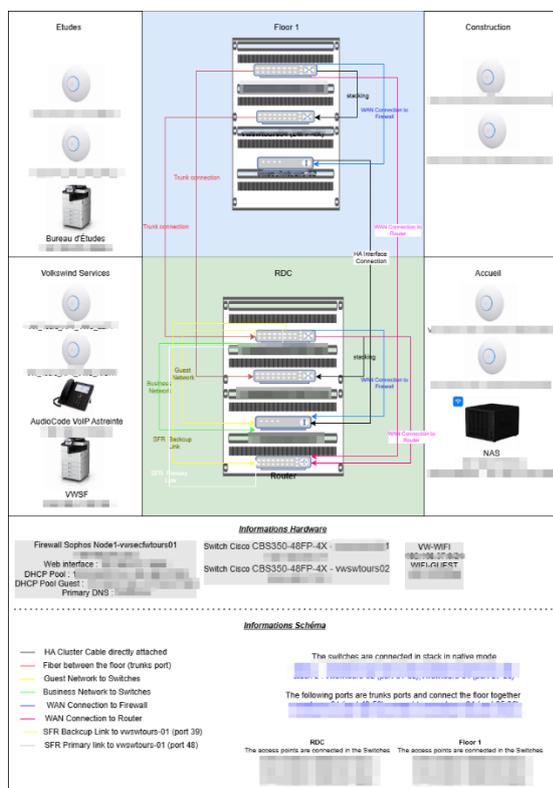


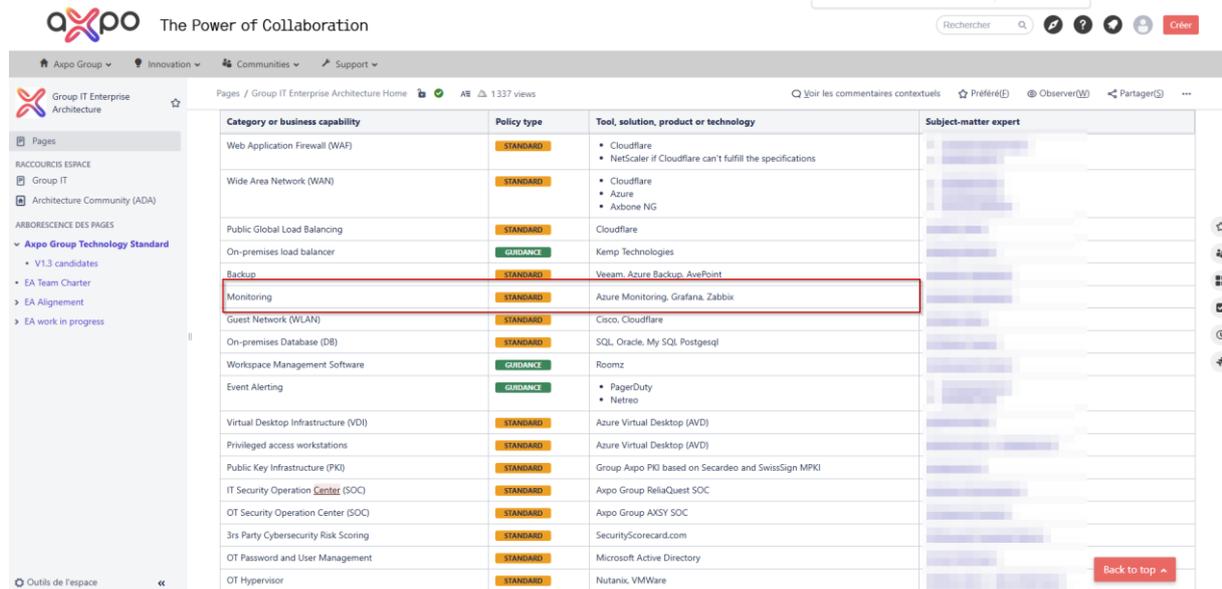
Dans le cadre de mes missions actuelles, mon responsable m'a confié un nouvel ordre de mission portant sur la mise en place d'une solution de supervision pour notre infrastructure réseau, et plus particulièrement pour nos firewalls et nos switches. La supervision consiste à surveiller en temps réel l'état de santé et la performance de nos équipements informatiques afin de détecter rapidement toute anomalie, panne ou dégradation de service. Cela permet d'assurer une haute disponibilité du réseau, d'anticiper les incidents avant qu'ils n'impactent la production, et de renforcer la sécurité en repérant immédiatement des comportements inhabituels sur les équipements critiques comme les firewalls. Une bonne solution de supervision offre également des outils de reporting, d'alerting (alertes par email, SMS ou autres moyens), ainsi que des tableaux de bord clairs pour suivre les métriques réseau, comme le trafic, les erreurs, les coupures, ou encore l'état des interfaces.

Voici le schémas réseau de notre infrastructure afin de percevoir les hôtes qui seront monitorés :



« En tant que collaborateur chez Volkswind, je suis tenu de respecter les politiques internes établies par AXPO concernant les choix technologiques et solutions logicielles. À ce titre, lors de la mise en œuvre de solutions spécifiques, je suis soumis à l'obligation d'utiliser les outils identifiés comme standards, recommandés ou obligatoire par l'organisation, tels que définis sur le site interne dédié d'AXPO. Par exemple, pour les projets relatifs au Monitoring, je dois utiliser Azure Monitoring, Grafana ou Zabbix conformément à son statut "Standard" imposé par l'entreprise.

## Ces choix stratégiques garantissent une cohérence technologique, facilitent la maintenance et optimisent le support technique interne. »



The screenshot shows the Axpo Group IT Enterprise Architecture Home page. The page features a navigation menu on the left and a main content area with a table of IT policies. The table has four columns: Category or business capability, Policy type, Tool, solution, product or technology, and Subject-matter expert. The 'Monitoring' row is highlighted with a red border.

Category or business capability	Policy type	Tool, solution, product or technology	Subject-matter expert
Web Application Firewall (WAF)	STANDARD	• Cloudflare • NetScaler if Cloudflare can't fulfill the specifications	
Wide Area Network (WAN)	STANDARD	• Cloudflare • Azure • Axbone NG	
Public Global Load Balancing	STANDARD	Cloudflare	
On-premises load balancer	GUIDANCE	Kemp Technologies	
Backup	STANDARD	Veeam, Azure Backup, AvePoint	
Monitoring	STANDARD	Azure Monitoring, Grafana, Zabbix	
Guest Network (WLAN)	STANDARD	Cisco, Cloudflare	
On-premises Database (DB)	STANDARD	SQL, Oracle, My SQL, Postgesql	
Workspace Management Software	GUIDANCE	Roomiz	
Event Alerting	GUIDANCE	• PagerDuty • Netreo	
Virtual Desktop Infrastructure (VDI)	STANDARD	Azure Virtual Desktop (AVD)	
Privileged access workstations	STANDARD	Azure Virtual Desktop (AVD)	
Public Key Infrastructure (PKI)	STANDARD	Group Axpo PKI based on Secardeo and SwissSign MPKI	
IT Security Operation Center (SOC)	STANDARD	Axpo Group ReliaQuest SOC	
OT Security Operation Center (SOC)	STANDARD	Axpo Group AKSY SOC	
3rs Party Cybersecurity Risk Scoring	STANDARD	SecurityScorecard.com	
OT Password and User Management	STANDARD	Microsoft Active Directory	
OT Hypervisor	STANDARD	Nutanix, VMware	

Mon responsable m'a tout de même demandé de faire un Benchmarking des différentes supervisions pour étudier réellement le besoin. Afin de répondre efficacement à cette mission et dans un souci de maîtrise des coûts, je me suis orienté vers une étude des solutions gratuites : Zabbix et Grafana

**Tableau de Comparaison :**

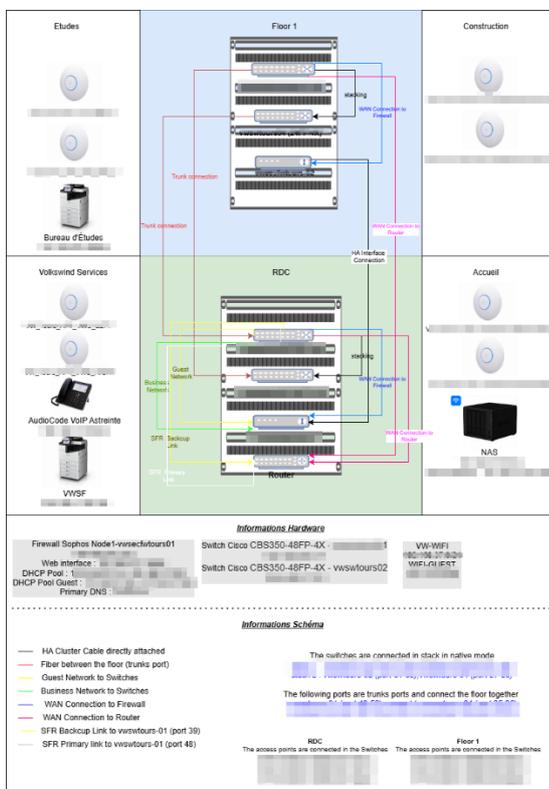
<b>Critère</b>	<b>Zabbix</b>	<b>Grafana</b>
<b>Fonction</b>	<b>Supervision complète (infrastructure, réseau, services) avec alertes</b>	<b>Virtualisation de données mais dépends du backend (InfluxDB, Prometheus)</b>
<b>Modèle de déploiement</b>	<b>Open Source</b>	<b>Open Source</b>
<b>Gestion SNMP</b>	<b>Intégré nativement (Template Cisco)</b>	<b>SNMP Exporters à installer et configurer</b>
<b>Alerte / Notifications</b>	<b>Oui et flexible</b>	<b>Complexe s'il faut gérer SNMP et autres pour collecter les données</b>
<b>Prise en main de l'outil</b>	<b>Interface dense</b>	<b>Complexe avec SNMP selon plusieurs sites</b>
<b>Base de données</b>	<b>SQL</b>	<b>Dépends du backend utilisé</b>
<b>Dashboard</b>	<b>Simple et fonctionnel</b>	<b>Personnalisable et moderne</b>
<b>Prix</b>	<b>Gratuit</b>	<b>Gratuit</b>

**Au vu de la comparaison des solutions, J'ai choisi d'utiliser Zabbix comme solution de supervision principalement pour sa simplicité de mise en œuvre et sa capacité à répondre efficacement aux besoins d'une petite infrastructure réseau. Contrairement à Grafana qui est plus complexe, Zabbix offre une solution tout-en-un intégrant à la fois la collecte de données, le stockage, la gestion des alertes et la visualisation, sans nécessiter l'ajout d'outils externes pour ces fonctions de base. Il gère également les bases de données de manière native, avec une configuration simple via MySQL ou PostgreSQL, ce qui facilite l'installation et la maintenance sur le long terme.**

**Un autre avantage est la prise en charge native du protocole SNMP, ce qui permet une supervision directe des équipements réseau comme les switches et les firewalls sans avoir à installer d'agents supplémentaires. Cette compatibilité immédiate avec SNMP rend Zabbix parfaitement adapté à mon environnement, composé essentiellement de quelques équipements réseau à superviser dans un contexte cloud léger.**

Dans le cadre de mes missions actuelles, mon responsable m'a confié un nouvel ordre de mission portant sur la mise en place d'une solution de supervision pour notre infrastructure réseau, et plus particulièrement pour nos firewalls et nos switchs. La supervision consiste à surveiller en temps réel l'état de santé et la performance de nos équipements informatiques afin de détecter rapidement toute anomalie, panne ou dégradation de service. Cela permet d'assurer une haute disponibilité du réseau, d'anticiper les incidents avant qu'ils n'impactent la production, et de renforcer la sécurité en repérant immédiatement des comportements inhabituels sur les équipements critiques comme les firewalls. Une bonne solution de supervision offre également des outils de reporting, d'alerting (alertes par email, SMS ou autres moyens), ainsi que des tableaux de bord clairs pour suivre les métriques réseau, comme le trafic, les erreurs, les coupures, ou encore l'état des interfaces.

Voici le schémas réseau de notre infrastructure afin de percevoir les hôtes qui seront monitorés :



« En tant que collaborateur chez Volkswind, je suis tenu de respecter les politiques internes établies par AXPO concernant les choix technologiques et solutions logicielles. À ce titre, lors de la mise en œuvre de solutions spécifiques, je suis soumis à l'obligation d'utiliser les outils identifiés comme standards, recommandés ou obligatoire par l'organisation, tels que définis sur le site interne dédié d'AXPO. Par exemple, pour les projets relatifs au Monitoring, je dois

utiliser Azure Monitoring, Grafana ou Zabbix conformément à son statut "Standard" imposé par l'entreprise.

Ces choix stratégiques garantissent une cohérence technologique, facilitent la maintenance et optimisent le support technique interne. »

The screenshot shows the Axpo Group IT Enterprise Architecture page. The table lists various IT capabilities, their policy types, and the tools used for each. The 'Monitoring' row is highlighted with a red box.

Category or business capability	Policy type	Tool, solution, product or technology	Subject-matter expert
Web Application Firewall (WAF)	STANDARD	• Cloudflare • NetScaler if Cloudflare can't fulfill the specifications	
Wide Area Network (WAN)	STANDARD	• Cloudflare • Azure • Axbone NG	
Public Global Load Balancing	STANDARD	Cloudflare	
On-premises load balancer	GUIDANCE	Kemp Technologies	
Backup	STANDARD	Veeam, Azure Backup, AvePoint	
Monitoring	STANDARD	Azure Monitoring, Grafana, Zabbix	
Guest Network (WLAN)	STANDARD	Cisco, Cloudflare	
On-premises Database (DB)	STANDARD	SQL, Oracle, My SQL, Postgresql	
Workspace Management Software	GUIDANCE	Roomz	
Event Alerting	GUIDANCE	• PagerDuty • Netreo	
Virtual Desktop Infrastructure (VDI)	STANDARD	Azure Virtual Desktop (AVD)	
Privileged access workstations	STANDARD	Azure Virtual Desktop (AVD)	
Public Key Infrastructure (PKI)	STANDARD	Group Axpo PKI based on Secardeo and SwissSign MPKI	
IT Security Operation Center (SOC)	STANDARD	Axpo Group ReliaQuest SOC	
OT Security Operation Center (SOC)	STANDARD	Axpo Group AXSY SOC	
3rs Party Cybersecurity Risk Scoring	STANDARD	SecurityScorecard.com	
OT Password and User Management	STANDARD	Microsoft Active Directory	
OT Hypervisor	STANDARD	Nutanix, VMWare	

Mon responsable m'a tout de même demandé de faire un Benchmarking des différentes supervisions pour étudier réellement le besoin. Afin de répondre efficacement à cette mission et dans un souci de maîtrise des coûts, je me suis orienté vers une étude des solutions gratuites : Zabbix et Grafana

**Tableau de Comparaison :**

<b>Critère</b>	<b>Zabbix</b>	<b>Grafana</b>
<b>Fonction</b>	<b>Supervision complète (infrastructure, réseau, services) avec alertes</b>	<b>Virtualisation de données mais dépends du backend (InfluxDB, Prometheus)</b>
<b>Modèle de déploiement</b>	<b>Open Source</b>	<b>Open Source</b>
<b>Gestion SNMP</b>	<b>Intégré nativement (Template Cisco)</b>	<b>SNMP Exporters à installer et configurer</b>
<b>Alerte / Notifications</b>	<b>Oui et flexible</b>	<b>Complexe s'il faut gérer SNMP et autres pour collecter les données</b>
<b>Prise en main de l'outil</b>	<b>Interface dense</b>	<b>Complexe avec SNMP selon plusieurs sites</b>
<b>Base de données</b>	<b>SQL</b>	<b>Dépends du backend utilisé</b>
<b>Dashboard</b>	<b>Simple et fonctionnel</b>	<b>Personnalisable et moderne</b>
<b>Prix</b>	<b>Gratuit</b>	<b>Gratuit</b>

Au vu de la comparaison des solutions, J'ai choisi d'utiliser Zabbix comme solution de supervision principalement pour sa simplicité de mise en œuvre et sa capacité à répondre efficacement aux besoins d'une petite infrastructure réseau. Contrairement à Grafana qui est plus complexe, Zabbix offre une solution tout-en-un intégrant à la fois la collecte de données, le stockage, la gestion des alertes et la visualisation, sans nécessiter l'ajout d'outils externes pour ces fonctions de base. Il gère également les bases de données de manière native, avec une configuration simple via MySQL ou PostgreSQL, ce qui facilite l'installation et la maintenance sur le long terme.

**Un autre avantage est la prise en charge native du protocole SNMP, ce qui permet une supervision directe des équipements réseau comme les switches et les firewalls sans avoir à installer d'agents supplémentaires. Cette compatibilité immédiate avec SNMP rend Zabbix parfaitement adapté à mon environnement, composé essentiellement de quelques équipements réseau à superviser dans un contexte cloud léger.**

Pour configurer nos switches, je me suis connecté via ssh :

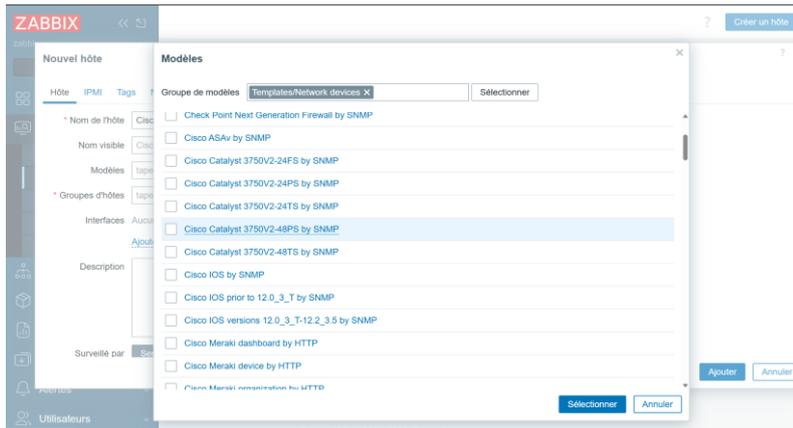
```
conf t
```

```
snmp-server community public RO
```

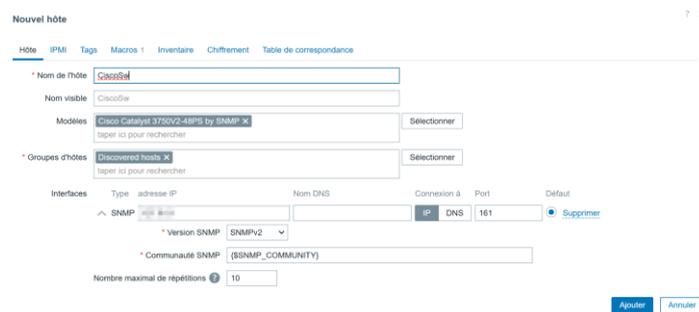
```
snmp-server location "test"
```

```
sh ver
```

Ensuite sur l'interface de Zabbix, on choisi le modèle de notre switch :



On renseigne les informations :



Dans Macro, on renseigne le nom de la communauté créer précédemment dans les configurations lors de l'activation du SNMP sur le switch :



Résultat :

Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
CiscoSw		SNMP	class: network target: cisco target: cisco-ios ...	Enabled	Latest data 14	Problems	Graphs	Dashboards 1	Web

