Supervision Zabbix et PRTG

HEGO Maxence

Objectif :

Afin de renforcer la sécurité de notre **SI**, on souhaite mettre en place un **outil de supervision.** Lors de ce TP on va ainsi installer et tester deux outils de supervision : **Zabbix et PRTG** dans le but de les comparer et voir lequel est le plus adapter à nos besoins.

Partie 1 – Installation et configuration Zabbix

Note :

On commence par tester Zabbix, voyons comment installer et configurer ce service dans l'objectif de monitorer notre SI.

Partie A – Installation Zabbix

Note :

On installe le serveur Zabbix sur une debian 12, on suit ce tutoriel disponible sur le site de zabbix : https://www.zabbix.com/download?os_distribution=debian

Installation BDD :

Mise à jour du système :

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

Installation de la base de données, on choisi mariadb :

```
apt install mariadb-server mariadb-client -y
```

Terminer installation de Mariadb :

```
mysql_secure_installation
```

Installation des dépendances :

```
apt install apache2 php php-mysql php-mysqli php-ldap php-bcmath php-mbstring php-gd php-xml php-curl -y
```

Ajout du repository Zabbix :

```
wget https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debian12_all.deb
```

```
dpkg -i zabbix-release_6.4-1+debian12_all.deb
```

```
apt update
```

Installation de Zabbix server, Frontend et Agent :

```
apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent -y
```

Configuration de la BDD :

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

Dans mariadb :

```
CREATE DATABASE zabbix CHARACTER SET utf8mb4 COLLATE utf8mb4_bin;
CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'sio%2025';
GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```

Importation du schéma de la BDD :

```
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -p zabbix
```

Configuration de Zabbix Server :

```
nano /etc/zabbix/zabbix_server.conf
```

Dans le fichier de configuration on change ces lignes :

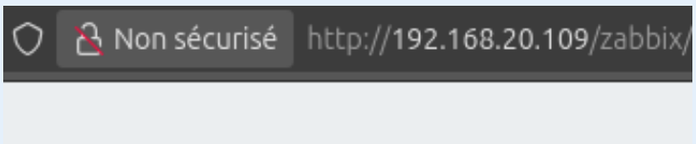
```
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=votre_mot_de_passe_securise
```

Activation des services :

```
systemctl restart apache2
systemctl enable zabbix-server zabbix-agent
systemctl start zabbix-server zabbix-agent
```

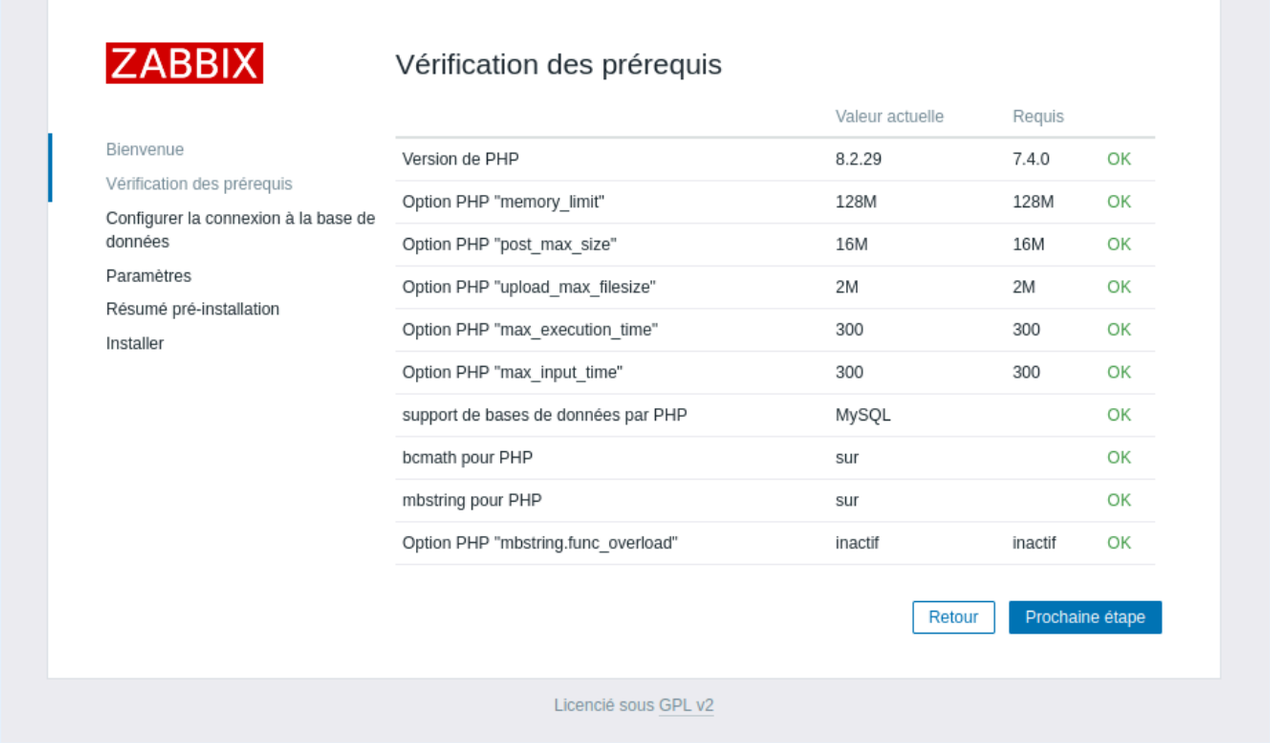
Interface Web :

On vérifie que l'installation fonctionne en se connectant à l'interface web : http://192.168.20.109/zabbix (IP de notre serveur Zabbix)

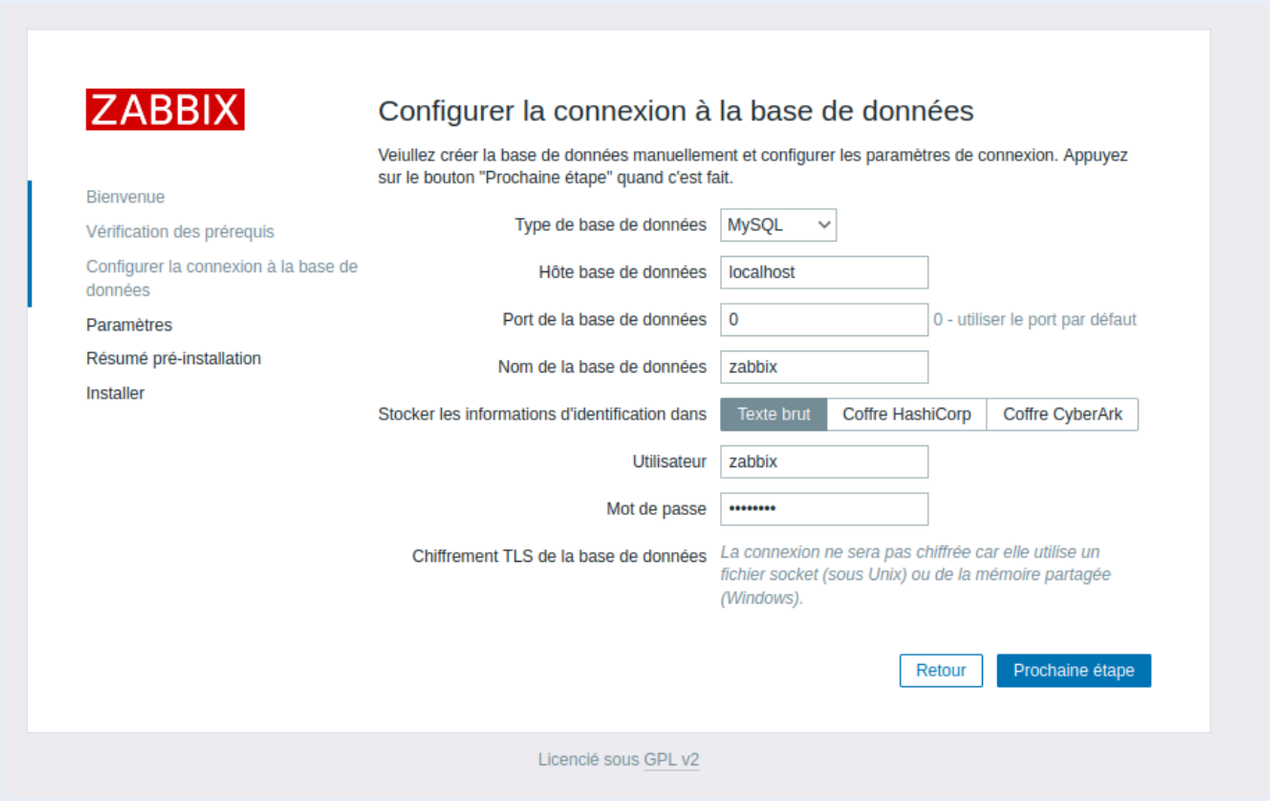


On arrive sur cette page d'accueil :

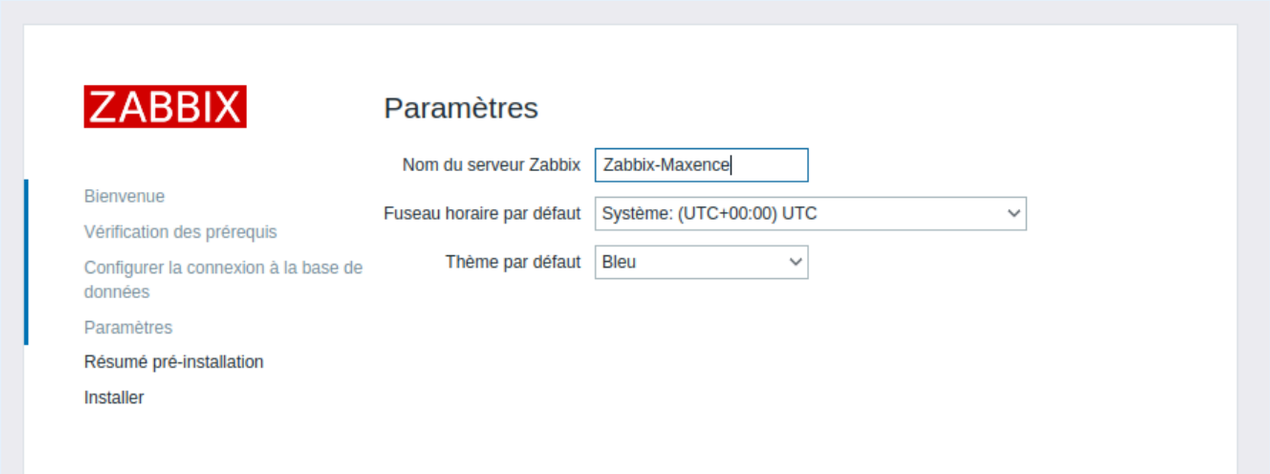
On vérifie que tout les prérequis sont bien installés :



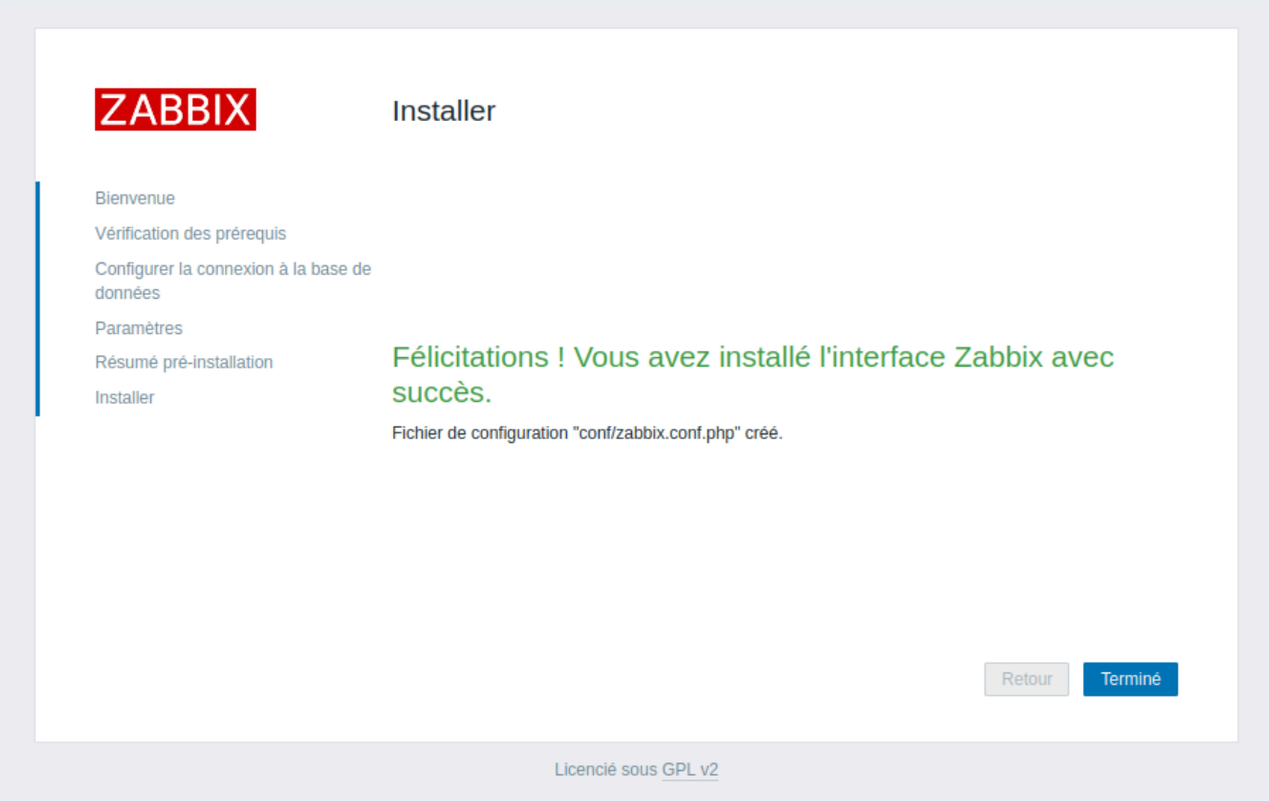
On configure la connexion à la BDD:



On nomme maintenant notre serveur Zabbix :



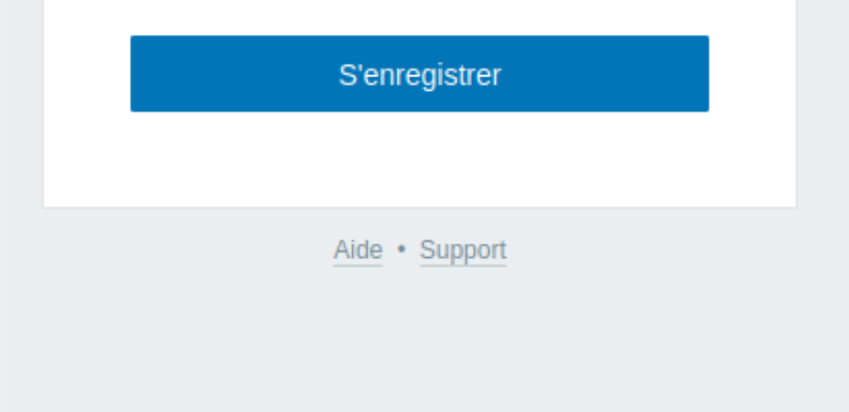
On termine l'installation :



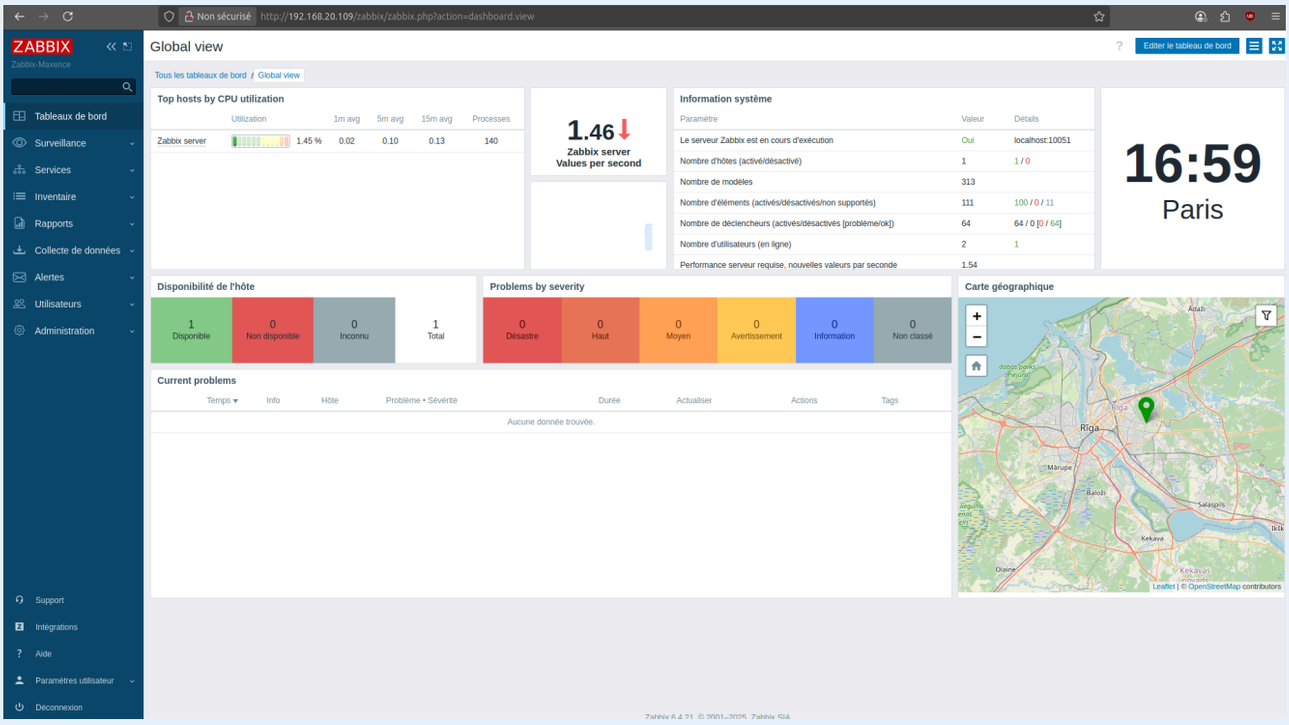
Connexion Interface Web :

On peut maintenant se connecter à la pge de monitoring.

On entre le login et le mot de passe : **Admin** et **zabbix**



On arrive sur cette page d'acceuil :



Partie B – Installation des agents

Note :

On commence par installer l'agent sur la VM Linux. La VM est une debian 12 sans interface graphique.

Installation Agent :

On installe l'agent Zabbix :

```
apt update
apt install zabbix-agent
```

```
root@debian12:~# apt install zabbix-agent
```

Fichier de configuration :

On modifie ces lignes dans le fichier de configuration :

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

```
Server=192.168.1.109
ServerActive=192.168.1.109
Hostname=Linux-client
```

```
root@debian12:~# nano /etc/zabbix/zabbix_agentd.conf_
```

```
### Option: Server
#       List of comma delimited IP addres
#       Incoming connections will be acce
#       If IPv6 support is enabled then
#       and '::/0' will allow any IPv4 or
#       '0.0.0.0/0' can be used to allow
#       Example: Server=127.0.0.1,192.168
#
# Mandatory: yes, if StartAgents is not e
# Default:
# Server=

Server=192.168.20.109
```

```
ServerActive=192.168.20.109

### Option: Hostname
#       List of comma delimited unic
#       Required for active checks a
#       Value is acquired from Hostr
#
# Mandatory: no
# Default:
Hostname=Linux-client_
```

On redemare et on active l'agent :

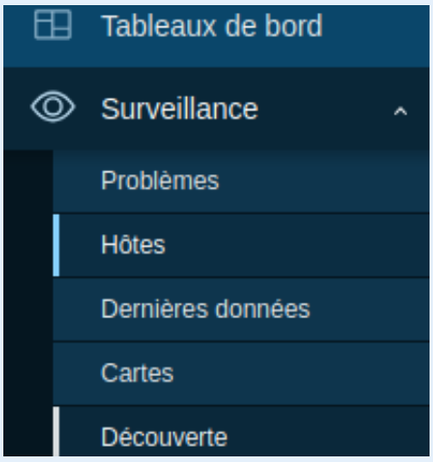
```
systemctl restart zabbix-agent
systemctl enable zabbix-agent
```

```
root@debian12:~#
root@debian12:~#
root@debian12:~# systemctl restart zabbix-agent
root@debian12:~# systemctl enable zabbix-agent
```

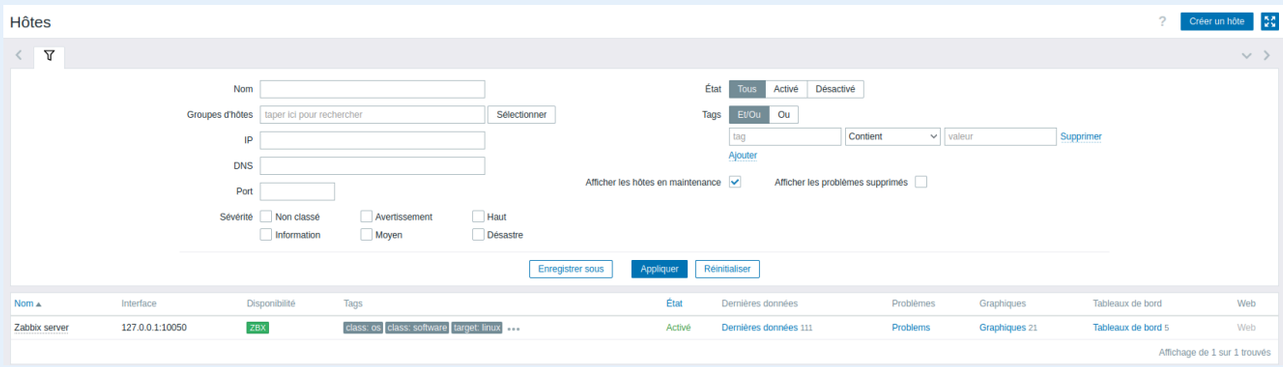
Ajout agent depuis interface web :

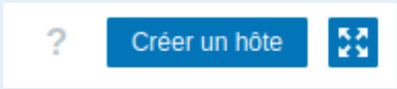
Maintenant que l'agent est installé, on veut créer l'hôte sur l'interface web.

Depuis l'interface Web, on va dans Surveillance > Hôtes :



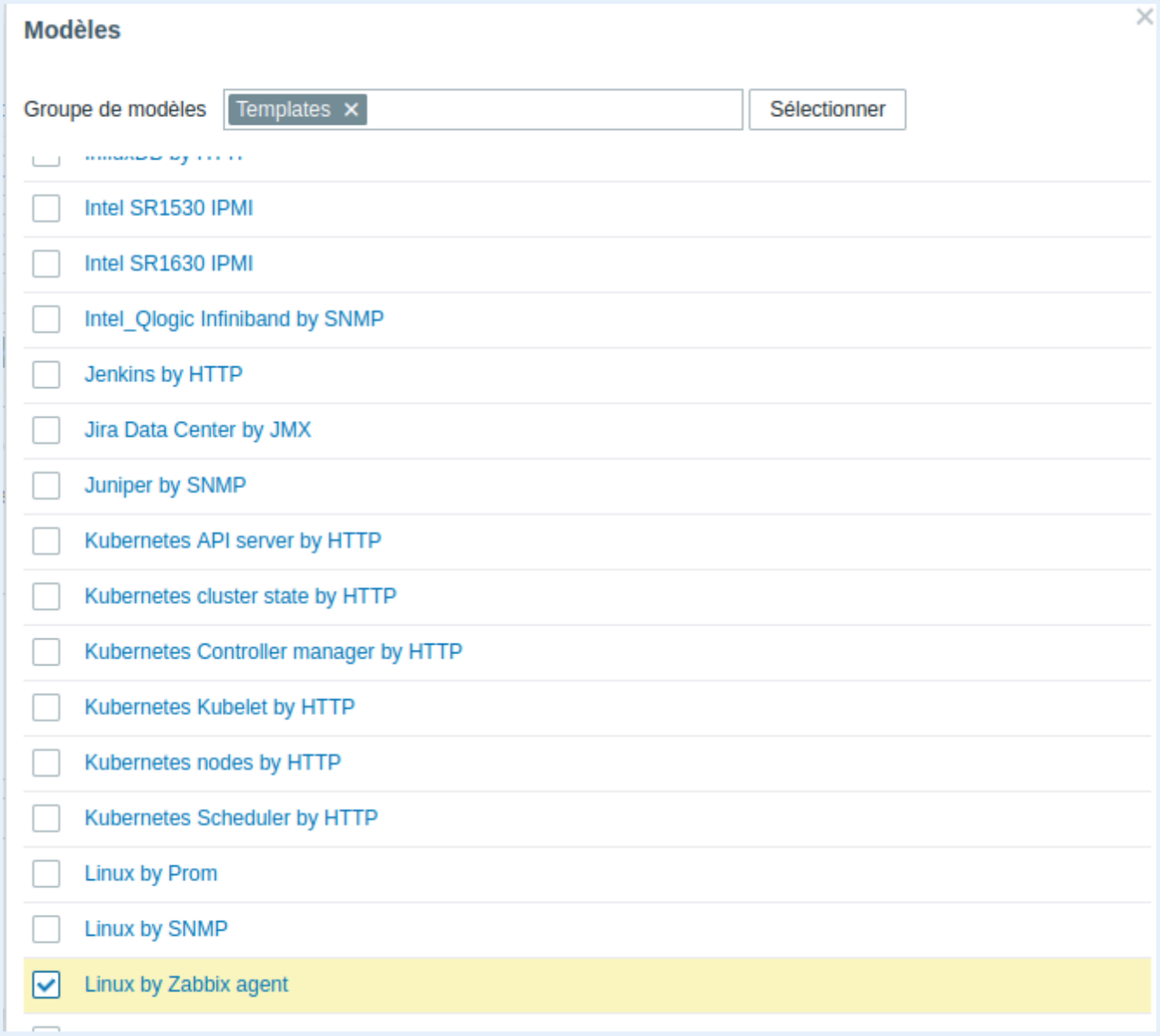
On arrive sur cette page, on sélectionne créer un hôte en haut à droite :





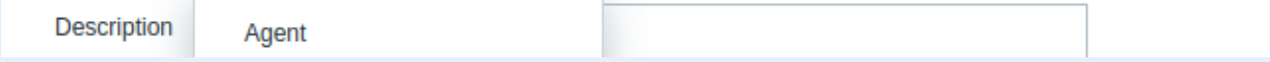
On défini le nom du nouvel hôte :

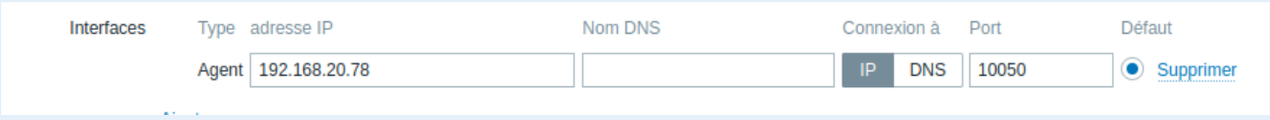
Puis on défini le modèle de template :



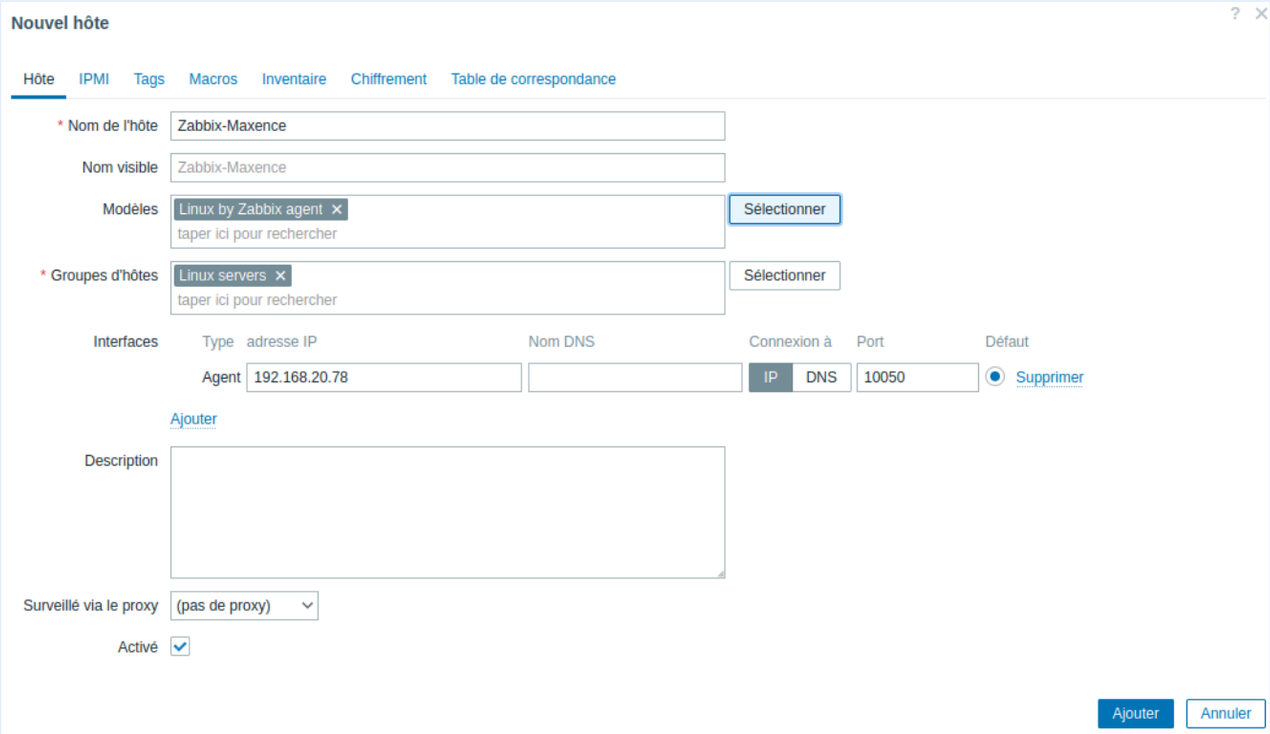
On choisi ensuite dans quel groupe on met la machine :

On va maintenant ajouter l'interface :

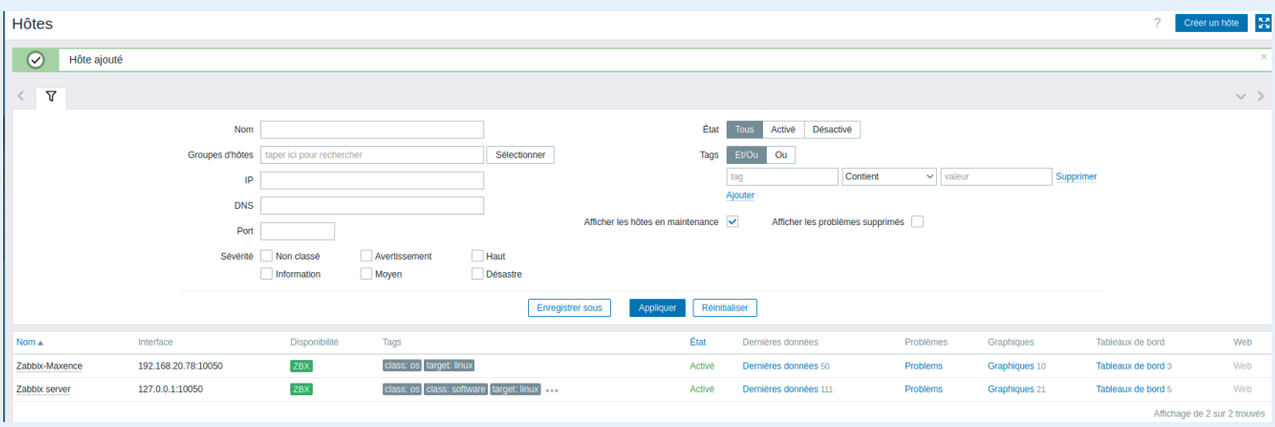




On termine l'installation en cliquant sur ajouter :



On a bien un nouvel agent qui apparaît :



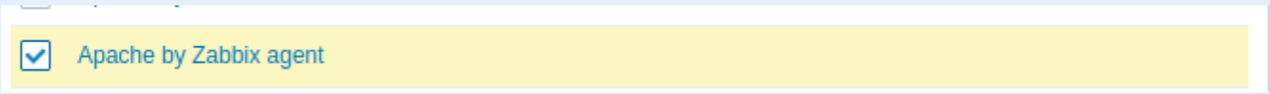
b. Installation agent serveur LAMP :

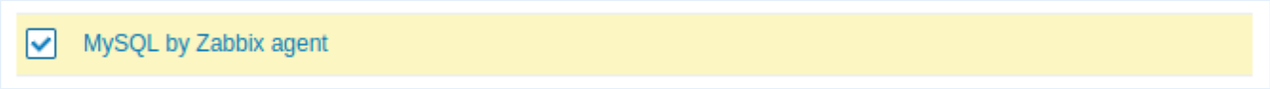
Note :

On va maintenant installer un agent sur un serveur LAMP. La procédure d'installation est identique que lors de l'installation de l'agent sur la VM debian 12. La seule chose qui change est lors de la création de l'hôte sur l'interface web de zabbix.

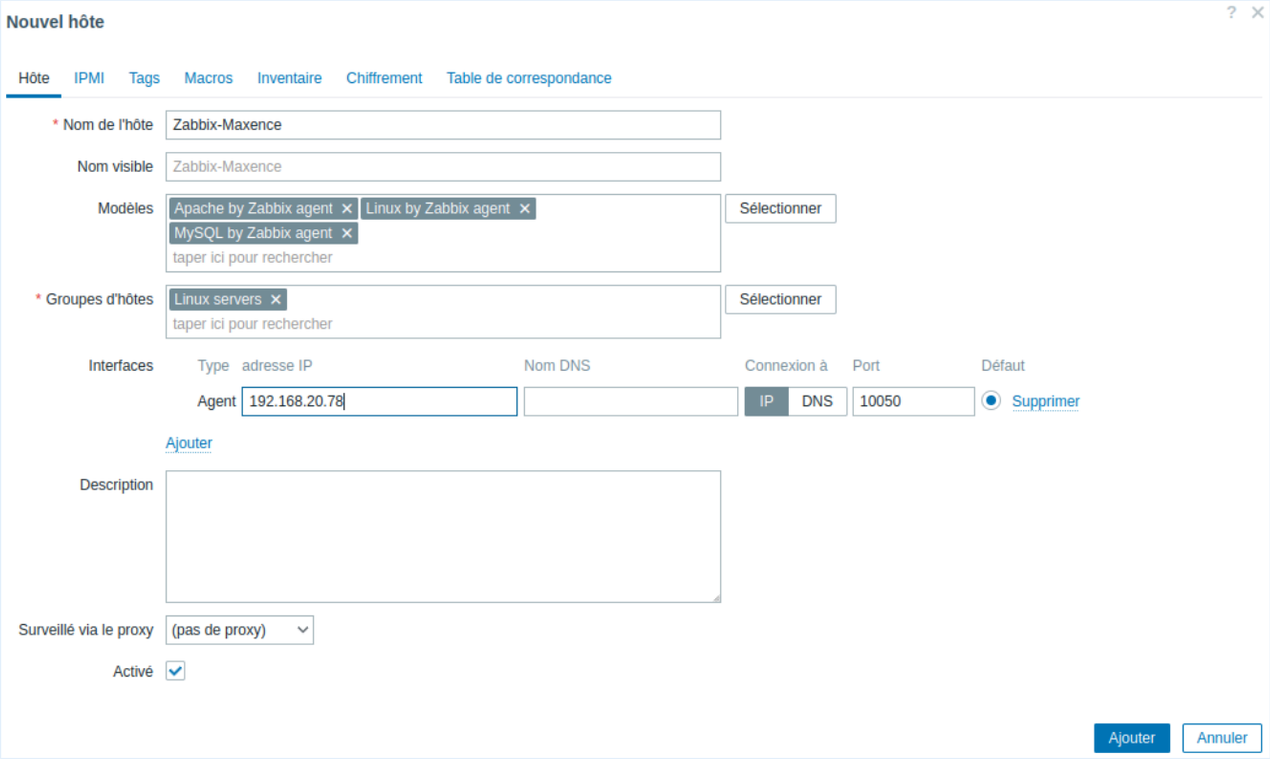
Ajout agent depuis interface Web :

On suit la même procédure en nommant l'hôte puis, lors de la sélection des modèles de template, on sélectionne Appache by zabbix agent et mysql ny zabbix agent en plus de Linux by zabbix agent :

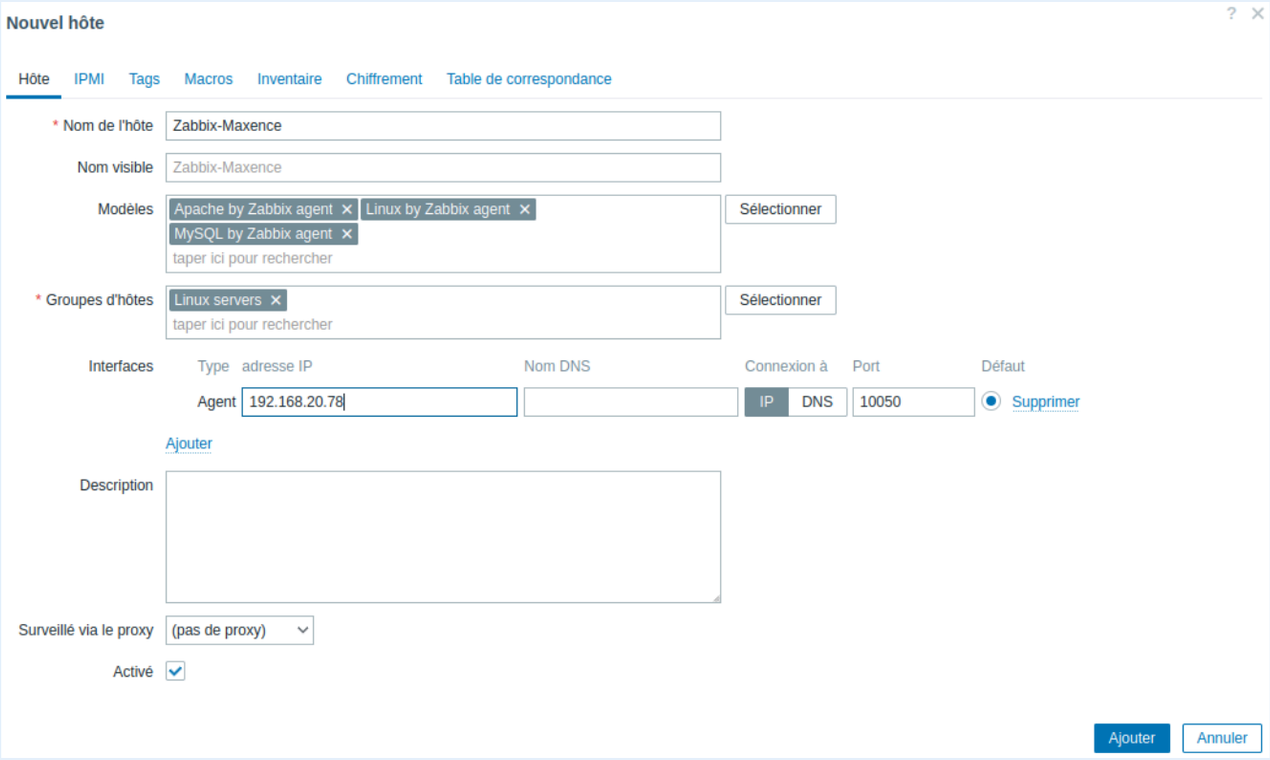




Par la suite on ajoute l'interface comme précédemment. On peut maintenant ajouter ce nouvel hôte :



Le serveur LAMP apparaît bien dans les hôtes surveillés :



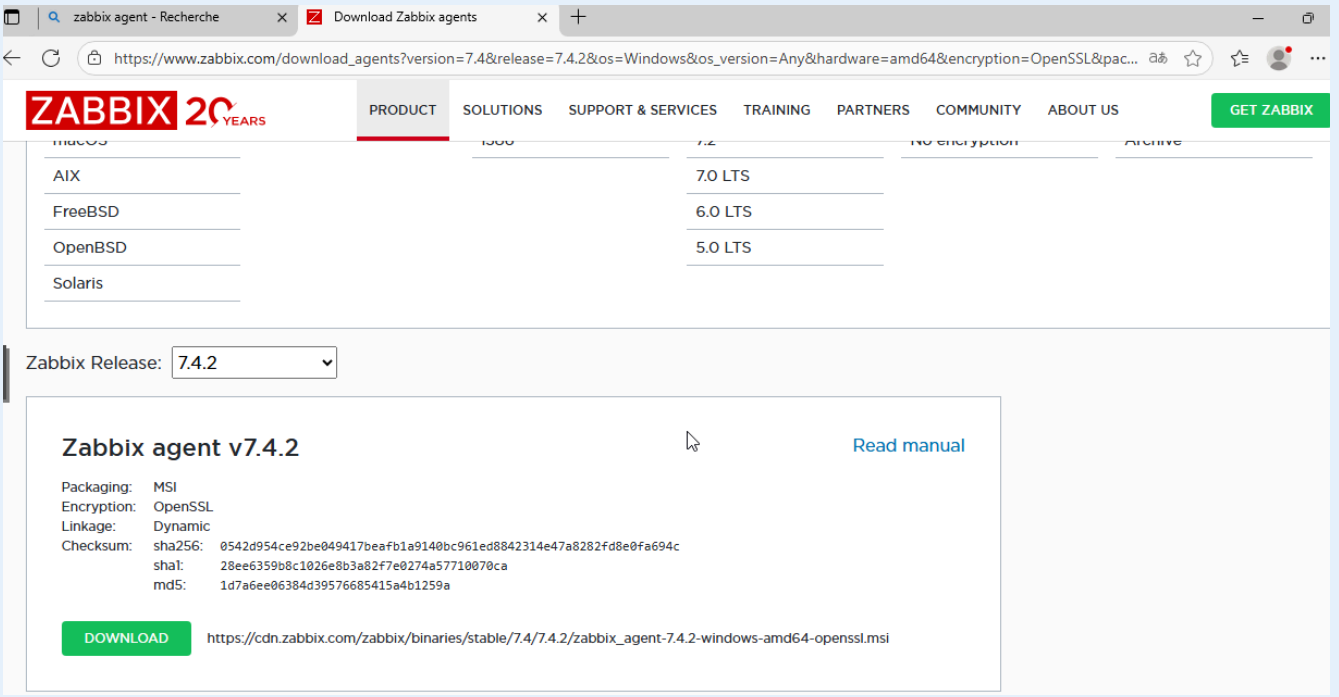
c. Installation agent Windows 11 :

Note :

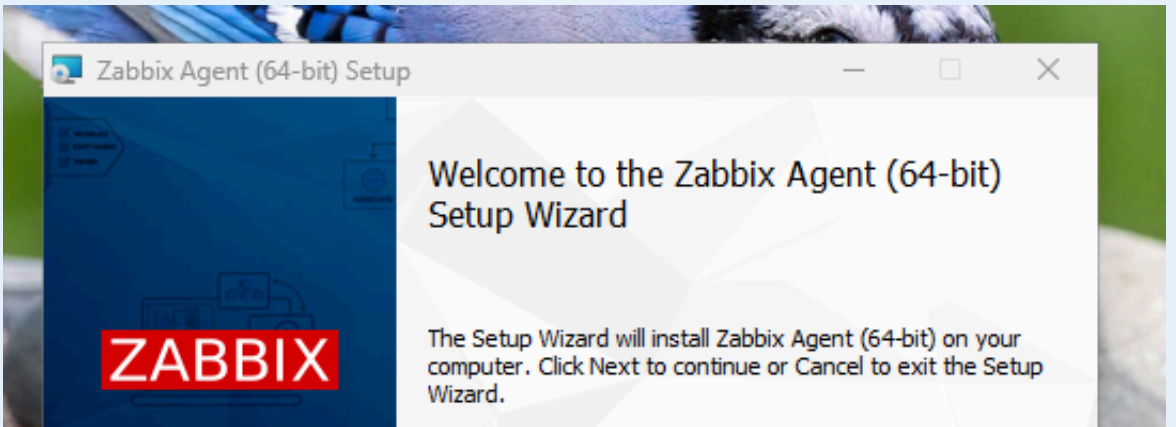
On passe maintenant à l'installation de l'agent sur la VM Windows 11.

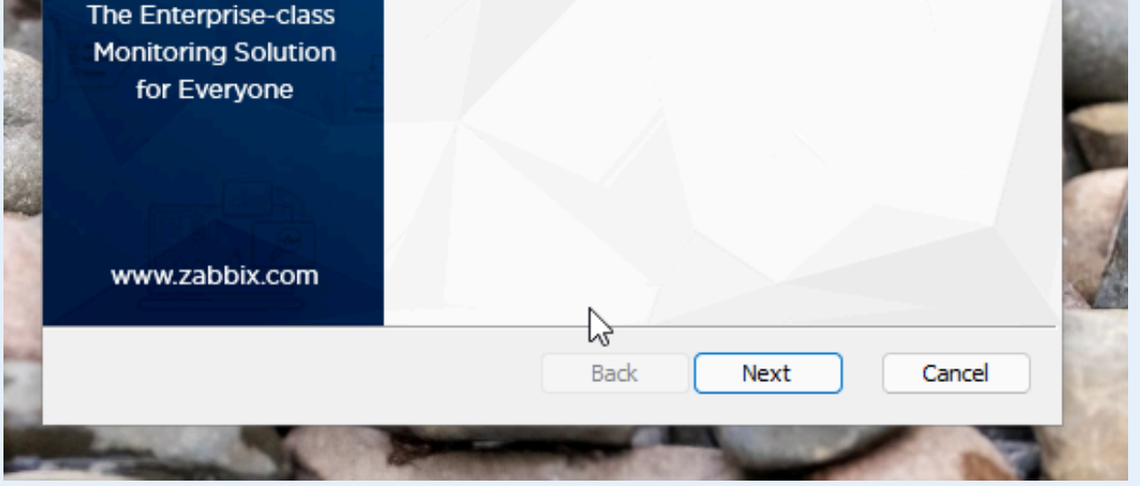
Installation agent :

On commence par aller sur le site de Zabbix depuis un navigateur web pour télecharger l'agent. Le site : https://www.zabbix.com/download_agents?version=6.4&distribution=windows&architecture=64bit&package=msi

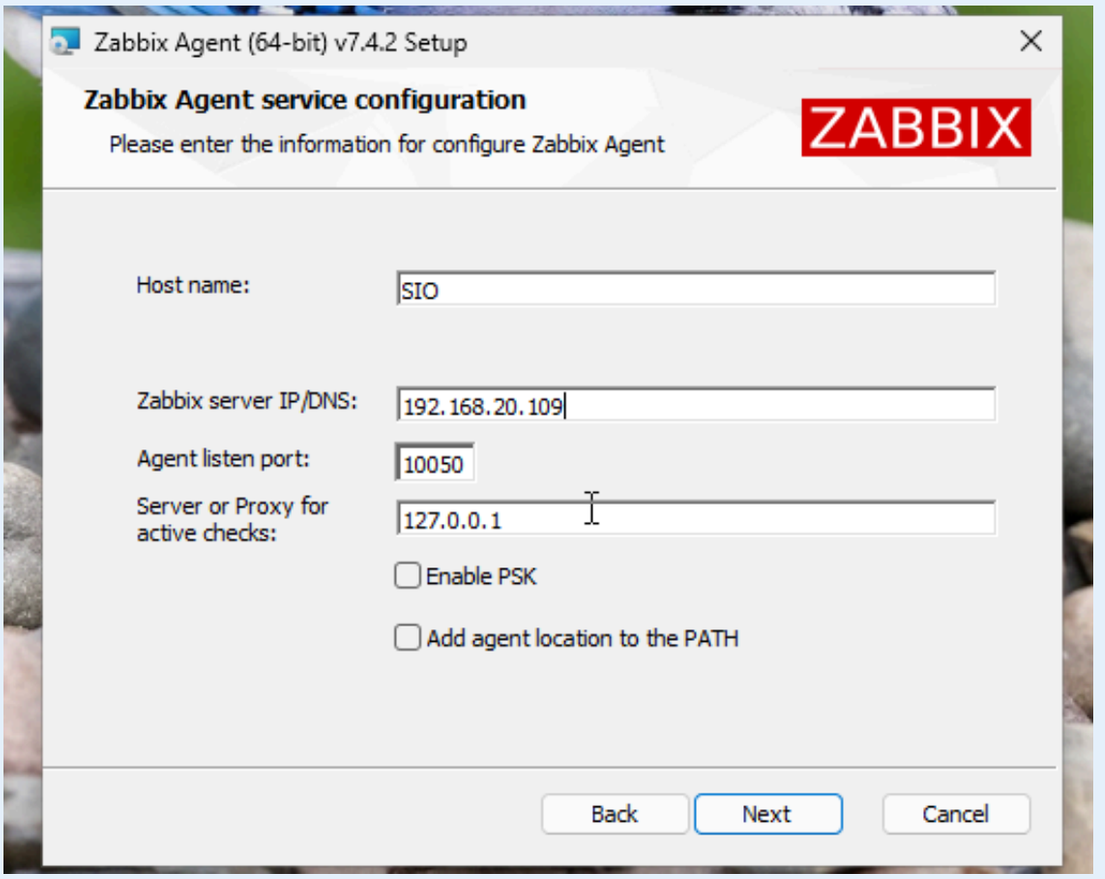


On lance ensuite le programme d'installation :

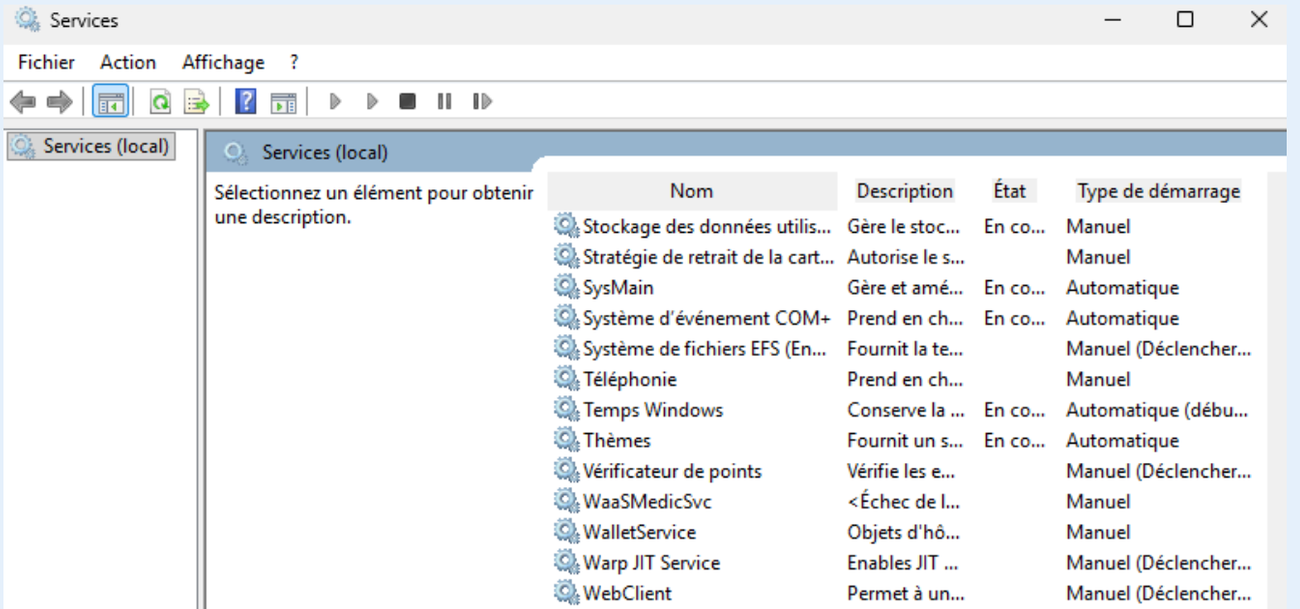


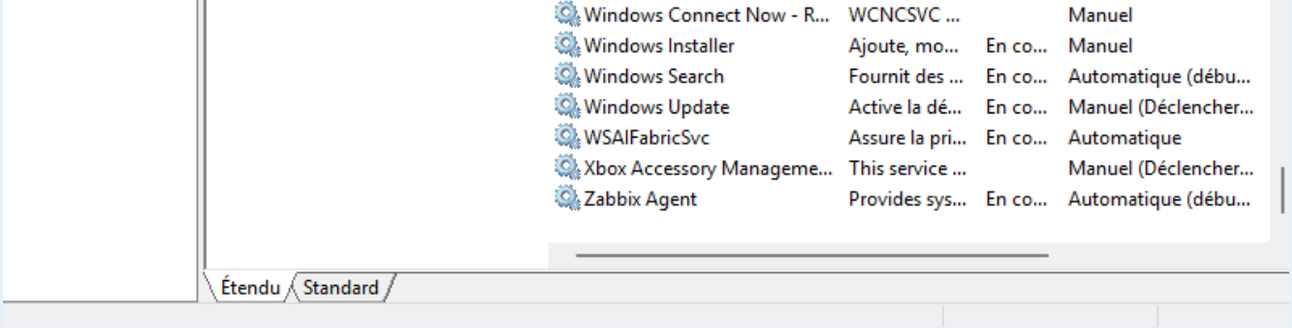


Lors de l'installation, on renseigne le nom d'hôte de la VM Windows11 puis on entre l'adresse IP du serveur Zabbix :



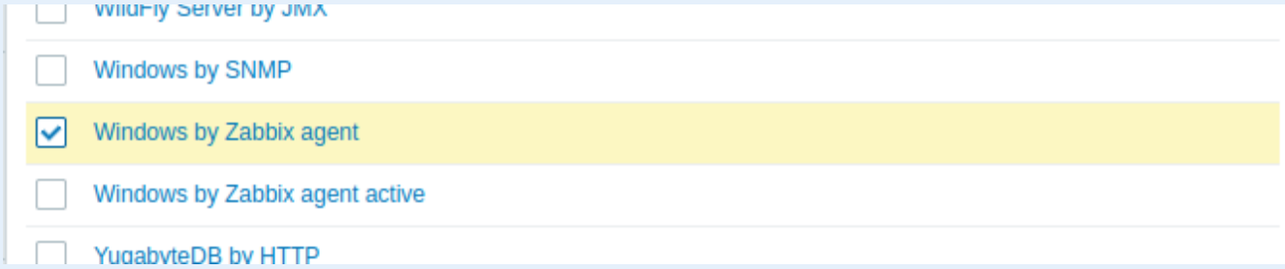
On peut vérifier que le service fonctionne en allant dans service :

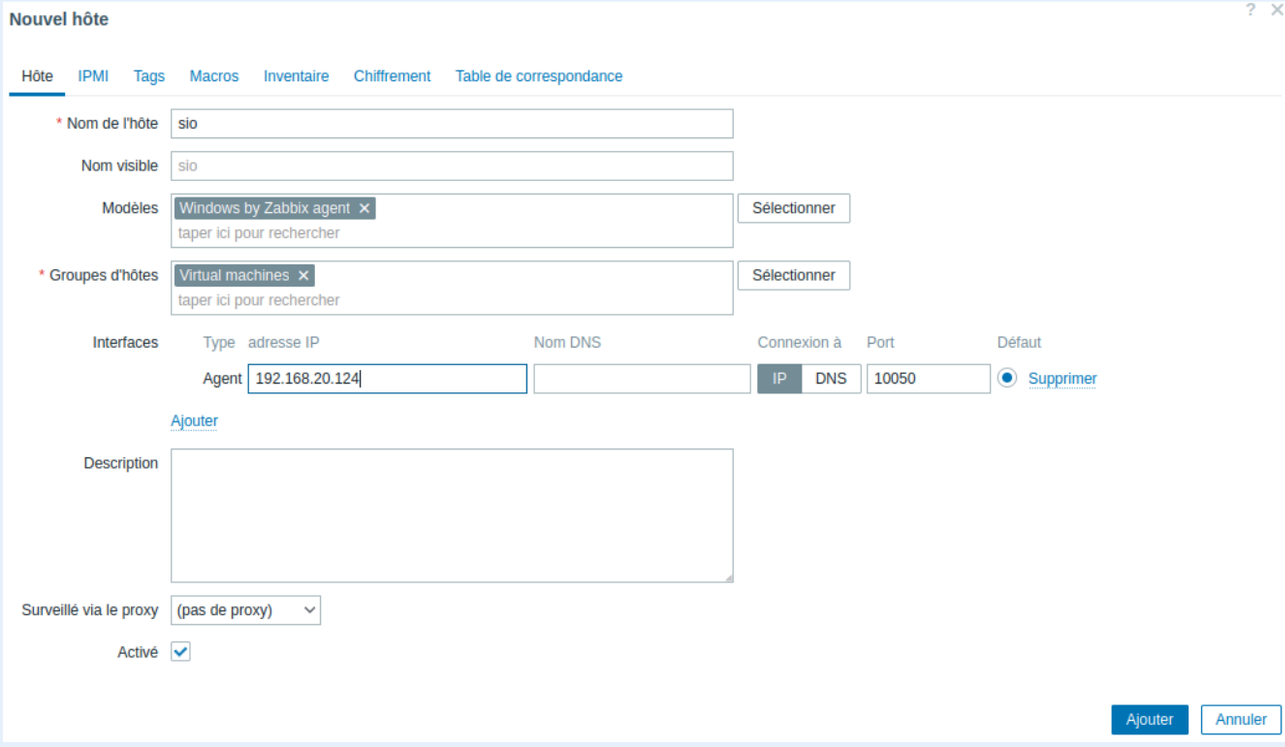




Ajout agent depuis interface web :

Même procéde que pour les agents Linux, on change juste le template utilisé :



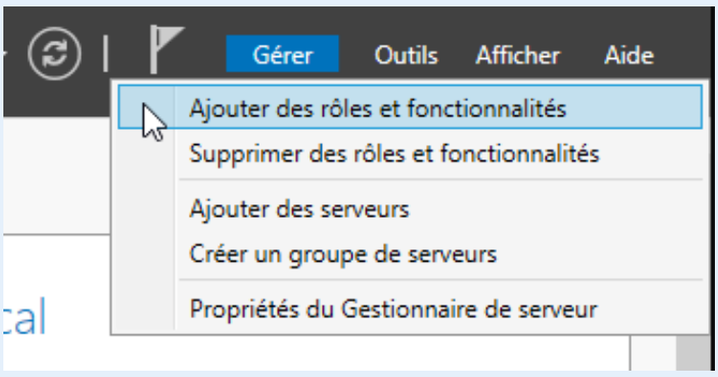


Nom	Interface	Disponibilité	Tags
Linux-client	192.168.20.87:10050	ZBX	class: os, target: linux
sio	192.168.20.124:10050	ZBX	class: os, target: windows

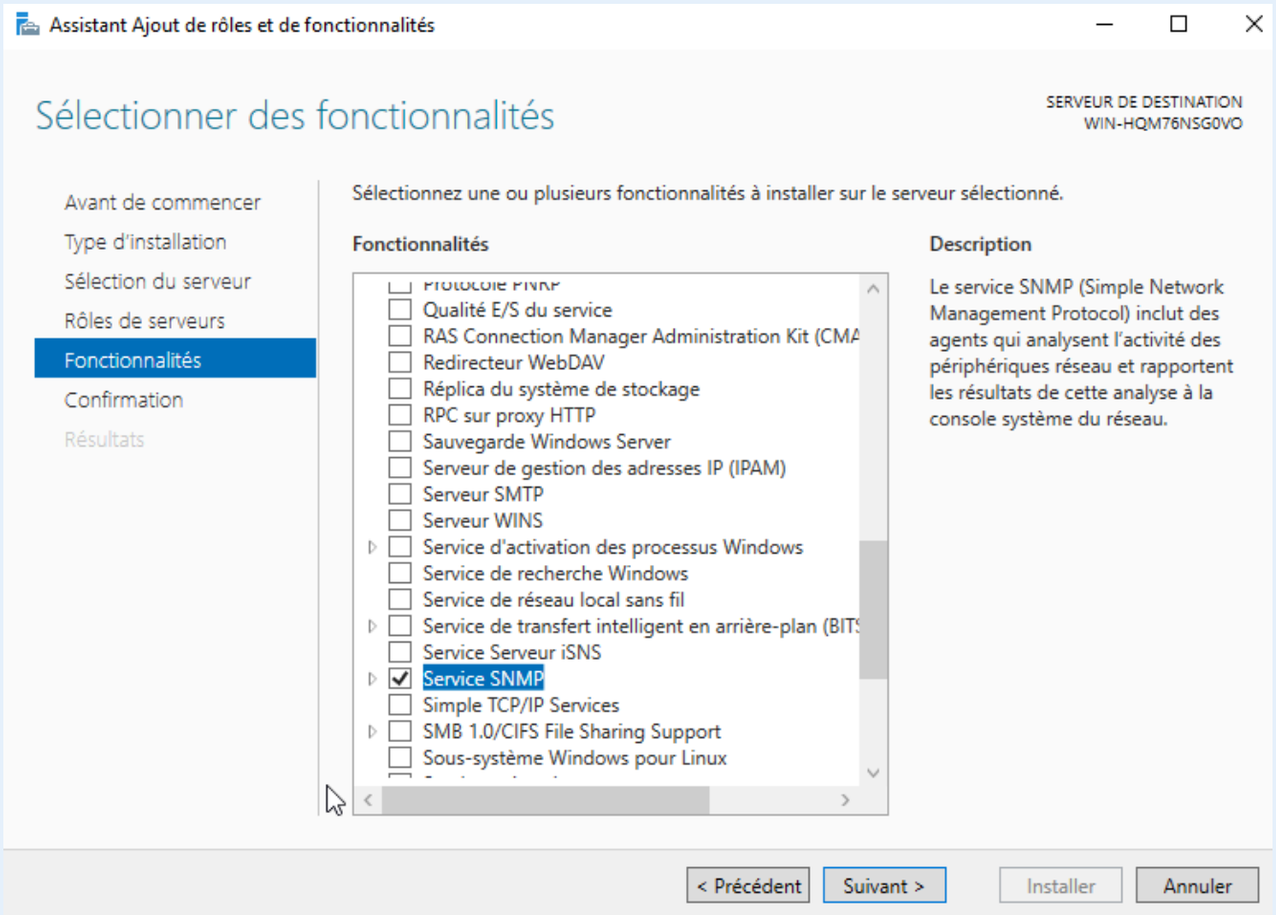
Partie C – SNMP

Installation SNMP :

Dans le server manager, on clique sur gérer puis ajouter des rôles et fonctionnalités :

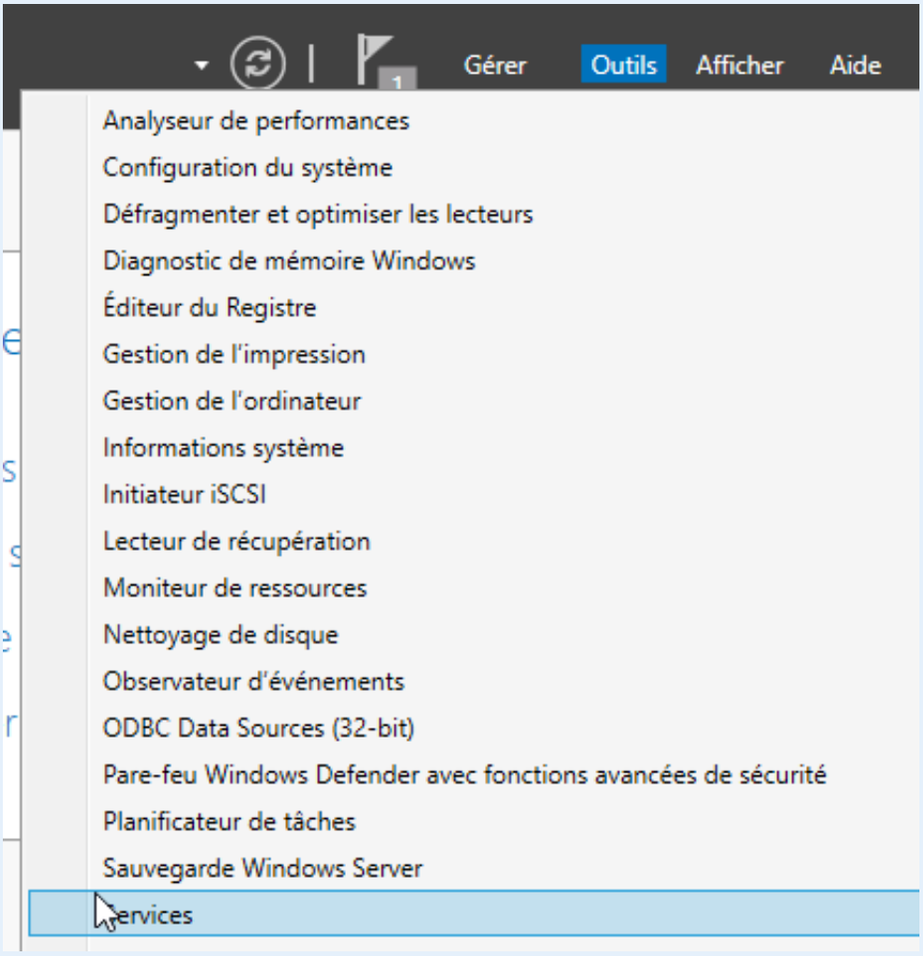


Dans fonctionnalité, on ajoute le service snmp :

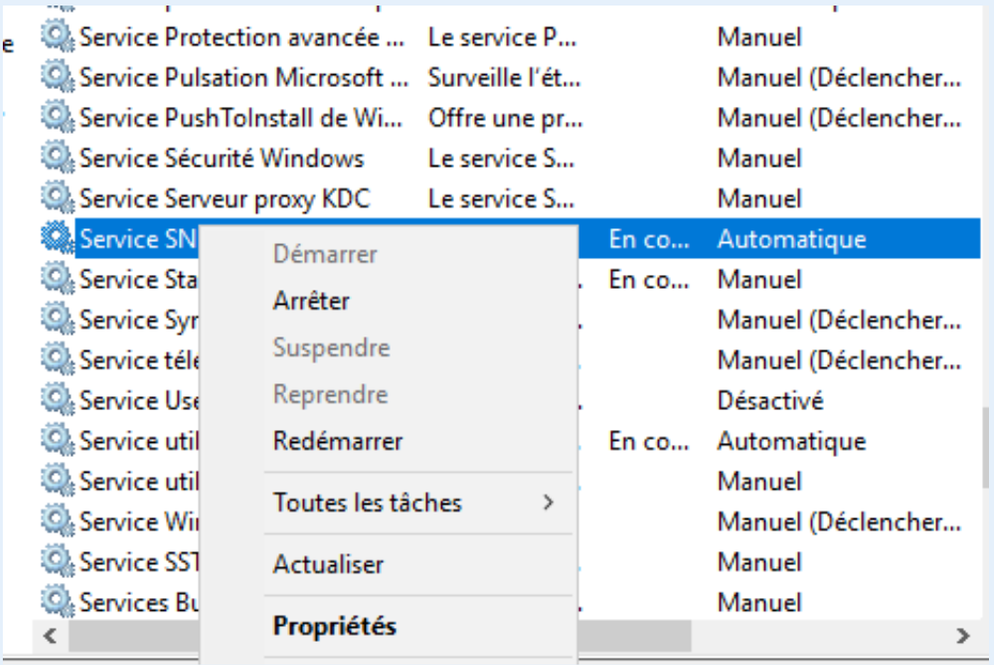


Configuration SNMP :

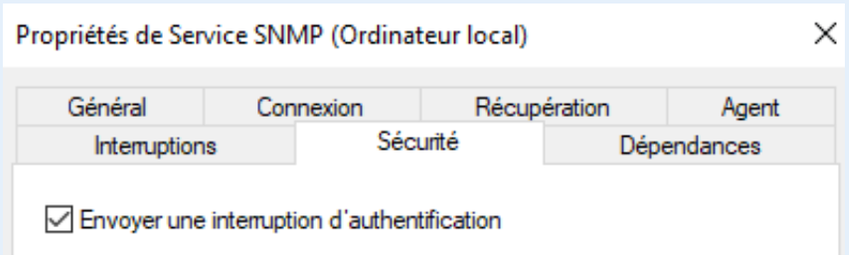
On va maintenant dans Outils > Service :

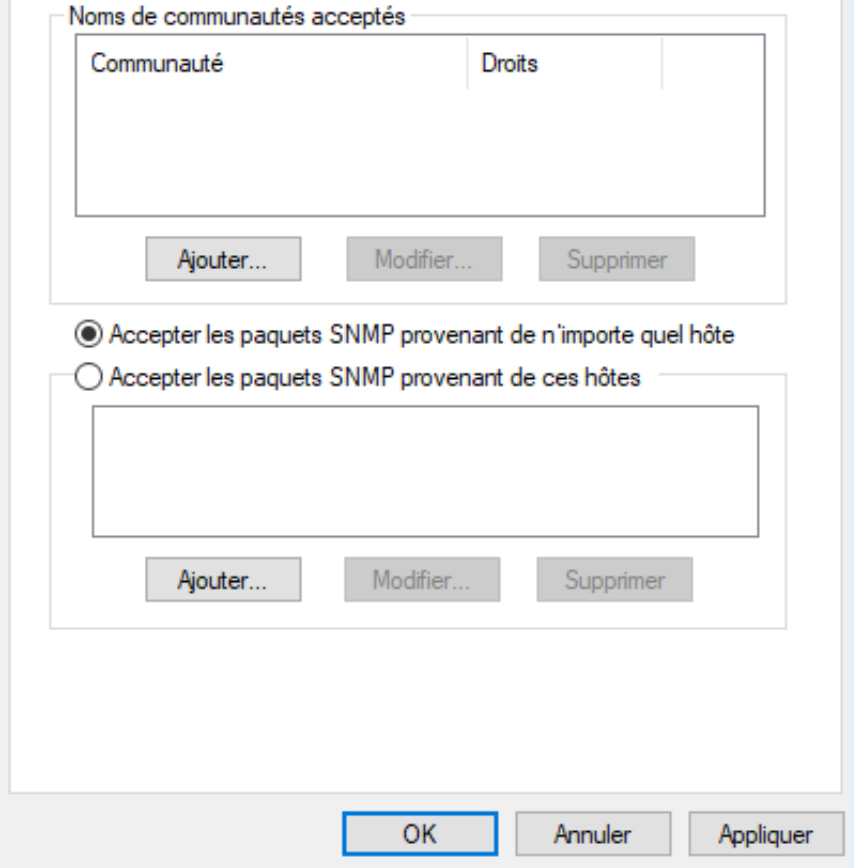


On double clique sur service SNMP :

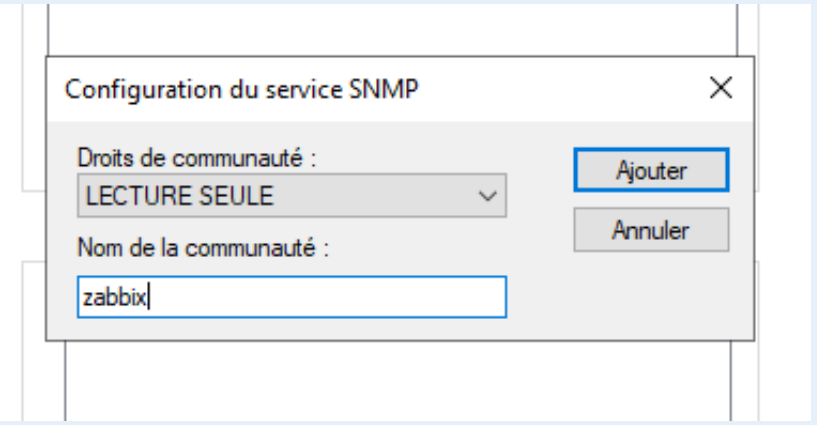


Dans l'onglet sécurité, on accepte les paquets SNMP provenant de n'importe quelle hôte :

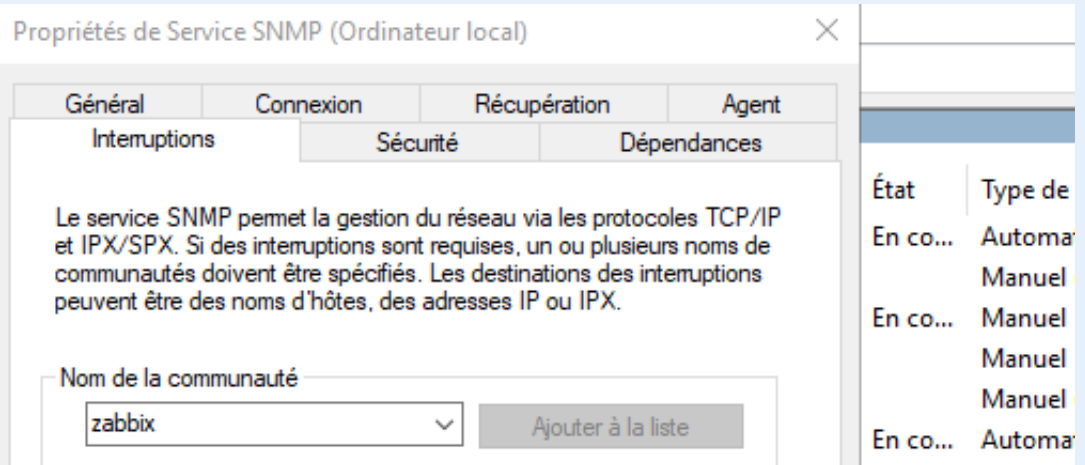


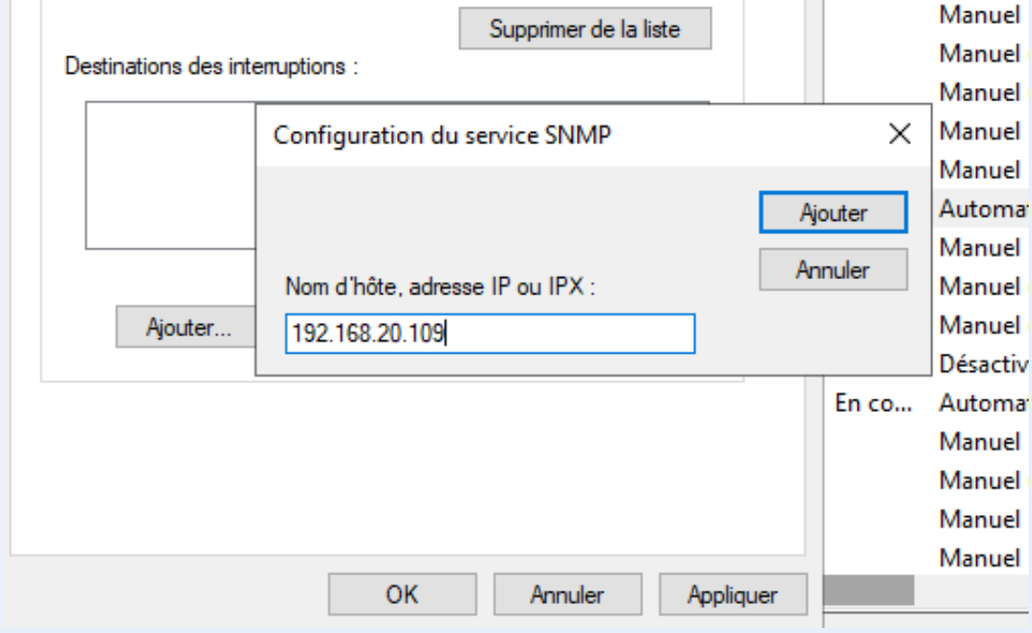


Puis on ajoute une communauté, je la nomme Zabbix :



On va ensuite dans interruption et pour la communauté Zabbix on ajoute l'adresse IP du serveur Zabbix :



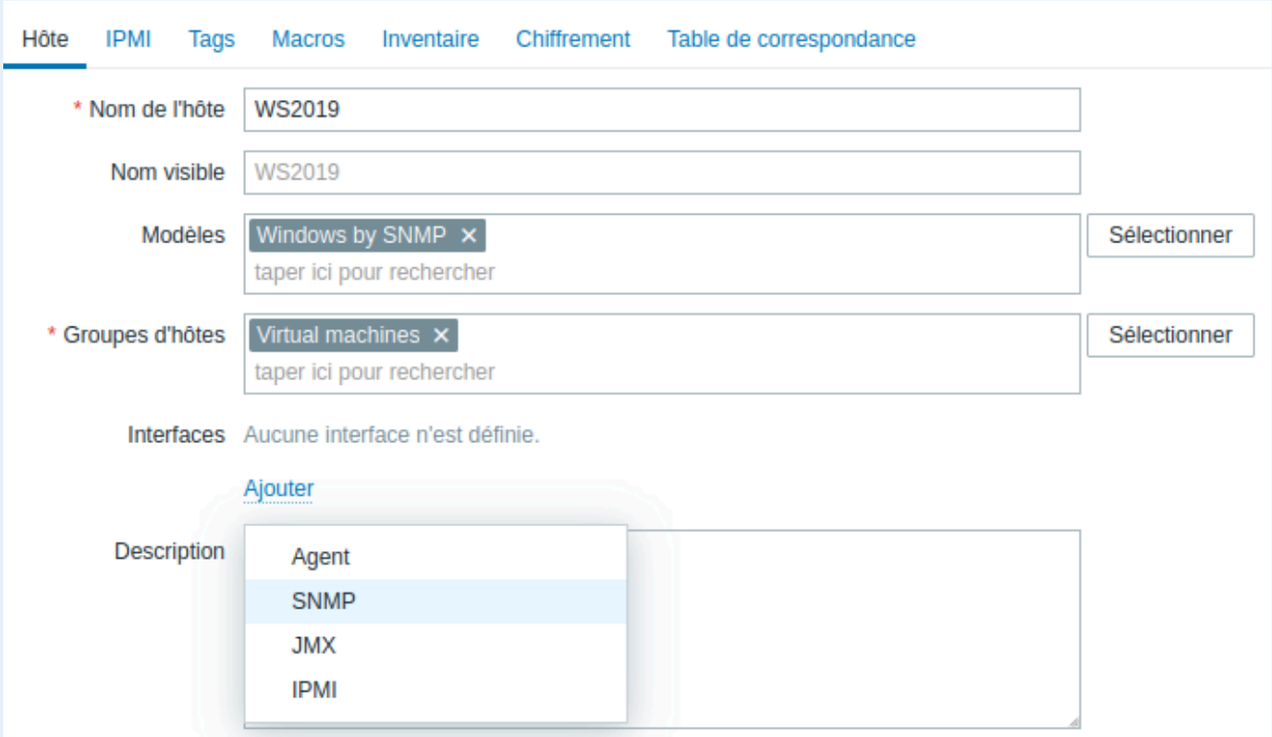


Configuration depuis interface Web :

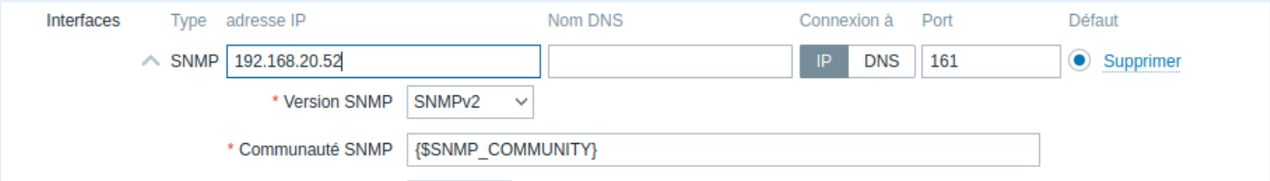
On peut maintenant depuis l'interface Web ajouter un nouvel hôte pour le Windows Server.

Comme pour la VM Windows, on défini le nom, on attribue un groupe et un modèle de template, on prends comme modèle Windows by SNMP.

On ajoute ensuite une interface SNMP :



On entre alors l'IP du Windows Server :



Utiliser des requêtes combinées

On obtient bien les informations pour le Windows Server :

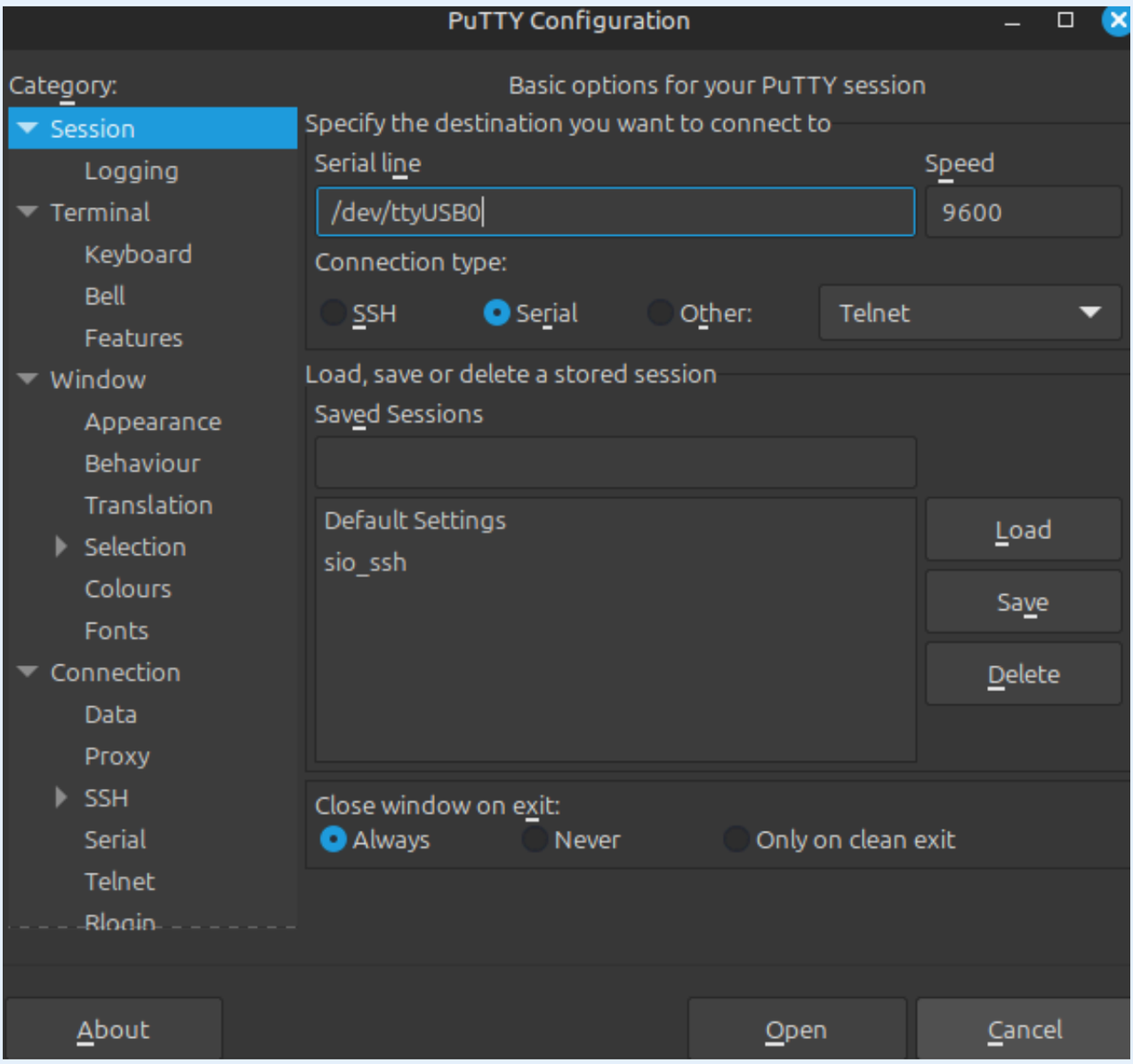
WS2019	192.168.20.52:161	SNMP	class: os target: windows

b. Installation SNMP sur Switch :

Configuration Switch :

On veut maintenant pouvoir surveiller un switch. On commence par la configuration du switch.

On commence par se connecter au switch en mode console en utilisant putty :



On met en place un accès telnet en définissant une ip pour le Vlan 1 :

```
Switch-G1(config)#interface vlan 1
Switch-G1(config-if)#ip add
Switch-G1(config-if)#ip address 192.168.20.221 255.255.255.0
```

```
Switch-G1(config)#line vty 0 15
Switch-G1(config-line)#pass
Switch-G1(config-line)#password sio%2025
Switch-G1(config-line)#login
Switch-G1(config-line)#exit
```

```
Switch-G1(config)#enable password sio%2025
```

On peut maintenant se connecter en telnet :

```
root@maxence-ThinkPad-P16s-Gen-2:/home/maxence# telnet 192.168.20.221
Trying 192.168.20.221...
Connected to 192.168.20.221.
Escape character is '^]'.


User Access Verification

Password:
Switch-G1>en
Password:
Switch-G1#conf t
```

On peut maintenant configurer le snmp avec le nom de la communauté :

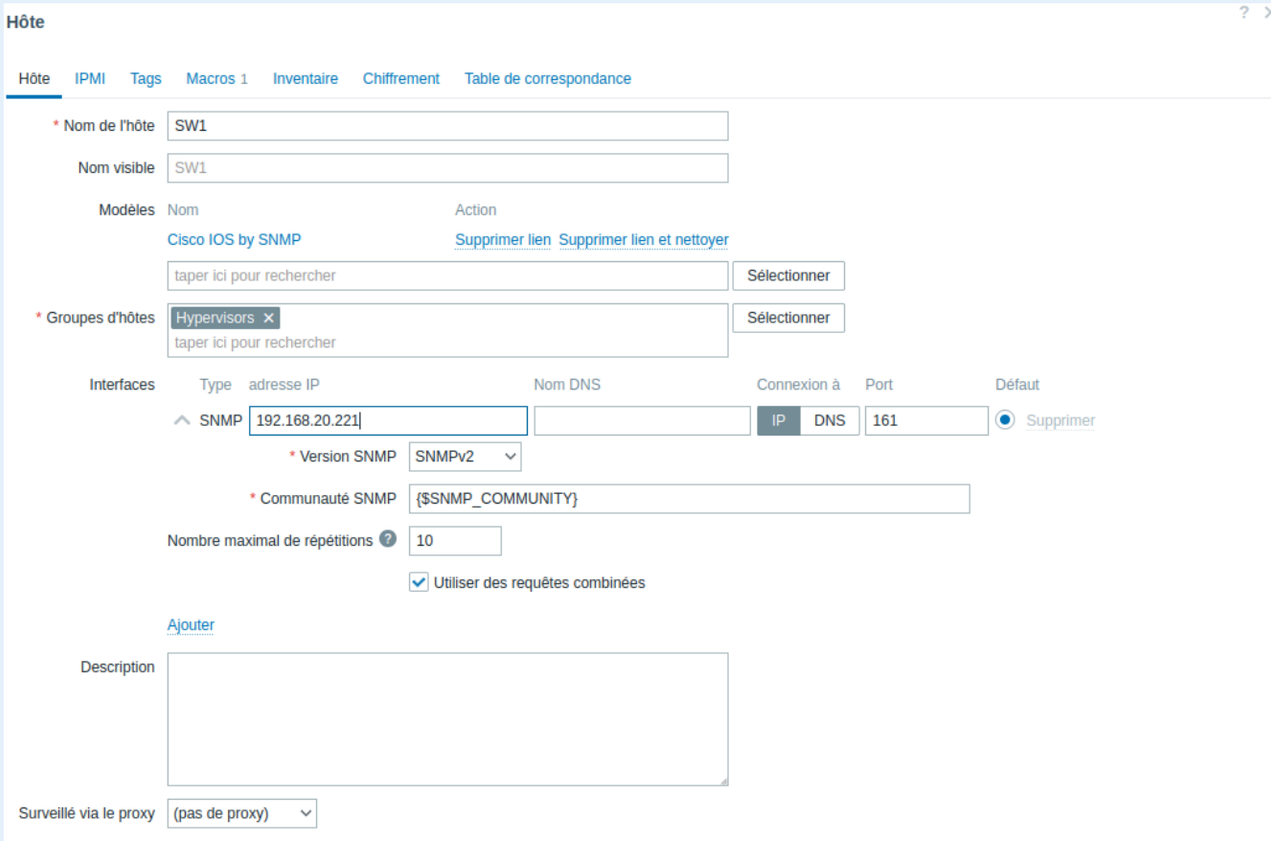
```
Switch-G1(config)#snmp-server community Zabbix-Maxence RO
```

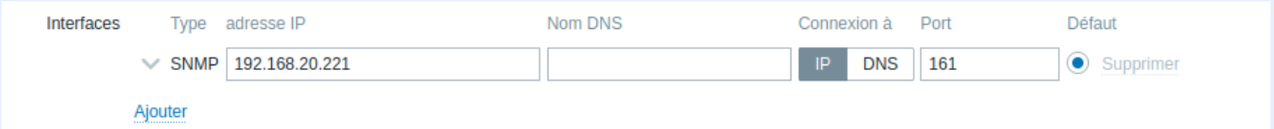
On défini ensuite l'adresse de l'hôte :

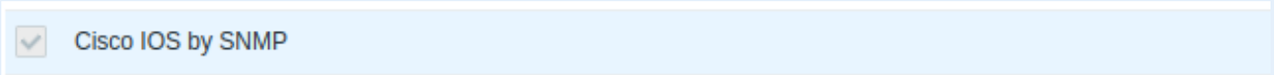
```
Switch-G1(config)#snmp-server host 192.168.20.109 Zabbix-Maxence
```

Configuration depuis interface Web :

On passe maintenant à la configuration depuis l'interface web :





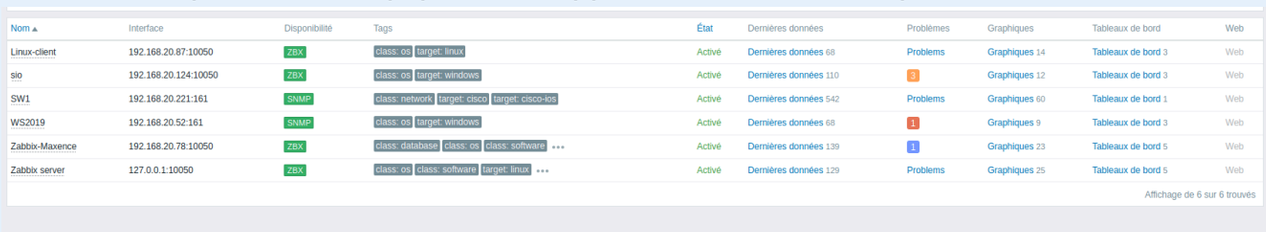


Dans macros on entre le nom de la commmunauté :

Le switch apparaît bien :

Tout les équipements :

On observe que tout les équipements apparaissent bien, la supervision fonctionne.



Nom	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	Graphiques	Tableaux de bord	Web
Linux-client	192.168.20.87:10050	ZBX	class: os target: linux	Activé	Dernières données 68	Problems	Graphiques 14	Tableaux de bord 3	Web
sio	192.168.20.124:10050	ZBX	class: os target: windows	Activé	Dernières données 110	3	Graphiques 12	Tableaux de bord 3	Web
SW1	192.168.20.221:161	SNMP	class: network target: cisco target: cisco-ios	Activé	Dernières données 542	Problems	Graphiques 60	Tableaux de bord 1	Web
WS2019	192.168.20.52:161	SNMP	class: os target: windows	Activé	Dernières données 68	1	Graphiques 9	Tableaux de bord 3	Web
Zabbix-Maxence	192.168.20.78:10050	ZBX	class: database class: os class: software ...	Activé	Dernières données 139	1	Graphiques 23	Tableaux de bord 5	Web
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux ...	Activé	Dernières données 129	Problems	Graphiques 25	Tableaux de bord 5	Web

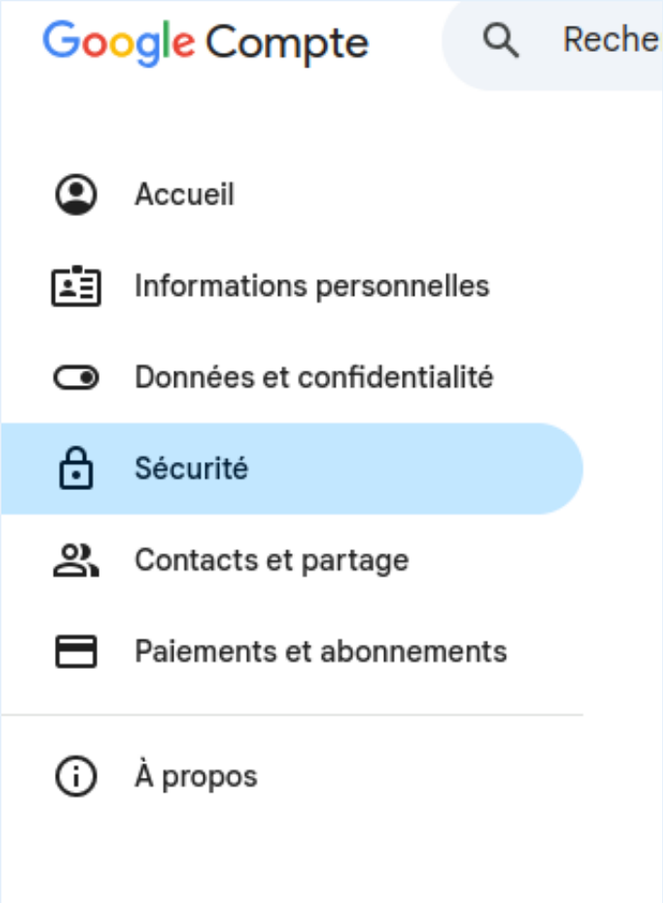
Affichage de 6 sur 6 trouvés

Partie D – Alertes et interfaces

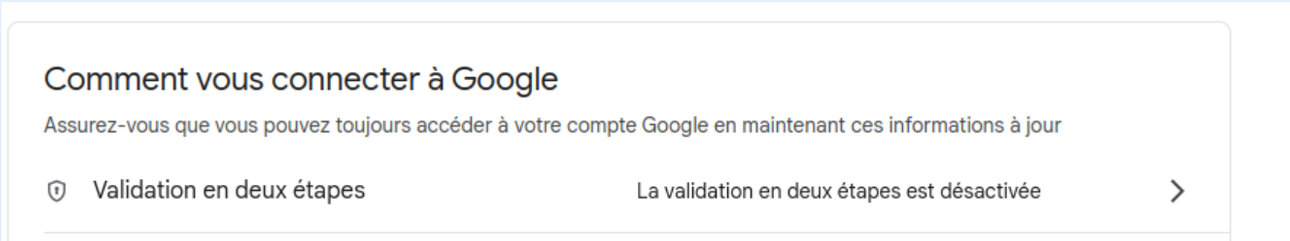
Configuration boite mail :

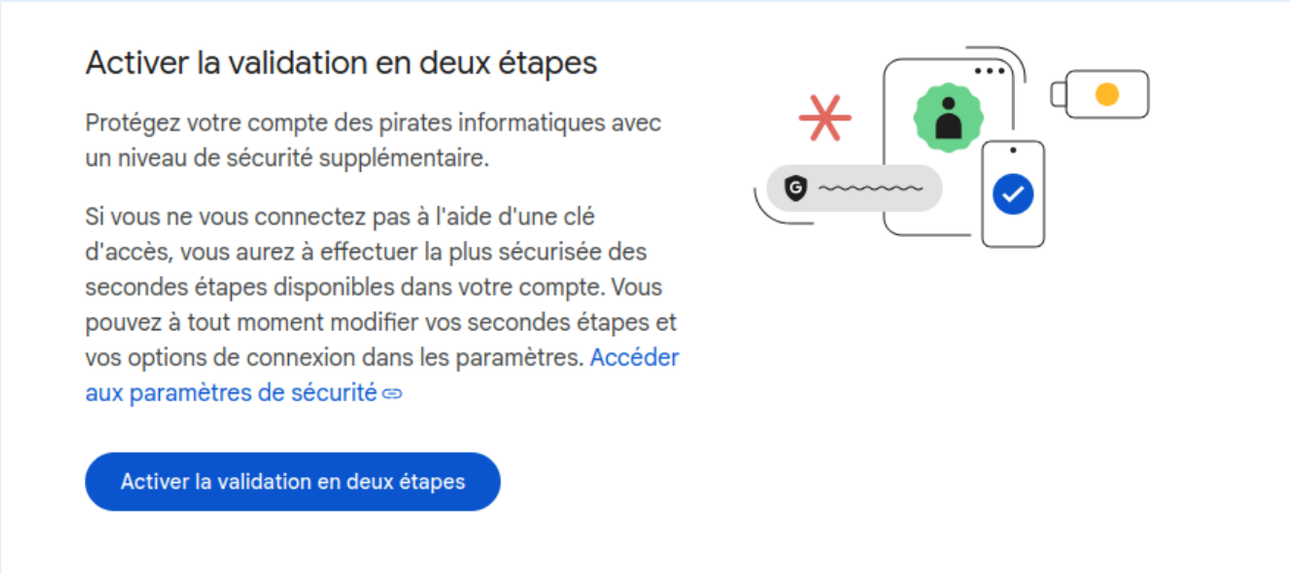
Avant toute chose, on doit configurer la boite mail de l'admin qui reçoit les mails. On utilise un compte gmail.

On va dans paramètres > sécurité :

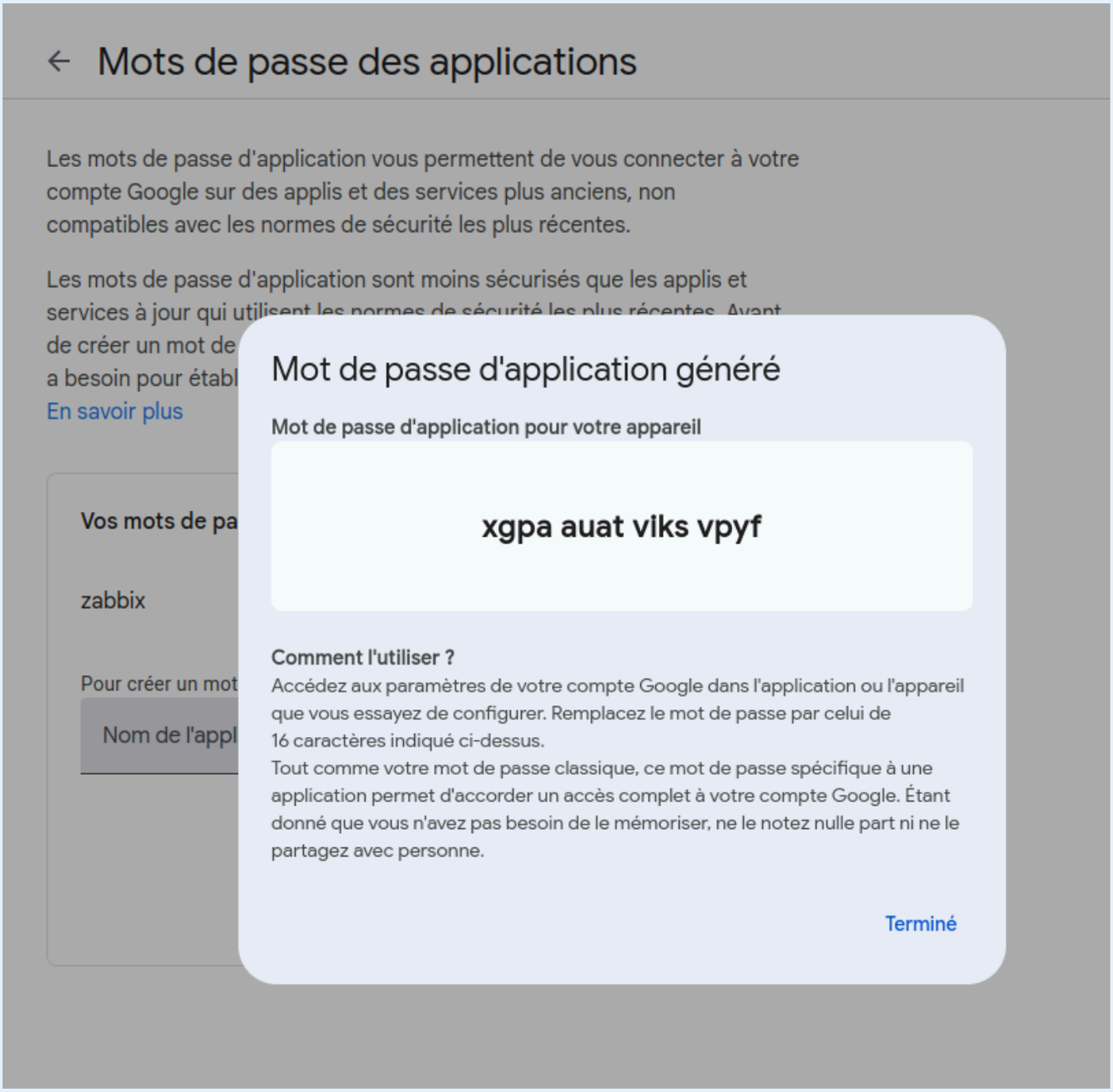


On active la validation à deux étapes :





On se rend ensuite sur ce lien : https://myaccount.google.com/apppasswords et on génere un nouveau mot de passe pour une application que l'on garde de coté.



Configuration SMTP :

Pour pouvoir recevoir des mails on a besoin d'installer un serveur SMTP. On l'installe sur la VM qui héberge le Zabbix.

```
root@debian12:~# apt install ssmtp
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Le paquet suivant a été installé automatiquement et n'est plus nécessaire :
  linux-image-6.1.0-27-amd64
```

On modifie ensuite le fichier de configuration :

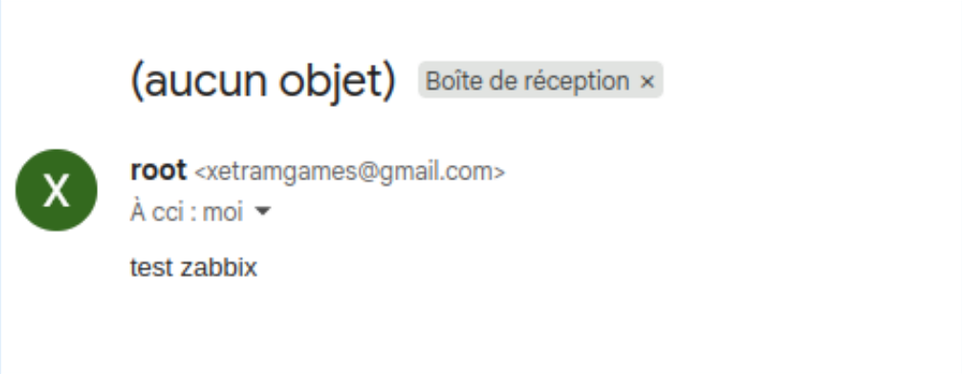
```
root@debian12:~# nano /etc/ssmtp/ssmtp.conf
```

On entre les informations suivantes : notre mail, le hubmail et le mot de passe que l'on a génère précédemment.

```
#
# Config file for sSMTP sendmail
#
# The person who gets all mail for userids < 1000
# Make this empty to disable rewriting.
root=xetramgames@gmail.com

# The place where the mail goes. The actual machine name is required no
# MX records are consulted. Commonly mailhosts are named mail.domain.com
mailhub=smtp.gmail.com:465

# Where will the mail seem to come from?
#rewriteDomain=

# The full hostname
hostname=debian12

# Are users allowed to set their own From: address?
# YES - Allow the user to specify their own From: address
# NO - Use the system generated From: address
FromLineOverride=YES
AuthUser=xetramgames@gmail.com
AuthPass=ohveentpfqitnvja
UseTLS=YES
```

On réalise un test pour vérifier que le service fonctionne bien :

```
root@debian12:~# echo "test zabbix" | ssmtp xetramgames@gmail.com
```

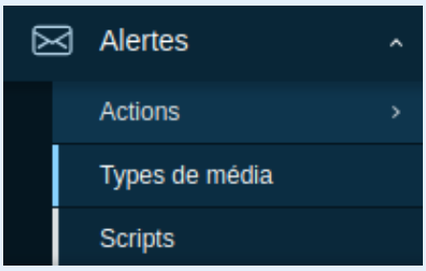


C'est bon le service ssmtp fonctionne.

Alerte Mail :

On veut activer les alertes par mail.

On va dans Alerte > Type de média:



On décide d'activer les alertes par mail :

Nom ▲	Type	État	Utilisé dans les actions
Brevis.one	Webhook	Désactivé	
Discord	Webhook	Désactivé	
Email	Courriel	Activé	
Email (HTML)	Courriel	Activé	
Event-Driven Ansible	Webhook	Désactivé	
Express.ms	Webhook	Désactivé	

On configure maintenant le média mail en entrant le serveur SMTP et en entrant notre courriel :

Types de média

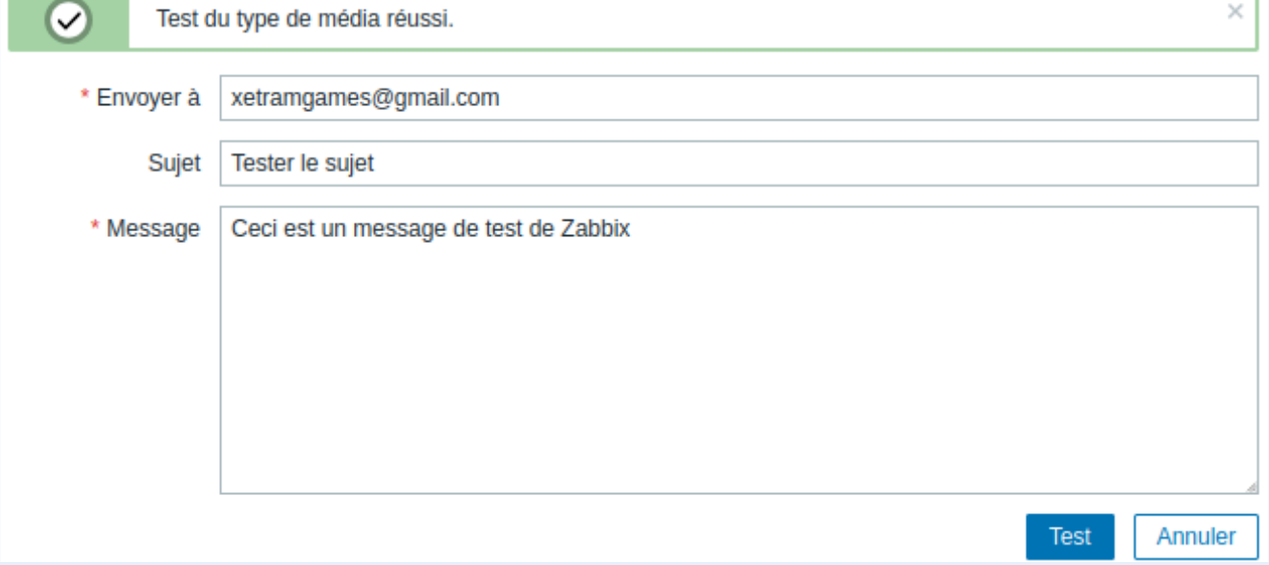
Type de média | Modèles de messages 5 | Options

* Nom	Email
Type	Courriel
Fournisseur de messagerie	Generic SMTP
* serveur SMTP	smtp.gmail.com
Port du serveur SMTP	465
* Courriel	xetramgames@gmail.com
SMTP helo	gmail.com
Sécurité de la connexion	Aucun / STARTTLS / SSL/TLS
Vérifier le pair SSL	☐
Vérifier l'hôte SSL	☐
Authentification	Aucun / Nom d'utilisateur et mot de passe
Nom d'utilisateur	xetramgames@gmail.com
Mot de passe	••••••••••••••••
Format du message	HTML / Texte brut
Description	
Activé	☑

Actualiser | Clone | Supprimer | Annuler

On fait maintenant un test pour vérifier que le nouveau média est bien pris en compte :

Tester le type de média "Email"

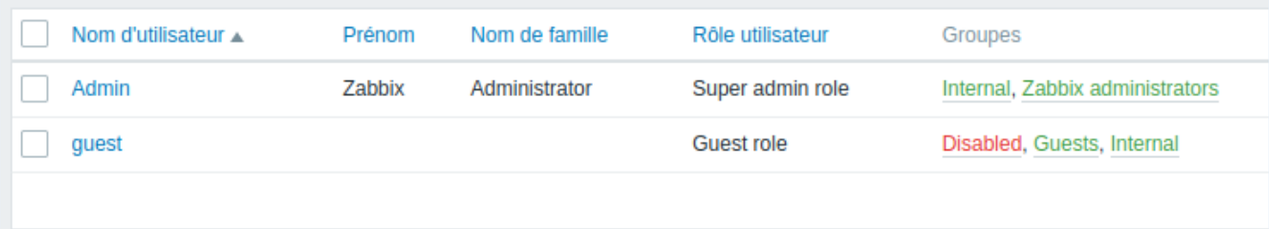


Utilisateur alerté :

On décide maintenant quelle est l'utilisateur qui reçoit les mail, pour nous ce sera l'administrateur :

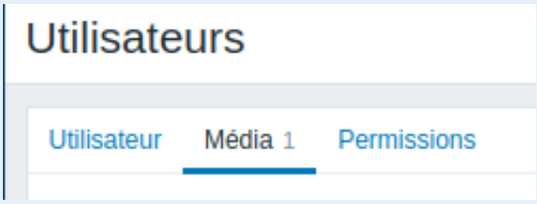
On va dans Utilisateurs > utilisateurs :

On sélectionne ensuite l'admin :

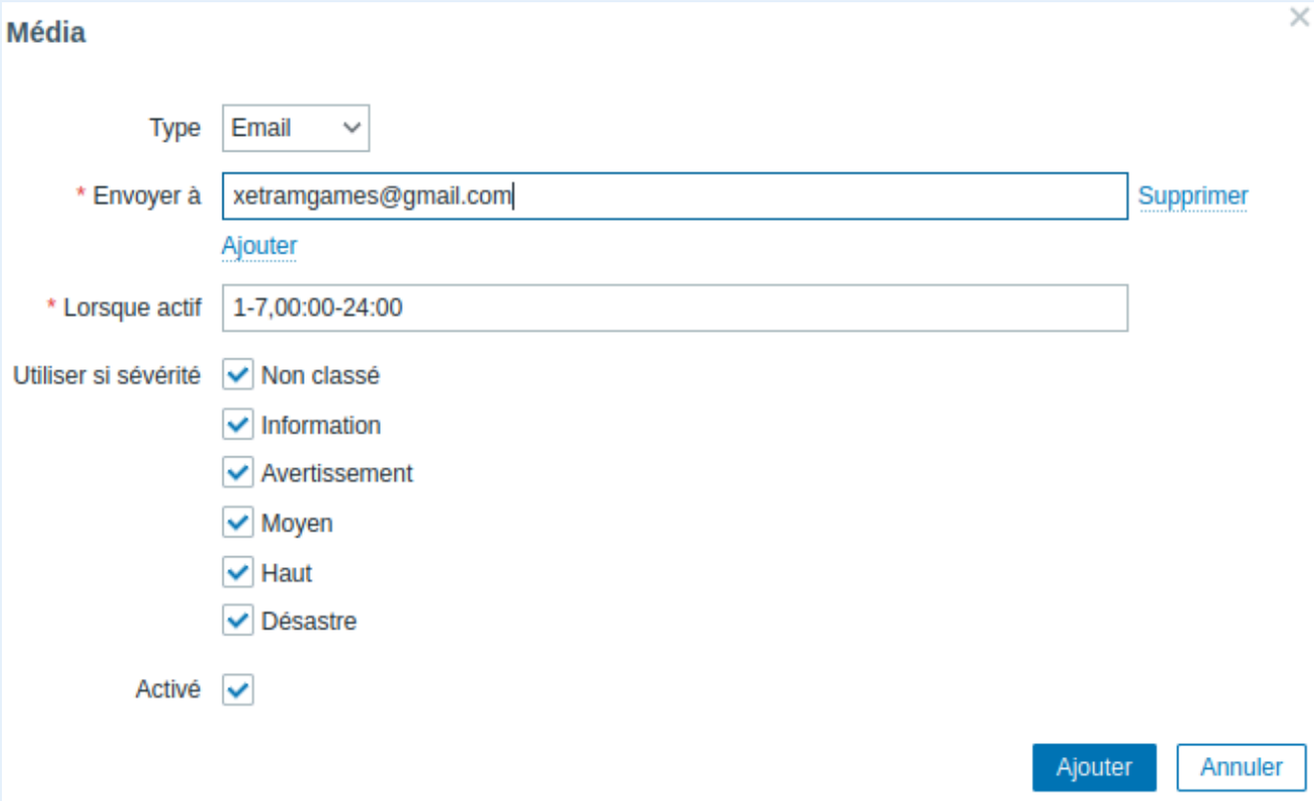


Nom d'utilisateur ▲	Prénom	Nom de famille	Rôle utilisateur	Groupes
Admin	Zabbix	Administrator	Super admin role	Internal, Zabbix administrators
guest			Guest role	Disabled, Guests, Internal

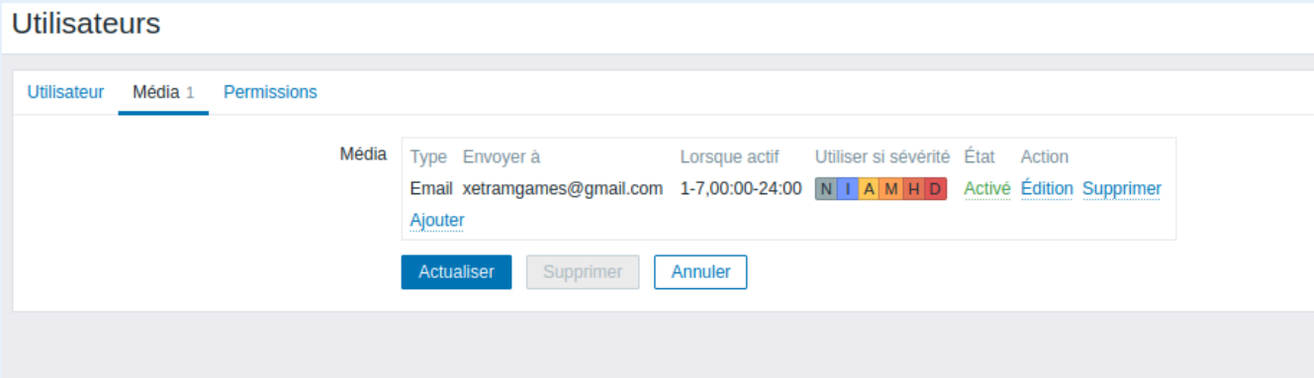
On va dans média et on fait ajouter :



On entre alors notre boite mail



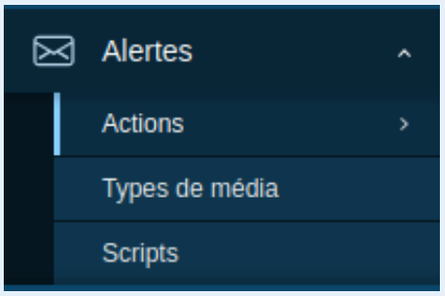
On voit bien le nouveau média pris en compte pour l'administrateur :



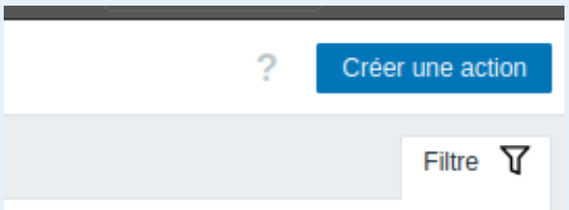
Création de l'alerte :

On va maintenant définir pour quelle problème notre admin reçoit une alerte mail.

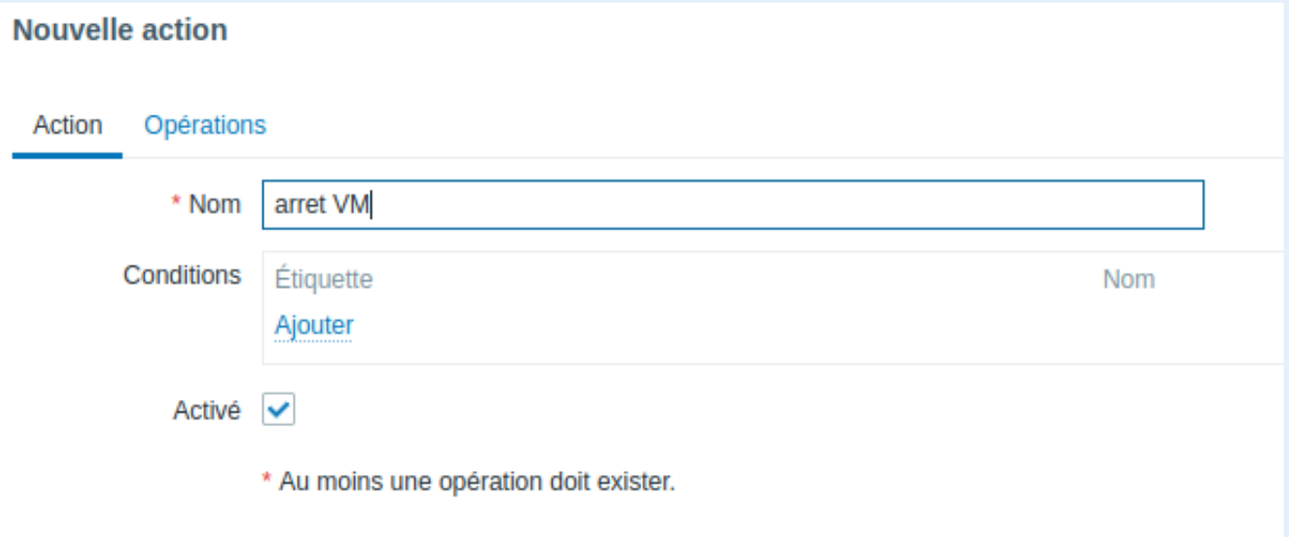
On va dans alertes > actions et on sélectionne action de déclencheur :



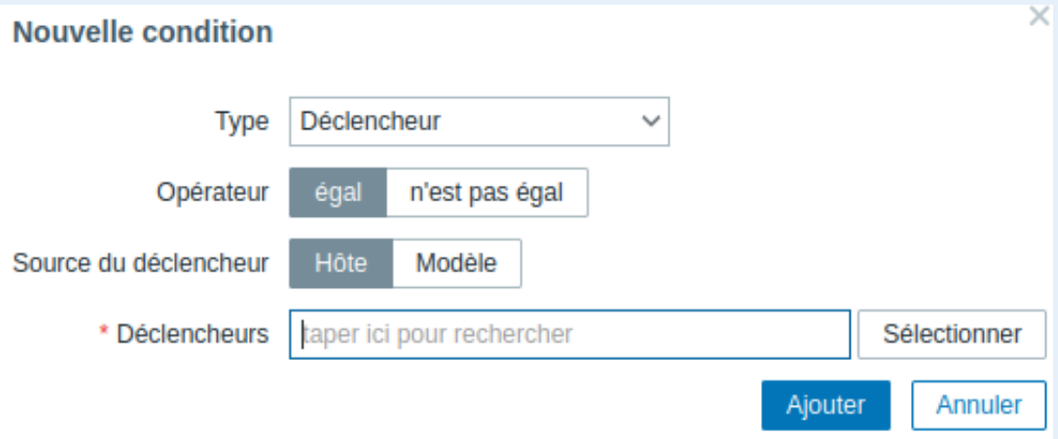
On crée une action



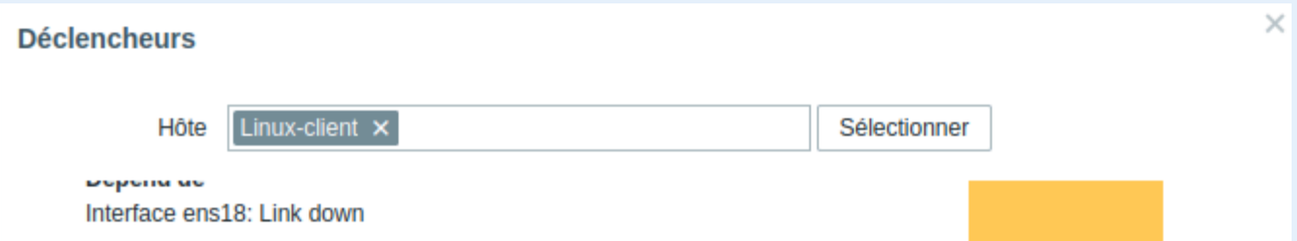
On nomme cette nouvelle action :



On sélectionne ensuite l'élement qui envoi le mail :



On choisi ensuite le problème pour lequel on veut être avertit :



Interface ens18: Link down	Moyen	Activé
Linux: /etc/passwd has been changed **Dépend de** Linux: Operating system description has changed Linux: System name has changed	Information	Activé
Linux: Configured max number of open filedescriptors is too low	Information	Activé
Linux: Configured max number of processes is too low **Dépend de** Linux: Getting closer to process limit	Information	Activé
Linux: Getting closer to process limit	Avertissement	Activé
Linux: High CPU utilization **Dépend de** Linux: Load average is too high	Avertissement	Activé
Linux: High memory utilization **Dépend de** Linux: Lack of available memory	Moyen	Activé
Linux: High swap space usage **Dépend de** Linux: Lack of available memory Linux: High memory utilization	Avertissement	Activé
Linux: Lack of available memory	Moyen	Activé
Linux: Linux-client has been restarted	Avertissement	Activé
Linux: Load average is too high	Moyen	Activé
Linux: Number of installed packages has been changed	Avertissement	Inconnu
Linux: Operating system description has changed **Dépend de** Linux: System name has changed	Information	Activé
Linux: System name has changed	Information	Activé
Linux: System time is out of sync	Avertissement	Activé
Linux: Zabbix agent is not available	Moyen	Activé
sda: Disk read/write request responses are too high	Avertissement	Activé

Sélectionner Annuler

On va ensuite dans opétations et on en ajoute une :

Nouvelle action

Action Opérations

* Durée de l'étape d'opération par défaut: 1h

Opérations: Étapes | Détails | Démarrer dans | Durée | Action
Ajouter

Opérations de récupération: Détails | Action
Ajouter

Opérations de mise à jour: Détails | Action
Ajouter

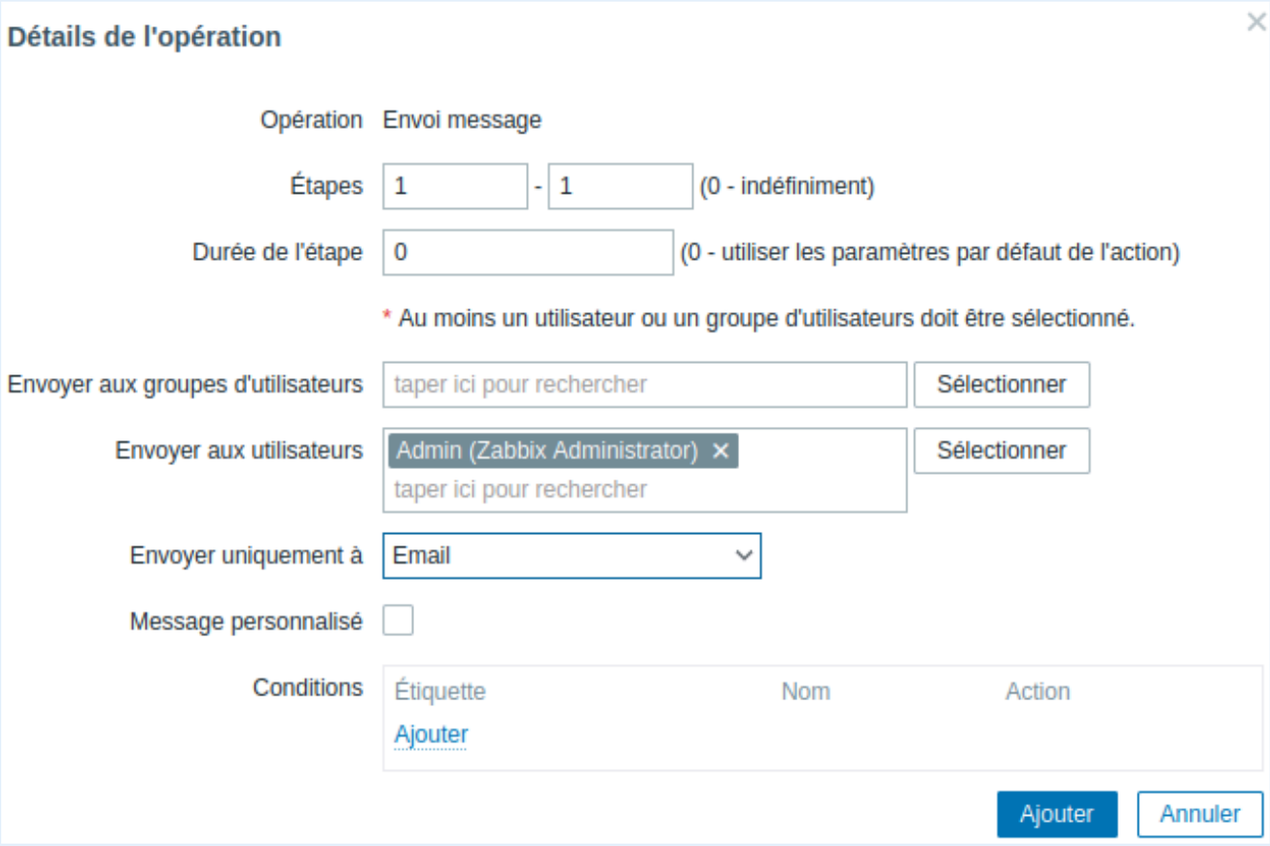
Interrompre les opérations en cas de problèmes symptomatiques ☑

Suspendre les opérations des problèmes supprimés ☑

Notifier les escalades annulées ☑

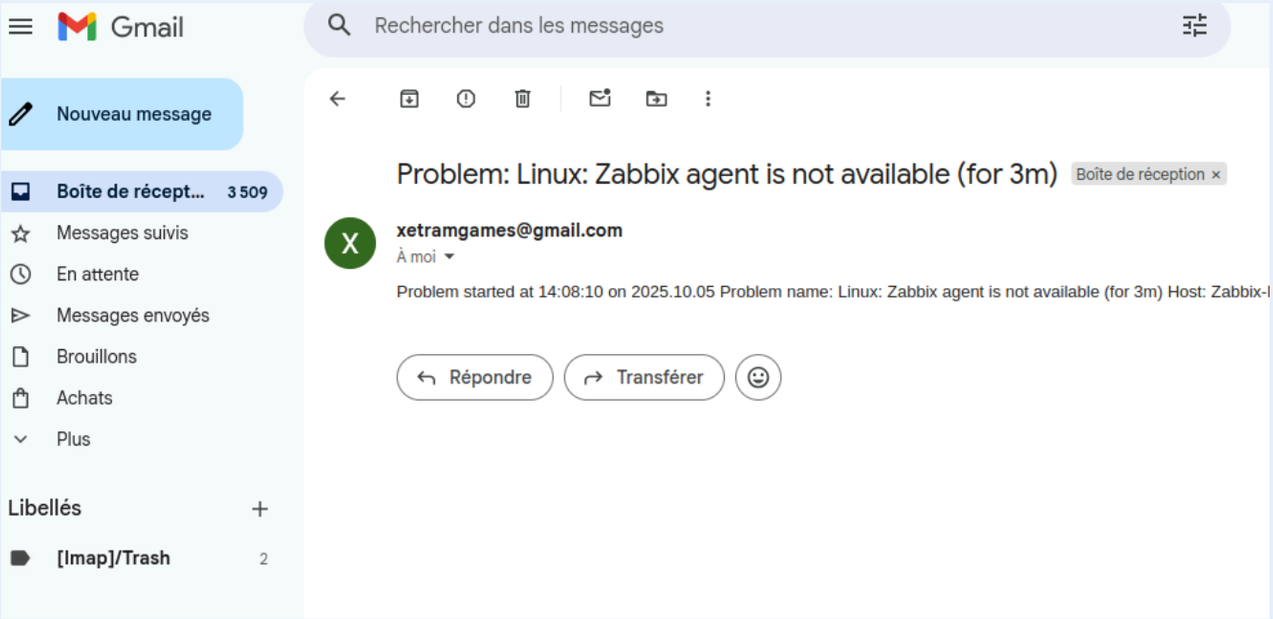
* Au moins une opération doit exister.

Enfin on sélectionne l'utilisateur ou les utilisateurs qui reçoivent l'alerte, ici l'admin reçoit une alerte mail.



Test :

On vérifie que l'alerte fonctionne, on éteint la VM et on vérifie que l'on réçoit bien l'alerte par mail.

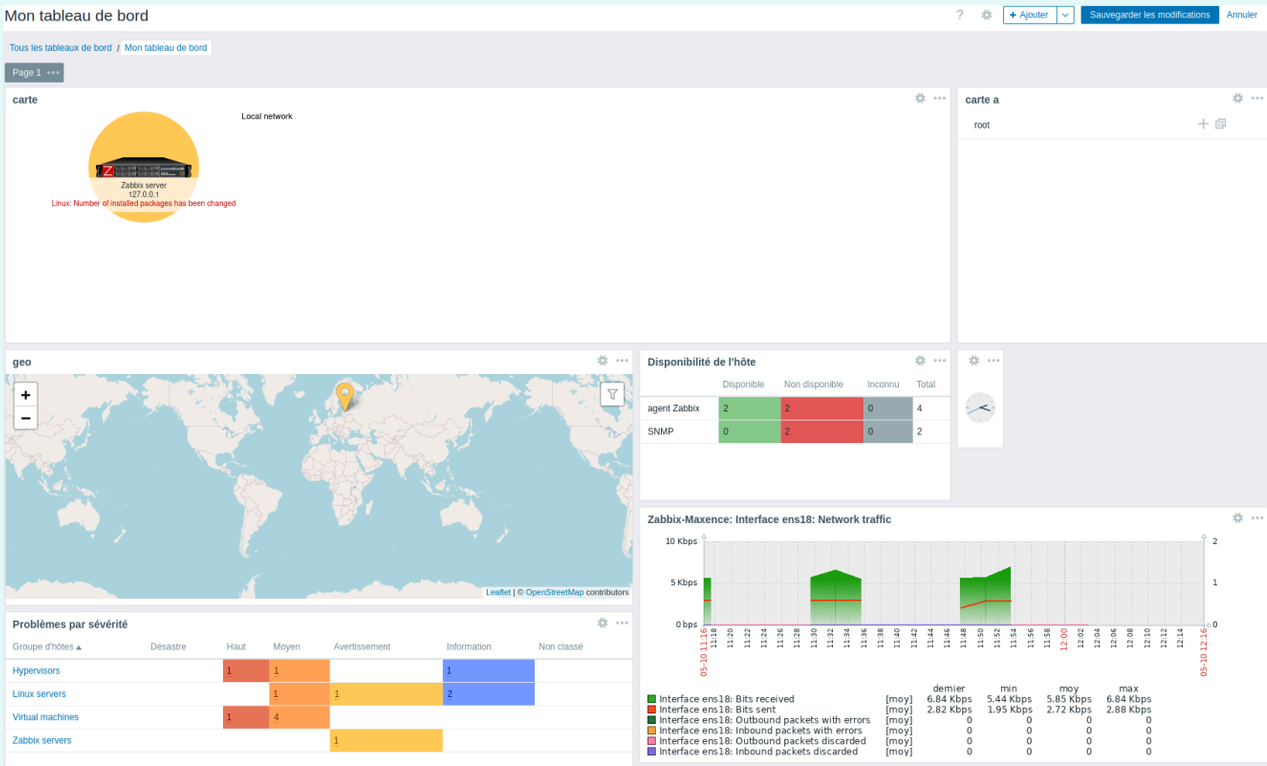


On reçoit bien le mail après que la machine se soit éteint.

Interface personnalisé :

Zabbix nous permet également de personnalisé notre interface pour plus de visibilité sur les équipements ou pour que l'on puisse se concentrer sur les éléments qui nous plaisent le plus.

Un exemple d'interfaces personnalisé :



Partie 2 – Comparaison avec PRTG

Comparaison des deux solutions :

Couts :

Zabbix est gratuit et open-source ce qui est un avantage sur son concurrent qui devient payant dès 100 capteurs, sachant que l'on peut déployer jusqu'à cinqs capteurs pour la surveillance d'une machine on arrive vite à la limite.

On peut en revanche avoir recours à un support qui est lui payant pour Zabbix, bon à savoir en cas de problème.

Installation :

PPRTG est nettement plus simple à deployer que Zabbix qui nécessite des compétences en OS Linux, PRTG peu donc d'avérer une alternative pour un petit SI n'utillisant que Windows.

Cas d'usage recommandé :

- PRTG :

Besoin d'une solution rapide à déployer et pour une équipe en info avec peu de connaissances en OS Linux, avec une infra windows dominante et si 100 capteurs suffisent ou que l'entreprise est prête à mettre le budget.

- Zabbix :

Zabbix est gratuit et ne nécessite que quelques compétences en Linux, adapté pour ceux qui préferent l'open source. De plus Zabbix est hautement customisable et peut donc être déployé pour des SI nécessitant du sur mesure. En plus comme c'est gratuit on peut l'utiliser pour de la supervision de grande échelle.

Verdict :

La solution Zabbix est la plus adpaté à nos besoins, nottament pour L'AP en raison des grandes possibiltées de customisation, de plus j'ai une préférence à titre individuel pour les solutions open-source quand c'est possible.