MISE EN PLACE D'UN SERVEUR DE SUPERVISION AVEC ZABBIX

Cédric BAUDIMENT
AgroMousquetaires – Site d'Antartic 2

BTS SIO SISR
Greta Drôme / Ardèche
2024 / 2026

I/ Cahier des charges

1- Descriptif de l'existant

L'infrastructure réseau sur laquelle s'appuie ce projet est hébergée sur un hyperviseur Proxmox VE, qui centralise l'ensemble des machines virtuelles du parc. Le réseau est segmenté en cinq VLANs distincts :

- le VLAN 10 (172.30.10.0/24) dédié à la production
- le VLAN 20 (172.30.20.0/24) pour la redondance
- le VLAN 30 pour les postes clients
- une DMZ interne (192.168.0.x / 192.168.1.x) accueillant les services exposés
- le VLAN 99 (172.30.99.0/24) réservé à l'administration.

Le routage inter-VLAN ainsi que le filtrage du trafic sont assurés par un pare-feu pfSense CE, déployé en configuration CARP Active/Passive afin de garantir la haute disponibilité du service.

Côté serveurs, l'infrastructure comprend un Windows Server 2025 assurant les rôles d'annuaire Active Directory, de DNS, de DHCP, de serveur de fichiers selon le modèle AGDLP, ainsi que la PKI interne via AD CS et la sauvegarde avec VEEAM. Plusieurs services applicatifs sont quant à eux hébergés sur des machines Debian 13 : GLPI pour la gestion du parc informatique, Nextcloud pour le stockage de fichiers, FOG pour le déploiement d'images système, Guacamole pour l'accès distant, et OpenVPN pour les connexions VPN.

À ce stade, aucun outil de supervision n'est en place. La surveillance de l'infrastructure repose uniquement sur des vérifications manuelles et ponctuelles, ce qui ne permet pas de détecter les incidents en temps réel. Les administrateurs ne disposent d'aucune visibilité sur l'état des services, l'utilisation des ressources ou l'historique de performance des équipements. Les pannes ne sont généralement identifiées qu'après signalement des utilisateurs, ce qui représente un risque opérationnel significatif pour la continuité de service.

2- Besoins

Afin de compléter l'infrastructure réseau, il est nécessaire de mettre en place une solution de supervision. L'objectif est de disposer d'une visibilité centralisée et en temps réel sur l'ensemble des équipements et services, afin de garantir la continuité de fonctionnement du système d'information.

La solution attendue doit permettre de surveiller en permanence l'état de disponibilité des équipements réseau et des serveurs, qu'ils soient sous Windows ou Linux. Elle doit également être capable de collecter et d'historiser des indicateurs de performance tels que l'utilisation du processeur, de la mémoire vive, de l'espace disque ou encore de la bande passante réseau.

Un système d'alertes est indispensable : les administrateurs doivent être notifiés automatiquement dès qu'un service devient indisponible ou qu'un seuil critique est franchi, sans avoir à attendre le signalement d'un utilisateur. Cette réactivité est essentielle pour limiter l'impact des incidents sur la production.

La solution doit également offrir une interface de consultation claire, permettant aux administrateurs de visualiser rapidement l'état global de l'infrastructure et d'accéder à l'historique des événements en cas d'analyse post-incident.

Enfin, la solution retenue devra s'intégrer sans rupture dans l'infrastructure existante, en supportant les protocoles standards utilisés dans l'environnement, et en étant accessible depuis le VLAN d'administration.

3- Contraintes

La principale contrainte de ce projet est d'ordre temporel. La mise en place de la solution de supervision doit être finalisée avant le mois d'avril, délai que je me suis fixé volontairement afin de disposer d'une marge suffisante pour tester l'ensemble de la solution et corriger les éventuels dysfonctionnements avant le passage de l'épreuve E6 du BTS SIO. Une mise en place tardive ne laisserait pas le temps nécessaire pour identifier et résoudre les problèmes qui pourraient survenir, ce qui représenterait un risque pour la présentation.

Sur le plan technique, la solution doit s'intégrer dans une infrastructure déjà en production, ce qui impose de ne pas perturber les services existants lors de son déploiement. Les interventions devront être réalisées avec précaution, en veillant à la compatibilité avec les équipements et systèmes déjà en place.

Enfin, ce projet s'inscrit dans le cadre d'une formation en alternance, ce qui implique que les ressources humaines disponibles se limitent à un seul intervenant, sans équipe dédiée. Le temps consacré au projet doit donc être optimisé pour respecter l'échéance fixée.

II/ Ressources

1- Ressources mises à disposition

L'infrastructure utilisée pour la réalisation du projet repose sur un environnement virtualisé mis à disposition dans le cadre de la formation. Cet environnement est hébergé sur une ferme de serveurs administrée par le GRETA, permettant aux étudiants de déployer et d'administrer différentes machines virtuelles pour leurs travaux pratiques et projets.

La virtualisation est assurée par l'hyperviseur open source Proxmox VE, qui permet de créer et de gérer plusieurs machines virtuelles au sein d'un même environnement physique. Cette plateforme facilite la mise en place d'une infrastructure réseau complète tout en offrant la possibilité de modifier ou de reconstruire rapidement les systèmes en cas de besoin.

L'environnement dispose également d'un accès à Internet, ce qui permet notamment de télécharger les différents systèmes d'exploitation, les logiciels nécessaires au déploiement des services ainsi que les mises à jour de sécurité. Cet accès est également indispensable pour tester les services destinés à être accessibles depuis l'extérieur du réseau, comme le futur service de cloud privé.

Les ressources matérielles allouées à l'infrastructure sont les suivantes :

- un espace de stockage total de 800 Go destiné à l'hébergement des machines virtuelles et de leurs données
- 64 Go de mémoire vive (RAM) permettant de faire fonctionner simultanément plusieurs serveurs et services
- 6 cœurs de processeur dédiés au fonctionnement de l'ensemble des machines virtuelles.

Ces ressources permettent de déployer l'ensemble des éléments de l'infrastructure nécessaires au projet, notamment les serveurs, les pares-feux, les services réseau ainsi que le futur serveur de fichiers.

2- Ressource nécessaire à la mise en place

La mise en place de l'infrastructure et des différents services associés nécessite l'utilisation de plusieurs systèmes d'exploitation déployés sous forme de machines virtuelles. Pour cela, différentes images ISO sont utilisées afin d'installer les systèmes nécessaires au fonctionnement du réseau et des services.

Tout d'abord, l'installation de pare-feu virtuels repose sur le système pfSense. Ce logiciel permet d'assurer plusieurs fonctions essentielles au sein de l'infrastructure, notamment le routage entre les différents VLAN, le filtrage des flux réseau et la protection du système d'information. Deux instances sont déployées afin de garantir une redondance et d'améliorer la disponibilité du service.

Le système Windows Server 2025 est utilisé pour l'hébergement de plusieurs services d'infrastructure. Ce type de serveur peut notamment être utilisé pour la gestion de l'administration du réseau, l'hébergement de services internes ou encore la gestion des utilisateurs selon les besoins de l'infrastructure.

Les postes clients du réseau fonctionnent sous Windows 11. Ces machines permettent de tester l'accès aux différents services mis en place dans l'infrastructure, notamment l'accès aux ressources internes et aux services accessibles via le réseau.

Enfin, certaines machines virtuelles reposent sur le système d'exploitation libre Debian, notamment pour l'hébergement de services web ou applicatifs. Ce système est particulièrement adapté pour ce type d'usage en raison de sa stabilité et de sa large compatibilité avec de nombreux logiciels serveur. La version utilisée dans le cadre de ce projet est Debian 13, qui servira notamment de base pour le déploiement du service de cloud privé.

L'ensemble de ces systèmes constitue la base logicielle nécessaire à la création des différentes machines virtuelles de l'infrastructure et au déploiement des services attendus dans le cadre du projet.

3- Gestion des ressources

Dans un environnement virtualisé, la gestion rigoureuse du processeur, de la mémoire vive et du stockage est indispensable pour garantir la stabilité des machines virtuelles. En utilisant la plateforme Proxmox VE, les ressources sont allouées sur mesure et ajustées selon l'importance de chaque service. Les éléments critiques, tels que les pare-feux pfSense et les serveurs applicatifs, bénéficient d'une priorité accrue pour assurer leur performance et la continuité du routage entre les VLAN. Parallèlement, les serveurs Windows Server 2025 et Debian 13 reçoivent des ressources adaptées à leurs rôles respectifs. Enfin, l'enveloppe globale de 800 Go de stockage est répartie stratégiquement afin de répondre aux besoins actuels tout en conservant une marge de manœuvre pour l'évolution future de l'infrastructure. Cette approche équilibrée permet d'allier performance système et flexibilité opérationnelle.

III/ Analyse

1- Descriptifs des solutions

Trois solutions de supervision ont été identifiées comme candidates pour répondre aux besoins exprimés :

- Zabbix est une solution open source de supervision réseau et système, développée et maintenue par la société Zabbix LLC. Elle est distribuée gratuitement sous licence GPL et

dispose d'une communauté active. Zabbix permet de surveiller un grand nombre d'équipements et de services grâce à des agents dédiés installés sur les hôtes, ou via des protocoles standards tels que SNMP, ICMP ou JMX. Elle offre un système de déclencheurs (triggers) permettant de définir des seuils d'alerte, ainsi qu'un tableau de bord personnalisable pour visualiser l'état de l'infrastructure en temps réel. Zabbix s'installe sur un serveur Linux et expose son interface via un navigateur web.

- PRTG Network Monitor est une solution commerciale éditée par la société allemande Paessler AG. Elle propose une approche basée sur des capteurs (sensors), chaque capteur surveillant un indicateur précis d'un équipement donné. PRTG est reconnue pour sa facilité de prise en main et son interface web moderne et intuitive. Elle intègre nativement de nombreux protocoles de supervision et propose des fonctionnalités avancées telles que la cartographie réseau automatique, les rapports planifiés et les notifications multicanaux. Son modèle de licence est basé sur le nombre de capteurs actifs, avec une version gratuite limitée à 100 capteurs et des licences payantes au-delà.
- Nagios est l'une des solutions de supervision open source les plus anciennes et les plus répandues dans le monde de l'administration système. Distribué gratuitement, il repose sur une architecture modulaire et extensible grâce à un large écosystème de plugins développés par la communauté. Nagios permet de surveiller la disponibilité des hôtes et des services, et d'émettre des alertes en cas d'incident. Il existe également une version commerciale, Nagios XI, qui enrichit Nagios Core d'une interface web plus moderne, d'un assistant de configuration et d'un support professionnel, moyennant l'achat d'une licence.

2- Comparaisons des solutions

Critère	Zabbix	PRTG	Nagios Core
Licence	Open source (GPL)	Commerciale (100 capteurs gratuits)	Open source (GPL)
Coût	Gratuit	Payant au-delà de 100 capteurs	Gratuit
Installation	Moyenne	Facile	Complexe
Interface web	Moderne, personnalisable	Très intuitive	Basique, vieillissante
Agents dédiés	Oui	Oui	Via plugins
Protocoles supportés	SNMP, ICMP, JMX, agent	SNMP, WMI, ICMP, agent	SNMP, ICMP, via plugins
Compatibilité Windows	Oui (agent)	Oui (natif)	Oui (via NSClient++)
Compatibilité Linux	Oui (agent)	Oui	Oui (agent)
Alertes et notifications	Oui (email, SMS, script)	Oui (email, SMS, push)	Oui (email, script)
Scalabilité	Très élevée	Élevée	Moyenne
Documentation	Complète et officielle	Complète et officielle	Communautaire
Support	Communautaire / payant	Inclus dans la licence	Communautaire / payant (XI)
Adapté à une petite infra	Oui	Oui	Oui

3- Choix d'une solution

Au regard de la comparaison effectuée, le choix s'est porté sur Zabbix pour la mise en place de la supervision de l'infrastructure.

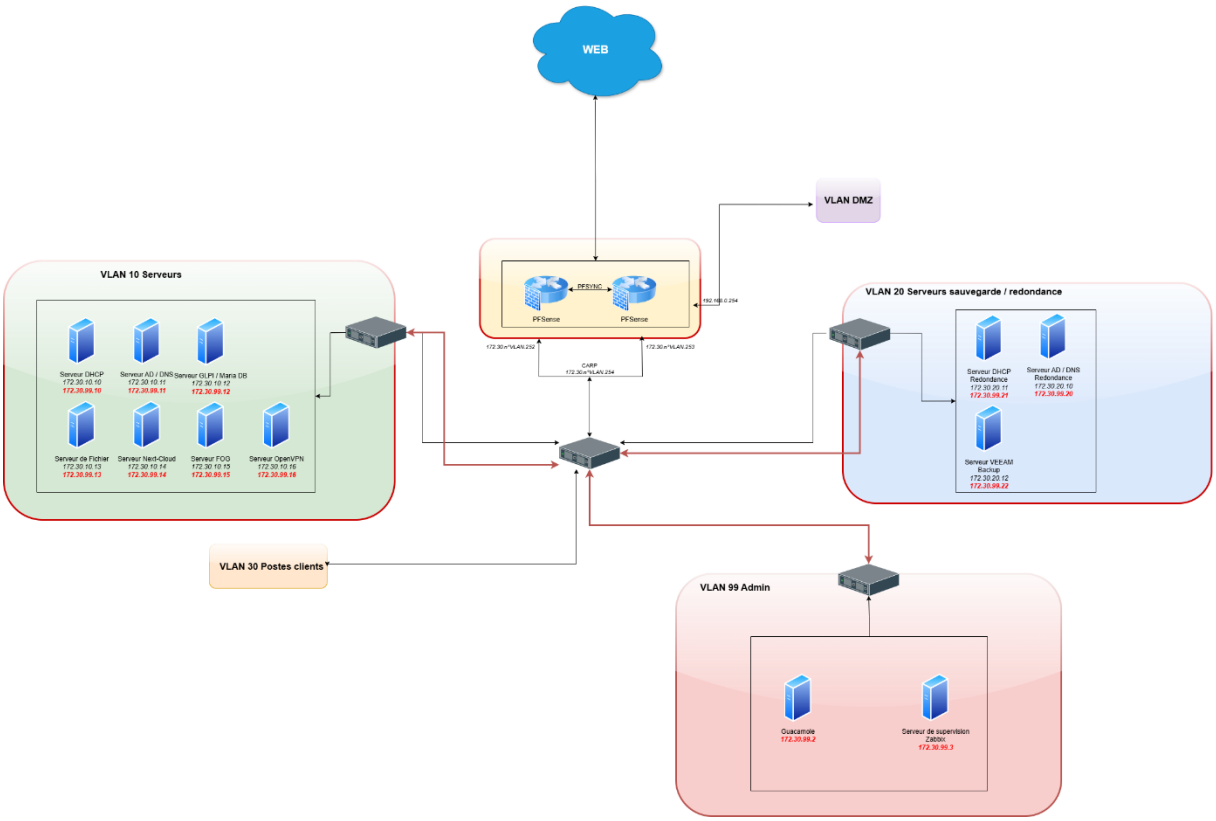
Nagios Core a été écarté principalement en raison de la complexité de son installation et de la vieillesse de son interface web. Bien que sa longévité témoigne de sa robustesse, sa prise en main nécessite un investissement temps important, notamment pour la configuration des plugins, ce qui n'est pas compatible avec les contraintes temporelles du projet.

PRTG Network Monitor, bien que très accessible et doté d'une interface particulièrement soignée, présente un modèle de licence commercial qui constitue un frein dans le cadre d'un projet scolaire. La version gratuite, limitée à 100 capteurs, pourrait s'avérer insuffisante à mesure que l'infrastructure évolue, et le coût des licences supérieures n'est pas justifiable dans ce contexte.

Zabbix répond à l'ensemble des besoins exprimés tout en étant entièrement gratuit et open source. Sa compatibilité native avec les environnements Windows et Linux, son système d'agents, ses nombreux protocoles supportés et son interface web moderne en font une solution particulièrement bien adaptée à l'infrastructure existante. Sa scalabilité permettra également de faire évoluer la supervision au fur et à mesure de la croissance du parc. Enfin, la richesse de sa documentation officielle constitue un atout non négligeable dans le cadre d'un projet mené par un seul intervenant.

4- Cartographie du réseau

a) Schéma



b) Plan d'adressage

VLAN 10 : Serveurs	
Réseau	*172.30.10.0*
Masque	*255.255.255.0*
Serveur DHCP	172.30.10.10
Serveur AD / DNS	172.30.10.11
Serveur GLPI / MariaDB	172.30.10.12
Serveur de fichier	172.30.10.13
Serveur Nextcloud	172.30.10.14
Serveur FOG	172.30.10.15
Serveur OpenVPN	172.30.10.16
Passerelle	*172.30.10.254*
Broadcast	*172.30.10.255*

VLAN 20 : Backup / redondance	
Réseau	*172.30.20.0*
Masque	*255.255.255.0*
Passerelle	*172.30.20.254*
Serveur AD / DNS redondance	172.30.20.10
Serveur DHCP redondant	172.30.20.11
Serveur VEEAM	172.30.20.12
Broadcast	*172.30.20.255*

VLAN 99 : Admin	
Réseau	*172.30.99.0*
Masque	*255.255.255.0*
Guacamole	172.30.99.2
Serveur Zabbix	172.30.99.3
Serveur DHCP	172.30.99.10
Serveur AD / DNS	172.30.99.11
Serveur GLPI / MariaDB	172.30.99.12
Serveur de fichier	172.30.99.13
Serveur Nextcloud	172.30.99.14
Serveur FOG	172.30.99.15
Serveur OpenVPN	172.30.99.16
Serveur AD / DNS redondance	172.30.99.20
Serveur DHCP redondant	172.30.99.21
Serveur VEEAM	172.30.99.22
Passerelle	*172.30.99.254*
Broadcast	*172.30.99.255*

Pare Feu LAN	
Réseau	172.30.1.0
Masque	255.255.255.0
PF 1	172.30.1.1
PF 2	172.30.1.2
CARP LAN	172.30.1.254
Broadcast	172.30.1.255

PFSync	
Réseau	172.30.2.0
Masque	255.255.255.0
PF 1	172.30.2.1
PF 2	172.30.2.2
Broadcast	172.30.1.255

c) Tables de routage

Réseau destination	Masque	Passerelle	Interface
172.30.10.0	/24	172.30.10.254	VLAN 10 (Serveurs)
172.30.20.0	/24	172.30.20.254	VLAN 20 (Backup)
172.30.99.0	/24	172.30.99.254	VLAN 99 (Admin)
172.30.2.0	/24	172.30.2.2	172.30.2.1
0.0.0.0	/0	FAI	WAN

5- Etude de l'impact sur le SI existant

a) Sécurité

L'intégration de Zabbix dans l'infrastructure existante implique plusieurs considérations en matière de sécurité qui doivent être anticipées.

Le serveur Zabbix sera hébergé dans le VLAN d'administration (VLAN 99), ce qui est cohérent avec sa fonction et limite son exposition aux autres segments du réseau. L'accès à l'interface web de supervision sera donc restreint aux postes d'administration, réduisant ainsi la surface d'attaque.

La communication entre le serveur Zabbix et les agents installés sur les hôtes supervisés transite exclusivement par le VLAN 99. Chaque serveur de l'infrastructure dispose en effet d'une seconde interface réseau connectée à ce VLAN d'administration, ce qui permet d'isoler totalement le trafic de supervision du reste du réseau de production. Les échanges entre le serveur Zabbix et ses agents ne sortent donc jamais du sous-réseau interne dédié à l'administration, ce qui réduit considérablement l'exposition de ces flux.

Les agents Zabbix installés sur les hôtes Windows et Linux disposent de droits d'accès limités au système sur lequel ils s'exécutent. Il est important de veiller à ce qu'ils fonctionnent avec le niveau de privilèges minimal nécessaire à la collecte des métriques, afin de limiter l'impact en cas de compromission.

L'interface web de Zabbix sera sécurisée par authentification, et les comptes d'accès seront créés avec des rôles distincts selon les besoins, en appliquant le principe du moindre privilège. L'intégration avec l'annuaire Active Directory pourra être envisagée afin de centraliser la gestion des accès.

Enfin, les communications entre l'interface web et le navigateur de l'administrateur seront chiffrées via HTTPS, en s'appuyant sur la PKI interne déjà en place via AD CS pour l'émission du certificat.

b) Performance

L'ajout d'une solution de supervision a un impact limité mais non négligeable sur les performances de l'infrastructure, qu'il convient d'évaluer en amont.

Du côté du serveur Zabbix lui-même, la charge générée dépend directement du nombre d'hôtes supervisés et de la fréquence de collecte des métriques. Dans le cadre de cette infrastructure, le nombre de machines surveillées reste modeste, ce qui ne nécessite pas de ressources matérielles importantes. Le serveur Zabbix sera hébergé sur une machine virtuelle Debian dédiée sous Proxmox, avec une allocation de ressources adaptée à la charge attendue.

Du côté des hôtes supervisés, l'agent Zabbix est un processus léger dont l'empreinte sur le système est très faible. Son impact sur les performances des serveurs Windows Server 2025 et Debian 13 est donc négligeable en utilisation normale. La fréquence de collecte des données sera configurée de manière raisonnée afin d'éviter une sollicitation excessive des hôtes ou du réseau.

Les échanges entre le serveur et les agents transitant exclusivement par le VLAN 99, le trafic de supervision n'entre pas en concurrence avec le trafic de production sur les autres VLANs. L'impact sur la bande passante du réseau de production est donc nul.

Enfin, la base de données utilisée par Zabbix pour stocker l'historique des métriques pourra nécessiter un espace disque croissant dans le temps. Une politique de rétention des données devra être définie afin de maîtriser la volumétrie et d'éviter une saturation du stockage à long terme.

c) Ergonomie

L'introduction de Zabbix dans l'infrastructure apporte une amélioration significative du confort de travail des administrateurs au quotidien.

Avant la mise en place de la supervision, l'état de l'infrastructure n'était consultable que par des vérifications manuelles et dispersées. Zabbix centralise l'ensemble de ces informations au sein d'une interface web unique, accessible depuis n'importe quel poste du VLAN d'administration. Les administrateurs disposent ainsi d'une vue globale et cohérente de l'infrastructure sans avoir à se connecter individuellement à chaque machine.

L'interface de Zabbix propose des tableaux de bord personnalisables, permettant d'adapter l'affichage aux besoins spécifiques de l'équipe d'administration. Il est possible de créer des vues synthétiques regroupant les indicateurs les plus pertinents, ce qui facilite la prise de décision rapide en cas d'incident.

Le système d'alertes automatiques contribue également à l'ergonomie globale de la supervision : les administrateurs n'ont plus besoin de surveiller activement l'infrastructure en permanence, les notifications prenant en charge la détection des anomalies. Cela permet de concentrer l'attention sur des tâches à plus forte valeur ajoutée.

Enfin, la courbe d'apprentissage de Zabbix, bien que présente, est facilitée par une documentation officielle complète et une communauté active. L'interface web, bien que dense, reste claire et structurée une fois la prise en main effectuée.

6- Phasage de l'intervention

La mise en place de Zabbix a été découpée en plusieurs phases successives afin d'organiser l'intervention de manière méthodique et de limiter les risques de perturbation de l'infrastructure existante.

La première phase consiste en la préparation de l'environnement. Elle comprend la création de la machine virtuelle Debian sur Proxmox, l'attribution de ses interfaces réseau dont une sur le VLAN de production et une sur le VLAN 99, ainsi que la configuration réseau de base du serveur. Cette phase inclut également la vérification des règles de pare-feu pfSense pour autoriser les flux nécessaires entre le serveur Zabbix et les futurs hôtes supervisés sur le VLAN 99.

La deuxième phase correspond à l'installation et à la configuration du serveur Zabbix, incluant la mise en place de la base de données MariaDB, du serveur Zabbix lui-même et de l'interface web. La

sécurisation de l'accès via HTTPS avec un certificat émis par la PKI interne fait également partie de cette phase.

La troisième phase concerne le déploiement des agents Zabbix sur l'ensemble des hôtes à superviser, qu'ils soient sous Windows Server 2025 ou Debian 13. Chaque agent sera configuré pour communiquer avec le serveur via l'interface du VLAN 99.

La quatrième phase est dédiée à la configuration de la supervision elle-même : création des hôtes dans l'interface Zabbix, application des templates adaptés à chaque type de machine, définition des seuils d'alerte et configuration des notifications.

Enfin, la cinquième et dernière phase correspond aux tests de validation, permettant de vérifier le bon fonctionnement de l'ensemble du dispositif avant la présentation de l'épreuve.

7- Prévision des tests de validation

Afin de s'assurer du bon fonctionnement de la solution avant la présentation de l'épreuve, plusieurs tests de validation ont été définis. Ils couvrent l'ensemble des aspects critiques de la supervision mise en place.

Un premier test consiste à vérifier la connectivité entre le serveur Zabbix et chaque agent déployé sur les hôtes supervisés, en s'assurant que les communications transitent bien exclusivement par le VLAN 99. Ce test permet de valider la bonne configuration réseau et les règles de pare-feu associées.

Un deuxième test porte sur la remontée des métriques. Pour chaque hôte supervisé, il s'agit de vérifier que les indicateurs de performance attendus, tels que l'utilisation du processeur, de la mémoire, de l'espace disque et de la bande passante, sont bien collectés et affichés dans l'interface web de Zabbix.

Un troisième test concerne le système d'alertes. Il consiste à simuler un incident, par exemple l'arrêt volontaire d'un service ou la saturation artificielle d'une ressource, afin de vérifier que le déclencheur correspondant s'active bien et qu'une notification est correctement émise.

Un quatrième test vérifie l'accessibilité de l'interface web depuis un poste du VLAN d'administration, en s'assurant que la connexion s'établit bien en HTTPS et que le certificat émis par la PKI interne est correctement reconnu.

Enfin, un dernier test global consiste à consulter le tableau de bord de Zabbix et à vérifier que l'ensemble des hôtes apparaissent en état opérationnel, offrant ainsi une vue cohérente et complète de l'infrastructure supervisée.

8- Déploiement

Le déploiement de Zabbix en environnement de production sera réalisé de manière progressive, en suivant le phasage défini précédemment, afin de minimiser tout risque de perturbation des services existants.

L'ensemble des opérations sera effectué depuis le VLAN d'administration, ce qui garantit que les interventions sur les hôtes supervisés ne transitent pas par le réseau de production. Le déploiement des agents sur les machines Windows Server sera réalisé manuellement dans un premier temps, avec la possibilité d'automatiser cette étape via une GPO ou un script PowerShell pour les déploiements

futurs. Sur les machines Debian, l'installation des agents sera effectuée via le gestionnaire de paquets apt.

Avant toute mise en production, une sauvegarde de l'état des machines concernées sera réalisée via VEEAM afin de disposer d'un point de restauration en cas de problème. Cette précaution est d'autant plus importante que certains serveurs hébergent des services critiques pour l'infrastructure, tels que l'annuaire Active Directory ou la base de données de GLPI.

Une fois le déploiement terminé et les tests de validation effectués, le tableau de bord de Zabbix sera configuré pour offrir une vue synthétique de l'ensemble de l'infrastructure. Les seuils d'alerte seront ajustés si nécessaire en fonction des observations relevées lors de la phase de test, afin d'éviter les faux positifs et de s'assurer que les notifications émises correspondent à des incidents réels.

Le déploiement sera considéré comme finalisé lorsque l'ensemble des hôtes sera visible et supervisé dans l'interface Zabbix, que les alertes fonctionneront correctement et que l'accès à l'interface web sera sécurisé et opérationnel depuis le VLAN d'administration.

IV/ Mise en place

1- Réalisation

- Installation et configuration du serveur sous Debian 13
- Installation d'un serveur zabbix

2- Rapport de tests

L'ensemble des tests définis en phase d'analyse a été réalisé à l'issue du déploiement. Les agents Zabbix ont été déployés avec succès sur les sept hôtes de l'infrastructure, aussi bien sur les serveurs Windows Server 2025 que sur les machines Debian 13. L'ensemble des hôtes affiche l'indicateur ZBX en vert dans l'interface, confirmant la bonne communication avec le serveur de supervision via le VLAN 99. La remontée des métriques a été vérifiée pour chaque hôte et fonctionne correctement. Aucun dysfonctionnement n'a été constaté lors du déploiement.

3- Rapport de déploiement

Le déploiement de Zabbix s'est déroulé conformément au phasage prévu. Le serveur Zabbix a été installé sur une machine virtuelle Debian 13 dédiée, hébergée sur Proxmox et connectée au VLAN d'administration. L'ensemble de la chaîne, base de données MariaDB, serveur Zabbix et interface web Apache, a été mis en service sans difficulté.

Les agents ont ensuite été déployés sur les sept hôtes de l'infrastructure. Sur les machines Debian 13, l'installation s'est effectuée via le gestionnaire de paquets apt après ajout du dépôt officiel Zabbix. Sur les serveurs Windows Server 2025, l'agent a été installé via le programme d'installation MSI, et la règle de pare-feu nécessaire a été ajoutée via PowerShell. Chaque hôte a été intégré dans l'interface Zabbix avec le template adapté à son système d'exploitation.

L'ensemble du déploiement a été réalisé dans les délais fixés, laissant la marge prévue pour les tests et corrections éventuelles avant le passage de l'épreuve E6.

V/ Bilan

1- Conclusion

La mise en place de Zabbix au sein de l'infrastructure cbaudiment.fr répond pleinement aux besoins exprimés dans le cahier des charges. L'infrastructure dispose désormais d'un outil de supervision centralisé, capable de surveiller en temps réel l'ensemble des serveurs Windows et Linux, de collecter et d'historiser leurs indicateurs de performance, et d'alerter les administrateurs en cas d'incident.

Le choix de Zabbix s'est révélé pertinent dans ce contexte : sa compatibilité native avec les environnements hétérogènes, la légèreté de ses agents et la richesse de son interface web en font une solution bien adaptée à une infrastructure de cette taille. Son caractère open source constitue par ailleurs un avantage non négligeable dans le cadre d'un projet scolaire.

Ce projet a permis de mettre en pratique des compétences transversales en administration système et réseau, en intervenant aussi bien sur des environnements Linux que Windows, et en intégrant la solution dans une infrastructure existante sans perturber les services en production.

2- Auto-évaluation

Ce projet m'a permis de consolider mes connaissances en supervision réseau, domaine que je n'avais pas encore eu l'occasion d'aborder concrètement. La prise en main de Zabbix, depuis l'installation du serveur jusqu'au déploiement des agents, m'a donné une vision plus complète du rôle de l'administrateur système, qui ne se limite pas à maintenir des services en fonctionnement mais doit également en assurer la visibilité et la traçabilité.

Le fait que le déploiement se soit déroulé sans incident majeur m'a permis de respecter le planning fixé et de disposer du recul nécessaire pour documenter la procédure de manière claire et reproductible. Cette rigueur de documentation est un axe que je souhaite continuer à développer, notamment en vue de l'épreuve E6.