Scénario 3 - Supervision et alerting des services critiques

Supervision

Noms : **NDONGO TOVOR**

Prénoms : **Moïse Glory**

Classe BTS 2 SIO / Groupe 1

Année 2026

Entreprise fictive : EcoSolar Solutions

Sommaires

Table des matières

Analyse du besoin

Contexte général

Ecosolar Solutions est une entreprise Française fondée en 2010, dédiée au développement et à la fabrication de panneaux solaires à haut rendement. Basée à Toulouse, elle réunit près d'une cinquantaine de collaborateurs répartis entre les bureaux et un atelier de production de haute technologie, avec une perspective de croissance atteignant 80 salariés dans les prochaines années. L'entreprise évolue dans un secteur exigeant, où innovation, performance énergétique et maîtrise de la chaîne de production constituent des enjeux majeurs.

Depuis plusieurs années, l'infrastructure informatique interne n'a pas bénéficié des investissements nécessaires et s'est principalement construite par ajouts successifs, sans véritable schéma directeur. Avec l'augmentation de la production, la montée en puissance de l'ERP/CRM, la sensibilité accrue des données (brevets, secrets industriels, documents internes) et la nécessité d'assurer la mobilité des équipes commerciales, le SI montre ses limites. L'entreprise EcoSolar décide d'investir dans le renouvellement et sa modernisation de son infrastructure réseaux. Ainsi, il décide de faire appel à l'entreprise WILD CORP, dont je fais partie, pour les accompagnés dans ce projet.

Mon projet vise à améliorer l'infrastructure de l'entreprise EcoSolar solution en mettant en place un superviseur d'infrastructure moderne, qui permettra à l'entreprise de veiller sur l'intégralité de son équipements informatiques. Notre mission couvre notamment l'analyse du SI existant, la définition d'une architecture cible moderne et sécurisée, l'intégration du datacenter récemment acquis, ainsi que la mise en place de mesures de sécurité conformes aux bonnes pratiques actuelles (segmentation réseau, gestion des accès distants, renforcement des services critiques, souveraineté des données, etc…).

Contexte Technique

Avant l'intervention de WildCorp, le système d'information d'EcoSolar Solutions reposait sur une infrastructure locale relativement simple, construite au fil du temps par petites évolutions successives. L'ensemble du réseau et des services informatiques fonctionne, mais sans réelle cohérence d'architecture ni prise en compte des bonnes pratiques modernes en matière de sécurité, performance ou de résilience.

Réseau actuel

L'infrastructure réseau interne est organisée autour d'un **unique réseau local IPv4 192.168.10.0/24**, sans aucune segmentation ni VLAN. Tous les équipements (serveurs, postes utilisateurs, tablettes, imprimantes, VoIP, ERP, etc.) cohabitent donc sur le même plan d'adressage, ce qui augmente les risques de sécurité et complique le diagnostic en cas d'incident. Le switch principal est un **Cisco 3560** configuré par défaut, un seul VLAN, aucun routage inter-VLAN, aucun contrôle d'accès, ni gestion avancée.
Un seul point d'accès Wi-Fi (Cisco C9136I) dessert l'ensemble des collaborateurs de bureau et de l'atelier, en WPA2, sans réseau séparé invité ou industriel.

Infrastructures informatiques

Le cœur du SI repose sur un unique serveur physique **DELL PowerEdge R720** qui héberge un hyperviseur **Proxmox VE** faisant tourner six machines virtuelles :

- Un serveur Windows AD/DNS/DHCP,
- Un serveur Windows pour le partage de fichiers,
- Trois serveurs Debian (ERP Dolibarr, téléphonie XiVO, messagerie Poste.io),
- Un serveur Debian GLPI.

L'accès à Internet est assuré par un firewall **pfSense (Netgate SG-2440)**, mais la politique de filtrage en place est extrêmement permissive, avec une règle ***"any-to-any"*** complète sur le LAN. La box opérateur est configurée en mode bridge, transmettant directement l'adresse IP publique au firewall.

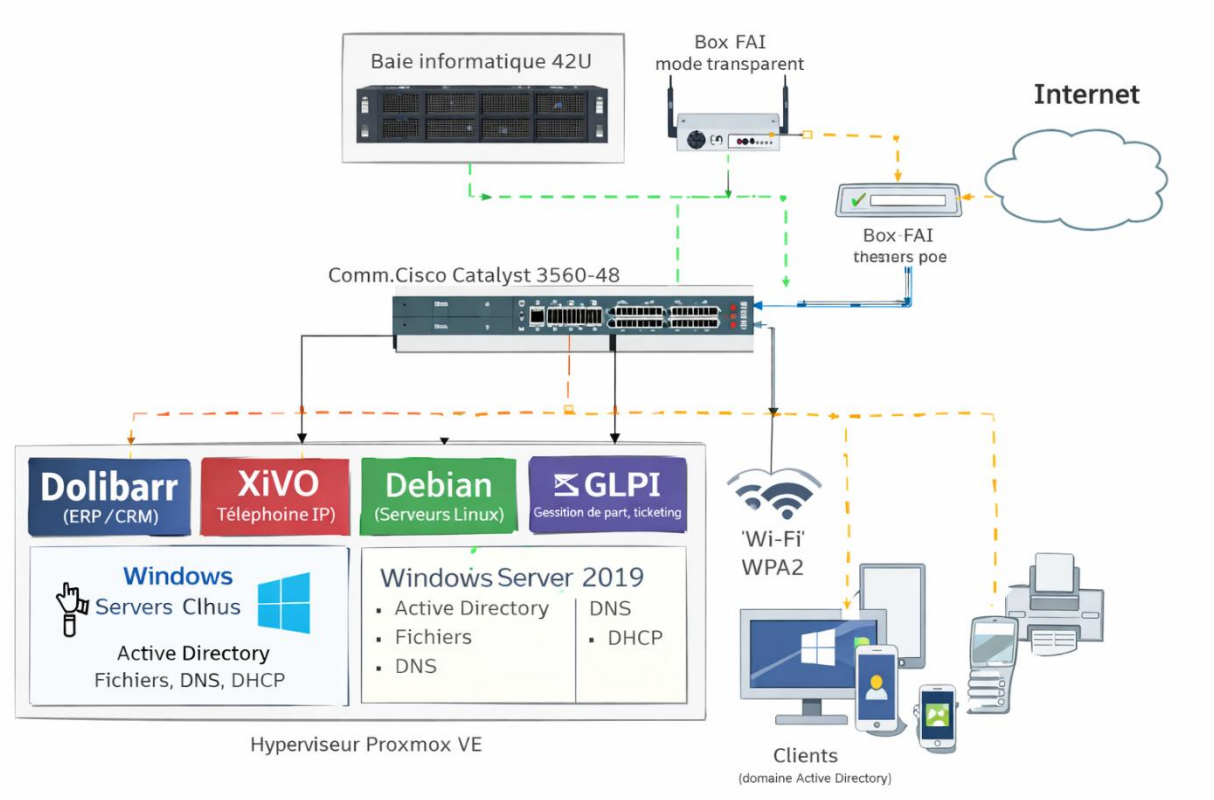
Absence de supervision

Aucun système de **supervision centralisée** n'est déployé, c'est-à-dire, pas de monitoring réseau ; pas de surveillance des serveurs ou de leurs services ; et pas d'alertes en cas de panne, surcharge ou attaque.

Absence PRA et PCA

De plus, EcoSolar Solutions ne dispose d'aucun **Plan de Reprise d'Activité (PRA)** ni **Plan de Continuité d'Activité (PCA)**. L'ensemble des services repose sur

un unique hyperviseur et une unique baie locale, dépourvue d'onduleur, faisant de l'infrastructure un point de défaillance critique. Aucune stratégie de sauvegarde structurée ou externalisée n'est mentionnée, et aucun lien n'existe encore avec la baie du datacenter de Marseille nouvellement acquise.



Expression du besoin

Le système d'information d'EcoSolar Solutions a été construit progressivement, sans architecture directrice, ce qui entraîne aujourd'hui de nombreuses limites tel que :

- Un **réseau non segmenté**, rendant difficile la sécurisation et le contrôle des flux ;
- Une **infrastructure unique et non redondée**, reposant sur un seul hyperviseur et sans PRA/PCA ;
- **Aucune supervision** du réseau ni des serveurs ;
- Des **accès distants non sécurisés** et inadaptés aux besoins des commerciaux ;
- Une **sécurité insuffisante** face à la sensibilité des données (brevets, R&D, documents internes) ;
- Une **absence d'exploitation** du datacenter récemment acquis ;
- Un SI qui ne peut plus soutenir la croissance de l'entreprise ni répondre aux enjeux de disponibilité.

Ces contraintes deviennent critiques à mesure que l'entreprise se développe et manipule de plus en plus de données pouvant être sensible.

Le besoin principal

Le besoin principal est de Concevoir une nouvelle architecture réseau et système sécurisée, segmentée, évolutive et supervisée, pour garantir la disponibilité, l'intégrité et la confidentialité des services essentiels d'EcoSolar Solutions.

Ce besoin principal inclut, une segmentation du réseau, un renforcement de la sécurité interne, une infrastructure plus résiliente pouvant intégrer le **datacenter**, une gestion sécurisée des **accès distants** (VPN, MFA), une **supervision centralisée**, une stratégie de **sauvegarde/PRA** robuste.

Les besoins secondaires

Il y’a en effet des besoins organisationnels

La mise en place des procédures et bonnes pratiques (RGPD).

L’intégrer le SI dans une démarche plus structurée (schéma directeur, gouvernance IT).

Objectifs du projet

L’objectif du scénario 3, est de garantir une visibilité complète et en temps réel sur l’état du système d’information d’EcoSolar Solutions. La mise en place d’une supervision centralisée répond directement aux besoins essentiels identifiés : amélioration de la disponibilité, réduction des risques, anticipation des incidents et protection des services critiques de l’entreprise.

Objectif opérationnel principal

Mettre en œuvre une supervision centralisée de l’infrastructure et des services critiques, répond aux besoins d’**EcoSolar Solution** en termes de **Disponibilité, intégrité, et de confidentialité.**

Disponibilité
La supervision permet de détecter rapidement les anomalies (surcharge, panne, service arrêté). Des alertes en temps réel permettent une **intervention proactive** avant qu’un incident n’impacte la production. Cela améliore la continuité de service, surtout pour des applications essentielles comme l’ERP, la messagerie, l’AD ou la téléphonie.

Intégrité
La surveillance des performances (CPU, RAM, stockage), des services actifs et des journaux permet de repérer des comportements anormaux, potentiellement liés à des erreurs système, à une corruption de données ou à une attaque. Cela contribue à préserver la cohérence et le bon fonctionnement des services critiques.

Confidentialité
Une supervision bien configurée n'expose pas d’informations sensibles à des tiers. Au contraire, elle garantit que les services liés à l’authentification (AD, VPN, messagerie) fonctionnent correctement et qu’aucun comportement inattendu ne menace la sécurité des accès.

Conditions de réalisation

Conditions générales de réalisation

Durée de la réalisation

La réalisation de ce projet m'a pris 8 semaines, à compter du lundi 01 décembre 2025 au dimanche 25 janvier 2026.

Travail individuel ou en équipe :

Pour ce projet, j'ai travaillé avec deux collègues de classe Elsa AYACHE, et Samy DESMAZEAUX. Ensemble nous nous sommes arrangés sur les choix de scénario, la planification des tâches à réaliser individuellement, et ensemble. Puis nous nous sommes aidez mutuellement tout au long du projet pour arriver à nos fins.

Encadrement par le formateur

Mon formateur en cours de d'infrastructure réseaux et Cybersécurités, **Mohamed LEDJAR** a endossé de rôle fictif de consultant au compte de l'entreprise EcoSolar Solution, pour nous orienter au mieux sur les tâches à réaliser.

Contraintes pédagogiques (méthode de projet

(AGILE/Scrum avec sprint d'1 jour, organisation de la documentation dans un dépôt GitHub, livrables demandés ...)

Contraintes techniques (solutions open source, ressources limités)

Nous avons fait face à un gros bug de notre serveur PROXMOX dès le départ, il était quasiment impossible de taper une ligne de commande sur notre VM Debian sans avoir une succession de bug ou de coupure. Après avoir analyser notre infrastructure réseau, nous nous sommes rendu compte que le switch était connecté à notre router en Fast internet, au lieu de Giga beat. Cependant, après avoir corrigé cette erreur, nous n'avons pas eu beaucoup d'amélioration. Nous avons alors tenté de mettre en place un VLAN, pour améliorer la fluidité du réseau sans succès, car le switch ne pouvait pas contenir de VLAN.

Ressources fournies au départ

Dans le cadre du projet d'infrastructure pour l'entreprise EcoSolar Solutions, plusieurs ressources techniques, matérielles et logicielles sont mises à disposition afin de permettre la conception, la mise en œuvre et la validation de la solution retenue.

Ressources matérielles

Les ressources matérielles utiliser dans la réalisation de ce projet sont : mon ordinateur portable personnelle DELL, mon ordinateur professionnelle Lenovo, un serveur Proxmox, un firewall pfSense, des VM serveur dans Proxmox, et une vm d'administration.

Ressources logicielles

Les logicielles utiliser dans la réalisation de ce projet sont : **Proxmox VE 8.3-1** pour la virtualisation, **Windows Server 2019 Standard** : Active Directory (DNS, DHCP, Serveur de fichiers), **Debian 12** pour les serveurs Linux, **Dolibarr** (ERP / CRM), **XiVO** (téléphonie IP), **Poste.io** (serveur de messagerie), **GLPI** (gestion de parc et ticketing), **pfSense** (pare-feu, routage, sécurité réseau)

L'ensemble des machines virtuelles est déjà déployé et fonctionnel dans l'environnement Proxmox fourni par l'organisme de formation.

Comme solution de secours j'ai utilisé VirtualBox, et GNS3. Avec ces logiciels, je peux tenter de réaliser le système de supervision avec Zabbix.

Ressources documentaires

La documentation utiliser dans la réalisation de ce projet sont : les documents ESS, Annexe II.E du référentiel, documentation constructeur, guides ANSSI/CIS.

Au départ, L'environnement de travail reposait sur une infrastructure virtualisée fournie par le centre de formation, reproduisant fidèlement le système d'information existant de l'entreprise EcoSolar Solutions. Puis un problème avec cette infrastructure m'a poussé à me tourner vers des solutions locales, c'est-à-dire sur mon ordinateur avec VirtualBox et GNS3.

Résultats attendus

Un réseau segmenté fonctionnel avec règles firewall correctes.

Le projet vise la mise en place d'une **segmentation logique du réseau** afin d'isoler les différents services et limiter les risques de propagation d'incidents ou d'attaques. Concrètement, l'infrastructure cible repose sur la création de **VLAN dédiés**

Une supervision complète avec Zabbix, Centreon, ou Prometheus.

Afin de garantir la **disponibilité et la performance** des services critiques, une solution de supervision centralisée est mise en place à l'aide de **Zabbix, Centreon ou Prometheus.**

La supervision couvre les serveurs (Linux et Windows), les machines virtuels, l'hyperviseur Proxmox, les services critiques (AD, ERP, messagerie, téléphonie), les ressources système (CPU, RAM, stockage, réseau)

Des indicateurs de performance sont définis (KPI), taux d'utilisation CPU/RAM, espace disque disponible, disponibilité des services, latence réseau. Des **alertes automatisées** permettent d'anticiper les incidents et d'intervenir rapidement en cas d'anomalie.
Cette supervision améliore significativement la **qualité de service** et s'inscrit dans une démarche proactive de gestion du SI.

Une solution de sauvegarde automatisée avec test de restauration.

Le projet intègre une solution de **sauvegarde centralisée et automatisée** afin d'assurer la protection des données de l'entreprise et la continuité d'activité.

La solution retenue repose sur des sauvegardes régulières des machines virtuelles, des sauvegardes des données critiques (ERP, fichiers, bases de données), une planification automatisée.

- Un VPN opérationnel sécurisant les échanges intersites

Dans le cadre de l'extension du système d'information vers le **datacenter de Marseille**, un **VPN sécurisé** est mis en place afin de garantir la confidentialité des échanges entre les sites.

Le VPN permet de relier le site de Toulouse au datacenter, de chiffrer l'ensemble des flux réseau, d'assurer une communication sécurisée entre les infrastructures

- Un cluster Proxmox fonctionnel avec bascule HA

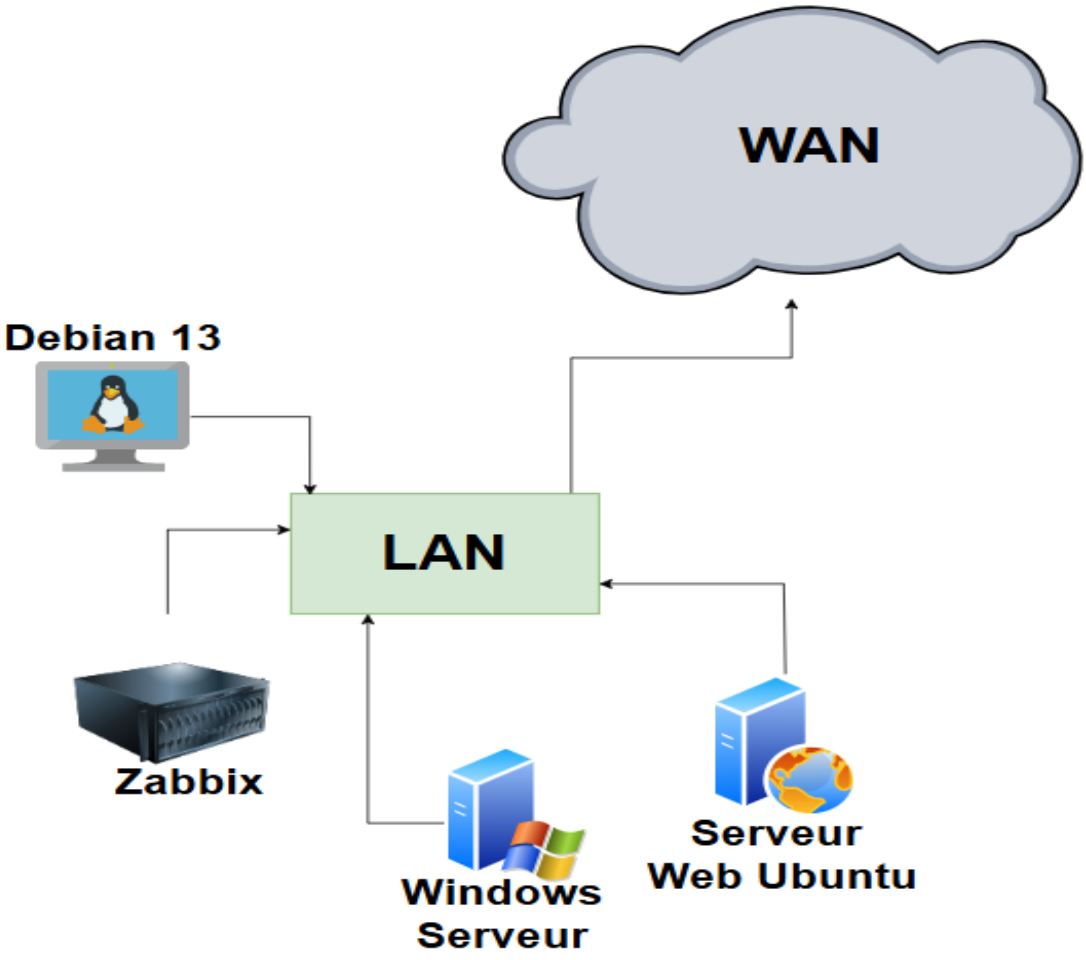
Le projet prévoit la mise en place d'un **cluster Proxmox** afin d'améliorer la **disponibilité des services virtualisés**.

Le cluster permet la mutualisation des ressources, la surveillance de l'état des nœuds, la **bascule automatique (HA)** des machines virtuelles en cas de défaillance d'un hôte.

Conception

Architecture cible

Schéma réseau cible



Cahier des charges technique

1. Objectifs généraux

Le présent cahier des charges technique a pour objectif de définir les choix technologiques et les exigences techniques nécessaires à la mise en œuvre d'une infrastructure réseau sécurisée, disponible et évolutive pour l'entreprise EcoSolar Solutions.

La solution retenue doit permettre :

La sécurisation du système d'information

La continuité des services critiques

L'administration centralisée de l'infrastructure

L'accompagnement de la croissance de l'entreprise

L'intégration future du datacenter de Marseille

2. Exigences fonctionnelles

2.1 Réseau et sécurité

Mise en place d'une segmentation réseau par VLAN

Isolation logique des services et des usages

Routage inter-VLAN contrôlé et sécurisé

Journalisation des flux critiques

2.2 Pare-feu et filtrage

Utilisation d'un firewall centralisé OpnSense

Politique de filtrage restrictive par défaut

Règles spécifiques selon les VLANs

Protection contre les flux non autorisés

Possibilité d'évolution vers IDS/IPS

2.3 Supervision

Déploiement d’une solution de supervision centralisée

Surveillance des serveurs

Services et équipements réseau

Collecte des indicateurs de performance

Mise en place d’alertes automatisées

Historisation des données.

2.4 Sauvegarde et continuité d’activité

Sauvegardes automatisées des machines virtuelles

Sauvegardes des données critiques

Conservation de plusieurs points de restauration

Contribution à un Plan de Reprise d’Activité (PRA)

2.5 Haute disponibilité

Mise en place d’un cluster Proxmox

Surveillance des nœuds

Bascule automatique des machines virtuelles

Priorisation des services critiques

3. Exigences techniques

3.1 Matériel

Serveurs physiques ou virtuel compatibles avec Proxmox VE, GNS3, VirtualBox.

Machine virtuel type linux, et Windows.

Firewall dédié Netgate / PFSense or OpenVPN

3.2 Logiciels et solutions retenues

Fonction	Solution retenue	Justification
Virtualisation	VirtualBox	Open source
Pare-feu	OpenSense	Sécurité, flexibilité, communauté
Supervision	Zabbix	Supervision complète, alertes
Sauvegarde	Proxmox Backup Server	Sauvegarde VM, restauration fiable
Systèmes	Debian, Ubuntu, / Windows Server	Stabilité, compatibilité métier

4. Exigences de sécurité

Respect des bonnes pratiques ANSSI et CIS

Séparation des flux utilisateurs / serveurs

Accès administrateurs restreints et tracés

Comptes nominatifs

Mises à jour régulières des systèmes

Sauvegardes protégées contre l’altération

5. Exigences de disponibilité et de performance

Disponibilité élevée des services critiques

Réduction des temps d’indisponibilité

Supervision proactive

Capacité à absorber une montée en charge

Surveillance des performances système

6. Exigences d’exploitation et de maintenance

Documentation technique complète

Procédures d’exploitation claires

Administration centralisée

Possibilité d’évolution sans remise à plat complète

Suivi des incidents et actions correctives

7. Contraintes

Solutions open source et gratuites

Ressources matérielles limitées

Environnement de test isolé

Déploiement progressif

Respect du cadre pédagogique BTS SIO SISR

Mise en œuvre

Description détaillée de la réalisation professionnelle

1. Choix de l'environnement de maquettage

Afin de démontrer la faisabilité technique de la solution de supervision proposée à EcoSolar Solutions, j'ai choisi de mettre en œuvre un environnement virtuel à l'aide de l'outil **VirtualBox**.

Ce choix permet de reproduire une infrastructure réseau réaliste, simuler des équipements réseau et des serveurs, valider le fonctionnement de la supervision sans impacter le SI réel, tester les flux et la communication entre les composants.

La maquette est utilisée comme **preuve de concept (POC)** pour la supervision centralisée avec Zabbix.

2. Présentation de la topologie mise en place

La topologie VirtualBox mise en œuvre se compose des éléments suivants :

Zabbix :
Serveur de supervision Zabbix (Linux), chargé de collecter les métriques et d'émettre les alertes.

Serveur web Ubuntu :
Serveur hébergeant un service capable de répondre aux requêtes HTTP/HTTPS.

VM Debian :
un ordinateur fictif qui tourne à l'intérieur d'un ordinateur physique et qui utilise **Debian** comme système d'exploitation.

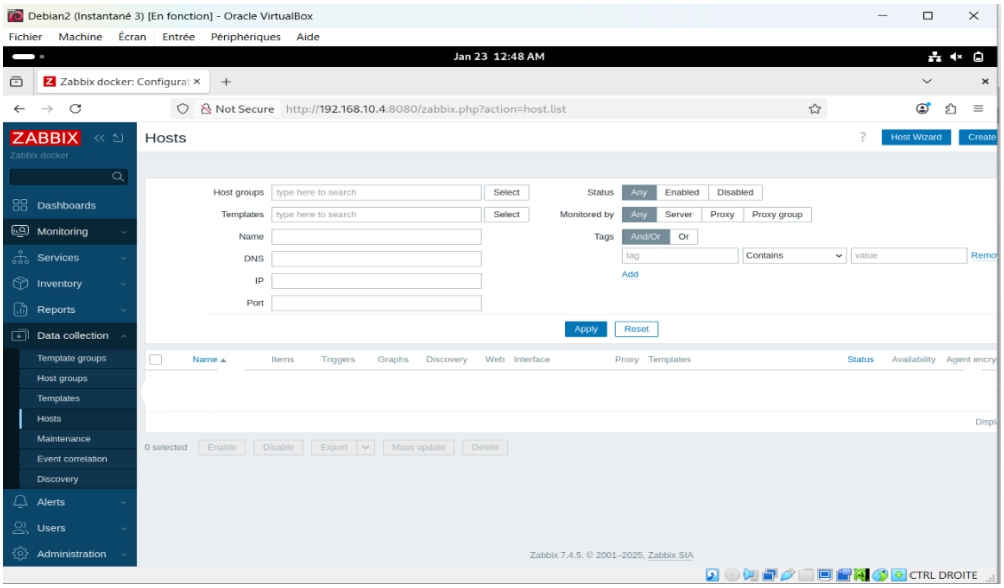
Windows serveur :
Un Windows Server, spécialement pour faire tourner des **services réseau**, des **applications d'entreprise** et gérer des **infrastructures informatiques**. C'est un système pensé pour les administrateurs et les environnements professionnels.

3. Déploiement du serveur Zabbix

J’ai commencé par le déploiement d’une machine virtuelle de type linux dédiée à la supervision.

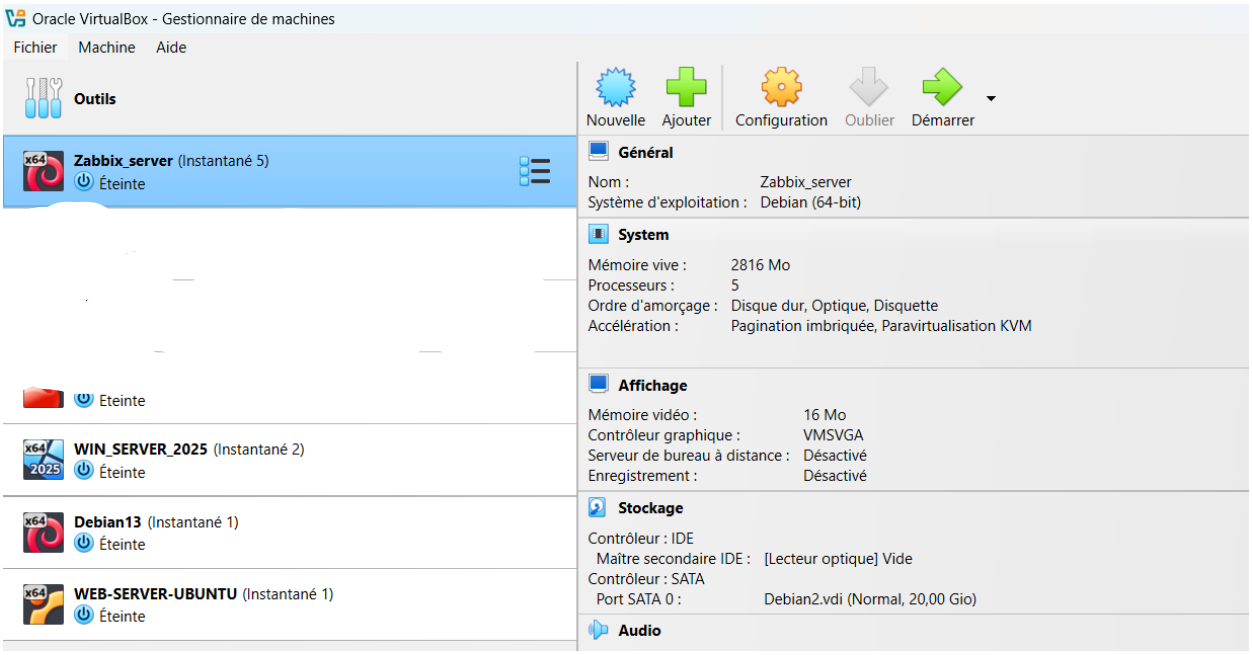
Les actions réalisées sont : l’installation du système d’exploitation Debian (Linux), configuration de l’adressage réseau, vérification de la connectivité avec le reste de la topologie, installation de la stack Zabbix (serveur, frontend web, base de données)

Une fois l’installation terminée, j’ai vérifié l’accès de l’interface web Zabbix depuis le navigateur Firefox de la Debian, validant ainsi le bon fonctionnement du service.



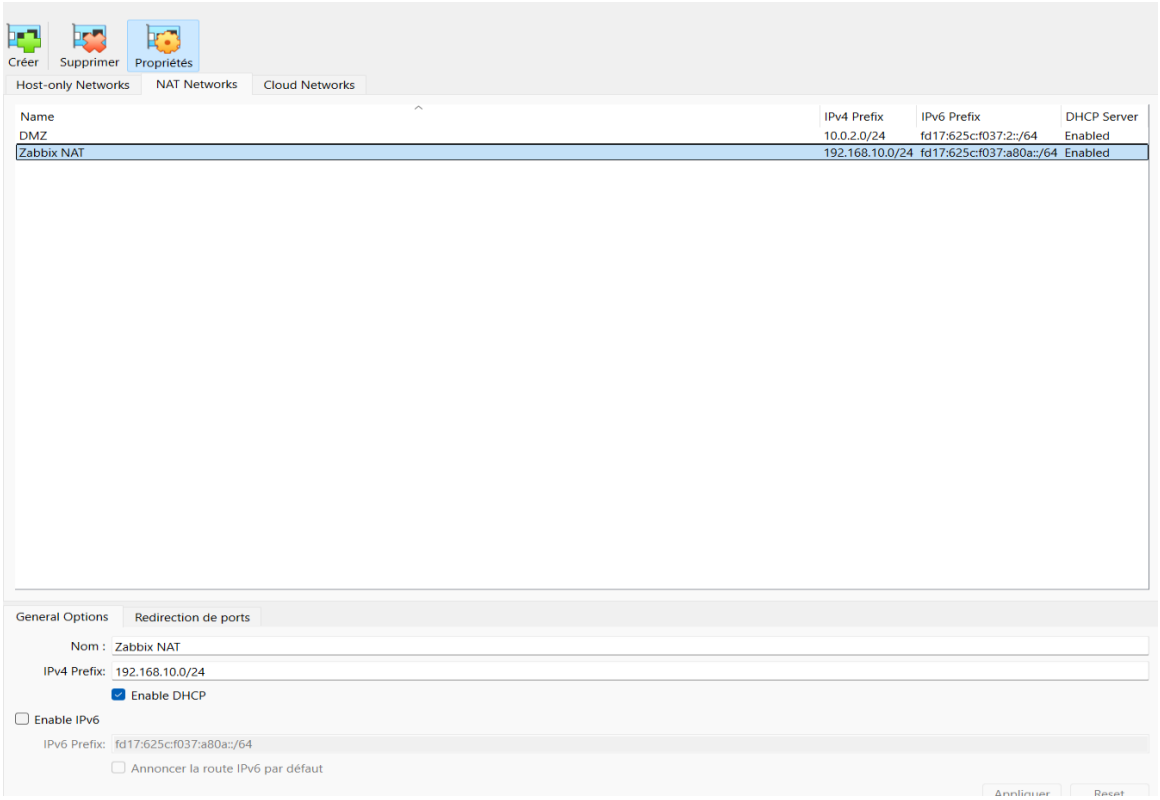
4. Déploiement des machines et serveurs virtuels

Avec les iso téléchargé sur les sites officiels des systèmes (Debian, Ubuntu, et Microsoft) j'ai déployé toute les machines et les services nécessaires. J'ai également pris le soin de les configurés correctement.



5. Configuration réseau et connectivité

Après l'installation du serveur Zabbix, j'ai créé un réseau NAT Zabbix depuis VirtualBox dédier à la supervision.

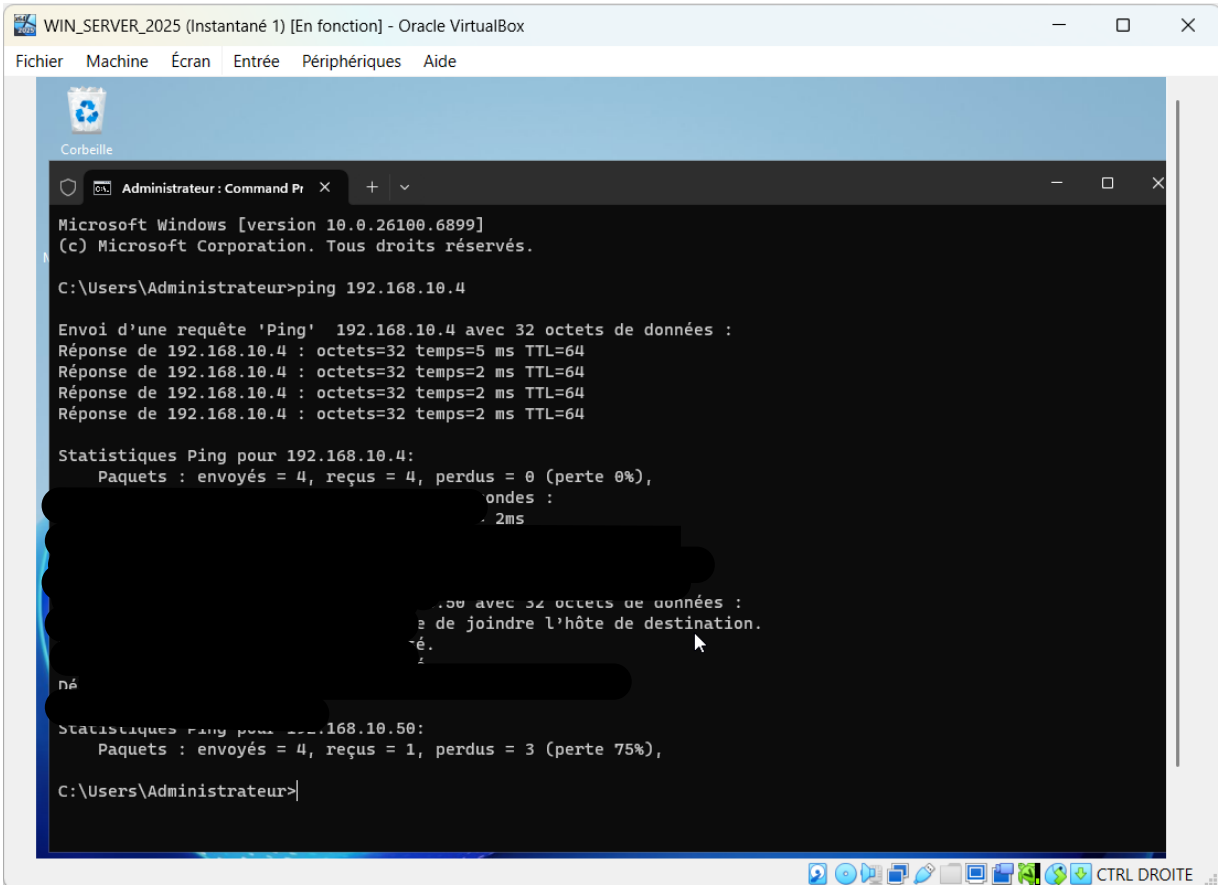


Cela permet un accès à **WAN** (internet) tout en facilitant la connectivité réseau afin de permettre la communication entre le serveur Zabbix, les équipements à supervisés, et le poste client dans le **LAN**.

Les tests effectués incluent :

Tests de connectivité ICMP (ping)

Cette vérification permet de s’assurer que les flux nécessaires à la supervision sont fonctionnels.



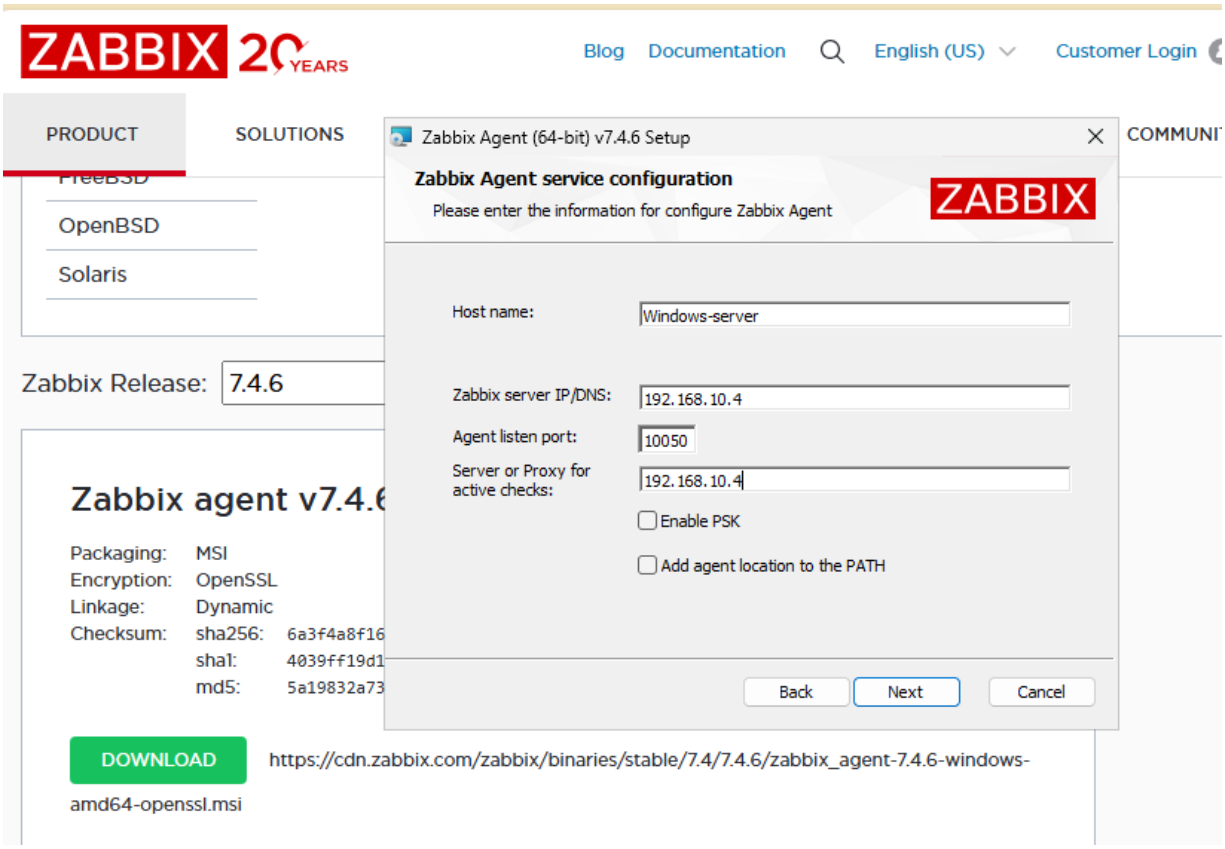
6. Mise en place de la supervision avec Zabbix

Une fois le serveur opérationnel, j'ai procédé à la configuration de la supervision.

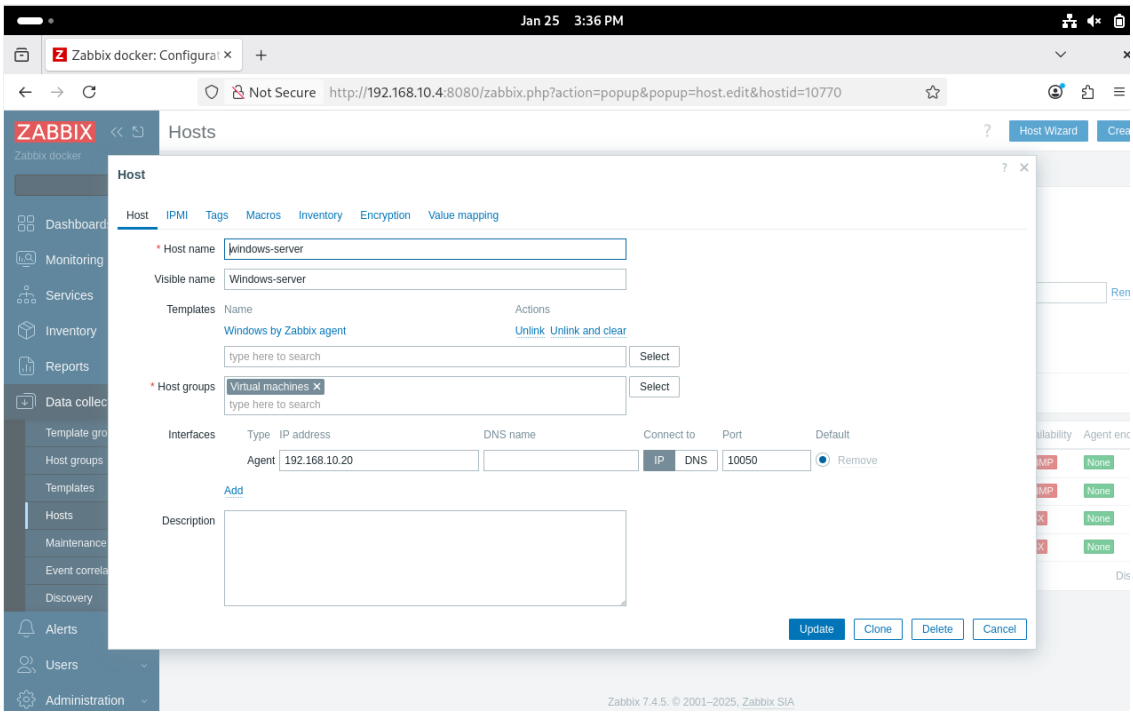
Les étapes réalisées :

- Installation de agents Zabbix et du protocole SNMP

Pour le Windows serveur j'ai installé l'agent Zabbix. Tout d'abord il a fallu prendre une version qui correspond au serveur Zabbix, il s'agit ici de la version 7.4.6. En suite il a fallu renseigner l'adresse du serveur Zabbix, ainsi que le port 10050.

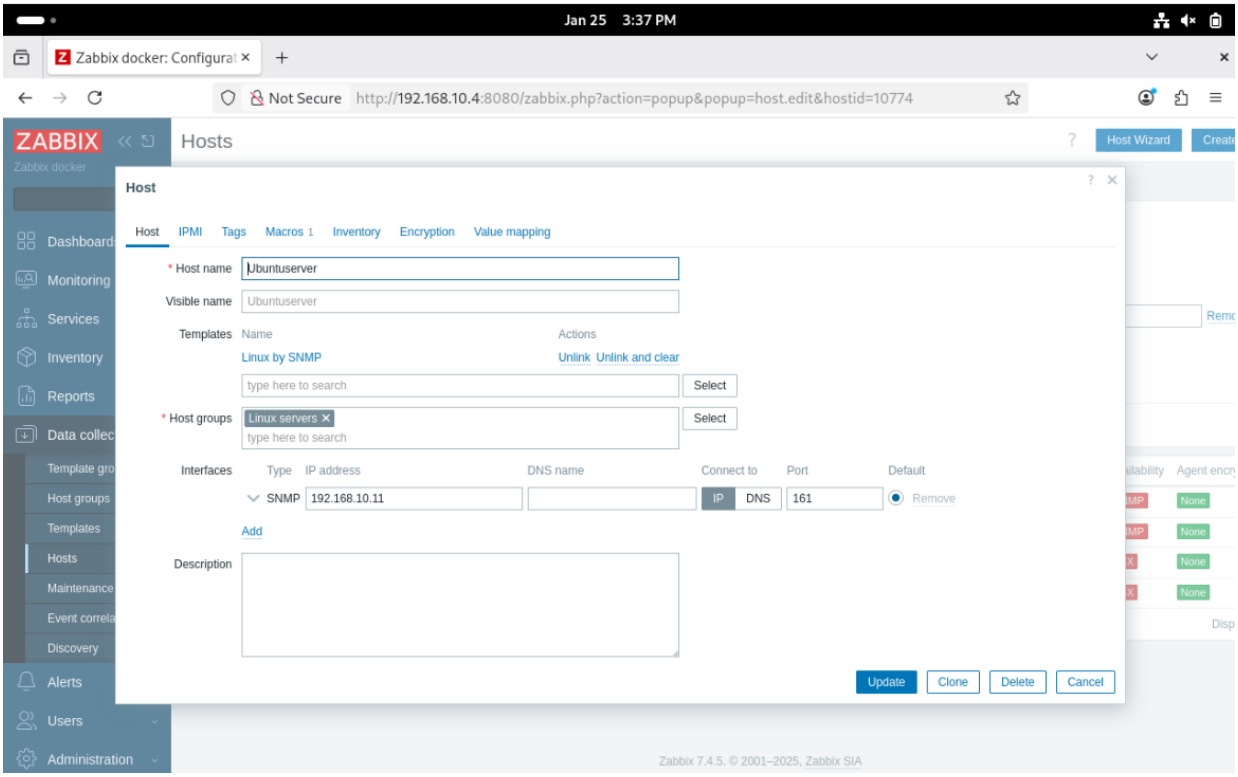


Ensuite, j’ai créé dans Zabbix le Host du Windows serveur ; j’ai renseigné l’IP de la machine (192.168.10.20), le Template, et le Host groupe.



Pour les machines de types linux, je suis passé par le protocole SNMP, par ce que l'installation de l'agent Zabbix sur les machines de type linux rencontrais des problèmes. J'ai alors installé et activer le protocole SNMP, puis renseigner l'IP du serveur dans le fichier.

Ensuite j'ai créé le Host de la machine dans le serveur Zabbix.

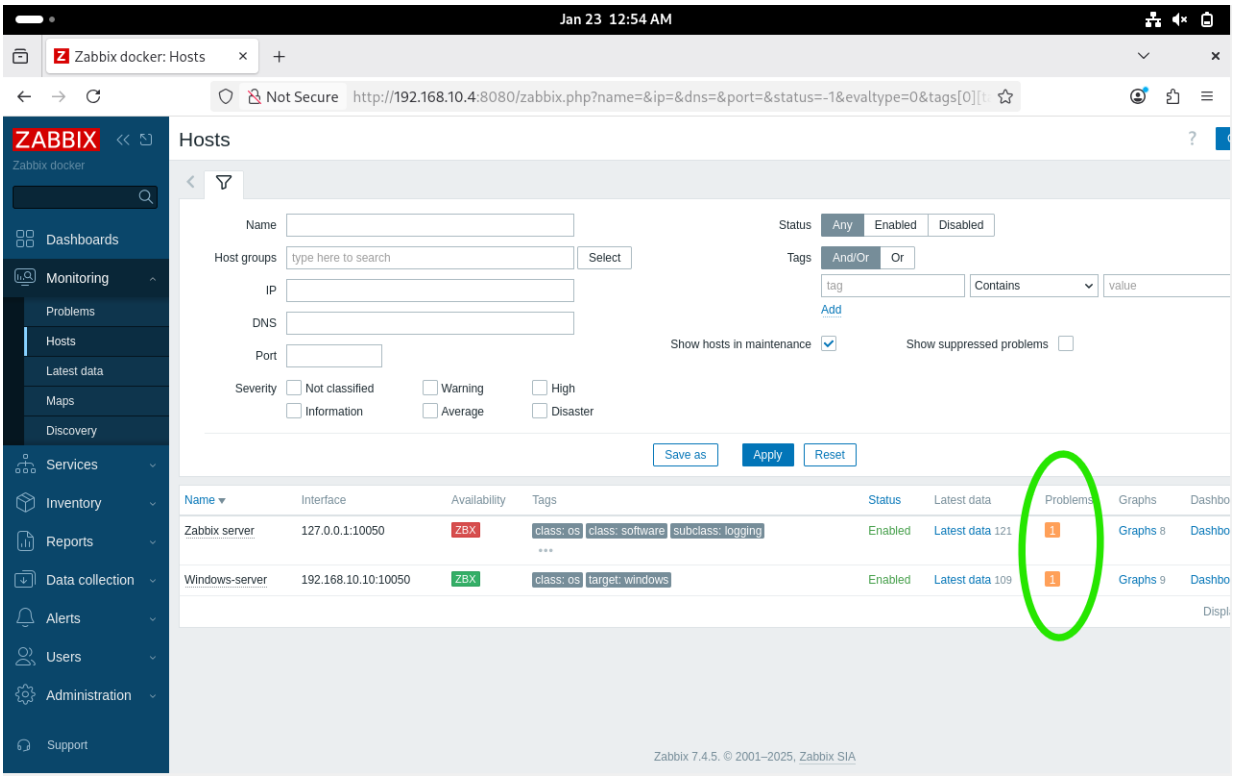


Ces configurations permettent d'obtenir une **vision en temps réel** de l'état des équipements supervisés.

7. Validation de la solution

Pour valider la solution, j'ai réalisé plusieurs tests :

- Arrêt volontaire d'un service supervisé
- Coupure réseau simulée
- Observation du déclenchement des alertes dans Zabbix



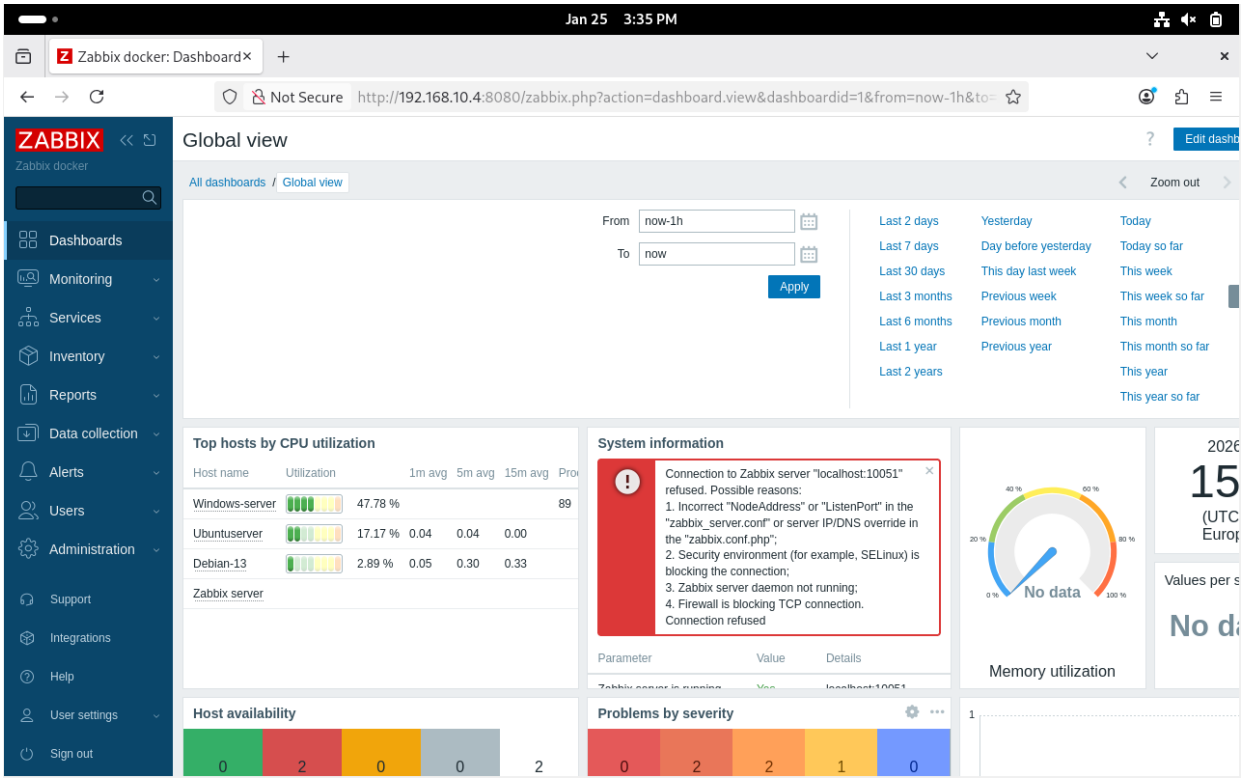
Les résultats observés confirment que :

- La supervision est fonctionnelle
- Les alertes sont correctement générées
- La solution répond aux besoins exprimés dans le cahier des charges

8. Apport de la solution pour EcoSolar Solutions

Cette maquette démontre que la mise en place d'une supervision centralisée avec Zabbix est techniquement réalisable, adaptée à l'infrastructure d'EcoSolar Solutions, conforme aux bonnes pratiques de supervision, et extensible à l'ensemble du SI réel (serveurs, équipements réseau, datacenter)

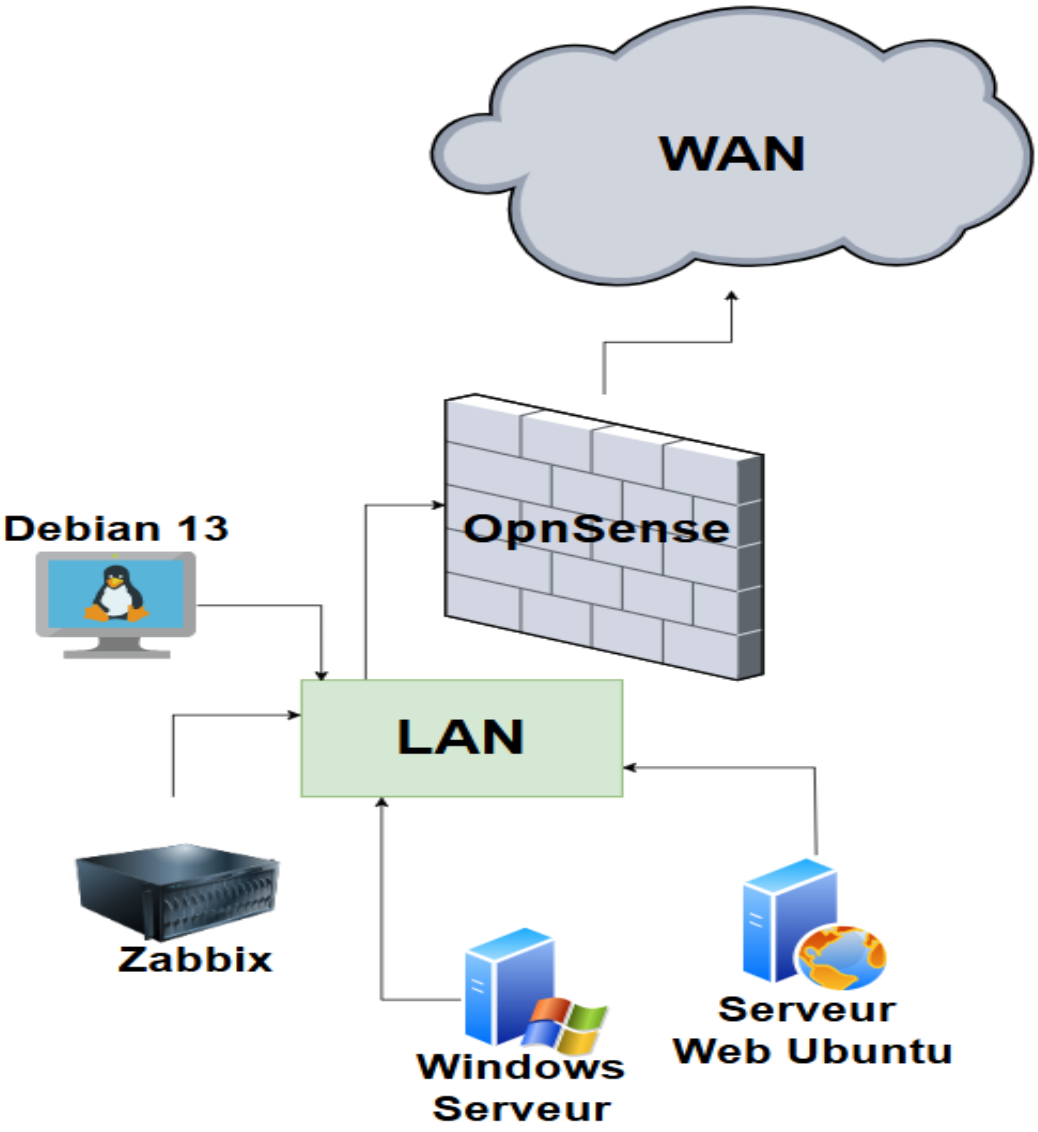
Validation de Zabbix



Pistes d’amélioration

Comme amélioration à ce projet, je peux rajouter un parfeu Opnsense, cela représentera la sécurité de notre LAN, lors de la communication avec le WAN.

Schéma représentatif



Compétences du référentiel travaillées

Le projet de mise en place d'une solution de supervision pour l'entreprise EcoSolar Solutions m'a permis de mobiliser et de développer plusieurs compétences du référentiel BTS SIO option SISR.

1. Concevoir une solution d'infrastructure réseau

Dans le cadre de ce projet, j'ai été amené à analyser le contexte technique existant de l'entreprise EcoSolar Solutions afin d'identifier les besoins en matière de supervision, de sécurité et de disponibilité.

J'ai conçu une **architecture cible** intégrant une supervision centralisée avec Zabbix, j'ai déployé des machines virtuelles qui ont joué le rôle de serveur. J'ai aussi configuré le tout pour une communication réseau opérationnels.

La conception s'est appuyée sur l'analyse du besoin, la rédaction d'un cahier des charges technique, et la définition des objectifs de sécurité (confidentialité, intégrité, disponibilité)

2. Installer, tester et déployer une solution d'infrastructure réseau

J'ai mis en œuvre une **maquette fonctionnelle** à l'aide de l'hyperviseur VirtualBox afin de démontrer la faisabilité de la solution proposée.

Cette étape m'a permis de déployer un serveur Zabbix, configurer la connectivité réseau, et intégrer des hôtes supervisés.

Des tests fonctionnels ont été réalisés afin de valider la remontée des métriques, le déclenchement des alertes et l'accessibilité de l'interface de supervision.

3. Exploiter, dépanner et superviser une solution d'infrastructure réseau

La mise en place de la supervision avec Zabbix m'a permis de développer des compétences liées à l'exploitation et au suivi d'une infrastructure.

J'ai notamment surveillé l'état de fonctionnement des équipements, analysé les indicateurs de performance, simulé des incidents pour vérifier la détection et l'alerte, et interprété les données remontées par l'outil de supervision.

Cette démarche s'inscrit dans une logique de **gestion proactive** du système d'information.

4. Administrer et sécuriser une infrastructure

Le projet m’a permis de mettre en pratique des notions essentielles de sécurité informatique, notamment :

Le principe du moindre privilège

La maîtrise des flux réseau

La sécurisation des accès aux services

La protection des données sensibles

La solution proposée contribue directement à renforcer la sécurité globale du système d’information de l’entreprise.

5. Documenter et communiquer autour d’une solution technique

Tout au long du projet, j’ai rédigé une **documentation technique structurée**, incluant l’analyse du besoin, les choix techniques argumentés, la description détaillée de la mise en œuvre, et les tests réalisés et les résultats obtenus.

Cette documentation est destinée à être exploitée par un administrateur réseau ou système et facilite la maintenance et l’évolution future de la solution.

Conclusion

Ce projet réalisé pour l'entreprise EcoSolar Solutions m'a permis de mettre en pratique l'ensemble des étapes nécessaires à la conception, au déploiement et à l'exploitation d'une solution d'infrastructure réseau.

À travers la mise en place d'une maquette de supervision avec Zabbix, j'ai su analyser un besoin réel, concevoir une solution adaptée aux enjeux de sécurité et de disponibilité, puis la valider techniquement à l'aide d'un environnement de test basé sur l'hyperviseur VirtualBox. Cette démarche m'a permis de démontrer la faisabilité de la solution tout en respectant les contraintes techniques et pédagogiques du projet.

La solution proposée apporte à EcoSolar Solutions une meilleure visibilité sur l'état de son système d'information, une capacité de détection proactive des incidents et une base solide pour l'évolution future de son infrastructure, notamment dans un contexte de croissance et d'ouverture vers un datacenter.

Sur le plan personnel, ce projet m'a permis de renforcer mes compétences techniques en supervision, en réseaux et en administration système, mais également de développer une démarche professionnelle basée sur l'analyse, la rigueur et la documentation. Il constitue une expérience concrète et valorisable dans le cadre de l'épreuve du BTS SIO option SISR. J'ai aussi fait preuve de gestion de stress dans les moments où je rencontrais des problèmes, et des difficultés tout au long de la réalisation de ce projet.