Caron Cyprien

BTS SIO 2

CAMPUS CARLO ACUTIS
PÔLE D'ENSEIGNEMENT SUPÉRIEUR - VERNON

Document de validation de compétences

AP-4 SUPERVIZ

18/11-16/12/2025

Groupe 1

1. Présentation du contexte d'entreprise

En 2001, deux coopératives agricoles de la région brestoise ont fusionné et donné naissance à la société coopérative agricole Savéol (qui signifie « lever de Soleil » en breton).
Savéol a été rejointe en 2012 par la coopérative du "Val Nantais" spécialisée notamment dans la Culture de mâche ainsi que par la société d'intérêt collectif agricole "Les primeurs du mistral" produisant également des tomates à Lançon de Provence près de Marseille. En deux décennies, Savéol est devenue le leader de la production de tomates en France (plus de 70 000 tonnes par an).

La société Savéol propose des prestations pour environ une centaine de maraichers adhérents, principalement situés dans le département du Finistère. Ces prestations sont les suivantes : gestion la chaîne commerciale (marketing, conditionnement, commercialisation et livraison) ; conseil technique en agronomie ; recherche et développement de nouvelles espèces et de modes de production innovants plus respectueux de l'environnement.

A l'heure actuelle, 80% de la production est commercialisée sur le territoire métropolitain et 20% part à l'export vers les pays limitrophes de la France. La valorisation et la commercialisation des produits frais fragiles que sont les tomates et les fraises nécessitent une organisation et une logistique particulièrement rodées et efficaces. En effet, la récolte quotidienne, qui peut dépasser les 800 tonnes, sera déposée par les producteurs serristes dans l'une des deux stations de conditionnement afin d'être emballée dans un packaging adapté au mode de vente et de transport. Les clients de Savéol (des enseignes de grande et moyenne surface ou des grossistes) sont assurés que leur commande sera livrée le lendemain au plus tard.

L'esprit d'innovation qui anime les administrateurs de la coopérative Savéol dans ses choix d'évolution se ressent aussi au niveau du pilotage et de la gestion de son système d'information. Le périmètre d'action de l'équipe du service informatique est diversifié et concerne la gestion de projet, le développement d'applications, l'assistance fonctionnelle utilisateur, la supervision et l'administration ainsi que la maintenance système et réseau.

Le service informatique, sous la direction de M. Netralli, compte une nouvelle chef de projet, Mme Farez, trois techniciens réseau et système, ainsi que deux personnes en charge des solutions logicielles.

Vous êtes accueillis au sein de cette équipe. Il vous est précisé que votre domaine d'intervention concernera les fonctions liées à la gestion et à l'évolution de l'infrastructure système et réseau du siège de SAVEOL.

2. Objectifs attendus

L'entreprise SAVEOL souhaite mettre en place une solution de supervision professionnelle pour surveiller l'ensemble de son infrastructure informatique (serveurs et équipements réseaux) de manière proactive.

Environnement

L'entreprise a choisi d'héberger la solution de supervision en interne sous forme virtualisée, côté LAN. Un serveur de gestion des incidents est déjà en place mais ne permet qu'une gestion réactive des problèmes.

Forme de l'objet

On souhaite une solution de supervision accessible via une interface web, permettant :

- La surveillance en temps réel des serveurs Linux et Windows (occupation disque, taux de charge, carte réseau, services)
- La supervision des équipements réseaux stratégiques (switchs, routeurs)
- L'envoi automatique d'alertes par mail aux techniciens responsables en cas de dépassement de seuil critique
- L'affichage d'une carte globale représentant l'infrastructure supervisée
- Le regroupement des serveurs par système d'exploitation

Le système doit permettre une visualisation claire de l'état de l'infrastructure et générer des notifications automatiques selon les seuils de tolérance définis.

Accessibilité/Sécurité

L'environnement doit être accessible aux seuls membres de l'équipe IT de l'entreprise. Le DSI exige une sécurité maximale compatible avec les éléments présents.

Vous devrez réaliser une recherche approfondie et documenter l'ensemble des recommandations de sécurité à mettre en œuvre lors de la configuration du protocole SNMP. Cette documentation devra lister les bonnes pratiques permettant de sécuriser les échanges entre la solution de supervision et les équipements supervisés.

Missions à Réaliser

Organisation et planification du travail

• Élaborer un planning détaillé du projet en utilisant un outil de gestion de tâches (Trello, Gantt), en répartissant clairement les responsabilités entre les membres de l'équipe et en définissant les jalons jusqu'à la date limite du 16 décembre 2025.

Recherche et choix de la solution

• Comparer au minimum 2 solutions de supervision gratuites (Zabbix, Nagios, Centreon, etc.) et présenter leurs caractéristiques au DSI.

• Effectuer une recherche documentée sur les recommandations de sécurité ANSSI relatives au protocole SNMP et lister l'ensemble des bonnes pratiques à appliquer.

Actualisation du schéma réseau

• Actualiser le schéma réseau existant pour y intégrer la nouvelle infrastructure de supervision (serveur de monitoring, flux SNMP, zones de supervision).

• Documenter les flux réseau générés par la solution de supervision.

Installation de l'infrastructure de supervision

• Créer et configurer la machine virtuelle qui hébergera la solution de supervision côté LAN.

• Installer le système d'exploitation et le logiciel de monitoring retenu.

• Sécuriser l'accès à l'interface de supervision selon les recommandations étudiées.

Sécurisation des flux réseau

• Identifier et documenter les flux SNMP nécessaires entre le serveur de supervision et les équipements supervisés.

• Configurer les règles du pare-feu ZyXEL pour autoriser uniquement les communications légitimes liées à la supervision.

• Tester et valider le bon fonctionnement des règles mises en place.

Mise en place de la surveillance des équipements

• Configurer les seuils de surveillance pour chaque type d'équipement (occupation disque, charge CPU, mémoire, état des interfaces réseau).

• Installer et configurer les agents SNMP sur l'ensemble des serveurs Linux et Windows.

• Paramétrer la supervision des équipements réseau (switchs, routeurs) sur leurs interfaces stratégiques.

• Organiser les équipements supervisés par catégories (serveurs Linux, serveurs Windows, équipements réseau).

Création de la vue d'ensemble de l'infrastructure

• Créer une carte globale de l'infrastructure supervisée dans l'interface du logiciel de monitoring.

• Organiser la visualisation pour permettre une compréhension immédiate de l'état du système d'information.

Configuration des alertes et notifications

• Configurer le système de notifications automatiques par mail en cas de dépassement des seuils critiques.

• Définir les destinataires selon leur domaine de responsabilité : un technicien pour la partie réseau, un autre pour la partie système.

• Tester le bon fonctionnement des alertes avec différents scénarios d'incidents.

Phase de tests et validation du système

• Élaborer un plan de tests complet couvrant tous les aspects de la supervision (serveurs, équipements réseau, alertes).

• Réaliser les tests et documenter les résultats dans un rapport de test détaillé.

• Corriger les éventuels dysfonctionnements identifiés.

Production de la documentation projet

• Rédiger la documentation technique complète incluant la configuration du serveur de supervision et de tous les éléments supervisés.

• Produire un guide utilisateur clair et illustré pour former l'équipe IT à l'utilisation quotidienne de l'outil de supervision.

• Rassembler l'ensemble des documents (schéma réseau, rapport de tests, recommandations SNMP, documentation technique et utilisateur) dans un dossier projet finalisé.

1. Organisation et planification du travail

Groupe : 1 *N°1*

Chef de projet : Cyprien *Nom : caron*

Durée prévisionnelle du projet : **12 h 00**

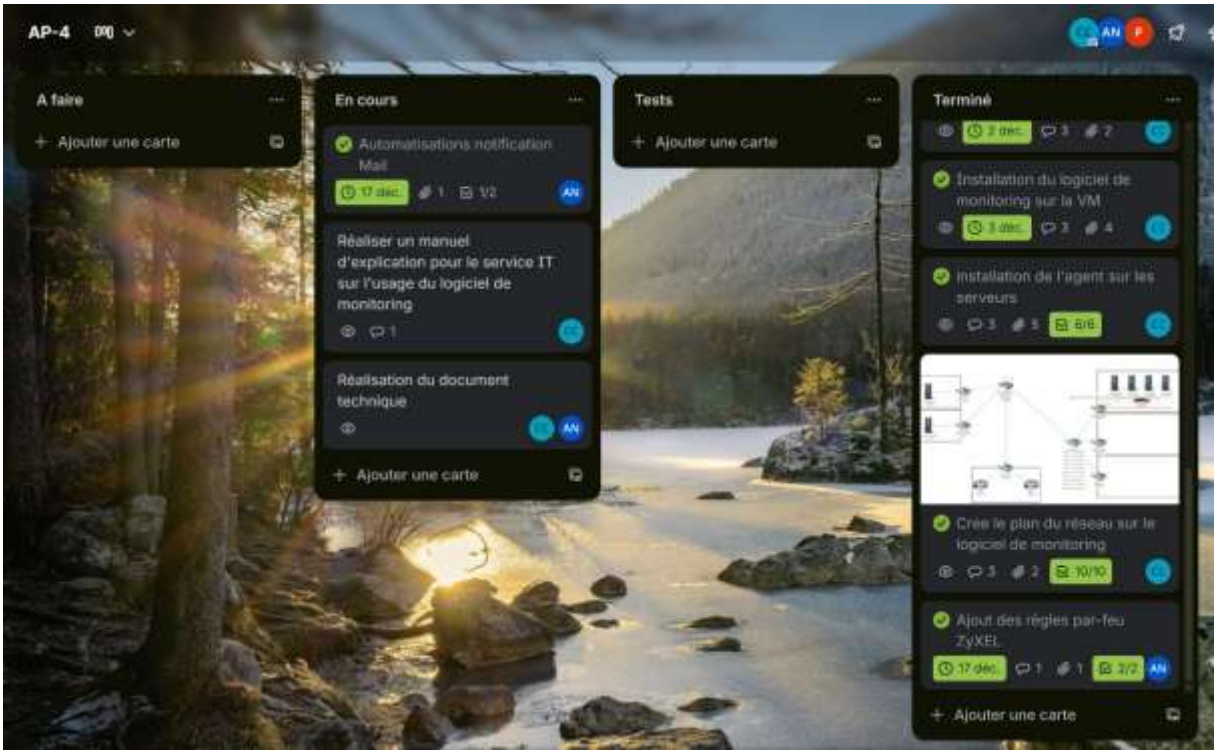
Durée réelle du projet : **9 h 20**

N°	Activité	Etudiant	Planning	Temps
1	Réalisation du schéma réseau	Cyprien	Prévisionnel	2:00
			Réel	1:00
2	Récupération et réinitialisation des équipements d'interconnexion	Abdelaadim	Prévisionnel	1:00
			Réel	4:00
3	Câblage	Cyprien	Prévisionnel	1:00
			Réel	0:10
4	Repérage	Abdelaadim	Prévisionnel	1:00
			Réel	0:10
5.1	Mise en place des VLAN et du VTP	Cyprien	Prévisionnel	1:00
			Réel	0:50
5.2	Routage InterVLAN	Cyprien	Prévisionnel	1:00
			Réel	0:30
5.3	Configuration du dhcp	Cyprien	Prévisionnel	1:00
			Réel	0:30
6	Administration à distance centralisée	Abdelaadim	Prévisionnel	2:00
			Réel	2:00
7	Sauvegarde	Abdelaadim	Prévisionnel	2:00
			Réel	0:10

Réalisation d'un diagramme de Gantt pour l'attribution des tâches et la répartition du temps.

Réalisation du schéma réseau	Cyprien
Récupération et réinitialisation des équipements d'interconnexion	Abdelaadim
Câblage	Cyprien
Repérage	Abdelaadim
Mise en place des VLAN et du VTP	Cyprien
Routage InterVLAN	Cyprien
Configuration du dhcp	Cyprien
Administration à distance centralisée	Abdelaadim
Sauvegarde	Abdelaadim

Création d'un Trello pour le suivi des activités.



2. Recherche et choix de la solution

Comparaison des logiciels de monitoring : Zabbix vs PRTG

Critères	Zabbix	PRTG
Type de logiciel	Open-source	Propriétaire (avec version gratuite)
Coût	Gratuit, nécessite des ressources pour l'installation	Tarification selon le nombre de capteurs (version gratuite limitée à 100 capteurs)
Interface utilisateur	Web, personnalisable	Interface web intuitive, facile d'utilisation
Fonctionnalités	Surveillance réseau, serveurs, applications, alertes avancées	Surveillance complète : réseau, serveurs, applications, capteurs externes
Configuration	Plus complexe, nécessite des compétences techniques	Configuration simple et rapide
Alertes	Système d'alerte configurable, avec escalades	Notifications faciles à configurer, options multiples
Plan de l'infra	Cartographie d'infrastructure, visualisation avancée	Cartographie basique de réseau et d'infrastructure

Analyse des caractéristiques :

Zabbix

Avantages :

Gratuit et open-source, permettant personnalisation complète.

Haute scalabilité, idéale pour grands environnements.

Alertes avancées et visualisations efficaces.

PRTG

Avantages :

Facile à installer et configurer, interface intuitive.

Support technique inclus, avantage pour petites équipes.

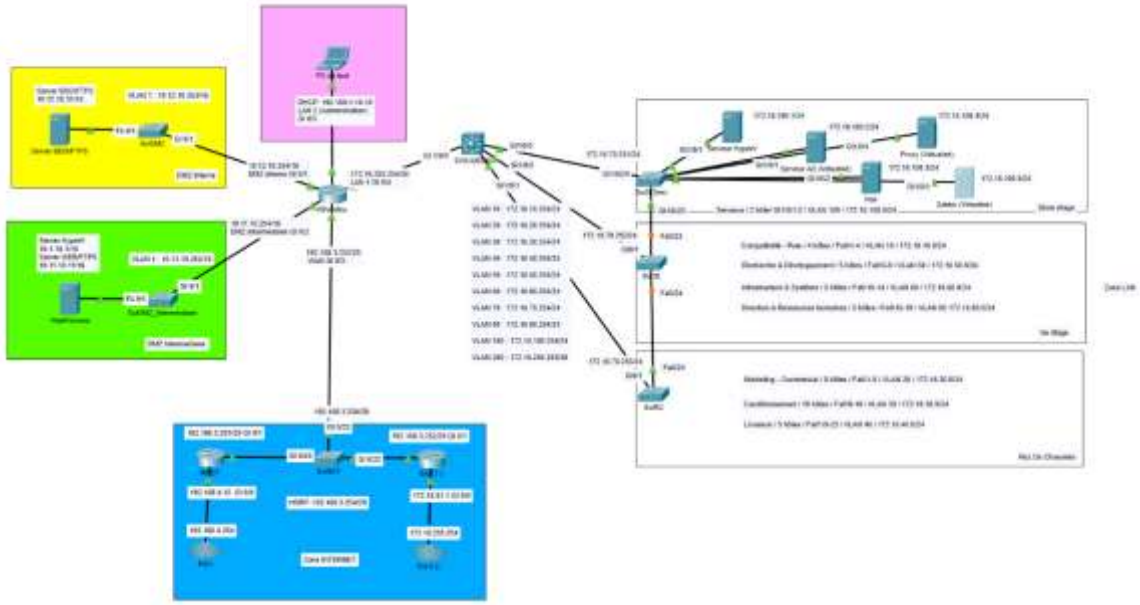
Inconvénients :

Coût élevé pour grands environnements, augmentation du nombre de capteurs.

Moins de flexibilité en termes de personnalisation par rapport à Zabbix.

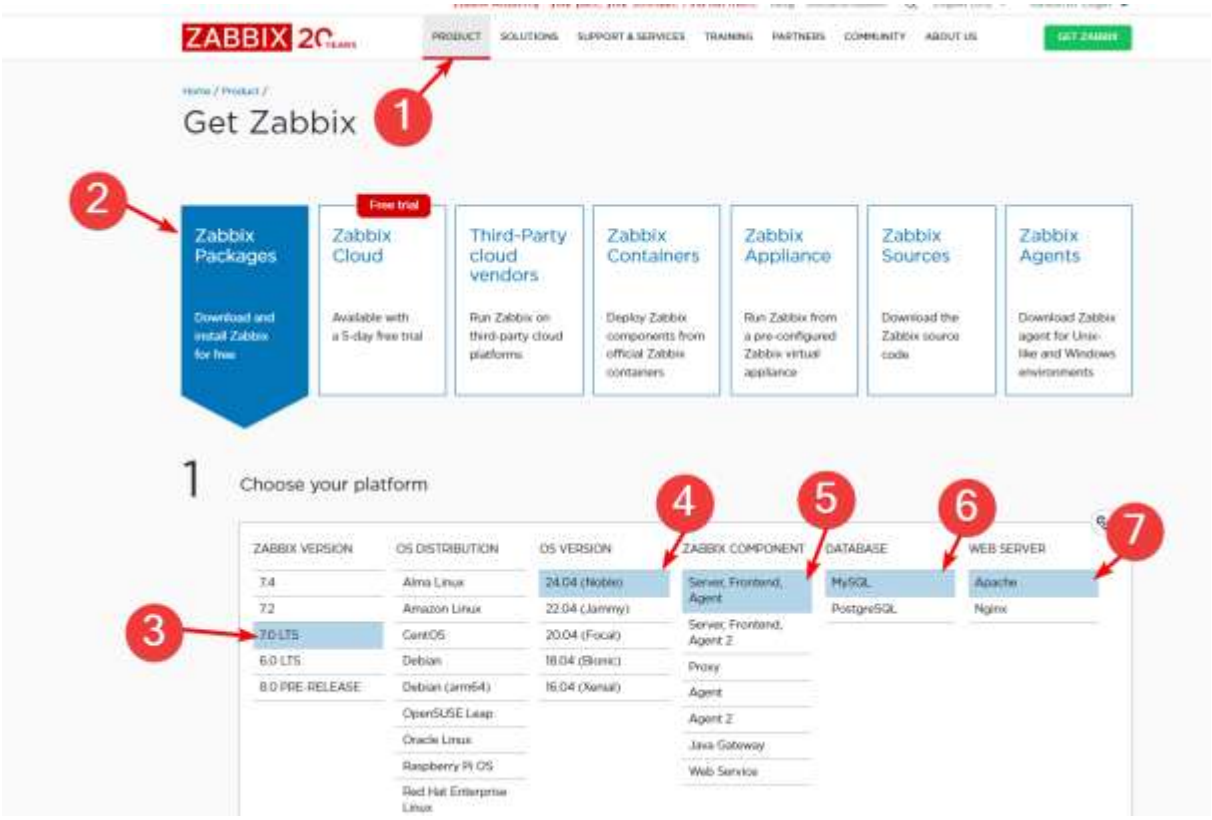
À l'issue de ce comparatif, la solution retenue est Zabbix.

3. Actualisation du schéma réseau



4. Installation de l'infrastructure de supervision

Rendez-vous sur le site de Zabbix puis aller dans download [ici :]



Sélectionner la version souhaitée pour ma part j'ai choisi la « **7.0 LTS** » car c'est la dernière stable.

Puis rentrer les commande inquées ci-dessous

```
# passer en mode super admin
ubuntu-zabbix@zabbix:~$ Sudo su
[sudo] password for ubuntu-zabbix:
root@zabbix:/home/ubuntu-zabbix#

# installer le répertoire Zabbix
root@zabbix:/home/ubuntu-zabbix# wget
https://repo.zabbix.com/zabbix/7.0/ubuntu-arm64/pool/main/z/zabbix-
release/zabbix-release_latest_7.0+ubuntu24.04_all.deb

# extraire le contenu du paquet installé
root@zabbix:/home/ubuntu-zabbix# dpkg -i Zabbix
release_latest_7.0+ubuntu24.04_all.deb

# mise à jour de la liste des paquets
root@zabbix:/home/ubuntu-zabbix# apt update

# installation de Zabbix serveur, et de l'agent
root@zabbix:/home/ubuntu-zabbix# apt install zabbix-server-mysql zabbix-frontend-
php zabbix-apache-conf zabbix-sql-scripts zabbix-agent

#installation de MariaDB
root@zabbix:/home/ubuntu-zabbix# apt install mariadb-server

# création de la base de données
root@zabbix:/home/ubuntu-zabbix# mysql -uroot -p
password
MariaDB [(none)]> create database zabbix character set utf8mb4 collate utf8mb4_bin;
MariaDB [(none)]> create user zabbix@localhost identified by 'password';
MariaDB [(none)]> grant all privileges on zabbix.* to zabbix@localhost;
MariaDB [(none)]> set global log_bin_trust_function_creators = 1;
MariaDB [(none)]> quit;

# exécution des commandes SQL présente dans le fichier « zabbix_sql »
root@zabbix:/home/ubuntu-zabbix#  zcat /usr/share/zabbix-sql-
scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p Zabbix

# Desactive la confiance dans les créateurs de fonction
MariaDB [(none)]> set global log_bin_trust_function_creators = 0;
MariaDB [(none)]> quit;

# modification du fichier de conf zabbix
root@zabbix:/home/ubuntu-zabbix# nano /etc/zabbix/zabbix_server.conf
```

#modification du fichier de conf pour déclarer le mdp de la base de données


```
# redémarre le serveur Zabbix et active le démarrage par défaut
systemctl restart zabbix-server zabbix-agent apache2
systemctl enable zabbix-server zabbix-agent apache2
```

5. Mise en place de la surveillance des équipements

Pour Linux

Installation de l'agent sur un linux classique

```
#Récupération du repo et décompresser le repo que vous venez d'installer
wget https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest_7.0+ubuntu24.04_all.deb
dpkg -i zabbix-release_latest_7.0+ubuntu24.04_all.deb

#Mise à jour des paquets et installation de l'agent
apt update
apt install zabbix-agent
```

Générer la PSK dans un fichier

```
root@srvweb:/home/srv_web# mkdir /home/zabbix
root@srvweb:/home/srv_web# cd /home/zabbix/
root@srvweb:/home/zabbix# openssl rand -hex 128 > secret.psk
```

Configuration de l'agent

```
#Modification du fichier de conf de l'agent
nano /etc/zabbix/zabbix_agentd.conf
```

Modifier ces lignes dans le fichier « Zabbix_agents.conf »

```
Server=172.16.100.5 (@IP du serveur zabbix)
ServerActive=172.16.100.5 (@IP du serveur zabbix)
Hostname=Server-Interne (Nom de l'agent configuré sur le serveur zabbix)

TLSConnect=psk
```

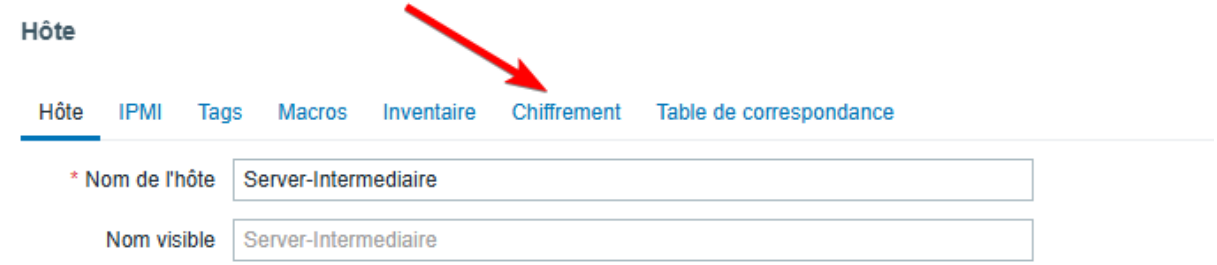
```
TLSAccept=psk
TLSPSKFile=/home/zabbix/secret.psk
TLSPSKIdentity=Server-Intermediaire
```

```
ServerActive=172.16.100.5

### Option: Hostname
#       List of comma delimited unique, case sensitive hostnames.
#       Required for active checks and must match hostnames as configured on th
#       Value is acquired from HostnameItem if undefined.
#
# Mandatory: no
# Default:
# Hostname=

Hostname=Server-Intermediaire
```

```
TLSConnect=psk
TLSAccept=psk
TLSPSKFile=/home/zabbix/secret.psk
TLSPSKIdentity=Server-Intermediaire
```

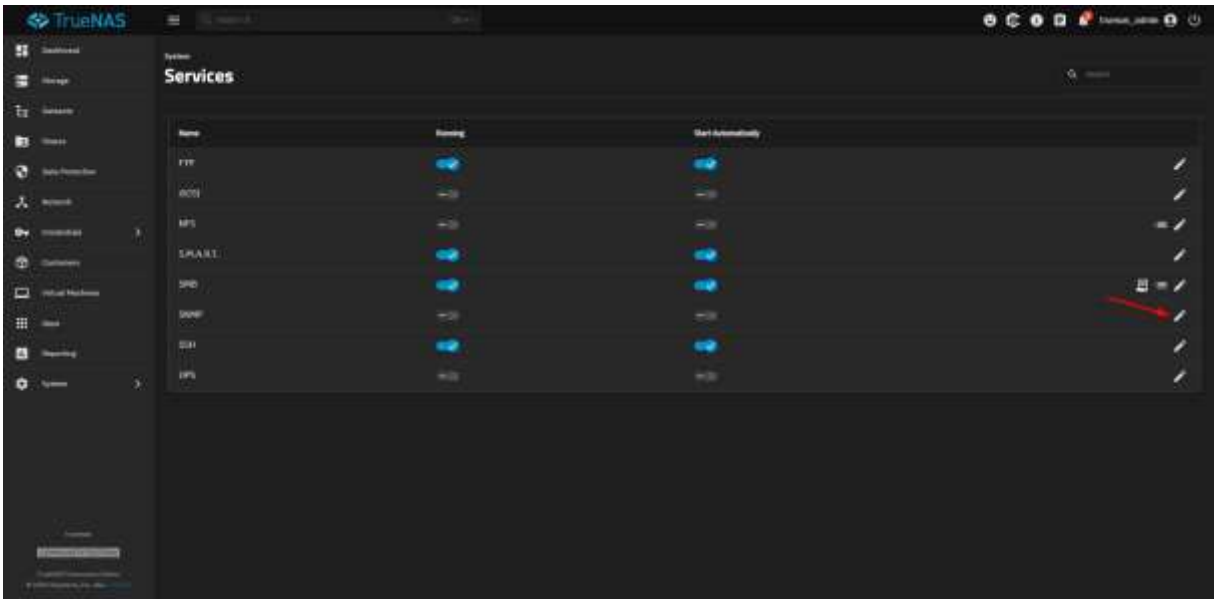
Puis redémarrer l'agent

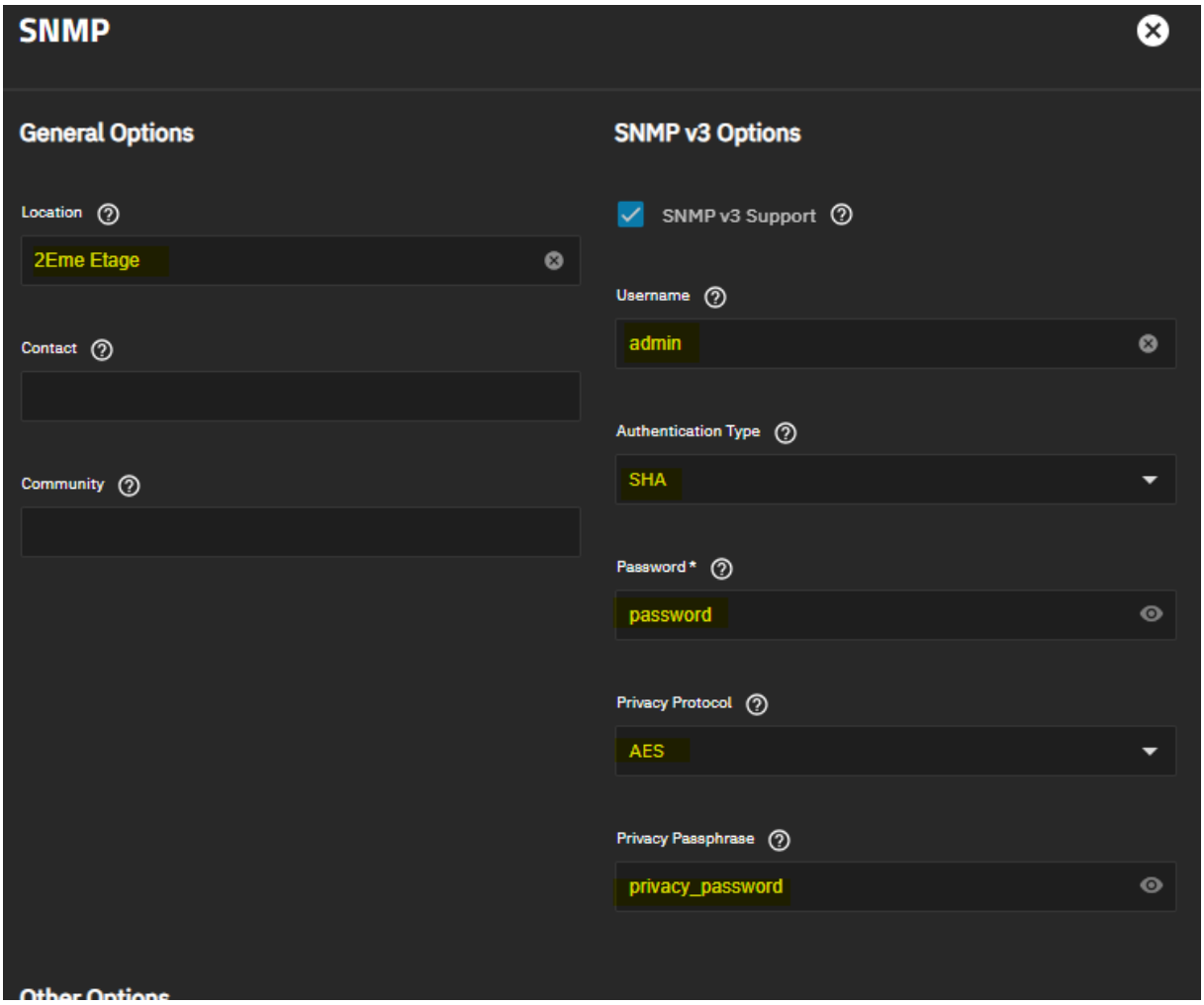
```
systemctl restart zabbix-agent
systemctl enable zabbix-agent
```



Installation de l'agent sur truenas

Modifier la configuration SNMP



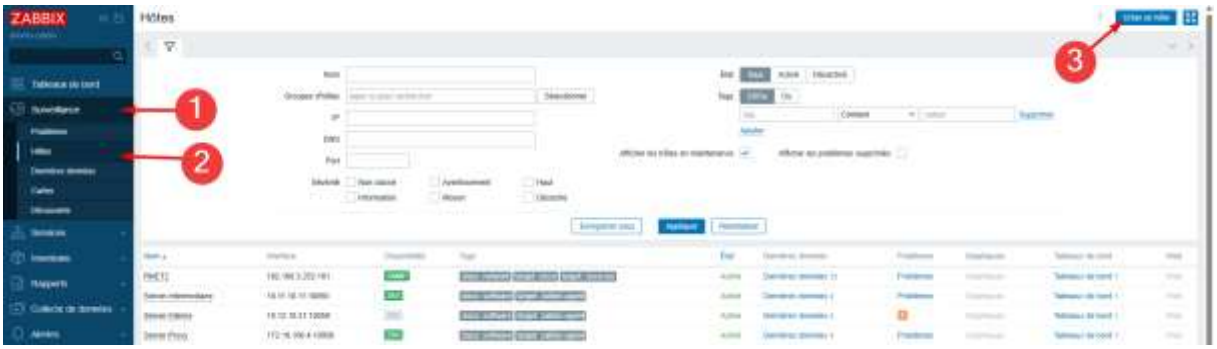


Activer le service SNMP et activer le démarrage automatique

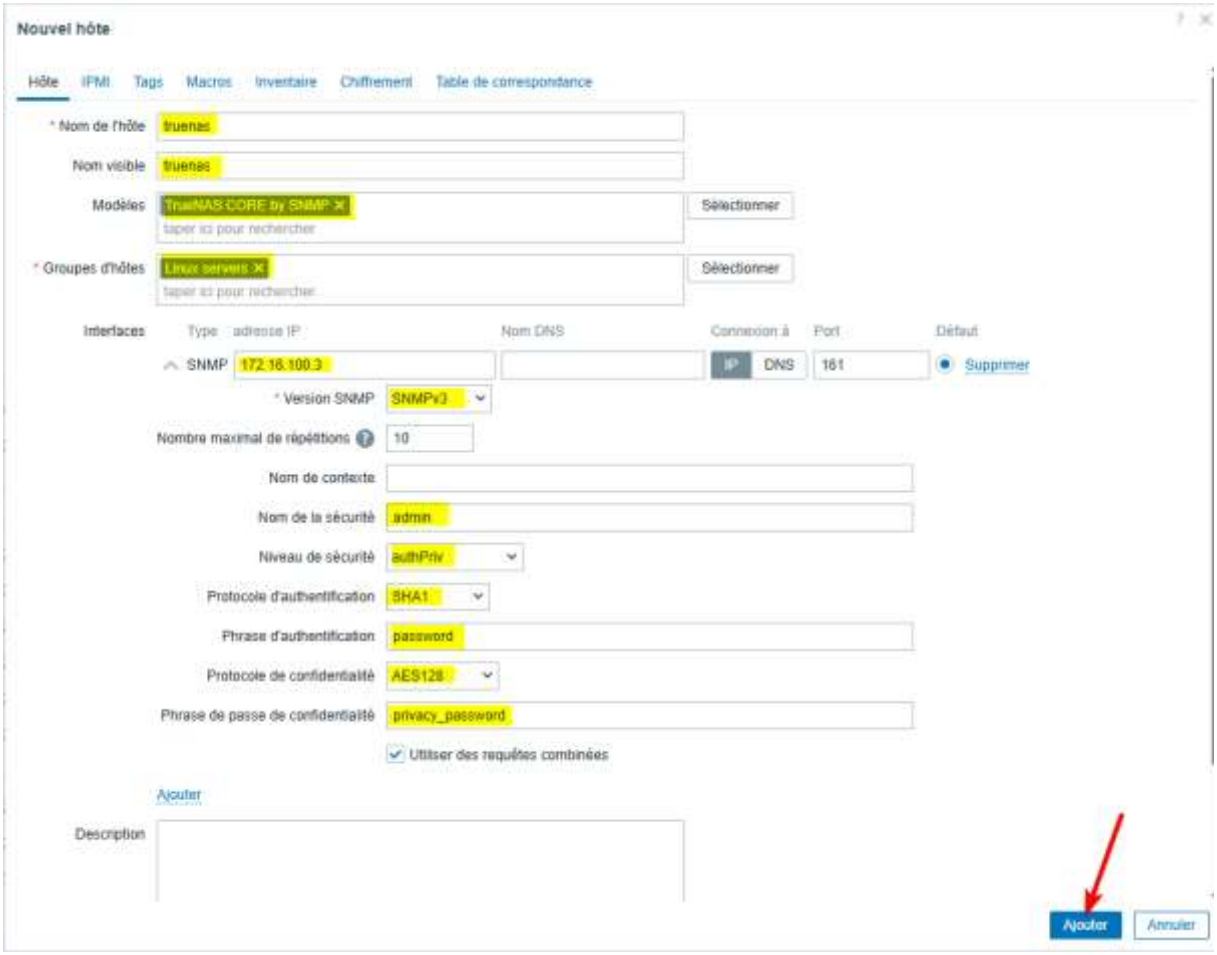
Installer le paquet pour activer le SNMP v3 et tester la connexion avec TrueNas

```
root@zabbix:/home/ubuntu-zabbix# apt install snmpd snmp libsnmp-dev -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
snmpd est déjà la version la plus récente (5.9.4+dfsg-1.1ubuntu3.1).
snmpd passé en « installé manuellement ».
libsnmp-dev est déjà la version la plus récente (5.9.4+dfsg-1.1ubuntu3.1).
Les NOUVEAUX paquets suivants seront installés :
  snmp
0 mis à jour, 1 nouvellement installés, 0 à enlever et 14 non mis à jour.
Il est nécessaire de prendre 180 ko dans les archives.
Après cette opération, 729 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 snmp amd64 5.9.4+dfsg-1.1ubuntu3.1 [180 kB]
180 ko réceptionnés en 0s (1 392 ko/s)
Sélection du paquet snmp précédemment désélectionné.
(Lecture de la base de données... 138585 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../snmp_5.9.4+dfsg-1.1ubuntu3.1_amd64.deb ...
Dépaquetage de snmp (5.9.4+dfsg-1.1ubuntu3.1) ...
Paramétrage de snmp (5.9.4+dfsg-1.1ubuntu3.1) ...
Traitement des actions différées (« triggers ») pour man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@zabbix:/home/ubuntu-zabbix# snmpwalk -v3 -a SHA -A password -x AES -X privacy_password -l authPriv -u admin 172.16.100.3 | head -10
iso.3.6.1.2.1.1.1.0 = STRING: "TrueNAS-25.04.2.4. Hardware: x86_64 Intel(R) Xeon(R) E-2124 CPU @ 3.30GHz. Software: Linux 6.12.15-production+truen
as (revision #1 SMP PREEMPT_DYNAMIC Mon Sep  8 18:50:34 UTC 2025)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.50536.3.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (43597) 0:07:15.97
iso.3.6.1.2.1.1.4.0 = STRING: "unknown@localhost"
iso.3.6.1.2.1.1.5.0 = STRING: "truenas"
iso.3.6.1.2.1.1.6.0 = STRING: "2Eme Etage"
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
root@zabbix:/home/ubuntu-zabbix#
```

Création de l’hôte sur Zabbix

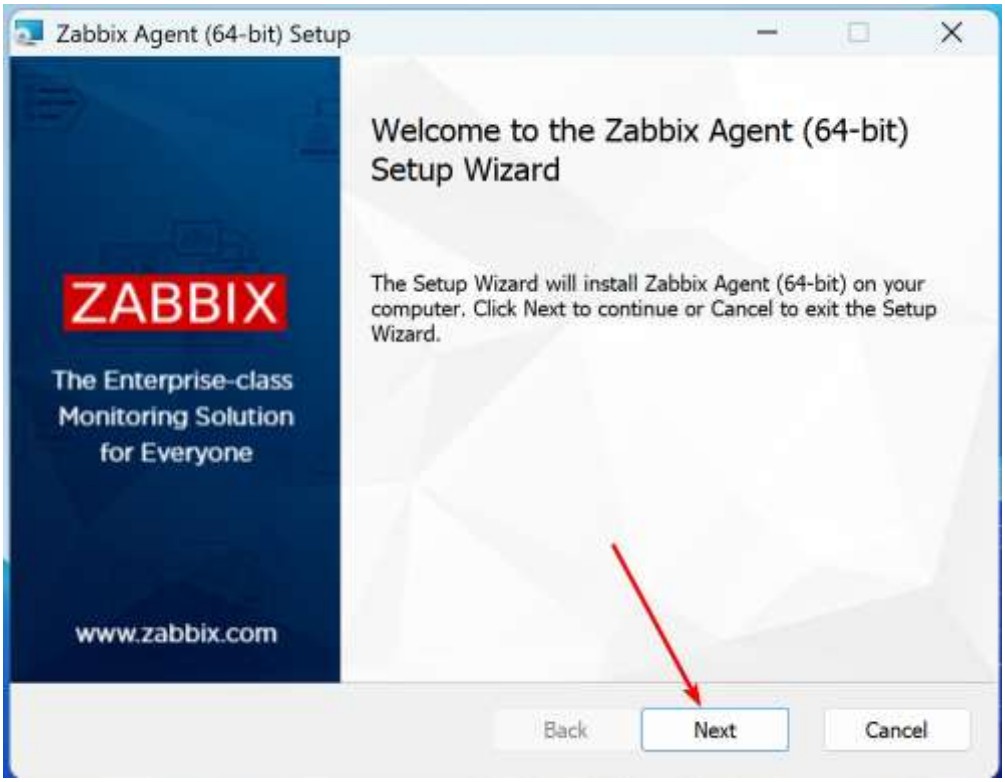


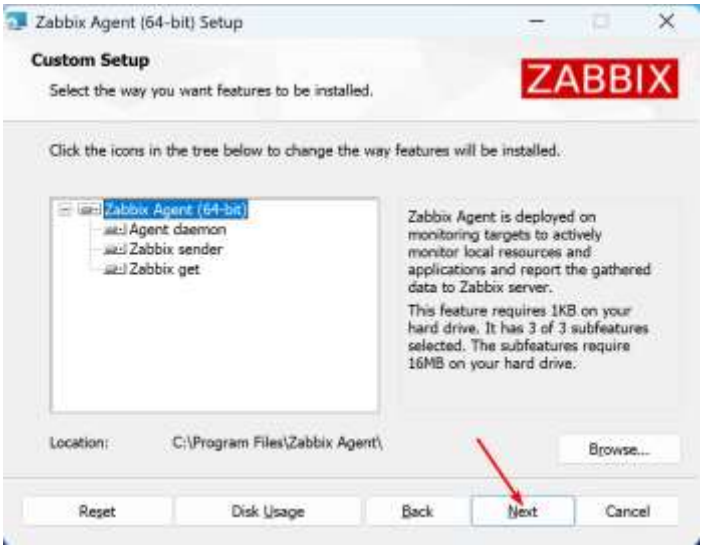
Insérer les informations comme dans la capture d’écran ci-dessous :



Pour Windows

Installation de l'agent





Remplissez les infos du serveur :

IP : 172.16.100.5

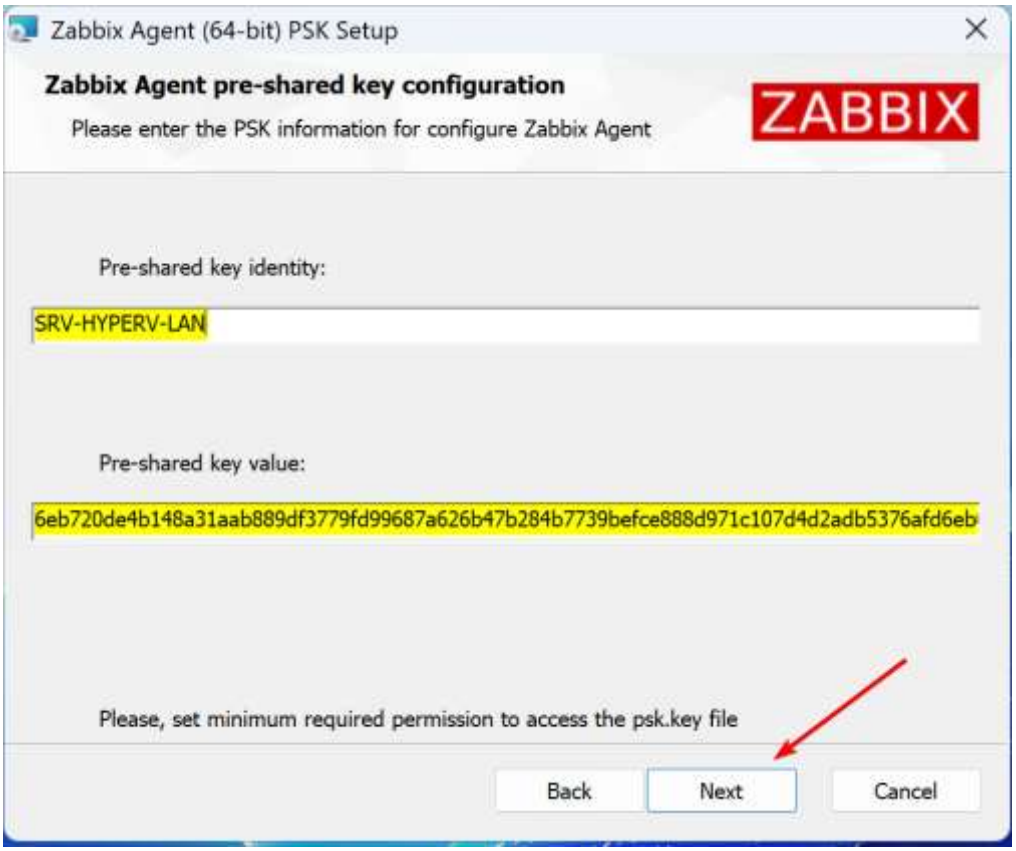
Port : 10050

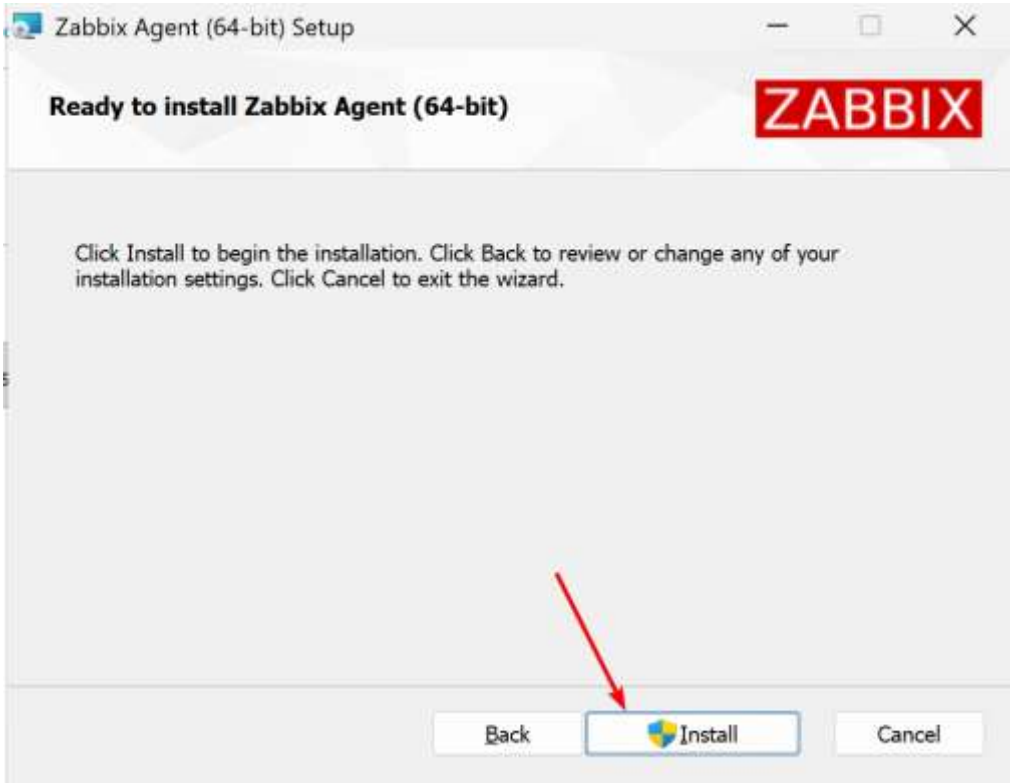
Et cocher les cases suivantes « enable PSK » et « add agent … »

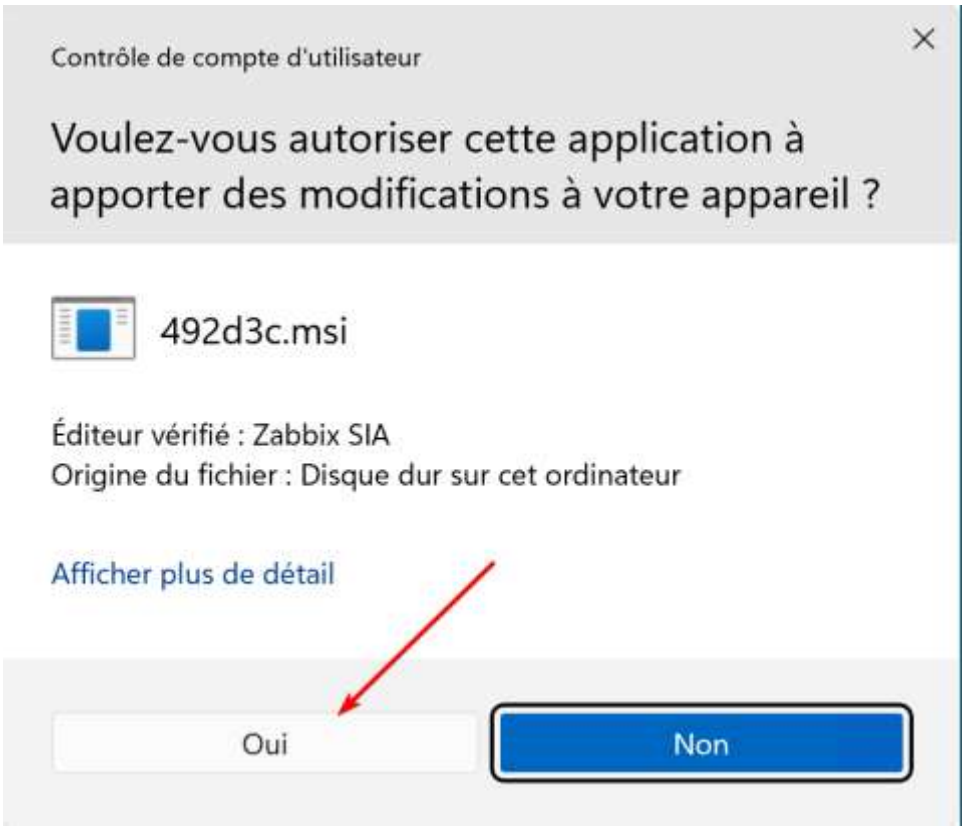
Puis générer une PSK de 128 caractères

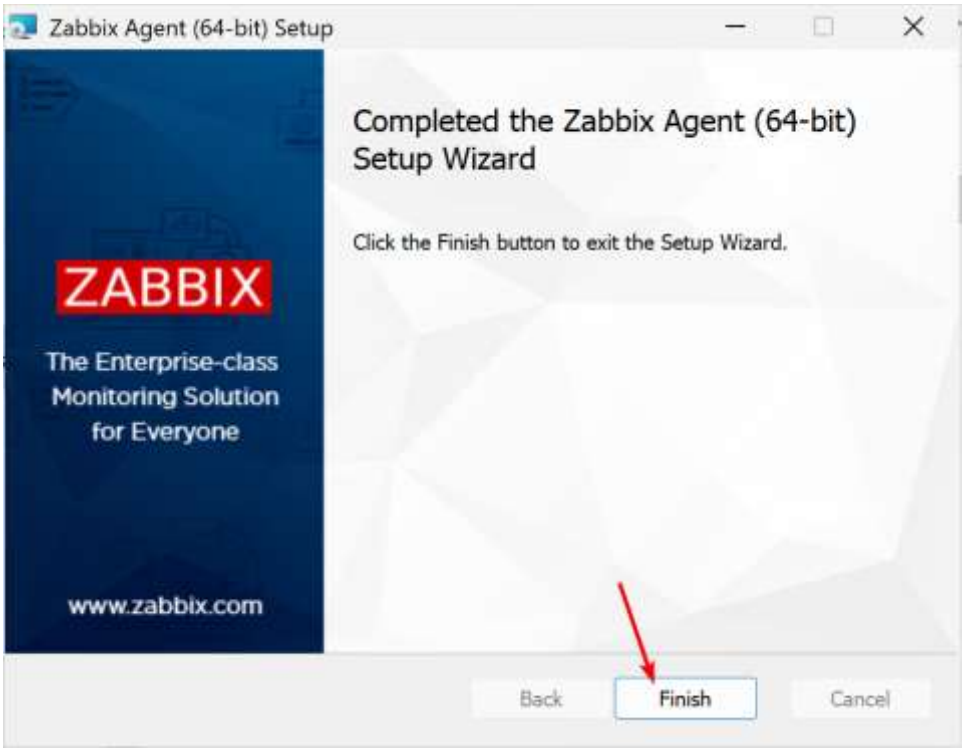
```
root@zabbix:/home/ubuntu-zabbix# openssl rand -hex 128
6eb720de4b148a31aab889df3779fd99687a626b47b284b7739befce888d971c107d4d2adb5376afd6eb0991f74ed908d1199b98f365fcab6577911f0
3aeec35754d06f0927ebcce458dcb6de64a1f19a96e77b8f456fda4b6baf6d2fe467b3749ecd0e87c870747a61ec7a56efe5c31cb10dd9
root@zabbix:/home/ubuntu-zabbix#
```

Et entrer l'ID et la PSK qui vient d'être générée

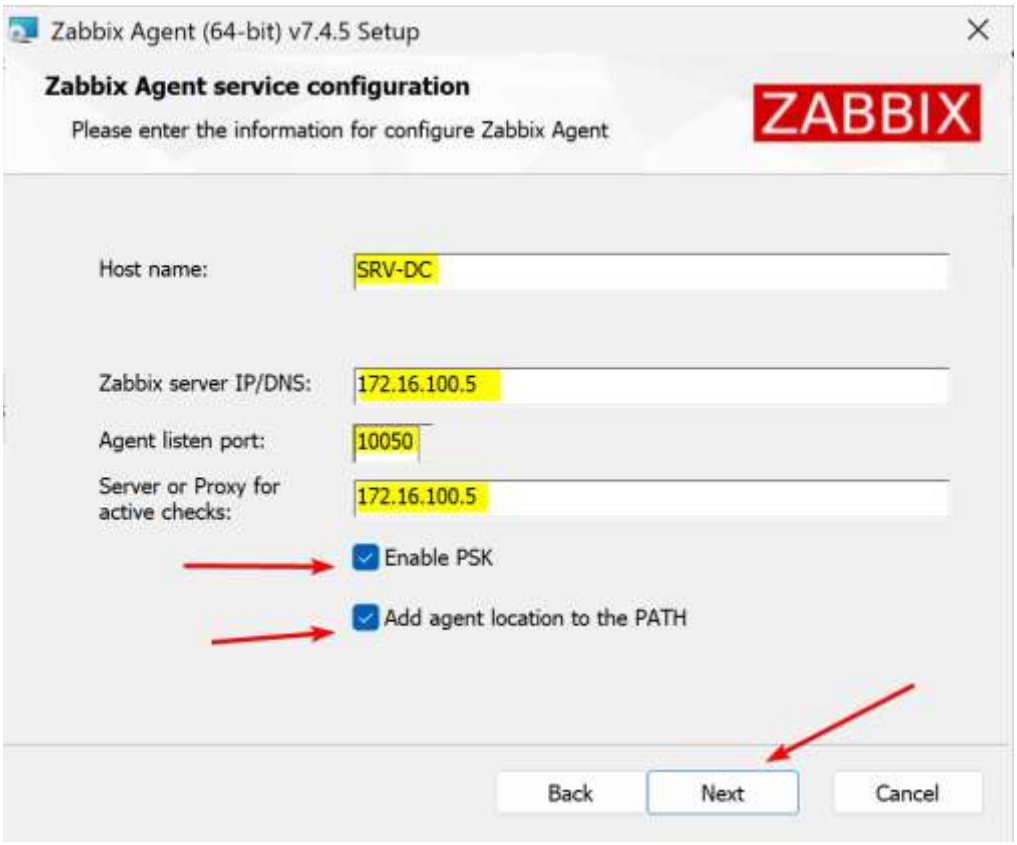

Zabbix Agent (64-bit) PSK Setup
Zabbix Agent pre-shared key configuration
Please enter the PSK information for configure Zabbix Agent
ZABBIX
Pre-shared key identity:
SRV-HYPERV-LAN
Pre-shared key value:
6eb720de4b148a31aab889df3779fd99687a626b47b284b7739befce888d971c107d4d2adb5376afd6eb
Please, set minimum required permission to access the psk.key file
Back
Next
Cancel

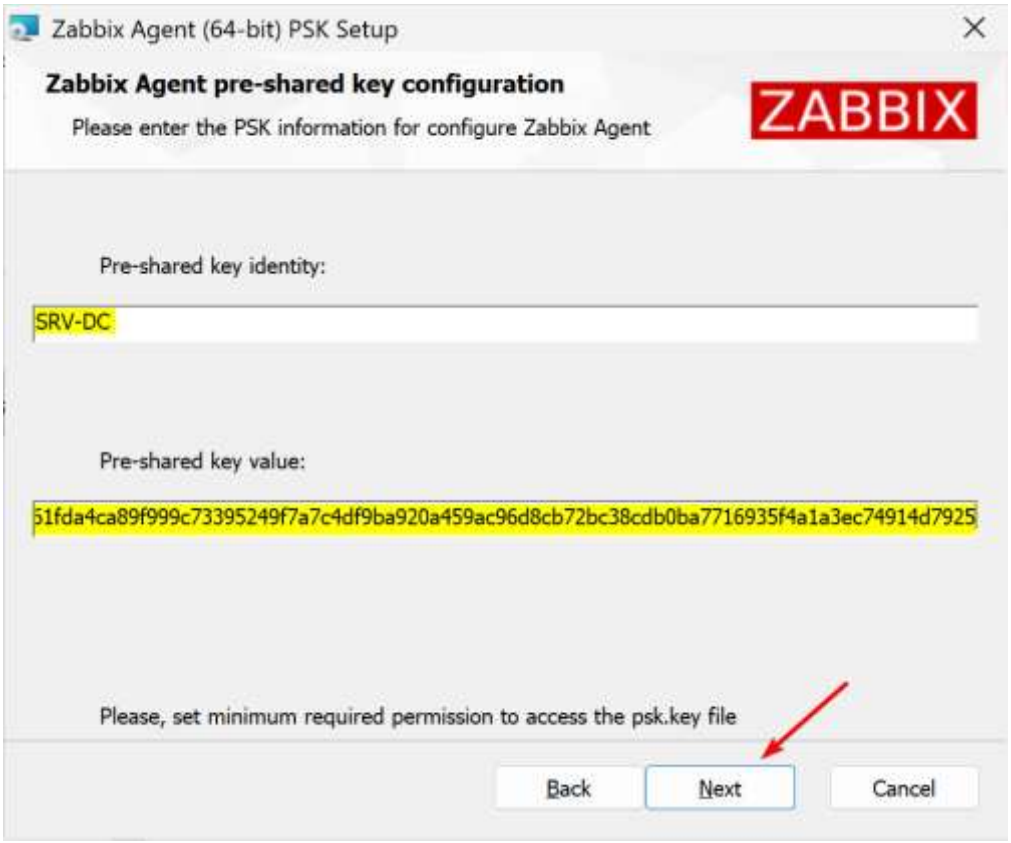

Zabbix Agent (64-bit) Setup
Ready to install Zabbix Agent (64-bit)
ZABBIX
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel



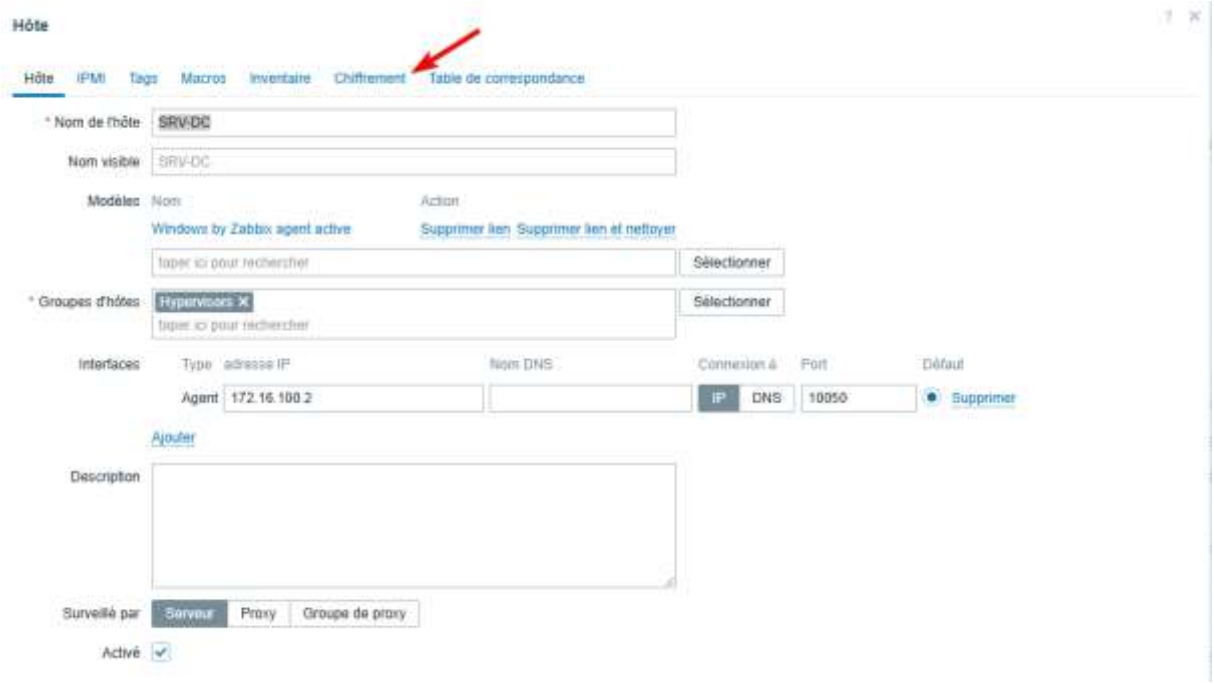


L'installation est finie sur le serveur HYPER-V maintenant il faut faire de même avec le SRV-DC


Zabbix Agent (64-bit) v7.4.5 Setup
Zabbix Agent service configuration
Please enter the information for configure Zabbix Agent
ZABBIX
Host name:
SRV-DC
Zabbix server IP/DNS:
172.16.100.5
Agent listen port:
10050
Server or Proxy for active checks:
172.16.100.5
Enable PSK
Add agent location to the PATH
Back
Next
Cancel


Zabbix Agent (64-bit) PSK Setup
Zabbix Agent pre-shared key configuration
Please enter the PSK information for configure Zabbix Agent
ZABBIX
Pre-shared key identity:
SRV-DC
Pre-shared key value:
51fda4ca89f999c73395249f7a7c4df9ba920a459ac96d8cb72bc38cdb0ba7716935f4a1a3ec74914d7925
Please, set minimum required permission to access the psk.key file
Back
Next
Cancel

Une fois cela fait il faut aller sur Zabbix sur l'hôte concerné donc « SRV-DC » et « SRV-HYPERV-LAN »



Aller dans chiffrement puis activer le PSK et entrer les informations configurées précédemment

Pour les équipements d'interconnexion

Sur le serveur zabbix :

Installation de « libsnmp-dev » pour pouvoir configurer un utilisateur/mot de passe pour l'authentification entre le serveur zabbix et nos clients via le protocole snmp

```
apt install libsnmp-dev
```

Mise en arrêt du service snmpd pour la création d'un user

```
sudo service snmpd stop
```

Création d'un user authPrivUser avec pour mot de passe myauthphrase le tout sécurisé en SHA1 pour l'authentification et en AES128 pour la communication

Net-snmp-config –create-snmpv3-user -ro -a SHA-1 -A "myauthphrase" -x AES -X myprivphrase authPrivUser

Remise en route du service snmpd après la création de notre user

```
sudo service snmpd start
```

Sur chaque équipement d'interconnexion :

1. Crée le groupe de sécurité V3

```
snmp-server group zabbix v3 priv
```

2. Crée l'utilisateur V3, ses mots de passe et les protocoles

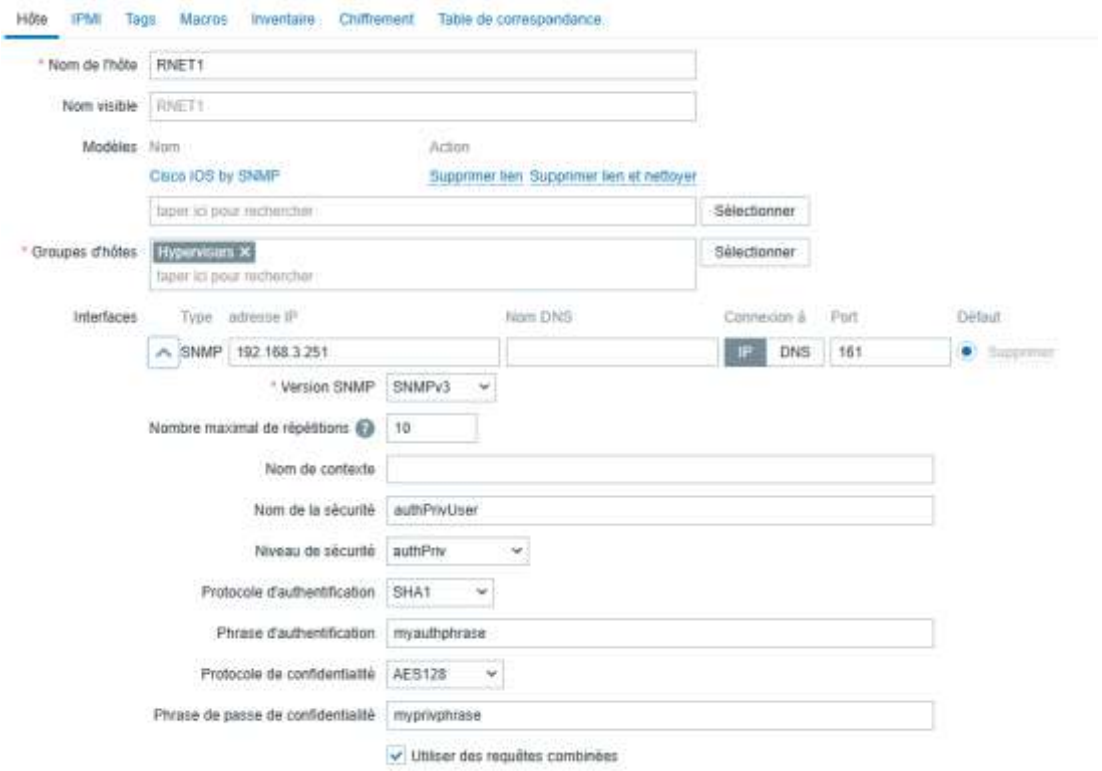
snmp-server user authPrivUser zabbix v3 auth sha myauthphrase priv aes 128 myprivphrase

3. Configure l'envoi des Traps (notifications) V3 vers le serveur Zabbix (172.16.100.5)

```
snmp-server host 172.16.100.5 version 3 priv authPrivUser
```

Sur l'interface Web de Zabbix :

On renseigne pour chaque équipement son nom, son IP, le port utilisé pour le snmp (161), la version SNMPv3 pour la sécurité, notre Utilisateur (authPrivUser), son mot de passe (myauthphrase) et les protocoles de sécurité utilisés

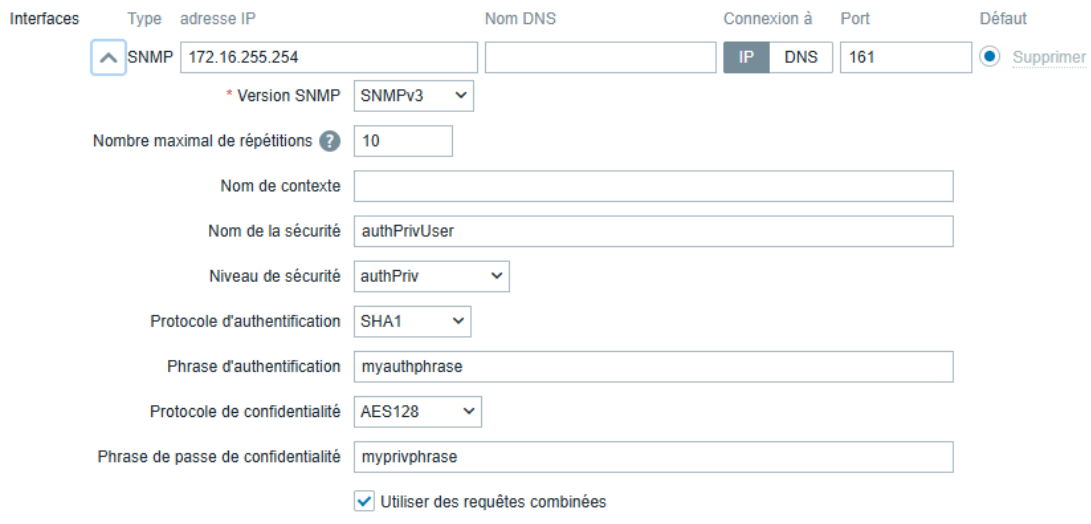


Sur le zyxel :

Créer un utilisateur dans les Objets/Users du Zyxel pour l'authentification sur le serveur SNMPv3

Activation du SNMP, activation de la version 3 et choix de l'utilisateur et des protocoles de sécurité pour l'authentification et la communication

Et enfin, on ajoute le zyxel au serveur zabbix sur l'interface web

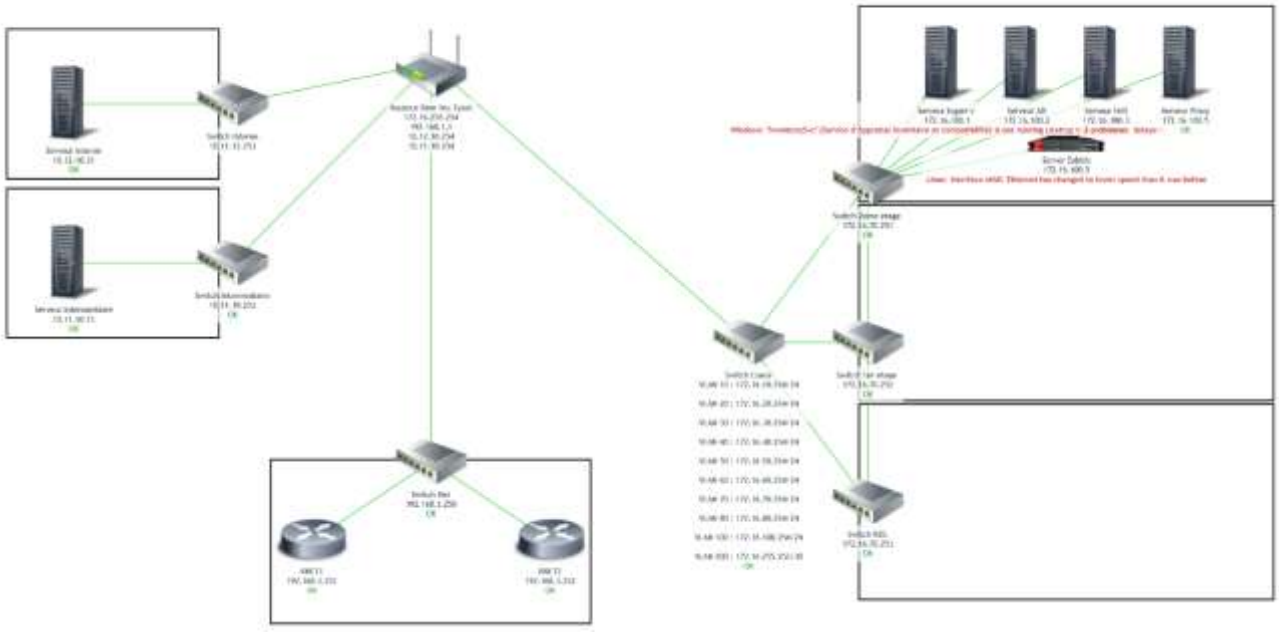


6. Sécurisation des flux réseau

Pour sécuriser les flux, il faut d'abord identifier tous ceux qui utilisent le protocole SNMP afin de les migrer vers SNMPv3, puis répéter la procédure expliquée ci-dessus.

Equipement en SNMP
Switch 2eme étage
Switch 1er étage
Switch RC
Switch Coeur
Zyxel
Switch Intermédiaire
Switch Interne
Switch Net
Routeur 1
Routeur 2

7. Création de la vue d'ensemble de l'infrastructure

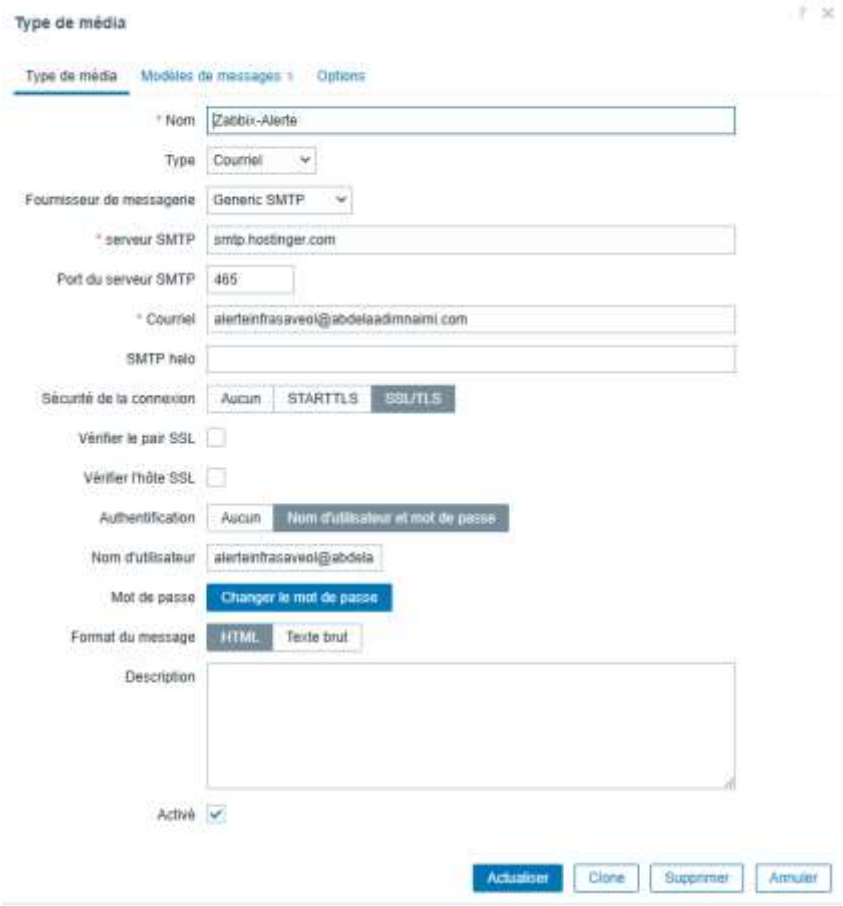


8. Configuration des alertes et notifications

Sur le serveur Zabbix :

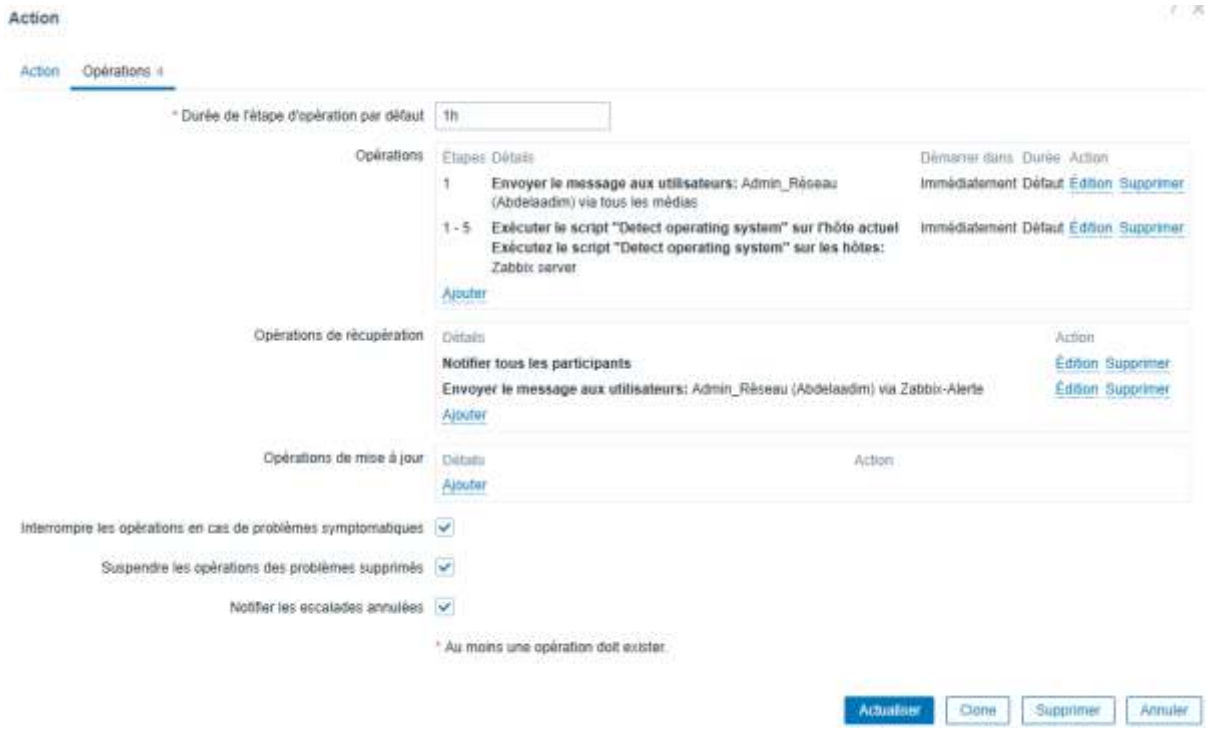
On configure 2 utilisateurs

Création d'un type de média pour que notre serveur Zabbix puisse nous envoyer les mails d'alerte depuis l'adresse qu'on lui a créé « alerteinfrasaveol@abdelaadimnaimi.com »



Création de 2 actions de déclencheur, « Report problèmes Réseau » pour signaler les alertes concernant les équipements d'interconnexion (Switchs, Routeurs, etc.) et « Report problèmes Système » pour signaler les alertes concernant les serveurs

Paramétrage de l'action de déclencheur pour envoyer les alertes à l'administrateur réseau « Abdelaadim »



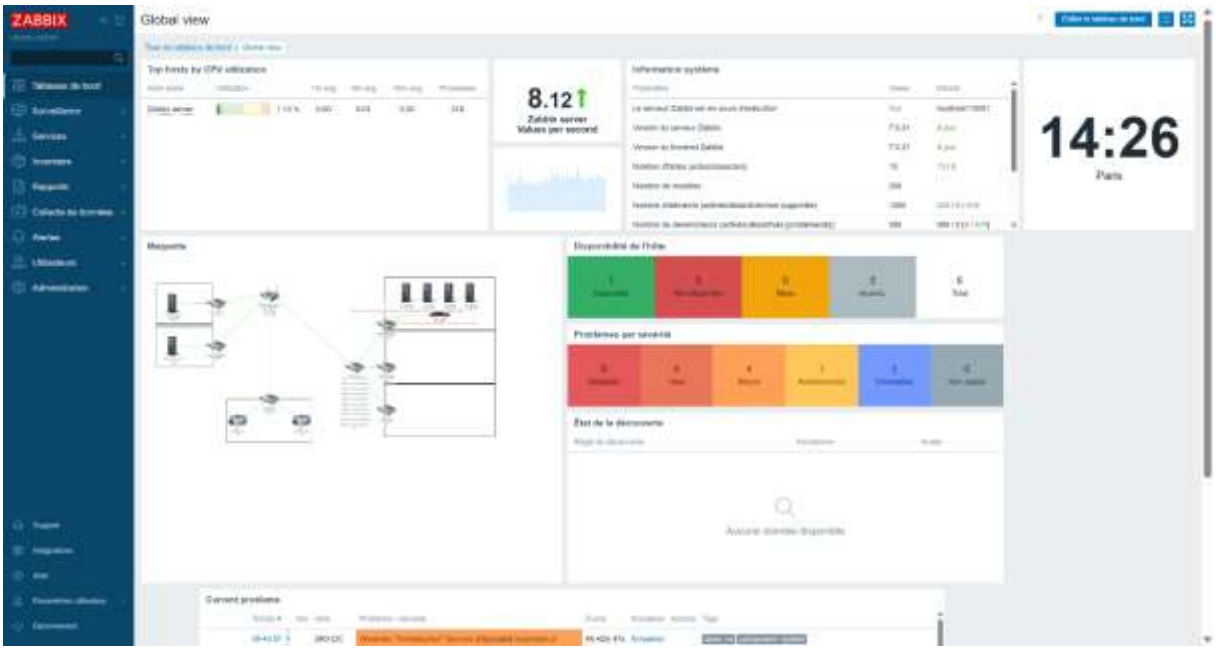
Paramétrage de l'action de déclencheur pour envoyer les alertes à l'administrateur système « Cyprien »

9. Production de la documentation projet

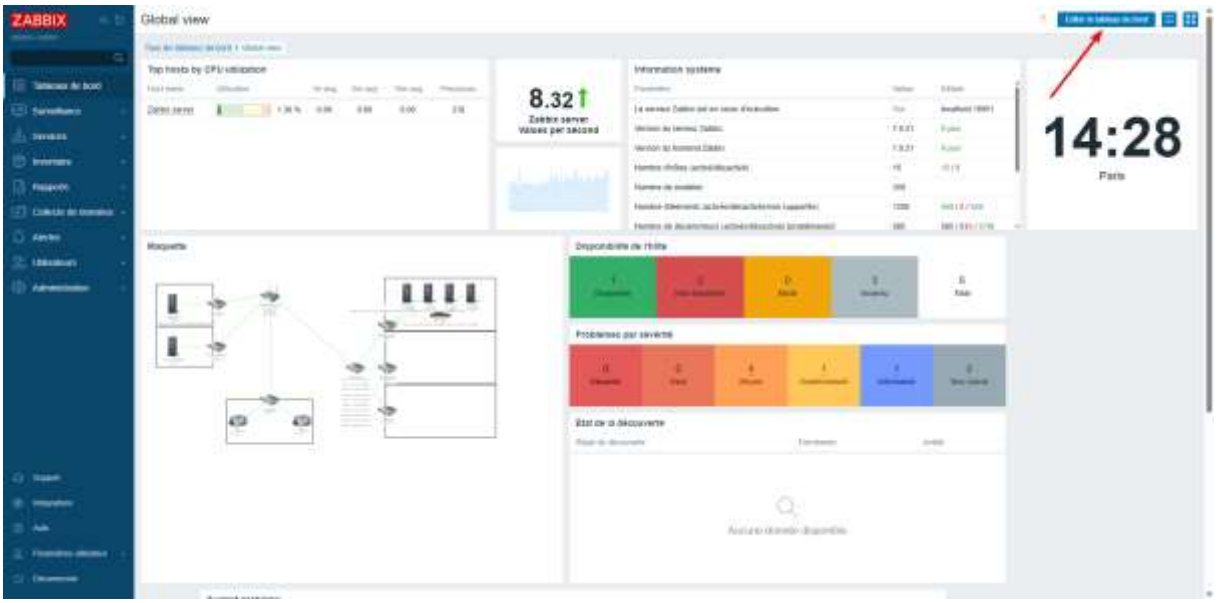
Documentation utilisation Zabbix

Création et /ou modification du tableau de bord

Vous arriverez en premier temp sur cette page elle est modifiable a votre guise

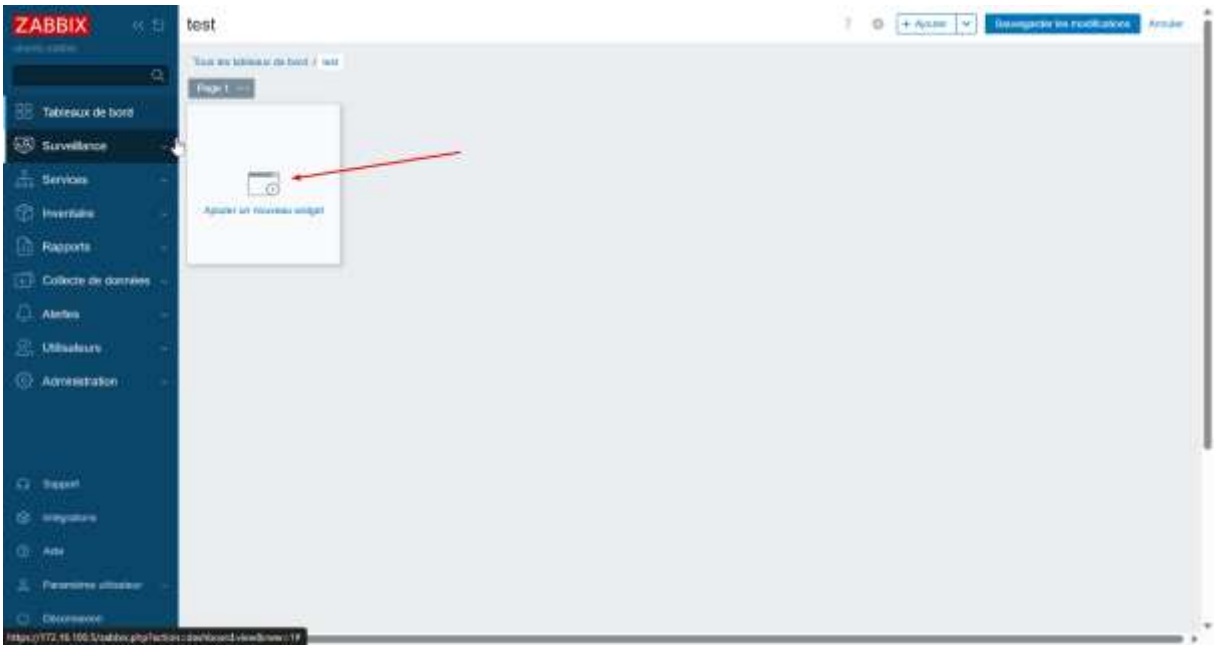


Pour la modifier il faut cliquer sur éditer le tableau de bord

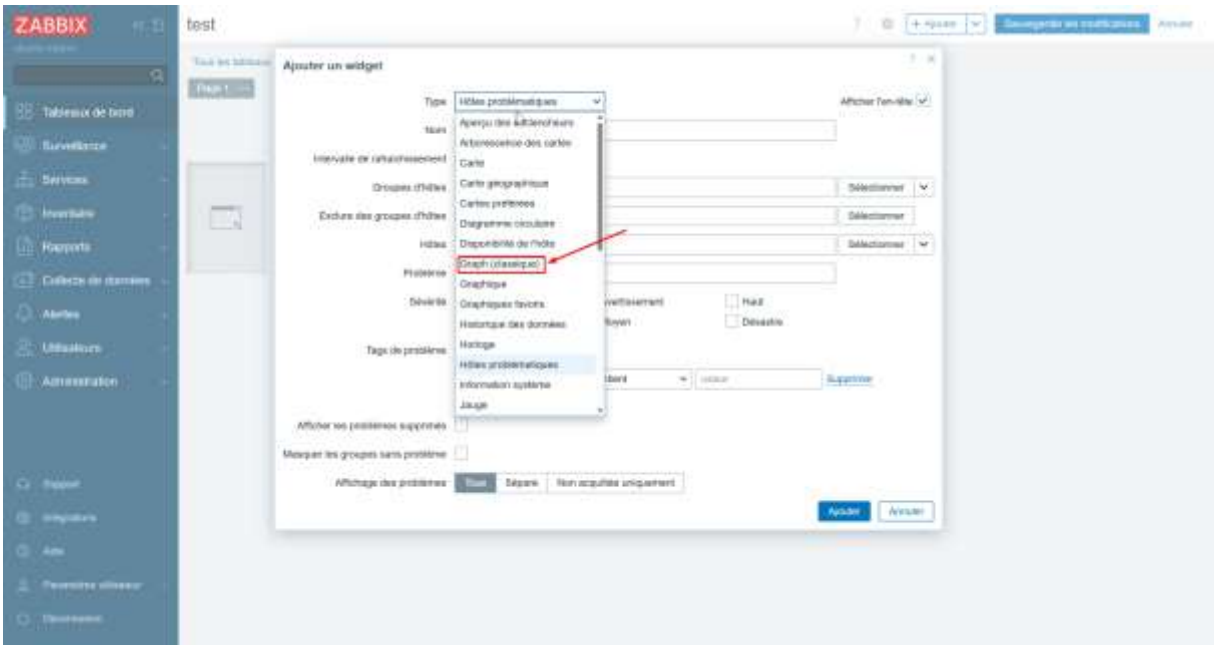


Si vous souhaiter supprimer une case il faut cliquer sur les trois petits points en haut a droite puis cliquer sur supprimer

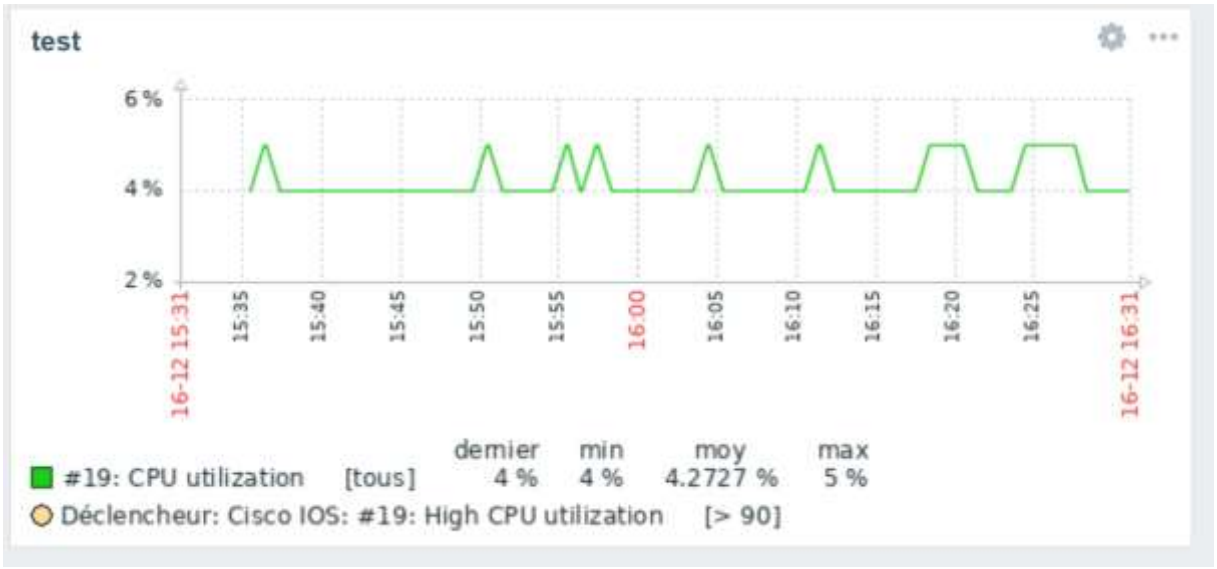
Si vous voulez ajouter un tableau ou une information si vous passer votre souris sur un endroit vide du tableau



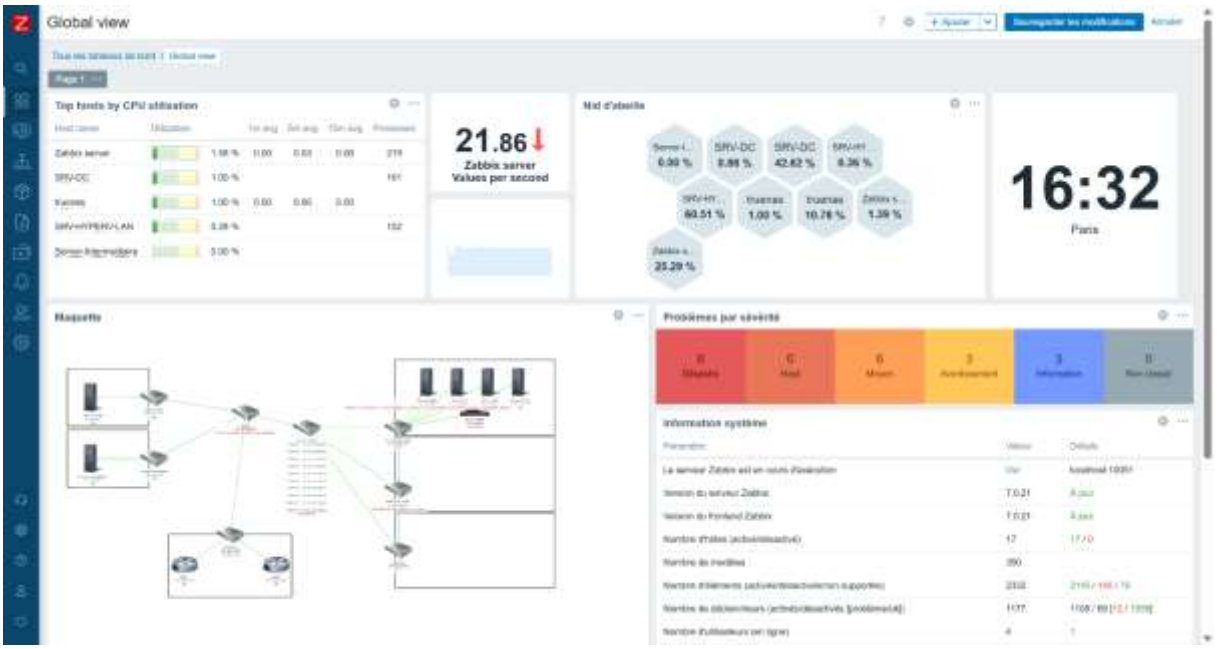
Sélectionner ce que vous voulez pour ma part j'ai choisi un graphique



Et voila vous avez le graphique



Voici un exemple de configuration de l'interface Zabbix



Installation de l'agent

Pour Linux

Installation de l'agent sur un linux classique

```
#Récupération du repo et décompresser le repo que vous venez d'installer
wget https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest_7.0+ubuntu24.04_all.deb
dpkg -i zabbix-release_latest_7.0+ubuntu24.04_all.deb

#Mise à jour des paquets et installation de l'agent
apt update
apt install zabbix-agent
```

Générer la PSK dans un fichier

```
root@srvweb:/home/srv_web# mkdir /home/zabbix
root@srvweb:/home/srv_web# cd /home/zabbix/
root@srvweb:/home/zabbix# openssl rand -hex 128 > secret.psk
```

Configuration de l'agent

```
#Modification du fichier de conf de l'agent
nano /etc/zabbix/zabbix_agentd.conf
```

Modifier ces lignes dans le fichier « Zabbix_agents.conf »

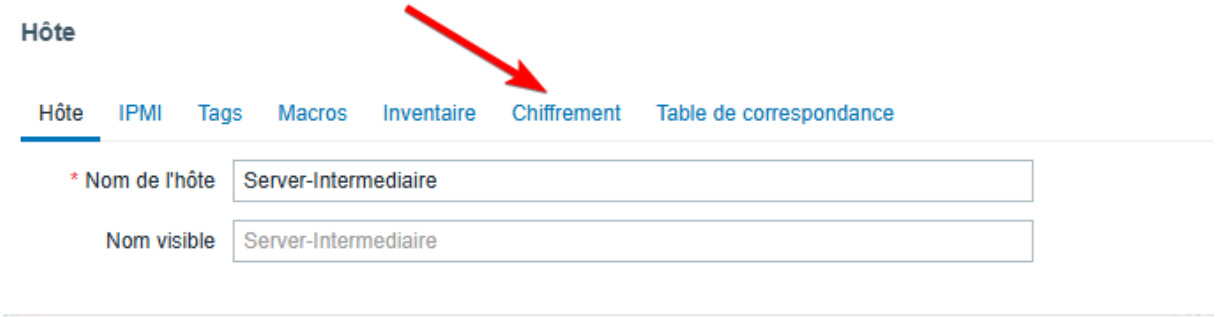
```
Server=172.16.100.5 (@IP du serveur zabbix)
ServerActive=172.16.100.5 (@IP du serveur zabbix)
Hostname=Server-Interne (Nom de l'agent configuré sur le serveur zabbix)

TLSConnect=psk
TLSAccept=psk
TLSPSKFile=/home/zabbix/secret.psk
TLSPSKIdentity=Server-Intermediaire
```

```
ServerActive=172.16.100.5

### Option: Hostname
#       List of comma delimited unique, case sensitive hostnames.
#       Required for active checks and must match hostnames as configured on th
#       Value is acquired from HostnameItem if undefined.
#
# Mandatory: no
# Default:
# Hostname=

Hostname=Server-Intermediaire
```

```
TLSConnect=psk
TLSAccept=psk
TLSPSKFile=/home/zabbix/secret.psk
TLSPSKIdentity=Server-Intermediaire
```

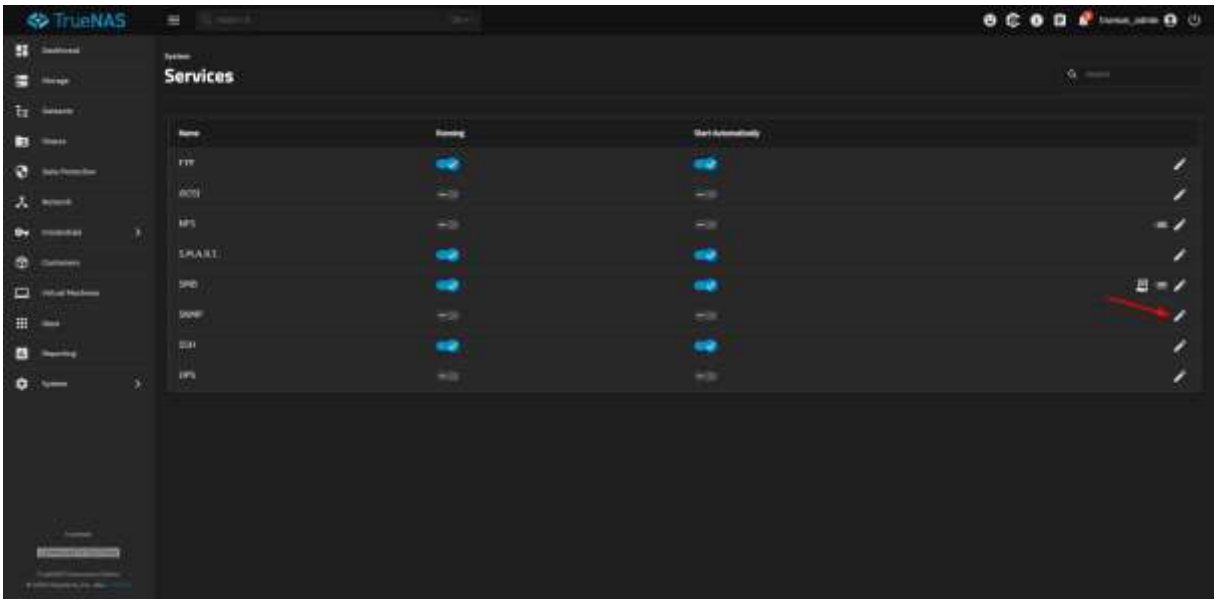
Puis redémarrer l'agent

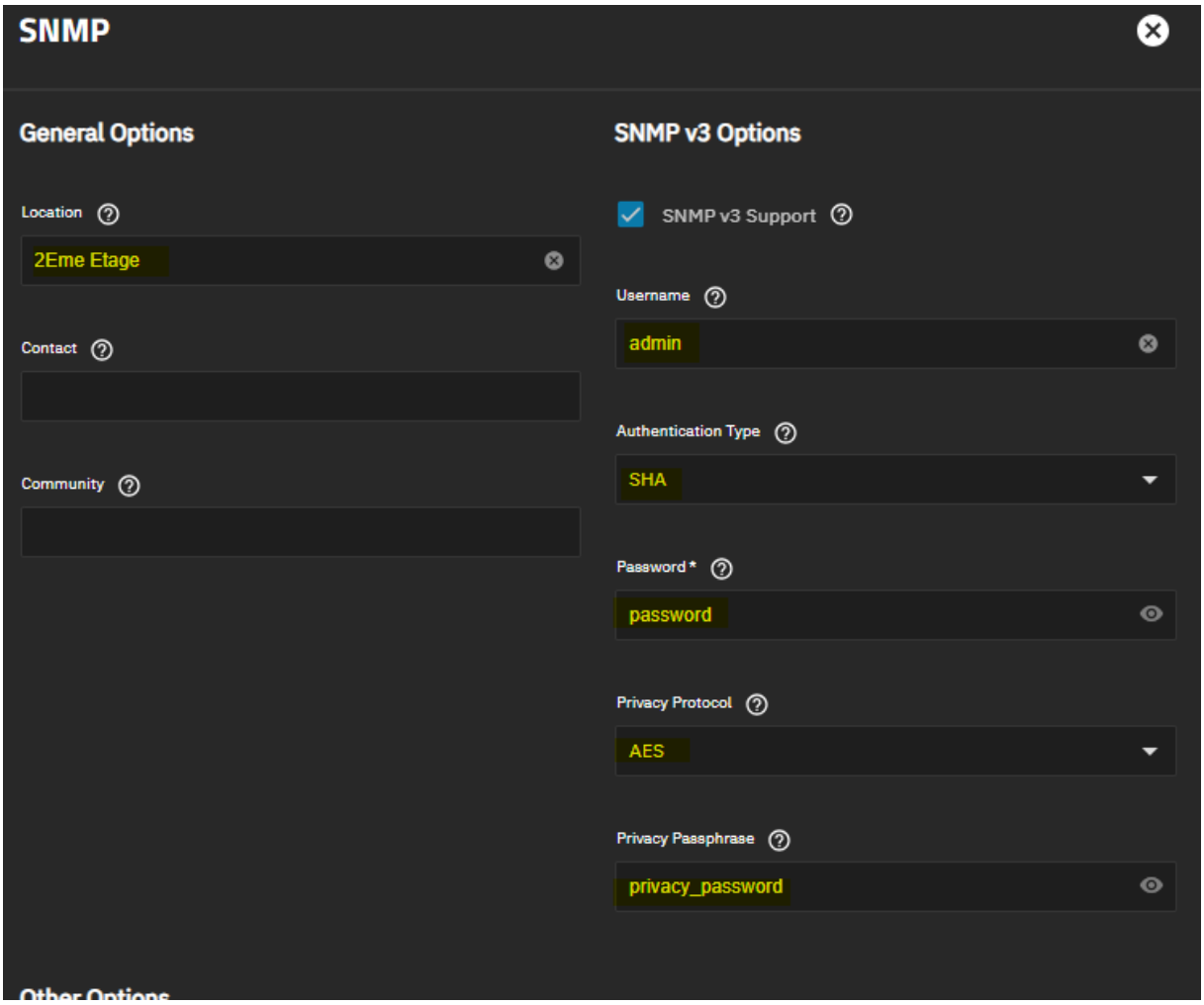
```
systemctl restart zabbix-agent
systemctl enable zabbix-agent
```



Installation de l'agent sur truenas

Modifier la configuration SNMP



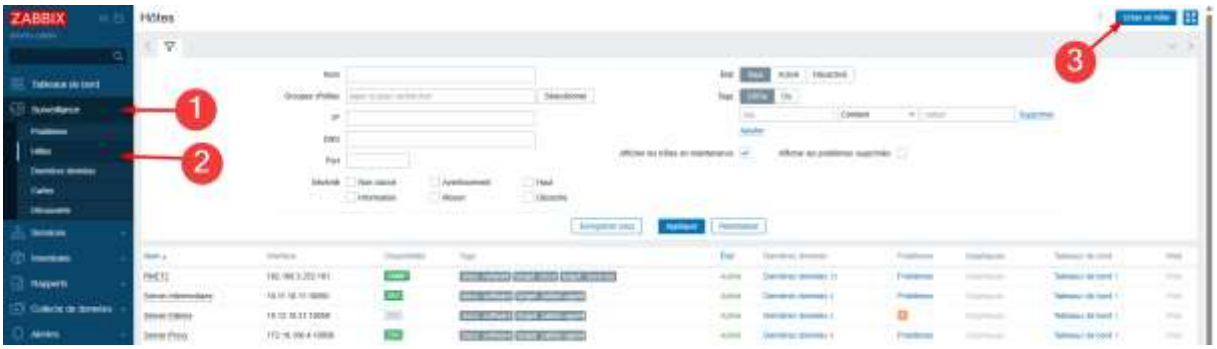


Activer le service SNMP et activer le démarrage automatique

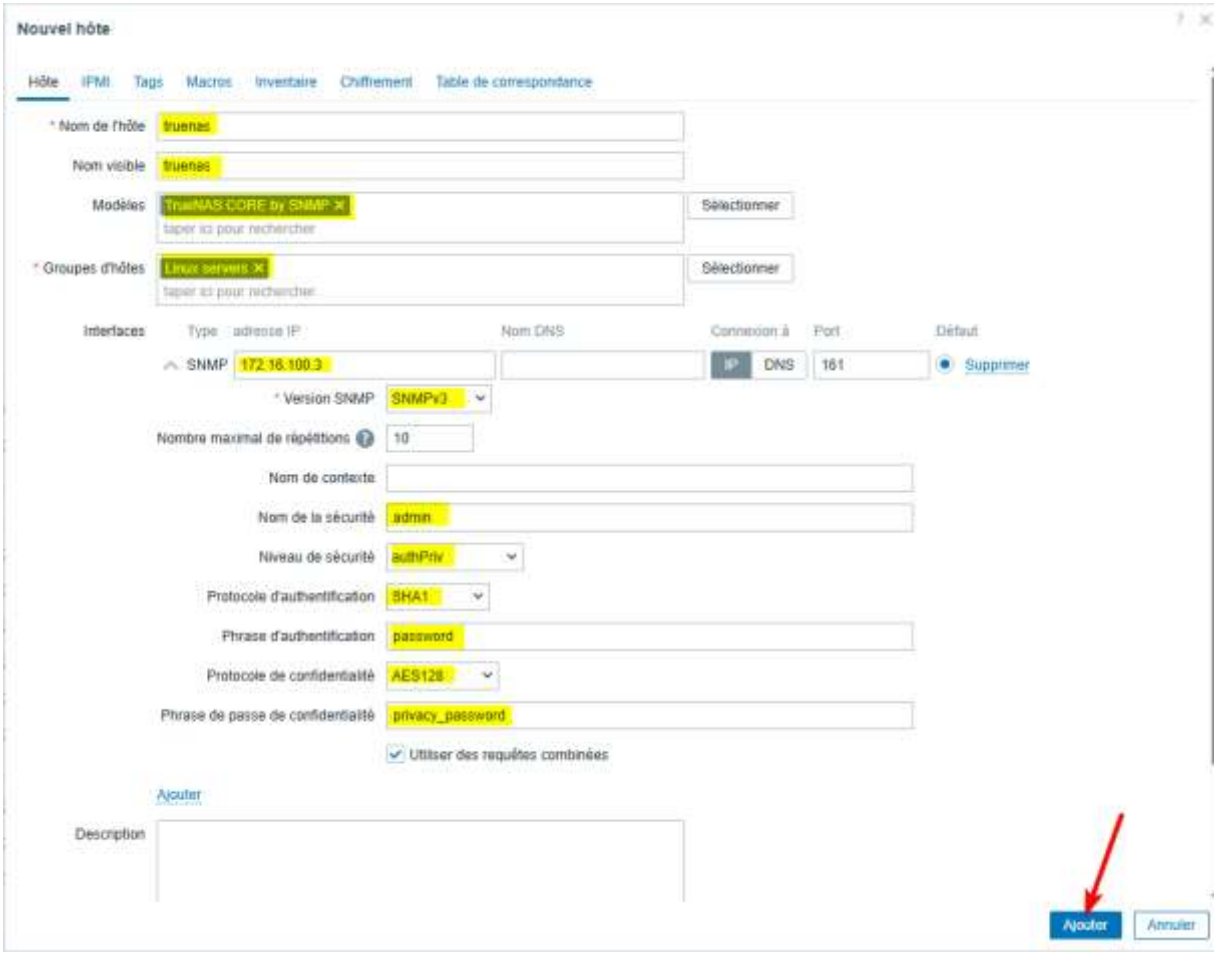
Installer le paquet pour activer le SNMP v3 et tester la connexion avec TrueNas

```
root@zabbix:/home/ubuntu-zabbix# apt install snmpd snmp libsnmp-dev -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
snmpd est déjà la version la plus récente (5.9.4+dfsg-1.1ubuntu3.1).
snmpd passé en « installé manuellement ».
libsnmp-dev est déjà la version la plus récente (5.9.4+dfsg-1.1ubuntu3.1).
Les NOUVEAUX paquets suivants seront installés :
  snmp
0 mis à jour, 1 nouvellement installés, 0 à enlever et 14 non mis à jour.
Il est nécessaire de prendre 180 ko dans les archives.
Après cette opération, 729 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 snmp amd64 5.9.4+dfsg-1.1ubuntu3.1 [180 kB]
180 ko réceptionnés en 0s (1 392 ko/s)
Sélection du paquet snmp précédemment désélectionné.
(Lecture de la base de données... 138585 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../snmp_5.9.4+dfsg-1.1ubuntu3.1_amd64.deb ...
Dépaquetage de snmp (5.9.4+dfsg-1.1ubuntu3.1) ...
Paramétrage de snmp (5.9.4+dfsg-1.1ubuntu3.1) ...
Traitement des actions différées (« triggers ») pour man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@zabbix:/home/ubuntu-zabbix# snmpwalk -v3 -a SHA -A password -x AES -X privacy_password -l authPriv -u admin 172.16.100.3 | head -10
iso.3.6.1.2.1.1.1.0 = STRING: "TrueNAS-25.04.2.4. Hardware: x86_64 Intel(R) Xeon(R) E-2124 CPU @ 3.30GHz. Software: Linux 6.12.15-production+truen
as (revision #1 SMP PREEMPT_DYNAMIC Mon Sep  8 18:50:34 UTC 2025)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.50536.3.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (43597) 0:07:15.97
iso.3.6.1.2.1.1.4.0 = STRING: "unknown@localhost"
iso.3.6.1.2.1.1.5.0 = STRING: "truenas"
iso.3.6.1.2.1.1.6.0 = STRING: "2Eme Etage"
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
root@zabbix:/home/ubuntu-zabbix#
```

Création de l’hôte sur Zabbix

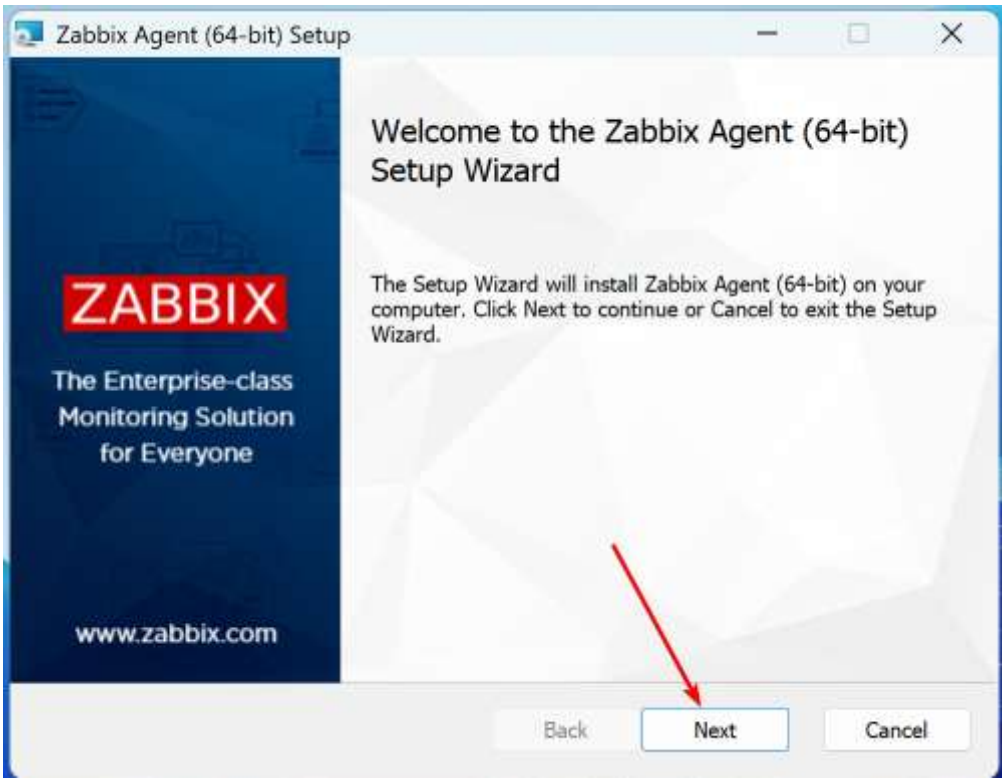


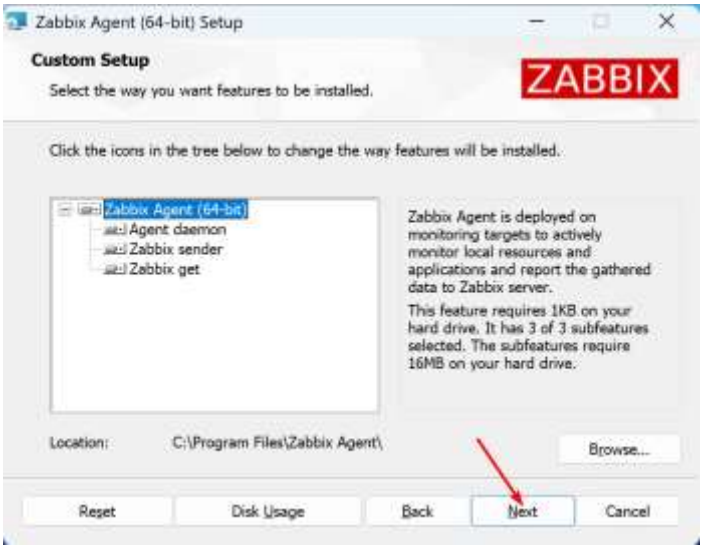
Insérer les informations comme dans la capture d’écran ci-dessous :



Pour Windows

Installation de l'agent



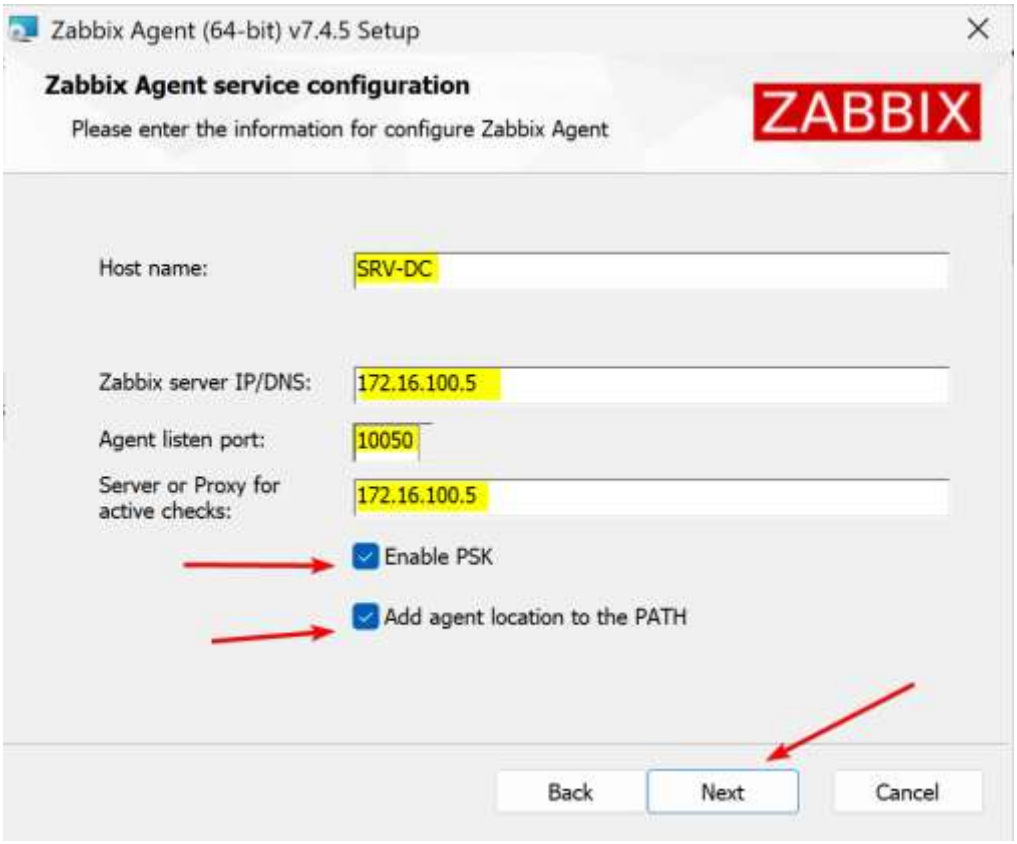


Remplissez les infos du serveur :

IP : 172.16.100.5

Port : 10050

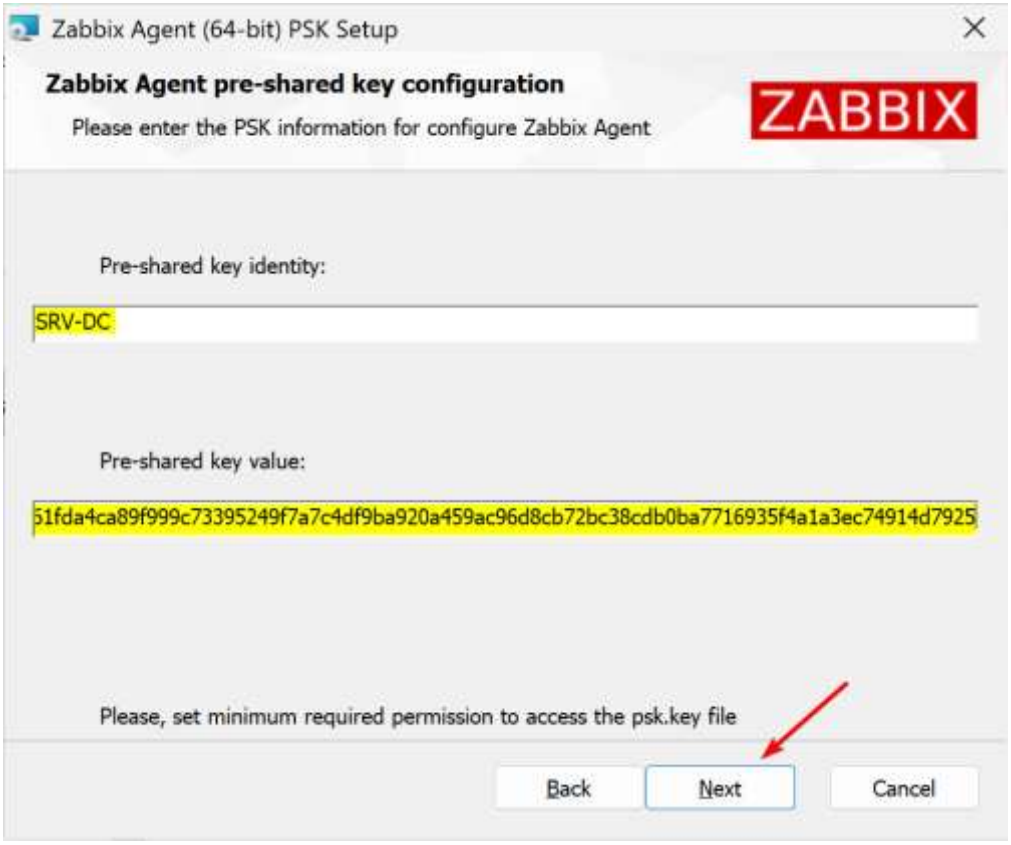
Et cocher les cases suivantes « enable PSK » et « add agent … »

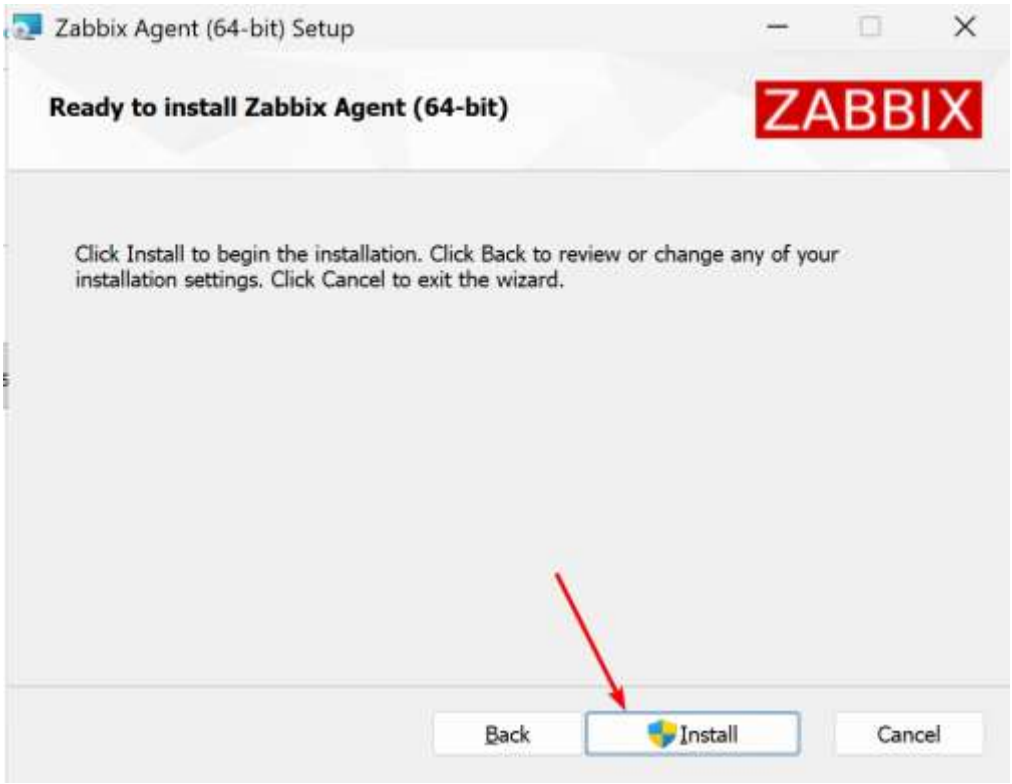


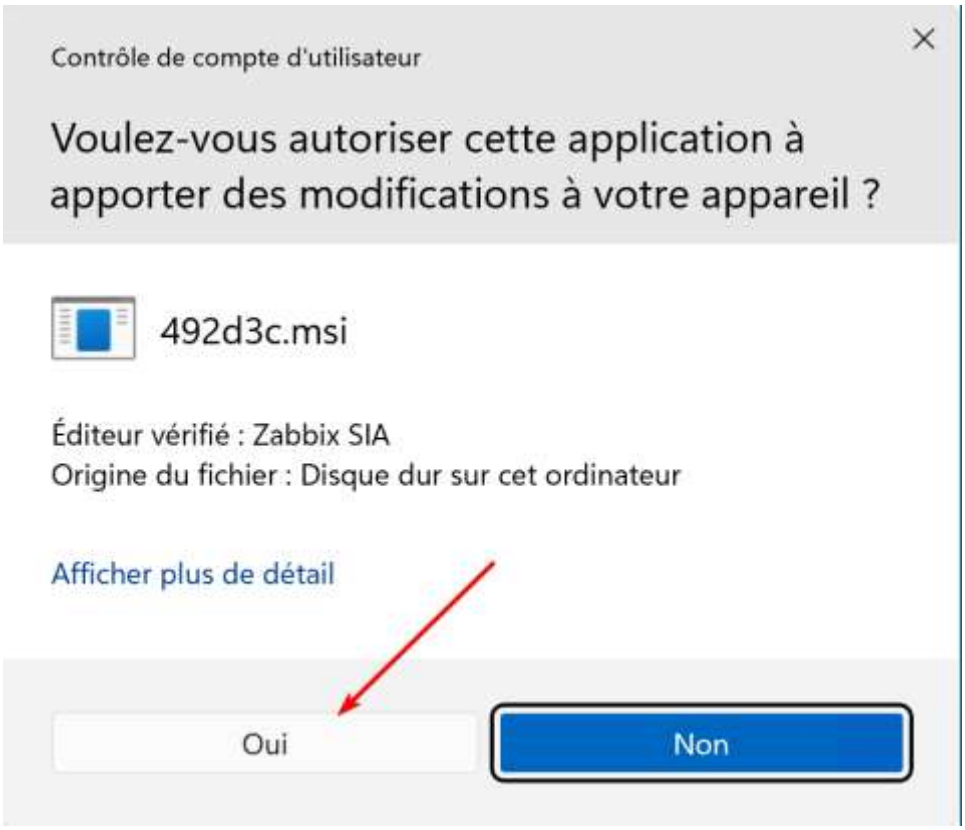
Puis générer une PSK de 128 caractères

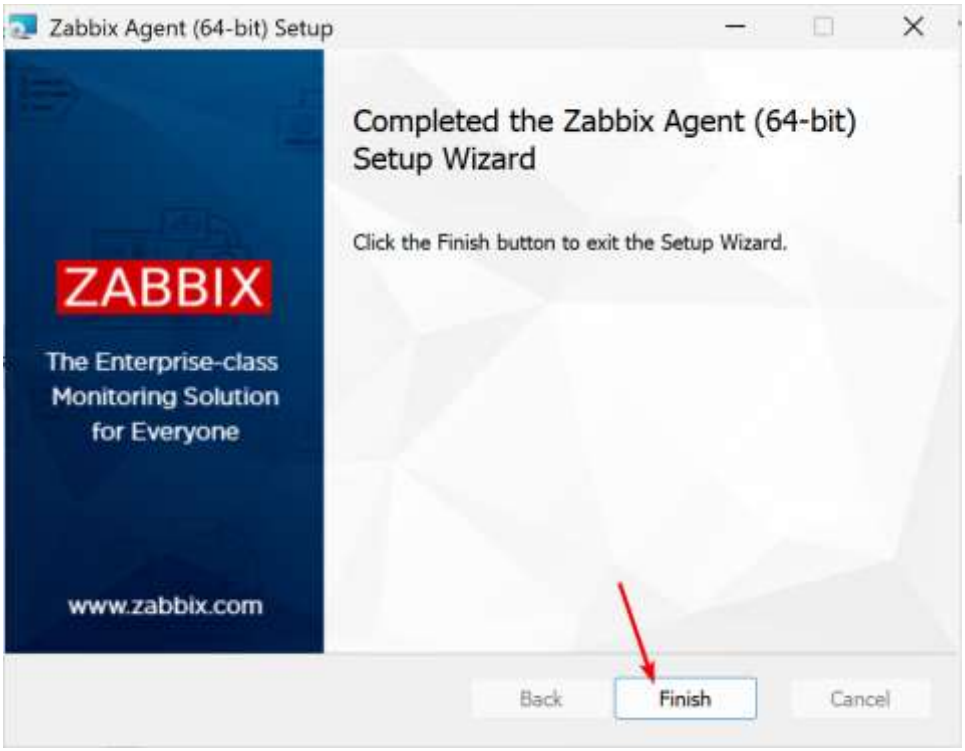
```
root@zabbix:/home/ubuntu-zabbix# openssl rand -hex 128
6eb720de4b148a31aab889df3779fd99687a626b47b284b7739befce888d971c107d4d2adb5376afd6eb0991f74ed908d1199b98f365fcab6577911f0
3aeec35754d06f0927ebcce458dcb6de64a1f19a96e77b8f456fda4b6baf6d2fe467b3749ecd0e87c870747a61ec7a56efe5c31cb10dd9
root@zabbix:/home/ubuntu-zabbix#
```

Et entrer l'ID et la PSK qui vient d'être générée

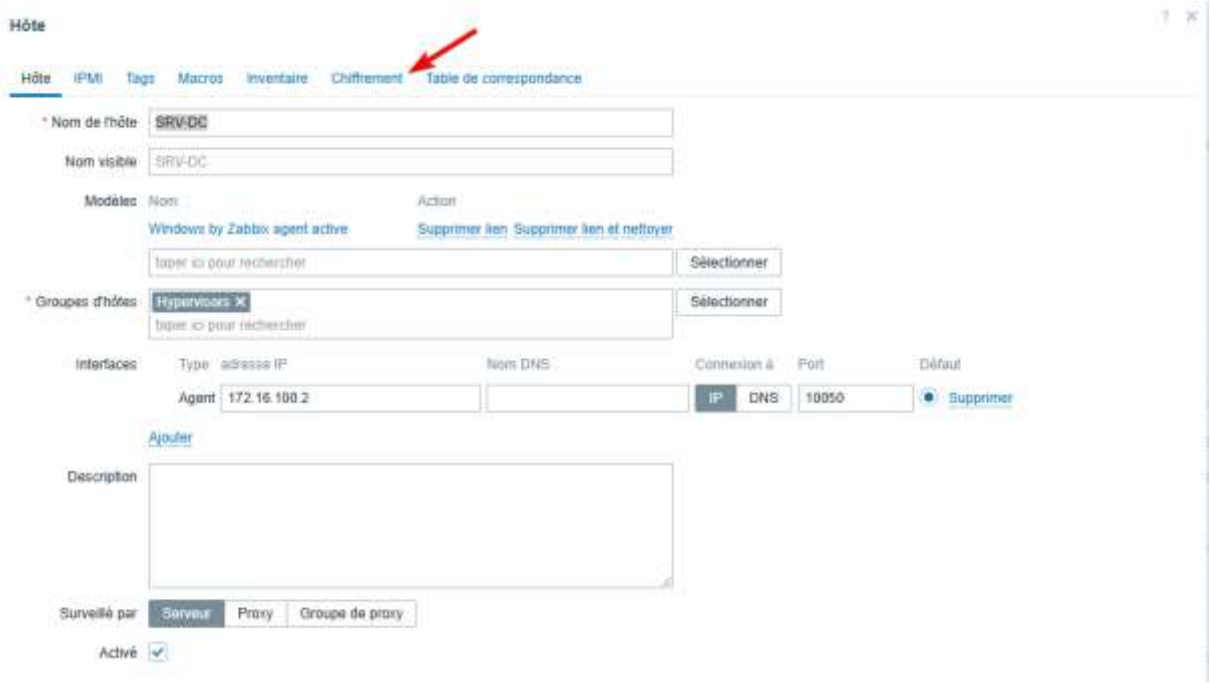

Zabbix Agent (64-bit) PSK Setup
Zabbix Agent pre-shared key configuration
Please enter the PSK information for configure Zabbix Agent
ZABBIX
Pre-shared key identity:
SRV-DC
Pre-shared key value:
61fda4ca89f999c73395249f7a7c4df9ba920a459ac96d8cb72bc38cdb0ba7716935f4a1a3ec74914d7925
Please, set minimum required permission to access the psk.key file
Back
Next
Cancel


Zabbix Agent (64-bit) Setup
Ready to install Zabbix Agent (64-bit)
ZABBIX
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel


Contrôle de compte d'utilisateur
Voulez-vous autoriser cette application à apporter des modifications à votre appareil ?
492d3c.msi
Éditeur vérifié : Zabbix SIA
Origine du fichier : Disque dur sur cet ordinateur
Afficher plus de détail
Oui
Non


Zabbix Agent (64-bit) Setup
ZABBIX
The Enterprise-class Monitoring Solution for Everyone
www.zabbix.com
Completed the Zabbix Agent (64-bit) Setup Wizard
Click the Finish button to exit the Setup Wizard.
Back
Finish
Cancel

Une fois cela fait il faut aller sur Zabbix sur l'hôte concerné donc « SRV-DC » et « SRV-HYPERV-LAN »



Aller dans chiffrement puis activer le PSK et entrer les informations configurées précédemment

Equipement d'interconnexion

1. Crée le groupe de sécurité V3

```
snmp-server group zabbix v3 priv
```

2. Crée l'utilisateur V3, ses mots de passe et les protocoles

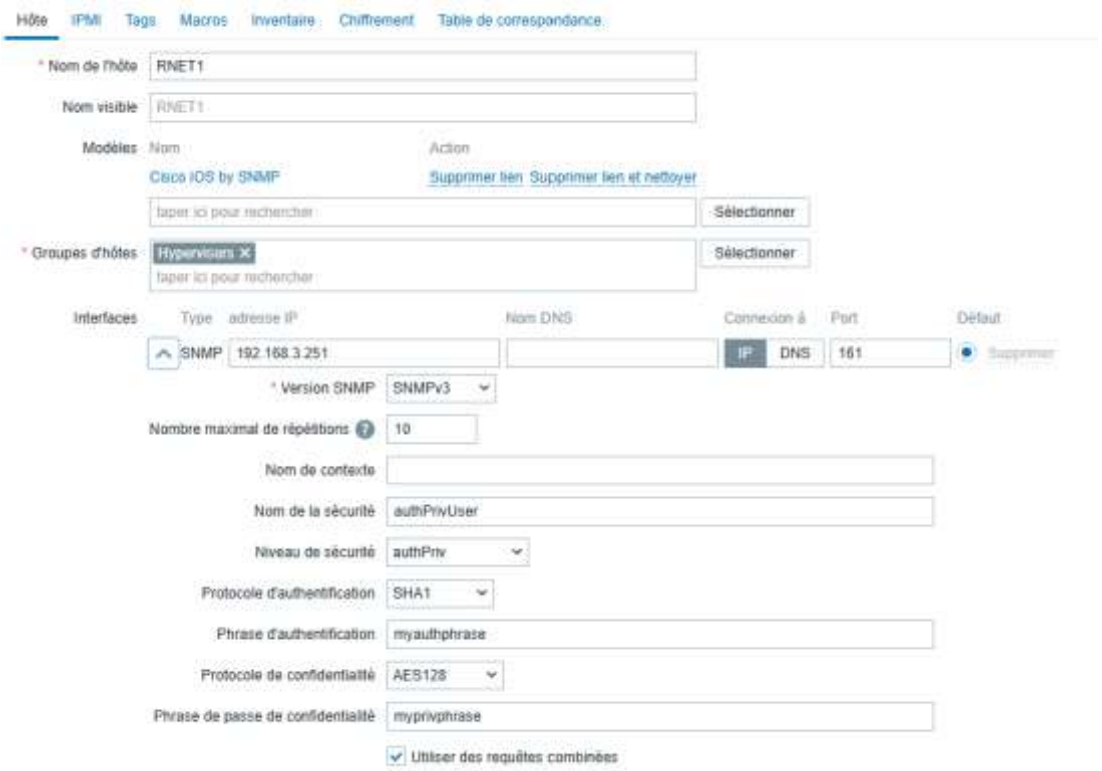
snmp-server user authPrivUser zabbix v3 auth sha myauthphrase priv aes 128 myprivphrase

3. Configure l'envoi des Traps (notifications) V3 vers le serveur Zabbix (172.16.100.5)

```
snmp-server host 172.16.100.5 version 3 priv authPrivUser
```

Sur l'interface Web de Zabbix :

On renseigne pour chaque équipement son nom, son IP, le port utilisé pour le snmp (161), la version SNMPv3 pour la sécurité, notre Utilisateur (authPrivUser), son mot de passe (myauthphrase) et les protocoles de sécurité utilisés

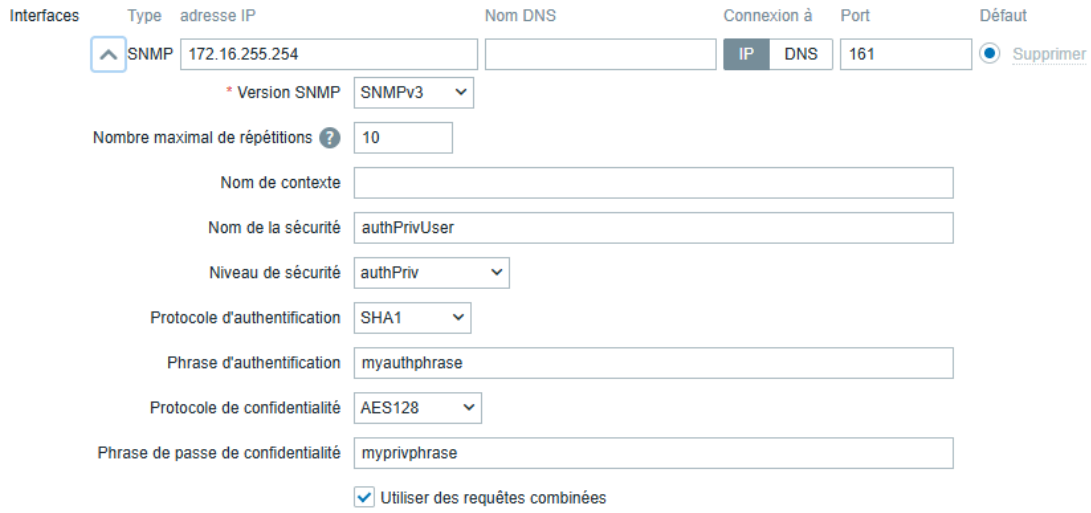


Sur le zyxel :

Créer un utilisateur dans les Objets/Users du Zyxel pour l'authentification sur le serveur SNMPv3

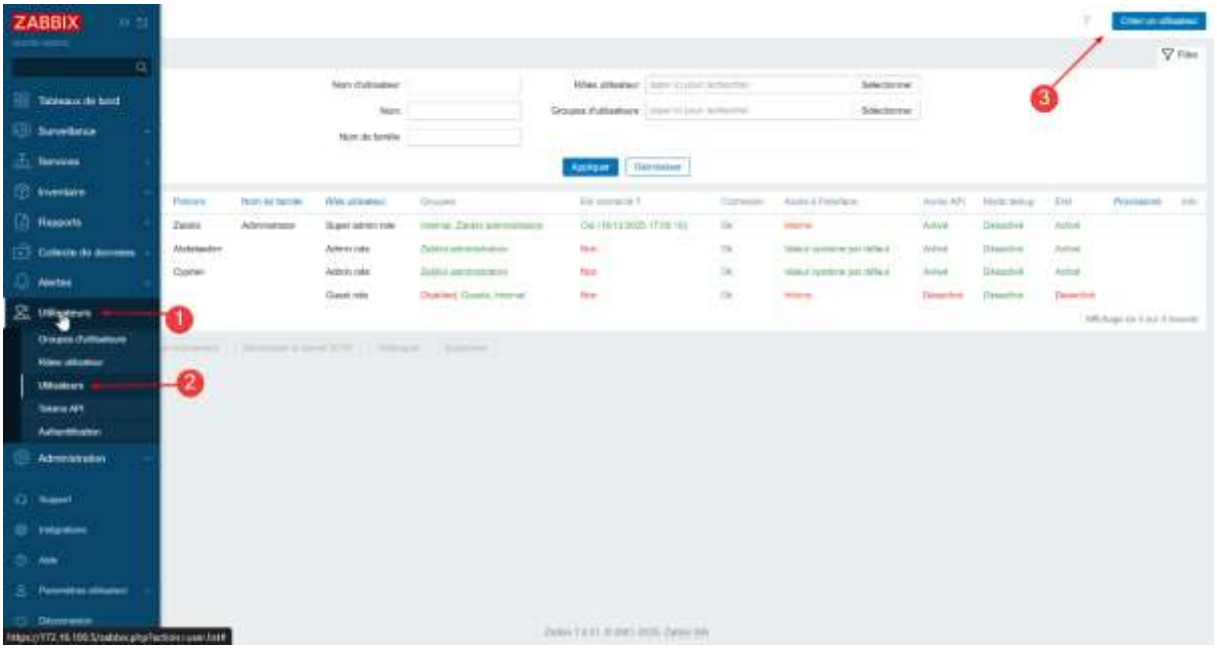
Activation du SNMP, activation de la version 3 et choix de l'utilisateur et des protocoles de sécurité pour l'authentification et la communication

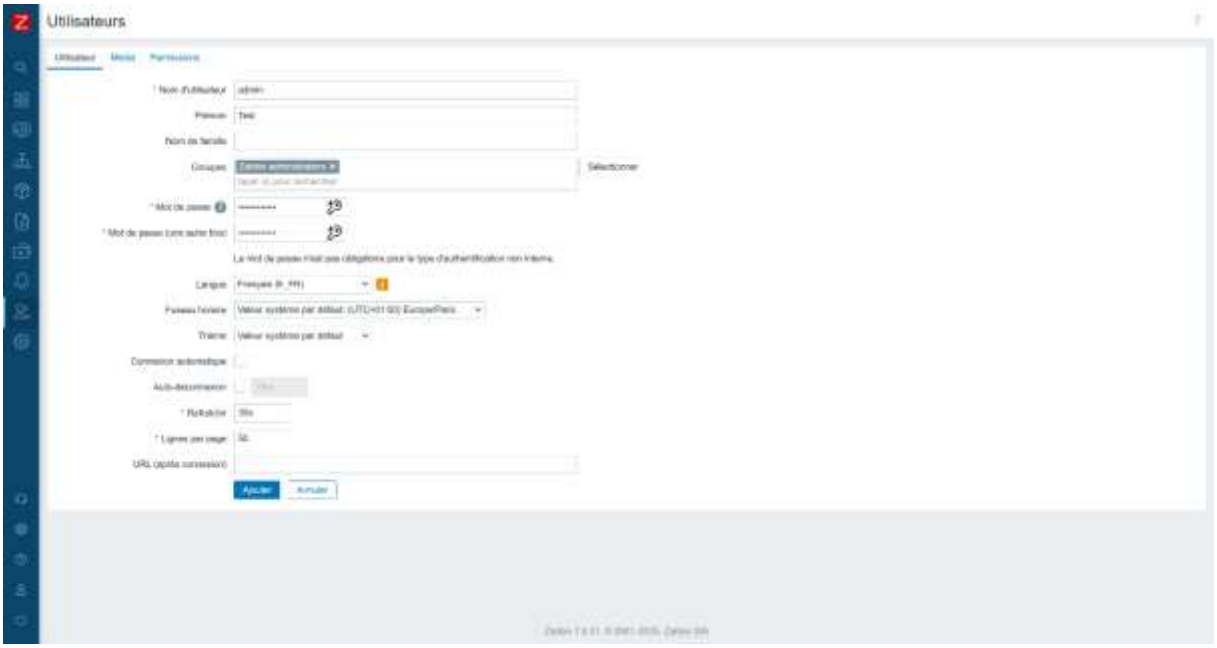
Et enfin, on ajoute le ZyXEL au serveur Zabbix sur l'interface web

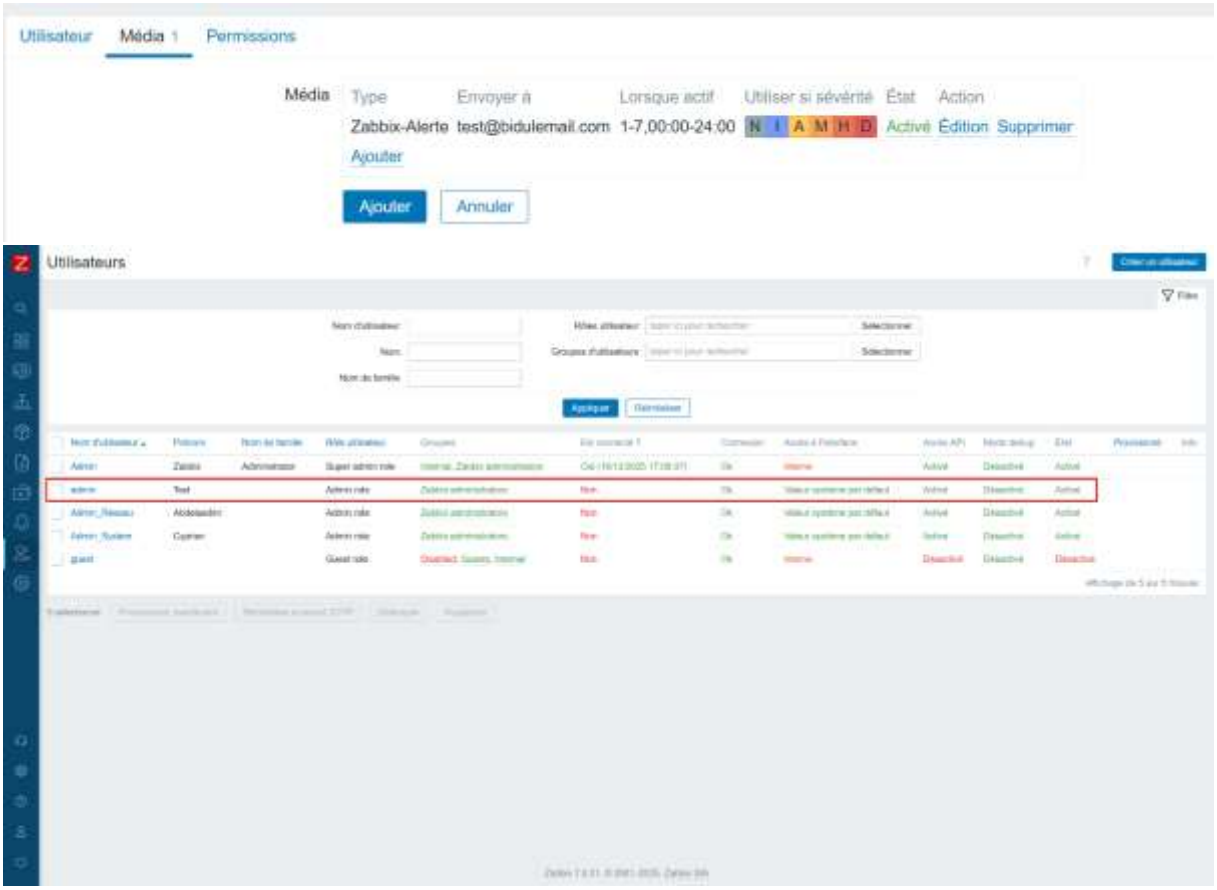


Mise en place des alertes

Création des user

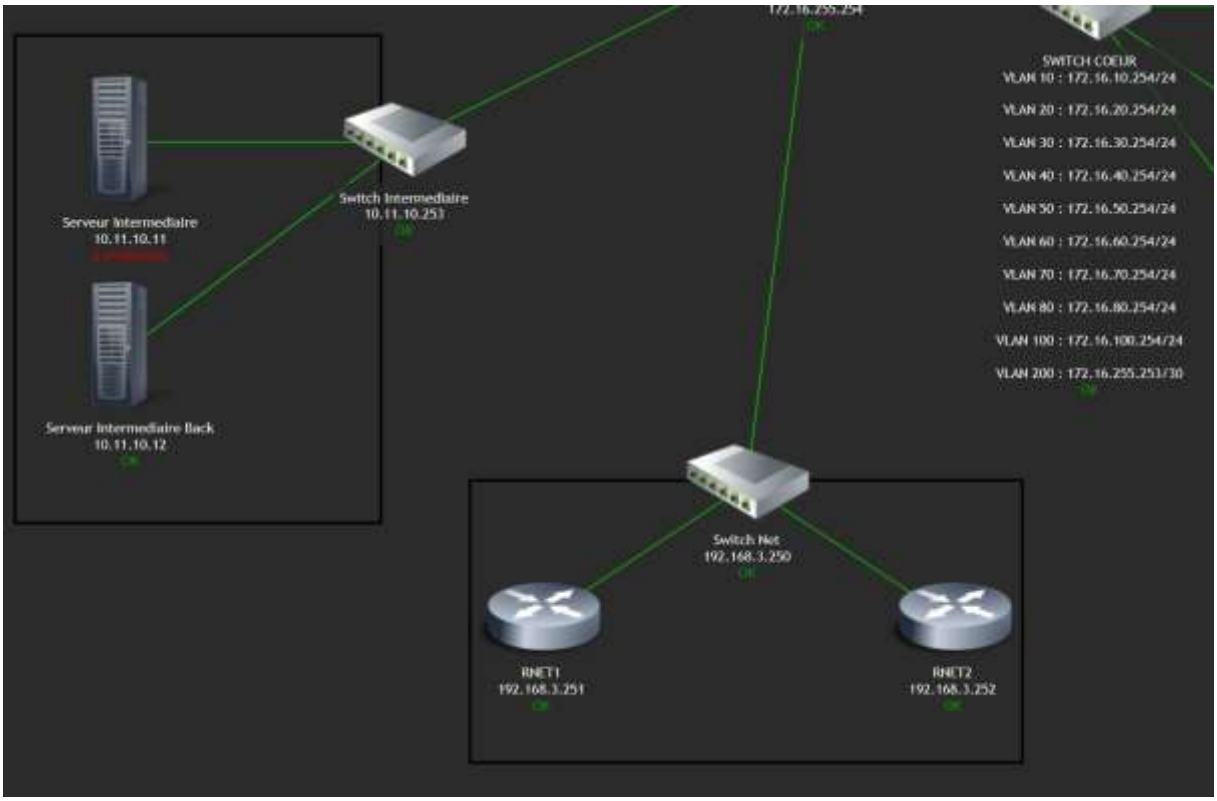






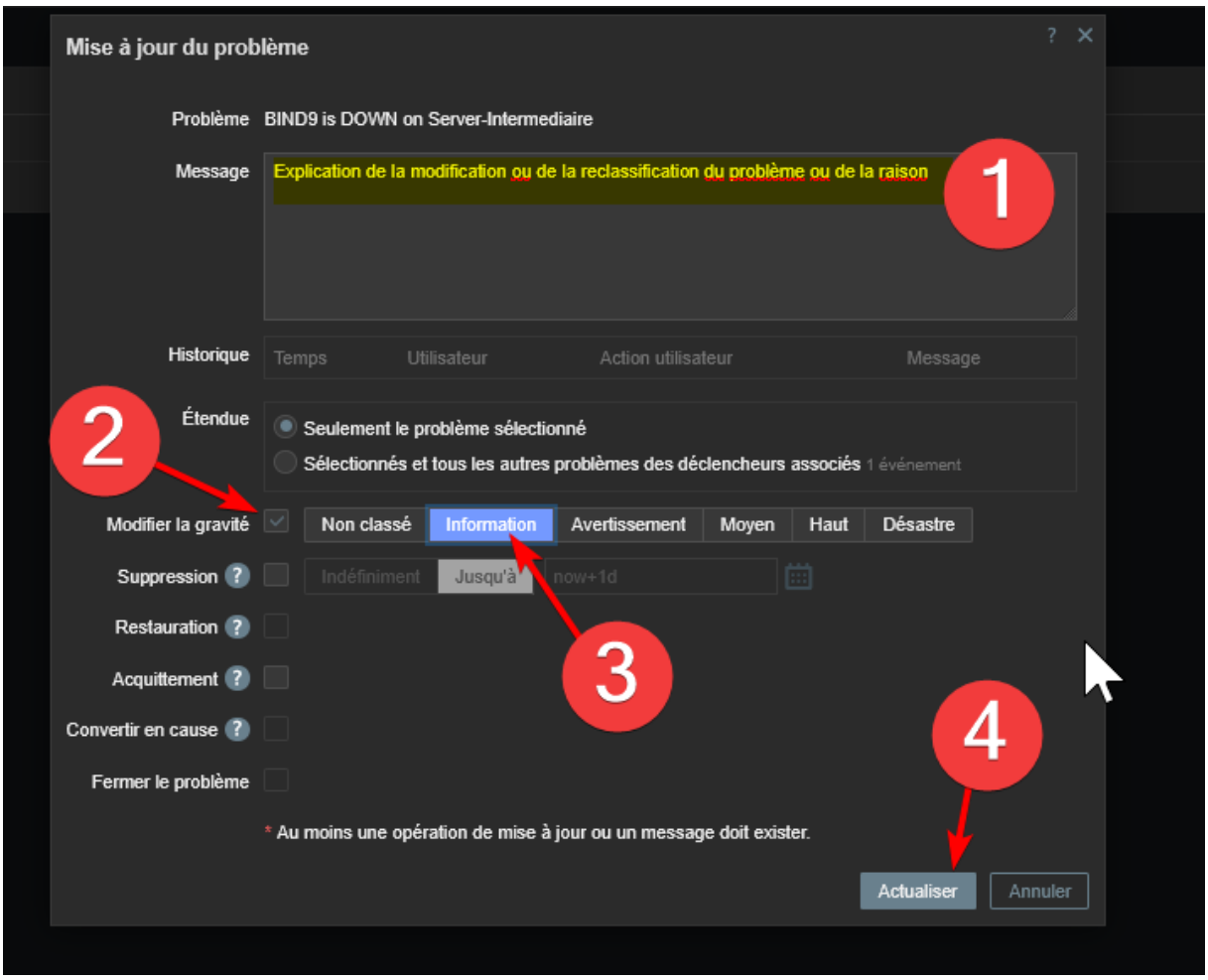
Prendre en charge une alerte :

Vous allez avoir une notification sur la carte :



Via l'hôte :

Pour expliquer ou modifier le problème cliquer dessus-> Actualiser->(voir screen)



Ou alors via un mail :


Problem: BIND9 is DOWN on Server-Intermediaire
From alert@cyprien-caron.fr
to me
Problem started at 13:16:02 on 2026.06.02
Problem name: BIND9 is DOWN on Server-Intermediaire
Host: Server-Intermediaire
Severity: High
Operational data: 0
Original problem ID: 4647