Projet 1 - BTS SIO SISR

Supervision et alerting des services critiques

Société : EcoSolar Solutions

Sofiane Belaroussi
BTS SIO – Option SISR
Année scolaire 2025–2026

Sommaire

---

1. Présentation de l'entreprise

1.1 Contexte

EcoSolar Solutions est une entreprise française spécialisée dans la conception et la fabrication de panneaux solaires à haut rendement. Face à sa croissance et à l'augmentation de sa dépendance aux outils informatiques, la direction a engagé une modernisation de son système d'information afin d'améliorer sa sécurité, sa disponibilité et sa capacité à accompagner les besoins futurs de l'entreprise.

Dans ce contexte, EcoSolar Solutions a confié l'infogérance de son infrastructure à la société WildCorp, au sein de laquelle j'interviens en tant qu'administrateur systèmes et réseaux.

1.2 Présentation du système d'information existant

Le système d'information d'EcoSolar Solutions est hébergé principalement sur une infrastructure locale située sur le site de Toulouse. L'entreprise dispose d'un hyperviseur Proxmox VE permettant d'héberger l'ensemble des serveurs virtuels nécessaires à son activité.

L'infrastructure est organisée autour d'un réseau local 192.168.128.0/24 protégé par un firewall pfSense assurant l'accès à Internet. Les différents équipements sont raccordés à un commutateur Cisco central.

Les principaux services de l'entreprise sont hébergés sous forme de machines virtuelles :

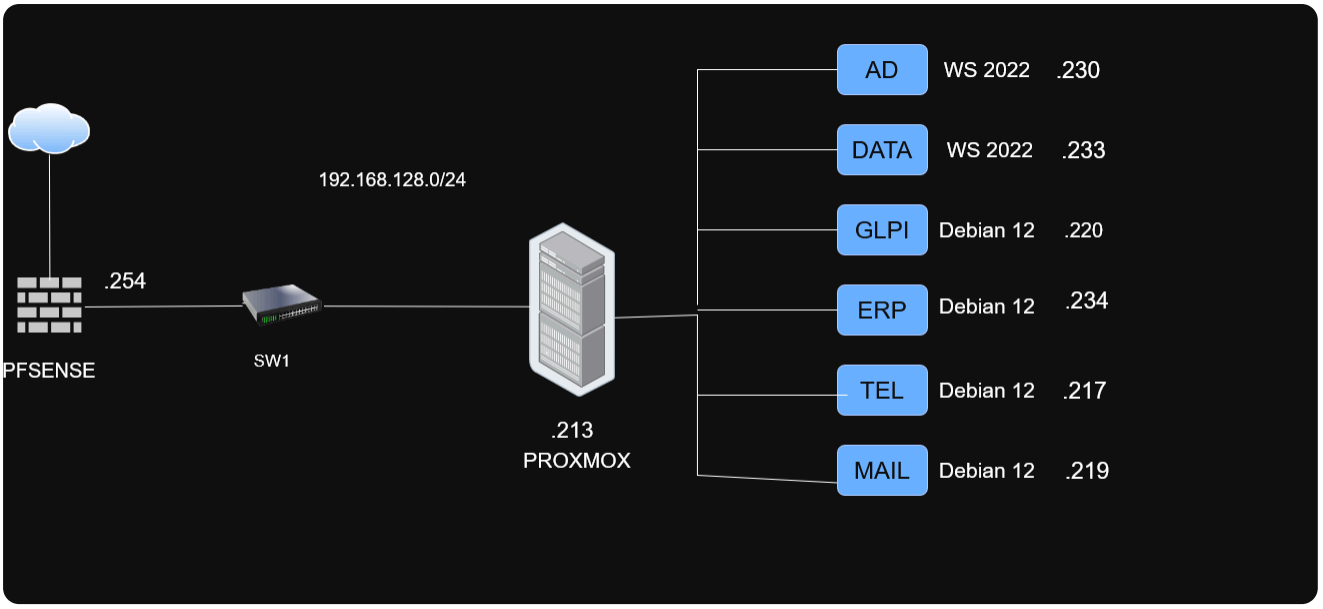
- Un contrôleur de domaine Active Directory
- Un serveur de fichiers destiné au stockage et au partage des données
- Un serveur ERP
- Un serveur de téléphonie
- Un serveur de messagerie

L'ensemble de ces services est essentiel au bon fonctionnement de l'entreprise. Cependant, aucun outil de supervision centralisé n'est actuellement déployé pour surveiller leur disponibilité ou leurs performances.

Cette situation rend plus difficile la détection rapide des incidents et justifie la mise en place d'une solution de monitoring dédiée.

1.3 Schéma de l'infrastructure actuelle

La figure suivante présente l'architecture logique actuelle du système d'information d'EcoSolar Solutions.



1.4 Objectifs du projet

L'une des problématiques identifiées concerne l'absence d'une solution centralisée de supervision permettant de surveiller efficacement les serveurs et les services critiques de l'entreprise.

Le présent projet a donc pour objectif de concevoir et déployer une solution de monitoring afin d'améliorer la visibilité sur l'état de l'infrastructure, détecter rapidement les incidents et contribuer à l'amélioration de la qualité de service du système d'information

---

2. Analyse du besoin

2.1 Besoins de l'entreprise

EcoSolar Solutions souhaite améliorer la supervision de son infrastructure informatique afin de mieux surveiller l'état de ses serveurs et de ses services. Aujourd'hui, l'entreprise ne dispose pas d'un outil centralisé permettant de détecter rapidement les pannes ou les dysfonctionnements pouvant impacter l'activité.

L'objectif est de mettre en place une solution de monitoring capable de surveiller les équipements critiques du système d'information, tels que l'hyperviseur Proxmox, les serveurs Windows et Linux ainsi que les services métiers comme l'ERP, la messagerie ou l'Active Directory.

L'entreprise souhaite également recevoir des alertes en cas d'incident et disposer de tableaux de bord lui permettant de suivre l'état général de son infrastructure.

2.2 Contraintes du projet

La solution choisie doit être compatible avec l'infrastructure existante composée de serveurs Windows Server, Debian Linux et Proxmox VE.

Elle doit également être simple à administrer, adaptée aux besoins d'une PME et pouvoir évoluer dans le temps pour accompagner le développement de l'entreprise et les futurs projets d'infrastructure.

Enfin, l'accès à l'outil de supervision devra être sécurisé afin de protéger les informations techniques du système d'information.

2.3 Attentes de l'entreprise

L'entreprise souhaite pouvoir :

- Superviser ses serveurs et équipements réseau
- Contrôler la disponibilité des services critiques
- Être alertée rapidement en cas de panne ou d'anomalie
- Suivre les performances de l'infrastructure
- Disposer d'une vue centralisée de l'état du système d'information
- Anticiper les incidents avant qu'ils n'impactent les utilisateurs

Cette solution doit permettre d'améliorer la disponibilité des services et de faciliter le travail d'administration et de maintenance de l'infrastructure.

---

3. Étude des solutions

3.1 Comparaison

Afin de répondre au besoin de supervision de l'infrastructure d'EcoSolar Solutions, J'ai étudié plusieurs solutions de monitoring, parmis les plus connues et utilisées en entreprises.

Critère	Zabbix	Centreon	Prometheus + Grafana
Open Source	Oui	Oui (version Community)	Oui

Critère	Zabbix	Centreon	Prometheus + Grafana
Supervision serveurs Windows/Linux	Très bonne	Très bonne	Bonne
Supervision équipements réseau (SNMP)	Très bonne	Très bonne	Moyenne
Supervision Proxmox	Native via templates	Possible	Nécessite plusieurs exports
Gestion des alertes	Très complète	Très complète	Via Alertmanager
Tableaux de bord	Intégrés	Intégrés	Excellents avec Grafana
Simplicité de déploiement	Bonne	Moyenne	Complexe - Mais simple en conteneur
Solution tout-en-un	Oui	Oui	Non
Adaptée à une PME	Oui	Oui	Partiellement

3.2 Analyse des solutions

Centreon est une solution mature et très utilisée dans les grandes entreprises. Elle dispose de nombreuses fonctionnalités mais son administration est généralement plus complexe et certaines fonctionnalités avancées sont davantage mises en avant dans les versions commerciales.

Prometheus associé à Grafana est aujourd'hui une référence dans les environnements DevOps et Cloud Native. Cette solution est particulièrement adaptée aux architectures basées sur Docker, Kubernetes ou les microservices. Cependant, elle nécessite plusieurs composants pour obtenir une plateforme complète de supervision et n'est pas spécifiquement conçue pour superviser une infrastructure classique composée principalement de serveurs, équipements réseau et machines virtuelles.

Zabbix est une solution de supervision complète qui intègre nativement la collecte des métriques, la gestion des alertes, l'historisation des données et les tableaux de bord. Elle dispose de nombreux modèles de supervision prêts à l'emploi pour Windows, Linux, Proxmox et les équipements réseau. Son architecture correspond particulièrement bien à l'infrastructure actuelle d'EcoSolar Solutions, qui repose principalement sur des serveurs virtualisés et des équipements réseau traditionnels.

3.2 Solution retenue

À l'issue de cette étude, la solution **Zabbix** a été retenue.

Ce choix s'explique par plusieurs raisons :

- Solution entièrement open source

- Architecture tout-en-un simplifiant le déploiement et l'exploitation
- Compatibilité native avec les serveurs Windows, Linux et Proxmox
- Support du protocole SNMP pour les équipements réseau
- Gestion avancée des alertes et des notifications
- Grande communauté et documentation abondante
- Solution particulièrement adaptée à une infrastructure de type PME reposant sur des serveurs et des machines virtuelles

Zabbix répond donc pleinement aux besoins exprimés par EcoSolar Solutions tout en limitant la complexité d'administration et les coûts de mise en œuvre.

---

4. Architecture retenue

4.1 Schéma général de la solution

J'ai choisi de déployer la solution Zabbix sur une nouvelle machine virtuelle Debian 13 hébergée sur l'hyperviseur Proxmox VE de l'entreprise.

Cette machine dispose de l'adresse IP 192.168.128.4/24 et constitue le serveur central de supervision. Son rôle est de collecter les informations provenant des différents équipements supervisés, de stocker les données de supervision et de générer des alertes en cas d'incident.

L'ensemble des équipements critiques de l'entreprise est intégré dans le périmètre de supervision :

- Hyperviseur Proxmox VE
- Firewall pfSense
- Serveur AD (192.168.128.230)
- Serveur DATA (192.168.128.233)
- Serveur GLPI (192.168.128.220)
- Serveur ERP Dolibarr (192.168.128.234)
- Serveur Téléphonie XiVO (192.168.128.217)
- Serveur MAIL Poste.io (192.168.128.219)

4.2 Architecture logique

L'architecture mise en place repose sur un modèle client-serveur.

Le serveur Zabbix collecte les informations remontées par les différents équipements supervisés. Pour cela, un agent Zabbix est installé sur chacun des serveurs Windows et Linux de l'infrastructure.

La communication entre le serveur Zabbix et les agents s'effectue via le protocole TCP sur le port 10050. Le serveur Zabbix interroge régulièrement les agents afin de récupérer les données de supervision.
Le firewall pfSense est supervisé via SNMP.

4.3 Déploiement de la solution

Après la création de la machine virtuelle Debian 13, les différents composants de Zabbix ont été installés et configurés.

Les équipements à superviser ont ensuite été ajoutés dans l'inventaire Zabbix. Pour chaque serveur Windows ou Linux, l'agent Zabbix a été déployé puis associé au serveur de supervision.

Afin de simplifier la configuration et de respecter les bonnes pratiques recommandées par l'éditeur, des modèles (Templates) natifs ont été utilisés pour chaque système d'exploitation.

Ca me permet de bénéficier rapidement d'un ensemble cohérent de métriques, de graphiques et de règles d'alerte sans avoir à créer manuellement chaque élément de supervision.

4.4 Configuration et personnalisation

Une fois la supervision opérationnelle, plusieurs ajustements ont été réalisés afin d'améliorer la qualité des alertes remontées.

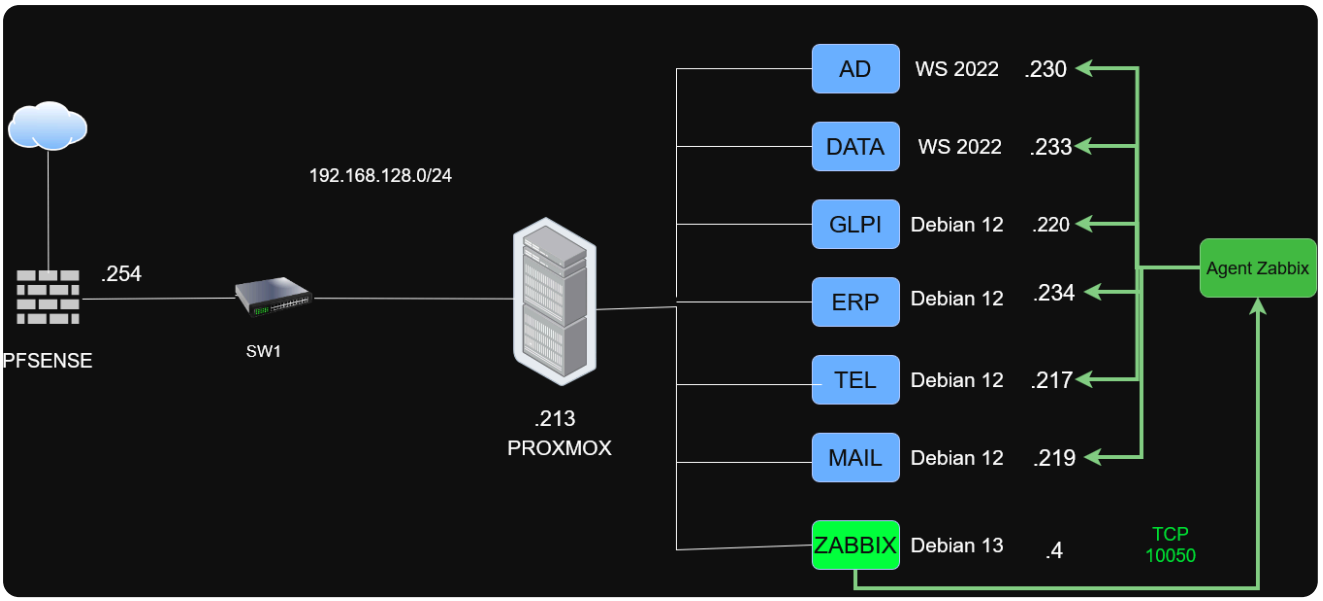
Certains déclencheurs générant des faux positifs ont été désactivés. Par exemple, certains services Windows configurés en démarrage automatique différé ou utilisés uniquement dans des cas spécifiques étaient signalés comme arrêtés alors que leur fonctionnement était normal.

Cette phase d'optimisation a permis de réduire le nombre d'alertes inutiles et de concentrer l'attention des administrateurs sur les événements réellement importants.

Enfin, un tableau de bord personnalisé a été créé afin de fournir une vision synthétique de l'état du système d'information. Ce dashboard permet de visualiser

rapidement la disponibilité des équipements, les incidents en cours ainsi que les principales métriques de performance des serveurs et services critiques.

4.5 Schéma final



---

5. Déploiement de l'infrastructure

- Déploiement de la VM
- Configuration de la VM
- Installation Zabbix
- Déploiement des agents
- Vérification remontée
- Création dashboard
- Configuration envoie mail sur alerte

5. Déploiement de l'infrastructure

5.1 Préparation du serveur Zabbix

Avant de procéder à l'installation de Zabbix, une nouvelle machine virtuelle Debian 13 a été créée sur l'hyperviseur Proxmox VE de l'entreprise.

Afin de respecter les bonnes pratiques d'administration système, plusieurs opérations de préparation ont été réalisées :

- Installation de Debian 13 sans interface graphique afin de limiter la consommation de ressources et la surface d'attaque.
- Configuration d'une adresse IP statique (192.168.128.4/24) dans le fichier `/etc/network/interfaces`.
- Création d'un compte administrateur dédié au projet.
- Ajout de cet utilisateur au groupe sudo afin de permettre l'exécution des tâches d'administration.
- Activation du service SSH pour permettre l'administration à distance.
- Mise à jour complète du système après l'installation.
- Vérification de la connectivité réseau depuis le poste d'administration à l'aide des commandes de test réseau.

Cette phase de préparation permet de disposer d'un système propre, sécurisé et prêt à recevoir les composants de supervision.

5.2 Dimensionnement de la machine virtuelle

*Sources : https://www.zabbix.com/documentation/4.0/fr/manual/installation/requirements

Le dimensionnement de la machine virtuelle a été réalisé à partir des recommandations officielles de Zabbix concernant les environnements de petite et moyenne taille.

L'infrastructure à superviser comprend seulement quelques serveurs virtuels, un hyperviseur et un firewall. Les besoins restent donc relativement modestes comparés aux environnements de production de grande taille.

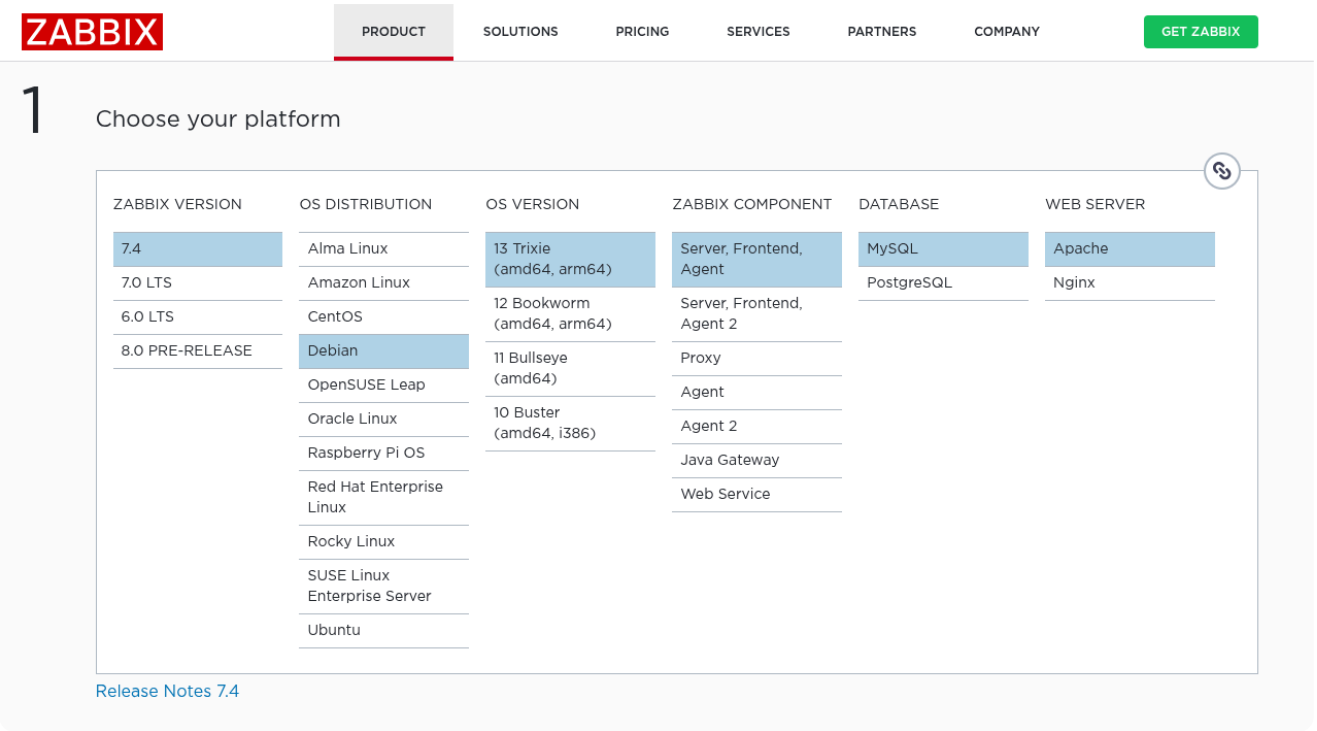
Les préconisations officielles indiquent qu'un environnement de taille moyenne peut fonctionner avec 2 vCPU et 2 Go de mémoire vive pour environ 500 hôtes supervisés.

Compte tenu du faible nombre d'équipements à superviser dans le cadre du projet, les ressources ont été adaptées afin de conserver une marge de fonctionnement tout en limitant la consommation des ressources de l'hyperviseur.

Le stockage a également été dimensionné afin de permettre la conservation de l'historique des métriques collectées et des événements générés par la supervision.

5.3 Installation de Zabbix

Pour le déploiement de la solution, la documentation officielle de Zabbix a été utilisée. Celle-ci fournit les procédures d'installation adaptées à chaque système d'exploitation supporté ainsi que les commandes nécessaires à l'installation des différents composants.



*Sources : https://www.zabbix.com/download?zabbix=7.4&os_distribution=debian&os_version=13&components=server_frontend_agent&db=mysql&ws=apache

L'installation a été réalisée à partir de la documentation correspondant à Zabbix 7.4 sur Debian 13. Cette procédure comprend notamment :

- L'ajout du dépôt officiel Zabbix.
- L'installation du serveur Zabbix.
- L'installation de la base de données MariaDB.
- L'installation de l'interface web.
- L'installation de l'agent Zabbix.
- La configuration des différents services nécessaires au fonctionnement de la plateforme.

L'utilisation de la documentation officielle permet de garantir la compatibilité avec la version déployée et de suivre les recommandations de l'éditeur.

5.4 Vérification du fonctionnement

Une fois l'installation terminée, plusieurs vérifications ont été effectuées afin de valider le bon fonctionnement de la plateforme.

Les services Zabbix, Apache et MariaDB ont été contrôlés afin de s'assurer de leur démarrage automatique et de leur bon état de fonctionnement.

L'accès à l'interface web a ensuite été testé depuis le poste d'administration afin de vérifier l'accessibilité du portail de supervision.

Enfin, les premiers équipements ont été intégrés dans Zabbix afin de confirmer la remontée correcte des informations de supervision et la communication entre les agents et le serveur Zabbix.

6. Mise en supervision des équipements

Après la validation du fonctionnement de la plateforme Zabbix, les équipements critiques d'EcoSolar
Solutions ont été intégrés dans le périmètre de supervision. Cette partie présente la mise en supervision des
serveurs Windows et Linux, du firewall pfSense, du cluster Proxmox VE, ainsi que la création du tableau de
bord et du système de notification.
La structure retenue suit la logique du déploiement : ajout des hôtes, collecte par agent ou par protocole
adapté, visualisation des données, puis validation par des tests d'alerte.

6.1

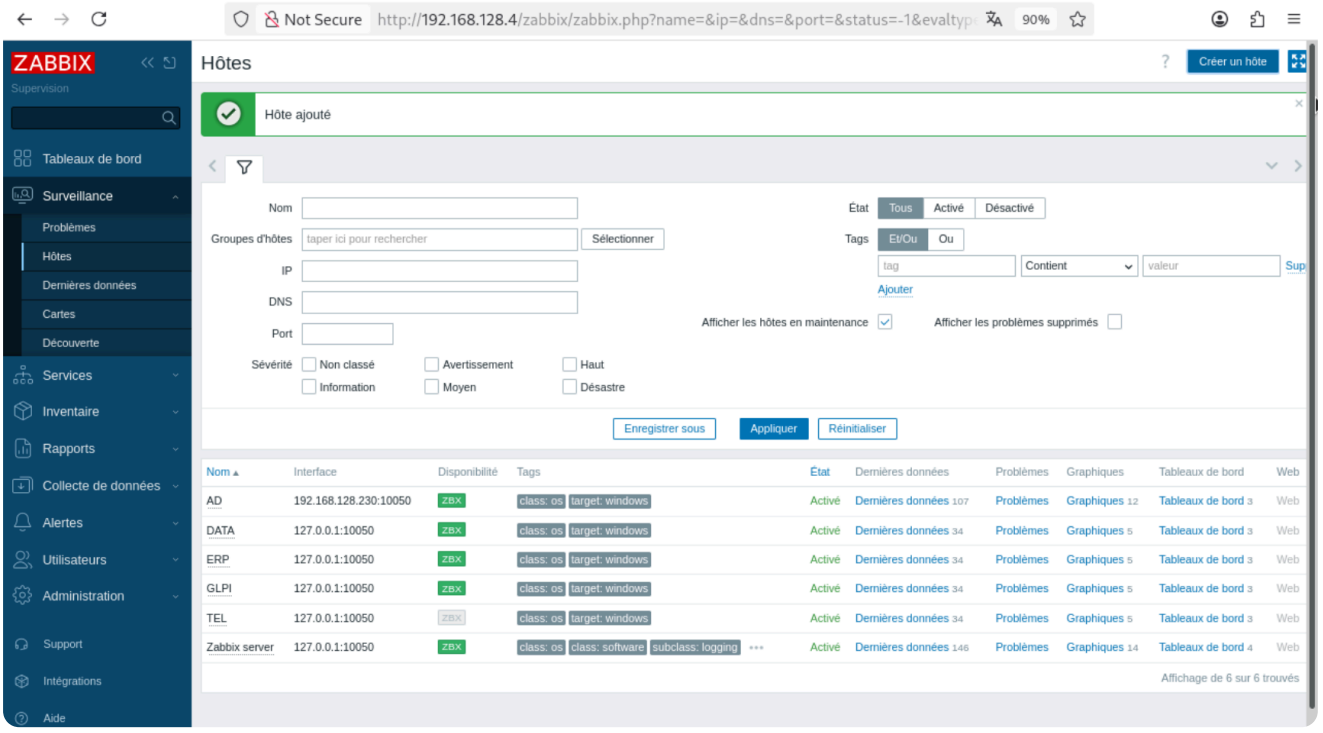
Objectif

Déclarer dans Zabbix les équipements à superviser afin de centraliser la surveillance des serveurs et
services critiques de l'entreprise.

Réalisation

• Les serveurs AD, DATA, ERP, TEL, MAIL et le serveur Zabbix ont été ajoutés comme hôtes supervisés par
agent Zabbix.

• Le firewall pfSense a été ajouté avec une interface SNMP sur le port UDP 161.
• Le cluster Proxmox VE a été ajouté avec le modèle Proxmox VE by HTTP afin d'interroger l'API sur le port
8006.
• Les hôtes ont été organisés dans des groupes comme Virtual machines et Hypervisors pour faciliter le
filtrage et l'exploitation.



Résultat obtenu

La liste des hôtes confirme que les équipements supervisés apparaissent dans Zabbix avec leur état actif.
Les serveurs supervisés par agent disposent d'un indicateur ZBX.

6.2 Déploiement des agents Zabbix sur les serveurs Windows et Linux

Objectif

Collecter les métriques système des serveurs Windows et Linux : disponibilité, CPU, mémoire, stockage, réseau et état de l'agent.

Réalisation

Sur les serveurs Windows AD et DATA, l'agent Zabbix a été installé à partir du paquet MSI officiel.
• Le port TCP 10050 a été autorisé dans le pare-feu Windows afin de permettre au serveur Zabbix
d'interroger l'agent.
• Sur les serveurs Linux ERP, TEL et MAIL, le dépôt Zabbix 7.4 a été ajouté puis l'agent zabbix-agent a été
installé.
• Le fichier /etc/zabbix/zabbix_agentd.conf a été adapté avec l'adresse du serveur Zabbix, l'option
ServerActive et le nom d'hôte correspondant.
• Les services agents ont été redémarrés et activés au démarrage avec systemctl.

Déploiement des agents Zabbix, avec Linux pour ERP/TEL/MAIL

```
apt update
apt install wget gnupg -y
wget https://repo.zabbix.com/zabbix/7.4/release/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.4+debian12_all.deb
dpkg -i zabbix-release_latest_7.4+debian12_all.deb
apt update
apt install zabbix-agent -y
nano /etc/zabbix/zabbix_agentd.conf
systemctl restart zabbix-agent
systemctl enable zabbix-agent
systemctl status zabbix-agent
```

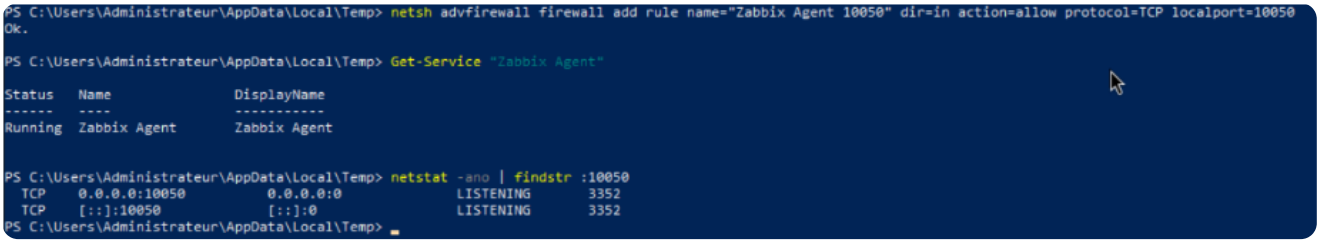
Déploiement des agents Zabbix, avec Powershell pour DATA et AD qui sont sous Windows Server

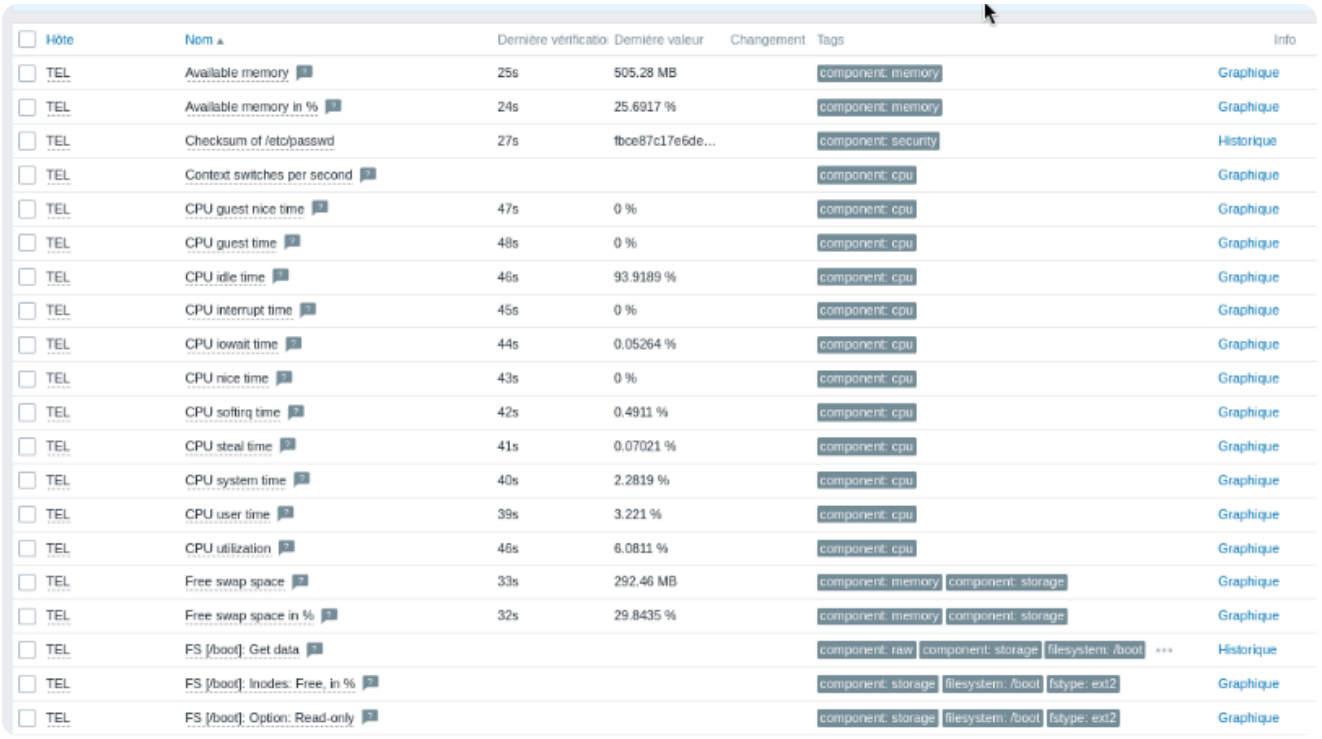
```
cd $env:TEMP
Invoke-WebRequest -Uri "https://cdn.zabbix.com/zabbix/binaries/stable/7.4/7.4.11/zabbix_agent-7.4.11-windows-amd64-openssl.msi" -OutFile "zabbix_agent.msi"
msiexec /i zabbix_agent.msi /qn SERVER=192.168.128.4 SERVERACTIVE=192.168.128.4 HOSTNAME=DATA/AD
Start-Service "Zabbix Agent"
Set-Service "Zabbix Agent" -StartupType Automatic
netsh advfirewall firewall add rule name="Zabbix Agent 10050" dir=in action=allow protocol=TCP localport=10050
Get-Service "Zabbix Agent"
```

netstat -ano | findstr :10050
notepad "C:\Program Files\Zabbix Agent\zabbix_agentd.conf"
Restart-Service "Zabbix Agent"
Get-Service "Zabbix Agent"

Capture

Le fonctionnement du déploiement de supervision est démontrable à travers la présence de l'agent zabbix dans le serveur mais aussi à travers l'interface de zabbix visant à démontrer l'accès constant au serveur et à ce qui est supervisé dessus. Il y a donc une communication entre le serveur zabbix et les agents.





Hôte	Nom	Dernière vérificatio	Dernière valeur	Changement	Tags	Info
TEL	Available memory	25s	505.28 MB		component: memory	Graphique
TEL	Available memory in %	24s	25.6917 %		component: memory	Graphique
TEL	Checksum of /etc/passwd	27s	fbce87c17e6de...		component: security	Historique
TEL	Context switches per second				component: cpu	Graphique
TEL	CPU guest nice time	47s	0 %		component: cpu	Graphique
TEL	CPU guest time	48s	0 %		component: cpu	Graphique
TEL	CPU idle time	46s	93.9189 %		component: cpu	Graphique
TEL	CPU interrupt time	45s	0 %		component: cpu	Graphique
TEL	CPU iowait time	44s	0.05264 %		component: cpu	Graphique
TEL	CPU nice time	43s	0 %		component: cpu	Graphique
TEL	CPU softirq time	42s	0.4911 %		component: cpu	Graphique
TEL	CPU steal time	41s	0.07021 %		component: cpu	Graphique
TEL	CPU system time	40s	2.2819 %		component: cpu	Graphique
TEL	CPU user time	39s	3.221 %		component: cpu	Graphique
TEL	CPU utilization	46s	6.0811 %		component: cpu	Graphique
TEL	Free swap space	33s	292.46 MB		component: memory, component: storage	Graphique
TEL	Free swap space in %	32s	29.8435 %		component: memory, component: storage	Graphique
TEL	FS [/boot]: Get data				component: raw, component: storage, filesystem: /boot	Historique
TEL	FS [/boot]: Inodes: Free, in %				component: storage, filesystem: /boot, fstype: ext2	Graphique
TEL	FS [/boot]: Option: Read-only				component: storage, filesystem: /boot, fstype: ext2	Graphique

Résultat obtenu

Les réseaux communiquent correctement.

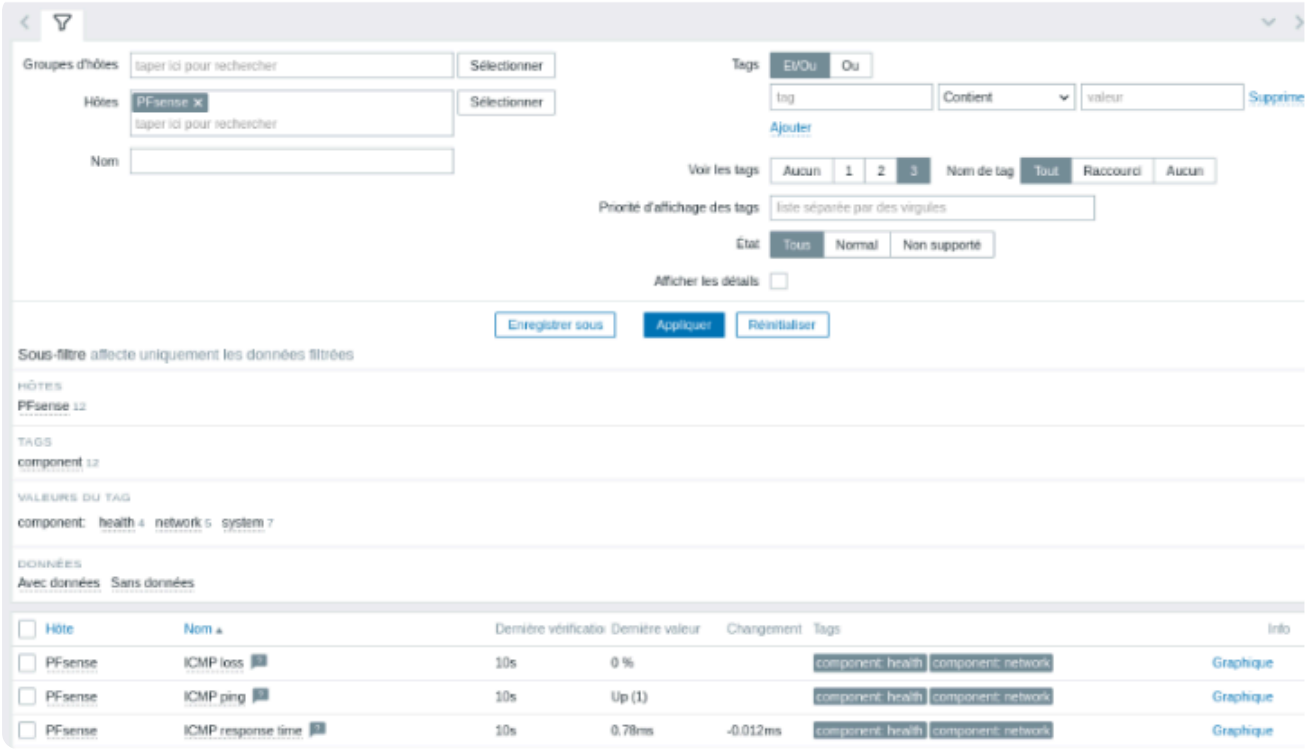
6.3 Supervision du firewall pfSense via SNMP

Objectif

Superviser le firewall pfSense sans installer d'agent, en utilisant le protocole SNMP adapté aux équipements
réseau.

Réalisations

Le service SNMP a été activé dans l'interface pfSense.
• La communauté de lecture utilisée dans le lab est public et l'écoute a été limitée à l'interface LAN.
• Une règle firewall a été ajoutée pour autoriser le serveur Zabbix 192.168.128.4 à interroger pfSense en
UDP 161.
• Dans Zabbix, l'hôte pfSense a été configuré avec une interface SNMP et le modèle Generic by SNMP.



Résultat obtenu

Le test snmpwalk retourne le nom système Firewall-01.ecosolarsolutions.local. Cela confirme que Zabbixpeut

interroger le firewall via SNMP et que la règle UDP 161 est opérationnelle.

6.4 Intégration du cluster Proxmox VE via HTTP/API

Objectif

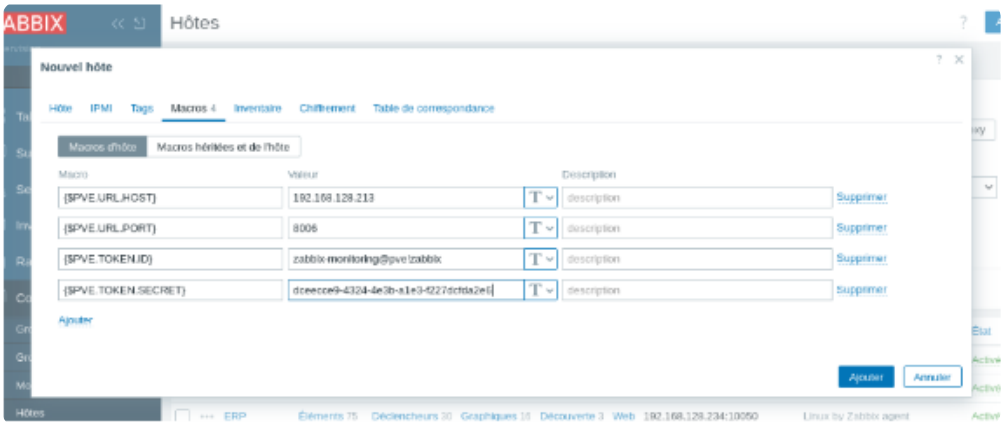
Superviser l'infrastructure de virtualisation Proxmox VE afin d'obtenir l'état des noeuds, des machines virtuelles, des conteneurs et des stockages.

Réalisation

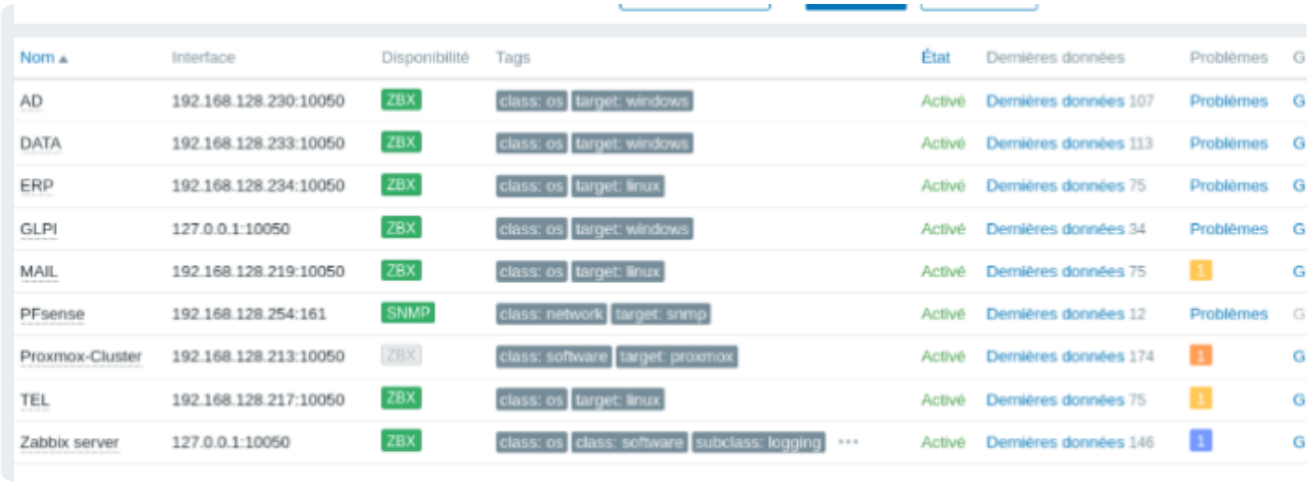
• Un utilisateur dédié zabbix-monitoring@pve a été créé dans Proxmox afin d'éviter l'utilisation du compte
administrateur root@pam.
• Un jeton d'API a été généré pour permettre à Zabbix d'interroger Proxmox de manière sécurisée.
• Le rôle PVEAuditor a été attribué sur le chemin / avec propagation activée, ce qui donne un accès en
lecture seule adapté à la supervision.
• Dans Zabbix, l'hôte Proxmox-Cluster utilise le modèle Proxmox VE by HTTP et les macros
{PVE.URL.HOST}, {PVE.URL.PORT}, {PVE.TOKEN.ID} et {PVE.TOKEN.SECRET}.

“Pasted image 20260611024717.png” ne peut être trouvé.

Permission PVEAuditor accordée à l'utilisateur de supervision.



Macros utilisées par le modèle Proxmox VE by HTTP.



Nom ▲	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	G
AD	192.168.128.230:10050	ZBX	class: os target: windows	Activé	Dernières données 107	Problèmes	G
DATA	192.168.128.233:10050	ZBX	class: os target: windows	Activé	Dernières données 113	Problèmes	G
ERP	192.168.128.234:10050	ZBX	class: os target: linux	Activé	Dernières données 75	Problèmes	G
GLPI	127.0.0.1:10050	ZBX	class: os target: windows	Activé	Dernières données 34	Problèmes	G
MAIL	192.168.128.219:10050	ZBX	class: os target: linux	Activé	Dernières données 75	1	G
PFsense	192.168.128.254:161	SNMP	class: network target: snmp	Activé	Dernières données 12	Problèmes	G
Proxmox-Cluster	192.168.128.213:10050	ZBX	class: software target: proxmox	Activé	Dernières données 174	1	G
TEL	192.168.128.217:10050	ZBX	class: os target: linux	Activé	Dernières données 75	1	G
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software subclass: logging •••	Activé	Dernières données 146	1	G

Hôte Proxmox-Cluster avec données remontées dans Zabbix.

Résultat obtenu

Le cluster Proxmox remonte ses informations par l'API HTTPS sur le port 8006. Le badge ZBX peut rester
gris car la supervision ne passe pas par l'agent 10050, mais les dernières données et les problèmes.
Proxmox confirment la collecte HTTP/API.

6.5 Création et personnalisation du tableau de bord

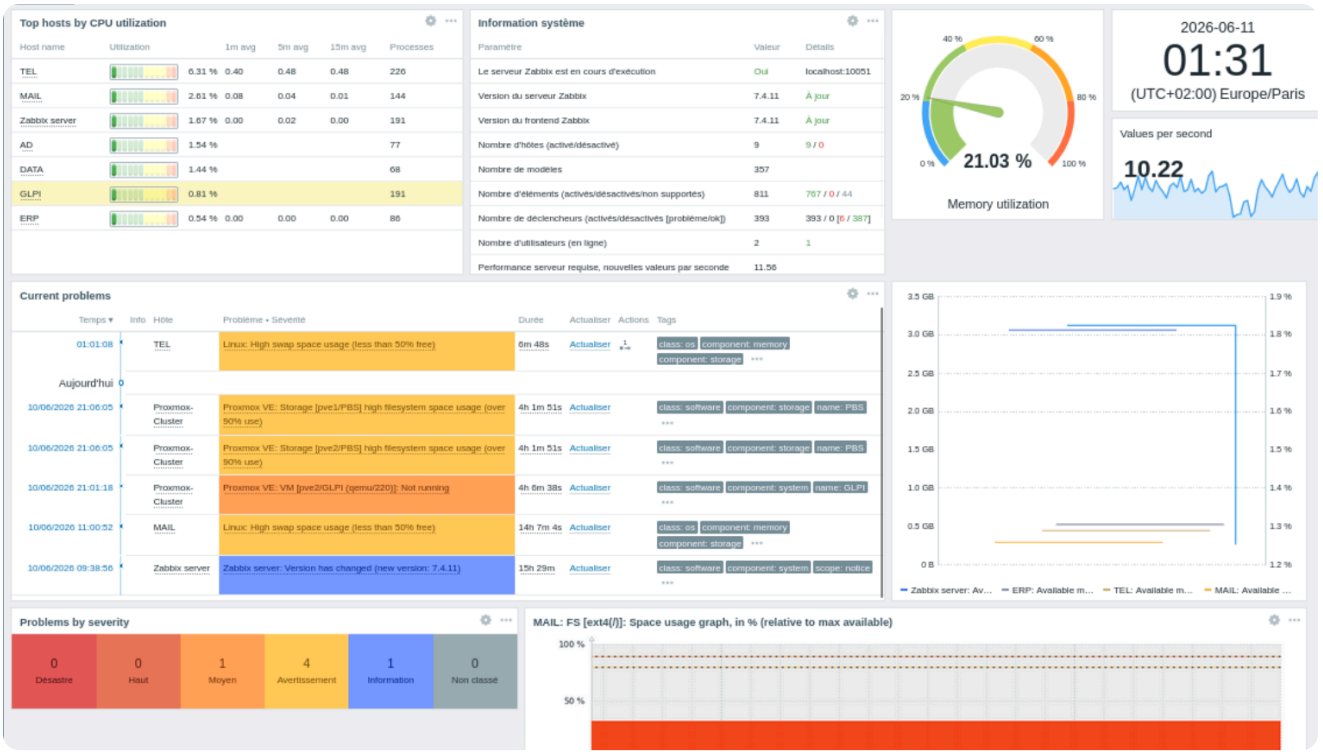
Objectif

Fournir une vue synthétique permettant d'identifier rapidement l'état de l'infrastructure et les incidents en
cours

Réalisation

• Le tableau de bord regroupe les widgets de disponibilité des hôtes, problèmes courants, problèmes par
sévérité, utilisation CPU et mémoire.
• Des widgets spécifiques ont été ajoutés pour les serveurs ayant des rôles particuliers, par exemple le
stockage et la swap pour le serveur MAIL.
• Les données Proxmox et pfSense permettent aussi de suivre l'état de l'infrastructure de virtualisation et du
firewall.

Tableau de bord de supervision personnalisé



Le tableau de bord permet de visualiser en un seul écran les hôtes disponibles, les problèmes actifs, les
niveaux de sévérité, les indicateurs de charge et les points sensibles comme le stockage

---

6.6 Mise en place du système d'alerting par e-mail

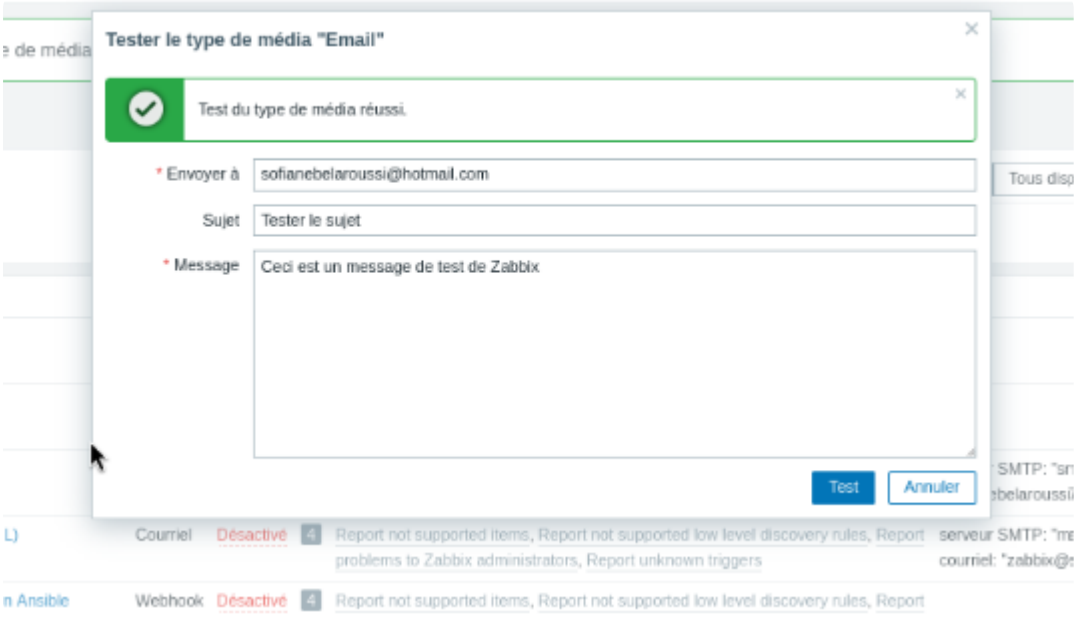
Objectif

Alerter automatiquement l'administrateur lorsqu'un incident est détecté, par exemple une VM arrêtée, un agent indisponible ou un seuil de stockage dépassé

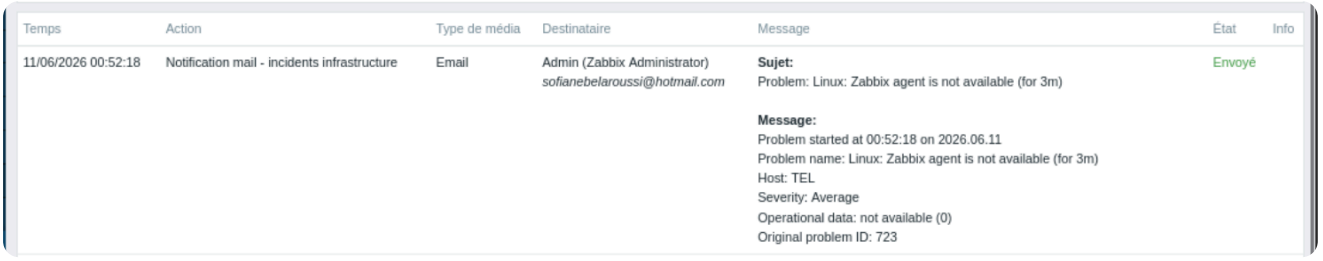
Réalisation
• Un type de média Email a été configuré dans Zabbix avec un compte Gmail et un mot de passe
d'application.
• Le média Email a été associé à l'utilisateur administrateur Zabbix avec une disponibilité 24h/24 et 7j/7.
• Une action de déclencheur a été créée avec la condition Sévérité du déclencheur

supérieure ou égale à Avertissement.
• L'opération envoie un message à l'utilisateur Admin via le média Email.

Test réussi du type de média Email afin de voir si le mail est joignable.

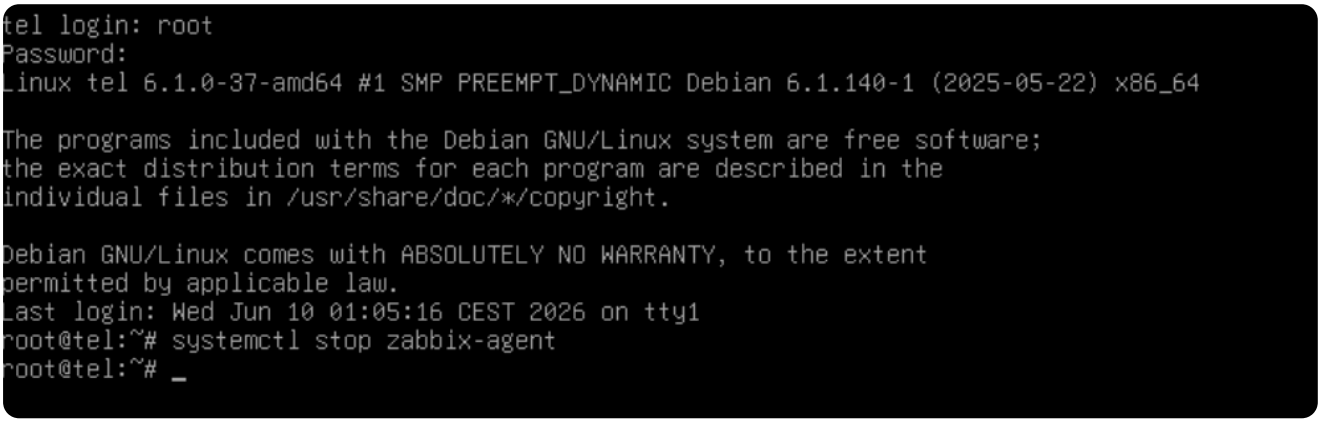


Dans le journal des notifications on peut y voir que la notification a été envoyé



6.7 Tests de validation de la supervision

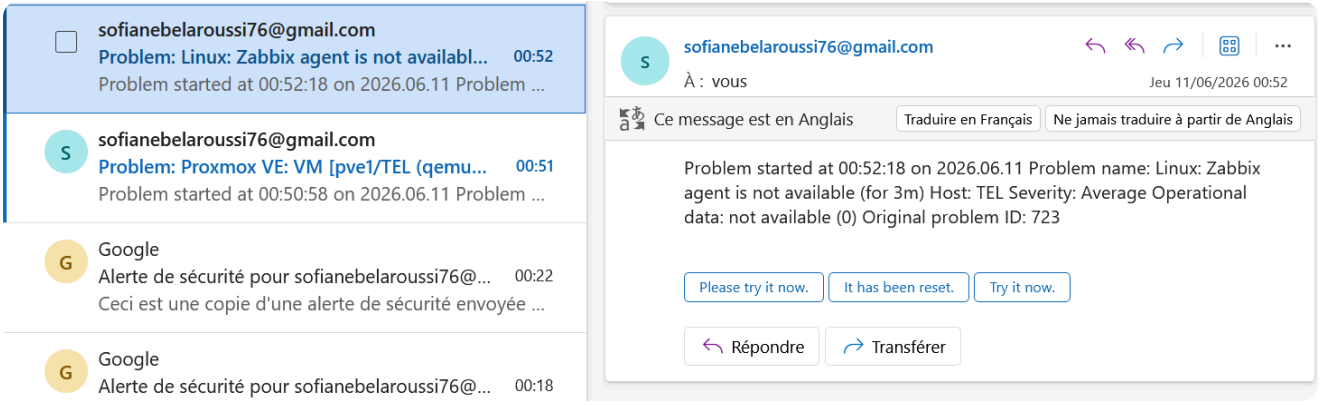
Le test a été fait avec le serveur TEL, qui a été éteint afin de voir si l'on est notifié par mail



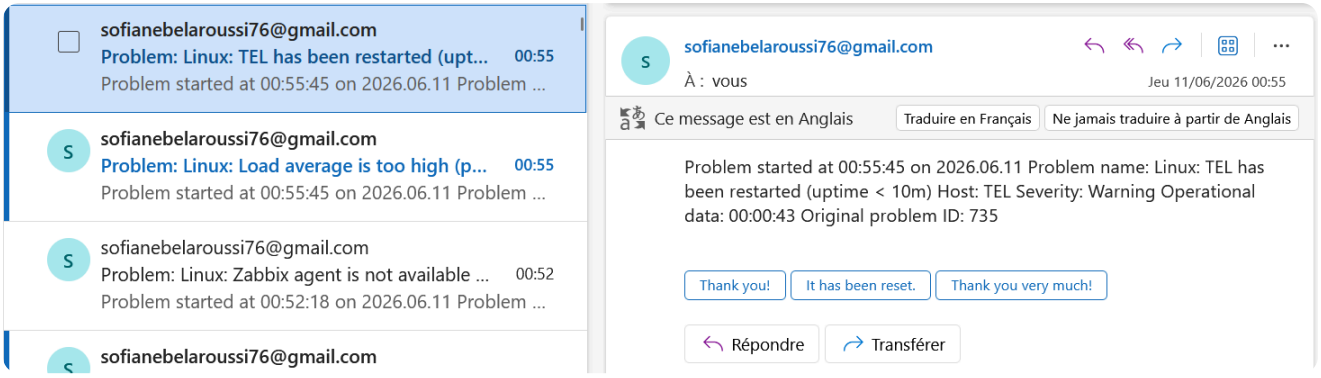
Objectif

Valider le fonctionnement réel de la supervision et de l'alerting en provoquant des incidents contrôlés

On peut voir que l'arrêt de marche du serveur est remonté sur l'adresse mail



On peut voir aussi qu'après la réactivation du serveur l'apparition d'un mail comme quoi le serveur s'est redémarré



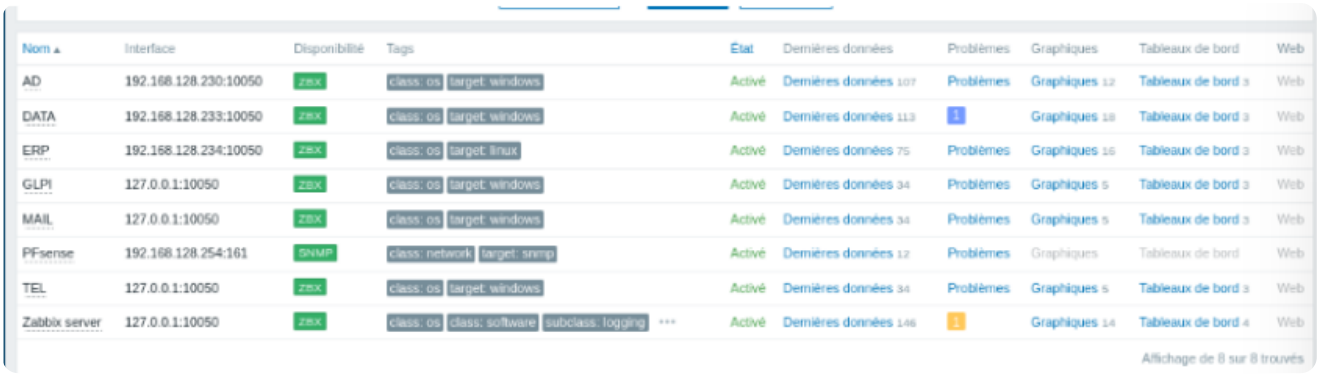
Résultats obtenues

Zabbix détecte les incidents attendus et déclenche les notifications configurées. Les tests confirment la cohérence entre les métriques collectées, les déclencheurs et le système d'alerte.

6.8. Tests et validation

Méthodologie

La supervision mise en place répond aux attentes d'EcoSolar Solutions : elle permet de centraliser la surveillance, de suivre les performances, de détecter les incidents et d'alerter automatiquement l'administrateur en cas d'anomalie.



Nom ▲	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	Graphiques	Tableaux de bord	Web
AD	192.168.128.230:10050	ZBX	class: os target: windows	Activé	Dernières données 107	Problèmes	Graphiques 12	Tableaux de bord 3	Web
DATA	192.168.128.233:10050	ZBX	class: os target: windows	Activé	Dernières données 113	1	Graphiques 18	Tableaux de bord 3	Web
ERP	192.168.128.234:10050	ZBX	class: os target: linux	Activé	Dernières données 75	Problèmes	Graphiques 16	Tableaux de bord 3	Web
GLPI	127.0.0.1:10050	ZBX	class: os target: windows	Activé	Dernières données 34	Problèmes	Graphiques 5	Tableaux de bord 3	Web
MAIL	127.0.0.1:10050	ZBX	class: os target: windows	Activé	Dernières données 34	Problèmes	Graphiques 5	Tableaux de bord 3	Web
PFsense	192.168.128.254:161	SNMP	class: network target: snmp	Activé	Dernières données 12	Problèmes	Graphiques	Tableaux de bord	Web
TEL	127.0.0.1:10050	ZBX	class: os target: windows	Activé	Dernières données 34	Problèmes	Graphiques 5	Tableaux de bord 3	Web
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software subclass: logging •••	Activé	Dernières données 146	1	Graphiques 14	Tableaux de bord 4	Web

Affichage de 8 sur 8 trouvés

---

7. Conclusion

Le projet a permis de répondre aux objectifs fixés par EcoSolar Solutions : mettre en place une supervision centralisée, surveiller les serveurs et équipements critiques, visualiser l'état de l'infrastructure et recevoir des alertes en cas d'incident.

Zabbix a été installé sur une VM Debian 13 dédiée. Les serveurs Windows et Linux ont été supervisés avec l'agent Zabbix, le firewall pfSense via SNMP et le cluster Proxmox VE via l'API HTTP. Un tableau de bord personnalisé a également été créé afin de suivre rapidement les métriques importantes : disponibilité, CPU, mémoire, disque, état des agents, stockage et machines virtuelles.

Le système d'alerting par e-mail a été testé avec l'arrêt de la VM TEL. L'incident a bien été détecté par Zabbix et une notification a été envoyée à l'administrateur. La solution est donc fonctionnelle et adaptée à une infrastructure de type PME.

---

8. Perspectives d'amélioration

Plusieurs améliorations peuvent être envisagées pour rendre la solution plus complète et plus proche d'un environnement de production :

- passer de SNMPv2 à SNMPv3 pour sécuriser la supervision de pfSense ;
- ajouter des alertes personnalisées sur les sauvegardes, l'espace disque DATA et les services critiques ;
- sécuriser l'accès à Zabbix avec HTTPS, des comptes nominatifs et des droits adaptés ;
- étendre la supervision aux futurs serveurs et équipements réseau de l'entreprise.

Glossaire

Zabbix
Outil de supervision open source permettant de surveiller les serveurs, les équipements réseau, les services et les performances du système d'information, avec un système d'alertes et de tableaux de bord.

Supervision
Ensemble des mécanismes permettant de surveiller en temps réel l'état, la disponibilité et les performances des équipements et services informatiques.

Monitoring
Terme anglais désignant la supervision continue des systèmes informatiques afin de détecter les anomalies et anticiper les incidents.

Alerting
Mécanisme de notification automatique déclenché lorsqu'un seuil critique est dépassé ou lorsqu'un incident est détecté (mail, SMS, etc.).

Dashboard (tableau de bord)
Interface graphique regroupant des indicateurs clés permettant de visualiser rapidement l'état du système d'information.

CPU (Central Processing Unit)
Processeur de la machine chargé d'exécuter les instructions. Sa charge permet d'évaluer les performances d'un serveur.

RAM (Random Access Memory)
Mémoire vive utilisée par le système pour exécuter les applications. Une saturation de

la RAM peut entraîner un ralentissement ou une panne.

Trafic réseau

Volume de données échangées sur une interface réseau. Il permet d'analyser la charge, les
performances et les éventuels goulots d'étranglement.

SNMP (Simple Network Management Protocol)

Protocole permettant de collecter des informations sur les équipements réseau (switch, firewall, routeur) à des fins de supervision.

SNMPv2

Version de SNMP utilisant une communauté en clair pour l'authentification. Simple à mettre en
œuvre mais moins sécurisée.

SNMPv3

Version sécurisée de SNMP intégrant une authentification et un chiffrement des échanges,
recommandée pour respecter les bonnes pratiques de sécurité.

Agent Zabbix

Logiciel installé sur un serveur permettant de transmettre les métriques système (CPU, RAM, disque, services) au serveur Zabbix.