ZABBIX

L'objectif de ce TP est de superviser le réseau M2L en utilisant le protocole SNMP via le programme Zabbix.

Le protocole SNMP (Simple Network Management Protocol), est un protocole de couche 7 du modèle OSI utilisant les ports 161 et 162 en UDP.

Ce protocole permet à une application de gestion (ici, Zabbix), de demander des informations à des machines clientes (ordinateurs, routeurs, switches, firewall, …) que l'on veut superviser.

Le SNMP utilise des OID, qui sont des identifiants d'objets, permettant d'identifier de manière unique l'information que nous recherchons.

Par exemple, l'OID 1.3.6.1.2.1.2.2.1.10 permet d'identifier l'objet représentant le trafic reçu sur l'interface d'un switch.

Le protocole SNMP fonctionne grâce à des « communautés », que l'on autorise en lecture et/ou écriture sur la machine à superviser, afin que le serveur puisse communiquer avec cette machine, cela joue un rôle d'identifiant. Sans savoir la communauté, l'application de gestion ne pourra pas récupérer les informations de la machine cliente.

Au fil du temp, trois versions de ce protocole ont vu le jour, ajoutant plus de sécurité :

Feature	SNMPv1	SNMPv2c	SNMPv3
Get	Yes	Yes	Yes
GetNext	Yes	Yes	Yes
Set	Yes	Yes	Yes
GetBulk	No	Yes	Yes
Trap	Yes	Yes	Yes
Inform	No	Yes	Yes
Community strings	Yes	Yes	No
User based secuirty	No	No	Yes
Message authentication	No	No	Yes
Message encryption	No	No	Yes

Mise en place de la supervision

1. Installation de Zabbix Server sur Ubuntu 22.04 :

Installer apache et un serveur mysql et activer les services au démarrage

```
root@ray-zabbix:/home/rayan# systemctl enable mysql
Synchronizing state of mysql.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable mysql
root@ray-zabbix:/home/rayan# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
root@ray-zabbix:/home/rayan# systemctl start apache2
root@ray-zabbix:/home/rayan# systemctl start mysql
root@ray-zabbix:/home/rayan# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-03-15 22:51:02 UTC; 18s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 13701 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 13712 (apache2)
      Tasks: 55 (limit: 2234)
     Memory: 5.2M
        CPU: 26ms
     CGroup: /system.slice/apache2.service
             ├─13712 /usr/sbin/apache2 -k start
             ├─13713 /usr/sbin/apache2 -k start
             └─13714 /usr/sbin/apache2 -k start

mars 15 22:51:02 ray-zabbix systemd[1]: Starting The Apache HTTP Server...
mars 15 22:51:02 ray-zabbix apachectl[13711]: AH00558: apache2: Could not reliably determine the server's fully qualifi
mars 15 22:51:02 ray-zabbix systemd[1]: Started The Apache HTTP Server.
lines 1-17/17 (END)
systemctl status mysql
● mysql.service - MySQL Community Server
     Loaded: loaded (/lib/systemd/system/mysql.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-03-15 22:51:11 UTC; 15s ago
    Process: 13771 ExecStartPre=/usr/share/mysql/mysql-systemd-start pre (code=exited, status=0/SUCCESS)
   Main PID: 13779 (mysqld)
     Status: "Server is operational"
      Tasks: 39 (limit: 2234)
     Memory: 365.2M
        CPU: 811ms
     CGroup: /system.slice/mysql.service
             └─13779 /usr/sbin/mysqld

mars 15 22:51:10 ray-zabbix systemd[1]: Starting MySQL Community Server...
mars 15 22:51:11 ray-zabbix systemd[1]: Started MySQL Community Server.
root@ray-zabbix:/home/rayan#
```

Installer le dépôt officiel Zabbix :

wget https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.4-1+ubuntu22.04_all.deb
dpkg -i zabbix-release_6.4-1+ubuntu22.04_all.deb
apt update

```
Réception de :20 http://fr.archive.ubuntu.com/ubuntu jammy-backports/main Translation-en [9 800 B]
Réception de :21 http://fr.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [14,0 kB]
Réception de :22 http://fr.archive.ubuntu.com/ubuntu jammy-security/main Translation-en [142 kB]
root@ray-zabbix:/home/rayan#
Réception de :24 http://fr.archive.ubuntu.com/ubuntu jammy-security/universe Translation-en [114 kB]
Réception de :25 http://fr.archive.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [996 B]
Réception de :26 https://repo.zabbix.com/zabbix/6.4/ubuntu jammy/main Sources [1 939 B]
Réception de :27 https://repo.zabbix.com/zabbix/6.4/ubuntu jammy/main amd64 Packages [5 490 B]
Reading package lists... Done
```

On peut voir ici que les informations du dépôt Zabbix nous sont biens parvenus.

Installation de Zabbix serveur, sa page WEB et son agent.

(En plus d'utiliser le protocole SNMP, Zabbix propose son propre agent installable sur les machines à superviser, cela permet d'avoir une certaine continuité en cas de soucis avec le protocole SNMP.)

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

Création de la BDD et de l'utilisateur pour Zabbix :

Nom de la BDD : zabbix
User : zabbix
MDP : Erty1234

```
root@ray-zabbix:/home/rayan# mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.32-0ubuntu0.22.04.2 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0,13 sec)

mysql> create user zabbix@localhost identified by 'Erty1234';
Query OK, 0 rows affected (0,02 sec)

mysql> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0,34 sec)

mysql> set global log_bin_trust_function_creators = 1;
Query OK, 0 rows affected (0,00 sec)

mysql> quit;
Bye
```

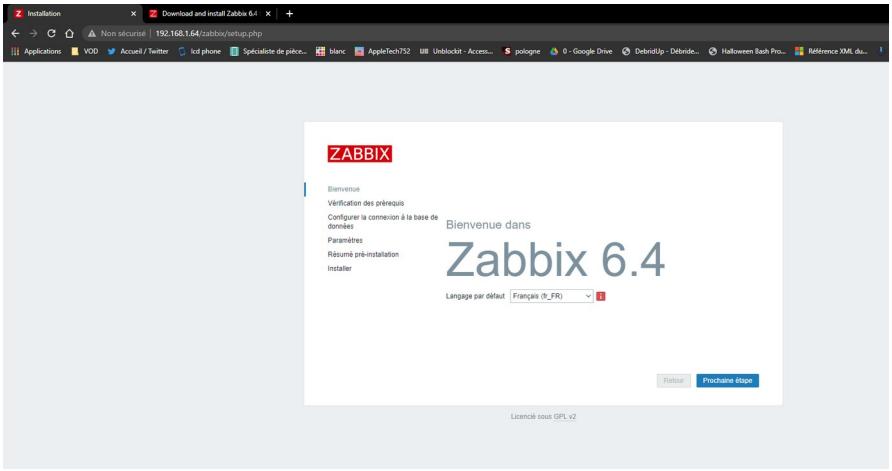
Importer le schéma initial de la BDD, puis vérification que l'importation à bien été faite.

```
root@ray-zabbix:/home/rayan# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8 |
mb4 -uzabbix -p zabbix
Enter password:
root@ray-zabbix:/home/rayan# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
Server version: 8.0.32-0ubuntu0.22.04.2 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use zabbix
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+----------------------------+
| Tables_in_zabbix           |
+----------------------------+
| acknowledges               |
| actions                    |
| alerts                     |
| auditlog                   |
| autoreg_host               |
| changelog                  |
| conditions                 |
| config                     |
| config_autoreg_tls         |
| connector                  |
| connector_tag              |
```

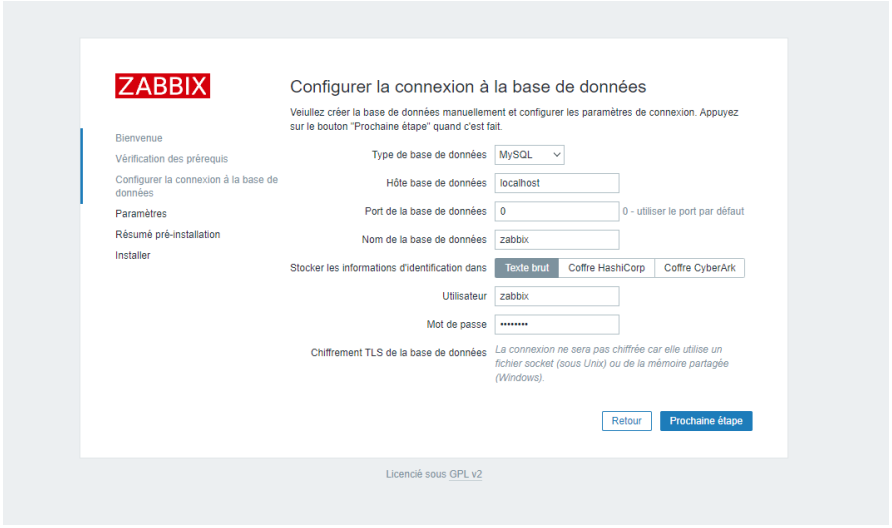
Afin que le serveur Zabbix puisse se connecter à la base de données, on spécifie dans le fichier /etc/zabbix/zabbix_server.conf, le nom de la base, le nom de l'utilisateur mysql ainsi que son mot de passe.

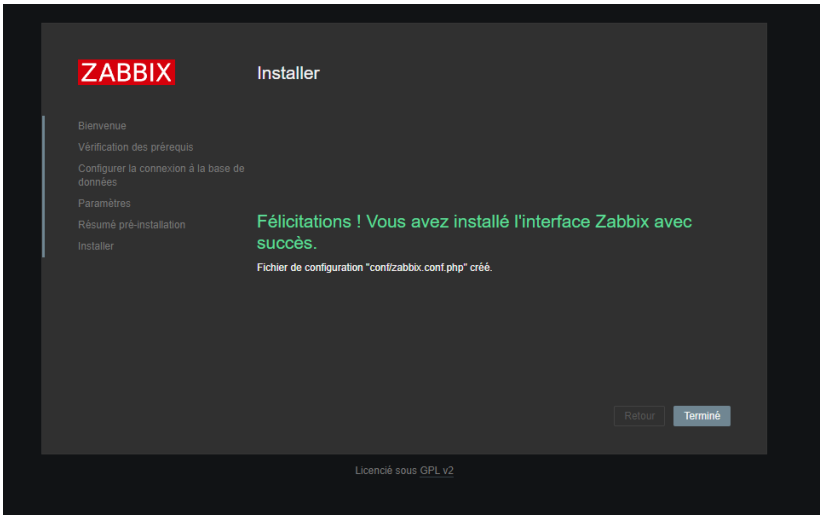
```
root@ray-zabbix: /home/rayan
  GNU nano 6.2                                  /etc/zabbix/zabbix_server.conf *
#
# Mandatory: no
# Default:
# DBUser=

DBUser=zabbix

### Option: DBPassword
#       Database password.
#       Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=Erty1234

### Option: DBSocket
#       Path to MySQL socket.
#
```

Après avoir redémarrer les services zabbix-server zabbix-agent apache2 et les avoir activés au démarrage (« service enable ... »), on peut accéder à la page web en tapant l'@IP/zabbix :



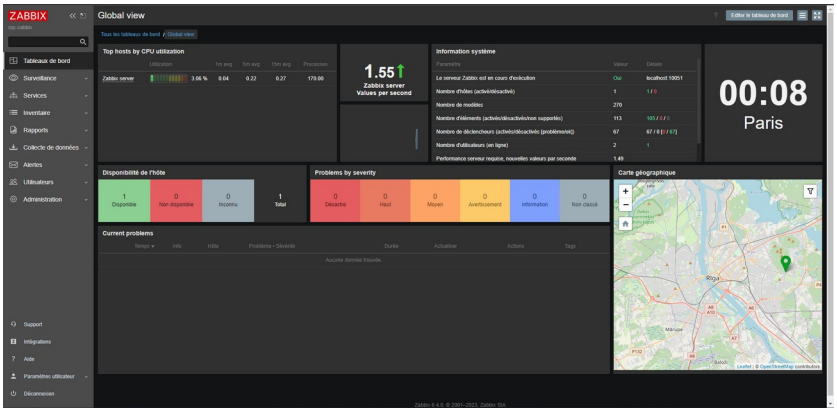
Ici, on nous demande les informations de la BDD :





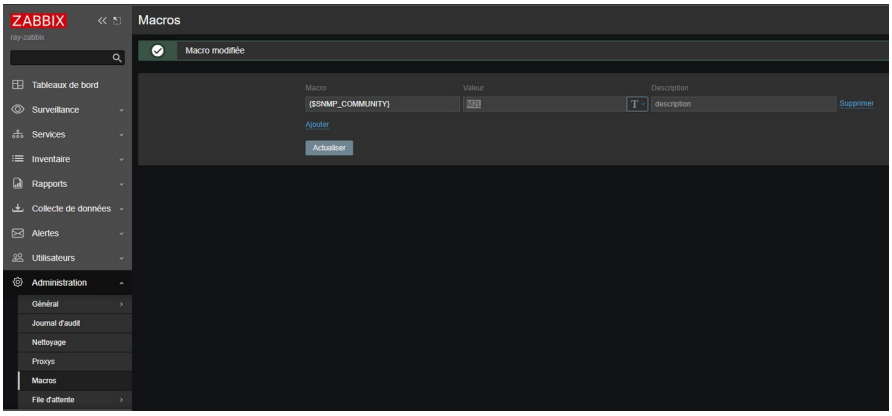
Les identifiants par défauts sont :

User : Admin
Password : zabbix
Nous voilà enfin sur l’interface de Zabbix :



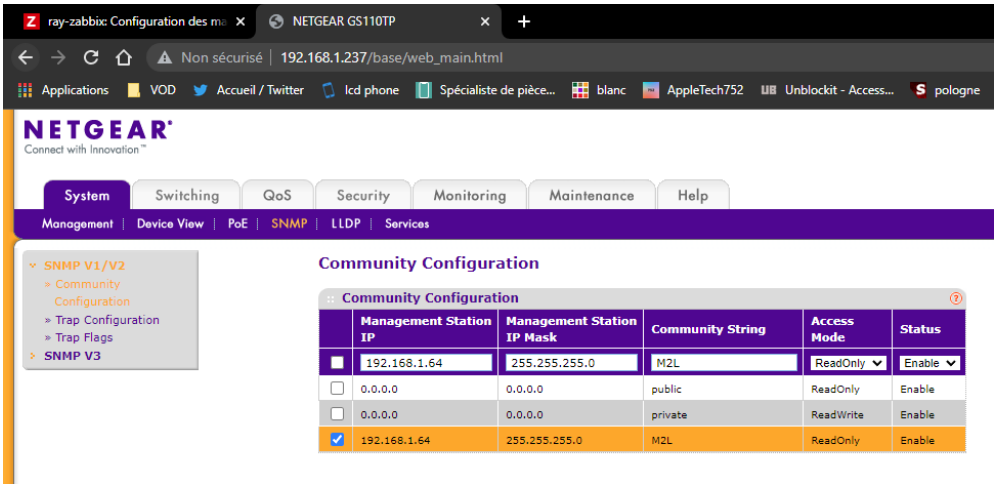
Etant donné que nous allons utiliser le protocole SNMP dans le cadre de cette mission, nous allons spécifier une communauté SNMP à utiliser pour tous les hôtes afin de faciliter la création d'hôtes.

« Administration », « Macros » puis pour la variable {$SNMP_COMMUNITY}, saisir « M2L » dans « Valeur ». « M2L » sera le nom de la communauté par défaut à la création d'un hôte, c'est cette communauté qu'il faudra inscrire sur chaque client.



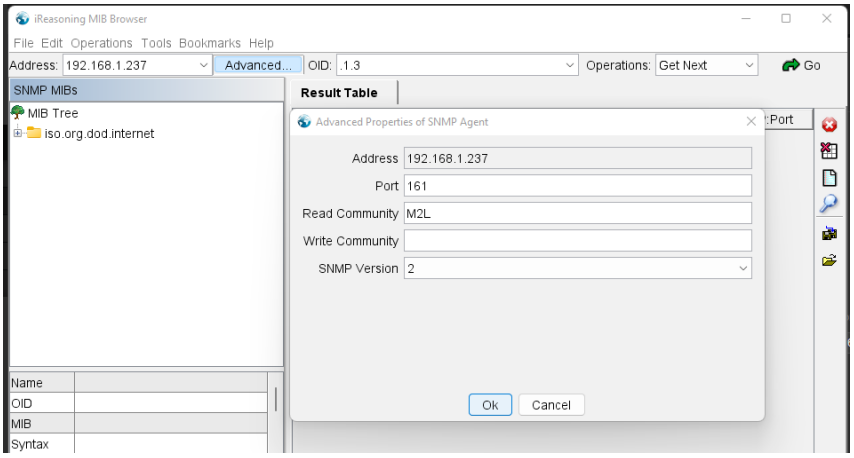
Supervision du Switch Netgear

Sur l'interface d'administration du switch dans l'onglet « System » puis « SNMP », il est possible d'y ajouter les communautés. On va donc y rajouter la communauté M2L avec l'adresse IP du serveur pouvant agir sur cette communauté SNMP :

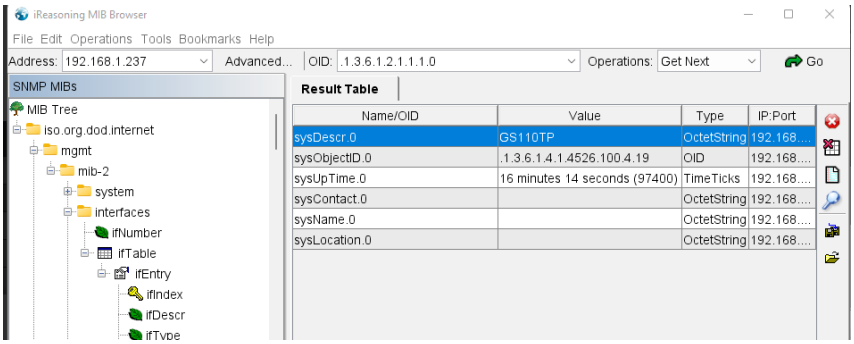


Afin de s'assurer que le SNMP fonctionne bien sur le switch, on utilise « MIB Browser » afin de vérifier si l'on récupère bien des informations sur le Switch :

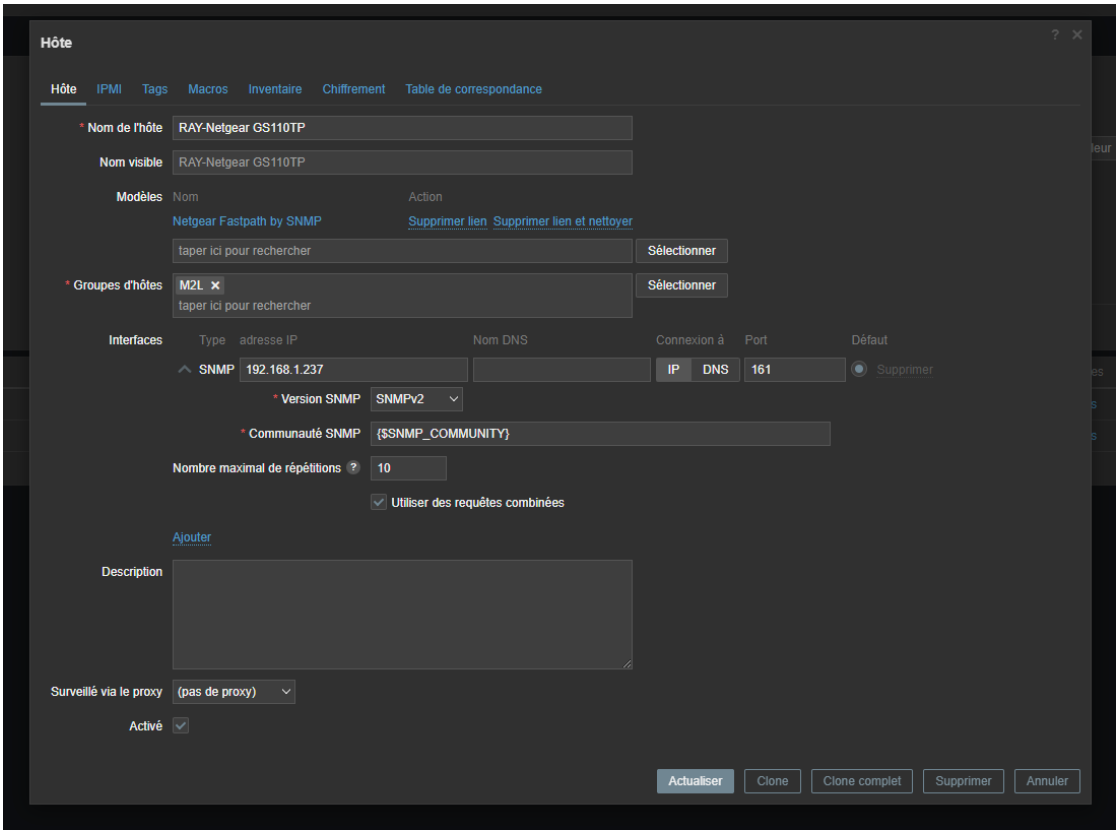
Ici, on entre les informations du client (l'adresse IP, la communauté ainsi que la version du SNMP)



Ici, nous recevons les réponses du client nous renvoyant ses informations.



Une fois cette vérification effectuée, nous sommes sûr que le SNMP à bien été configura côté client, on peut donc rajouter l'hôte sur le serveur Zabbix dans « Surveillance », « Hôte », « Créer un hôte » :



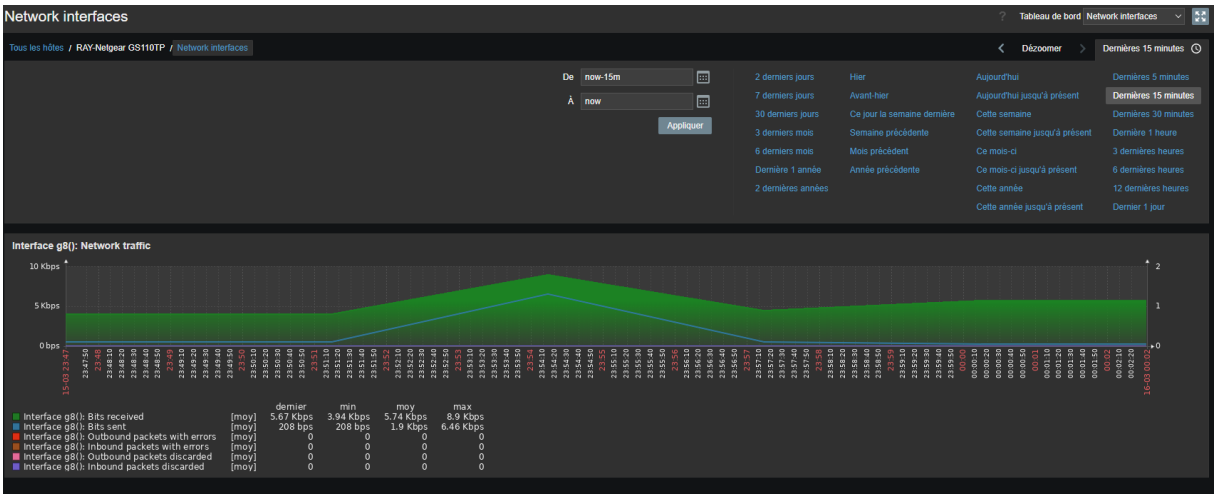
Dans modèle, on va aller dans le groupe Template/Network puis récupérer le Template Netgear installé par défaut sur le serveur.

Dans interfaces, nous allons ajouter le protocole SNMP en précisant l'@IP. La variable {$SNMP_COMMUNITY} ayant été configurée précédemment, nous n'avons pas besoin de la modifier.

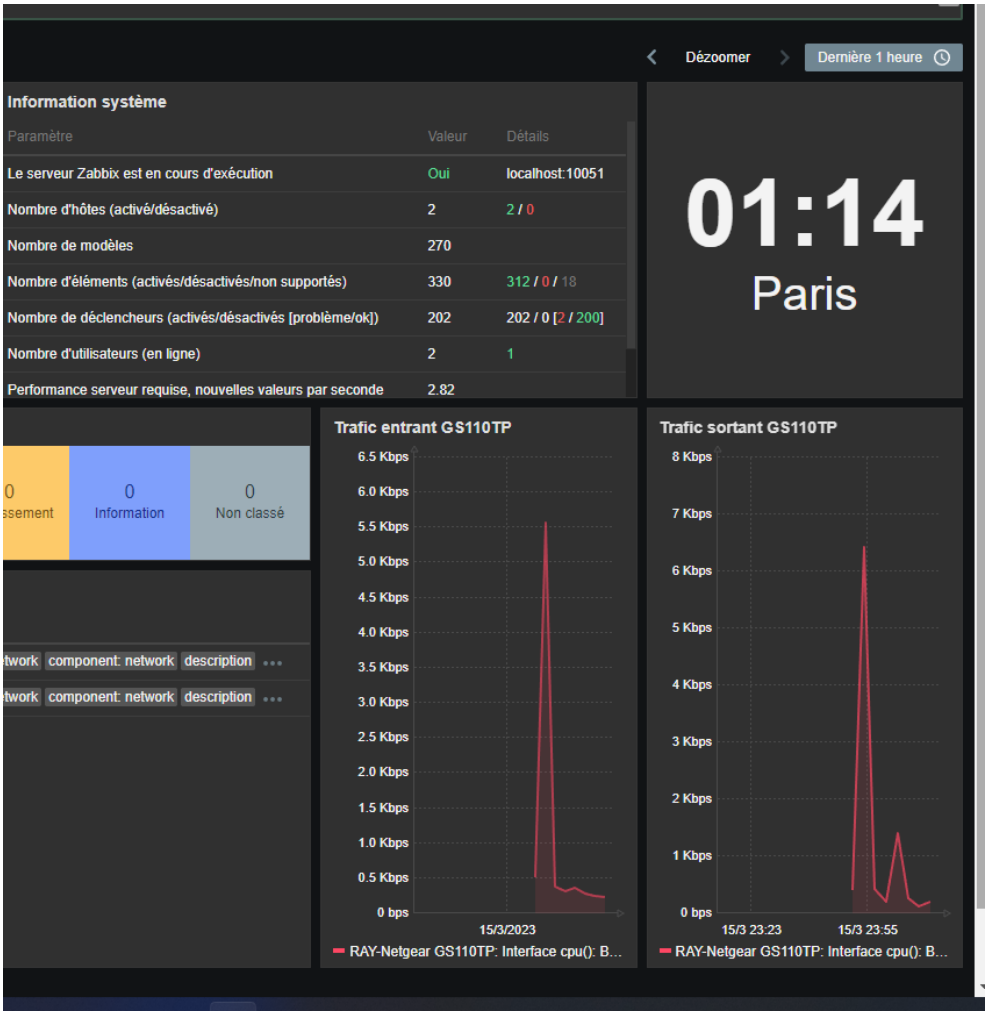
Une fois enregistré, nous attendons quelques secondes jusqu'à que « SNMP » s'affiche en vert, afin que Zabbix commence à récupérer les informations du switch via SNMP, puis nous pouvons cliquer sur « Dernières données » afin de voir les informations que Zabbix a pu récupérer du switch.

RAY-Netgear GS110TP	Interface cpu(): Bits sent	1m 22s	208 bps	-240 bps
RAY-Netgear GS110TP	Interface cpu(): Inbound packets discarded	1m 23s	0	
RAY-Netgear GS110TP	Interface cpu(): Inbound packets with errors	1m 23s	0	
RAY-Netgear GS110TP	Interface cpu(): Interface type	13m 23s	other (1)	
RAY-Netgear GS110TP	Interface cpu(): Operational status	23s	down (2)	
RAY-Netgear GS110TP	Interface cpu(): Outbound packets discarded	1m 22s	0	
RAY-Netgear GS110TP	Interface cpu(): Outbound packets with errors	1m 22s	0	
RAY-Netgear GS110TP	Interface cpu(): Speed	13m 23s	0 bps	
RAY-Netgear GS110TP	Interface CPU Interface for Slot: 5 Port: 1: Bits received	1m 23s	320 bps	-64 bps
RAY-Netgear GS110TP	Interface CPU Interface for Slot: 5 Port: 1: Bits sent	1m 22s	208 bps	-264 bps
RAY-Netgear GS110TP	Interface CPU Interface for Slot: 5 Port: 1: Speed	1m 22s	0 bps	
RAY-Netgear GS110TP	Interface g1(): Bits received	1m 23s	0 bps	
RAY-Netgear GS110TP	Interface g1(): Bits sent	1m 22s	0 bps	
RAY-Netgear GS110TP	Interface g1(): Inbound packets discarded	1m 23s	0	
RAY-Netgear GS110TP	Interface g1(): Inbound packets with errors	1m 22s	0	
RAY-Netgear GS110TP	Interface g1(): Interface type	13m 23s	ethernetCsmacd (6)	
RAY-Netgear GS110TP	Interface g1(): Operational status	23s	down (2)	
RAY-Netgear GS110TP	Interface g1(): Outbound packets discarded	1m 23s	0	
RAY-Netgear GS110TP	Interface g1(): Outbound packets with errors	1m 22s	0	
RAY-Netgear GS110TP	Interface g1(): Speed	13m 23s	0 bps	
RAY-Netgear GS110TP	Interface g2(): Bits received	1m 23s	0 bps	
RAY-Netgear GS110TP	Interface g2(): Bits sent	1m 22s	0 bps	
RAY-Netgear GS110TP	Interface g2(): Inbound packets discarded	1m 22s	0	
RAY-Netgear GS110TP	Interface g2(): Inbound packets with errors	1m 22s	0	
RAY-Netgear GS110TP	Interface g2(): Interface type	13m 23s	ethernetCsmacd (6)	
RAY-Netgear GS110TP	Interface g2(): Operational status	23s	down (2)	
RAY-Netgear GS110TP	Interface g2(): Outbound packets discarded	1m 22s	0	
RAY-Netgear GS110TP	Interface g2(): Outbound packets with errors	1m 22s	0	
RAY-Netgear GS110TP	Interface g2(): Speed	13m 23s	0 bps	

Dans l'onglet « Graphique », nous pouvons interpréter de manière visuelle les informations récupérés du switch. Exemple ici, nous voyons le trafic échangé sur le port 8 du switch depuis 15min.

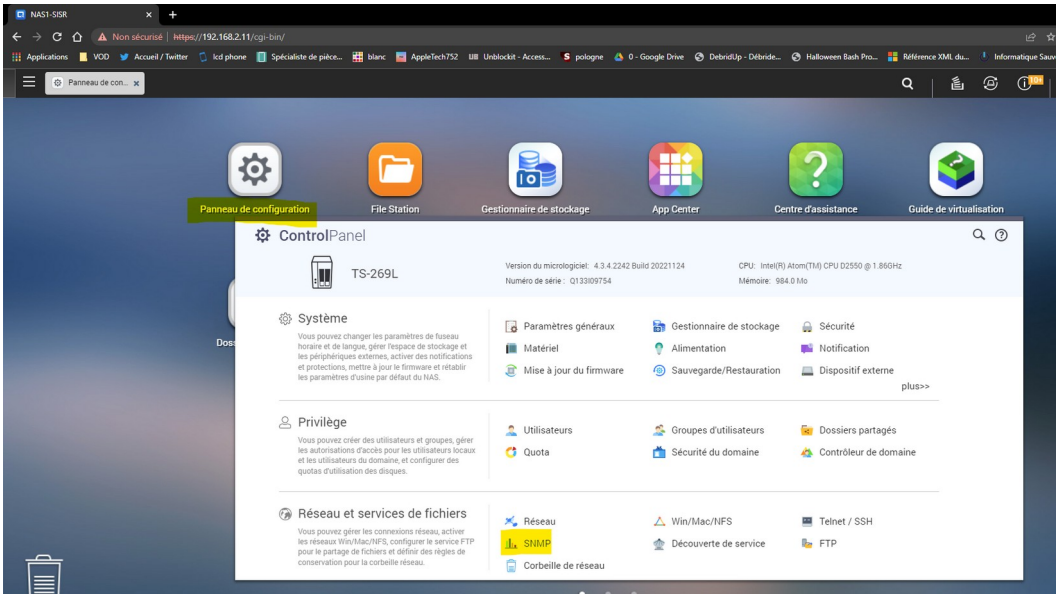


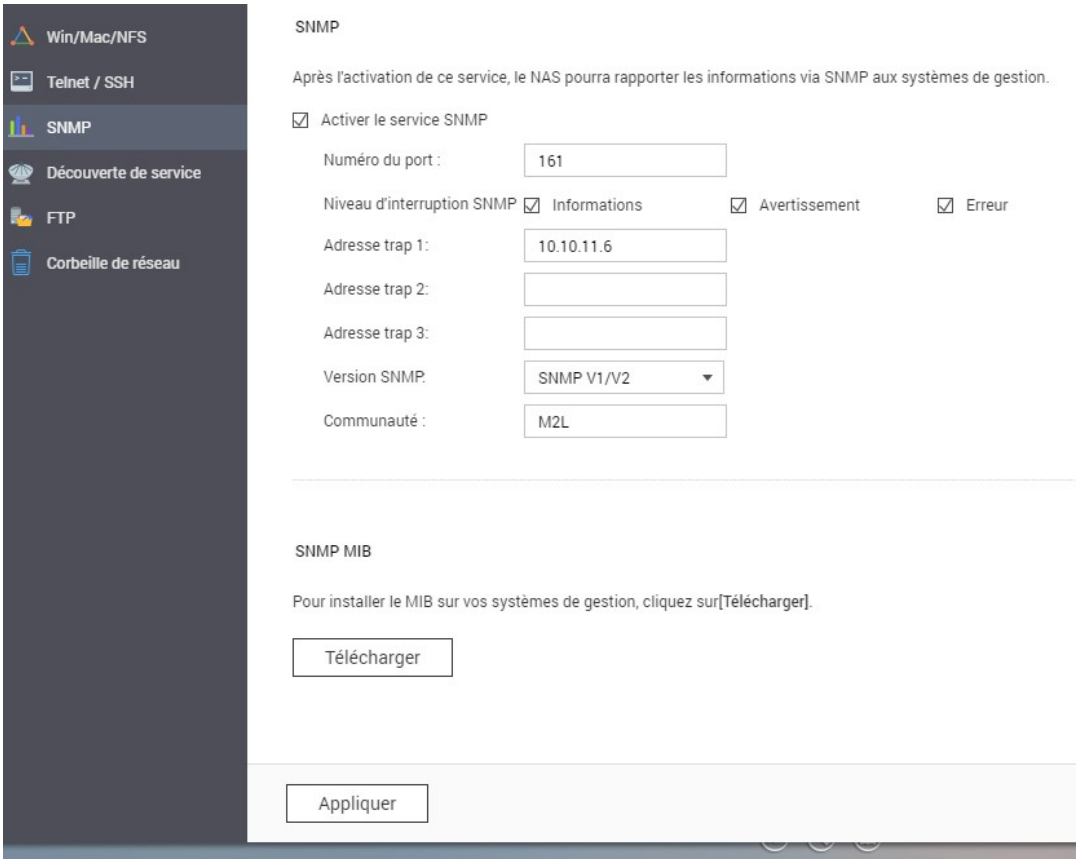
Sur le tableau de bord de la page d'accueil, il est maintenant possible de créer des graphiques ou autre style d'affichage en utilisant les donnés émis par le Switch en SNMP, comme par exemple ici le trafic entrant et sortant du switch.


Dézoomer
Dernière 1 heure
Information système
Paramètre
Valeur
Détails
Le serveur Zabbix est en cours d'exécution
Oui
localhost:10051
Nombre d'hôtes (activé/désactivé)
2
2 / 0
Nombre de modèles
270
Nombre d'éléments (activés/désactivés/non supportés)
330
312 / 0 / 18
Nombre de déclencheurs (activés/désactivés [problème/ok])
202
202 / 0 [2 / 200]
Nombre d'utilisateurs (en ligne)
2
1
Performance serveur requise, nouvelles valeurs par seconde
2.82
01:14
Paris
0
Information
0
Non classé
component: network
description
component: network
description
Trafic entrant GS110TP
6.5 Kbps
6.0 Kbps
5.5 Kbps
5.0 Kbps
4.5 Kbps
4.0 Kbps
3.5 Kbps
3.0 Kbps
2.5 Kbps
2.0 Kbps
1.5 Kbps
1.0 Kbps
0.5 Kbps
0 bps
15/3/2023
RAY-Netgear GS110TP: Interface cpu(): B...
Trafic sortant GS110TP
8 Kbps
7 Kbps
6 Kbps
5 Kbps
4 Kbps
3 Kbps
2 Kbps
1 Kbps
0 bps
15/3 23:23
15/3 23:55
RAY-Netgear GS110TP: Interface cpu(): B...

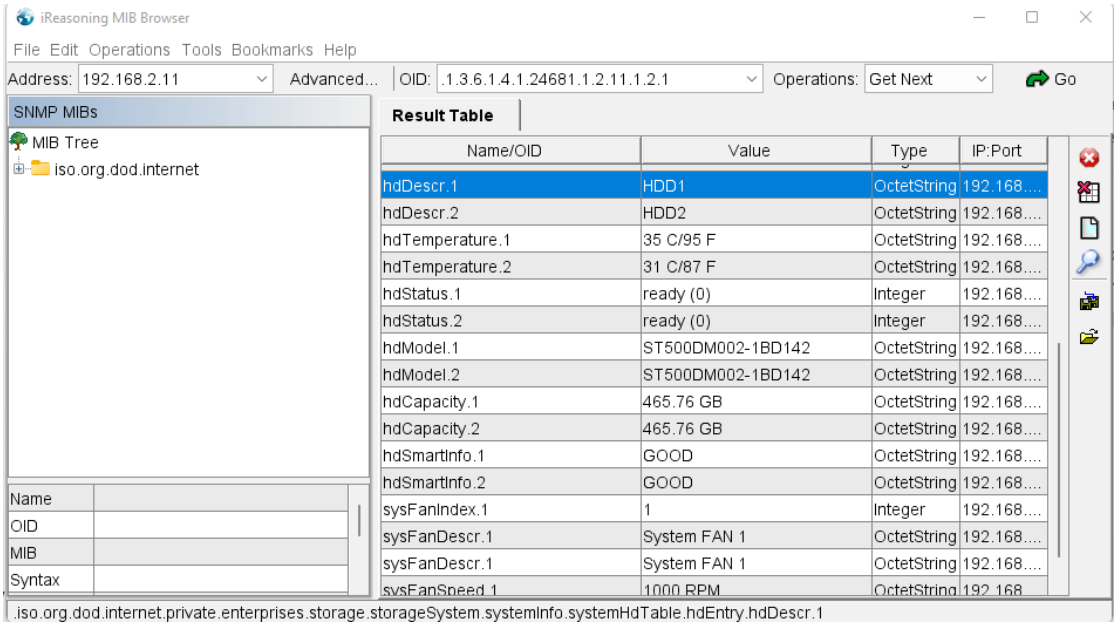
Supervision du NAS

Sur le NAS QNAP, nous allons aller dans « Panneau de configuration », puis dans « SNMP » afin d'activer le protocole et de préciser la communauté.





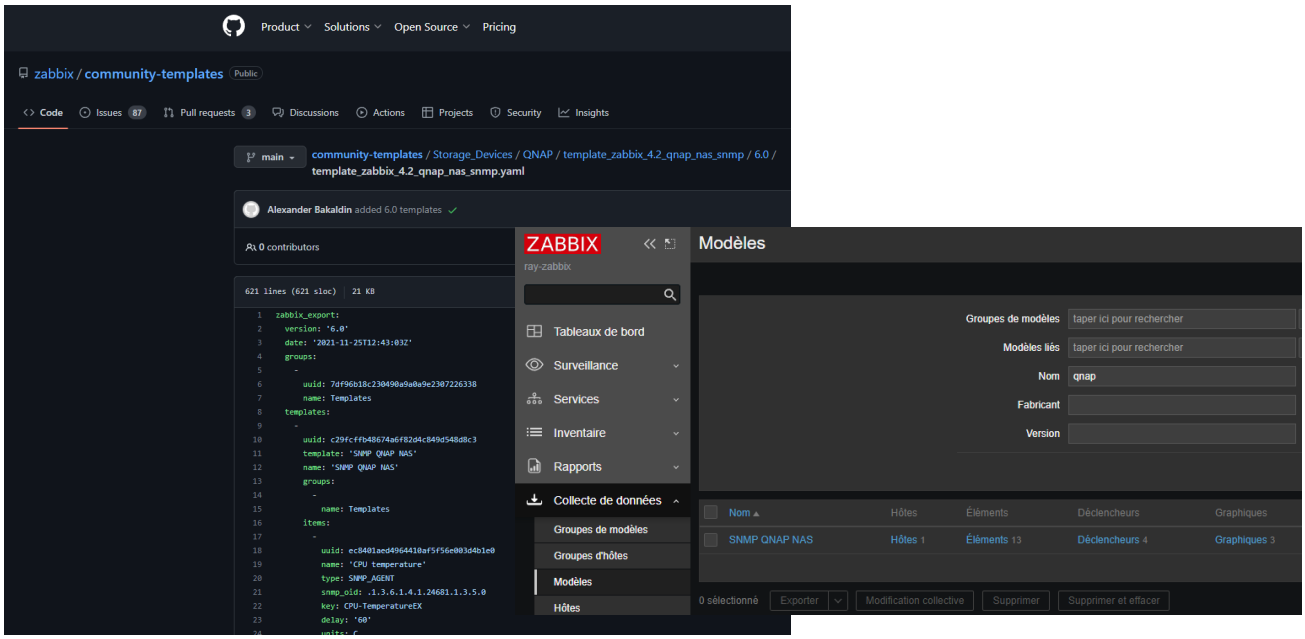
Pour tester le SNMP, on télécharge le MIB du NAS QNAP puis on l'importe dans MIB Browser.



On voit sur cette capture d’écran les informations remonter du NAS en SNMP.

Maintenant que nous savons que le NAS a bien été configuré, importons-le dans Zabbix.

Zabbix n’a pas de modèle (équivalent au MIB pour ce logiciel) pour les NAS de la marque QNAP, il faut donc en récupérer un sur internet puis l’importer sur Zabbix (« Collecte de données », « Modèles », « Importer »).



Puis nous rajoutons l'hôte en sélectionnant le protocole SNMP ainsi que le modèle précédemment importé, les informations vont automatiquement remonter dans Zabbix puis il sera possible de créer des graphiques ou de rajouter les informations du NAS sur le tableau de bord Zabbix.