BTS SIO
Ancelin
Robin

PPE 2

TRAÇABILITÉ ET SUPERVISION DE LA SANTÉ ET DE LA SÉCURITÉ DU SYSTÈME D'INFORMATION

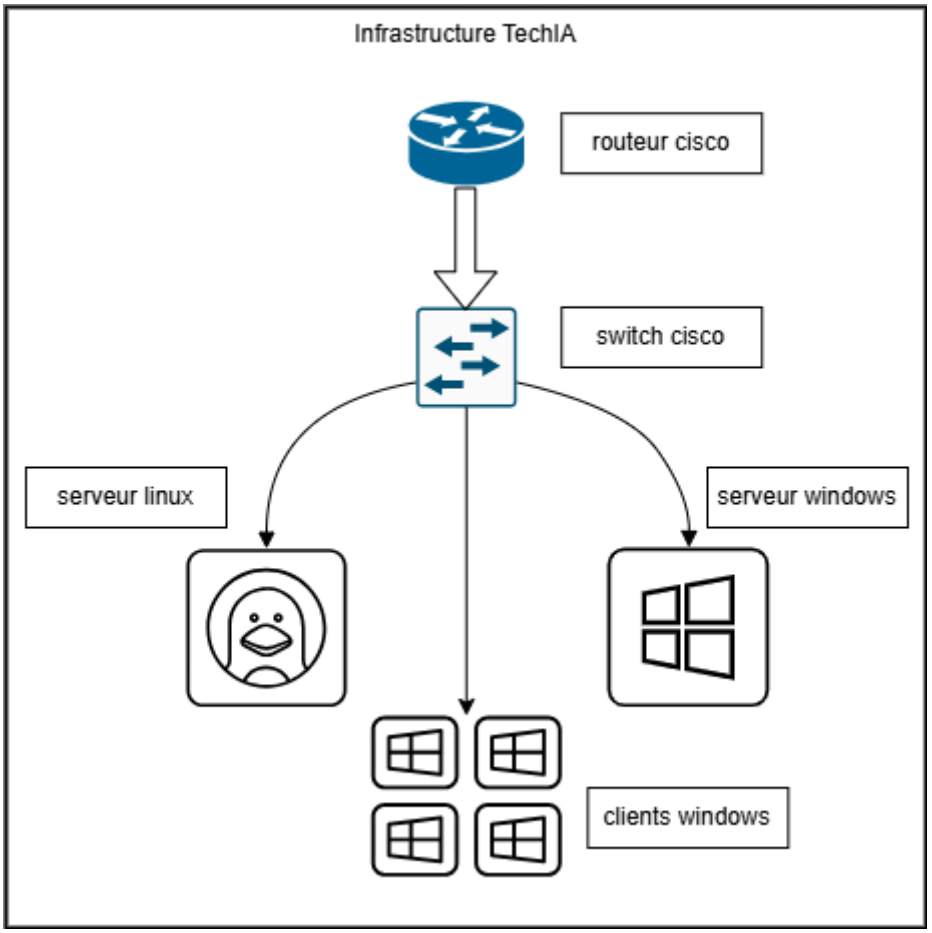
Sommaire

1) Introduction

a) Contexte

Dans le cadre du projet de supervision et de traçabilité de l'infrastructure de TechIA, l'entreprise ZSecure, prestataire pour TechIA, a choisi d'installer **Zabbix** et **Graylog** sur une même machine Debian. **Zabbix** assurera la supervision en temps réel des équipements, incluant un serveur Windows, un serveur Linux, un switch et un routeur, permettant ainsi une surveillance de l'état de santé des appareils. En parallèle, **Graylog** sera déployé pour centraliser et analyser les logs générés par ces équipements, garantissant une meilleure traçabilité des événements.

b) Schéma



voici le schéma de l'infrastructure de TechIA.

c) Informations utiles

équipements	ip
routeur	192.168.1.1
switch	192.168.1.2
serveur linux	192.168.1.3
serveur windows	192.168.1.4
clients windows	192.168.1.10-20
Zabbix/Graylog	192.168.1.100

Les identifiants général : admin / Azerty123!

Sera configurer sur les hôtes, sauf windows, SNMP V3 (authPriv) :

- `USERNAME` → `admin`
- `PROTOCOLE_PASSWORD` → `SHA`
- `PASSWORD` → `Azerty123!`
- `PROTOCOLE_PASSPHRASE` → `AES`
- `PASSPHRASE` → `Azerty123!`

2) Zabbix

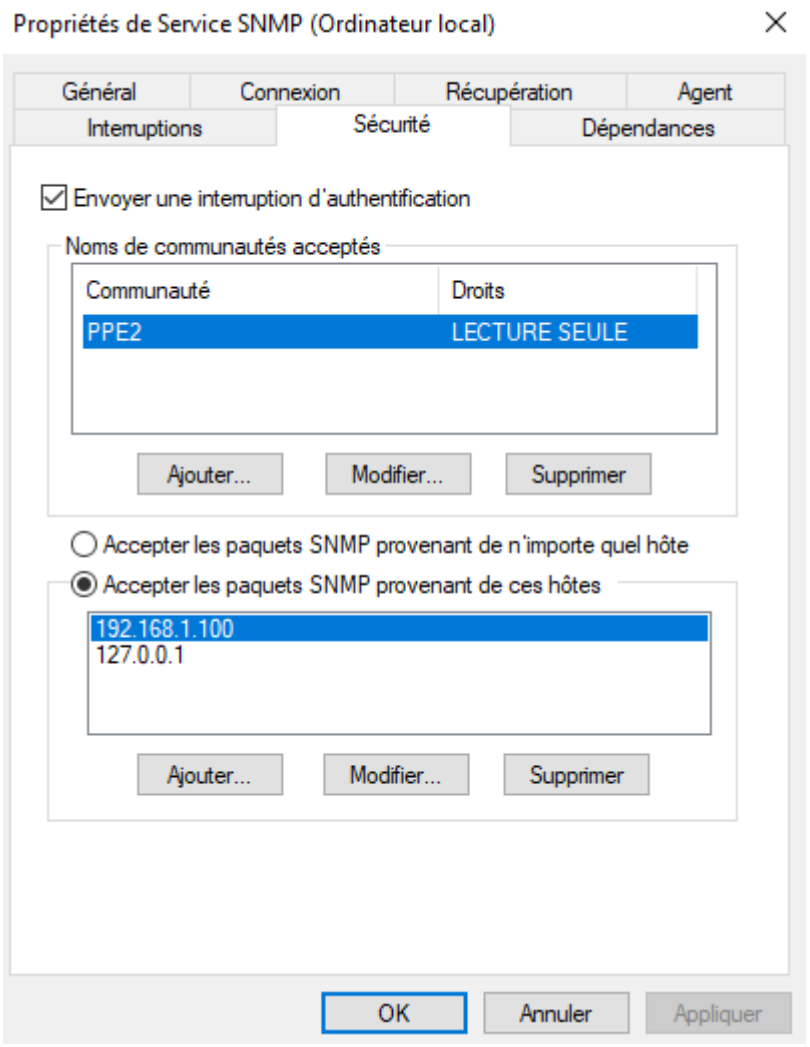
Routeur	192.168.1.1:161	SNMP	class: network target: cisco target: cisco-ios	Activé	Dernières données 96
SRV-LINUX	192.168.1.3:10050	ZBX	class: os class: software target: apache •••	Activé	Dernières données 78
SRV-WINDOWS	192.168.1.4:161	SNMP	class: os target: windows	Activé	Dernières données 23
switch	192.168.1.2:161	SNMP	class: network target: cisco target: cisco-ios	Activé	Dernières données 263

a) Serveur Windows

Le serveur Windows sera supervisé pour les performances. La template Windows by SNMP sera utilisée.

Conf Windows :

```
Add-WindowsFeature SNMP-Service
```



b) Serveur Linux

Le serveur linux sera supervisé pour les performances et le service web apache. La template Apache by Zabbix agent et Linux by Zabbix agent seront utilisées.

Conf linux :

```
sudo nano /etc/snmp/snmpd.conf
createUser admin SHA Azerty123! AES Azerty123!
rouser admin authPriv
```

```
sudo nano /etc/zabbix/zabbix_agentd.conf
Server=192.168.1.100
ServerActive=192.168.1.100
Hostname=SRV-LINUX
```

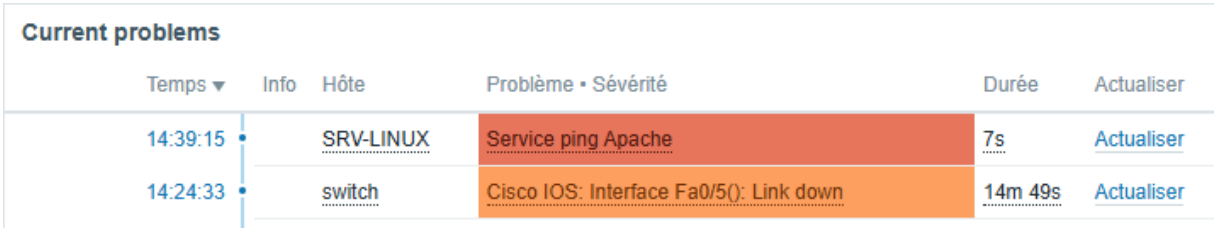
c) Routeur / switch

Les appareils cisco seront supervisés pour le trafic réseaux et la connectique de câbles. La template Cisco IOS SNMP sera utilisée.

Configuration cisco :

```
snmp-server group SNMPv3Group v3 priv
snmp-server user admin SNMPv3Group v3 auth sha Azerty123!
priv aes 128 Azerty123!
```

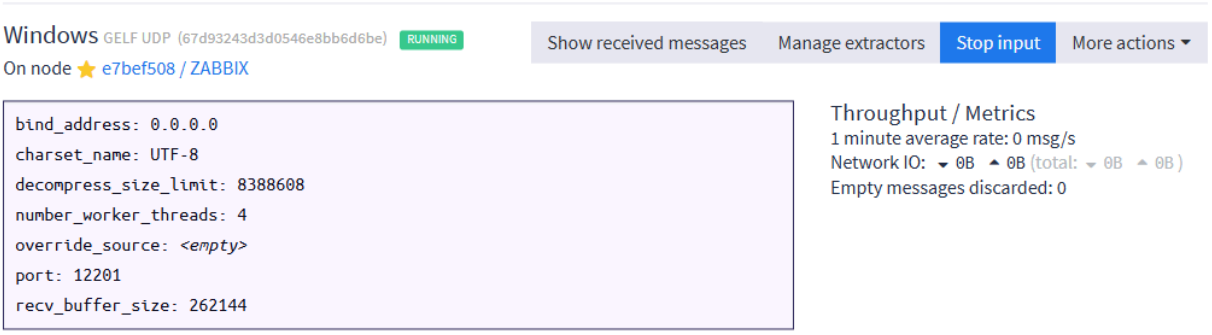
On peut donc maintenant surveiller nos hôtes :



3) Graylog

a) Serveur Windows

Sur graylogs : création d'un inputs GELF UDP



Windows :

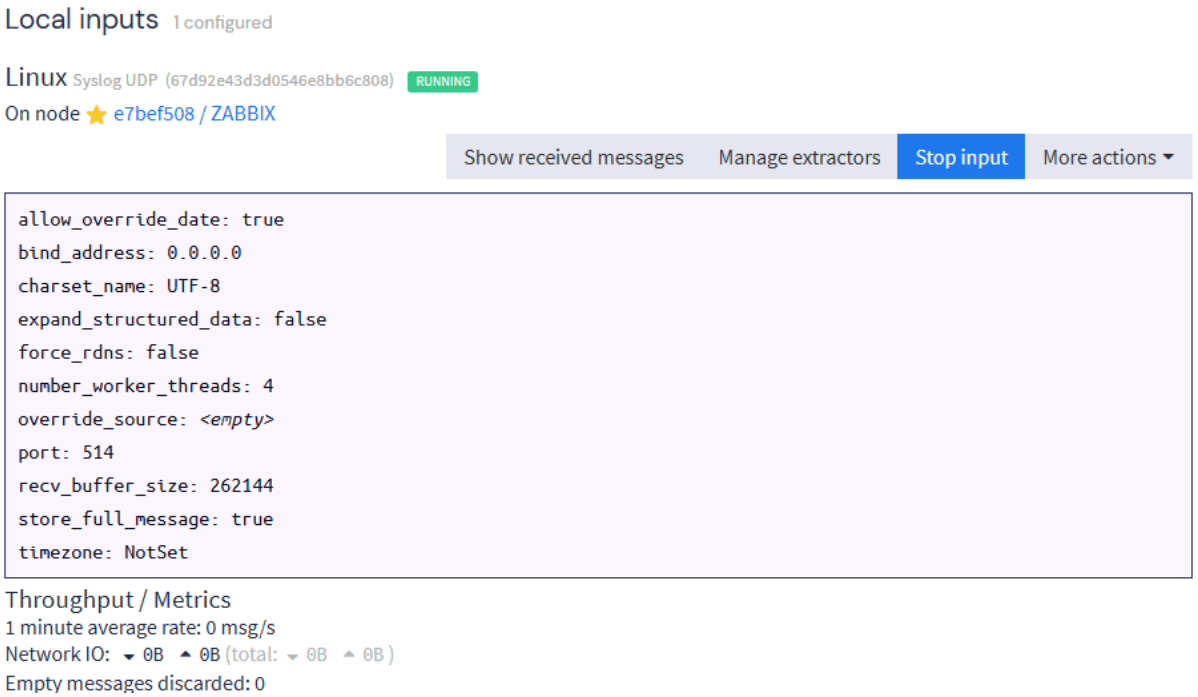
On va téléchargé NXlog
Modifié dans C:\Program Files\nxlog\conf\nxlog.conf et ajouter à la fin:

```
<Input in>
    Module      im_msvistalog
</Input>
<Extension gelf>
    Module        xm_gelf
</Extension>
<Output graylog_udp>
    Module        om_udp
    Host          192.168.1.100 #IP graylog
    Port      12201 # PORT
    OutputType    GELF_UDP # TYPE de input
</Output>
 <Route 1>
     Path        in => graylog_udp
 </Route>
```

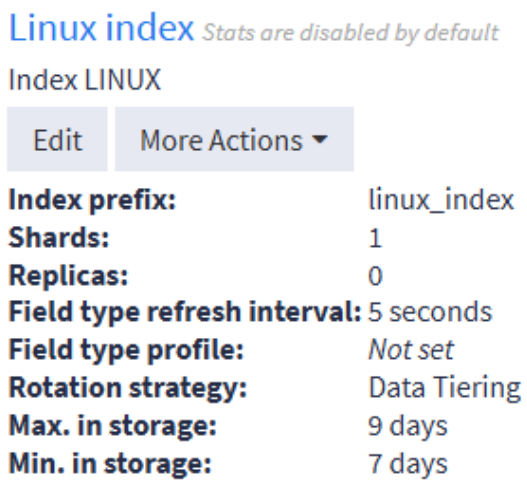
La stratégie de groupe est aussi modifiée pour auditer le rdp.

b) Serveur Linux

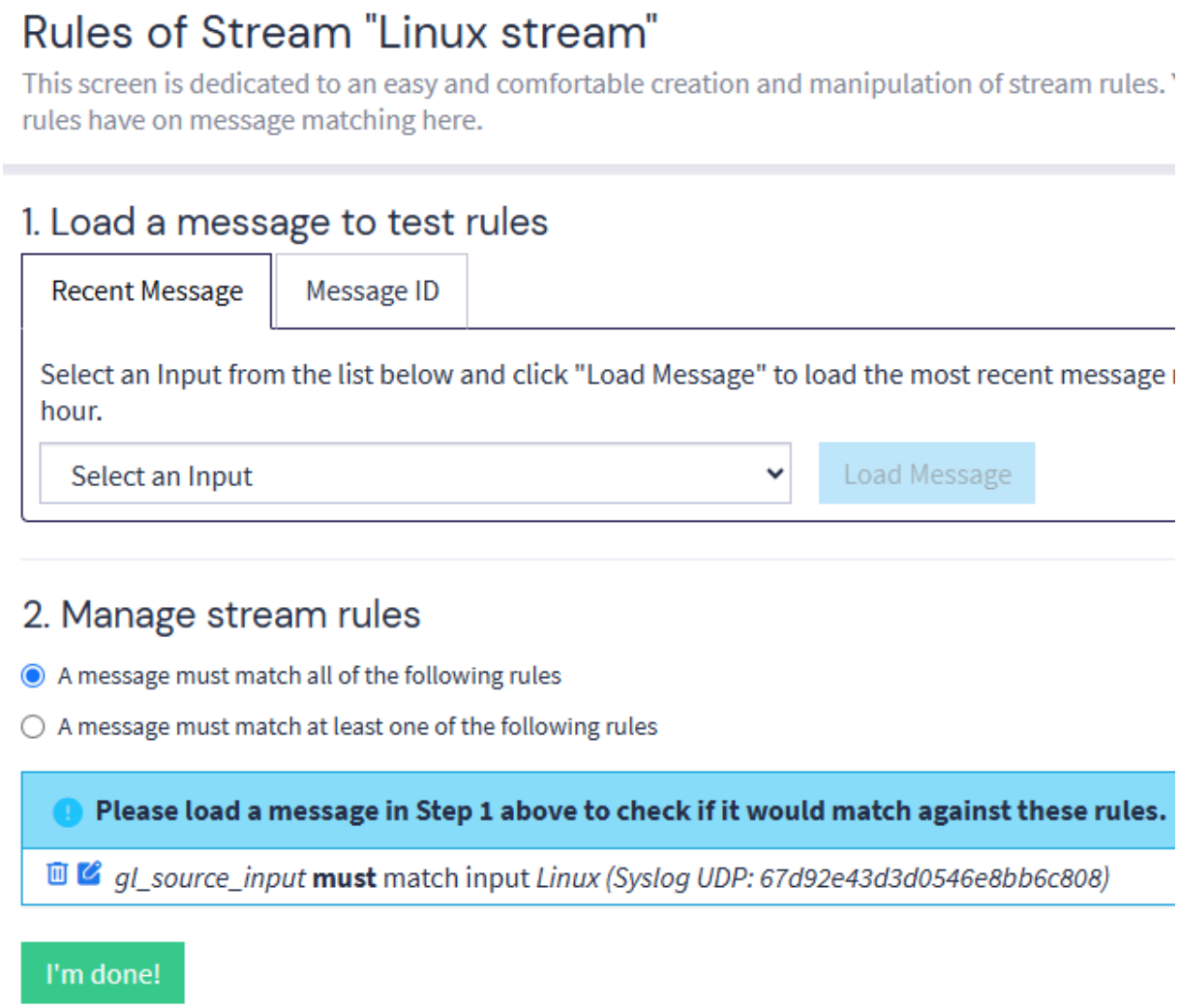
Sur graylog : Création d'un inputs Syslog UDP



Création d'un index linux :



Création d'un stream et règles stream :



Sur linux :

```
sudo apt-get install rsyslog

sudo nano /etc/rsyslog.d/10-graylog.conf

*.* @192.168.1.100:514;RSYSLOG_SyslogProtocol23Format

sudo systemctl restart rsyslog.service
```

On peut donc voir les logs de notre linux et du windows :