SIO

2023-2025

ZABBIX & PRTG

Axel Hespel &
Nicolas Debut

INSTALLATION DE ZABBIX

DIFFICULTÉ : ★★☆

Vous aurez besoin d'Apache 2 et de MySQL.
Ensuite, ajoutez le dépôt Zabbix.
Vous pouvez suivre la source indiquée en bas de la page.
Ensuite, rendez-vous sur IP/zabbix.
L'installation est assez basique.

Source

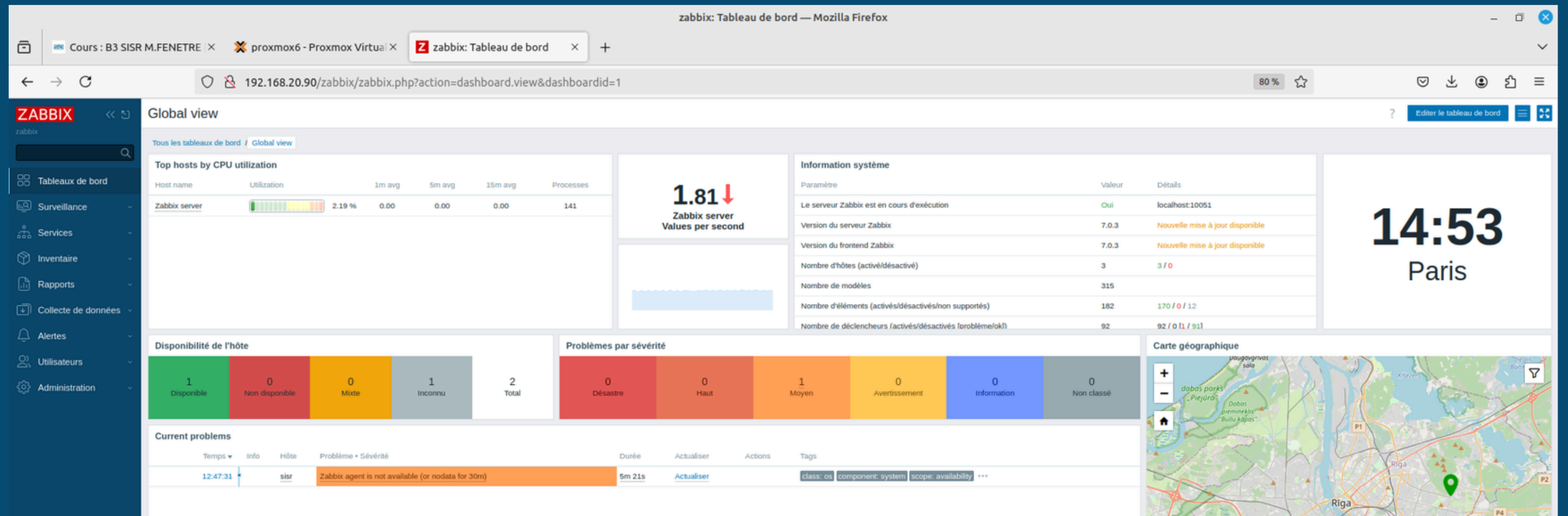
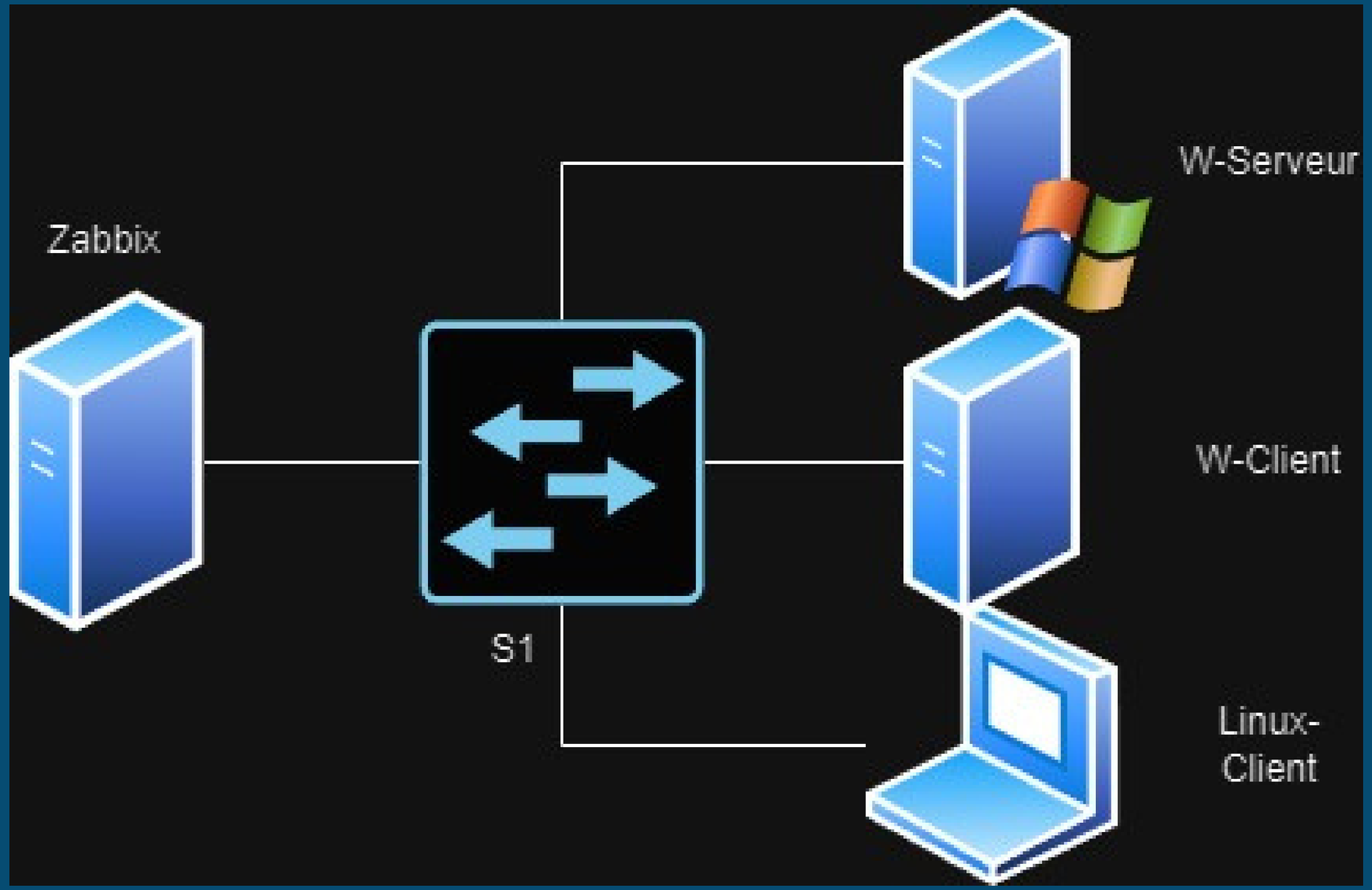


SCHÉMA DU SI



UTILISATION DE ZABBIX

Zabbix est utile pour le monitoring, car il permet d’obtenir des informations importantes en temps réel. Ces dernières sont reçues par des hôtes, qui peuvent être de tout type : utilisateur, serveur, switch, etc.
Les données sont transmises via le protocole SNMP au serveur NMS.
Il est également possible de générer des alertes qui apparaîtront sur la page d’accueil de Zabbix.

Source

PROTOCOLE SNMP

Le protocole SNMP fonctionne sur un système maître-esclave, où le serveur Zabbix (NMS) récupère les trames des agents SNMP.
Nous disposons d'une MIB (Management Information Base) qui permet de gérer les entités du réseau depuis le NMS.
Enfin, les appareils gérés (managed devices), qui sont les "esclaves", envoient leurs données au serveur Zabbix.

PROTOCOLE SNMP

Le protocole SNMP marche par commande, que zabbix automatise :

Get	GetNext	GetBulk	Set	Response	Trap	Inform
Il s'agit d'une demande envoyée par NMS à l'appareil géré. Et il est exécuté pour récupérer une ou plusieurs valeurs de MIB.	Il est similaire à GET. Mais il récupère généralement la valeur du prochain OID (Object Identifier) dans l'arborescence MIB.	Il est utilisé pour récupérer une masse de données à partir d'une grande table MIB.	Il est effectué par NMS pour modifier la valeur de l'appareil géré.	Elle est effectuée par l'agent en réponse aux opérations GetRequest, GetNextRequest, GetBulkRequest et SetRequest.	Cette opération est initiée par l'agent. Elle est utilisée pour notifier NMS d'une défaillance ou d'un événement survenant sur un appareil géré.	Cette opération est initiée par l'agent. Elle est similaire à TRAP, mais après que l'agent a envoyé une demande d'information, NMS doit envoyer un paquet InformResponse en réponse à l'agent.

EXEMPLE D ALERTE

Zabbix permet de réaliser des alertes directement. Elles sont très diversifiées, mais vous devez les configurer manuellement, car elles ne sont pas automatiques. Vous pouvez également configurer les alertes par e-mail.
Ces alertes sont utilisées pour gérer le serveur, car le flux d’information peut être très conséquent.
PS : Je n’ai pas eu le temps de faire les tests en raison de mon absence et de ma maladie.

Source

CONFIGURATION SNMP

Switch :

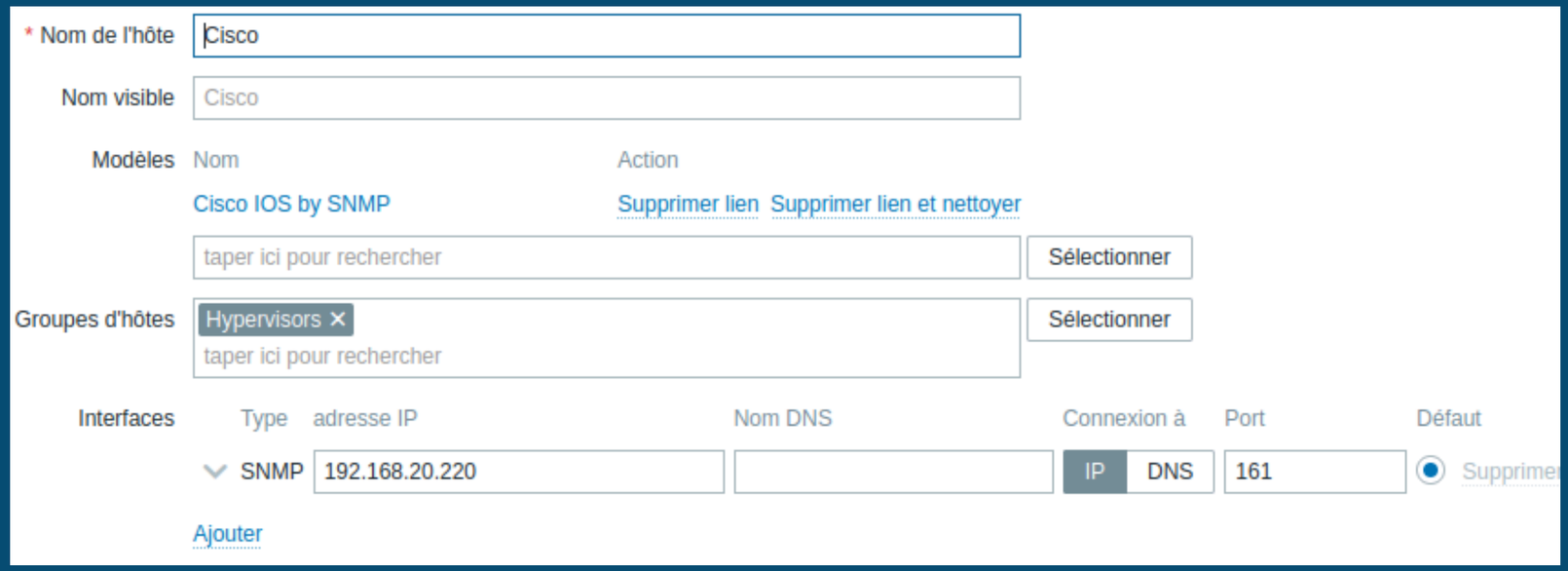
```
00:47:08: %DTP-5-DOMAINMISMATCH: Unable to perform tru
Switch(config-if)#no snmp-server community public RO
Switch(config)#snmp-server enable traps ?
```

```
Switch(config-if)#interface vlan 1
Switch(config-if)#192.168.20.220
```

```
Switch(config)#snmp-server host 192.168.20.140 public
```

CONFIGURATION SNMP

Sur zabbix:



Ip du switch : 192.168.20.220

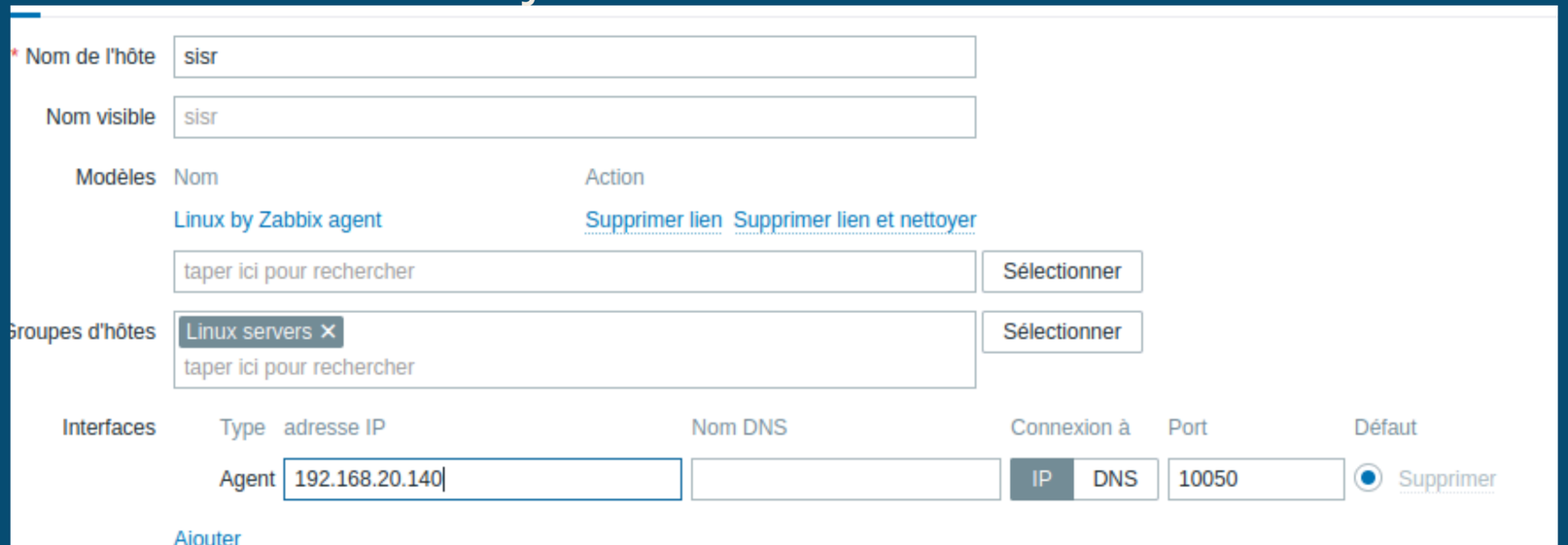
Vous devez également avoir une COMUNITY, seulement les membres de la meme comunity communique entre eux

CONFIGURATION AGENT/ LINUX

Télécharger l’agent zabbix : https://serverspace.io/support/help/installing-zabbix-agent-on-ubuntu/

Ensuite modifier la config : nano /etc/zabbix/zabbix_agentd.conf

modifier l’ip du serveur visé en celui de votre zabbix, ensuite ajouter un hotes



CHOIX DE SOLUTION

En entreprise, j’aurai le choix d’utiliser Zabbix. Je n’ai pas de comparaison avec PRTG, n’ayant pas été présent, mais j'ai remarqué les qualités de Zabbix. Premièrement, sur Linux, la stabilité est bien supérieure à celle de Windows. En effet, si notre serveur de supervision tombe, nous nous retrouvons sans rien.
De plus, son installation et sa configuration sont claires, la documentation étant suffisante. La façon d’augmenter le nombre d’esclaves est également plutôt facile.
Je préconise donc cette solution, qui a été testée et est facile à utiliser. Cependant, la sécurité reste un facteur important. Bien que le protocole soit clair, sa configuration représente également un avantage notable.