TP 4 – Installation du serveur de supervision Zabbix en machine virtuelle
Bloc 2 – BTS SIO 2

Objectifs :	Prérequis :
• Savoir préconfigurer un serveur Debian 11 afin d'installer un service spécifique. • Être capable d'installer un outil de supervision de réseaux et de services. • Être capable de paramétrer intégralement un outil de supervision.	• Posséder les compétences de bases en administration des réseaux. • Posséder les compétences de base en administration système GNU/Linux.

Attention ! Lors de toute la durée de la séquence sur la supervision avec Zabbix, vous devrez vous référer à la documentation officielle ou celle fournie par votre enseignant et non sur des tutoriels trouvés au hasard sur le Net. Il faut choisir une documentation en fonction du niveau de fiabilité de cette dernière.

https://www.zabbix.com/documentation/4.0/fr/manual

Avant de démarrer ! Vous devez toujours avoir à l'esprit les éléments de réflexion suivants : A chaque étape, VOUS DEVEZ effectuer les recherches qui s'imposent afin de clarifier chaque terme, chaque fonction, chaque module qui est énoncé. Rien ne sert de courir et d'enchaîner les commandes si vous ne comprenez rien à ce que vous faîtes !

A. Préparation à l'installation du service Zabbix

Vous devez disposer d'un machine virtuelle Debian 11 possédant 1 CPU et 2 cœurs, 4 Go de RAM et d'une carte réseau virtuelle en bridge sur le réseau pédagogique.

Pour connaitre les prérequis concernant l'installation d'un serveur Zabbix en fonction de votre contexte et vos besoins :
https://www.zabbix.com/documentation/6.0/

Démarrez votre machine Debian 11 puis réalisez les configurations de base. Notez chaque commande utilisée pour réaliser l'opération demandée :

1. Vérifier que le système Debian utilisé est à jour.

   apt update && apt upgrade

2. Vérifier que les vmWare Tools sont installés et procéder à l'installation le cas échéant

   apt install open-vm-tools

3. Définir un nom à votre serveur (zabbix-xx) xx étant vos initiales.

   nano /etc/hostname

4. Attribuer une adresse IPv4 fixe à votre VM (172.16.4X.XXX) à l'aide de votre plage dédiée. Penser à appliquer les modifications effectuées dans le fichier de configuration.

   nano /etc/network/interface

5. Faire correspondre 127.0.0.1 et 172.16.4X.XXX à vos noms de machine (zabbix-xx et zabbix-xx.lansio.sfda37.fr).

   nano /etc/hosts

6. Installer un client ntp et synchroniser l'heure du système Debian

   ```
   $ sudo apt install ntpdate && sudo ntpdate-debian
   ```

7. Redémarrer le serveur afin que toutes les modifications soient appliquées.

   reboot

Attention ! Réaliser un snapshot de la machine virtuelle à la fin de cette étape.

B. Procédure d'installation du serveur Zabbix

Pour que le serveur Zabbix puisse fonctionner correctement, un environnement LAMP (Linux Apache MariaDB PHP) doit être correctement installé et fonctionnel.

```
$ sudo apt install apache2 libapache2-mod-php
$ sudo apt install php php-mysql php-mysqlnd php-ldap php-bcmath php-mbstring
$ sudo apt install php-gd php-pdo php-xml
```

a) Configurer le service de bases de données relationnelles MariaDB

```
$ sudo mysql_secure_installation
```

- Définir comme mot de passe root pour le service MariaDB azerty2QWERTY.
- Interdire les connexions anonymes au SGBD.
- Interdire l'accès root au SGBD à distance par le réseau.
- Supprimer la base de données de test.
- Recharger la table des privilèges.

b) Création de la base de données Zabbix

```
$ sudo mysql -u root -p
```

```
MariaDB [(none)]> create database zabbix character set utf8 collate utf8_bin;
MariaDB [(none)]> grant all privileges on zabbix.* to zabbix@localhost identified by 'qwerty2AZERTY';
MariaDB [(none)]> quit;
```

Expliquer à l'aide de recherche sur internet ce que réalisent les deux premières commandes SQL présentées ci-dessus.

Créer une BDD avec le nom zabbix et un ensemble de règles permettant la comparaison de caractères dans un jeu.

Autoriser tous les droits a l'utilisateur zabbix sur la BDD zabbix.
De plus cette commande permet de créer l'utilisateur par la même occassion.

c) Mettre à jour votre fuseau horaire dans le fichier de configuration php.ini

```
$ sudo nano /etc/php/7.4/apache2/php.ini
```

```
[Date]
; Defines the default timezone used by the date functions
; http://php.net/date.timezone
date.timezone = 'Europe/Paris'
```

d) Ajouter les dépôts (miroirs) spécifiques au service Zabbix

```
$ wget https://repo.zabbix.com/zabbix/5.5/debian/pool/main/z/zabbix-release/zabbix-release_5.5-1%2Bdebian11_all.deb
$ sudo dpkg -i zabbix-release_5.5-1+debian11_all.deb
$ sudo apt update
```

e) Installer le service Zabbix

```
$ sudo apt install zabbix-server-mysql zabbix-proxy-mysql zabbix-frontend-php zabbix-agent
$ sudo apt install zabbix-apache-conf zabbix-sql-scripts
```

f) Importer les tables et le schema initiale dans la base de données Zabbix

```
$ zcat /usr/share/doc/zabbix-sql-scripts/mysql/create.sql.gz | mysql -u zabbix -p zabbix
```

Éditer le fichier de configuration du serveur Zabbix afin de définir les paramètres lui permettant d'accéder à la base de données créée précédemment (hôte, nom de la base, login, password, etc.).

```
nano /etc/zabbix/zabbix-server.conf
```

Redémarrer les services zabbix-server et zabbix-agent et leurs permettre de démarrer automatiquement lors du lancement du système d'exploitation.

```
systemctl restart zabbix-server
systemctl restart zabbix-agent
```

Vérifier le fichier de configuration apache de l'interface web Zabbix et notamment la directive concernant le fuseau horaire.

```
$ sudoedit /etc/zabbix/apache.conf
```

```
php_value max_execution_time 300
php_value memory_limit 128M
php_value post_max_size 16M
php_value upload_max_filesize 2M
php_value max_input_time 300
php_value max_input_vars 10000
php_value always_populate_raw_post_data -1
php_value date.timezone Europe/Paris
```

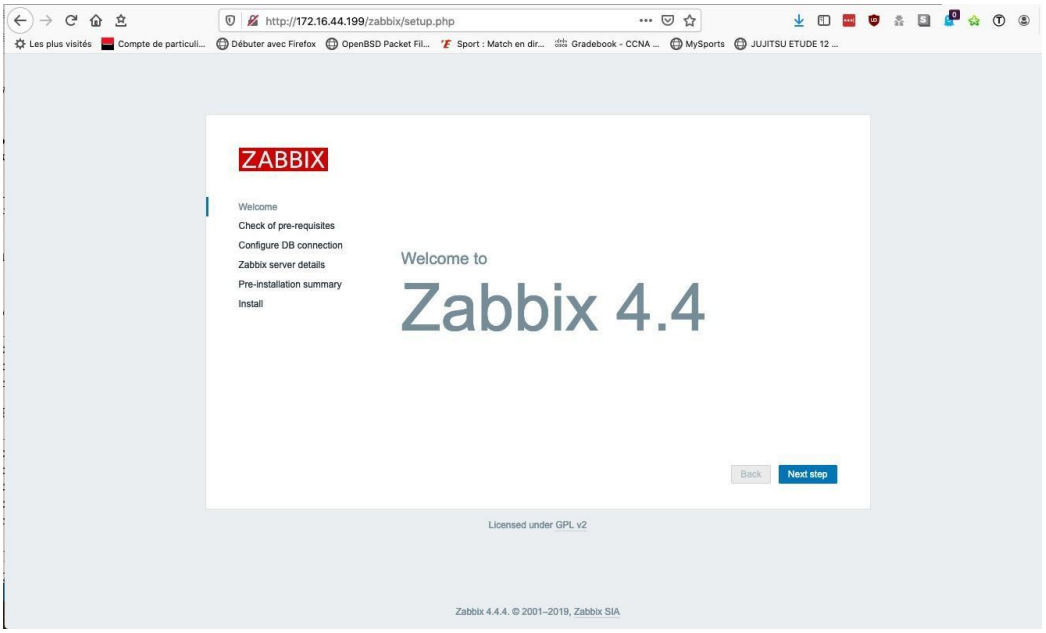
Redémarrer le service Apache 2 pour prendre en compte les modifications apportées

Attention ! Réaliser un snapshot de la machine virtuelle à la fin de cette étape.

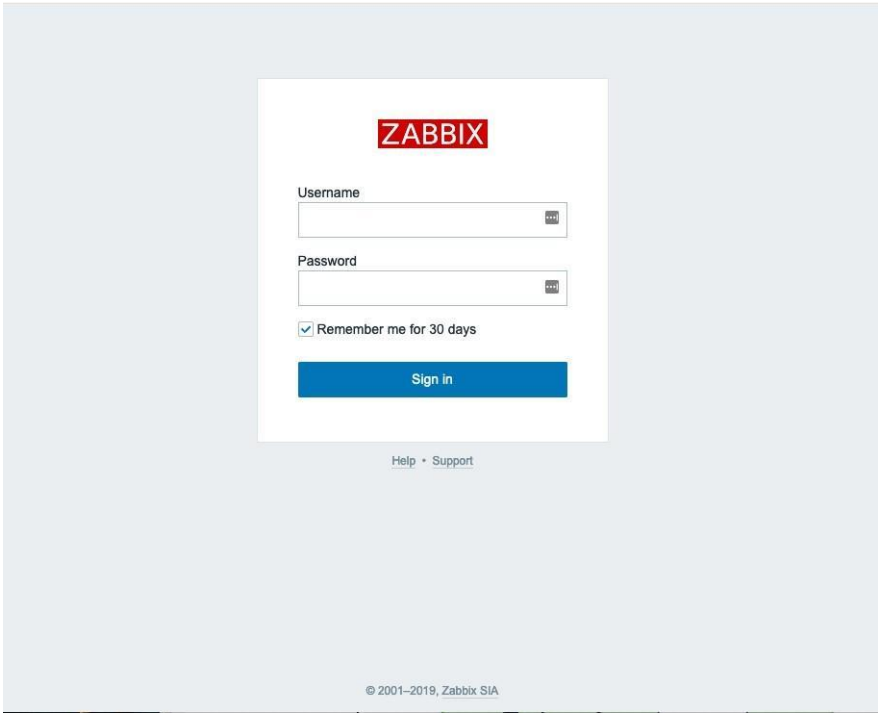
C. Accès à l'interface web d'administration

Pour vous connecter sur l'interface web de gestion du serveur Zabbix, entrez l'URL suivante dans votre navigateur préféré :

http://SERVER_IP/zabbix

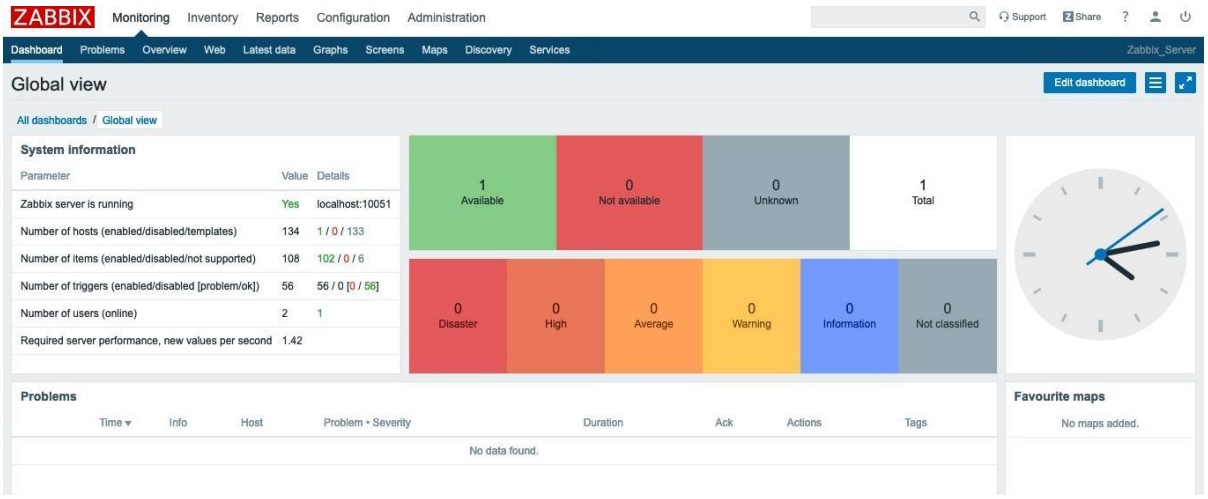


Après avoir passé la phase d'initialisation de l'interface vous devriez vous retrouver sur la page d'authentification. Par défaut le login est admin et le mot de passe zabbix.



D. Configuration de base de l'interface d'administration de Zabbix

1. Changer le mot de passe de l'utilisateur Admin en azerty2QWERTY.
2. Basculer la langue en Français.



Enfin pour terminer ce TP, cliquer sur le menu Surveillance, puis Dernières Données et Sélectionner le serveur Zabbix puis cliquer sur Appliquer.

Analyser le résultat obtenu.

Available memory pour savoir la RAM disponible

Checksum of /etc/pasword pour verifier si le mot de passe n’a pas été modifier.

System looktime /description/localtime pour les infos système.

Numbers of CPUs pour le nombre de coeur du processeurs.

Attention ! Réaliser un snapshot de la machine virtuelle à la fin de cette étape.

Vous avez désormais un serveur de supervision Zabbix fonctionnel et prêt à l’emploi !

TP 5 – Prise en main du serveur de supervision Zabbix
Bloc 2 – BTS SIO 2

Objectifs :

- Être capable d'effectuer une première prise en main de l'outil de supervision Zabbix.
- Comprendre le fonctionnement et la structure de l'outil Zabbix.
- Réaliser une première supervision simple de service réseau et de systèmes d'exploitation.

Prérequis :

- Savoir préconfigurer un serveur Debian 11 afin d'installer un service spécifique.
- Être capable d'installer un outil de supervision de réseaux et de services.
- Être capable de paramétrer intégralement un outil de supervision.

Attention ! Lors de toute la durée de la séquence sur la supervision avec Zabbix, vous devrez vous référer à la documentation officielle ou celle fournie par votre enseignant et non sur des tutoriels trouvés au hasard sur le Net. Il faut choisir une documentation en fonction du niveau de fiabilité de cette dernière.

https://www.zabbix.com/documentation/6.0/

Avant de démarrer ! Vous devez toujours avoir à l'esprit les éléments de réflexion suivants : A chaque étape, VOUS DEVEZ effectuer les recherches qui s'imposent afin de clarifier chaque terme, chaque fonction, chaque module qui est énoncé. Rien ne sert de courir et d'enchaîner les commandes si vous ne comprenez rien à ce que vous faîtes !

A. Gestion des utilisateurs

Le respect des bonnes pratiques vous oblige à ne pas utiliser de compte générique Administrateur et de privilégier des comptes nominatifs.

1. Créez-vous un compte nominatif à l'aide de l'interface d'administration Zabbix. Votre utilisateur devra être Administrateur. Vous vous assurerez que votre profil est bien en français et que la remontée de toutes les alertes est bien effective pour votre nouveau compte.

Attention ! Réaliser un snapshot de la machine virtuelle à la fin de cette étape.

B. Mise en place de vérifications réseaux simples

Si vous souhaitez juste vérifier le bon fonctionnement réseau d'un hôte (ICMP écho) ou d'un service (SSH, HTTP, HTTPS, FTP), il n'est nullement nécessaire d'installer un agent Zabbix ou d'utiliser le service SNMP.

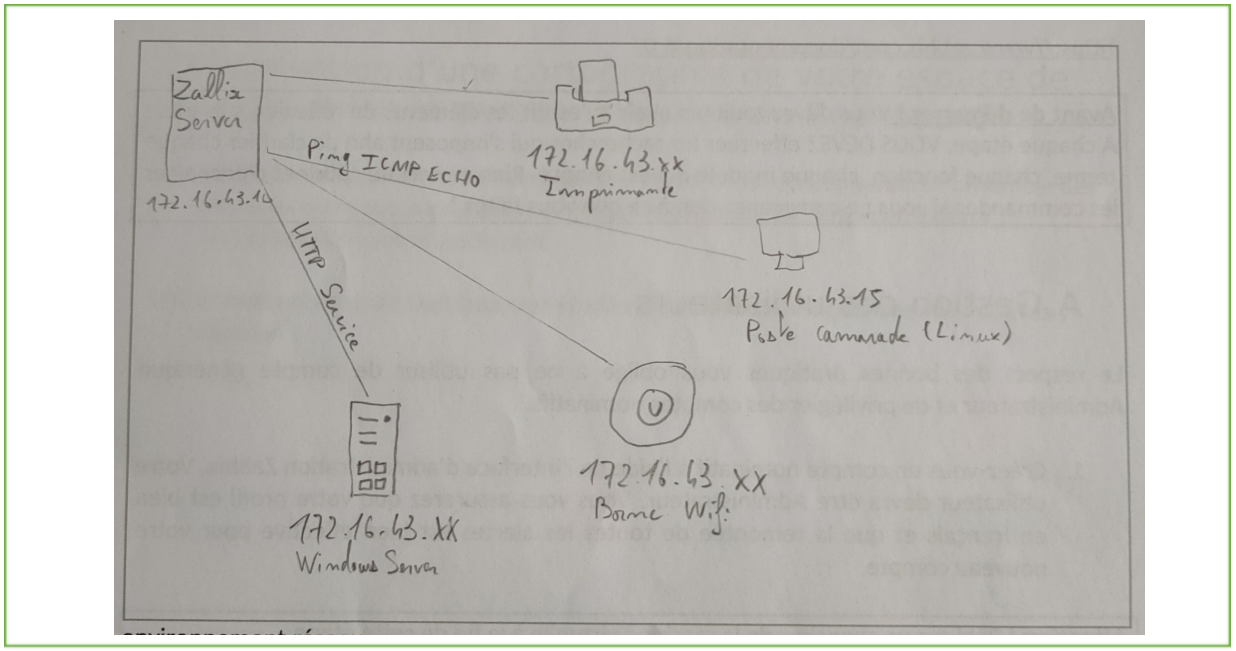
Via le serveur Zabbix, vous pouvez mettre en œuvre une supervision simple via le protocole ICMP ou TCP/UDP.

2. Créer un nouvel hôte qui représentera votre passerelle (172.16.47.254). Créer un nouvel élément vous permettant de vérifier que cette dernière répond au Ping (ICMP ECHO). En cas de succès, la valeur retournée sera égale à 1. En cas d'échec, la valeur retournée sera égale à 0. Créer un déclencheur permettant de lancer une alerte en cas d'échec du ping.

3. Déployer une nouvelle VM Debian qui disposera d'une adresse IP fixe sur le VLAN pédagogique. Puis superviser le service SSH de cette dernière toutes les 30 secondes en utilisant les mêmes étapes que pour l'hôte précédent (création d'un hôte, d'un élément et d'un déclencheur). Couper le service SSH sur la VM Debian et vérifier qu'une alerte remonte bien sur votre outil de supervision.

Aide ! Si vous devez superviser plusieurs services réseaux, il est possible de cloner des éléments et de modifier uniquement le numéro de port ou le nom de service afin de gagner du temps.

4. Dessinez une maquette incluant tous les éléments que vous souhaitez superviser à l'aide de vérifications réseaux simples.



En vous référant à votre schéma, essayez de superviser tout ce qui se trouve dans votre environnement réseau :

- Serveurs Windows et GNU/Linux de la section
- Imprimante
- Borne Wifi
- Les postes ou VM de vos camarades.

Aide ! Au lieu de devoir créer systématiquement des éléments et des déclencheurs, il existe des modèles que vous pouvez lier à vos hôtes afin de gagner en rapidité et en efficacité.

Si vous faîtes le choix d'utiliser des modèles, explorez en détail les paramètres des éléments et des déclencheurs qui seront liés à ces derniers. Prenez en note ce qui vous parait important.

Attention ! Réaliser un snapshot de la machine virtuelle à la fin de cette étape.

C. Supervision de systèmes Windows et GNU/Linux à l'aide de l'agent Zabbix

Il est possible de superviser ce type d'OS à l'aide du protocole SNMP mais il est conseillé lorsque cela est possible de passer par l'agent dédié Zabbix. Cet agent sera installé sur l'élément supervisé et permettra de fournir des informations intéressantes sur le système et les applications de façon optimisée (et chiffrée si on le souhaite).

La documentation concernant l'agent Zabbix et les valeurs que l'on peut tester avec sont présents via l'URL :
https://www.zabbix.com/documentation/6.0/fr/manual/config/items/itemtypes/zabbix_agent

Vous devez avoir à disposition une machine virtuelle Windows 2019 Server, une VM Debian 11 et une VM Windows 10 en plus de votre serveur de supervision.

5. Installez un agent Zabbix sur chaque machine à superviser et configurez-le correctement.

6. Sur la VM Debian, installez un service web Apache2. Puis à l'aide de l'agent, créez des éléments afin de superviser le port 80 TCP, d'obtenir le nom de la machine et de mesurer le trafic entrant sur la carte réseau. Observez le graphique généré par la mesure.

7. Sur le serveur de supervision, installez l'outil zabbix-get et réalisez des tests afin de récupérer un certain nombre de valeurs et vous assurez que la communication entre le serveur et l'agent zabbix du client est bien fonctionnnel.

   Ex : $ zabbix_get -s 172.16.4X.XXX -k system.hostname
   $ zabbix_get --help

8. Supervisez la VM Windows 10 à l'aide du modèle Template OS Windows by Zabbix agent. Que permet de superviser ce modèle ? Quel est la limite de ce type de configuration ?

   Ce modèle permet de suppervisé plusieurs information système, tels que la RAM, le processeur, la taille disponible du disque dur, le debits réseau.

9. Supervisez la VM Windows 2019 Server afin d'obtenir l'espace disque disponible sur ce dernier. Une alerte de type Moyen doit être levée lorsque 70% de l'espace disque sera utilisée, puis une alerte de type Haut lorsque 90% de l'espace sera utilisée puis une alerte de type désastre lorsque 100% de l'espace disque sera occupée.

10. Créez un modèle pour la supervision de tous vos serveurs GNU/Linux où vous vérifierez l'espace disque utilisé, la mémoire vive et le CPU utilisés, le trafic entrant et sortant sur votre carte réseau et la réponse aux requêtes ICMP écho. Puis appliquez-le aux hôtes appropriés.

11. Faîtes-vous plaisir et supervisez tout ce qui vous semble nécessaire à l'aide de l'agent Zabbix (Windows, GNU/Linux, *BSD).

12. BONUS : Paramétrez le serveur et l'agent afin que les communications entre eux soient chiffrées.

D. Réalisation d'une cartographie de votre espace de supervision et personnalisation du Dashboard

13. Réalisez une première carte nommée lan-SIO où vous ferez apparaître l'ensemble des éléments que vous avez supervisés depuis le début du TP. Cette carte devra apparaître dans votre Dashboard.

14. Personnalisez votre Dashboard et étudiez les différents Widgets que vous pouvez y déposer.

TP 6 – Utilisation du protocole SNMP avec Zabbix
Bloc 2 – BTS SIO 2

Objectifs :	Prérequis :
Savoir configurer le service SNMP sur des systèmes et des éléments réseaux actifs. Superviser des hôtes à l'aide du protocole SNMP. Comprendre le fonctionnement de ce protocole.	Être capable d'effectuer une première prise en main de l'outil de supervision Zabbix. Comprendre le fonctionnement et la structure de l'outil Zabbix. Réaliser une première supervision simple de service réseau et de systèmes d'exploitation.

Attention ! Lors de toute la durée de la séquence sur la supervision avec Zabbix, vous devrez vous référer à la documentation officielle ou celle fournie par votre enseignant et non sur des tutoriels trouvés au hasard sur le Net. Il faut choisir une documentation en fonction du niveau de fiabilité de cette dernière.

https://www.zabbix.com/documentation/5.0/fr/manual

Avant de démarrer ! Vous devez toujours avoir à l'esprit les éléments de réflexion suivants : A chaque étape, VOUS DEVEZ effectuer les recherches qui s'imposent afin de clarifier chaque terme, chaque fonction, chaque module qui est énoncé. Rien ne sert de courir et d'enchaîner les commandes si vous ne comprenez rien à ce que vous faîtes !

A. Préambule

Notre serveur de Supervision demande donc à d'autres serveurs de lui fournir des informations sur l'état de leur processeur, de leur disque, de leur mémoire, … Imaginez ce qui pourrait se passer si nos serveurs se mettaient à répondre automatiquement à n'importe quel "premier venu" pour lui fournir ce type de renseignements… La sécurité de nos serveurs serait immédiatement gravement mise en danger. C'est donc un processus normal qui fait que nos serveurs, bien que sollicités par Zabbix via le protocole SNMP, ne lui répondent pas de manière automatique. Autant le PING, s'il est toléré par le pare-feu local va obtenir une réponse (protocole ICMP), autant l'information de l'état d'un CPU, … ne peut pas transiter seule et sans contrôle sur un réseau.

Le but du protocole SNMP (ports UDP 161 et 162) de véhiculer tous ces types d'informations surtout dans le cas d'équipements où l'agent Zabbix ne peut être installé (Switch, Routeur, Téléphone IP, Onduleur, Borne Wifi).

Il est par contre indispensable que chacun des deux partenaires parle le même langage, n° de version de SNMP, nom de la communauté commune, type d'accès ro ou rw.

> **Attention !** SNMP version 1 n'est pas du tout sécurisé. Il faut éviter de l'utiliser sauf si aucune autre alternative est possible. SNMP v3 est très sécurisé (SSL/TLS), il est préférable de le mettre en œuvre. Le bémol est que trop peu d'éléments actifs réseaux ne supportent pas cette version.

Nous utiliserons donc dans ce TP le version 2c de SNMP généralement disponible sur la quasi-totalité des éléments à superviser.

B. Activation et configuration de SNMP sur les hôtes que vous souhaitez superviser

Debian GNU/Linux

1. Installer le paquet snmpd à l'aide de la commande apt

   apt install snmpd

2. Configurer l'agent SNMP fraîchement installé à l'aide de son fichier de configuration

   nano /etc/snmp/snmpd.conf

3. Vérifier un certain nombre de paramètres afin que le service SNMP soit opérationnel

```
agentAddress udp:161,udp6:[::1]:161
 rocommunity public default
sysLocation Lycée Sainte-Marguerite – SIO
sysContact QDemouliere <quentin.demouliere@ac-orleans-tours.fr>
```

4. Enfin redémarrez le service SNMP pour prendre en compte les modifications.

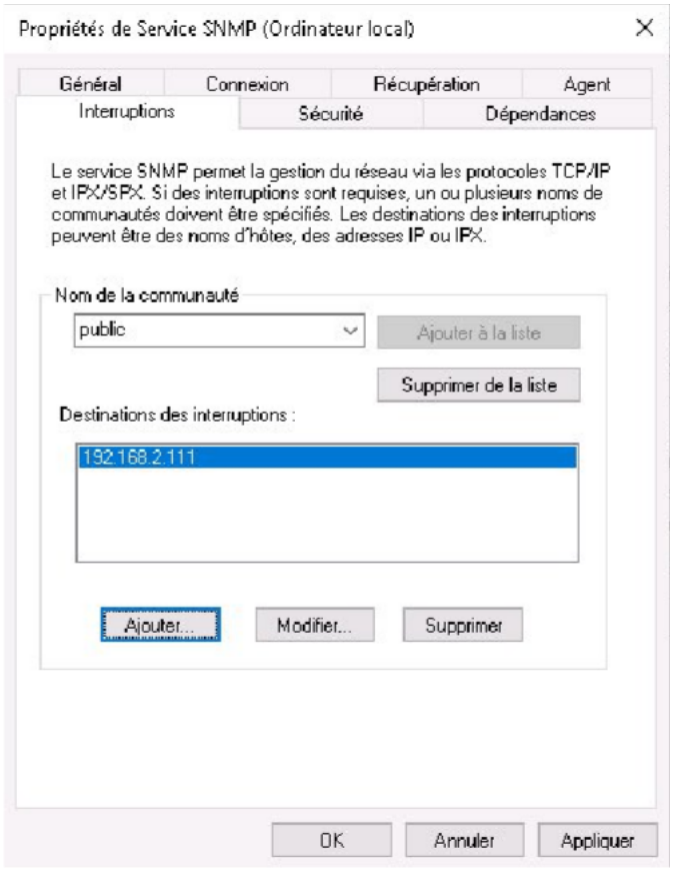
   systemctl restart snmpd

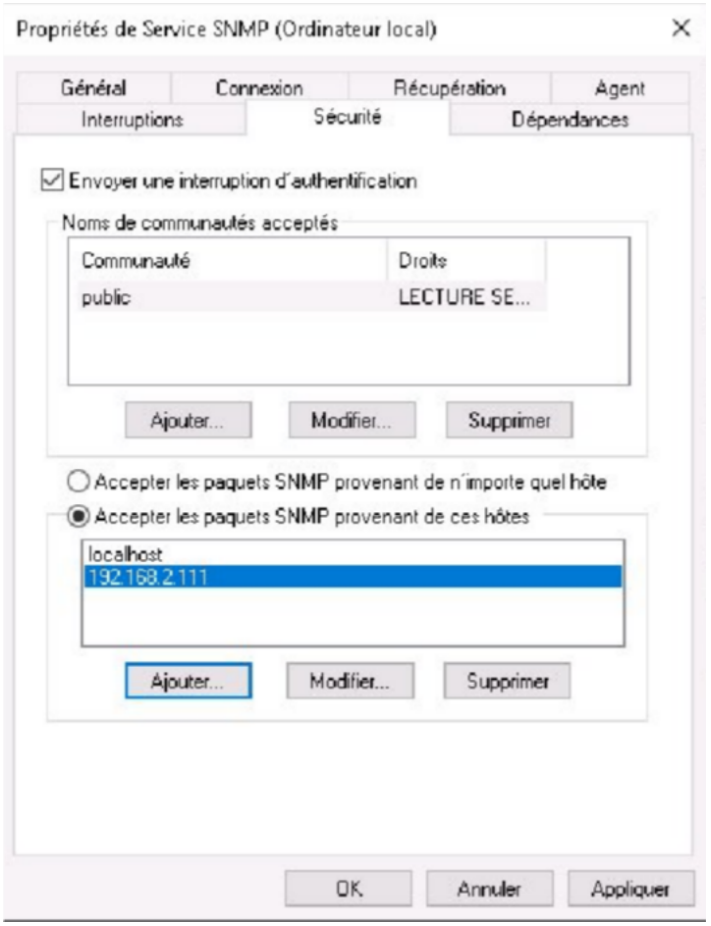
Windows 2016 Server

Pour installer le service SNMP, ouvrez l'assistant d'ajout de rôles et de fonctionnalités et cochez Service SNMP dans le menu Fonctionnalités. Valider l'installation.

Vérifier l'état du service. Ce dernier doit être démarré de manière automatique puis paramétrez-le pour indiquer une communauté publique ainsi qu'un contact et une adresse de serveur de supervision.

Assurez-vous que votre pare-feu Windows autorise le trafic SNMP entrant et sortant et créez les règles de filtrage nécessaires si besoin. Redémarrez le service pour appliquer les modifications.


Propriétés de Service SNMP (Ordinateur local)
Général
Connexion
Récupération
Agent
Interruptions
Sécurité
Dépendances
Le service SNMP permet la gestion du réseau via les protocoles TCP/IP et IPX/SPX. Si des interruptions sont requises, un ou plusieurs noms de communautés doivent être spécifiés. Les destinations des interruptions peuvent être des noms d'hôtes, des adresses IP ou IPX.
Nom de la communauté
public
Ajouter à la liste
Supprimer de la liste
Destinations des interruptions :
192.168.2.111
Ajouter...
Modifier...
Supprimer
OK
Annuler
Appliquer


Propriétés de Service SNMP (Ordinateur local)
Général
Connexion
Récupération
Agent
Interruptions
Sécurité
Dépendances
Envoyer une interruption d'authentification
Noms de communautés acceptés
Communauté
Droits
public
LECTURE SE...
Ajouter...
Modifier...
Supprimer
Accepter les paquets SNMP provenant de n'importe quel hôte
Accepter les paquets SNMP provenant de ces hôtes
localhost
192.168.2.111
Ajouter...
Modifier...
Supprimer
OK
Annuler
Appliquer

Commutateurs et routeurs Cisco

À l'aide d'Internet et de la documentation officielle Cisco (www.cisco.com), activez le service SNMP en n'oubliant pas d'être en Read-Only avec la communauté publique.

Notez les commandes que vous avez tapées sur le routeur et sur le commutateur pour mener à bien l'opération.

snmp-server community antonin RO
exit
write
sh run

Imprimantes réseaux ou d'autres types d'équipement

1. Sur l'équipement, activer le protocole SNMP (par le menu intégré de l'imprimante ou bien, le cas échéant, par l'interface web de configuration de l'imprimante).

2. Configurer l'agent SNMP par le menu de l'équipement ou par son interface web.

3. Vérifier que le paramètre community est configuré à public (le nom de votre communauté SNMP en minuscules).

C. Mise en œuvre de la supervision d'hôte à l'aide de SNMP

Vous devez superviser sur votre serveur Zabbix un routeur Cisco de TP, un commutateur Cisco de TP, un Windows Server 2016, un Debian GNU/Linux.

Installez le paquet snmp (le client) sur le serveur de supervision. Puis testez que l'accès SNMP à vos différents hôtes est bien opérationnel à l'aide de la commande :

Si SNMP est correctement paramétré sur votre hôte à superviser, vous devriez obtenir un message de ce type :

```
[UDP: [172.16.44.198]:161->[0.0.0.0]:48256]=>[Linux debianzbx-qd 4.19.0-6-amd64 #1 SMP
 Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64] Up: 0:00:03.57
Interfaces: 0, Recv/Trans packets: 0/0 | IP: 0/0
```

Créez les hôtes dans votre outil de supervision et veillez bien à ce qu'ils soient configurés avec SNMP. Vérifiez qu'ils soient opérationnels.

Appliquez le modèle qui vous semble le plus approprié à chacun puis analysez quels sont les éléments qui sont sollicités ainsi que les déclencheurs qui soulèveront des alarmes. Expliquez quelles sont les données remontées à l'aide de ces modèles et quelles alarmes seront déclenchées.

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Réalisez une capture de trame entre le serveur et l'agent SNMP et observez les échanges réalisés avec ce protocole.

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

D. Utilisation personnalisée des modèles et du protocole SNMP

Nous avons utilisé les modèles préinstallés dans l'outil de supervision. L'avantage de l'utilisation de ces modèles est la rapidité de déploiement. L'inconvénient réside dans le manque de personnalisation.

Ainsi vous devez trouver une méthode afin de superviser un hôte Debian GNU/Linux en respectant les critères suivants :

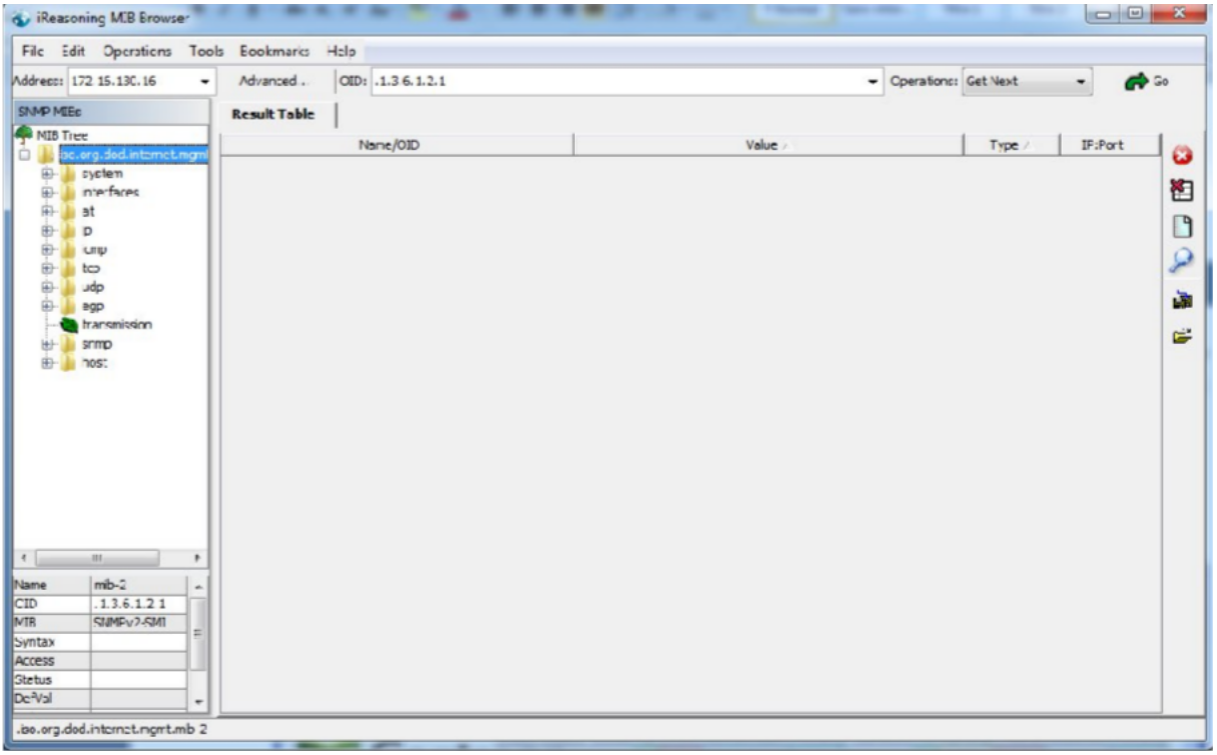
1. Superviser le trafic de la carte réseau.
2. Superviser le processus sshd sur la machine. Nous voudrions obtenir une alerte Haute si le nombre de processus SSH est strictement inférieur à 1 ou strictement supérieur à 7.
3. La racine de votre serveur (/) doit être supervisée. Nous voulons savoir combien de place il reste en pourcentage sur cette dernière.

Sur votre commutateur Cisco nous voudrions pouvoir superviser le débit passant par les différentes interfaces de celui-ci. Nous voudrions savoir également quelles interfaces sont allumées ou éteintes.

Aide ! Il est possible d'utiliser, ou dupliquer des templates existants afin de vous aider. Analyser les aussi pour voir comment fonctionne leurs éléments et leurs déclencheurs.

E. Utiliser un outil de type MIB Browser

Sur vos postes clients de type Windows 10, téléchargez et installez un MIB Browser comme la version Personnal Edition de iReasoning MIB Browser : http://ireasoning.com/mibbrowser.shtml.



L'intérêt de cet outil est de pouvoir déterminer quel est le N° d'O.I.D. identifiant chaque paramètre d'un système ou d'une machine.

Il existe d'abord des MIBs universelles et normalisées qui sont déjà intégrées dans le MIB Browser et visualisables dans l'explorateur de MIB à gauche de la fenêtre : parcourez-les et vous comprendrez vite ce qu'elles identifient, chacune. Par exemple, pour savoir depuis combien de temps (en centièmes de secondes !) un système est en fonction ?

.....

.....

.....

Il existe ensuite des MIBs standardisées mais qu'il vous faut ajouter vous-mêmes dans le MIB Browser et qui deviendront alors elles aussi visualisables dans l'explorateur de MIB à gauche de la fenêtre ; si, par exemple, vous souhaitez interroger par SNMP des imprimantes de votre organisation, il vous faut importer une MIB standardisée qui identifie les paramètres communs à toutes les imprimantes de la planète, quelle que soit son type, son fabricant, ou son modèle.

Ainsi, récupérez sur Internet les MIBS de votre commutateur Cisco, de votre imprimante réseau et du firewall Stormshield SN310. Puis intégrez-les à votre MIB Browser. Prenez le temps d'analyser les résultats et les différents paramètres accessibles.

À l'aide du serveur Zabbix, mesurez le niveau de toner de l'imprimante réseau de la section (trouver son OID dans le navigateur de MIB, puis créer un hôte dans Zabbix avec un élément de type SNMP est l'OID qui représente l'information que l'on souhaite).

Mesurez combien de paquets ICMP ont déjà été envoyés à l'interface de management (VLAN correspondant) de l'un de vos switchs de TP.

Pour votre Firewall Stormshield, vous devez récupérer le nom de l'appliance, la version de SNS utilisée et le trafic entrant et sortant de votre interface in. En cas de 3 échecs successifs au ping, une alerte doit être levée.