2025/2026

Mise en place d’une infrastructure de supervision avec Zabbix sur AWS

2ACI

Réalisée par : Marwane OUAHID.

Encadrer par : prof. Azeddine KHIAT.

Lien repo github : <https://github.com/ouahidmarwane/Aws-Zabbix-monitoring/tree/main>

Table des matières

[1. Introduction : 2](#_Toc218477909)

[2. Objectifs du projet : 2](#_Toc218477910)

[3. Architecture générale de l’infrastructure : 2](#_Toc218477911)

[L’architecture repose sur : 2](#_Toc218477912)

[4. Configuration du réseau AWS (VPC) : 3](#_Toc218477913)

[4.1 Création du VPC 3](#_Toc218477914)

[4.2 Sous-réseaux 3](#_Toc218477915)

[4.3 Passerelle Internet (Internet Gateway) 4](#_Toc218477916)

[4.4 Tables de routage 4](#_Toc218477917)

[5. Déploiement de Zabbix Server avec Docker : 9](#_Toc218477918)

[5.1 Installation de Docker 9](#_Toc218477919)

[5.2 Fichier docker-compose.yml 9](#_Toc218477920)

[5.3 Lancement des conteneurs 10](#_Toc218477921)

[6. Accès à l’interface Web Zabbix : 10](#_Toc218477922)

[7. Installation et configuration des agents Zabbix 11](#_Toc218477923)

[7.1 Client Linux 11](#_Toc218477924)

[7.2 Client Windows 12](#_Toc218477925)

[Interface Zabbix Création des hôtes : 14](#_Toc218477926)

[14](#_Toc218477927)

[Conclusion : 14](#_Toc218477928)

[Figure 1:Mapping des ressources VPC (VPC, sous-réseaux, tables de routage) 4](#_Toc218477937)

[Figure 2:Détails du VPC (nom, ID, CIDR) 4](#_Toc218477938)

[Figure 3: Liste des sous-réseaux publics et privés avec CIDR 5](#_Toc218477939)

[Figure 4:Écran montrant la passerelle Internet attachée au VPC 5](#_Toc218477940)

[Figure 5: Table de routage publique routes 6](#_Toc218477941)

[Figure 6: Table de routage publique associations 6](#_Toc218477942)

[Figure 7: Table de routage privée (associations) 7](#_Toc218477943)

[Figure 8: Les instances 8](#_Toc218477944)

[Figure 9: Groupe de sécurité Zabbix server 8](#_Toc218477945)

[Figure 10: Groupe de sécurité de Client Linux 9](#_Toc218477946)

[Figure 11: Groupe de sécurité Client Windows 9](#_Toc218477947)

[Figure 12: Installation de Docker (docker --version) 10](#_Toc218477948)

[Figure 13: Contenu du fichier docker-compose.yml 11](#_Toc218477949)

[Figure 14: Résultat de docker ps montrant les conteneurs actifs 11](#_Toc218477950)

[Figure 15: Interface Zabbix 12](#_Toc218477951)

[Figure 16: Service actif (systemctl status zabbix-agent) 13](#_Toc218477952)

[Figure 17: Connexion RDP 13](#_Toc218477953)

[Figure 18: Insertion d’IP de Serveur Zabbix a Client Windows 14](#_Toc218477954)

[Figure 19: Insertion d’IP de Serveur Active Zabbix a Client Windows 14](#_Toc218477955)

[Figure 20:Hotes Zabbix 15](#_Toc218477956)

# 1. Introduction :

Dans le cadre de ce projet, l’objectif est de **mettre en place une solution de supervision centralisée** permettant de surveiller des machines **Linux et Windows** à l’aide de **Zabbix**, déployé sur une **infrastructure cloud AWS**.  
La supervision permet de suivre l’état des systèmes, détecter les anomalies et assurer la disponibilité des services.

# 2. Objectifs du projet :

Les objectifs principaux sont :

* Déployer un **serveur Zabbix** sur une instance **EC2 Ubuntu**
* Superviser :
  + Un **client Linux**
  + Un **client Windows**
* Utiliser **Zabbix Agent** pour la collecte des métriques
* Mettre en place la communication réseau entre les agents et le serveur
* Accéder à l’interface web de Zabbix
* Vérifier la remontée des données de supervision

# 3. Architecture générale de l’infrastructure :

## L’architecture repose sur :

* **Un VPC AWS**
* **Deux sous-réseaux publics**
* **Deux sous-réseaux privés**
* **Une passerelle Internet (Internet Gateway)**
* **Des tables de routage séparées (publique / privée)**
* **Instances EC2 Linux et Windows**
* **Zabbix Server conteneurisé avec Docker**

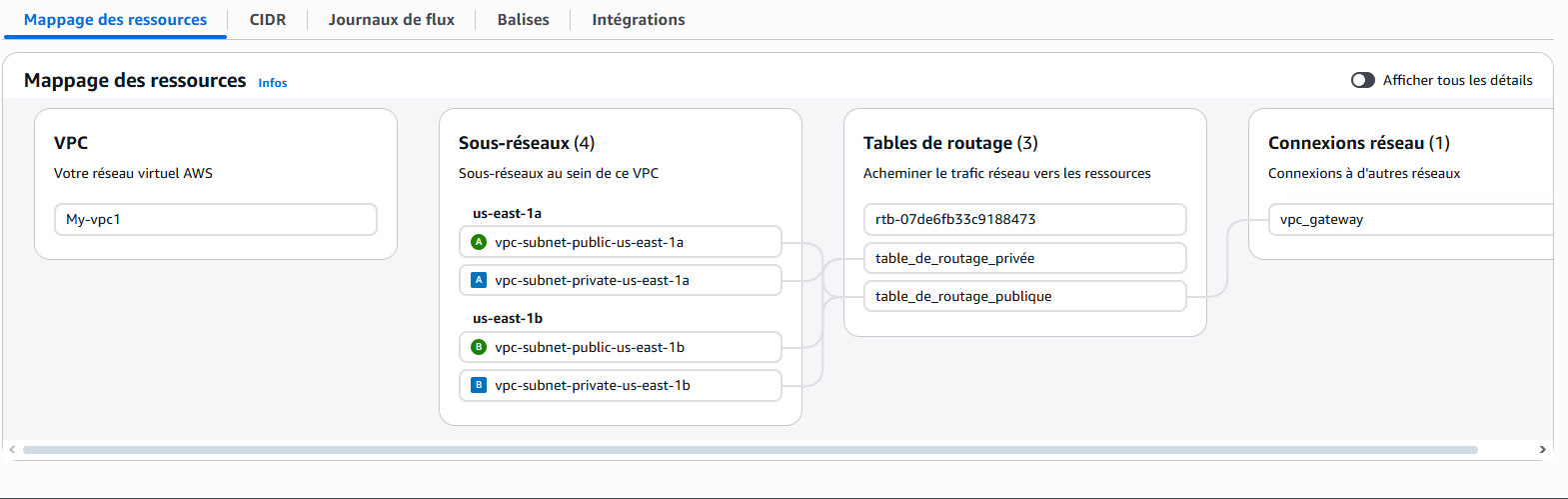


Figure 1:Mapping des ressources VPC (VPC, sous-réseaux, tables de routage)

## 4. Configuration du réseau AWS (VPC) :

### 4.1 Création du VPC

Une VPC nommée **My-vpc1** a été créé avec un CIDR privé.

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

Figure 2:Détails du VPC (nom, ID, CIDR)

### 4.2 Sous-réseaux

Deux zones de disponibilité ont été utilisées :

* **Us-east-1a**
* **Us-east-1b**

Chaque zone contient :

* 1 sous-réseau public
* 1 sous-réseau privé

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

Figure 3: Liste des sous-réseaux publics et privés avec CIDR

### 4.3 Passerelle Internet (Internet Gateway)

Une **Internet Gateway** a été créée et attachée au VPC afin de permettre l’accès Internet aux sous-réseaux publics.

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

Figure 4:Écran montrant la passerelle Internet attachée au VPC

### 4.4 Tables de routage

* **Table de routage publique**
  + Route 0.0.0.0/0 → Internet Gateway
  + Associée aux sous-réseaux publics
* **Table de routage privée :**
  + Routes internes uniquement
  + Associée aux sous-réseaux privés

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

Figure 5: Table de routage publique routes

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

Figure 6: Table de routage publique associations

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

Figure 7: Table de routage privée (associations)

**5.1 Environnement utilisé**

* **Cloud** : Amazon Web Services (AWS)
* **Région AWS** : us-east-1
* **Serveur Zabbix** :
  + Instance EC2
  + OS : Ubuntu Server
  + Déploiement via **Docker & Docker Compose**
* **Clients supervisés** :
  + Linux (Ubuntu)
  + Windows 10/11

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

Figure 8: Les instances

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

Figure 9: Groupe de sécurité Zabbix server

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

Figure 10: Groupe de sécurité de Client Linux

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

Figure 11: Groupe de sécurité Client Windows

J’ai ajouté Le ICMP dans les groupes de sécurités pour faire des pings pour assurer que les instances communiquent entre eux dans le même VPC.

## 5. Déploiement de Zabbix Server avec Docker :

### 5.1 Installation de Docker

Docker a été installé sur l’instance Linux destinée au serveur Zabbix afin de faciliter le déploiement.

Une image contenant texte, capture d’écran, affichage, logiciel

Le contenu généré par l’IA peut être incorrect.

Figure 12: Installation de Docker (docker --version)

### 5.2 Fichier docker-compose.yml

Zabbix a été déployé à l’aide de **Docker Compose** avec :

* zabbix-server-mysql
* zabbix-web-nginx-mysql
* mysql

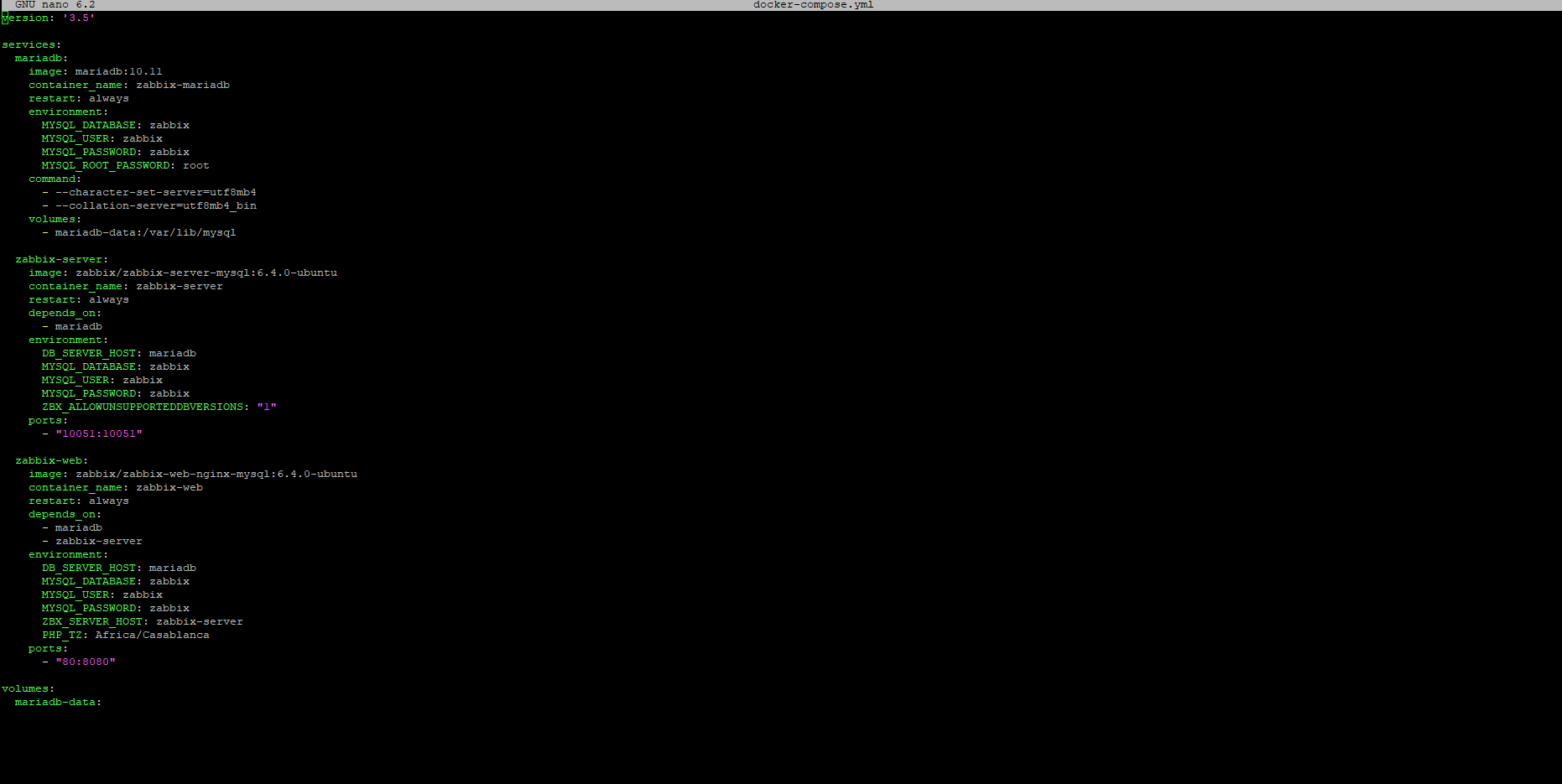


Figure 13: Contenu du fichier docker-compose.yml

### 5.3 Lancement des conteneurs

Les services ont été démarrés avec la commande :

sudo docker-compose up -d

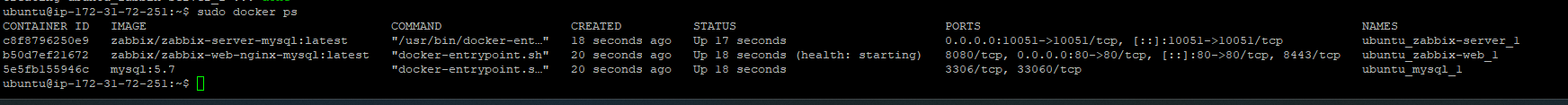


Figure 14: Résultat de docker ps montrant les conteneurs actifs

# 6. Accès à l’interface Web Zabbix :

L’interface Zabbix est accessible via un navigateur à l’adresse :

http:// 100.49.103.108 :80

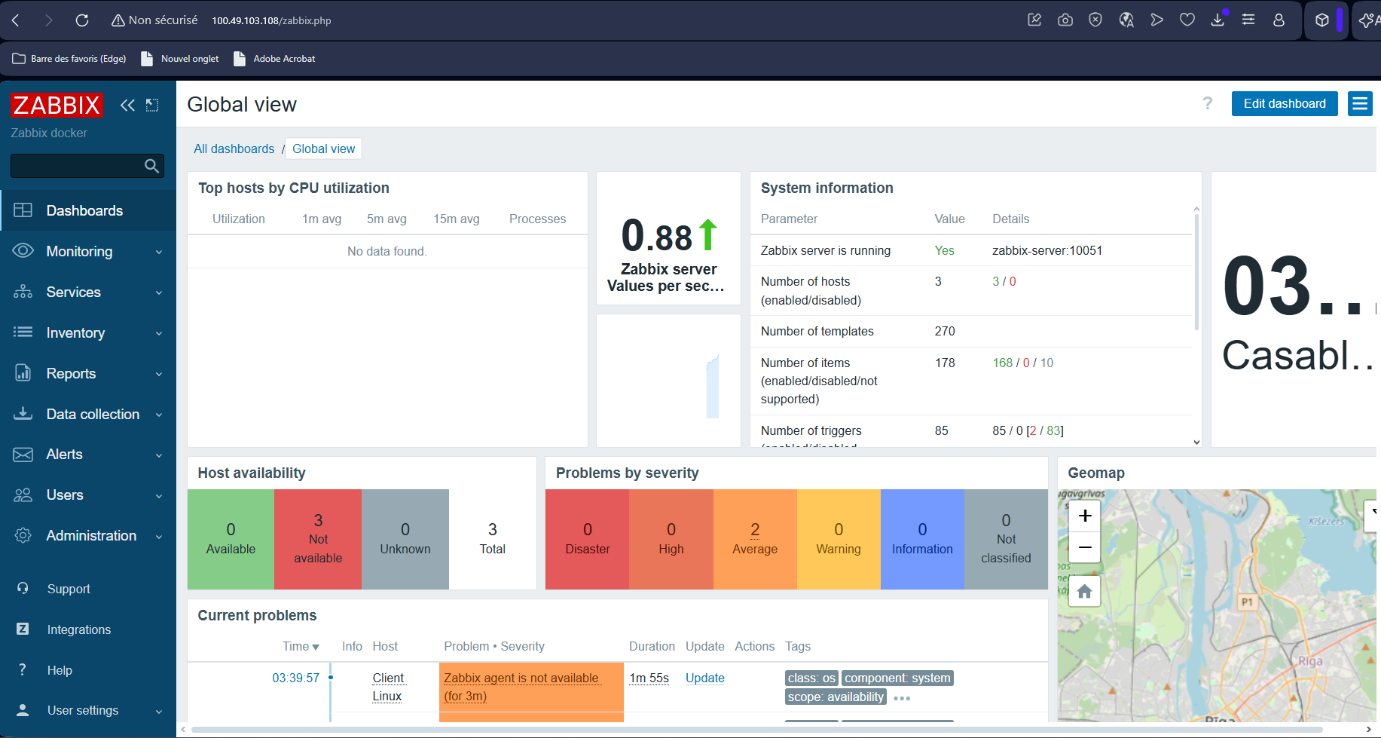


Figure 15: Interface Zabbix

# 7. Installation et configuration des agents Zabbix

### 7.1 Client Linux

* Installation de l’agent Zabbix
* Configuration du fichier zabbix\_agentd.conf
* Paramètres clés :
  + Server
  + ServerActive
  + Hostname

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Le contenu généré par l’IA peut être incorrect.

Figure 16: Service actif (systemctl status zabbix-agent)

### 7.2 Client Windows

* Installation de **Zabbix Agent (64-bit)**
* Configuration automatique lors de l’installation
* Vérification du fichier de log zabbix\_agentd.log

Une image contenant texte, capture d’écran, Logiciel multimédia, bleu vert

Le contenu généré par l’IA peut être incorrect.

Figure 17: Connexion RDP

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

Figure 18: Insertion d’IP de Serveur Zabbix a Client Windows

Une image contenant texte, capture d’écran, logiciel, Système d’exploitation

Le contenu généré par l’IA peut être incorrect.

Figure 19: Insertion d’IP de Serveur Active Zabbix a Client Windows

# Interface Zabbix Création des hôtes :

# 

Figure 20:Hotes Zabbix

Cette capture d'écran montre l'interface utilisée pour ajouter un nouvel hôte dans Zabbix. Vous pouvez voir les options permettant de spécifier le nom de l'hôte, son groupe, son adresse IP, etc.

# Conclusion :

Ce projet a permis de :

* Concevoir une architecture réseau AWS avec VPC et sous-réseaux
* Déployer un serveur de supervision moderne via **Docker Compose**
* Intégrer deux environnements distincts (Linux + Windows) via des agents Zabbix
* Mettre en pratique les concepts de supervision hybride

Améliorations futures possibles :

* Sécurisation : accès privé (VPN/Bastion), réduction des ports exposés publiquement
* Automatisation : Infrastructure as Code (Terraform/CloudFormation)
* Haute disponibilité : multi-AZ, base de données managée, sauvegardes et restauration