clé de sécurité, puis le lancement successif de trois instances via la console EC2.

3.1 Crédation de la Paire de Clés (Key Pair)

Pour sécuriser l'accès SSH (Linux) et le décryptage du mot de passe Administrateur (Windows), une paire de clés est requise.

1. Dans le menu de gauche de la console EC2, sous *Network & Security*, nous avons cliqué sur **Key Pairs**.
2. Clic sur le bouton orange **Create key pair**.
3. **Name** : key-projet-zabbix.
4. **Key pair type** : RSA.
5. **Private key file format** : .pem (Format standard pour OpenSSH).
6. Après validation, le fichier **key-projet-zabbix.pem** a été téléchargé automatiquement. Ce fichier est critique et a été stocké précieusement sur notre machine locale.

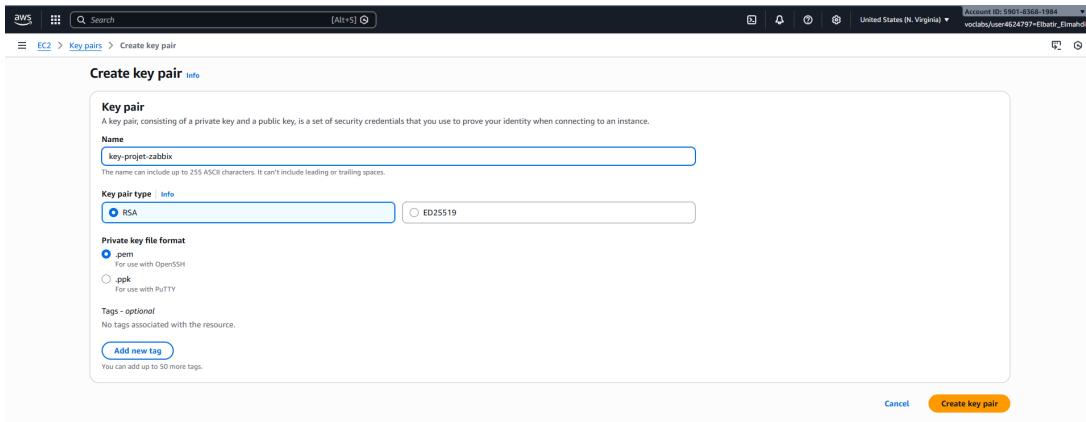


FIGURE 6 – Crédit de la Paire de Clés

3.2 Procédure de Lancement : Serveur Zabbix

Le serveur central nécessite des ressources suffisantes pour exécuter Docker et la base de données.

1. Depuis le tableau de bord EC2, nous avons cliqué sur **Launch Instances**.
2. **Name and tags** : Zabbix-Server.
3. **Application and OS Images (AMI)** : Sélection de **Ubuntu Server 24.04 LTS** (Free tier éligible).
4. **Instance type** : Nous avons sélectionné **t3.large** (2 vCPU, 8 Gio Mémoire).
5. **Key pair** : Sélection de **key-projet-zabbix**.
6. **Network settings** :
 - **VPC** : Zabbix-VPC (créé précédemment).
 - **Subnet** : Public-Subnet-1.
 - **Auto-assign Public IP** : Enable (Pour l'accès SSH et Web).
 - **Security Group** : Sélection de Zabbix-SG (créé précédemment).
7. **Storage** : 20 Gio gp3 (Pour stocker les logs et la base de données Docker).

3.3 Procédure de Lancement : Clients de Supervision

Nous avons répété l'opération pour les deux machines cibles, avec des configurations adaptées à leur OS.

- A. Client Linux (Ubuntu)**
 - **Name** : Elbatir-Client-Linux.
 - **AMI** : Ubuntu Server 24.04 LTS.
 - **Instance type** : t3.medium (2 vCPU, 4 Gio RAM).
- B. Client Windows Server**
 - **Name** : Elbatir-Client-Windows.
 - **AMI** : Microsoft Windows Server 2022 Base.
 - **Instance type** : t3.large (2 vCPU, 8 Gio RAM).

The screenshot shows the AWS Management Console with the EC2 service selected. The left sidebar shows navigation options like Dashboard, Global View, Events, Instances, Images, Elastic Block Store, Network & Security, and more. The main content area displays a table titled 'Instances (3) Info' with columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, and Public IPv4 IP. The table lists three instances: 'Zabbix-Server' (t3.large, 3/3 checks passed), 'Elbatir-Client-1' (t3.large, 3/3 checks passed), and 'Elbatir-Client-2' (t3.medium, 3/3 checks passed). All instances are currently running.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 IP	Elastic IP
Zabbix-Server	i-01f9d942edcf3aa4f	Running	t3.large	3/3 checks passed	View alarms +	us-east-1a	-	18.204.21.25	-
Elbatir-Client-1	i-021ed6c7bf2a46d	Running	t3.large	3/3 checks passed	View alarms +	us-east-1a	-	35.174.104.207	-
Elbatir-Client-2	i-06776a6f86e3a15e5	Running	t3.medium	3/3 checks passed	View alarms +	us-east-1a	-	52.91.175.236	-

FIGURE 7 – Vue d’ensemble des 3 instances EC2 en cours d’exécution (Status check : 2/2)

4 Déploiement du Serveur Zabbix

Le serveur de supervision a été déployé en utilisant la conteneurisation pour garantir l’isolation des services.

4.1 Connexion et Préparation

L'accès au serveur nécessite une clé privée sécurisée.

1. Sécurisation de la clé privée :

```
icacls "C:\Users\elbat\Desktop\projet_CyberOps\key-projet-zabbix.pem" /inheritance:r /grant:r "%$env:USERNAME%:R"
```

2. Connexion SSH :

```
ssh -i key-projet-zabbix.pem ubuntu@18.204.21.25
```

```
ubuntu@ip-10-0-1-114:~$ ssh -i key-projet-zabbix.pem ubuntu@18.204.21.25
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1015-aws x86_64)

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

System information as of Fri Jan 2 20:20:58 UTC 2026

System load: 0.0              Temperature:      -273.1 C
Usage of /: 9.4% of 18.33GB  Processes:        110
Memory usage: 2%              Users logged in:   0
Swap usage: 0%                IPv4 address for ens5: 10.0.1.114

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

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 &lt;command&gt;".
See "man sudo_root" for details.

ubuntu@ip-10-0-1-114:~$ |</pre>

```

FIGURE 8 – Connexion SSH Serveur Zabbix

4.2 Installation de Docker

L'installation par défaut via apt :

Procédure installation :

1. Update system :

```
$ sudo apt update && sudo apt upgrade -y
```

2. Installation :

```
# Install Docker
$ sudo apt install -y docker.io docker-compose
# Add user to docker group
$ sudo usermod -aG docker $USER
# Start Docker service
$ sudo systemctl enable docker
$ sudo systemctl start docker
```

3. Vérification de la version :

```
$ docker-compose --version
```

```

ubuntu@ip-10-0-1-114:~$ sudo apt install -y docker.io docker-compose
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
docker.io is already the newest version (28.2.2-0ubuntu1~24.04.1).
docker-compose is already the newest version (1.29.2-6ubuntu1).
^[[A0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
ubuntu@ip-10-0-1-114:~$ docker-compose --version
docker-compose version 1.29.2, build unknown
ubuntu@ip-10-0-1-114:~$ |

```

FIGURE 9 – Installation de Docker dans serveur Zabbix

4.3 Déploiement des Services

Nous avons créé le fichier d'orchestration `docker-compose.yml` à la racine du dossier utilisateur.

1. Contenu du fichier de configuration :

```

version: '3.5'
services:
  zabbix-db:
    image: mariadb:10.6
    container_name: zabbix-db
    restart: always
    environment:
      - MYSQL_DATABASE=zabbix
      - MYSQL_USER=zabbix
      - MYSQL_PASSWORD=zabbix_pwd
      - MYSQL_ROOT_PASSWORD=root_pwd
    volumes:
      - ./mysql_data:/var/lib/mysql

  zabbix-server:
    image: zabbix/zabbix-server-mysql:ubuntu-6.0-latest
    container_name: zabbix-server
    ports:
      - "10051:10051"
    environment:
      - DB_SERVER_HOST=zabbix-db
      - MYSQL_DATABASE=zabbix
      - MYSQL_USER=zabbix
      - MYSQL_PASSWORD=zabbix_pwd
      - MYSQL_ROOT_PASSWORD=root_pwd
    depends_on:
      - zabbix-db

  zabbix-web:
    image: zabbix/zabbix-web-nginx-mysql:ubuntu-6.0-latest
    container_name: zabbix-web
    ports:
      - "80:8080"
    environment:
      - ZBX_SERVER_HOST=zabbix-server

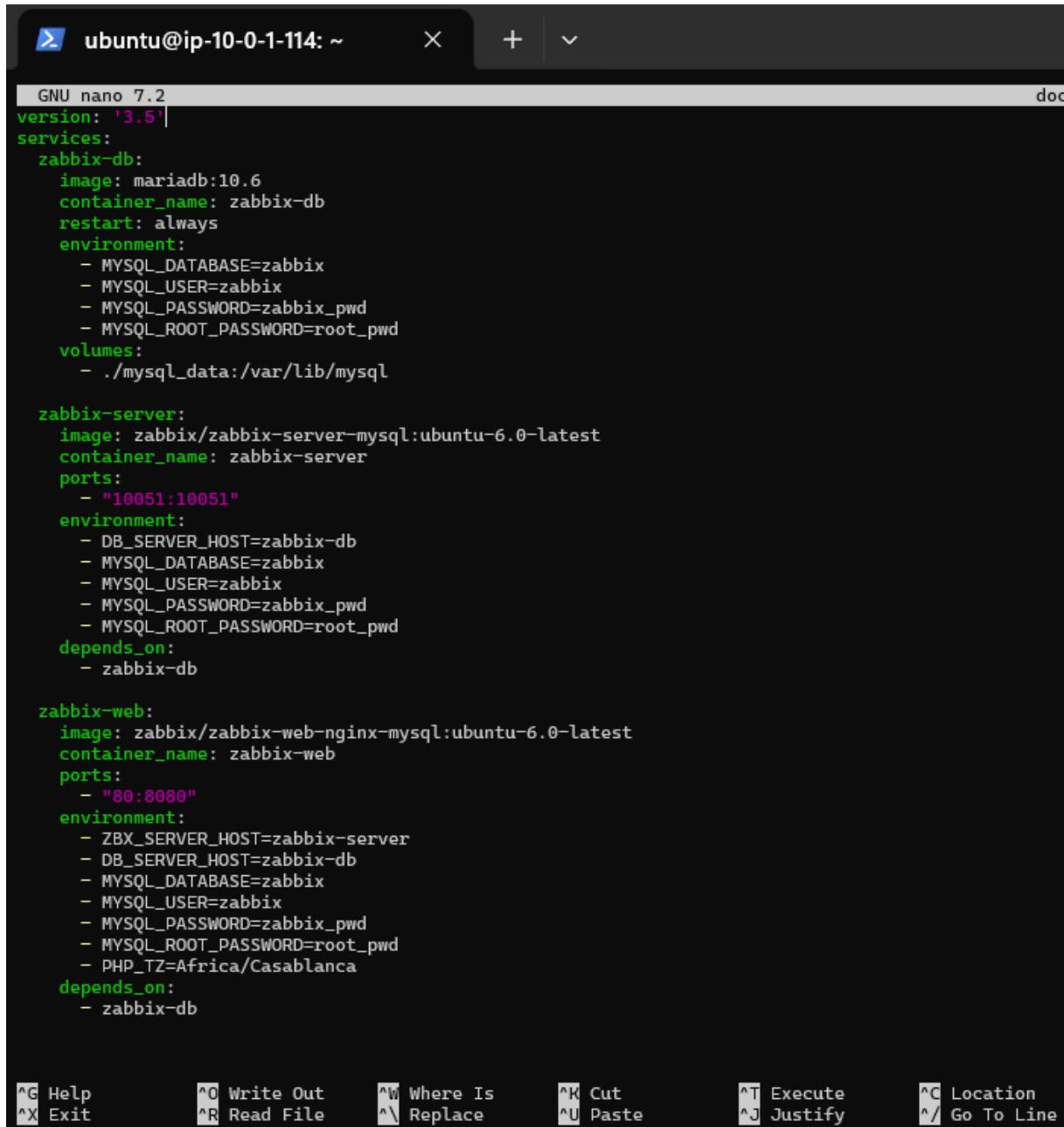
```

```

    - DB_SERVER_HOST=zabbix-db
    - MYSQL_DATABASE=zabbix
    - MYSQL_USER=zabbix
    - MYSQL_PASSWORD=zabbix_pwd
    - MYSQL_ROOT_PASSWORD=root_pwd
    - PHP_TZ=Africa/Casablanca
depends_on:
  - zabbix-db

```

Listing 1 – docker-compose.yml



The screenshot shows a terminal window titled "ubuntu@ip-10-0-1-114: ~". The file being edited is "docker-compose.yml". The content of the file is as follows:

```

version: '3.5'
services:
  zabbix-db:
    image: mariadb:10.6
    container_name: zabbix-db
    restart: always
    environment:
      - MYSQL_DATABASE=zabbix
      - MYSQL_USER=zabbix
      - MYSQL_PASSWORD=zabbix_pwd
      - MYSQL_ROOT_PASSWORD=root_pwd
    volumes:
      - ./mysql_data:/var/lib/mysql

  zabbix-server:
    image: zabbix/zabbix-server-mysql:ubuntu-6.0-latest
    container_name: zabbix-server
    ports:
      - "10051:10051"
    environment:
      - DB_SERVER_HOST=zabbix-db
      - MYSQL_DATABASE=zabbix
      - MYSQL_USER=zabbix
      - MYSQL_PASSWORD=zabbix_pwd
      - MYSQL_ROOT_PASSWORD=root_pwd
    depends_on:
      - zabbix-db

  zabbix-web:
    image: zabbix/zabbix-web-nginx-mysql:ubuntu-6.0-latest
    container_name: zabbix-web
    ports:
      - "80:8080"
    environment:
      - ZBX_SERVER_HOST=zabbix-server
      - DB_SERVER_HOST=zabbix-db
      - MYSQL_DATABASE=zabbix
      - MYSQL_USER=zabbix
      - MYSQL_PASSWORD=zabbix_pwd
      - MYSQL_ROOT_PASSWORD=root_pwd
      - PHP_TZ=Africa/Casablanca
    depends_on:
      - zabbix-db

```

At the bottom of the terminal window, there is a menu bar with the following options:

- ^G Help
- ^O Write Out
- ^W Where Is
- ^K Cut
- ^T Execute
- ^C Location
- ^X Exit
- ^R Read File
- ^\\ Replace
- ^U Paste
- ^J Justify
- ^/ Go To Line

FIGURE 10 – Docker-compose.yml)

2. Lancement de conteneur :

```
$ docker-compose up -d
```

```
ubuntu@ip-10-0-1-114:~/zabbix$ docker-compose up -d
Creating network "zabbix_default" with the default driver
Creating zabbix-db ... done
Creating zabbix-server ... done
Creating zabbix-web ... done
ubuntu@ip-10-0-1-114:~/zabbix$ docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
cf242f83dc4c zabbix/zabbix-web:nginx-mysql:ubuntu-6.0-latest "docker-entrypoint.sh" 34 seconds ago Up 34 seconds (healthy) 8080/tcp, 0.0.0.0:80->8080/tcp, [::]:80->8080/tcp zabbix-web
7ec0054e55e5 zabbix/zabbix-server-mysql:ubuntu-6.0-latest "/usr/bin/tini --" 34 seconds ago Up 34 seconds 0.0.0.0:10051->10051/tcp, [::]:10051->10051/tcp zabbix-server
3cb9b075sa32 mariadb:10.6 "docker-entrypoint.sh" 34 seconds ago Up 34 seconds 3306/tcp zabbix-db
ubuntu@ip-10-0-1-114:~/zabbix$ |
```

FIGURE 11 – Vérification des conteneurs actifs

Une fois les conteneurs stables, l'interface Web est devenue accessible sur l'IP Publique.

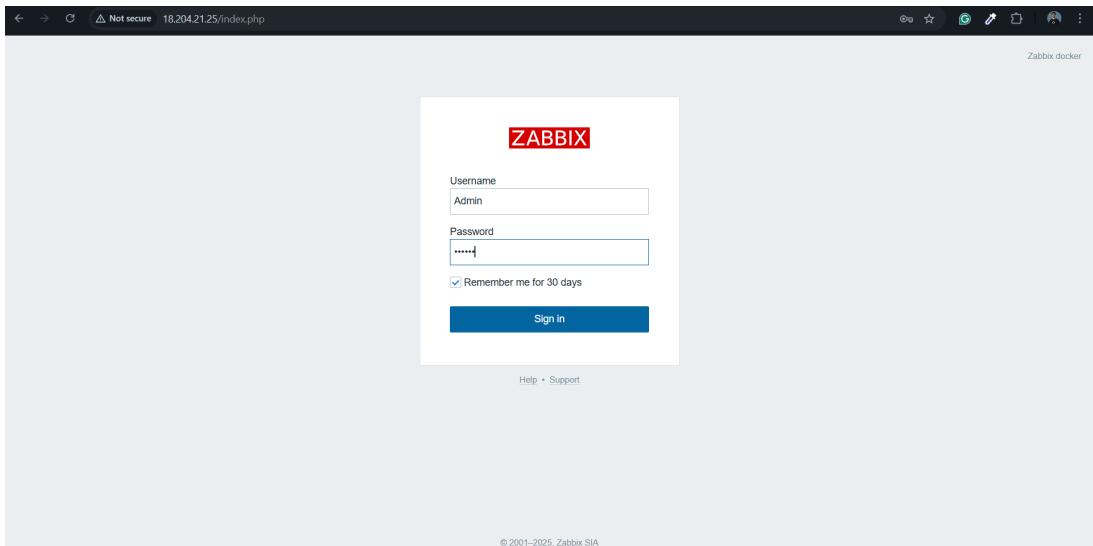


FIGURE 12 – Interface de Connexion Zabbix

En se connectant via Utilisateur : Admin et Mot de pass : zabbix

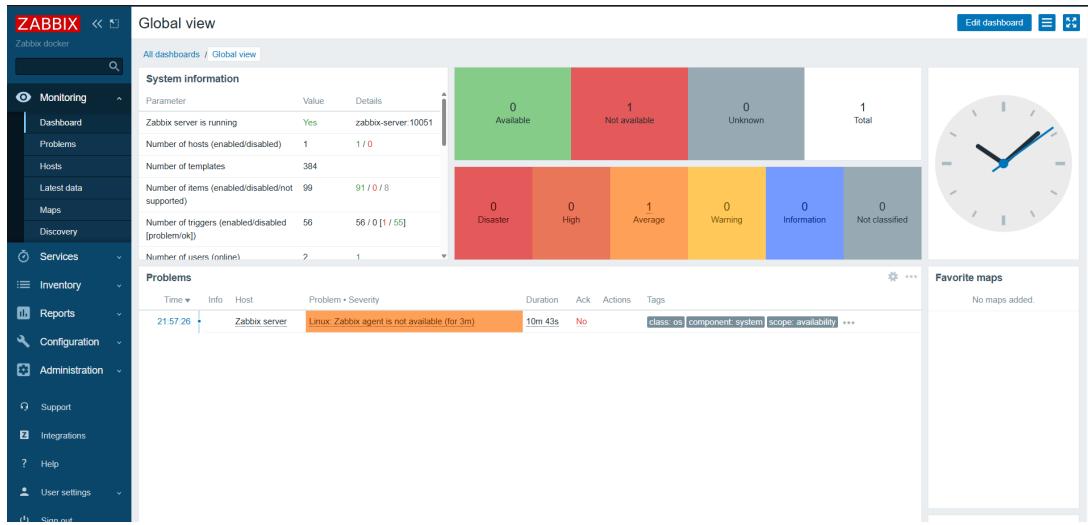


FIGURE 13 – Interface de Connexion Zabbix

5 Configuration des Clients (Agents)

5.1 Client Linux (Ubuntu)

Sur la machine Ubuntu 24.04, le paquet `zabbix-agent` n'était pas disponible dans les dépôts par défaut.

1. Ajout du dépôt officiel Zabbix :

```
$ wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-6+ubuntu24.04_all.deb
$ sudo dpkg -i zabbix-release_6.0-6+ubuntu24.04_all.deb
$ sudo apt update
```

```
ubuntu@ip-10-0-1-114:~/zabb x  ubuntu@ip-10-0-1-233:~ x + v
ubuntu@ip-10-0-1-233:~$ wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-6+ubuntu24.04_all.deb
--2026-01-02 21:14:25-- https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-6+ubuntu24.04_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0::2062:d001
Connecting to repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5708 (5.6K) [application/octet-stream]
Saving to: 'zabbix-release_6.0-6+ubuntu24.04_all.deb'

zabbix-release_6.0-6+ubuntu24 100%[=====] 5.57K --.-KB/s   in 0s
2026-01-02 21:14:25 (453 MB/s) - 'zabbix-release_6.0-6+ubuntu24.04_all.deb' saved [5708/5708]

ubuntu@ip-10-0-1-233:~$ sudo dpkg -i zabbix-release_6.0-6+ubuntu24.04_all.deb
Selecting previously unselected package zabbix-release.
(Reading database ... 71735 files and directories currently installed.)
Preparing to unpack zabbix-release_6.0-6+ubuntu24.04_all.deb ...
Unpacking zabbix-release (1:6.0-6+ubuntu24.04) ...
Setting up zabbix-release (1:6.0-6+ubuntu24.04) ...
ubuntu@ip-10-0-1-233:~$ sudo apt update
```

FIGURE 14 – Ajout du dépôt officiel Zabbix

2. Installation et Configuration :

```
$ sudo apt install zabbix-agent -y
$ sudo nano /etc/zabbix/zabbix_agentd.conf
```

Modification des paramètres pour pointer vers l'IP Privée du Serveur (10.0.1.252) :

```
# /etc/zabbix/zabbix_agentd.conf
Server=10.0.1.114
ServerActive=10.0.1.114
Hostname=Elbatir-Client-Linux
```

3. Redémarrage :

```
$ sudo systemctl restart zabbix-agent
$ sudo systemctl enable zabbix-agent
```

5.2 Client Windows

Pour Windows, l'installation est graphique.

- Récupération du mot de passe** : Dans la console AWS > Connect > RDP Client > "Get Password" en utilisant le fichier .pem.
- Connexion RDP** : Utilisation de l'outil "Bureau à distance".
- Installation** : Téléchargement de l'agent MSI Zabbix 6.0 LTS.
- Configuration** : Lors de l'installation, nous avons renseigné :
 - Zabbix Server IP : 10.0.1.252
 - Agent Listen Port : 10050
 - Hostname : Elbatir-Client-Windows
- Pare-feu** : Création d'une règle entrante sur le port 10050 dans le Pare-feu Windows Defender.

Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
Elbatir-Client-Linux	10.0.1.233:10050	ZBX	class:os target:linux	Enabled	Latest data 42	Problems 8	Graphs 2	Dashboards 2	Web
Elbatir-Client-Windows	10.0.1.218:10050	ZBX	class:os target:windows	Enabled	Latest data 41	Problems 6	Graphs 6	Dashboards 2	Web
Zabbix server	127.0.0.1:10050	ZBX	class:os class:software target:linux ***	Enabled	Latest data 99	Problems 1	Graphs 24	Dashboards 3	Web

FIGURE 15 – visualisations des hostes

6 Monitoring et Analyse des Métriques

Une fois l'infrastructure en place, la dernière étape a consisté à relier nos instances EC2 à l'interface de supervision pour visualiser les données collectées.

6.1 Visualisation des Graphiques

Grâce aux templates appliqués, Zabbix génère automatiquement des graphiques historiques sans configuration supplémentaire. Nous n'avons pas eu besoin de créer de tableau de bord complexe pour accéder aux données essentielles.

Pour visualiser l'état de santé des machines :

1. Nous sommes allés dans le menu **Monitoring > Hosts**.
2. Nous avons cliqué sur le lien **Graphs** correspondant à la machine **Elbatir-Client-Linux**.

Les graphiques ci-dessous illustrent la charge processeur (CPU Load) et la consommation de mémoire (RAM) collectée en temps réel. Ils prouvent que la chaîne de supervision est fonctionnelle de bout en bout.

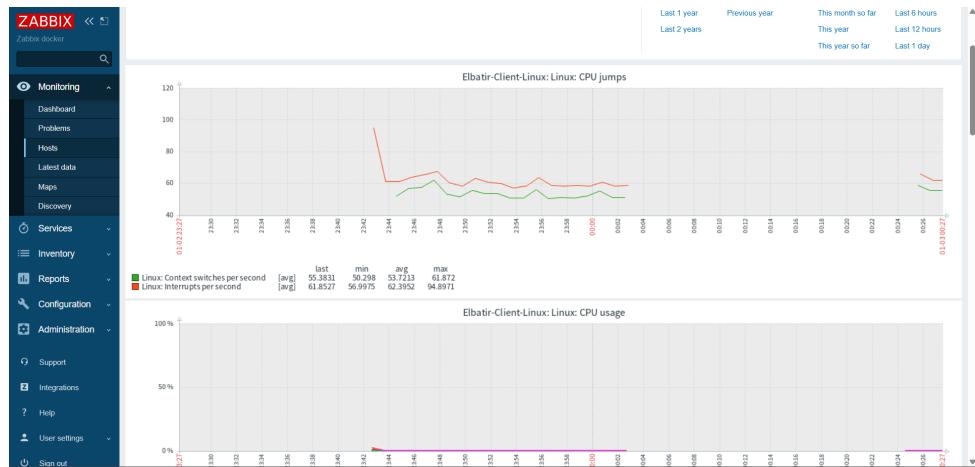


FIGURE 16 – Visualisation de la charge CPU du client Linux



FIGURE 17 – Visualisation de la charge RAM du client Linux

7 Conclusion

Ce projet a permis de valider des compétences clés en Cloud Computing et Administration Système. Nous avons réussi à déployer une architecture complète malgré plusieurs défis techniques :

- La gestion fine des **Security Groups AWS** pour permettre la communication inter-instances.
- La résolution de conflits de versions logicielles (**Docker Compose v1 vs v2**) sur Ubuntu 24.04.
- Le débogage de conteneurs Docker (Migration **MySQL vers MariaDB** et nettoyage de volumes) pour assurer la stabilité du backend.

L'infrastructure Zabbix est désormais opérationnelle et permet une surveillance proactive de l'ensemble du parc.