

Gyulan Gagneur

BTS SIO 2

Document de validation de compétences

AP 4 – SuperViz

25-18/11-12/2025

Binome: Bilel

1. Présentation du contexte d'entreprise

- **PRESBOIS SAS est une entreprise créée en 1998, spécialisée dans la production de panneaux de fibres de bois et de solutions pour les constructions en ossature bois.**
- **C'est la plus grande usine de production de ce type en France : elle consomme un million de tonnes de bois par an.**
- **Elle compte 42 salariés sur un site de 30 hectares.**
- **L'entreprise est très solide financièrement : elle prévoit de vendre 580 000 m³ de panneaux en 2024 pour un chiffre d'affaires estimé à 142 millions d'euros, dont 94 % destinés à l'exportation.**

2. Objectifs attendus

Le déploiement de cette nouvelle architecture répondra aux objectifs suivants :

1. Intégration et Périmètre de surveillance

- **Déploiement interne : Intégrer au sein du réseau local (LAN) un outil de supervision professionnel, sous la forme d'une machine virtuelle.**
- **Collecte sécurisée : S'appuyer sur le protocole SNMP, configuré de façon sécurisée, pour remonter les métriques de l'infrastructure.**
- **Couverture des serveurs : Contrôler l'état de santé de l'environnement Windows et Linux, en incluant l'analyse de l'espace de stockage, la charge processeur, l'état des cartes réseau et la disponibilité des services clés.**
- **Couverture du réseau : Surveiller le trafic et le statut des ports majeurs sur les équipements d'interconnexion (commutateurs et routeurs).**

2. Alertes et Affichage (Exploitation)

- **Anticipation des pannes : Assurer un suivi proactif visant à détecter les anomalies avant qu'elles ne provoquent des arrêts de production.**
- **Cartographie dynamique : Fournir à l'équipe informatique une interface centralisée affichant une carte globale de l'infrastructure en temps réel.**
- **Classification : Structurer l'interface en regroupant les matériels par familles et par systèmes pour rendre l'exploitation plus intuitive.**
- **Seuils et Routage des alertes : Configurer des niveaux d'alerte sur mesure ("Avertissement" et "Critique") pour chaque élément. En cas d'anomalie, un système de notification par courriel devra cibler le bon interlocuteur (l'alerte sera envoyée à l'administrateur système ou à l'administrateur réseau selon la nature de l'incident).**

3. Validation et Livrables du projet

- **Contrôle qualité : Élaborer et dérouler un plan de tests exhaustif pour prouver la fiabilité et la bonne réaction du système mis en place.**
- **Documentation d'architecture (Technique) : Rédiger un dossier technique consignnant les choix de configuration, les résultats de la phase de tests, ainsi qu'une mise à jour de la topologie réseau.**

- **Documentation d'exploitation (Utilisateur) : Créer un manuel de prise en main destiné aux équipes IT pour faciliter l'utilisation quotidienne de la plateforme.**

3. Plan de travail

Le projet est organisé en plusieurs actions (A1 à A10) permettant un déploiement progressif, testé et documenté.

- **A1 Comparaison des solutions et recommandation SNMP**
- **A2 Installation de la VM Zabbix**
- **A3 Ajout des serveurs sur Zabbix**
- **A4 Configuration SNMP des équipements réseaux et ajouts sur Zabbix**
- **A5 Amélioration et reproduction du schéma réseau sur Zabbix**
- **A6 Configuration des alertes via mail**
- **A7 Tests**

4. Réalisation

A1 : Comparaison des solutions et recommandation SNMP

Comparaison des deux solutions (Zabbix vs Centreon)

- **Zabbix est très complet : il permet de superviser à la fois le réseau, les serveurs Linux et Windows, ainsi que les services applicatifs. Il offre des alertes par mail, des graphiques détaillés, des cartes réseau et une grande scalabilité. Cependant, sa mise en place est plus complexe et demande une configuration plus importante, surtout pour les serveurs et services.**
- **Centreon brille par sa gestion des rapports (Reporting) et ses tableaux de bord orientés "métier" qui plaisent beaucoup aux décideurs. Sa popularité en France en fait une compétence très recherchée par les prestataires de services (ESN) comme LINS.**

Pourquoi retenir Zabbix pour le projet PRESBOIS ?

Le choix de Zabbix comme pilier de la supervision repose sur trois axes stratégiques adaptés à l'infrastructure de l'entreprise :

- **Omnivigilance de l'infrastructure** : Zabbix offre une console unique pour piloter aussi bien les équipements réseau (Cisco) que les serveurs (Linux/Windows) et les couches applicatives, assurant une cohérence globale du suivi.
- **Réactivité et Visualisation** : La solution transforme les données brutes en outils d'exploitation concrets : notifications par mail en cas d'alerte critique, graphiques d'analyse de tendance, cartes réseau dynamiques et rapports de disponibilité.
- **Évolutivité et Automatisation** : Malgré une configuration initiale exigeante, sa capacité à automatiser la découverte de nouveaux équipements et à s'adapter aux futurs besoins de croissance de PRESBOIS en fait l'outil le plus pérenne.

Recommandations pour la sécurisation du protocole SNMP

Pour garantir l'intégrité du système d'information et prévenir toute exfiltration de données, la configuration du protocole SNMP doit suivre un durcissement rigoureux :

1. Choix du Protocole et Chiffrement

- **Standard de sécurité** : Abandonner impérativement les versions v1 et v2c, dont les informations circulent sans protection, au profit de SNMPv3.
- **Mécanismes robustes** : Utiliser des algorithmes de hachage modernes pour l'authentification (SHA ou SHA-256) et le standard AES pour le chiffrement des communications.
- **Gestion des secrets** : Définir des comptes SNMP dédiés avec des mots de passe à haute complexité, en proscrivant les noms de communautés génériques (type "public").

2. Contrôle d'Accès et Surveillance

- **Isolation réseau** : Limiter strictement les flux SNMP aux seules adresses IP autorisées, prioritairement celle du serveur de supervision.
- **Moindre privilège** : Configurer les droits d'accès exclusivement en "Lecture Seule" (RO) pour interdire toute modification de configuration à distance via le protocole.
- **Défense périmétrique** : Filtrer les ports SNMP au niveau du pare-feu (Zyxel USG FLEX) et désactiver le service sur tous les équipements n'en ayant pas l'utilité.
- **Audit** : Activer systématiquement la journalisation (logs) pour identifier et analyser toute tentative d'accès non autorisée ou suspecte.

tentative d'accès suspecte.

A2 : Installation de la VM Zabbix

Il faut installer la VM ubuntu server 24.01 sur notre hyper-V et on procède à l'installation de Zabbix.

On doit configurer l'ip:

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Apr 10 10:16:02 CEST 2026 on tty1
groupe4@zabbix:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:3f:96:0d brd ff:ff:ff:ff:ff:ff
    inet 172.19.100.8/24 brd 172.19.100.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe3f:960d/64 scope link
        valid_lft forever preferred_lft forever
groupe4@zabbix:~$
```

On applique avec netplan apply puis on installe Zabbix avec :

wget

[https://repo.zabbix.com/zabbix/7.4/release/ubuntu/pool/main/z/zabbix-release/zabbix-release_](https://repo.zabbix.com/zabbix/7.4/release/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest_7.4+ubuntu24.04_all.deb)

[latest_7.4+ubuntu24.04_all.deb](#)

dpkg -i zabbix-release_latest_7.4+ubuntu24.04_all.deb

apt update

Et :

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

zabbix-agent

Ensuite on installe mysql avec la commande :

apt install mysql-server -y

Puis on configure la base de données :

mysql -uroot -p

[MDP]

mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;

mysql> create user zabbix@localhost identified by 'password';

mysql> grant all privileges on zabbix.* to zabbix@localhost;

```
mysql> set global log_bin_trust_function_creators = 1;
mysql> quit;
```

Ensuite on importe le schéma et les données nécessaires à Zabbix :

```
zcat /usr/share/zabbix/sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4
-uzabbix -p zabbix
```

On modifie la ligne suivante dans `nano /etc/zabbix/zabbix_server.conf` :

```
DBPassword=password
```

Et enfin on active Zabbix :

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

On peut voir que le service est actif :

```
root@zabbix:/home/groupe4# systemctl status zabbix-agent
● zabbix-agent.service - Zabbix Agent
   Loaded: loaded (/lib/systemd/system/zabbix-agent.service; vendor preset: enabled)
   Active: active (running) since Tue 2025-11-25 17:30:00 CET; 1min 47s ago
     Main PID: 2578 (zabbix_agentd)
       Tasks: 13 (limit: 4652)
      Memory: 9.3M
         CPU: 1min 997ms
    CGroup: /system.slice/zabbix-agent.service
           └─2578 /usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agentd.conf
             └─2579 /usr/sbin/zabbix_agentd: collector
               └─2580 /usr/sbin/zabbix_agentd: listener
                 └─2581 /usr/sbin/zabbix_agentd: listener
                   └─2582 /usr/sbin/zabbix_agentd: listener
                     └─2583 /usr/sbin/zabbix_agentd: listener
                       └─2584 /usr/sbin/zabbix_agentd: listener
                         └─2585 /usr/sbin/zabbix_agentd: listener
                           └─2586 /usr/sbin/zabbix_agentd: listener
                             └─2587 /usr/sbin/zabbix_agentd: listener
                               └─2588 /usr/sbin/zabbix_agentd: listener
                                 └─2589 /usr/sbin/zabbix_agentd: listener
                                   └─2590 /usr/sbin/zabbix_agentd: active chroot@zabbix:/home/groupe4# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; vendor preset: enabled)
   Active: active (running) since Tue 2025-11-25 17:30:00 CET; 1min 47s ago
     Docs: https://httpd.apache.org/docs/2.4/
     Main PID: 13304 (apache2)
       Tasks: 6 (limit: 4652)
      Memory: 21.3M
         CPU: 3.817s
    CGroup: /system.slice/apache2.service
           └─13304 /usr/sbin/apache2 -k start
             └─13307 /usr/sbin/apache2 -k start
               └─13308 /usr/sbin/apache2 -k start
                 └─13309 /usr/sbin/apache2 -k start
                   └─13310 /usr/sbin/apache2 -k start
```

On peut voir la page de connexion et on a accès au tableau de bord :

A3 : Ajout des serveurs sur Zabbix

Voici la méthode pour l'ajout sur Zabbix de nos Serveurs Windows :

Installation de l'agent Zabbix sur nos Windows Server :

On installe le .msi pour pouvoir installer l'agent : https://www.zabbix.com/fr/download_agents

OS DISTRIBUTION	OS VERSION	HARDWARE	ZABBIX VERSION	ENCRYPTION	PACKAGING
Windows	11, 10	amd64	7.4	OpenSSL	MSI
Linux	Server 2016 +	i386	7.0 LTS	No encryption	Archive
macOS	Server 2003 +		6.0 LTS		
AIX	XP (64bit) +				
FreeBSD					
OpenBSD					
Solaris					

Zabbix agent v7.4.9 [Read manual](#)

Packaging: MSI
 Encryption: OpenSSL
 Linkage: Dynamic
 Checksum: sha256: 7dc4517e12baae2cb3982a6b2e2a1d6a49e64ca498b8621d3cfff9304e1bf677
 sha1: 9e6f73fe189ca674f91c7ce6e265abff16d2d6ab
 md5: 1d106415b082845548ed035878d94355

[DOWNLOAD](https://cdn.zabbix.com/zabbix/binaries/stable/7.4/7.4.9/zabbix_agent-7.4.9-windows-amd64-openssl.msi) https://cdn.zabbix.com/zabbix/binaries/stable/7.4/7.4.9/zabbix_agent-7.4.9-windows-amd64-openssl.msi

Une fois le paquet installé faire un copier-coller dans le C:\

Ensuite, taper cette commande dans le CMD ou powershell

```
msiexec /i "C:\zabbix_agent-7.0-windows-amd64-openssl.msi" /qn
SERVER=IP_DU_SERVEUR_ZABBIX SERVERACTIVE=IP_DU_SERVEUR_ZABBIX
HOSTNAME=Nom_De_Ce_Serveur_Windows
```

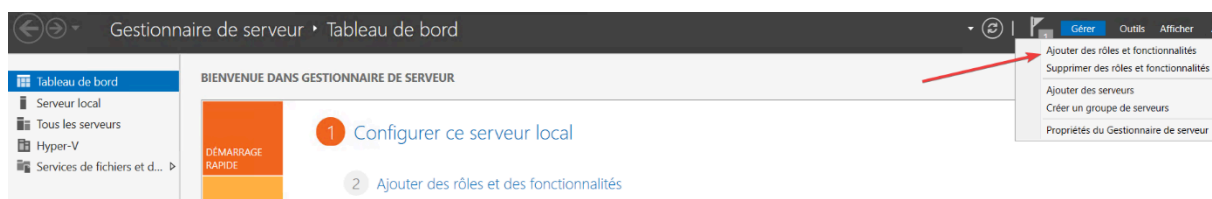
On ajoute les informations nécessaires ainsi que l'IP et le nom DNS pour les hôtes.

On vérifie que la connexion est bien faite et que c'est activé:

DNS	172.19.100.2:161	SNMP		Activé	Dernières données	Problèmes
hyper v	172.19.100.1:161	SNMP		Activé	Dernières données	Problèmes
srv-web	10.41.10.11:161	SNMP		Activé	Dernières données	Problèmes
srv_BDD	10.42.10.31:161	SNMP		Activé	Dernières données	Problèmes
srv_nas	172.19.100.3:161	SNMP		Activé	Dernières données	Problèmes
SwCoeur	172.19.100.254:161	SNMP		Activé	Dernières données	Problèmes
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux ***	Activé	Dernières données 121	Problèmes

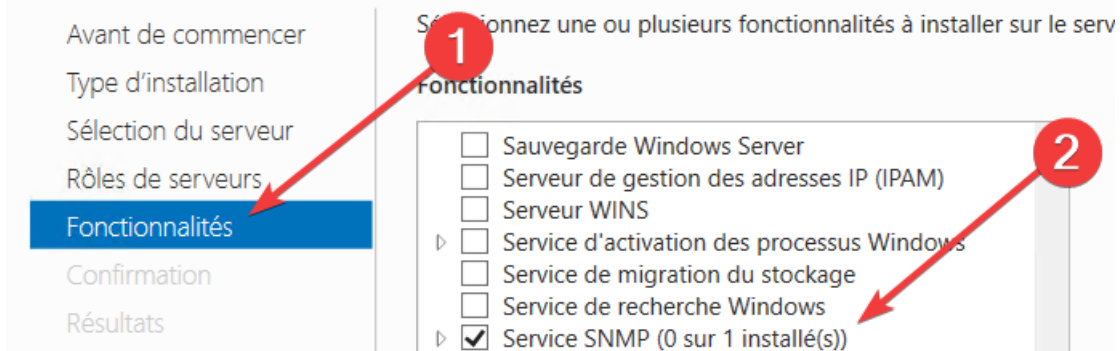
Installation de la fonctionnalité SNMP sur nos Windows Server :

Depuis le gestionnaire du serveur, on clique sur Gérer puis Ajouter des rôles et fonctionnalités :



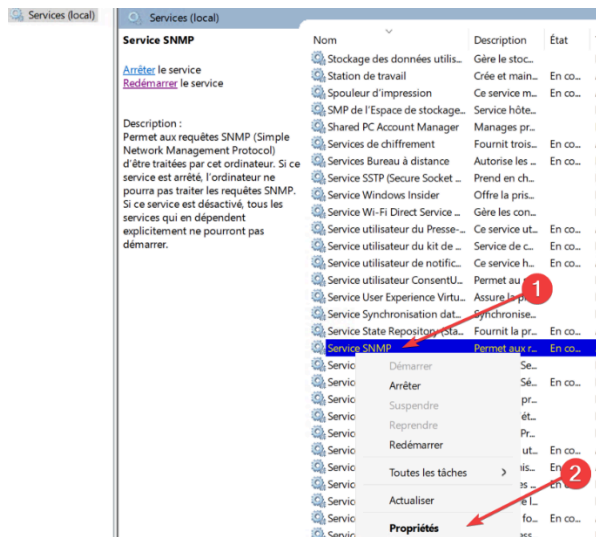
Ensuite on suit l'installateur et on ajoute SNMP :

Sélectionner des fonctionnalités

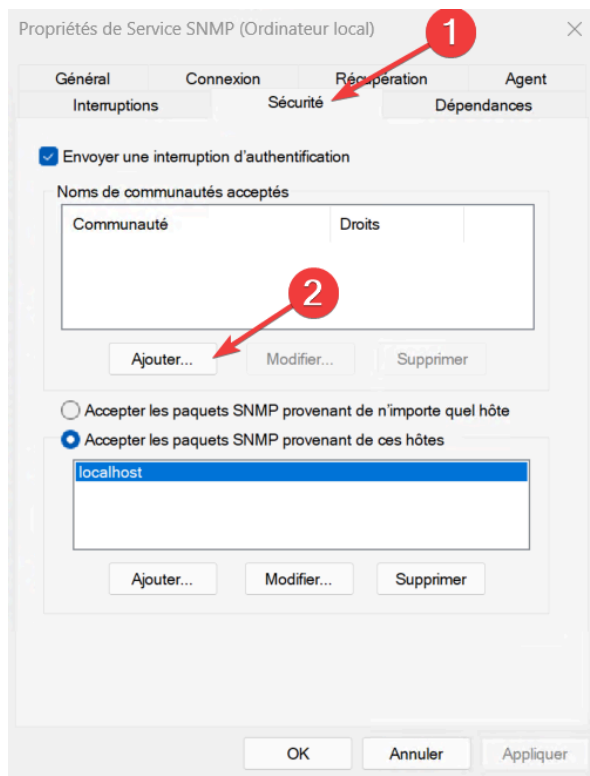


Et on termine l'installation.

On se retrouve dans le service SNMP et on va dans les propriétés sur service SNMP :



Ensuite on va dans Sécurité puis on ajoute une communauté (on peut mettre la même communauté pour tous les serveurs).



Après la création de la communauté, on ajoute l'autorisation de recevoir les paquets SNMP du serveur Zabbix

Et on ajoute les informations importantes comme le nom, le type de serveur, et le type de connexion :

* Nom de l'hôte

Nom visible

Modèles

Nom	Action
ZYXEL GS-4012F by SNMP	Supprimer lien Supprimer lien et nettoyer

Groupes d'hôtes

Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
<input type="button" value="↑"/>	SNMP	<input type="text" value="192.168.1.2"/>	<input type="text"/>	<input type="button" value="IP"/> <input type="button" value="DNS"/>	<input type="text" value="161"/>	<input checked="" type="radio"/> Supprimer
	* Version SNMP	<input type="text" value="SNMPv2"/>				
	* Communauté SNMP	<input type="text" value="admingrp4"/>				
	Nombre maximal de répétitions ?	<input type="text" value="10"/>				

Dans la partie Interfaces on ajoute l'IP du serveur que l'on veut superviser et on ajoute le nom de la communauté ainsi que le nom DNS :

Type	adresse IP	Nom DNS
SNMP	172.19.70.3	172.19.100.2
* Version SNMP		SNMPv2
* Communauté SNMP		admingrp4
Nombre maximal de répétitions ?		10
<input checked="" type="checkbox"/> Utiliser des requêtes combinées		

On vérifie la connexion au niveau de la disponibilité affichée sur Zabbix :



Configuration SNMP :

On installe la fonctionnalité SNMP via les commandes suivantes :

Sudo apt update

Sudo apt install snmp snmpd

Ensuite on modifie le fichier de configuration du SNMP via la commande **nano /etc/snmp/snmpd.conf**

Ensuite démarrer SNMP :

Systemctl restart snmpd

Systemctl enable snmpd

Ensuite on vérifie le fonctionnement du service :

```
root@srv-web:/home/administrateur# systemctl status snmpd
• snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
  Loaded: loaded (/usr/lib/systemd/system/snmpd.service; enabled; preset: enabled)
  Active: active (running) since Fri 2025-12-12 09:50:16 UTC; 2min 2s ago
```

Sur l'interface Zabbix on ajoute le serveur comme vue précédemment :

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

* Nom de l'hôte

Nom visible

Modèles

Nom	Action
linux by zabbix agent	Supprimer lien Supprimer lien et nettoyer

* Groupes d'hôtes

Interfaces

Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent	<input type="text" value="127.0.0.1"/>	<input type="text" value="172.19.100.2"/>	<input checked="" type="radio"/> IP <input type="radio"/> DNS	<input type="text" value="10050"/>	<input checked="" type="radio"/> Supprimer

[Ajouter](#)

Description

Avec l'installation de l'agent Zabbix sur Linux :

L'agent est un programme installé sur les serveurs windows pour permettre de lire en profondeur leur état et pour envoyer au serveur Zabbix ces informations.

1. Ajout du dépôt et installation

wget

```
https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-release_7.0-2+debian12_all.deb sudo dpkg -i zabbix-release_7.0-2+debian12_all.deb sudo apt update sudo apt install zabbix-agent -y
```

sudo apt update

On installe ensuite l'agent, on l'active et on vérifie son statut :

sudo apt install zabbix-agent

systemctl enable zabbix-agent

systemctl status zabbix-agent

2. Configuration de l'agent

Editer le fichier de configuration :

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

Modifier ces 3 lignes :

```
Server=IP_DU_SERVEUR_ZABBIX
```

```
Server=172.19.100.8
```

```
ServerActive=172.19.100.8
```

```
Hostname=Nom_De_Ce_Serveur_Linux
```

3. Démarrage et activation automatique :

```
sudo systemctl restart zabbix-agent
```

```
sudo systemctl enable zabbix-agent
```

```
• zabbix-agent.service - Zabbix Agent
  Loaded: loaded (/usr/lib/systemd/system/zabbix-agent.service; enabled; preset: enabled)
  Active: active (running) since Tue 2025-12-16 15:45:17 UTC; 44s ago
  Process: 4461 ExecStart=/usr/sbin/zabbix_agentd -c $CONFFILE (code=exited, status=0/SUCCESS)
  Main PID: 4463 (zabbix_agentd)
  Tasks: 13 (limit: 4605)
```

Ensuite on modifie le fichier de configuration de l'agent Zabbix (**nano**

/etc/zabbix/zabbix_agentd.conf) et on modifie mes lignes suivantes afin de spécifier notre serveur

Zabbix :

```
Server=172.19.100.8
```

```
ServerActive=172.19.100.8
```

On enregistre et on redémarre l'agent avec :

```
sudo systemctl restart zabbix-agent
```

Ensuite on ajoute l'hôte linux

Top hosts by CPU utilization ⚙️ ⋮

Host name	Utilization	1m avg	5m avg	15m avg	Processes
hyper.v					
DNS					
srv_BDD					
srv_nas					
srv-web					

*

SNMP

General Settings

Enable

Server Port:

Trap:

Community: (Optional)

Destination: (Optional)

Trap CAPWAP Event

SNMPv2c

Get Community:

Set Community:

SNMPv3

+ Add ✎ Edit 🗑 Remove

#	User	Authentication	Privacy
< < Page 0 of 0 >> > Show 50 items			

A4 : Activation du SNMP sur les switches

Enable

Conf t

Ip access-lits standard CL_ZABBIX

Permit Ip_du_serveur_zabbix

Exit

snmp-server community MotDePasseSNMP RO ACL_ZABBIX

RO (read only)

end

A5 : Amélioration et reproduction du schéma réseau sur Zabbix

On créer une carte depuis Surveillance < Cartes et on ajoute les équipements et serveurs ainsi que les liens :

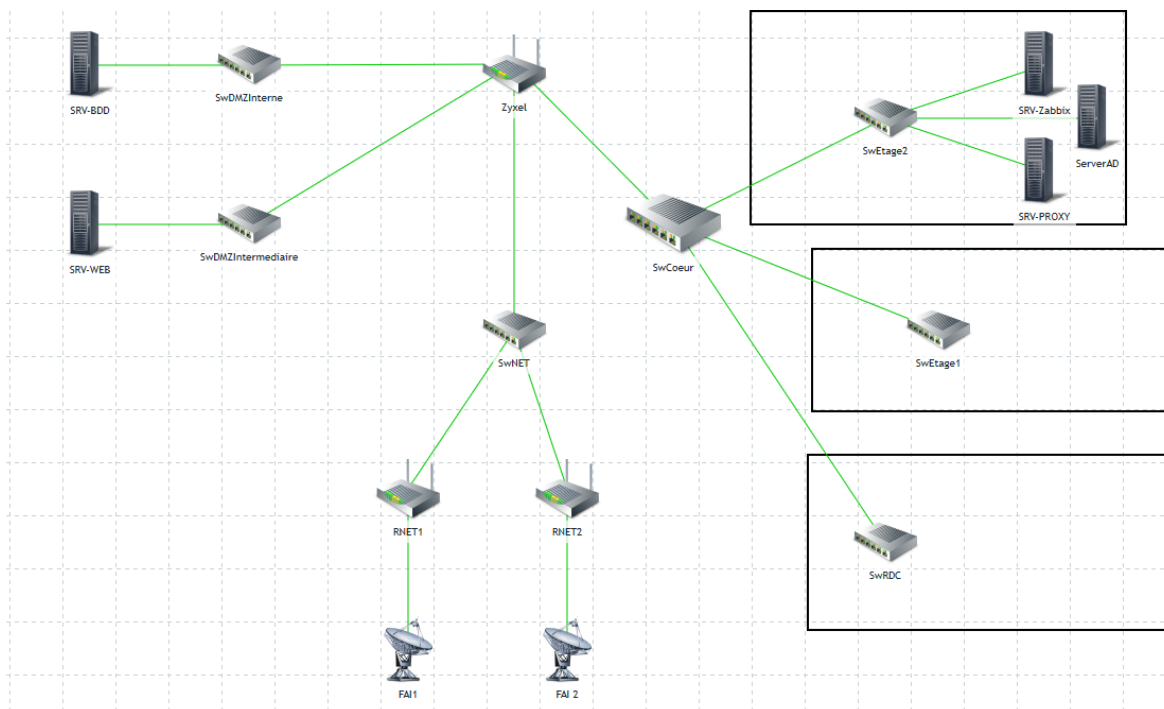
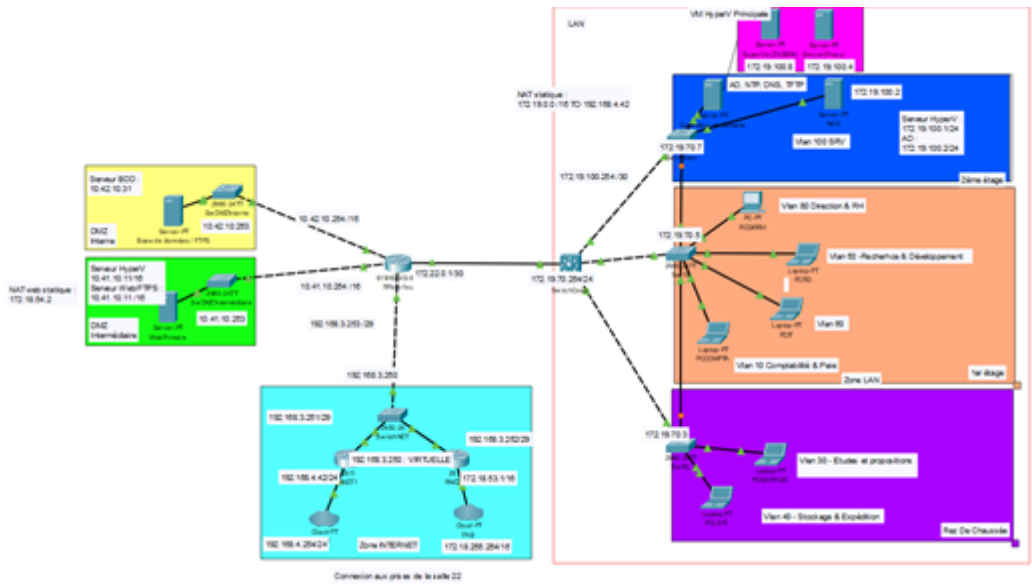


Schéma réseau qui est donc similaire à notre schéma réseau fait sur packet tracer :



A6 : Configuration des alertes via mail

J'ai choisit de configurer des mails sur ma boîte Gmail.

Sur l'interface web Zabbix, on créer un type de média :

Nom	Type	Etat	Utilisé dans les actions	Détails
Brevé one	Webhook	Désactivé	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	
Deucard	Webhook	Désactivé	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	
Email	Courriel	Désactivé	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	serveur SMTP: "mail.example.com", SMTP helo: "example.com", courriel: "zabbix@example.co
Email-alerte	Courriel	Désactivé	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	serveur SMTP: "smtp.hosting.com", SMTP helo: "no.ca.com", courriel: "HV@hadrien.vanderklem.fr"
Event-Driven Attribe	Webhook	Désactivé	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	
Express ms	Webhook	Désactivé	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	

Type de média ? x

Type de média Modèles de messages 5 Options

* Nom Email-alerte

Type Courriel

Fournisseur de messagerie Generic SMTP

* serveur SMTP smtp.hostinger.com

Port du serveur SMTP 587

* Courriel HV@hadrienvanderlekem.fr

SMTP helo rioca.com

Sécurité de la connexion Aucun STARTTLS SSL/TLS

Vérifier le pair SSL

Vérifier l'hôte SSL

Authentification Aucun Norm d'utilisateur et mot de passe OAuth

Nom d'utilisateur HV@hadrienvanderlekem

Mot de passe [Changer le mot de passe](#)

Format du message HTML Texte brut

Description

Activé

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

Ensuite on appuis sur désactivé pour activer le média :

Email-alerte Courriel **Désactivé**

Email-alerte Courriel **Activé**