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

- Projet 1 - BTS SIO SISR
  - Supervision et alerting des services critiques
    - Société : EcoSolar Solutions
- Sommaire
- 1. Présentation de l'entreprise
  - 1.1 Contexte
  - 1.2 Présentation du système d'information existant
  - 1.3 Schéma de l'infrastructure actuelle
  - 1.4 Objectifs du projet

- 2. Analyse du besoin
  - 2.1 Besoins de l'entreprise
  - 2.2 Contraintes du projet
  - 2.3 Attentes de l'entreprise
- 3. Étude des solutions
  - 3.1 Comparaison
    - 3.2 Analyse des solutions
  - 3.2 Solution retenue
- 4. Architecture retenue
  - 4.1 Schéma général de la solution
  - 4.2 Architecture logique
  - 4.3 Déploiement de la solution
  - 4.4 Configuration et personnalisation
  - 4.5 Schéma final
  - 4.6 Schéma logique et flux
- 5. Déploiement de l'infrastructure
- 5. Déploiement de l'infrastructure
  - 5.1 Préparation du serveur Zabbix
  - 5.2 Dimensionnement de la machine virtuelle
  - 5.3 Installation de Zabbix
  - 5.4 Vérification du fonctionnement
- 5.1 Installation des pare-feu
  - Objectif
  - Réalisation
    - Capture
    - Résultat obtenu
- 5.2 Mise en place du VPN IPsec
  - Objectif
  - Réalisation
    - Capture
    - Résultat obtenu
- 5.3 Installation Active Directory
- 5.4 Automatisation PowerShell
  - Objectif
  - Script

    - Résultat
- 5.5 Serveur de fichiers
- 5.6 GPO
- 5.7 GLPI
- 5.8 Dolibarr
- 6. Tests et validation
    - 6.1 Méthodologie
    - 6.2 Tableau de tests
- 7. Exploitation et maintenance
    - 7.1 Supervision
        - Captures
    - 7.2 Sauvegardes
        - Procédure de restauration
- 8. Sécurité
    - 8.1 Audit Active Directory
        - Outil
        - Résultats
        - Recommandations
    - 8.2 Audit Linux
        - Outil
        - Résultats
        - Recommandations
- 9. Gestion des incidents
    - Procédure
        - Exemple de ticket
- 10. Conclusion
- 11. Perspectives d'amélioration
- Glossaire

---

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 :

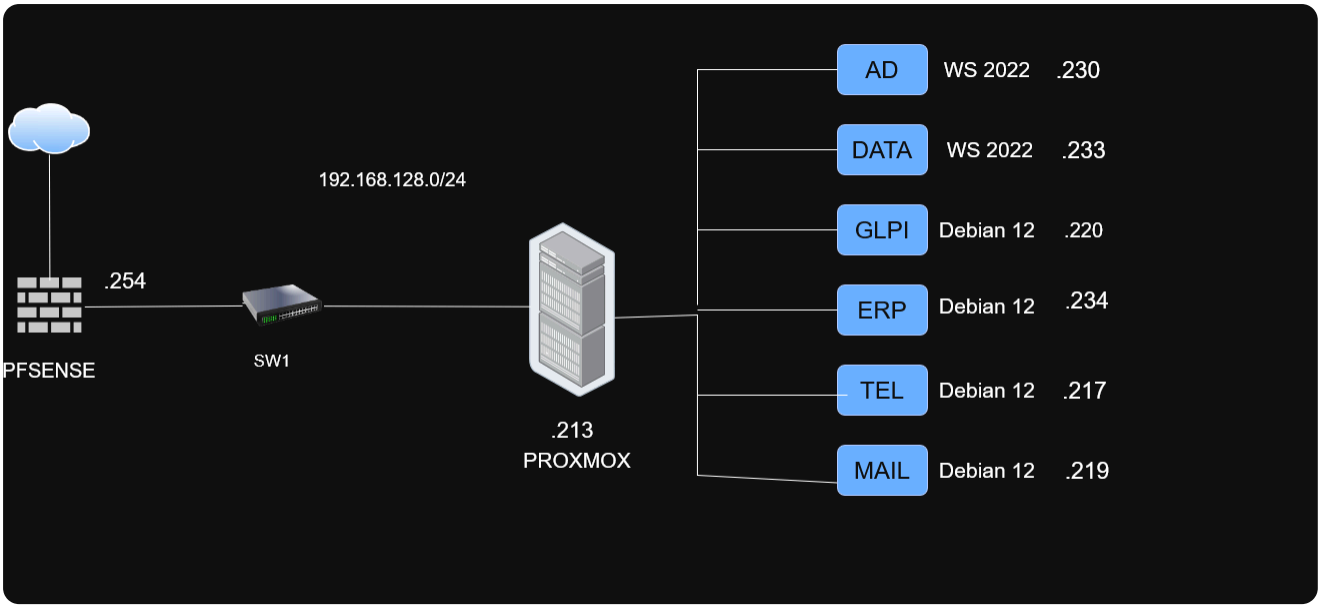
- Un contrôleur de domaine Active Directory assurant les services AD, DNS et DHCP
- Un serveur de fichiers destiné au stockage et au partage des données
- Un serveur ERP Dolibarr utilisé pour la gestion de l'activité de l'entreprise
- Un serveur de téléphonie IP XiVO
- Un serveur de messagerie Poste.io
- Un serveur GLPI utilisé pour la gestion du parc informatique et des tickets d'assistance

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
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

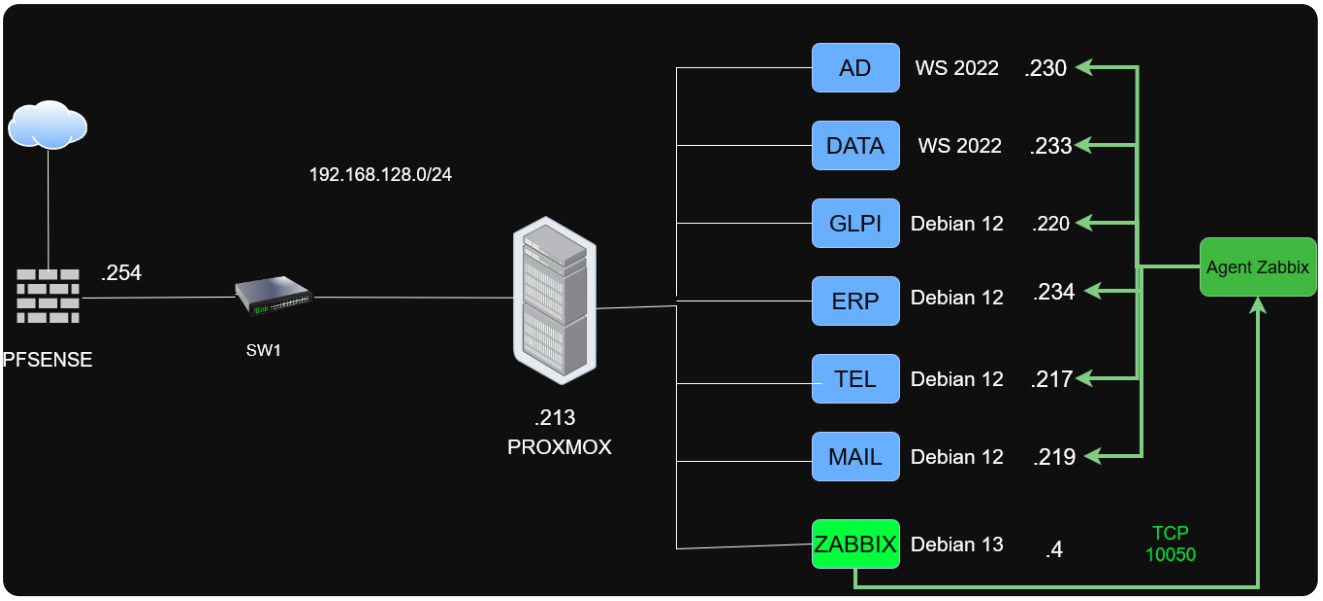
Une fois la supervision opérationnelle, plusieurs ajustements ont été réalisés afin d'améliorer la qualité des alertes remontées.

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.

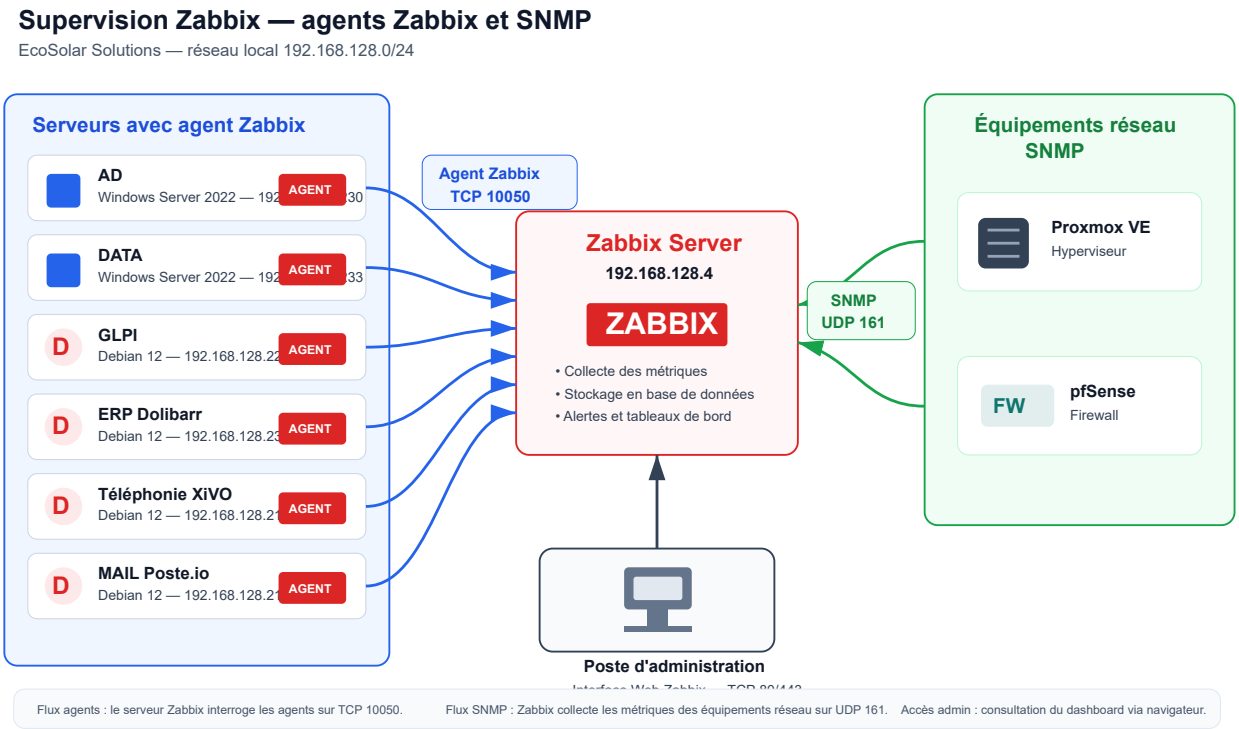
Cette phase d'optimisation a permis de réduire le nombre d'alertes inutiles et de concentrer l'attention des administrateurs sur les événements réellement importants.

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



4.6 Schéma logique et flux



5. Déploiement de l'infrastructure

- Déploiement de la VM
- COnfiguration de la VM
- Installation Zabbix
- Déploiement des agents
- Vérification remontée
- Désactivation indicateurs non essentiels (faux positifs)
- 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.

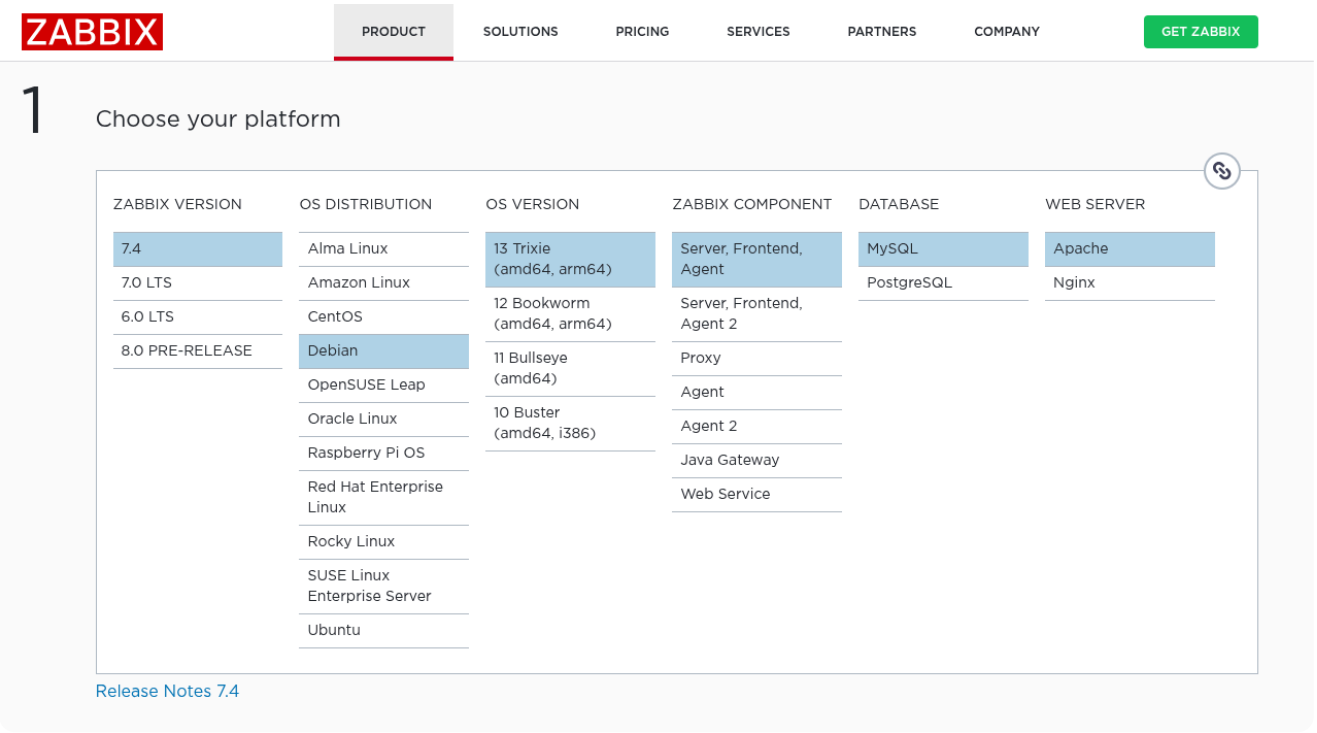
Les préconisations officielles indiquent qu'un environnement de taille moyenne peut fonctionner avec 2 vCPU et 2 Go de mémoire vive pour environ 500 hôtes supervisés.

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.

5.1 Installation des pare-feu

Objectif

Mettre en place la connectivité réseau.

Réalisation

Description.

Capture

(Insérer capture)

Résultat obtenu

La configuration est opérationnelle.

5.2 Mise en place du VPN IPsec

Objectif

Connecter les deux sites.

Réalisation

Description.

Capture

(Insérer capture)

Résultat obtenu

Les réseaux communiquent correctement.

5.3 Installation Active Directory

Même structure.

5.4 Automatisation PowerShell

Objectif

Automatiser la création des comptes.

Script

(Code)

Résultat

Description.

5.5 Serveur de fichiers

Même structure.

5.6 GPO

Même structure.

5.7 GLPI

Même structure.

5.8 Dolibarr

Même structure.

---

6. Tests et validation

6.1 Méthodologie

Les tests ont été réalisés afin de valider le fonctionnement de chaque composant.

6.2 Tableau de tests

Test	Résultat attendu	Résultat obtenu	Statut
Ping inter-sites	Réponse	OK	Validé
Connexion VPN	Connexion réussie	OK	Validé
Ouverture session AD	Authentification	OK	Validé

---

7. Exploitation et maintenance

7.1 Supervision

Présentation de Prometheus.

Captures

(Graphiques)

7.2 Sauvegardes

Description du plan de sauvegarde.

Procédure de restauration

Étapes détaillées.

---

8. Sécurité

8.1 Audit Active Directory

Outil

PingCastle

Résultats

Analyse.

Recommandations

Liste des actions correctives.

8.2 Audit Linux

Outil

Lynis

Résultats

Analyse.

Recommandations

Liste des actions correctives.

---

9. Gestion des incidents

Procédure

1. Détection
2. Qualification

3. Affectation
4. Résolution
5. Clôture

Exemple de ticket

(Capture GLPI)

---

10. Conclusion

Le projet a permis de mettre en place une infrastructure multi-sites sécurisée répondant aux besoins de VitaBigPharma.

Les principaux objectifs ont été atteints :

- authentification centralisée
- partage sécurisé des données
- communication inter-sites
- télétravail sécurisé
- supervision
- sauvegarde

La conclusion doit présenter les résultats par rapports aux besoins identifiés dans la section "2.1 Besoins fonctionnels"

---

11. Perspectives d'amélioration

Les évolutions possibles sont :

- haute disponibilité des pare-feux
- supervision avancée
- SIEM
- MFA
- PRA/PCA
- automatisation Ansible

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.
OID (Object Identifier)
Identifiant unique permettant de récupérer une information précise via SNMP (ex : trafic d'une
interface, état d'un port).
MIB (Management Information Base)
Base de données regroupant l'ensemble des OID disponibles sur un équipement supervisé via
SNMP.

CIA / DIC (Confidentialité, Intégrité, Disponibilité)
Principes fondamentaux de la sécurité informatique visant à protéger les données contre
l'accès non autorisé, la modification et l'indisponibilité.
Agent Zabbix
Logiciel installé sur un serveur permettant de transmettre les métriques système (CPU, RAM,
disque, services) au serveur Zabbix.
SNMP polling
Méthode par laquelle Zabbix interroge régulièrement un équipement SNMP afin de collecter
des données.