

Caron Cyprien

BTS SIO 2



## 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.

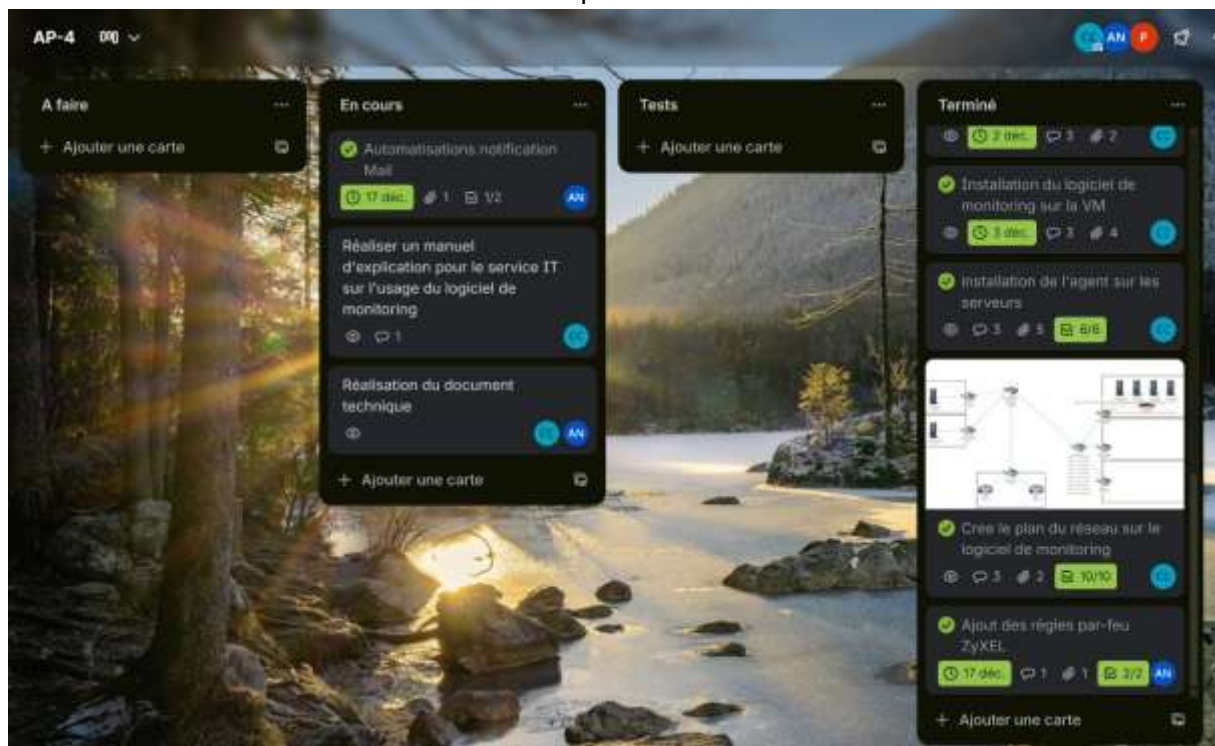
# 1. Organisation et planification du travail



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	Tarifcation 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.

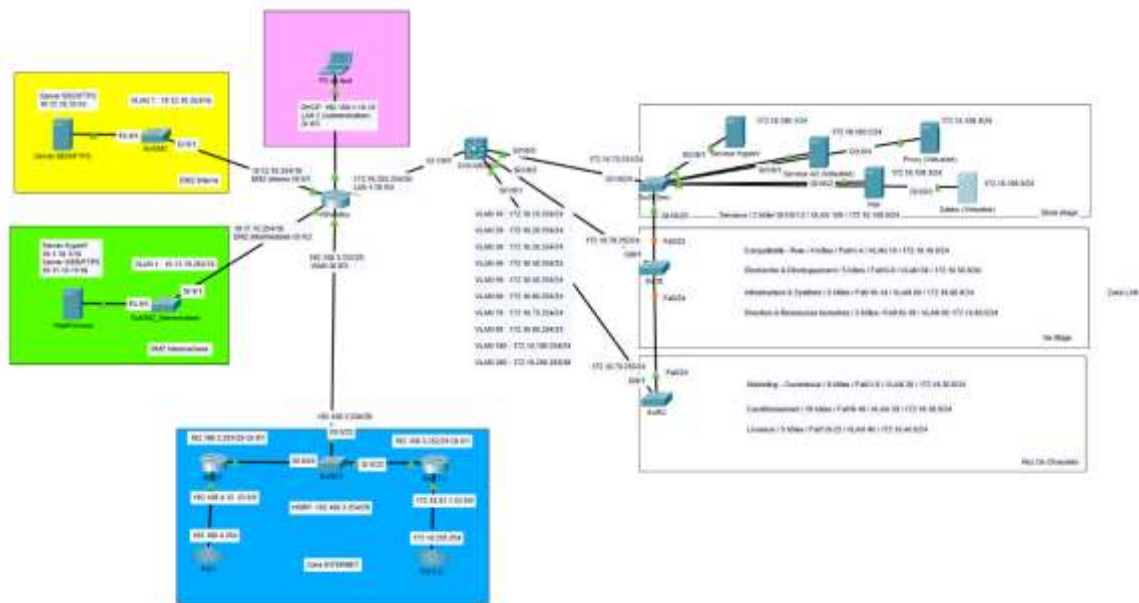
Inconvénients :

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](#) :

1 Choose your platform

ZABBIX VERSION	OS DISTRIBUTION	OS VERSION	ZABBIX COMPONENT	DATABASE	WEB SERVER
7.4	Alma Linux	24.04 (Hobbit)	Server, Frontend, Agent	MySQL	Apache
7.2	Amazon Linux	22.04 (Jammy)	Server, Frontend, Agent Z	PostgreSQL	Nginx
7.0-LTS	CentOS	20.04 (Focal)	Proxy		
6.0 LTS	Debian	18.04 (Bionic)	Agent		
8.0 PRE-RELEASE	Debian (arm64)	16.04 (Xenial)	Agent Z		
	OpenSUSE Leap		Java Gateway		
	Oracle Linux		Web Service		
	Raspberry Pi OS				
	Red Hat Enterprise Linux				

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

```
GNU nano 7.2 /etc/zabbix/zabbix_server.conf
# Schema name, used for PostgreSQL.
#
# Mandatory: no
# Default:
# DBSchema=
## Option: DBUser
# Database user.
#
# Mandatory: no
# Default:
# DBUser=
DBUser=zabbix
## Option: DBPassword
# Database password.
# Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=password
## Option: DBSocket
# Path to MySQL socket.
#
# Mandatory: no
# Default:
# DBSocket=
```

```
# 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
```

```
TLSCAccept=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 the
# Value is acquired from HostnameItem if undefined.
#
# Mandatory: no
# Default:
# Hostname=

Hostname=Server-Intermediaire
```

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

Puis redémarrer l'agent

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

## Hôte

Hôte IPMI Tags Macros Inventaire **Chiffrement** Table de correspondance

\* Nom de l'hôte Server-Intermediaire

Nom visible Server-Intermediaire

Hôte

Hôte IPMI Tags Macros Inventaire **Chiffrement** Table de correspondance

Connexion à l'hôte Pas de chiffrement **PSK** Certificat

Connexion de l'hôte  Pas de chiffrement  PSK  Certificat

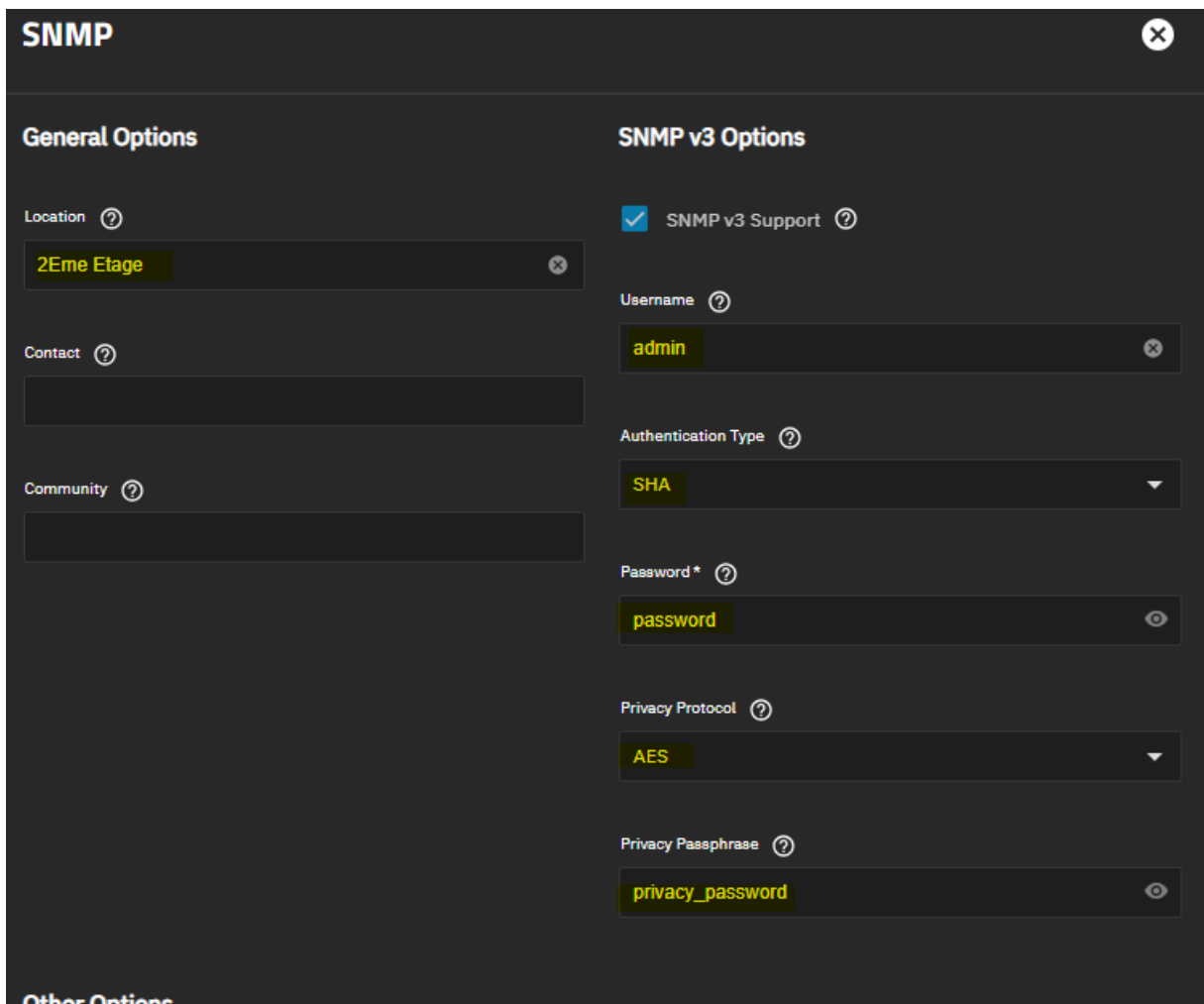
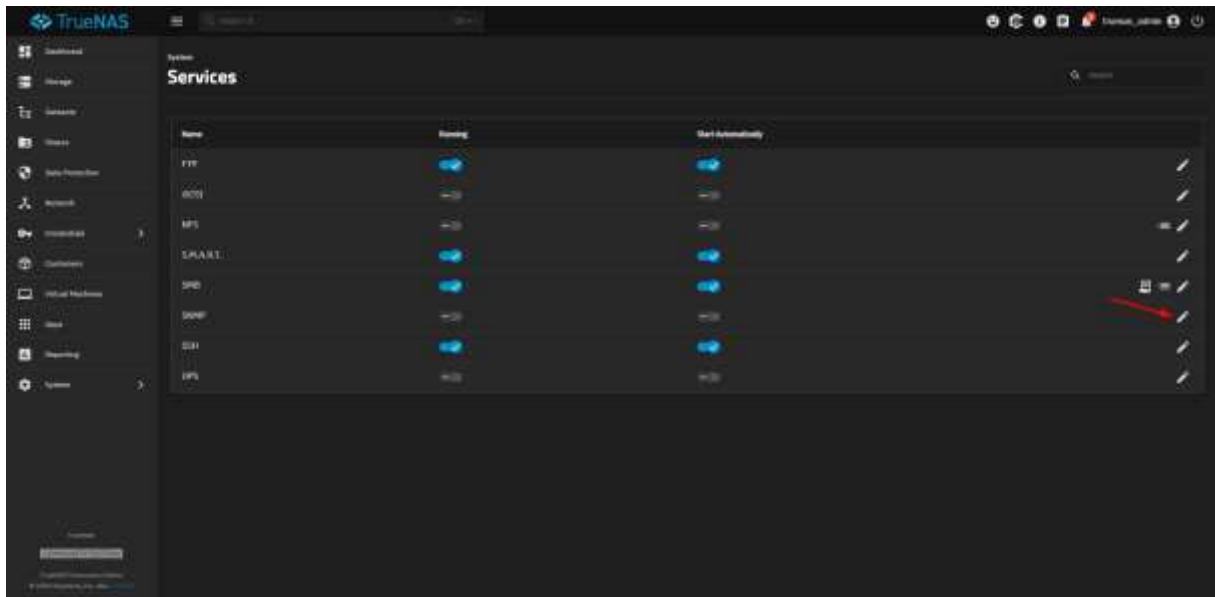
\* Identité PSK Server-Intermediaire

\* PSK 1eeef1205d17ee835f11228d9f858f5f29ccfbcd5f560a3cc88c71901d03586df34c9c407dbfdcae304e

Actualiser Clone Supprimer Annuler

*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 libsnp-dev -y 1
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 ».
libsnp-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.

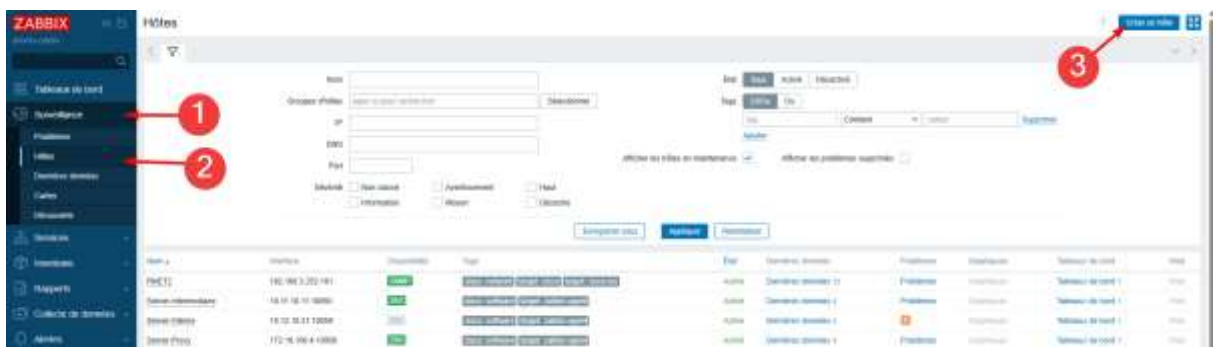
No containers need to be restarted.

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 -O SMI -A password -X AES -x privacy password -I authPriv -u admin 172.16.100.3 | head -10
as (revision #1 SMP PREEMPT_DYNAMIC Mon Sep  8 18:59:34 UTC 2025)
iso.3.6.1.2.1.1.1.2.0 = 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
iso.3.6.1.2.1.1.1.3.0 = OID: iso.3.6.1.4.1.58539.3.1
iso.3.6.1.2.1.1.1.4.0 = STRING: "unknown@localhost"
iso.3.6.1.2.1.1.3.0 = STRING: "truenas"
iso.3.6.1.2.1.1.6.0 = STRING: "2ème 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 :

Nouvel hôte

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

\* Nom de l'hôte:

Nom visible:

Modèles:  Sélectionner

\* Groupes d'hôtes:  Sélectionner

Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
SNMP		<input type="text" value="172.16.100.3"/>	<input type="text"/>	<input type="radio"/> IP	DNS	161

Version SNMP:

Nombre maximal de répétitions:

Nom de contexte:

Nom de la sécurité:

Niveau de sécurité:

Protocole d'authentification:

Phrase d'authentification:

Protocole de confidentialité:

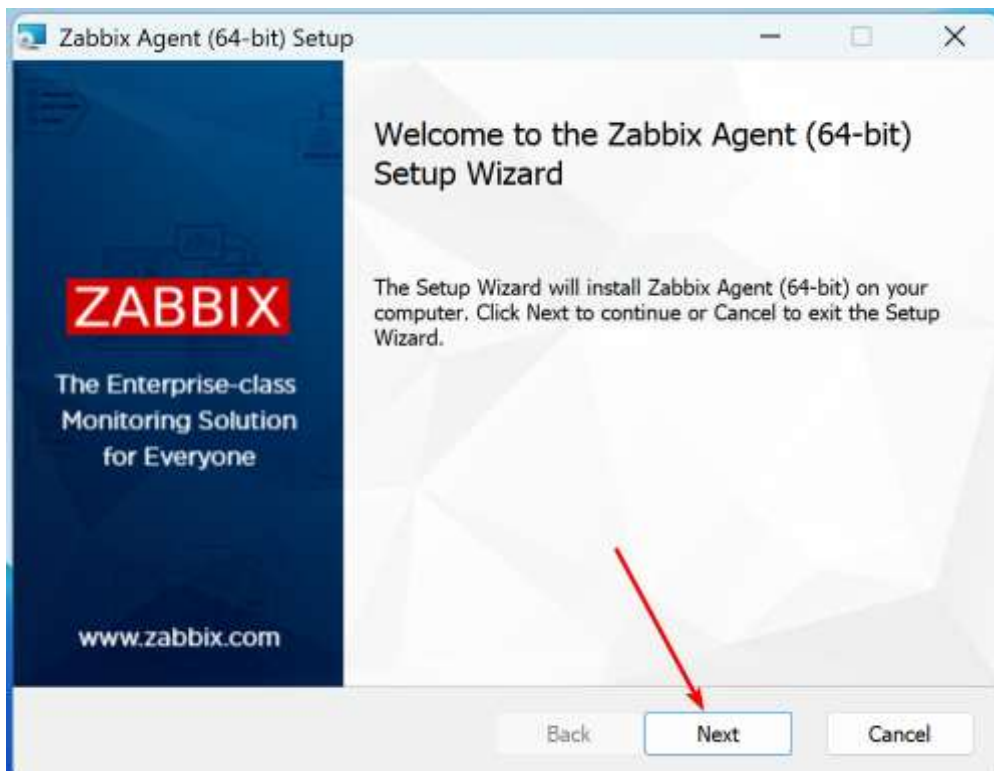
Phrase de passe de confidentialité:

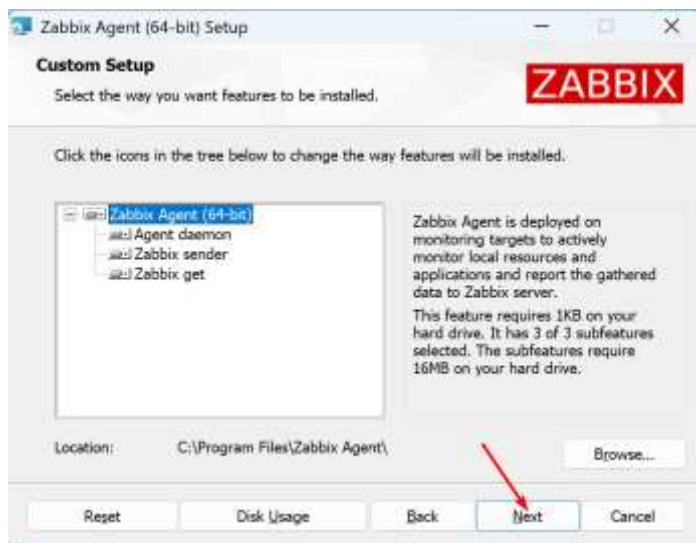
Utiliser des requêtes combinées

[Ajouter](#)

Description:

Pour Windows  
Installation de l'agent



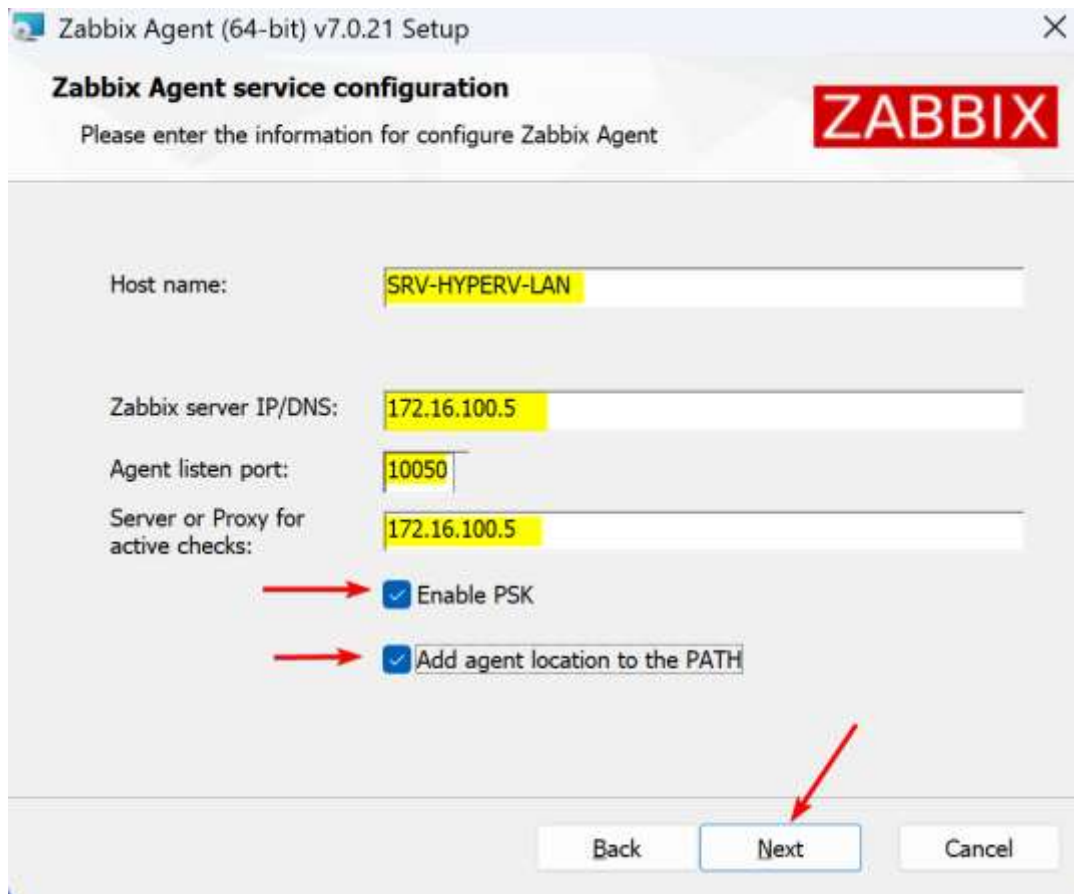


Remplissez les infos du serveur :

IP : 172.16.100.5

Port : 10050

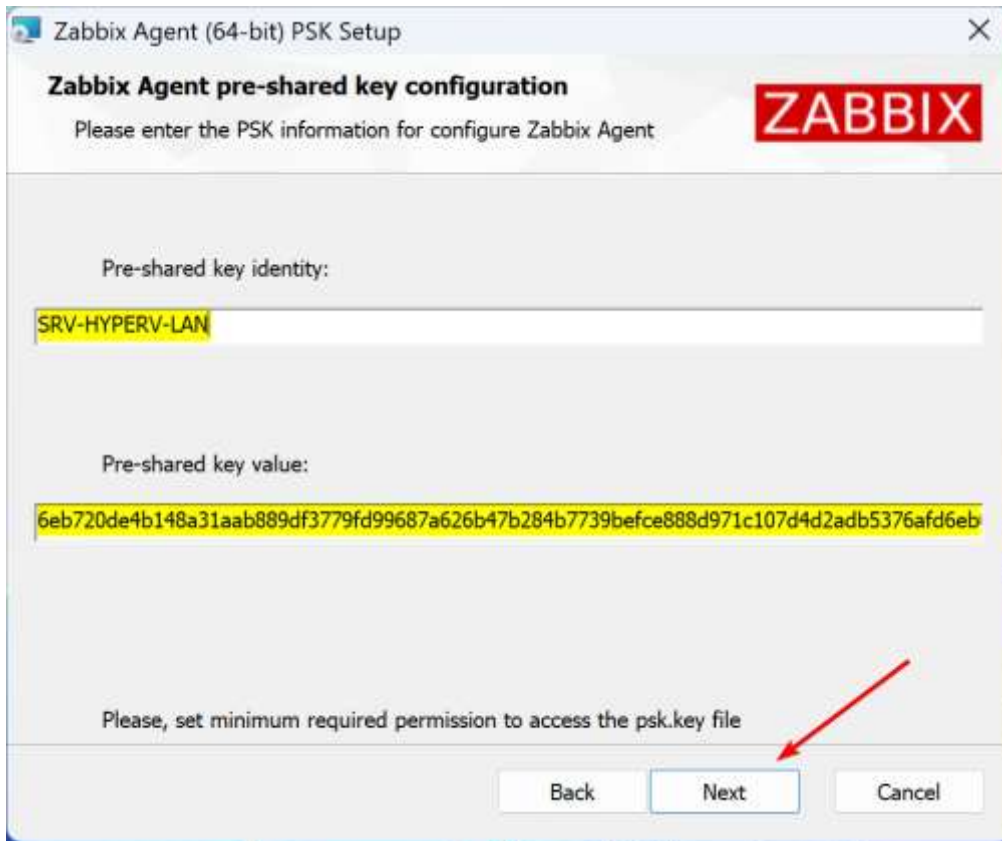
Et cocher les cases suivantes « enable PSK » et « add agent ... »

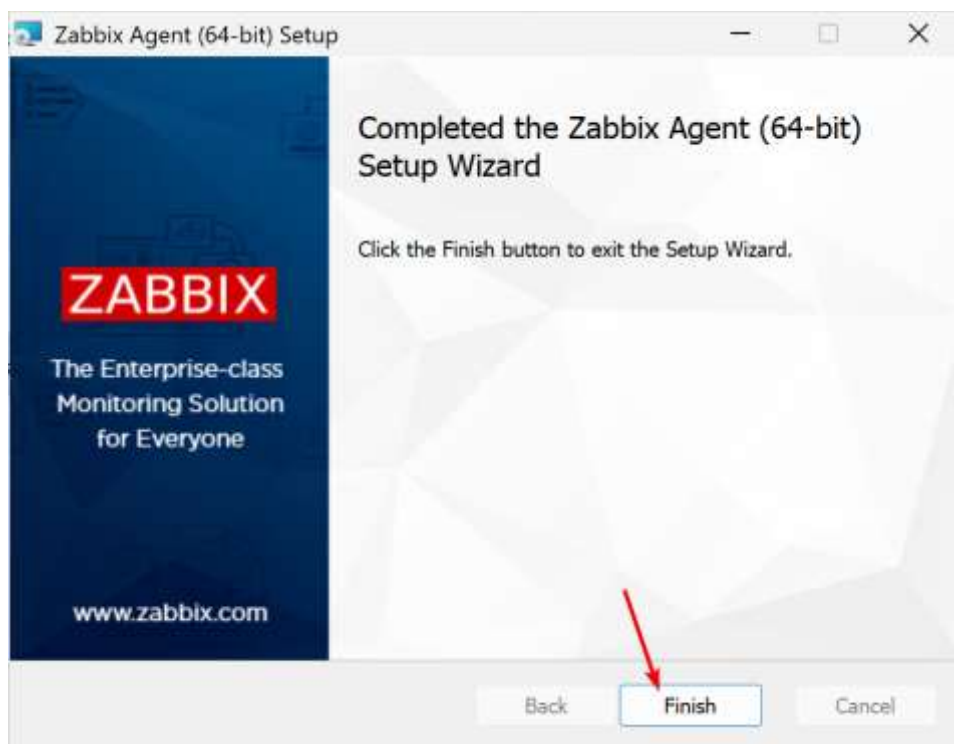
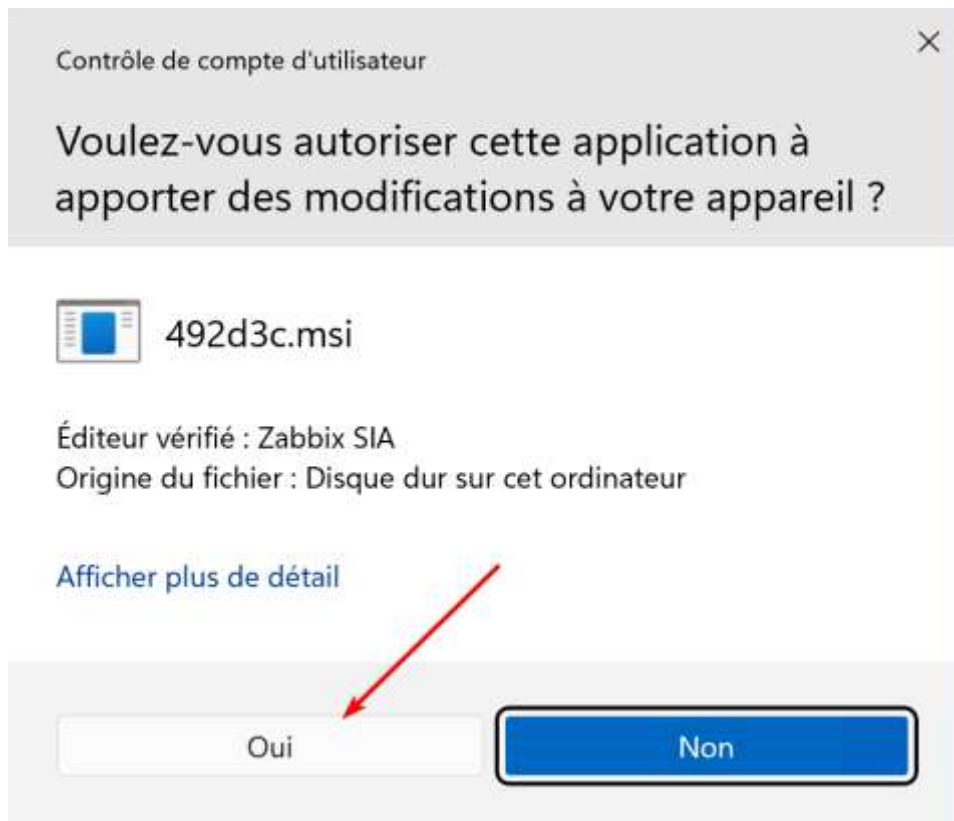


Puis générer une PSK de 128 caractères

```
root@zabbix: /home/ubuntu-zabbix# openssl rand -hex 128
6eb720de4b148a31aab889df3779fd99687a626b47b284b7739bfc0888d971c1b7d4d2adb5376afd5eb8991f74ed908d1199b98f365fcab6577911f8
3aeecc35754d86f6927ebc ce458dc b6de64a1f19a96e77b8f456fda4b6baf6d2fe467b3749ecd0e87c870747a61ec7a56efe5c31cb10dd9
root@zabbix: /home/ubuntu-zabbix#
```

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





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:

Zabbix server IP/DNS:

Agent listen port:

Server or Proxy for active checks:

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:

Pre-shared key value:

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 »

Hôte

Hôte IPMI Tags Macros Inventaire **Chiffrement** Table de correspondance

\* Nom de l'hôte: SRV-DC

Nom visible: SRV-DC

Modules: Nom: Windows by Zabbix agent active Action: Supprimer lien Supprimer lien et nettoyer

\* Groupes d'hôtes: Hypervisors X

Interfaces: Type: Agent adresse IP: 172.16.100.2 Nom DNS: Connexion à: IP DNS Port: 10050 Défaut: Supprimer

Description:

Surveillé par: Serveur Proxy Groupe de proxy

Activé:

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

Hôte

Hôte IPMI Tags Macros Inventaire **Chiffrement** Table de correspondance

Connexion à l'hôte: Pas de chiffrement PSK Certificat

Connexion de l'hôte:  Pas de chiffrement  PSK  Certificat

\* Identité PSK: SRV-DC

\* PSK: ea399f26dc0a1526909b3be9d81c924cdb3c658ff6a5a75b3401b4b4325b0b67b4ba4b90b57c19944

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

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

\* Nom de l'hôte: RNET1  
Nom visible: RNET1

Modèles: Nom Action  
Cisco IOS by SNMP Supprimer lien Supprimer lien et nettoyer  
taper ici pour rechercher -Sélectionner

\* Groupes d'hôtes: Hypervisors X Sélectionner  
taper ici pour rechercher

Interfaces

Type	adresse IP	Nom DNS	Connexion à	Port	Défait
SNMP	192.168.3.251		IP DNS	161	Supprimer

\* Version SNMP: SNMPv3

Nombre maximal de répétitions: 10

Nom de contexte:

Nom de la sécurité: authPrivUser

Niveau de sécurité: authPriv

Protocole d'authentification: SHA1

Phrase d'authentification: myauthphrase

Protocole de confidentialité: AES128

Phrase de passe de confidentialité: myprivphrase

Utiliser des requêtes combinées

## Sur le zyxel :

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

User

ID	User Name	User Type	Description	Creation Date	Password/Change Date	Reference
1	noop-user	ad-user	External LDAP User	Built-in	-	0
2	radius-user	ad-user	External RADIUS User	Built-in	-	0
3	ad-user	ad-user	External AD User	Built-in	-	0
4	billing-user	dynamic-guest	Billing Account User	Built-in	-	0
5	l2t-user	dynamic-guest	User Agreement User	Built-in	-	0
6	Mail-user	dynamic-guest	Free Trial User	Built-in	-	0
7	authPrivUser	User	SNMP User	2025/12/12	2025/12/12	1

Page 1 of 1 | Show 30 | Items

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

SNMP

General Settings

Enable

Server Port:

Trap: Community:  (Optional) Destination:  (Optional)

Trap CAPWAP Event

SNMPv2:

Get Community:

Set Community:

SNMPv3

ID	User	Authentication	Privacy	Privilege
1	authPrivUser	sha2	aes	Read-Only

Page 1 of 1 | Show 30 | Items

Service Control

Line	Address	Action
-	ALL	Accept

Page 1 of 1 | Show 30 | Items

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

Interfaces

Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
SNMP	172.16.255.254		IP DNS	161	<input checked="" type="radio"/> Supprimer

\* Version SNMP:

Nombre maximal de répétitions:

Nom de contexte:

Nom de la sécurité:

Niveau de sécurité:

Protocole d'authentification:

Phrase d'authentification:

Protocole de confidentialité:

Phrase de passe de confidentialité:

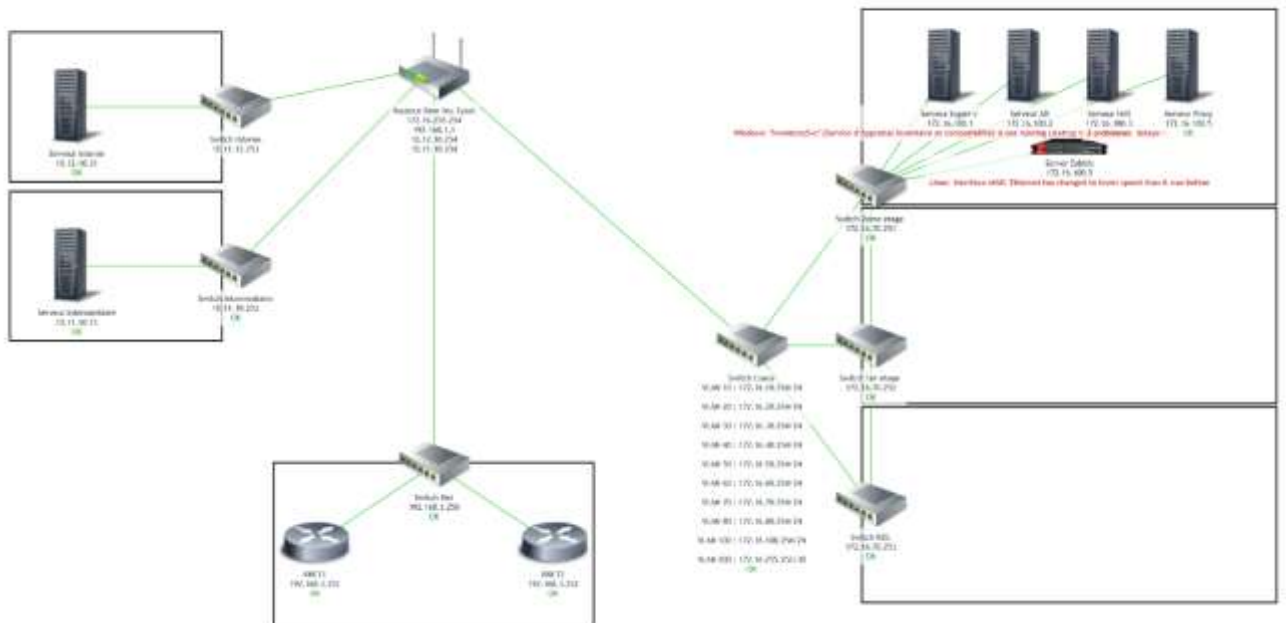
Utiliser des requêtes combinées

## 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 2 <sup>ème</sup> étage
Switch 1 <sup>er</sup> 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

<input type="checkbox"/>	Nom d'utilisateur	Widget	Nom de famille	Nom utilisateur	Groupes	Est connecté ?	Connexion	Autos à l'interface	Actif API	Multisite	Stat	Profil	...
<input type="checkbox"/>	admin	Admin	Administrateur	Super admin role	admin, Zabbix administrator	Non	OK	Active	Actif	Étiqueté	Active		
<input type="checkbox"/>	admin_Webots	Administrateur	Admin role	Zabbix administrator		Non	OK	Active	Actif	Étiqueté	Active		
<input type="checkbox"/>	admin_System	Admin	Admin role	Zabbix administrator		Non	OK	Active	Actif	Étiqueté	Active		

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@abdeladimnaimi.com »

Type de média

Type de média Modèles de messages Options

\* Nom Zabbix-Alerte

Type Courriel

Fournisseur de messagerie Genéric SMTP

\* serveur SMTP smtp.hostinger.com

Port du serveur SMTP 465

\* Courriel alerteinfrasaveol@abdeladimnaimi.com

SMTP helo

Sécurité de la connexion Aucun STARTTLS **SSL/TLS**

Vérifier la par SSL

Vérifier l'hôte SSL

Authentification Aucun **Nom d'utilisateur et mot de passe**

Nom d'utilisateur alerteinfrasaveol@abdeladimnaimi.com

Mot de passe **Changer le mot de passe**

Format du message **HTML** Texte brut

Description

Activé

Actualiser Clone Supprimer Annuler

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

Actions	Conditions	Opérations	État
<input type="checkbox"/> Report problèmes Réseau	<ul style="list-style-type: none"><li>Statut du déclencheur est supérieur ou égal à Moyen</li><li>filte égal Switch_1e</li><li>filte égal Switch_MC</li><li>filte égal Switch_Serveur</li><li>filte égal Switch</li><li>filte égal Switch_Couleur</li><li>filte égal Switch_intermediaire</li><li>filte égal Switch-DC</li><li>filte égal Switch</li><li>filte égal Switch_interna</li><li>filte égal Switch</li></ul>	<ul style="list-style-type: none"><li>Envoyer le message aux groupes d'utilisateurs: Zabbix administrateurs via tous les médias</li><li>Exécuter le script "Detect operating system" sur l'hôte actuel</li><li>Calculer le script "Detect operating system" sur les hôtes: Zabbix serveurs</li></ul>	Actif
<input type="checkbox"/> Report problèmes Système	<ul style="list-style-type: none"><li>Statut du déclencheur est supérieur ou égal à Moyen</li><li>filte égal Serveur-serveur</li><li>filte égal Serveur-Proxy</li><li>filte égal Serveur-Intermediaire</li><li>filte égal Serveur-Interne</li><li>filte égal Serveur-Intermediaire</li><li>filte égal Proxy</li></ul>	<ul style="list-style-type: none"><li>Envoyer le message aux groupes d'utilisateurs: Zabbix administrateurs via tous les médias</li><li>Exécuter le script "Detect operating system" sur l'hôte actuel</li><li>Calculer le script "Detect operating system" sur les hôtes: Zabbix serveurs</li></ul>	Actif

affichage 2 sur 2 items

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

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

Opérations	Etapes	Détails	Démarrer dans	Durée	Action
	1	Envoyer le message aux utilisateurs: Admin_Réseau (Abdelaadim) via tous les médias	Immédiatement	Défaut	<a href="#">Édition</a> <a href="#">Supprimer</a>
	1 - 5	Exécuter le script "Detect operating system" sur l'hôte actuel Exécutez le script "Detect operating system" sur les hôtes: Zabbix server	Immédiatement	Défaut	<a href="#">Édition</a> <a href="#">Supprimer</a>
	<a href="#">Ajouter</a>				
Opérations de récupération	Détails				Action
	Notifier tous les participants				<a href="#">Édition</a> <a href="#">Supprimer</a>
	Envoyer le message aux utilisateurs: Admin_Réseau (Abdelaadim) via Zabbix-Alerte				<a href="#">Édition</a> <a href="#">Supprimer</a>
	<a href="#">Ajouter</a>				
Opérations de mise à jour	Détails				Action
	<a href="#">Ajouter</a>				

Interrompre les opérations en cas de problèmes symptomatiques Suspendre les opérations des problèmes supprimés Notifier les escalades annulées 

\* Au moins une opération doit exister.

[Actualiser](#)[Cloner](#)[Supprimer](#)[Annuler](#)

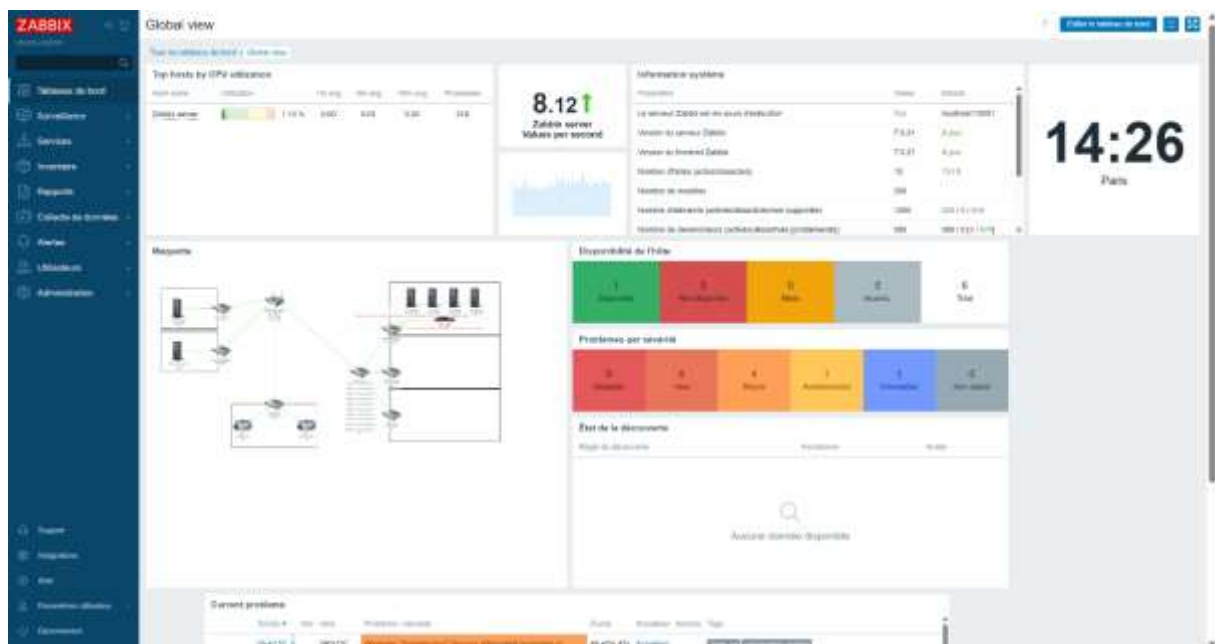
Paramétrage de l'action de déclencheur pour envoyer les alertes à l'administrateur système « Cyprien »

## 9. Production de la documentation projet

Documentation utilisation Zabbix

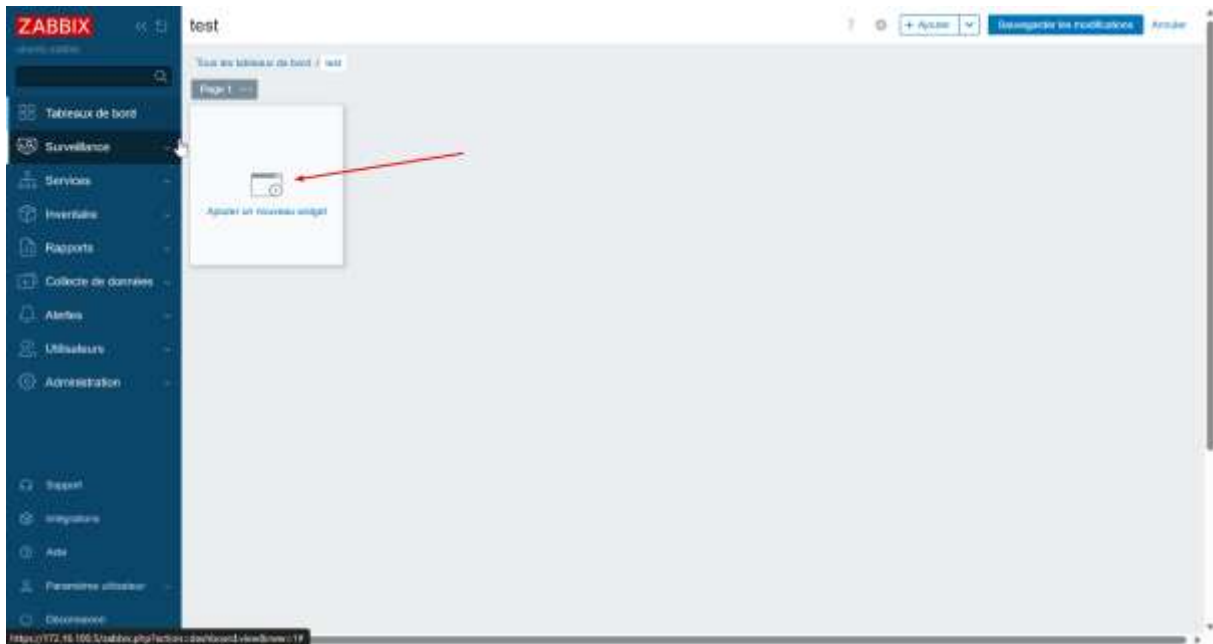
*Création et /ou modification du tableau de bord*

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

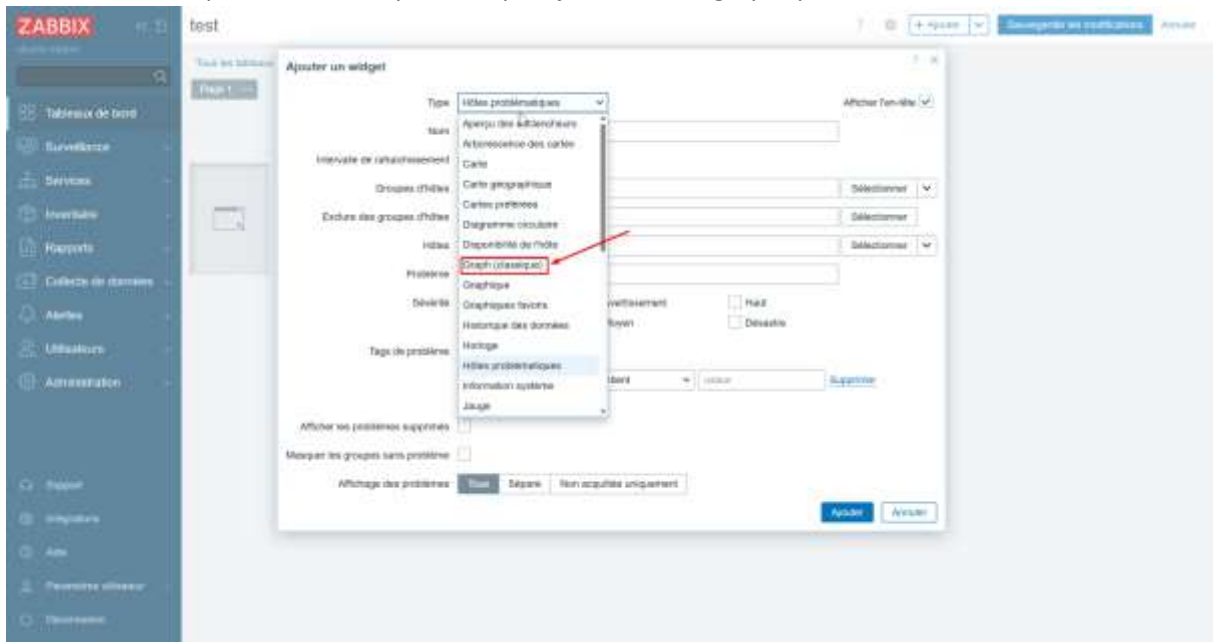


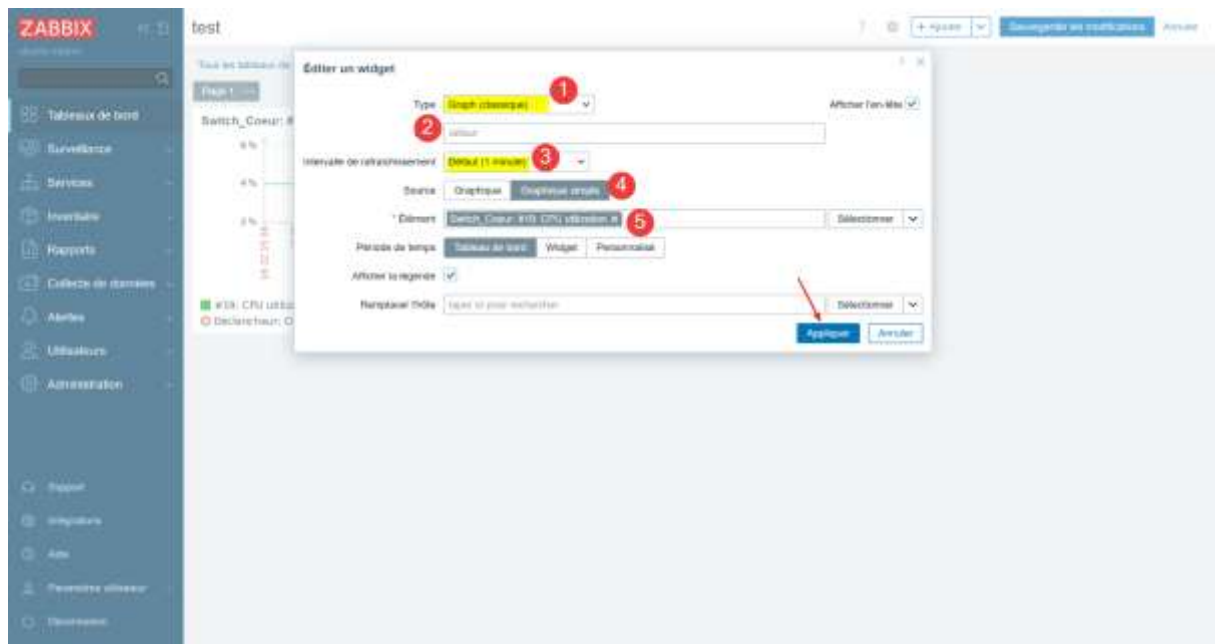
Pour la modifier il faut cliquer sur éditer le tableau de bord



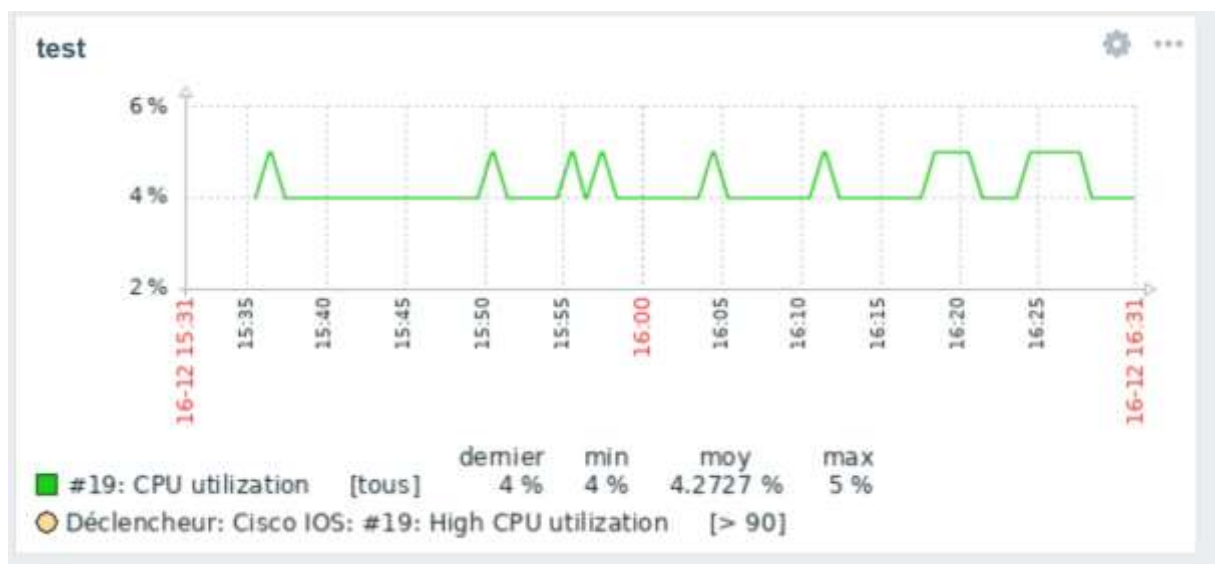


Sélectionner ce que vous voulez pour ma part j'ai choisi un graphique

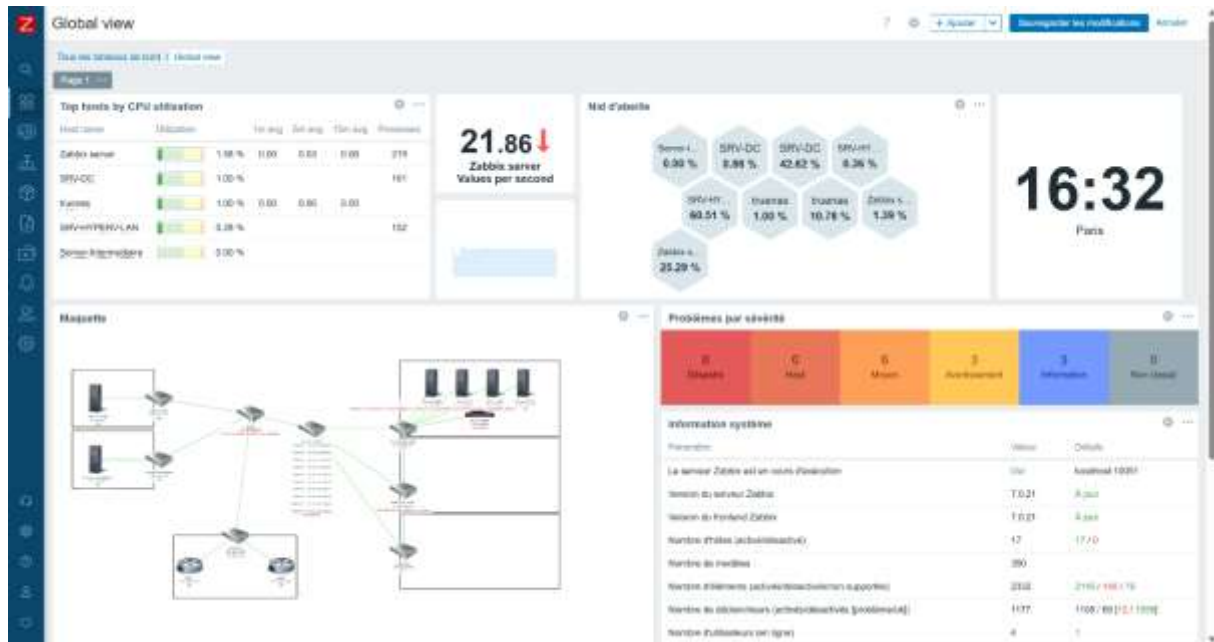




Et voila vous avez le graphique



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 the
# 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
```

### Hôte

Hôte IPMI Tags Macros Inventaire **Chiffrement** Table de correspondance

\* Nom de l'hôte   
Nom visible

**Hôte** [? X]

Hôte IPMI Tags Macros Inventaire **Chiffrement** Table de correspondance

Connexion à l'hôte  Pas de chiffrement  **PSK**  Certificat

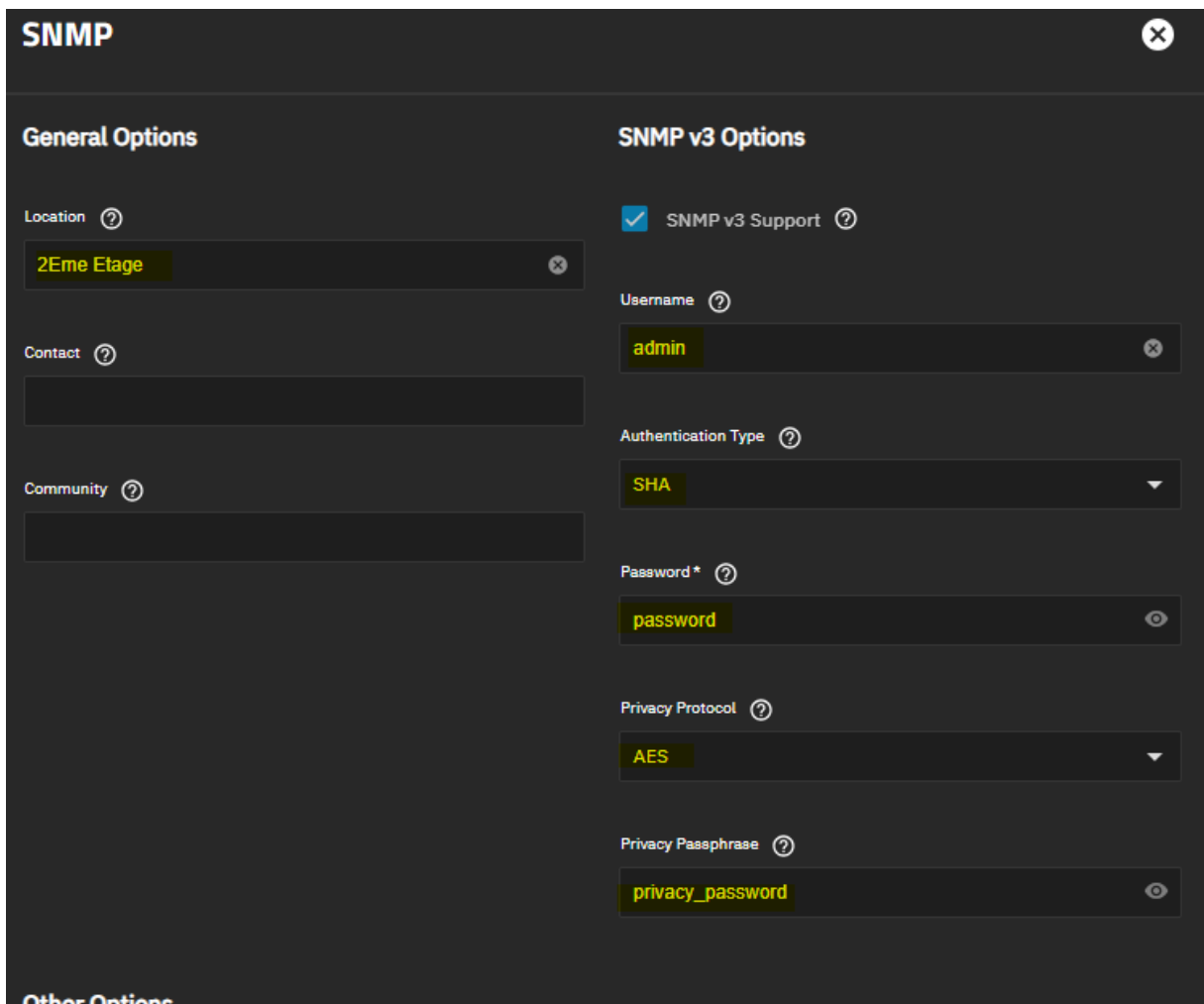
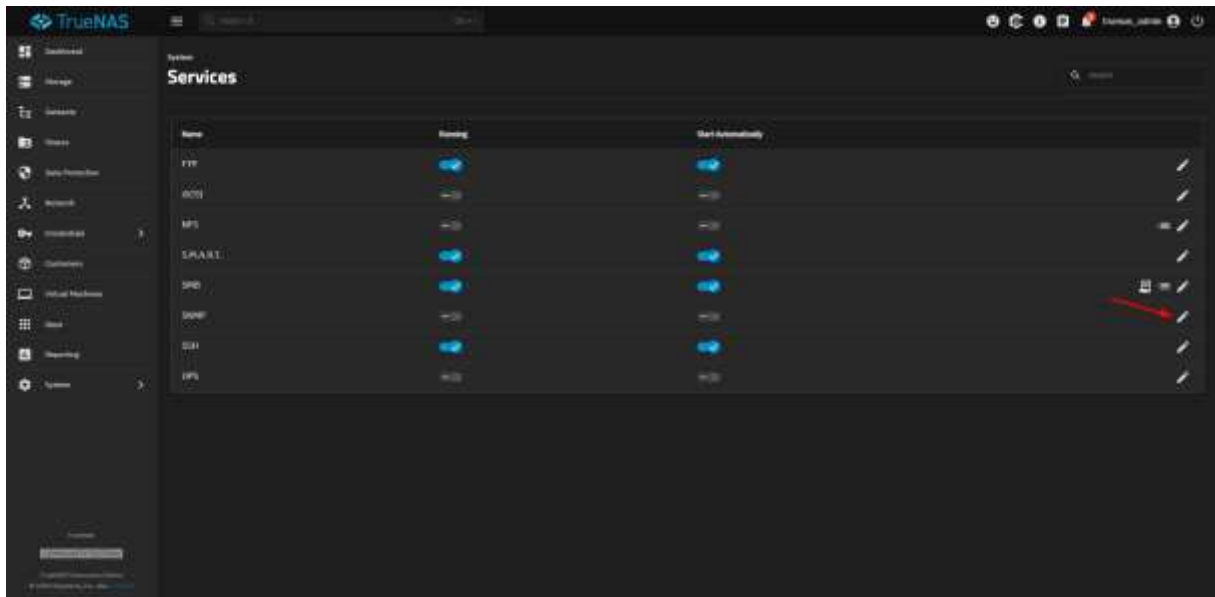
Connexion de l'hôte  Pas de chiffrement  **PSK**  Certificat

\* Identité PSK

\* PSK

*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 libsnp-dev -y 1
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 ».
libsnp-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.

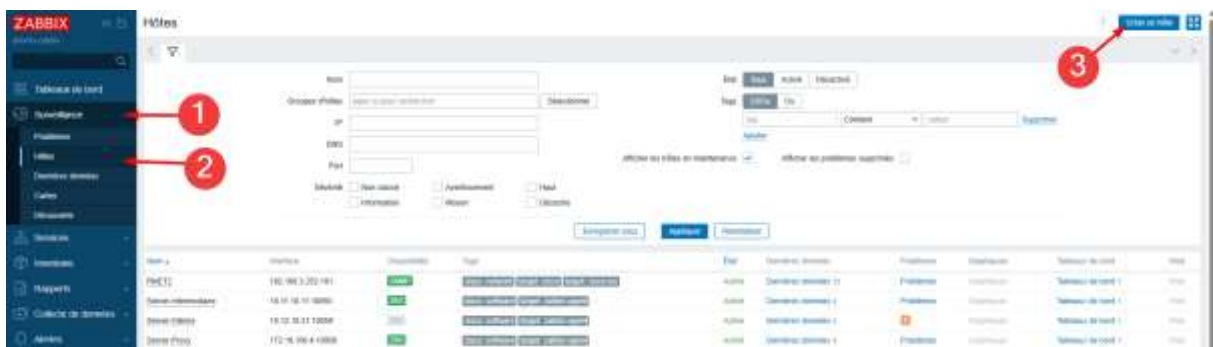
No containers need to be restarted.

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 -O SMI -A password -X AES -x privacy password -I authPriv -u admin 172.16.100.3 | head -10
as (revision #1 SMP PREEMPT_DYNAMIC Mon Sep  8 18:59:34 UTC 2025)
iso.3.6.1.2.1.1.1.2.0 = 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
iso.3.6.1.2.1.1.1.3.0 = OID: iso.3.6.1.4.1.58539.3.1
iso.3.6.1.2.1.1.1.4.0 = STRING: "unknown@localhost"
iso.3.6.1.2.1.1.3.0 = STRING: "truenas"
iso.3.6.1.2.1.1.6.0 = STRING: "2ème 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 :

Nouvel hôte

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

\* Nom de l'hôte:

Nom visible:

Modèles:  Sélectionner

\* Groupes d'hôtes:  Sélectionner

Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
SNMP		<input type="text" value="172.16.100.3"/>	<input type="text"/>	<input type="button" value="IP"/>	DNS	161 <input type="button" value="Supprimer"/>

\* Version SNMP:

Nombre maximal de répétitions:

Nom de contexte:

Nom de la sécurité:

Niveau de sécurité:

Protocole d'authentification:

Phrase d'authentification:

Protocole de confidentialité:

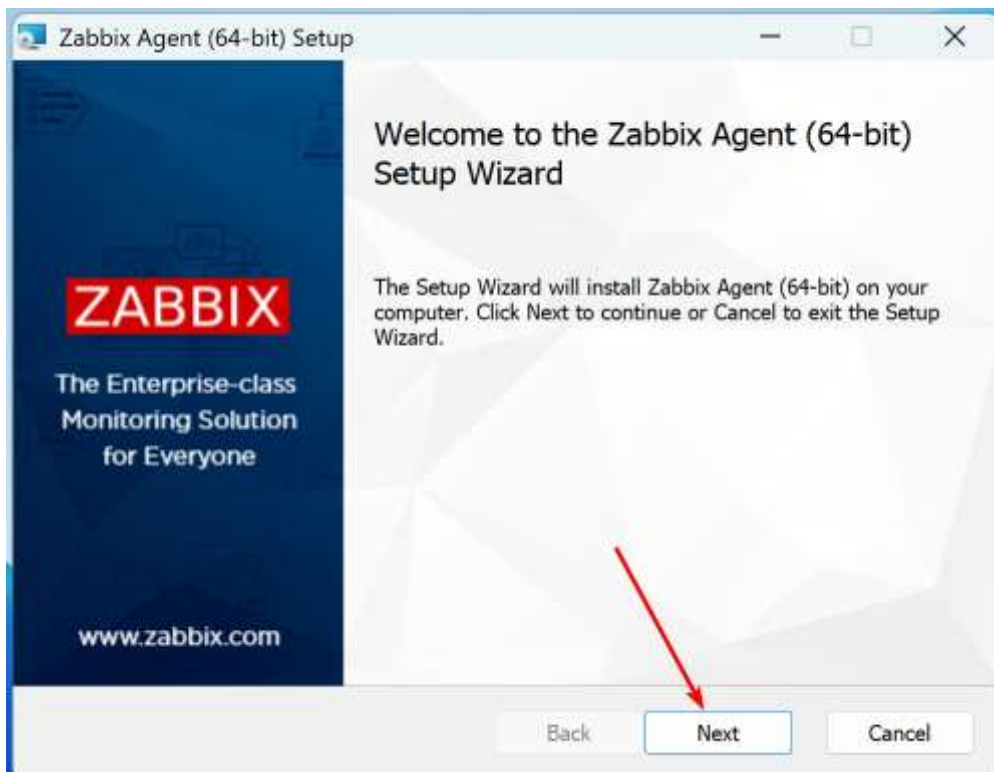
Phrase de passe de confidentialité:

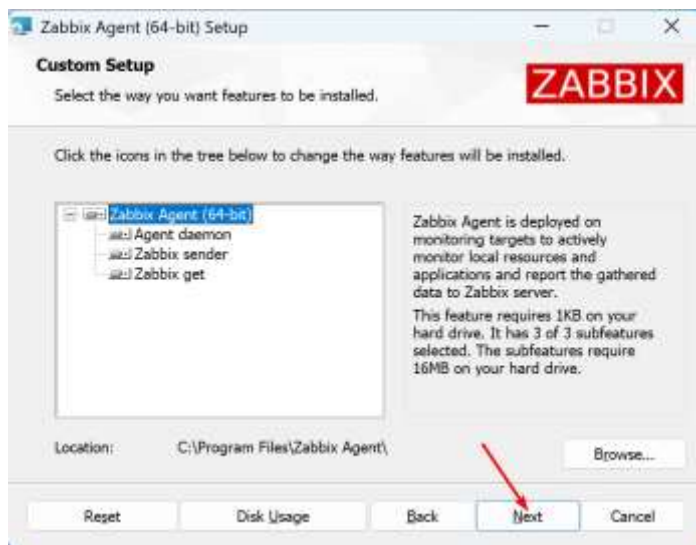
Utiliser des requêtes combinées

[Ajouter](#)

Description:

Pour Windows  
Installation de l'agent



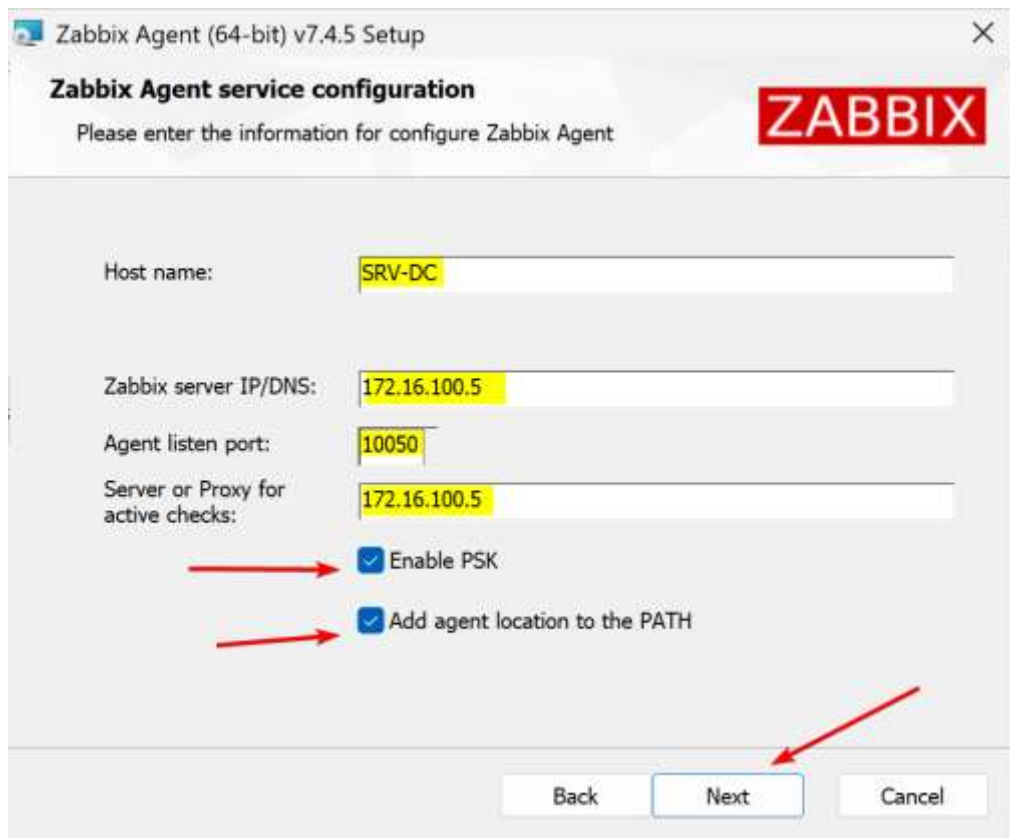


Remplissez les infos du serveur :

IP : 172.16.100.5

Port : 10050

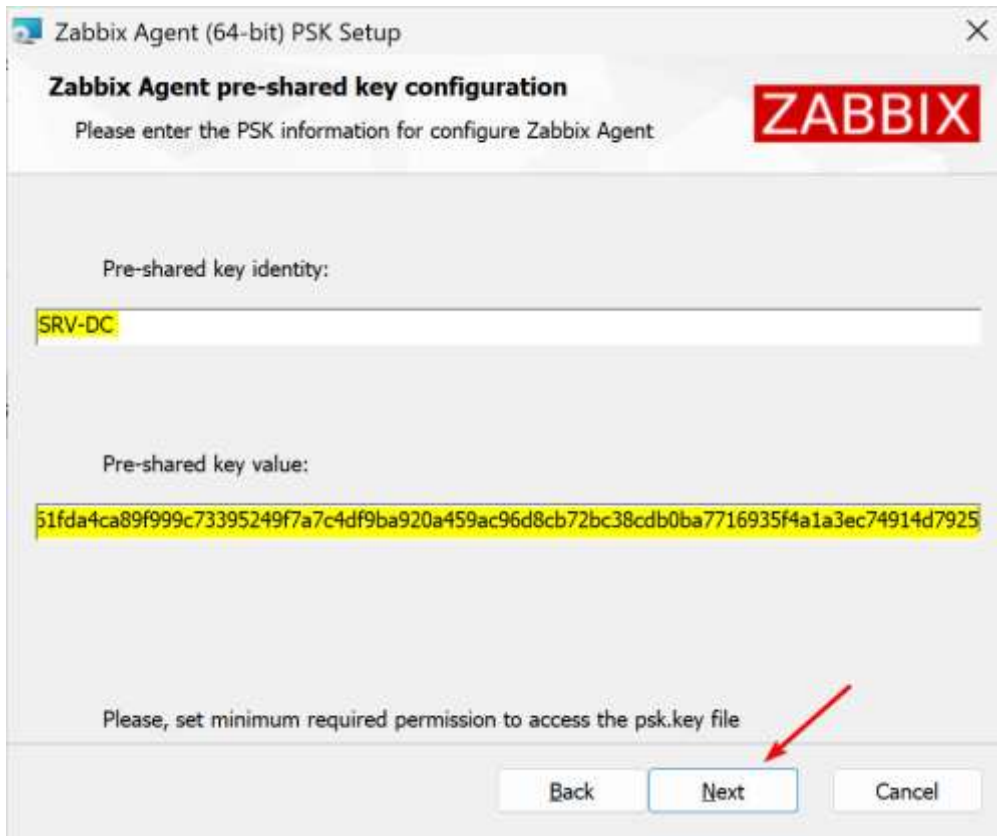
Et cocher les cases suivantes « enable PSK » et « add agent ... »

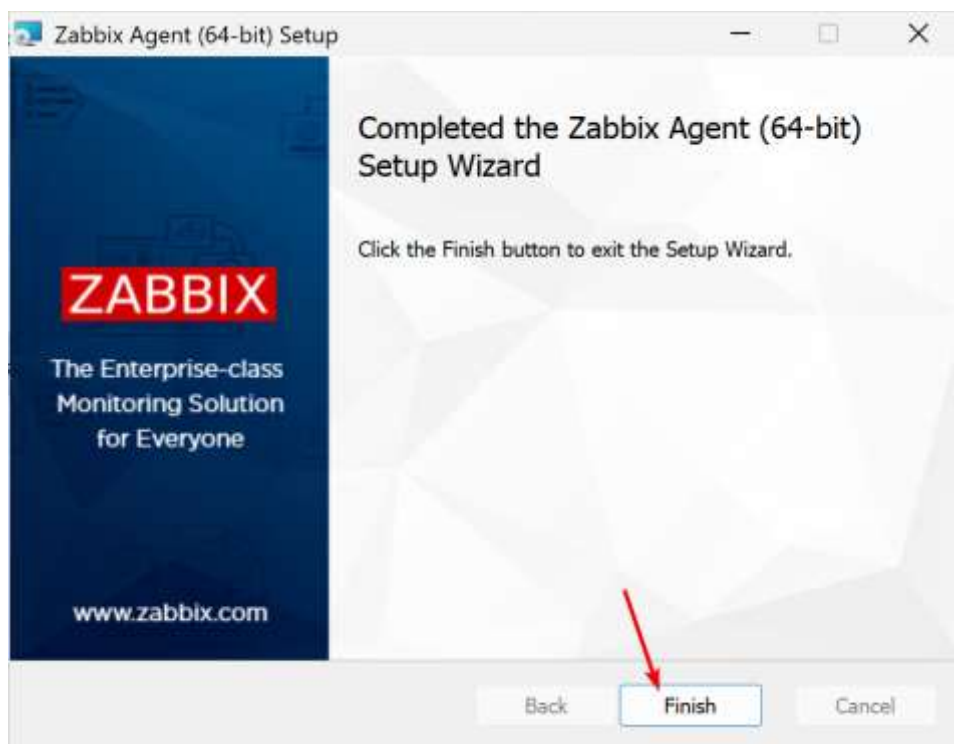
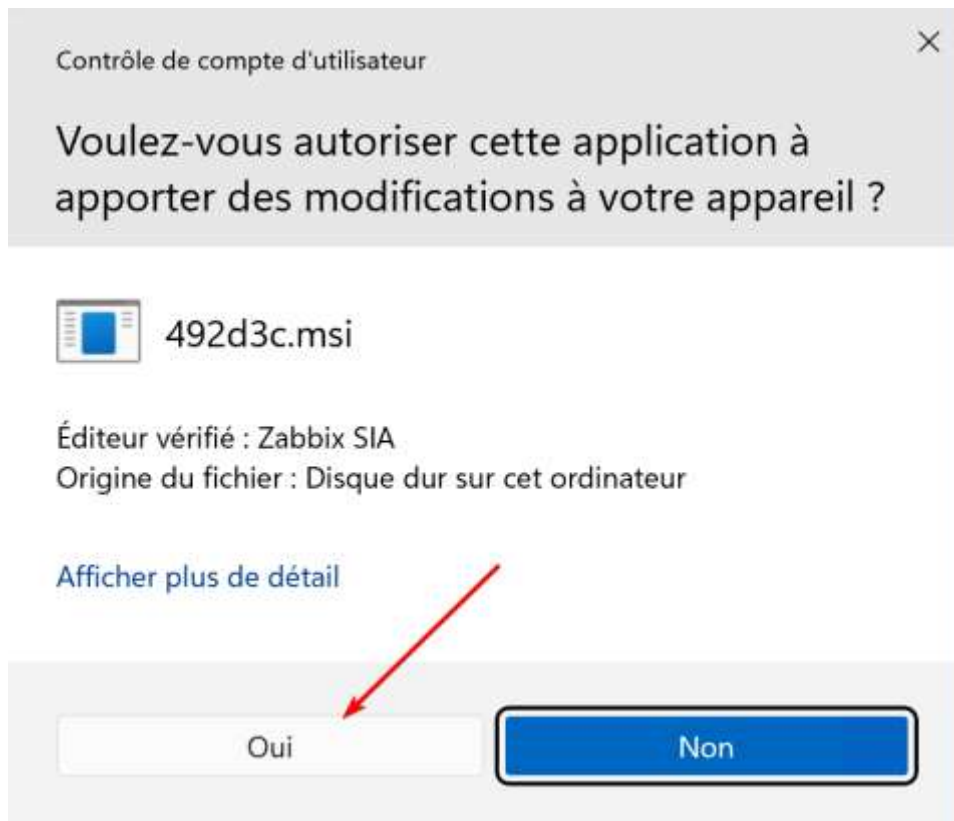


Puis générer une PSK de 128 caractères

```
root@zabbix: /home/ubuntu-zabbix# openssl rand -hex 128
6eb720de4b148a31aab889df3779fd99687a626b47b284b7739befce888d971c107d4d2adb5376afd6eb9991f74ed908d1199b98f365fcab6577911f6
3aeec35754d06f0927ebc ce458dcb8de64a1f19a96e77b8f456fda4b6baf0d2fe467b3749ecd0e87c870747a61ec7a56efe5c31cb10dd9
root@zabbix: /home/ubuntu-zabbix#
```

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





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

Hôte

Hôte IPMI Tags Macros Inventaire **Chiffrement** Table de correspondance

\* Nom de l'hôte: SRV-DC

Nom visible: SRV-DC

Modèles

Nom	Action
Windows by Zabbix agent active	Supprimer lien Supprimer lien et nettoyer

taper ici pour rechercher Sélectionner

\* Groupes d'hôtes: Hypervisors X

taper ici pour rechercher Sélectionner

Interfaces

Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent	172.16.100.2		IP DNS	10050	<input checked="" type="checkbox"/> Supprimer

Ajouter

Description

Surveillé par:  Serveur  Proxy  Groupe de proxy

Activé

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

Hôte

Hôte IPMI Tags Macros Inventaire **Chiffrement** Table de correspondance

Connexion à l'hôte:  Pas de chiffrement  PSK  Certificat

Connexion de l'hôte:  Pas de chiffrement  PSK  Certificat

\* Identité PSK: SRV-DC

\* PSK: ea399f26dc0a1526909b3be9d81c924cdb3c658ff6a5a75b3401b4b4325b0b67b4ba4b90b57c19944

## 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

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

\* Nom de l'hôte: RNET1

Nom visible: RNET1

Modèles

Nom	Action
Cisco IOS by SNMP	Supprimer lien Supprimer lien et nettoyer

taper ici pour rechercher -Sélectionner

\* Groupes d'hôtes

Hypervisors X Sélectionner

taper ici pour rechercher

Interfaces

Type	adresse IP	Nom DNS	Connexion à	Port	Défait
SNMP	192.168.3.251		IP DNS	161	Supprimer

\* Version SNMP: SNMPv3

Nombre maximal de répétitions: 10

Nom de contexte:

Nom de la sécurité: authPrivUser

Niveau de sécurité: authPriv

Protocole d'authentification: SHA1

Phrase d'authentification: myauthphrase

Protocole de confidentialité: AES128

Phrase de passe de confidentialité: myprivphrase

Utiliser des requêtes combinées

## Sur le zyxel :

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

ID	Nom	Type	Description	Création Date	Modification Date	Permissions
1	ldap-user	ext-user	External LDAP User	Built-in	-	0
2	radius-user	ext-user	External RADIUS User	Built-in	-	0
3	ad-user	ext-user	External AD User	Built-in	-	0
4	billing-user	dynamic-guest	Billing Account User	Built-in	-	0
5	ua-user	dynamic-guest	User Agreement User	Built-in	-	0
6	trial-user	dynamic-guest	Free Trial User	Built-in	-	0
7	authPrivUser	User	SNMP User	2025/12/12	2025/12/12	1

Page 1 of 1 | 1 | 1 | Show 30 | 6 | Peris

Displaying 1 - 7 of 7

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

The screenshot shows the Mikrotik WinBox interface for configuring SNMP. It is divided into three main sections: General Settings, a table of SNMPv3 users, and Service Control.

**General Settings:**

- Enable
- Server Port: 161
- Trap: Community: (Optional), Destination: (Optional)
- Trap CAPWAP Event
- SNMPv2: Get Community: public, Set Community: public
- SNMPv3

**SNMPv3 Users Table:**

ID	Username	Passwd	Privilege
1	authPrivUser	1234	Read-Only

**Service Control Table:**

Line	Address	Action
-	ALL	Accept

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

The screenshot shows the Zabbix web interface for adding a new interface. The 'Type' is set to 'SNMP' and the 'adresse IP' is '172.16.255.254'. The 'Connexion à' section is set to 'IP', 'DNS', and '161'. The 'Défaut' section has a 'Supprimer' button.

**Configuration details:**

- \* Version SNMP: SNMPv3
- Nombre maximal de répétitions: 10
- Nom de contexte: (empty)
- Nom de la sécurité: authPrivUser
- Niveau de sécurité: authPriv
- Protocole d'authentification: SHA1
- Phrase d'authentification: myauthphrase
- Protocole de confidentialité: AES128
- Phrase de passe de confidentialité: myprivphrase
- Utiliser des requêtes combinées

Mise en place des alertes

## Création des user

Nom de famille	Nom d'utilisateur	Groupe	Expiré automatiquement	Connexion	Accès à l'interface	Accès API	Mode debug	État	Paramètres
Zabbix	Admin	Super administrateur	Non	OK	Non	Actif	Désactivé	Actif	
Admin	Admin	Super administrateur	Non	OK	Non	Actif	Désactivé	Actif	
Guest	Guest	Utilisateur invité	Non	OK	Non	Désactivé	Désactivé	Désactivé	

Utilisateurs

Utilisateur    Menu    Paramètres

Nom d'utilisateur: admin

Prénom: Test

Nom de famille:

Groupe: Super administrateur

Mot de passe: [masked]

Mot de passe (confirmé): [masked]

Langue: Français (fr\_FR)

Fuseau horaire: Valeur système par défaut: UTC+01:00 Europe/Paris

Theme: Valeur système par défaut

Ajouter    Annuler

Zabbix 7.0.11 (2021-05-20), Zabbix SA

Utilisateur Média 1 Permissions

Média Type Envoyer à Lorsque actif Utiliser si sévère État Action

Zabbix-Alerte test@bidulemail.com 1-7,00-00-24-00 **N I A M H D** Active Edition Supprimer

Ajouter

Ajouter Annuler

Utilisateurs

Nom d'utilisateur: \_\_\_\_\_

Wile utilisateur:  Sélectionner

Nom: \_\_\_\_\_

Groupe d'utilisateurs:  Sélectionner

Nom de famille: \_\_\_\_\_

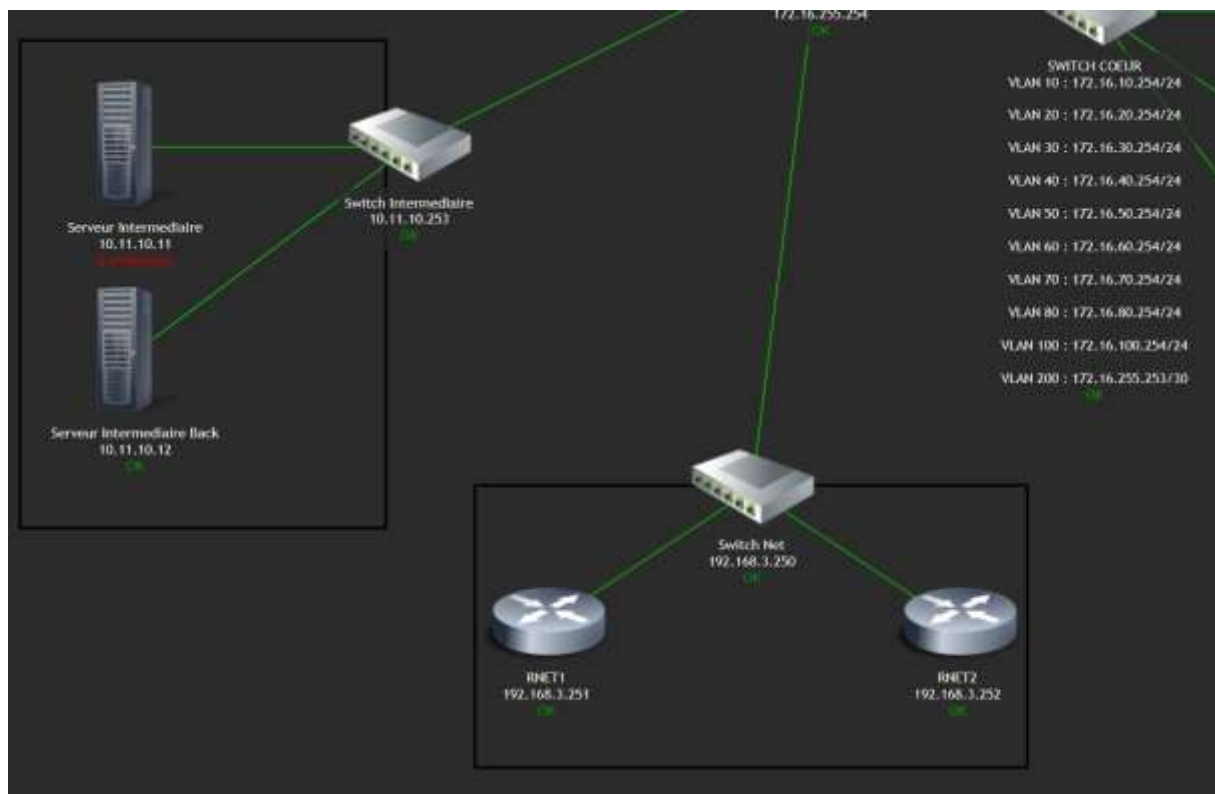
Ajouter Annuler

Nom d'utilisateur	Patron	Nom de famille	Wile utilisateur	Groupe	Est connecté	Compte	Accès à l'interface	Accès API	Heure de début	État	Préférences	Info
Admin	Zabbix	Administrateur	Super admin role	Admin, Zabbix administrateur	Oui (16122025 17:08:31)	OK	Active	Active	Active	Disponible	Active	
admin	Test		Admin role	Zabbix administrateur	Non	OK	Non	Non	Non	Disponible	Active	
Admin_News	Abonné		Admin role	Zabbix administrateur	Non	OK	Non	Non	Non	Disponible	Active	
Admin_System	Compte		Admin role	Zabbix administrateur	Non	OK	Non	Non	Non	Disponible	Active	
guest			Guest role	Default, System, normal	Non	OK	Non	Non	Non	Disponible	Disponible	

Zabbix 7.0.11 (c) 2007-2025, Zabbix SIA

Prendre en charge une alerte :

Vous allez avoir une notification sur la carte :

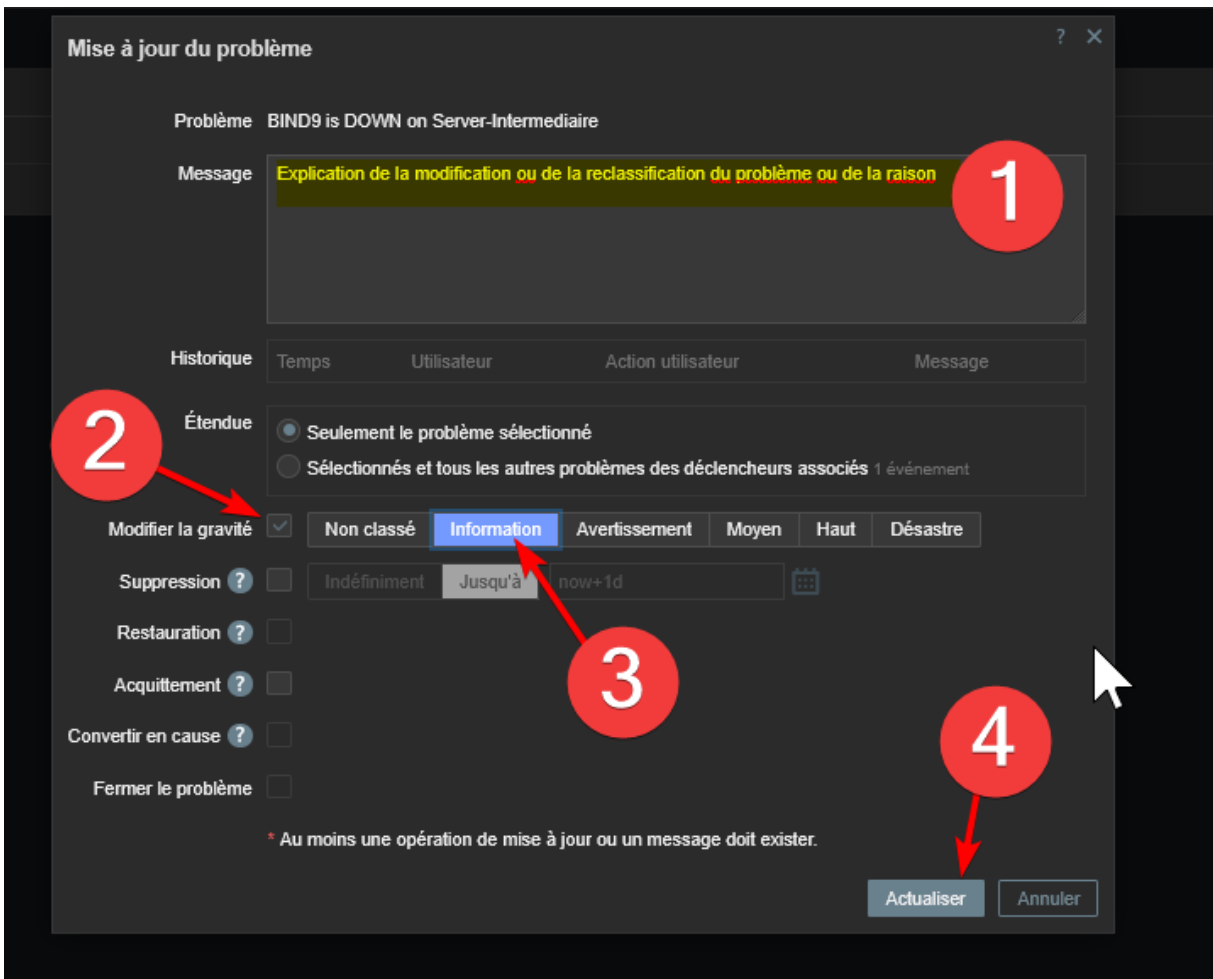


Via l'hôte :



Host	IP	Status	Services	Action	Details	Problèmes
RNET1	192.168.3.251-181	OK	ibm:network target:dhcp target:dhcp:file	Actuel	Cartesian données 11	Problèmes
RNET2	192.168.3.252-181	OK	ibm:network target:dhcp target:dhcp:file	Actuel	Cartesian données 11	Problèmes
Server-Intermediaire	10.11.10.11-10550	OK	ibm:db ibm:software target:apache	Actuel	Cartesian données 111	Problèmes
Server-Intermediaire-Back	10.11.10.12-10090	OK	ibm:db ibm:software target:apache	Actuel	Cartesian données 111	Problèmes

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



**Mise à jour du problème**

Problème BIND9 is DOWN on Server-Intermediaire

Message **Explication de la modification ou de la reclassification du problème ou de la raison** 1

Historique

Temps	Utilisateur	Action utilisateur	Message
-------	-------------	--------------------	---------

Étendue

Seulement le problème sélectionné

Sélectionnés et tous les autres problèmes des déclencheurs associés 1 événement

Modifier la gravité  Non classé **Information** 3 Avertissement Moyen Haut Désastre

Suppression ?  Indéfiniment Jusqu'à now+1d

Restauration ?

Acquittement ?

Convertir en cause ?

Fermer le problème

\* Au moins une opération de mise à jour ou un message doit exister.

Actualiser Annuler 4

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

