TP 3 sécurité des réseaux : Zabbix

SAID FARAH - RAYAN
BOUZGARROU - Mohamed
QUISPE QUISPE - Adrian

GROUPE 1
BUT2 R&T
S4 2024-2025

Table des matières

Introduction

Dans un monde de plus en plus connecté, la sécurité des réseaux locaux (LAN) est devenue une préoccupation majeure pour les organisations de toutes tailles. Les attaques informatiques, de plus en plus sophistiquées et fréquentes, ciblent les infrastructures réseau pour voler des données, perturber les services ou causer des dommages financiers. Face à ces menaces, la supervision proactive de la sécurité est essentielle pour détecter rapidement les anomalies, les intrusions et les comportements suspects sur le réseau. Elle permet de réagir efficacement aux incidents de sécurité, de minimiser les impacts et de protéger les actifs de l'organisation.

Ce TP a pour objectif de vous familiariser avec Zabbix, une solution de supervision open source puissante et flexible, conçue pour surveiller l'état et les performances des réseaux, des serveurs, des applications et des services. À travers ce TP, vous découvrirez comment installer et configurer Zabbix, superviser des serveurs et des services réseau, mettre en place des alertes de sécurité, et visualiser les données collectées via une interface web intuitive.

En réalisant ce TP, vous acquerrez des compétences pratiques en cybersécurité, notamment en matière de surveillance proactive des réseaux et de réponse aux incidents de sécurité. Ces compétences sont essentielles pour protéger les infrastructures informatiques modernes contre les menaces croissantes et pour assurer la continuité des services dans un environnement numérique en constante évolution.

1. Préparation des VMs

Installer Ubuntu Server sur chaque VM.

Configurer une adresse IP fixe pour chaque VM.

Server Zabbix :

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:03:15:59 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.174/24 brd 192.168.0.255 scope global dynamic noprefixroute e
np0s3
```

Client 1 :

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:98:b3:4d brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.137/24 brd 192.168.0.255 scope global dynamic noprefixroute e
np0s3
```

Client 2 :

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:b9:fd:e7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.2/24 brd 192.168.0.255 scope global dynamic noprefixroute enp
```

S'assurer que les VMs peuvent communiquer entre elles.

Ping du server Zabbix vers Client 1 et 2 :

```
server-zabbix@server-zabbix-VirtualBox:~/Bureau$ ping -c1 192.168.0.137
PING 192.168.0.137 (192.168.0.137) 56(84) bytes of data.
64 bytes from 192.168.0.137: icmp_seq=1 ttl=64 time=1.45 ms

--- 192.168.0.137 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.448/1.448/1.448/0.000 ms
server-zabbix@server-zabbix-VirtualBox:~/Bureau$ ping -c1 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=64 time=1.74 ms

--- 192.168.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.740/1.740/1.740/0.000 ms
```

Mettre à jour le système :

```
root@server-zabbix-VirtualBox:/home/server-zabbix/Bureau# apt update && apt upgr
ade -y
Atteint :1 http://security.ubuntu.com/ubuntu noble-security InRelease
Atteint :2 http://archive.ubuntu.com/ubuntu noble InRelease
Atteint :3 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Atteint :4 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
2 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les v
oir.
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
The following upgrades have been deferred due to phasing:
  cloud-init ubuntu-drivers-common
0 mis à jour, 0 nouvellement installés, 0 à enlever et 2 non mis à jour.
root@server-zabbix-VirtualBox:/home/server-zabbix/Bureau#
```

2. Installation des prérequis sur le serveur Zabbix

Installer un serveur web (Apache), une base de données (MySQL) et PHP :

```
root@server-zabbix-VirtualBox:/home/server-zabbix/Bureau# apt install apache2 my
sql-server php libapache2-mod-php php-mysql -y
Lecture des listes de paquets... Fait
```

Pendant l'installation de MySQL, définir un mot de passe root fort :

Rayan/*-

3. Étapes du TP

1. Installation et configuration du serveur Zabbix

Ajout du dépôt Zabbix :

```
root@server-zabbix-VirtualBox:/home/server-zabbix/Bureau# wget https://repo.zabb
ix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest_6.0%2B
ubuntu24.04_all.deb
--2025-03-21 16:10:40--  https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/z
abbix-release/zabbix-release_latest_6.0%2Bubuntu24.04_all.deb
Résolution de repo.zabbix.com (repo.zabbix.com)… 2604:a880:2:d0::2062:d001, 178.
128.6.101
Connexion à repo.zabbix.com (repo.zabbix.com)|2604:a880:2:d0::2062:d001|:443… co
nnecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 5708 (5,6K) [application/octet-stream]
Enregistre : ‘zabbix-release_latest_6.0+ubuntu24.04_all.deb’

zabbix-release_late 100%[===================>]   5,57K  --.-KB/s    ds 0s

2025-03-21 16:10:41 (1,26 GB/s) - ‘zabbix-release_latest_6.0+ubuntu24.04_all.deb
’ enregistré [5708/5708]

root@server-zabbix-VirtualBox:/home/server-zabbix/Bureau# dpkg -i zabbix-release
_latest_6.0+ubuntu24.04_all.deb
Sélection du paquet zabbix-release précédemment désélectionné.
(Lecture de la base de données... 189223 fichiers et répertoires déjà installés.
)
Préparation du dépaquetage de zabbix-release_latest_6.0+ubuntu24.04_all.deb ...
Dépaquetage de zabbix-release (1:6.0-6+ubuntu24.04) ...
Paramétrage de zabbix-release (1:6.0-6+ubuntu24.04) ...
root@server-zabbix-VirtualBox:/home/server-zabbix/Bureau#
```

```
root@server-zabbix-VirtualBox:/home/server-zabbix/Bureau# apt update
Atteint :1 http://archive.ubuntu.com/ubuntu noble InRelease
Atteint :2 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Atteint :3 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Atteint :4 http://security.ubuntu.com/ubuntu noble-security InRelease
Réception de :5 https://repo.zabbix.com/zabbix/6.0/ubuntu noble InRelease [3 220 B]
Réception de :6 https://repo.zabbix.com/zabbix/6.0/ubuntu noble/main Sources [17,5 k
B]
Réception de :7 https://repo.zabbix.com/zabbix/6.0/ubuntu noble/main amd64 Packages
[34,3 kB]
Réception de :8 https://repo.zabbix.com/zabbix/6.0/ubuntu noble/main all Packages [6
 947 B]
62,0 ko réceptionnés en 5s (13,5 ko/s)
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
2 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.
root@server-zabbix-VirtualBox:/home/server-zabbix/Bureau#
```

Installation des paquets Zabbix :

```
root@server-zabbix-VirtualBox:/home/server-zabbix/Bureau# apt install zabbix-server-
mysql zabbix-frontend-php zabbix-apache-conf zabbix-agent -y
Lecture des listes de paquets... Fait
```

Configuration de la base de données Zabbix :

```
server@debian:~$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 30
Server version: 10.5.28-MariaDB-0+deb11u1 Debian 11

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 [(none)]> CREATE DATABASE zabbix character set utf8 collate utf8_bin;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]> CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'Rayaaaaan/*-';

Query OK, 0 rows affected (0,004 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost' WITH
GRANT OPTION;
Query OK, 0 rows affected (0,002 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]> EXIT;
Bye
server@debian:~$
```

Configuration du serveur Zabbix :

```
#
# Mandatory: no
# Default:
DBPassword=Rayaaaaan/*-
```

Initialisation de la base de données Zabbix :

```
server@debian:~$ sudo mysql -u zabbix -p zabbix < zabbix-6.0.0/database/mysql/sc
hema.sql
Enter password:
server@debian:~$ sudo mysql -u zabbix -p zabbix < zabbix-6.0.0/database/mysql/
data.sql                images.sql              schema.sql
double.sql              Makefile.am
history_pk_prepare.sql  Makefile.in
server@debian:~$ sudo mysql -u zabbix -p zabbix < zabbix-6.0.0/database/mysql/im
ages.sql
Enter password:
server@debian:~$ sudo mysql -u zabbix -p zabbix < zabbix-6.0.0/database/mysql/da
ta.sql
Enter password:
```

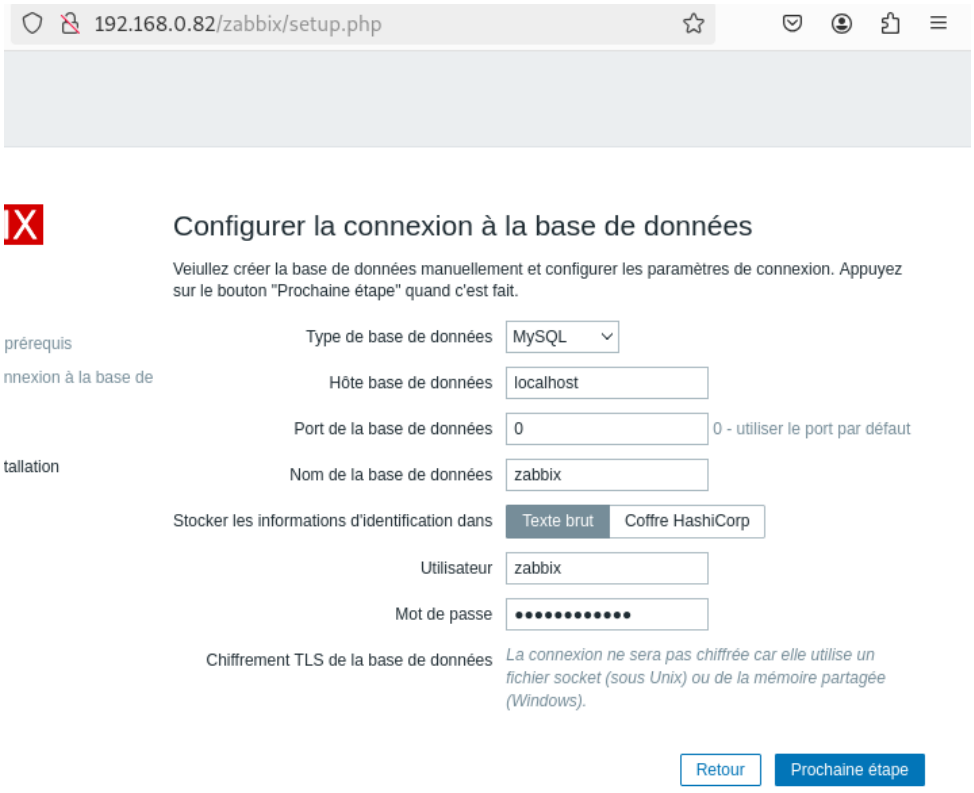
Configuration du frontend Zabbix :

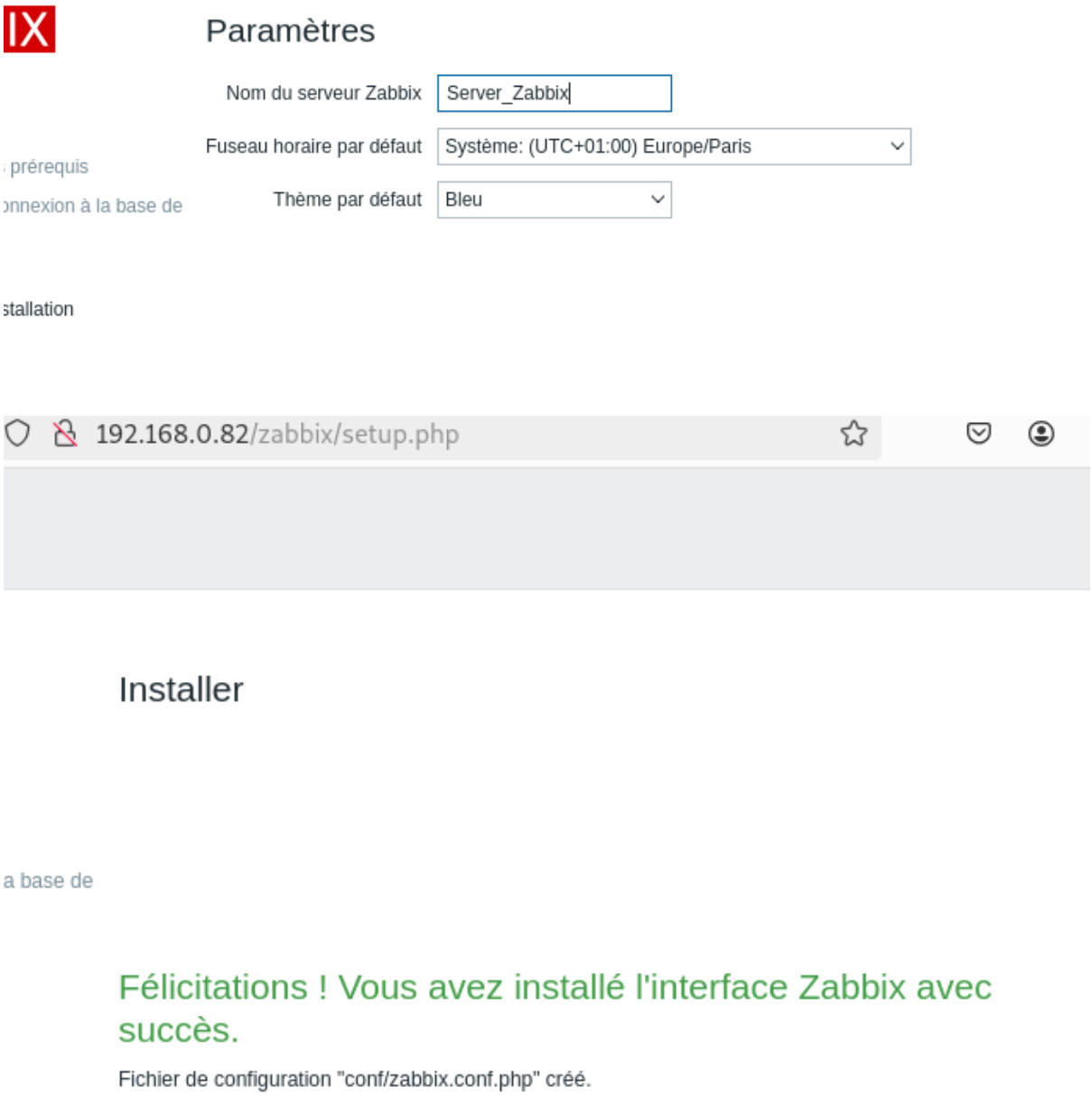
```
  GNU nano 7.2                        /etc/zabbix/apache.conf *
        php_value max_input_time 300
        php_value max_input_vars 10000
        php_value always_populate_raw_post_data -1
    </IfModule>

    <IfModule mod_php7.c>
        php_value max_execution_time 300
        php_value memory_limit 128M
        php_value post_max_size 16M
        php_value upload_max_filesize 2M
        php_value max_input_time 300
        php_value max_input_vars 10000
        php_value always_populate_raw_post_data -1
        php_value date.timezone Europe/Paris
    </IfModule>
</Directory>
```

Redémarrage des services Zabbix et Apache :

```
server@debian:~$ sudo systemctl restart zabbix-server zabbix-agent apache2

server@debian:~$
server@debian:~$ sudo systemctl enable zabbix-server zabbix-agent apache2
Synchronizing state of zabbix-server.service with SysV service script with /lib/
systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-server

Synchronizing state of zabbix-agent.service with SysV service script with /lib/s
ystemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
Synchronizing state of apache2.service with SysV service script with /lib/system
d/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
```

Accès à l'interface web de Zabbix :





2. Configuration des agents Zabbix sur les clients

1. Installation de l'agent Zabbix sur les clients :

```
client1@Client1:~$ wget https://repo.zabbix.com/zabbix/6.0/debian/pool/main/z/zabbix-release/zabbix-release_latest_6.0%2Bdebian11_all.deb
client1@Client1:~$ sudo dpkg -i zabbix-release_latest_6.0+debian11_all.deb
Sélection du paquet zabbix-release précédemment désélectionné.
client1@Client1:~$ apt update
```

```
client1@Client1:~$ sudo apt install zabbix-agent -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés
```

2. Configuration de l'agent Zabbix :

```
# Default:
# Server=

Server=192.168.0.82
```

```
# ServerActive=

ServerActive=192.168.0.82
```

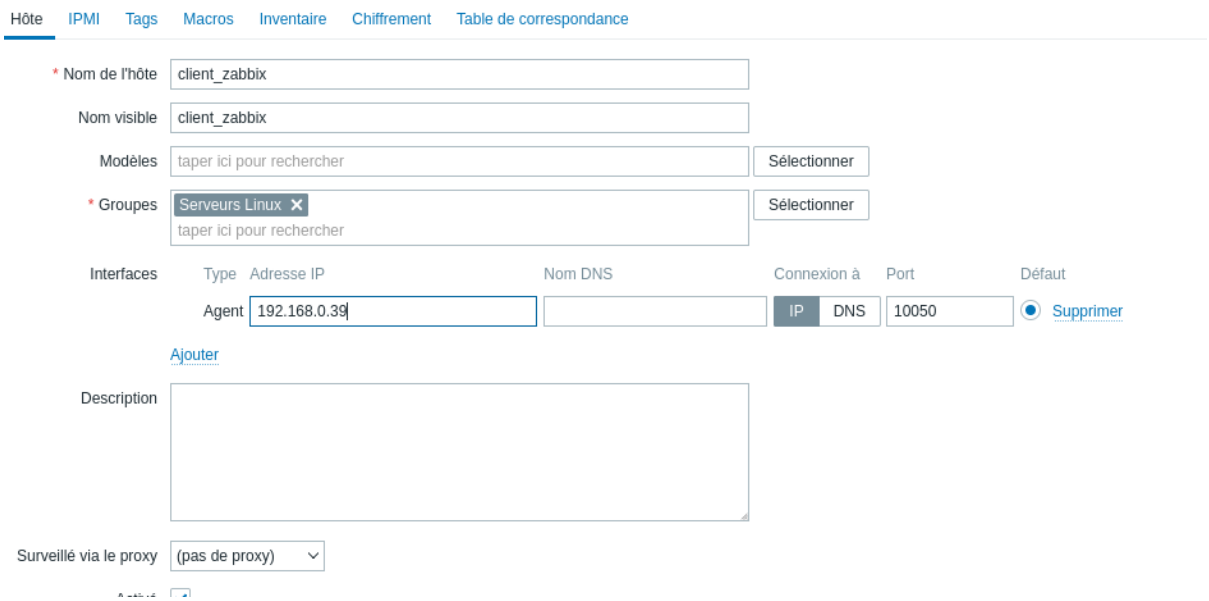
```
# Default:
# Hostname=

Hostname=client_zabbix
```

3. Redémarrage de l'agent Zabbix :

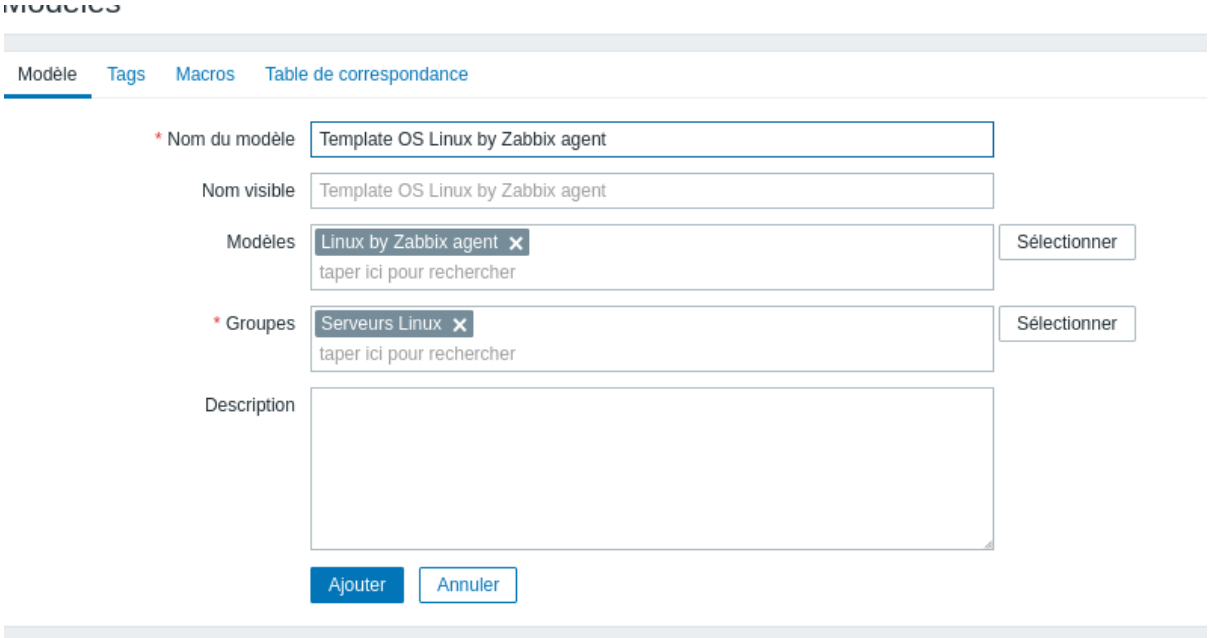
```
client1@Client1:~$ sudo systemctl restart zabbix-agent
sudo systemctl enable zabbix-agent
Synchronizing state of zabbix-agent.service with SysV service script with /lib/s
ystemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
client1@Client1:~$
```

3. Ajout des clients à superviser dans Zabbix

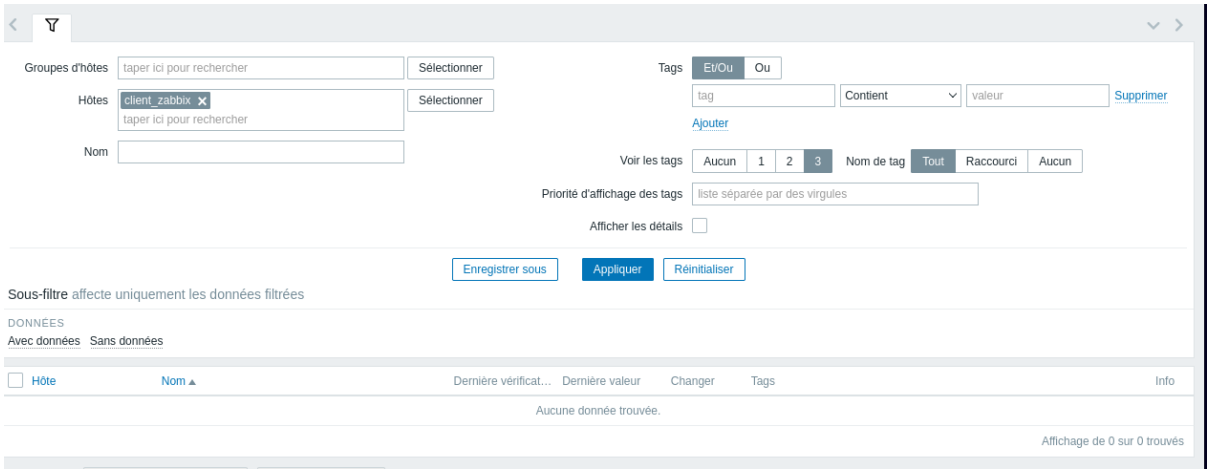
1. Ajout d'un hôte :



2. Association de modèles (templates) :



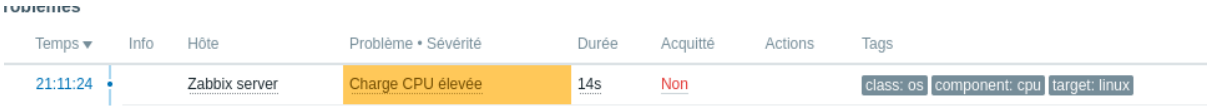
3. Vérification de la supervision :



4. Mise en place d'une alerte de sécurité simple

1. Création d'un déclencheur (trigger) :

2. Vérification du déclenchement de l'alerte :



4. Résultats attendus

Un serveur Zabbix opérationnel et accessible via l'interface web est le premier résultat attendu. Cela signifie que le serveur doit être correctement installé, configuré, et que l'interface web doit être accessible via un navigateur. Les utilisateurs doivent pouvoir se connecter avec les identifiants fournis, tels que Admin et zabbix par défaut. Ensuite, les agents Zabbix doivent être installés et configurés sur les clients. Ces agents doivent être capables de communiquer avec le serveur Zabbix, en utilisant l'adresse IP du serveur et un nom d'hôte unique pour chaque client. Les clients doivent ensuite être supervisés par le serveur Zabbix, avec des données collectées et affichées dans l'interface web. Cela inclut des métriques comme l'utilisation du CPU, la mémoire, le disque, et le réseau, visibles dans des sections comme "Dernières données". Enfin, une alerte de sécurité simple doit être mise en place et fonctionnelle. Cela implique la création d'un déclencheur pour surveiller un paramètre spécifique, comme l'utilisation du CPU, et la génération d'une alerte lorsque le seuil défini est dépassé. L'alerte doit être visible dans la section "Problèmes" de l'interface web.

5. Questions ouvertes pour les étudiants

Quels sont les autres éléments de sécurité que vous pourriez superviser avec Zabbix dans un réseau LAN ?

Zabbix peut superviser de nombreux éléments de sécurité dans un réseau LAN, tels que les tentatives de connexion échouées, les ports ouverts, les modifications de fichiers critiques, les activités réseau suspectes, et les mises à jour de sécurité. Il peut également surveiller les logs d'authentification, détecter des services non autorisés, et analyser le trafic réseau pour identifier des comportements anormaux.

Comment Zabbix peut-il aider à améliorer la réponse aux incidents de sécurité ?

Zabbix améliore la réponse aux incidents de sécurité en fournissant des alertes en temps réel, une visualisation centralisée des données, et la possibilité d'automatiser des tâches de réponse. Par exemple, il peut exécuter des scripts pour bloquer une adresse IP suspecte ou notifier les administrateurs via des canaux comme l'email ou Slack. Cela permet une réaction rapide et efficace aux menaces.

Quels sont les défis liés à la supervision de la sécurité dans un environnement de production réel ?

Les défis incluent la gestion des faux positifs (alertes non pertinentes), la volumétrie des données à surveiller, la complexité des environnements hétérogènes (multiples systèmes et applications), et la nécessité de maintenir à jour les règles de surveillance. De plus, la supervision doit être performante et scalable pour ne pas impacter les performances du réseau.

Comment Zabbix se compare-t-il à d'autres solutions de supervision open source ou commerciales ?

Zabbix est une solution open source flexible et extensible, mais elle peut nécessiter une configuration manuelle plus poussée que des outils commerciaux comme PRTG ou SolarWinds, qui offrent des interfaces plus conviviales. Comparé à Nagios, Zabbix est plus intuitif et intégré, tandis que Prometheus est plus adapté à la supervision de métriques dans des environnements cloud.

Quelles sont les compétences nécessaires pour administrer et utiliser efficacement Zabbix dans un contexte de sécurité ?

Les compétences nécessaires incluent des connaissances de base en réseaux (TCP/IP, DNS), en administration système (Linux/Windows), en bases de données (MySQL, PostgreSQL), et en scripting (Bash, Python). Une compréhension des concepts de cybersécurité, comme la détection d'intrusion et la gestion des vulnérabilités, est également essentielle pour configurer et interpréter les alertes et les tableaux de bord.

Conclusion

Ce TP permet aux étudiants de se familiariser avec Zabbix et de comprendre son utilité pour superviser la sécurité d'un réseau LAN. Ils apprendront à installer et configurer un serveur Zabbix, déployer des agents sur des clients, superviser des éléments critiques comme le CPU et la mémoire, et configurer des alertes. Ces compétences pratiques sont essentielles pour la surveillance proactive des réseaux et la réponse aux incidents de sécurité, des aspects cruciaux dans la protection des infrastructures informatiques modernes.