

Documentation Technique : Serveur de Supervision Zabbix

NEPAS COPIER

Table des matières

1. Présentation du projet.....	3
2. Informations sur le serveur.....	3
3. Installation de l'OS Ubuntu Server.....	3
Création de la VM sur Hyper-V.....	3
Configuration de l'OS.....	4
4. Architecture Zabbix.....	5
5. Configuration réseau.....	5
6. Services installés.....	5
7. Processus d'installation.....	5
a. Installation des prérequis.....	5
b. Installation et configuration de MySQL.....	6
c. Installation du serveur et de l'agent Zabbix.....	6
d. Importation du schéma de la base de données.....	6
e. Configuration de PHP et Apache.....	7
f. Démarrage du serveur Zabbix.....	7
g. Accès à l'interface Web.....	7
8. Configuration des hôtes supervisés.....	7
9. Tableaux de bord.....	8
10. Sécurité.....	9
10. Procédure d'installation pour utilisateur.....	9
Windows :.....	9
Linux :.....	9
Étape 1 : Télécharger et ajouter le dépôt Zabbix.....	9
Étape 2 : Installer Zabbix Agent.....	9
Étape 3 : Configurer Zabbix Agent.....	9
Étape 4 : Démarrer et Activer Zabbix Agent.....	10
Étape 5 : Ouvrir le Port du Pare-feu (si active).....	10
Découverte réseaux.....	10
Règles.....	11
Action.....	11
Ajout des hôtes.....	12
Suppression des hôtes.....	12

1. Présentation du projet

Les entreprises ByteMeUp, Pare-Fouine et Cloud Macronique ont décidé de s'associer pour répondre à un appel à projet d'une agence gouvernementale de cybersécurité. Ce projet simulera une/des cyberattaques sur des infrastructures diverses. Chaque entreprise ayant son domaine de compétences, elles ont décidé de monter chacune une infrastructure spécifique à celles-ci. Ces infrastructures auront un accès sécurisé vers l'extérieur, les 3 infrastructures seront interconnectées entre elles.

L'entreprise Cloud Macronique est spécialisée en réseau. Elle mettra en place une infrastructure avec un wifi sécurisé, un outil de supervision du réseau, un cœur de réseau et une segmentation réseau.

Au sein de cette entreprise, le projet consiste à mettre en place un serveur de supervision Zabbix pour surveiller l'état des équipements et serveurs dans l'infrastructure réseau. Zabbix est un outil open-source permettant de collecter, analyser et afficher des métriques de performance.

2. Informations sur le serveur

Nom du serveur : srv-supervision

Adresse IP : 172.16.20.16

Système d'exploitation : Ubuntu Server 22.04 LTS

Rôle : Serveur Zabbix

3. Installation de l'OS Ubuntu Server

Création de la VM sur Hyper-V

Dans l'Hyper-V allez dans créer un ordinateur virtuel et ceci s'affichera :

Spécifier le nom et l'emplacement

Avant de commencer

Spécifier le nom et l'emplacement

Spécifier la génération

Affecter la mémoire

Configurer la mise en réseau

Connecter un disque dur virtuel

Options d'installation

Résumé

Choisissez un nom et un emplacement pour cet ordinateur virtuel.


Le nom est affiché dans le Gestionnaire Hyper-V. Nous vous recommandons d'utiliser un nom qui vous permettra d'identifier facilement cet ordinateur virtuel, tel que le nom de la charge de travail ou du système d'exploitation invité.

Nom :

Vous pouvez créer un dossier ou utiliser un dossier existant pour stocker l'ordinateur virtuel. Si vous ne sélectionnez pas de dossier, l'ordinateur virtuel est stocké dans le dossier par défaut configuré pour ce serveur.

Stocker l'ordinateur virtuel à un autre emplacement

Emplacement :

 Si vous envisagez de créer des points de contrôle de cet ordinateur virtuel, choisissez un emplacement avec un espace libre suffisant. Les points de contrôle incluent les données des ordinateurs virtuels et peuvent nécessiter un espace considérable.

< Précédent

Configuration du serveur :

Nom : SRV-SUPERVISION

Mémoire : 4096 Mo

Réseaux : LAN

Disque Virtuel : 30Go

Configuration de l'OS

Pendant l'installation laisser toutes les configurations par default.

- Laisser en dhcp pour ensuite la changer.

- Activer le SSH server pour prendre à l'avenir la mais à distance.

- Configuration du du compte et du nom du serveur :

- Your name : admin
- Your server's name : srv-supervision
- Username : admin
- Password : r473iFhLU4

4. Architecture Zabbix

L'architecture Zabbix est composée des éléments suivants :

- Serveur Zabbix : Collecte et analyse les données des hôtes.
- Base de données MySQL : Stocke les configurations et les données de supervision.
- Interface Web : Permet l'affichage des données collectées sous forme de graphiques, tableaux et alertes.
- Agents Zabbix : Installés sur les hôtes supervisés pour remonter des métriques (CPU, RAM, réseau, etc.).

5. Configuration réseau

Adresse IP : 172.16.20.16/24

Passerelle par défaut : 172.16.20.254

DNS : 172.16.20.12

6. Services installés

Les services suivants ont été installés sur le serveur pour permettre le bon fonctionnement de Zabbix :

- Zabbix Server
- Zabbix Agent
- MariaDB (Base de données)
- Serveur Web Apache2
- PHP 8.1

7. Processus d'installation

Les étapes pour installer Zabbix sur le serveur sont les suivantes :

a. Installation des prérequis

Avant d'installer Zabbix, il faut s'assurer que le système est à jour :

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

Puis installer les paquets nécessaires :

```
sudo apt install -y apache2 mariadb-server mariadb-client php php-mysql libapache2-mod-php php-gd php-xml php-bcmath php-mbstring php-ldap php-zip php-curl
```

b. Installation et configuration de MySQL

Démarrage et sécurisation MySQL :

```
sudo systemctl start mariadb
```

```
sudo systemctl enable mariadb
```

```
sudo mysql_secure_installation
```

Création de la base de données et de l'utilisateur pour Zabbix :

```
sudo mysql -u root -p
```

Puis exécution de ces commandes dans MySQL :

```
CREATE DATABASE zabbix CHARACTER SET utf8mb4 COLLATE utf8mb4_bin;
```

```
CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'MonMotDePasse';
```

```
GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost';
```

```
FLUSH PRIVILEGES;
```

```
EXIT;
```

c. Installation du serveur et de l'agent Zabbix

Ajoute du dépôt zabbix :

```
wget https://repo.zabbix.com/zabbix/7.2/ubuntu/pool/main/z/zabbix-release/zabbix-release_7.2-1+ubuntu$(lsb_release -rs)_all.deb
```

```
sudo dpkg -i zabbix-release_7.2-1+ubuntu$(lsb_release -rs)_all.deb
```

```
sudo apt update
```

Installe le serveur Zabbix, l'interface web et l'agent :

```
sudo apt install -y zabbix-server-mysql zabbix-frontend-php zabbix-nginx-conf zabbix-agent
```

d. Importation du schéma de la base de données

Exécution des commandes suivantes :

```
zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -u zabbix -p zabbix
```

Puis modification du fichier de configuration /etc/zabbix/zabbix_server.conf :

```
DBPassword=MonMotDePasse
```

e. Configuration de PHP et Apache

Modification des paramètres PHP :

```
sudo nano /etc/php/*/apache2/php.ini
```

Changement de ces valeurs :

```
max_execution_time = 300
```

```
memory_limit = 128M
```

```
post_max_size = 16M
```

```
upload_max_filesize = 2M
```

```
date.timezone = Europe/Paris
```

Redémarrage d'Apache :

```
sudo systemctl restart apache2
```

f. Démarrage du serveur Zabbix

Activation et démarrage des services :

```
sudo systemctl restart zabbix-server zabbix-agent apache2
```

```
sudo systemctl enable zabbix-server zabbix-agent apache2
```

g. Accès à l'interface Web

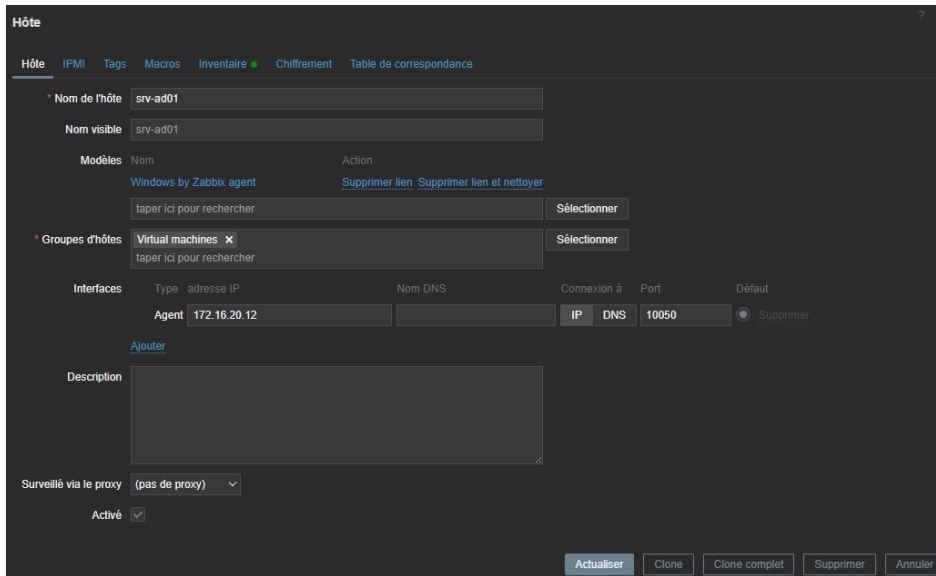
Accède à <https://172.16.20.16/zabbix> et suivre l'assistant de configuration.

8. Configuration des hôtes supervisés

Pour ajouter un hôte dans Zabbix :

1. Aller dans l'interface Web Zabbix.
2. Naviguer vers Collecte de données > Hôtes > Créer un hôte.
3. Spécifier les informations suivantes :
 - Nom de l'hôte
 - Adresse IP
 - Modèle (Template)
4. Sauvegarder les paramètres.

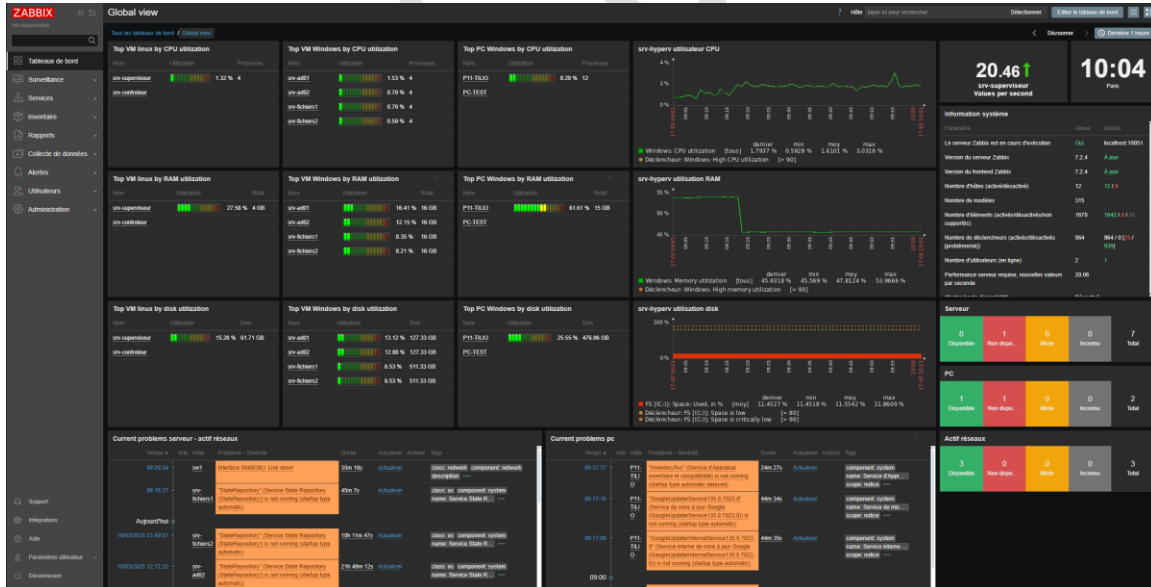
Exemple pour le serveur srv-ad01 :



9. Tableaux de bord

Les tableaux de bord permettent d'afficher des graphiques, des statistiques et des alertes pour les équipements supervisés.

Dans mon cas le tableau de bord possède plusieurs infos, voici l'exemple :



On peut voir :

- L'utilisation de la RAM, du CPU et des DISK en temps réel pour les VM linux et Windows et du serveur d'hypervision.
- Les informations du système ou est installer le Zabbix

- La disponibilité des Actif réseaux (les 2 switch et la bornes Wifi) et des serveurs (srv-ad01, srv-ad02, srv-controleur, srv-fichiers1, srv-fichiers1 , srv-hyperv et srv-supervision).
- Les alertes, problèmes, trier par date.
- Les ports des 2 switches avec le quel est up et down.

10. Sécurité

Sécurité :

- Utiliser un mot de passe fort pour les comptes administrateur.
- Activer le pare-feu UFW.

10. Procédure d'installation pour utilisateur

Windows :

Exécuter le fichier install_zabbix_admin dans \\cloud-macronique.local\Fichier\GPO\zabbix

Linux :

Étape 1 : Télécharger et ajouter le dépôt Zabbix

```
wget https://repo.zabbix.com/zabbix/7.2/ubuntu/pool/main/z/zabbix-release/zabbix-release_7.2-1+ubuntu$(lsb_release -rs)_all.deb
```

```
sudo dpkg -i zabbix-release_7.2-1+ubuntu$(lsb_release -rs)_all.deb
```

```
sudo apt update
```

```
sudo rpm -Uvh https://repo.zabbix.com/zabbix/7.2/rhel/$(rpm -E %rhel)/x86_64/zabbix-release-7.2-1.el$(rpm -E %rhel).noarch.rpm
```

```
sudo yum clean all
```

Étape 2 : Installer Zabbix Agent

```
sudo apt install zabbix-agent -y
```

```
sudo yum install zabbix-agent -y
```

Étape 3 : Configurer Zabbix Agent

```
sudo nano /etc/zabbix/zabbix_agentd.conf
```

Modifier ces lignes :

```
Server=172.16.20.16    # Adresse IP du serveur Zabbix
```

ServerActive=172.16.20.16

Hostname= « nom de l'hôte » # Nom de l'hôte

Étape 4 : Démarrer et Activer Zabbix Agent

```
sudo systemctl enable zabbix-agent
```

```
sudo systemctl start zabbix-agent
```

```
sudo systemctl status zabbix-agent
```

Étape 5 : Ouvrir le Port du Pare-feu (si active)

```
sudo ufw allow 10050/tcp
```

```
sudo ufw reload
```

Découverte réseaux

J'ai automatisé la découverte des pc Windows qui sont sur le DHCP ceci permet une automatisation et donc un gain de temps voici comment j'ai fait.

Règles

Règle de découverte

* Nom

Découvert par

* Plage d'adresses IP

* Intervalle d'actualisation

Contrôles simultanés maximum par type

* Vérifications

Type	Actions
agent Zabbix "agent.hostname"	Édition Supprimer
agent Zabbix "system.sw.os"	Édition Supprimer
Ajouter	

Critère d'unicité de l'équipement

adresse IP

agent Zabbix "agent.hostname"

agent Zabbix "system.sw.os"

Nom de l'hôte

Nom DNS

adresse IP

agent Zabbix "agent.hostname"

agent Zabbix "system.sw.os"

Nom visible

Nom de l'hôte

Nom DNS

adresse IP

agent Zabbix "agent.hostname"

agent Zabbix "system.sw.os"

Activé

Cette règle permet de faire une règle pour accepter que les pcs dans la plage d'@ 172.16.20.100-200. Et regarde ensuite si sont hostname est bon et le mettra pour le nom d'hôte et visible dans Zabbix.

Action

J'ai 2 actions une qui permet d'ajouter les hôtes et les lier à leurs modèles et l'autre de supprimer les hôtes inactifs.

Ajout des hôtes

Action

Action Opérations 2

* Nom Pc Windows zabbix agent

Conditions	Étiquette	Nom
A	Règle de découverte égal	Découverte Réseau dhcp windows

Ajouter

Pour que la condition soit valide il faut que la règle le soit aussi.

Opérations Détails

Ajouter aux groupes d'hôtes: pc

Lier les modèles: Windows by Zabbix agent

Ajouter

Opération permet d'ajouter l'hôtes dans un groupe pour une meilleur gestion. Et lui lie aussi un modèle dans notre cas l'agent Zabbix sur Windows.

Suppression des hôtes

Action

Action Opérations 1

* Nom Supp hôte inactif

Type de calcul Et A and B and C and D

Conditions	Étiquette	Nom	Action
A	IP hôte égal	172.16.20.100-200	Supprimer
B	Objet de découverte égal	Équipement	Supprimer
C	État de la découverte égal	Arrêté	Supprimer
D	Fonctionnement/Arrêt est supérieur ou égal à	3600	Supprimer

Ajouter

La condition A permet de vérifier que les hôtes dans la plage DHCP.

La condition B elle permet de vérifier que les hôtes dans Zabbix.

La condition C permet de vérifier si ça découverte réseaux est arrêté.

La condition D permet de vérifier depuis combien de temps dans notre cas 1h.

Et l'opération, elle supprime l'hôtes si les 4 conditions sont bonne.