|B3| TP N° 2: Supervision

Belerge Jérémy BTS SIO 2

Contextualisation :

Suite à une recrudescence de cyberattaques, le système d'information de la section SIO doit se renforcer. Deux étapes sont prévues :

1. **Mise en place d'un serveur de supervision**
2. **Mise en œuvre d'une solution de firewalling**

Ce TP se concentre sur la **mise en place de la supervision**.

🎯 Objectif

Tester deux solutions de supervision dans un environnement laboratoire et **justifier le choix de l'outil retenu**, en binôme. **Aucun critère économique n'est imposé.**

Sommaire

Consignes:

-Zabbix c'est quoi ?

Zabbix est un logiciel libre de supervision et de monitoring permettant de surveiller l'état d'infrastructures IT, réseaux, serveurs, applications et services en temps réel. Il collecte des données, génère des alertes et propose des tableaux de bord pour analyser la performance des systèmes surveillés.

Source : Wikipedia

Zabbix surveille en continu les serveurs, équipements réseau (commutateurs, routeurs), bases de données, services cloud et applications. Il fonctionne grâce à une architecture centralisée composée d'un serveur Zabbix, d'agents installés sur les machines à surveiller, d'une interface Web et éventuellement de proxys. Les données collectées permettent de visualiser l'état des ressources, générer des rapports et planifier la capacité

Source : Zabbix.com

Consignes:

-Installation de Zabbix

On installe le dêpot de Zabbix :

```
root@Jrm:~# wget https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_7.0-2+ubuntu22.04_all.deb
```

Puis on installe Mariadb :

```
root@Jrm:~# apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent -y
```

Puis MariaDB

```
root@Jrm:~# apt install mariadb-server -y
```

Puis MySql :

```
root@Jrm:~# mysql_secure_installation
```

On créer la base de donnée :

```
root@Jrm:~# mysql -u root -p
```

Consignes:

-Installation de Zabbix

A l'interieur on y ajoute :

```
CREATE DATABASE zabbix character set utf8mb4 collate utf8mb4_bin;
CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'motdepassefort';
GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```

On importe le schéma de la base de donnée Zabbix :

```
root@Jrm:~# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -p zabbix
```

```
root@Jrm:~# nano /etc/zabbix/zabbix_server.conf
```

```
DBUser=zabbix

### Option: DBPassword
#       Database password.
#       Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=Sio2025
```

Consignes:

-Installation de Zabbix

Puis on redémarre nos services :

```
root@Jrm:~# systemctl restart zabbix-server zabbix-agent apache2
root@Jrm:~# systemctl enable zabbix-server zabbix-agent apache
```

Depuis une machine client en tapant NOTREIP/zabbix on obtient :

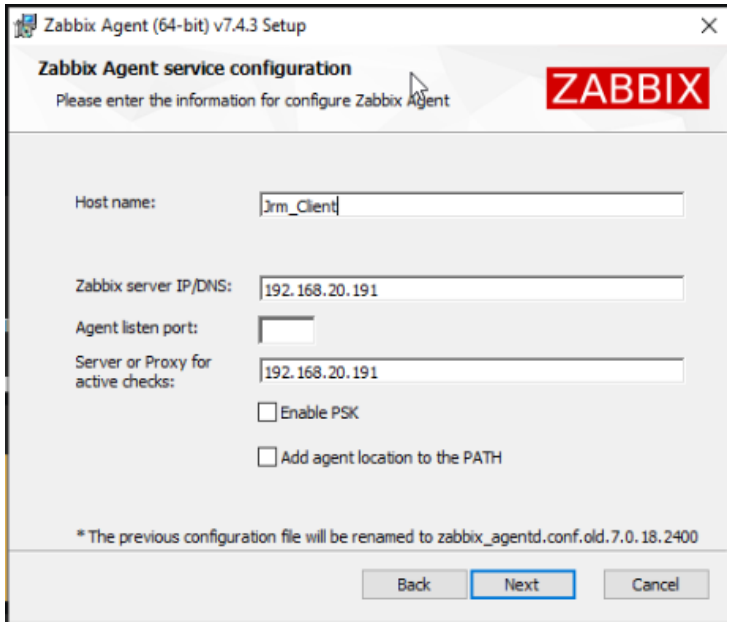
User : Admin
Password : zabbix

Consignes:

-Installation client Windows de Zabbix

Depuis une machine cliente on installe l'agent Zabbix disponible ici :

Puis on lance le .exe



Puis on y rentre notre IP : 192.168.20.191

Consignes:

-Installation client Linux de Zabbix

Pour installer le client Zabbix sous linux il suffit de suivre les étapes ci-dessous :

On installe le dêpot Zabbix sur le client :

```
-wget
https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-release_7.0-2+debian12_all.deb

-sudo dpkg -i zabbix-release_7.0-2+debian12_all.deb

-sudo apt update -y
```

Ensuite on installe l'agent Zabbix

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

Puis on rentre et modifie le fichier de configuration de l'agent

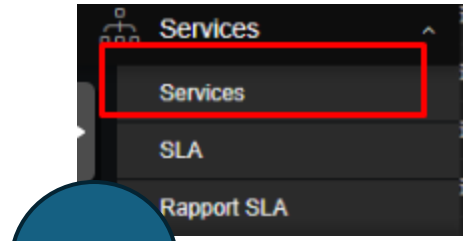
```
sudo nano /etc/zabbix/zabbix_agentd.conf
```

Server= 192.168.20.191
ServerActive=192.168.20.191
Hostname=nom_de_ta_machine

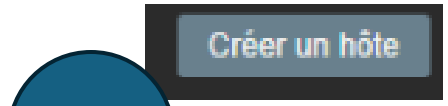
Consignes:

-Ajout d'un hôte

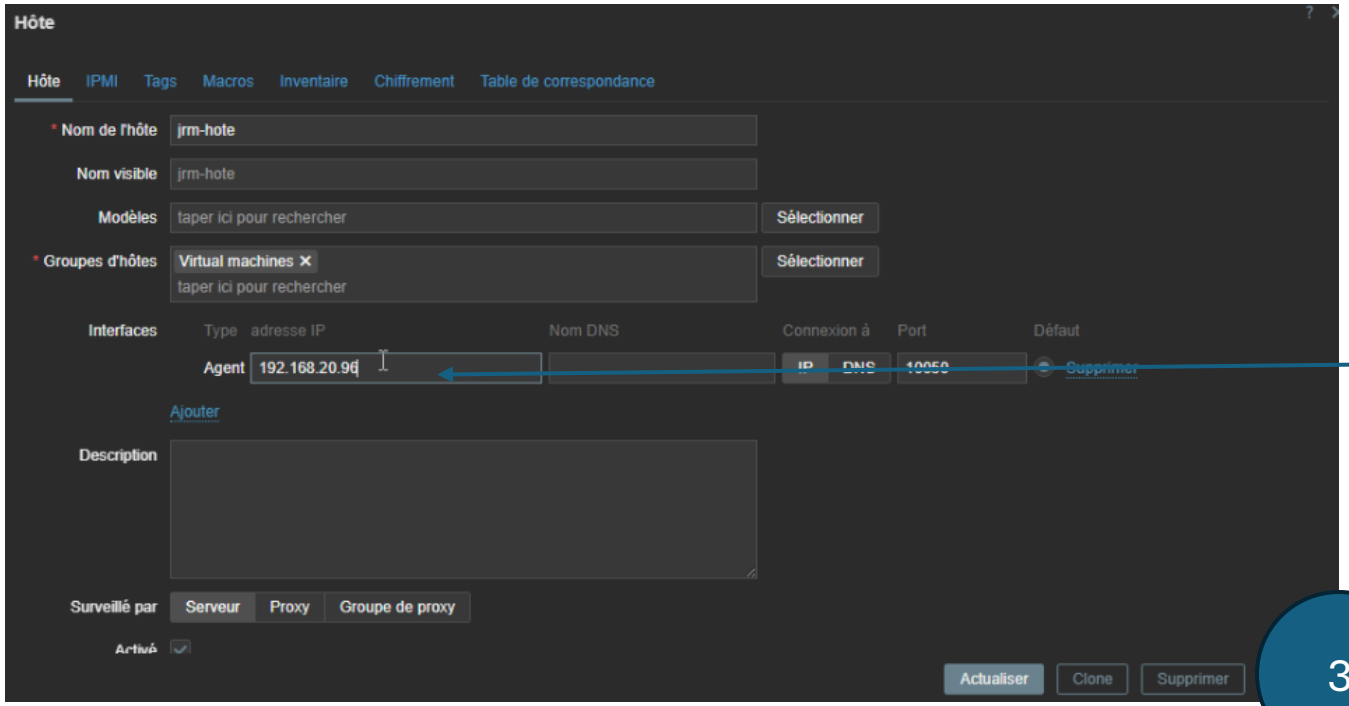
Depuis une Zabbix on ajoute notre client :



1



2



On rentre l'IP du client

3

Consignes:

-Zabbix pour les switch

```
SW-APGR7(config)#snmp-server community groupe7 RO
```

snmp-server → active ou configure le service **SNMP** sur le switch (outil de gestion à distance).

community → crée une **communauté SNMP**, c'est comme un mot de passe partagé.
groupe7 → nom de la communauté (choisi par l'administrateur).

RO → signifie **Read Only** : accès en **lecture seule**, donc on peut lire les infos mais

pas changer la configuration

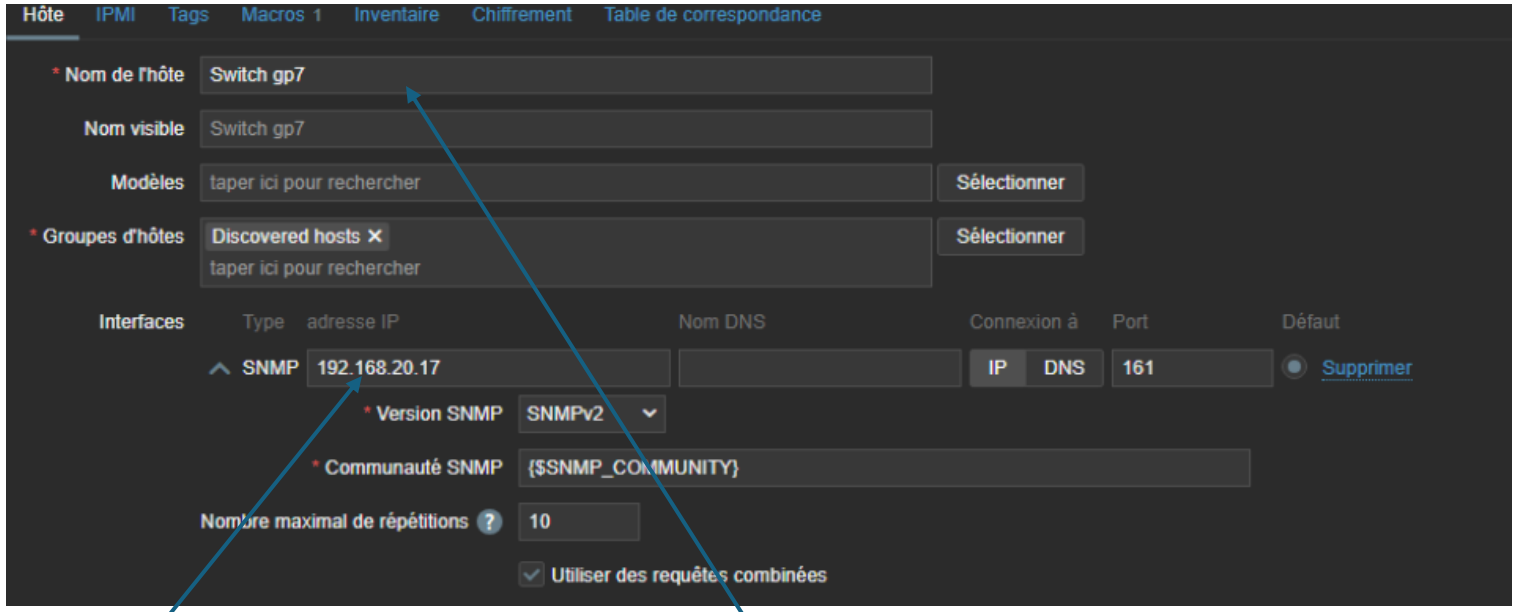
```
root@APGR7LAMP:~# apt install snmp
```

Puis on installe le service snmp sur notre serveur Zabbix.

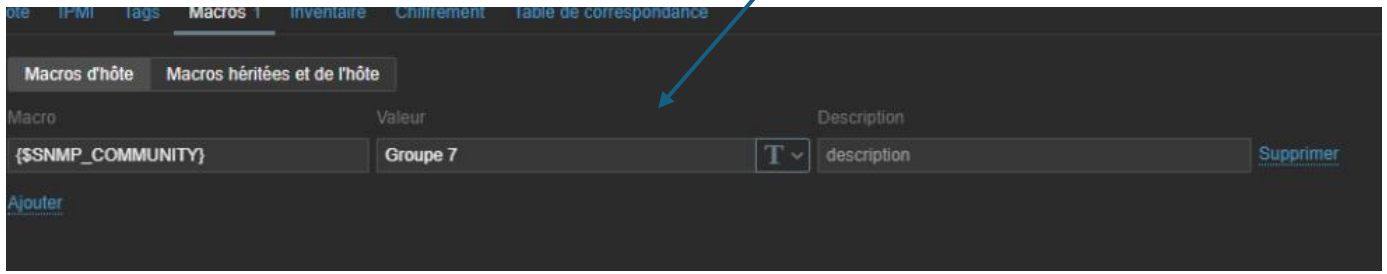
Consignes:

-Zabbix pour les switch

Depuis : "Configuration" > "Hôtes"



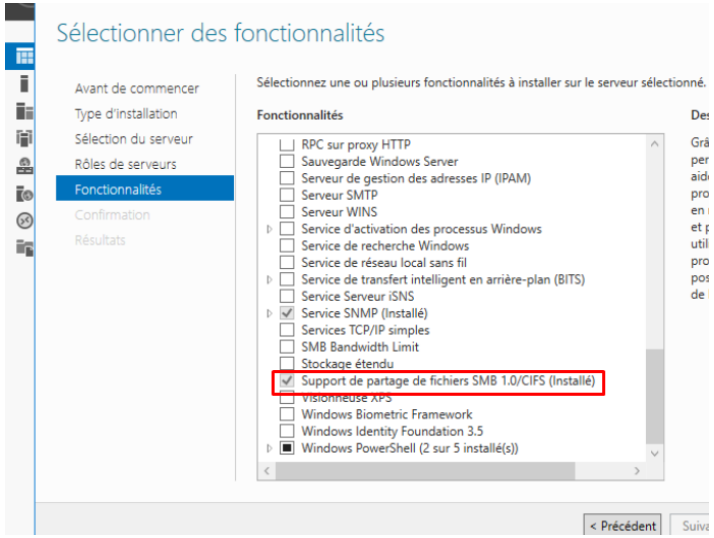
On ajoute l'IP de notre switch et un nom d'hôtes , cela génèrera une communauté SNMP a mettre dans l'option "macros" puis il faudra entrée le nom de la communauté "groupe 7'



Consignes:

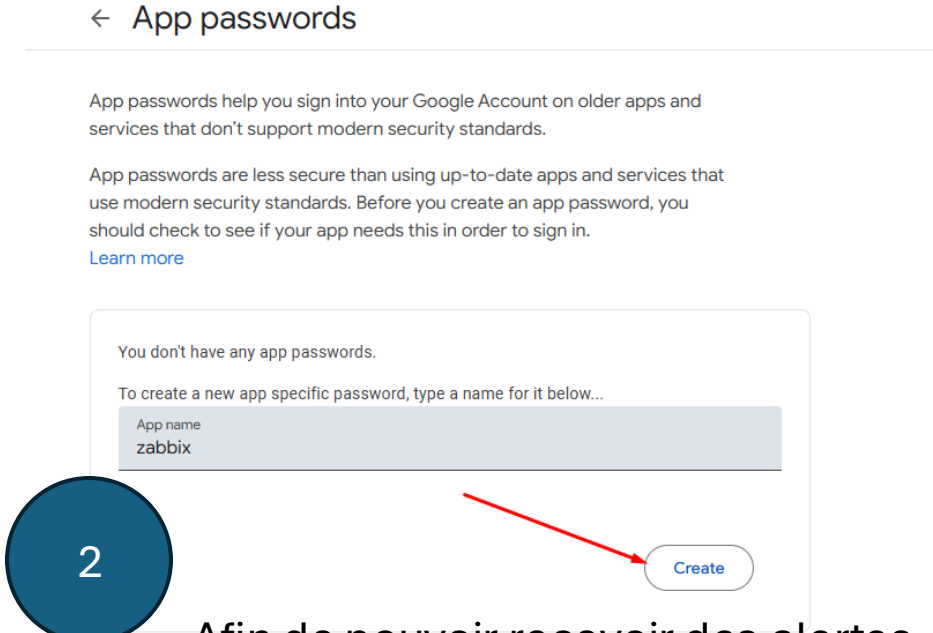
-Pour windows serveur?

-Envoyer une alerte par mail



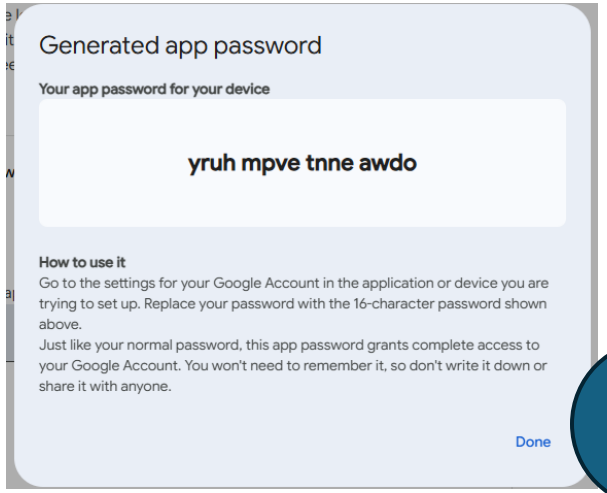
1

Zabbix utilise le protocole **SMB** pour accéder à des fichiers partagés sur Windows



2

Afin de pouvoir recevoir des alertes par email il nous faut accéder a cette page , y rentrer le nom le l'alerte

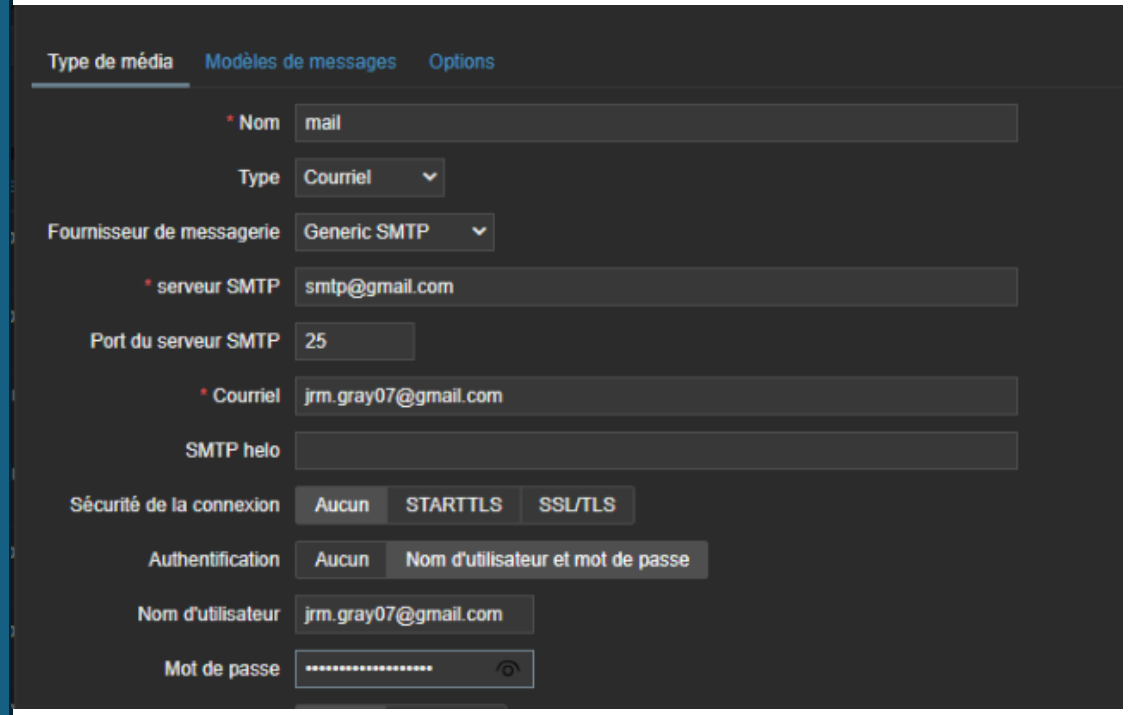


3

"Puis, un code apparaîtra.
Cela permettra à Zabbix de se connecter au mail

Consignes:

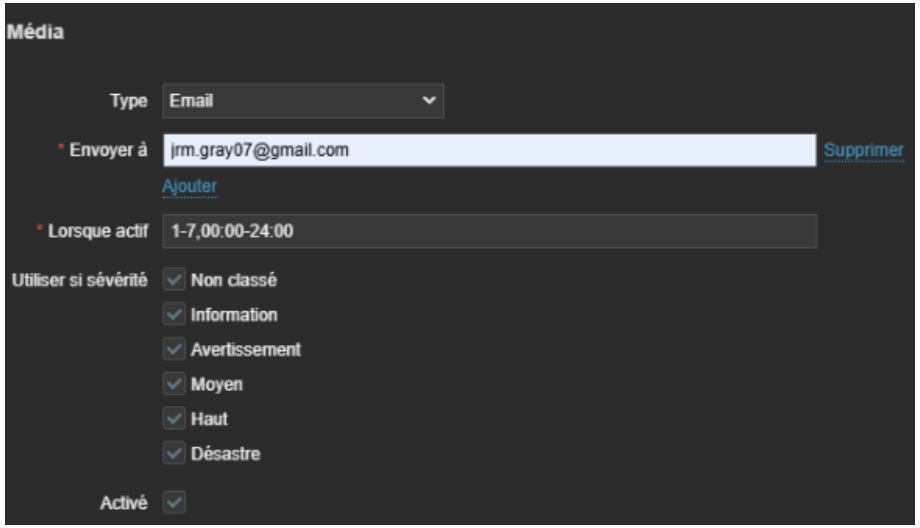
-Envoyer une alerte par mail



Il faudra créer un type de média pour y entrer notre mail qui recevra les alertes, dans la catégorie courriel, puis dans nom d'utilisateur, et y insérer le mot de passe qui apparaît dans la diapo précédente.

Depuis: Administration > Utilisateurs > crée un nouvel utilisateur > Média

Ce paramétrage permet à Zabbix d'envoyer automatiquement des notifications d'alerte à une personne par email (machine , switch , serveur)

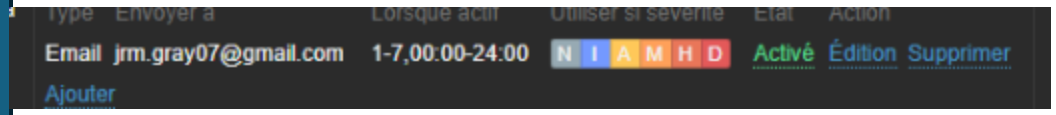


Consignes:

-Envoyer une alerte par mail

Il faut bien constater que ton e-mail est enregistré dans Zabbix pour vérifier que tu recevras les alertes par mail
Depuis : Administration > Utilisateurs> Média

Cela signifie que Zabbix enverra automatiquement des alertes à cette adresse lors d'un événement critique

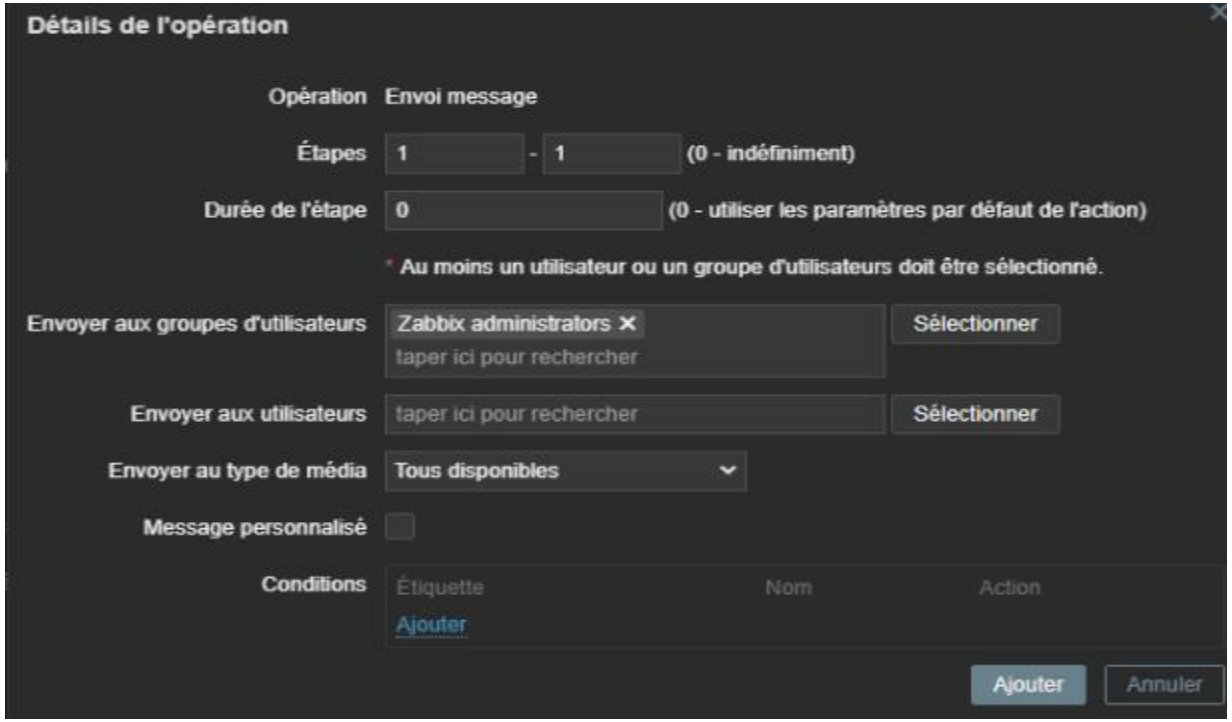


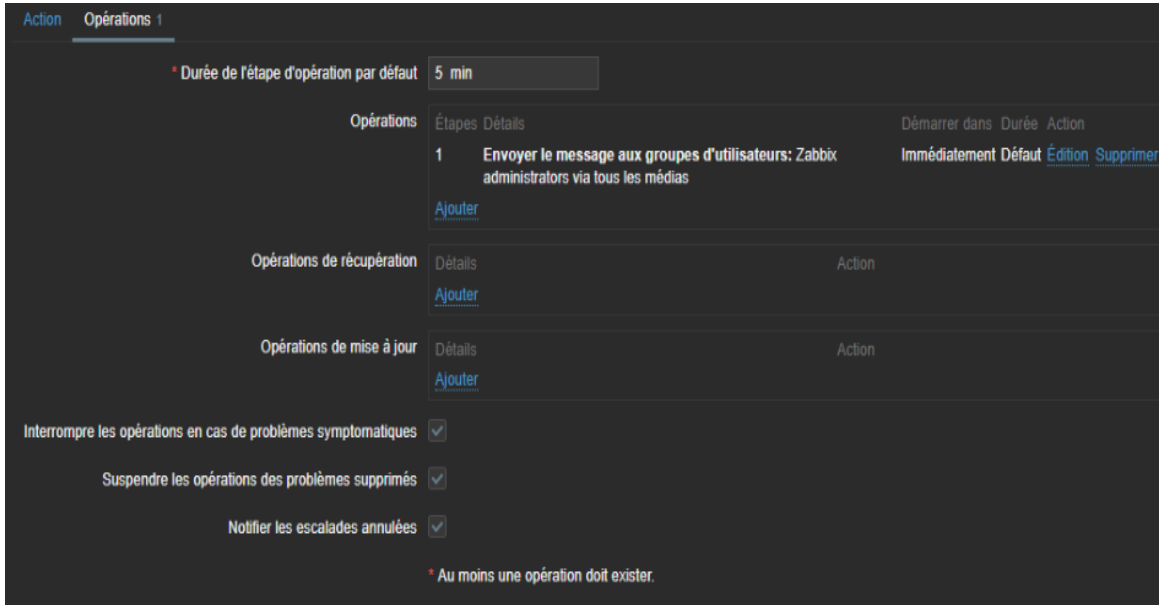
Ensuite il faudra créer une action (Alertes > Actions > Action de déclencheur > Créer une action)
On rentre le nom de l'action :

Consignes:

-Envoyer une alerte par mail

Dans la section Opérations, spécifie le ou les groupes d'utilisateurs à qui les alertes doivent être envoyées





C'est le temps en minutes (ici 5 min) pendant lequel une alerte est considérée active. Cela évite d'envoyer des notifications trop fréquemment si le problème persiste

Consignes:

-Conclusion

En conclusion, avec la configuration réalisée dans Zabbix, tu recevras bien un e-mail dès qu'une alerte est déclenchée : le système enverra automatiquement un message aux adresses e-mail ou groupes définis pour prévenir immédiatement d'un incident.

Zabbix est un outil de supervision centralisé pour les réseaux, serveurs, équipements et applications. Il permet :

- De surveiller en temps réel la disponibilité, la performance et l'état de tous tes équipements informatiques (via SNMP, agents, etc.).
- De générer des alertes automatiques dès qu'un problème ou une anomalie est détecté sans avoir besoin de surveiller en continu l'interface
- D'automatiser l'envoi de notifications (e-mail, SMS, messagerie, etc.) aux bonnes personnes pour une réaction rapide en cas d'incident.