PAGE DE GARDE DU DOSSIER PROFESSIONNEL

BREVET DE TECHNICIEN SUPÉRIEUR
SERVICES INFORMATIQUES AUX ORGANISATIONS

Session 2026

DOSSIER PROFESSIONNEL

NOM : MANAC'H

Prénom : Titouan

Établissement de formation (sur un seul des deux exemplaires du dossier)

Visa du représentant de l'équipe pédagogique attestant la réalité des activités professionnelles décrites dans le dossier (sur un seul des deux exemplaires du dossier) :

Nom et qualité du signataire	Date	Signature

Attestation sur l'honneur pour les candidats individuels (sur un seul des deux exemplaires du dossier) :

Je soussigné, Manac'h, Titouan, certifie que les activités décrites ainsi que les différentes informations reproduites dans ce dossier reflètent les activités professionnelles que j'ai personnellement réalisées au cours de ma formation.

Fait à Nantes
Date 24/04/2026

Signature

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation :**
Nom, prénom : MANAC'H Titouan	**N° candidat : 02542581894**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒	**Date :** 28 / 05 / 2026

Organisation support de la réalisation professionnelle
Entreprise fictive Oasis et prestataire Scylab

Intitulé de la réalisation professionnelle
Mise en place de l'outil de supervision Zabbix

Période de réalisation : *2024 - 2026* ***Lieu : CFA Fab'Academy Bouguenais (UIMM)***
Modalité : ***Seul(e)*** ☐ ***En équipe*** ☒

Compétences travaillées
- ☒ Concevoir une solution d'infrastructure réseau
- ☒ Installer, tester et déployer une solution d'infrastructure réseau
- ☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[1] (ressources fournies, résultats attendus)
Mise en place d'une solution de supervision dans l'infrastructure. Afin de répondre aux exigences de OASIS. La solution doit permettre d'assurer la supervision des hôtes de l'infrastructure virtualisée et sécurisée, des services essentiels

Description des ressources documentaires, matérielles et logicielles utilisées[2]
Serveurs HP, Proxmox, Zabbix, Pare-feux, Machines Virtuelles, Commutateurs HP

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.
[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

Modalités d'accès aux productions[3] et à leur documentation[4]

L'ensemble des documents lié à l'infrastructure sont trouvables sur le site Easi, Cette outils fournit par la Fab'Academy nous sert à stocker nos sauvegardes et documentation sur un espace externe.

Une kdbx contenant les mots de passes est disponible sur la VM CLI-P-MGMT sur le site de Paris.

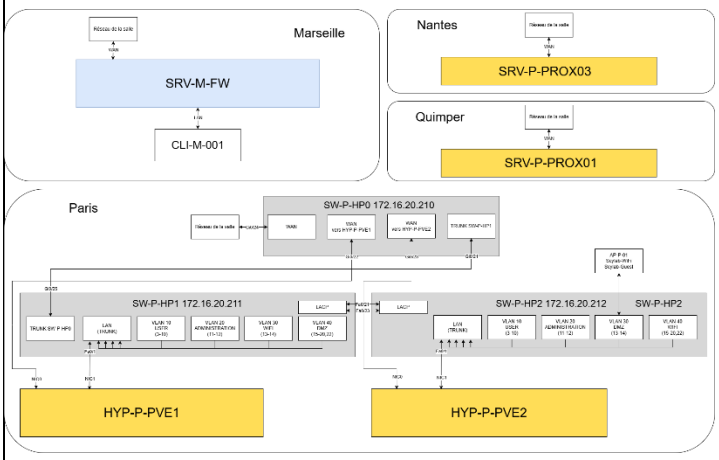
Mot de passe Keepass : Me*duse54-32

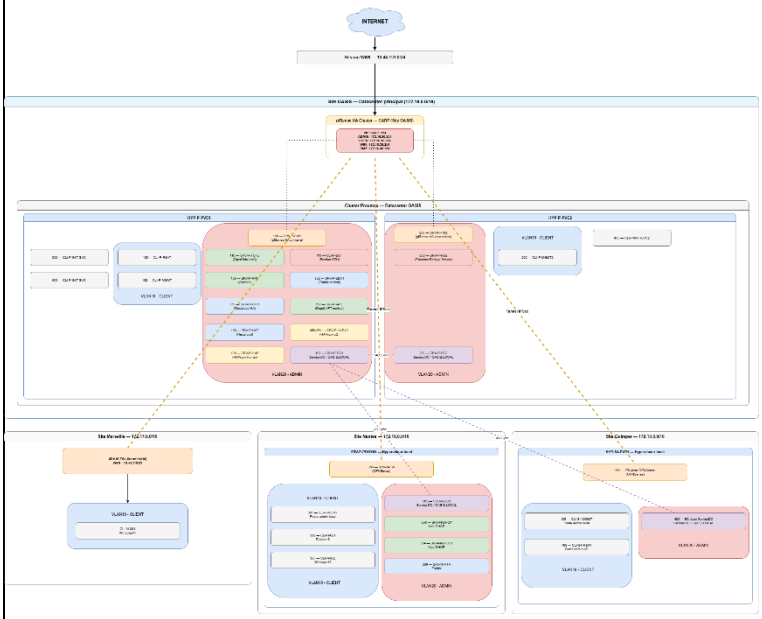
BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

Fiche descriptive de réalisation professionnelle
(verso, éventuellement pages suivantes)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs





[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[4] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

BTS Services informatiques aux organisations SESSION 2026
ANNEXE 10-A : Outil d'aide à l'appréciation de l'environnement technologique mobilisé par la personne candidate
Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

CONTRÔLE DE L'ENVIRONNEMENT TECHNOLOGIQUE
En référence à l'annexe II.E – « Environnement technologique pour la certification » du référentiel du BTS SIO

Identification[5]		**SISR**

1. Environnement commun aux deux options
1.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Un service d'authentification	**Samba AD**	
Un SGBD	**MariaDB**	
Un accès sécurisé à internet	**Firewall pfSense / OPNsense /Stormshieled**	
Un environnement de travail collaboratif	**Nextcloud**	
Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel libre (*open source)*	**Debian, Windows 11**	

[5] Nom et adresse du centre d'examen ou identification de la personne candidate individuelle (numéro, nom, prénom)

ANNEXE 10-A (suite) : Modèle d'attestation de respect de l'annexe II.E – « Environnement technologique pour la certification » du référentiel Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution de sauvegarde	Proxmox Backup Server	
Des ressources dont l'accès est sécurisé et soumis à habilitation	Nextcloud	
Deux types de terminaux dont un mobile (type *smartphone* ou encore tablette)	Tablette / PC Portable via connexion Wi-Fi	

1.2 Des outils sont mobilisés pour la gestion de la sécurité :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Gestion des incidents	GLPI	
Détection et prévention des intrusions	Stormshield	
Chiffrement	SSH, IPsec	
Analyse de trafic	Wireshark	

Rappel : les logiciels de simulation ou d'émulation sont utilisés en réponse à des besoins de l'organisation. Ils ne peuvent se substituer complètement à des équipements réels dans l'environnement technologique d'apprentissage.

ANNEXE 10-A (suite) : Modèle d'attestation de respect de l'annexe II.E « Environnement technologique pour la certification » du référentiel Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

2. Éléments spécifiques à l'option « Solutions d'infrastructure, systèmes et réseaux » (SISR)

Rappel de l'annexe II.E du référentiel : « *Une solution d'infrastructure réduite à une simulation par un logiciel ne peut être acceptée.* »

2.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Un réseau comportant plusieurs périmètres de sécurité	Segmentations VLAN	
Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	Nextcloud	
Un logiciel d'analyse de trames	Wireshark	
Un logiciel de gestion des configurations	Ansible	
Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	SSH	
Une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes	Zabbix	
Une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)	Firewall OPNsense, pfSense	

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution garantissant la continuité d'un service	**RAID 1, Proxmox Backup Server**	
Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	**RAID 1**	
Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	**DHCP, DNS, OPNsense, pfSense (CARP)**	

2.2 La structure et les activités de l'organisation s'appuient sur au moins une solution d'infrastructure opérationnelle parmi les suivantes :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution permettant la connexion sécurisée entre deux sites distants	**IPSec**	
Une solution permettant le déploiement des solutions techniques d'accès	**Ansible**	
Une solution gérée à l'aide de procédures automatisées écrites avec un langage de *scripting*	**Ansible**	
Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	**Stormshield**	

Table des matières

1. Rôle fonctionnel de la supervision

1.1 Qu'est-ce que la supervision ?

La supervision (ou monitoring) est un service informatique fondamental qui assure la surveillance en temps réel de l'état, des performances et de la disponibilité des équipements et services d'une infrastructure. Sans elle, les pannes, dégradations de performances et dépassements de capacité passent inaperçus jusqu'à ce qu'ils impactent les utilisateurs, souvent dans les pires moments. À l'échelle d'une infrastructure d'entreprise, une supervision centralisée devient indispensable pour garantir la continuité de service.

1.2 Fonctionnement

Le fonctionnement d'un système de supervision repose sur un cycle continu en quatre phases. Le serveur interroge régulièrement les équipements ou reçoit leurs métriques en mode actif, compare les valeurs collectées à des seuils définis, déclenche des alertes en cas de dépassement, et notifie les équipes concernées. Ce mécanisme garantit une détection proactive des anomalies avant qu'elles ne provoquent une interruption de service.

- Collecte : le serveur interroge les agents installés sur les équipements (mode passif) ou reçoit les métriques envoyées par les agents (mode actif). Les protocoles SNMP et ICMP permettent de superviser les équipements sans agent.
- Évaluation : les valeurs collectées sont comparées à des seuils configurés (triggers). Un trigger passe en état Problème dès que la condition est remplie par exemple, charge CPU supérieure à 90 % pendant 5 minutes consécutives.
- Notification : lorsqu'un trigger est déclenché, une action est exécutée envoi d'un email, d'un message Slack, appel d'un webhook avec gestion des escalades si le problème n'est pas acquitté dans le délai imparti.
- Résolution : lorsque la condition revient à la normale, le trigger repasse en état OK et une notification de résolution est envoyée. L'historique complet de l'incident est conservé en base de données.

1.3 Ce que collecte un serveur de supervision

Au-delà de la simple disponibilité (ping), un serveur de supervision collecte l'ensemble des indicateurs nécessaires à la bonne connaissance de l'état de l'infrastructure :

- Métriques système : utilisation CPU, RAM, espace disque, charge système, nombre de processus actifs
- Métriques réseau : bande passante consommée, taux d'erreurs et de pertes sur les interfaces, latence
- Disponibilité des services : état des services systemd, des ports TCP/UDP ouverts, des applications web (HTTP/HTTPS)
- Métriques applicatives : temps de réponse des bases de données, files de messages, serveurs web
- Journaux système (log monitoring) : détection de patterns d'erreurs dans les fichiers de logs
- Équipements réseau via SNMP : état des interfaces, température, alimentation des switches et routeurs

1.4 Supervision dans une infrastructure multi-sites

Dans un environnement où certains équipements sont hébergés sur des sites distants, le serveur de supervision reste centralisé sur le site principal. Les agents installés sur les machines distantes communiquent avec le serveur via les tunnels IPsec site-à-site déjà en place. Du point de vue de Zabbix, la communication avec un agent distant est identique à celle avec un agent local, c'est le tunnel IPsec qui assure de manière transparente l'acheminement du trafic. Il est simplement nécessaire que les politiques de sécurité des tunnels autorisent le trafic TCP/10051 entre les sites distants et le serveur Zabbix.

1.5 Enjeux de disponibilité

Le service de supervision est lui-même critique : une panne du serveur signifie la perte de visibilité totale sur l'infrastructure, sans aucune alerte en cas d'incident. Les équipes travaillent alors en aveugle. C'est pourquoi la supervision doit être déployée sur un serveur dédié, stable, avec des ressources dimensionnées correctement, et dont la configuration et la base de données sont sauvegardées et testées régulièrement.

2. Étude des solutions de supervision

2.1 Critères d'évaluation

Les solutions de supervision ont été évaluées selon les critères suivants :

- Open Source ou sous licence libre, adapté à un déploiement sur infrastructure Debian/Linux
- Supervision multi-protocoles : agent natif, SNMP, ICMP, HTTP
- Interface web de visualisation et de gestion intégrée
- Système d'alertes et de notifications configurable avec escalades
- Scalabilité : capacité à superviser plusieurs centaines d'équipements sans dégradation
- Disponibilité d'une API REST pour l'automatisation et les intégrations
- Coût total de déploiement et de licence
- Complexité de mise en œuvre et de maintenance quotidienne
- Pérennité de la solution et activité de la communauté

2.2 Tableau comparatif

Critère	Zabbix 7.0 LTS	Nagios Core	Prometheus + Grafana	PRTG
Licence	Open Source (GPL)	Open Source (GPL)	Open Source (Apache 2)	Propriétaire
Coût	Gratuit	Gratuit	Gratuit	Dès 2 149 €/an (500 capteurs)
Agent natif	Oui	Oui	Non	Oui
SNMP natif	Oui	Via plugins	Non	Oui
Interface web	Complète et intégrée	CGI (très limitée)	Grafana (séparé)	Complète
API REST	Oui	Non	Oui (Prometheus)	Oui
Alertes	Natif, escalades, dépend.	Natif mais complexe	AlertManager (séparé)	Natif
Découverte auto	Oui	Limitée	Non	Oui
Gestion secrets	Vault / CyberArk natifs	Non	Non	Non
Complexité	Moyenne	Élevée	Élevée	Faible
Communauté	Très active	Active	Très active	Support éditeur

2.3 Analyse des solutions

Zabbix 7.0 LTS

Solution open source mature et activement maintenue par Zabbix LLC, Zabbix propose une architecture complète avec agent natif performant (zabbix-agent2, écrit en Go), support SNMP/ICMP/HTTP intégré, interface web riche, API REST complète et système d'alertes flexible avec escalades. La version 7.0 LTS bénéficie d'un support garanti jusqu'en 2029 et intègre nativement deux gestionnaires de secrets d'entreprise (HashiCorp Vault et CyberArk), ce qu'aucune autre solution open source du marché ne propose nativement. Elle s'impose comme la solution de référence pour la supervision d'infrastructures Linux mixtes avec sites distants.

Nagios Core

Historiquement la référence de la supervision Linux, Nagios Core est aujourd'hui dépassé par son architecture monolithique et l'absence totale d'API REST. Toute l'administration passe par des fichiers de configuration et une interface web CGI vieillissante. Sa flexibilité repose entièrement sur des plugins tiers, ce qui représente une charge de maintenance importante. Nagios Core ne propose pas de gestion native des escalades, des dépendances entre services, ni de tableaux de bord modernes. Son seul atout reste sa légèreté et sa réputation historique, mais il n'est plus adapté à une infrastructure d'entreprise moderne.

Prometheus + Grafana

Stack moderne orientée métriques temporelles, Prometheus excelle dans les environnements conteneurisés (Docker, Kubernetes) où chaque service expose ses métriques via un endpoint HTTP. Son modèle pull implique de déployer un exporter spécifique pour chaque type de service ou d'équipement à superviser, multipliant les composants à maintenir. Prometheus ne supporte pas SNMP nativement et n'intègre pas d'interface de gestion des hôtes. Grafana, utilisé pour la visualisation, est un outil distinct qui ne gère pas nativement les alertes métier (acquittements, escalades, maintenances planifiées). Pour une infrastructure réseau traditionnelle avec sites distants, l'empilement de composants et la complexité globale sont significativement plus élevés que Zabbix.

PRTG (Paessler)

Solution propriétaire développée par Paessler, PRTG propose une expérience utilisateur soignée, une installation rapide et un support SNMP très complet. En revanche, son modèle de licence commercial basé sur le nombre de capteurs devient rapidement coûteux à mesure que l'infrastructure grandit : une installation de 500 capteurs démarre à environ 2 149 €/an, et les grandes infrastructures peuvent atteindre plusieurs dizaines de milliers d'euros annuels. Sa dépendance à Windows pour le serveur central et l'absence de code source ouvert en font un choix inadapté pour une infrastructure Linux/Open Source.

3. Solution retenue : Zabbix 7.0 LTS

Solution retenue
Zabbix 7.0 LTS déployé sur un serveur Debian 13 (Trixie) dédié dans le VLAN 20 (172.18.20.0/24). Les agents Zabbix 2 supervisent les serveurs locaux du VLAN 20 et les machines virtuelles des sites distants via les tunnels IPsec existants.

3.1 Justification du choix

- Open Source et gratuit, aucun coût de licence, support LTS garanti jusqu'en 2029
- Agent natif zabbix-agent2 (Go) : supervision système complète, faible empreinte mémoire, mode actif et passif
- Support SNMP natif : supervision des équipements réseau sans agent supplémentaire
- Transparence IPsec : les agents des sites distants communiquent exactement comme des agents locaux, sans configuration spécifique côté Zabbix
- Interface web complète et intégrée : dashboards, graphiques, cartes réseau, gestion centralisée de tous les hôtes
- Intégration native des gestionnaires de secrets : HashiCorp Vault et CyberArk Vault supportés nativement
- Système d'alertes avancé : notifications multi-canal avec escalades, dépendances et maintenances planifiées
- Templates officiels prêts à l'emploi : Linux, Windows, MySQL, Nginx, OPNsense, VMware, etc.

3.2 Gestion des secrets

Zabbix 7.0 propose nativement trois approches pour protéger les informations sensibles :

Mécanisme	Principe	Usage recommandé
Fichier Include séparé	DBPassword isolé dans un fichier dédié (640 root:zabbix), référencé par Include= dans zabbix_server.conf	Infrastructure interne sans gestionnaire de secrets, simple et efficace
HashiCorp Vault	Zabbix interroge Vault via son API pour récupérer les secrets à la volée. Configuré via VaultURL et VaultToken dans zabbix_server.conf	Infrastructures disposant déjà de HashiCorp Vault
CyberArk Vault	Intégration native CyberArk via VaultDBPath. Zabbix récupère les credentials depuis le coffre CyberArk au démarrage	Grandes entreprises avec CyberArk en place

Solution retenue pour oasis.local

La méthode du fichier Include séparé est retenue pour ce projet. Elle est native, sans dépendance externe, et offre une séparation propre entre configuration et secrets. Les options HashiCorp Vault et CyberArk restent disponibles si l'infrastructure évolue.

3.3 Architecture déployée

Composant	Rôle	Port
zabbix-server	Serveur central : collecte des métriques, évaluation des triggers, gestion des alertes	10051/TCP
zabbix-agent2 (local)	Agent sur les serveurs du VLAN 20	10050/TCP
zabbix-agent2 (distant)	Agent sur les VMs des sites distants ; communication via tunnel IPsec	10050/TCP via IPsec
zabbix-frontend-php	Interface web d'administration et de visualisation	443/TCP via Nginx
MariaDB	Base de données : configuration et historique des métriques	3306/TCP (localhost)
Nginx	Serveur web : interface en HTTPS avec certificat auto-signé	443/TCP

3.4 Plan d'adressage

Emplacement	Réseau	Rôle	Remarque
Site principal : VLAN 20	172.18.20.0/24	Serveur Zabbix (172.18.20.10) + serveurs supervisés locaux	Communication directe sur le LAN
Site distant A	Réseau distant A	VMs supervisées	Agents joignables via tunnel IPsec site-à-site
Site distant B	Réseau distant B	VMs supervisées	Agents joignables via tunnel IPsec site-à-site

4. Prérequis à la mise en place de Zabbix

4.1 Prérequis matériels et systèmes

- Un serveur (physique ou virtuel) sous Debian 13 (Trixie)
- Minimum recommandé : 2 vCPU, 2 Go de RAM, 60 Go de disque (OS inclus, permet une rétention confortable de 30 jours d'historique pour une dizaine d'hôtes)
- Interface réseau connectée au VLAN 20 (172.18.20.0/24)
- Accès Internet ou miroir APT disponible pour l'installation des paquets
- Entrée DNS : monitoring.oasis.local → 172.18.20.10

4.2 Prérequis réseau

- TCP/10051 entrant autorisé sur le serveur Zabbix depuis le VLAN 20 (agents locaux)
- TCP/10051 entrant autorisé dans les politiques des tunnels IPsec depuis chaque site distant vers 172.18.20.10
- TCP/443 entrant autorisé depuis les postes d'administration vers le serveur Zabbix
- Tunnels IPsec site-à-site opérationnels et stables avant le déploiement des agents distants
- Résolution DNS fonctionnelle pour le domaine oasis.local (172.18.20.1)
- NTP synchronisé sur le serveur et sur tous les équipements supervisés, locaux et distants

4.3 Prérequis logiciels

- Paquets requis : zabbix-server-mysql, zabbix-frontend-php, zabbix-nginx-conf, zabbix-sql-scripts, zabbix-agent2, mariadb-server, mariadb-client
- Nginx : serveur web pour l'interface (inclus avec zabbix-nginx-conf)
- PHP 8.x avec extensions Zabbix (installées automatiquement par les dépendances)

4.4 Informations à préparer

Paramètre	Valeur
IP Serveur Zabbix	172.18.20.10
Passerelle VLAN 20	172.18.20.254
Serveur DNS	172.18.20.1
Domaine	oasis.local
URL interface web	https://monitoring.oasis.local
Base de données	zabbix (MariaDB, localhost)
Utilisateur BDD Zabbix	adm_zabbix (localhost uniquement)
Gestion mot de passe BDD	Fichier secret séparé via directive Include

5. Mise en place de Zabbix

5.1 Préparation du serveur

Configuration de l'interface réseau

Ouvrir le fichier de configuration réseau :

```
nano /etc/network/interfaces
```

Configurer l'interface statique :

```
auto ens18
iface ens18 inet static
    address 172.18.20.10
    netmask 255.255.255.0
    gateway 172.18.20.254
    dns-nameservers 172.18.20.1
    dns-search oasis.local
```

```
systemctl restart networking
```

Mise à jour du système et installation de Zabbix

```
apt update && apt upgrade -y

# Ajouter le dépôt officiel Zabbix 7.0 pour Debian 13 (Trixie)
wget https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.0+debian13_all.deb
dpkg -i zabbix-release_latest_7.0+debian13_all.deb
apt update

# Installer les composants Zabbix, MariaDB et le client
apt install -y zabbix-server-mysql zabbix-frontend-php zabbix-nginx-conf zabbix-sql-scripts zabbix-agent2 mariadb-server mariadb-client
```

Sauvegarde des fichiers de configuration originaux

```
cp /etc/zabbix/zabbix_server.conf /etc/zabbix/zabbix_server.conf.bak
cp /etc/nginx/conf.d/zabbix.conf  /etc/nginx/conf.d/zabbix.conf.bak
```

5.2 Configuration de la base de données

Sécurisation initiale de MariaDB

Sur Debian 13 avec MariaDB 11.x, le script mysql_secure_installation a été remplacé par mariadb-secure-installation :

```
mariadb-secure-installation
```

> **Réponses recommandées**
> Switch to unix_socket auth : N ; Change root password : Y (mot de passe fort) ; Remove anonymous users : Y ; Disallow root login remotely : Y ; Remove test database : Y ; Reload privilege tables : Y

Création de la base et de l'utilisateur Zabbix

L'utilisateur MariaDB est nommé adm_zabbix (underscore est la convention standard MariaDB). La base de données conserve le nom zabbix, requis par Zabbix.

```
mysql -u root -p

-- Dans le prompt MariaDB :
CREATE DATABASE zabbix CHARACTER SET utf8mb4 COLLATE utf8mb4_bin;
CREATE USER 'adm_zabbix'@'localhost' IDENTIFIED BY 'MotDePasseGenere!';
GRANT ALL PRIVILEGES ON zabbix.* TO 'adm_zabbix'@'localhost';
FLUSH PRIVILEGES;
QUIT;
```

Import du schéma initial

```
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -u adm_zabbix -p zabbix

# L'import dure environ 2 minutes
```

5.3 Configuration de Zabbix Server

Création du fichier de secrets

Pour ne pas stocker le mot de passe de la base de données dans le fichier de configuration principal, Zabbix permet de le déléguer à un fichier séparé via la directive Include. Ce fichier reçoit des droits d'accès stricts : seul le service Zabbix (utilisateur système zabbix, créé automatiquement à l'installation du paquet) peut le lire.

```
# Créer le fichier de secrets
echo 'DBPassword=MotDePasseGenere!' > /etc/zabbix/zabbix_server.secret

# Restreindre l'accès
chmod 640 /etc/zabbix/zabbix_server.secret
chown root:zabbix /etc/zabbix/zabbix_server.secret
```

> **Comment fonctionne Include=/etc/zabbix/zabbix_server.secret**
> La directive Include indique au serveur Zabbix de lire un fichier supplémentaire et d'y importer les paramètres comme s'ils étaient écrits directement dans le fichier principal. En plaçant DBPassword dans ce fichier séparé avec des droits 640 (root:zabbix), le mot de passe n'est jamais visible dans le fichier de configuration principal. Seul le service Zabbix peut le lire.

Fichier de configuration principal

Le fichier zabbix_server.conf d'origine fait plusieurs centaines de lignes avec des paramètres système indispensables (PidFile, SocketDir, FpingLocation...). Il ne faut pas l'écraser. Ajouter les paramètres personnalisés en début de fichier.

```
nano /etc/zabbix/zabbix_server.conf
```

Ajouter ces lignes tout en début du fichier :

```
# Connexion à la base de données
DBHost=localhost
DBName=zabbix
DBUser=adm_zabbix
# Le mot de passe est lu depuis le fichier secret ci-dessous
Include=/etc/zabbix/zabbix_server.secret

# Performances (adapter selon la RAM disponible)
StartPollers=10
StartPingers=5
CacheSize=128M
HistoryCacheSize=64M
ValueCacheSize=64M

# Activer les scripts globaux (ping depuis l'interface web)
EnableGlobalScripts=1
```

Attention aux paramètres en double dans le fichier

Le fichier d'origine contient des paramètres système obligatoires (PidFile, SocketDir, FpingLocation) qu'il ne faut pas supprimer. Certains paramètres comme EnableGlobalScripts=0 sont déjà présents plus bas dans le fichier, la première valeur lue prend le dessus, mais pour éviter toute confusion il vaut mieux commenter la valeur d'origine. Exemple : sed -i 's/^EnableGlobalScripts=0/# EnableGlobalScripts=0/' /etc/zabbix/zabbix_server.conf

```
# Commenter les doublons potentiels dans le fichier de base
sed -i 's/^EnableGlobalScripts=0/# EnableGlobalScripts=0/'
/etc/zabbix/zabbix_server.conf

# Vérifier qu'il n'y a pas de doublon actif
grep -i EnableGlobalScripts /etc/zabbix/zabbix_server.conf

# Sécuriser le fichier de configuration
chmod 640 /etc/zabbix/zabbix_server.conf
chown root:zabbix /etc/zabbix/zabbix_server.conf
```

5.4 Configuration Nginx et HTTPS

Désactivation du site par défaut

Sur Debian, Nginx charge un site par défaut depuis sites-enabled qui prend le dessus sur la configuration Zabbix. Le supprimer pour laisser uniquement la configuration Zabbix active :

```
# Supprimer le lien symbolique (le fichier source dans sites-available est
conservé)
rm /etc/nginx/sites-enabled/default
```

> **Pourquoi conf.d et pas sites-enabled**
> Nginx charge automatiquement tous les fichiers dans conf.d/. La configuration Zabbix installée par le paquet zabbix-nginx-conf est déjà dans conf.d/zabbix.conf, il n'est pas nécessaire de la déplacer dans sites-enabled. Supprimer le site default suffit.

Certificat auto-signé pour usage interne

Le domaine monitoring.oasis.local étant un domaine DNS interne, un certificat Let's Encrypt (réservé aux domaines publics) n'est pas utilisable. Un certificat auto-signé chiffre intégralement les échanges entre le navigateur et l'interface Zabbix. La première connexion affiche un avertissement navigateur à accepter une seule fois.

```
mkdir -p /etc/nginx/ssl
openssl req -x509 -nodes -days 1095 -newkey rsa:4096 -keyout
/etc/nginx/ssl/zabbix.key -out /etc/nginx/ssl/zabbix.crt -subj
'/C=FR/ST=IDF/O=oasis.local/CN=monitoring.oasis.local'

chmod 600 /etc/nginx/ssl/zabbix.key
chmod 644 /etc/nginx/ssl/zabbix.crt
```

Configuration du bloc Nginx

Le paquet zabbix-nginx-conf installe une configuration complète et optimisée dans /etc/nginx/conf.d/zabbix.conf. Modifier uniquement la partie server pour ajouter SSL et les en-têtes de sécurité :

```
nano /etc/nginx/conf.d/zabbix.conf
```

```
server {
    listen 443 ssl;
    http2 on;
    server_name monitoring.oasis.local;

    ssl_certificate     /etc/nginx/ssl/zabbix.crt;
    ssl_certificate_key /etc/nginx/ssl/zabbix.key;
    ssl_protocols       TLSv1.2 TLSv1.3;
    ssl_ciphers         ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384;
```

```
    add_header Strict-Transport-Security 'max-age=31536000' always;
    add_header X-Frame-Options SAMEORIGIN;
    add_header X-Content-Type-Options nosniff;

    root  /usr/share/zabbix;
    index index.php;

    location / { try_files $uri $uri/ =404; }

    location ~ \.php$ {
        fastcgi_pass            unix:/var/run/php/zabbix.sock;
        fastcgi_split_path_info ^(.+\.php)(/.+)$;
        fastcgi_index           index.php;
        fastcgi_param           DOCUMENT_ROOT   /usr/share/zabbix;
        fastcgi_param           SCRIPT_FILENAME
/usr/share/zabbix$fastcgi_script_name;
        fastcgi_param           PATH_TRANSLATED
/usr/share/zabbix$fastcgi_script_name;
        include                 fastcgi_params;
        fastcgi_param           QUERY_STRING    $query_string;
        fastcgi_param           REQUEST_METHOD  $request_method;
        fastcgi_param           CONTENT_TYPE    $content_type;
        fastcgi_param           CONTENT_LENGTH  $content_length;
        fastcgi_intercept_errors        on;
        fastcgi_ignore_client_abort     off;
        fastcgi_connect_timeout         60;
        fastcgi_send_timeout            180;
        fastcgi_read_timeout            180;
        fastcgi_buffer_size             128k;
        fastcgi_buffers                 4 256k;
        fastcgi_busy_buffers_size       256k;
        fastcgi_temp_file_write_size    256k;
    }
    location ~* \.(htaccess|ini|log|sh|sql|conf)$ { deny all; }
}

server {
    listen 80;
    server_name monitoring.oasis.local;
    return 301 https://$host$request_uri;
}
```

```
nginx -t && systemctl reload nginx
```

5.5 Démarrage et activation des services

```
# Activer les services au démarrage système
systemctl enable zabbix-server zabbix-agent2 nginx mariadb

# Démarrer les services
systemctl start zabbix-server zabbix-agent2

# Vérifier le statut
systemctl status zabbix-server zabbix-agent2 nginx mariadb
```

> **En cas d'erreur au démarrage**
> Consulter les journaux : journalctl -u zabbix-server -n 50 --no-pager
> Vérifier la configuration : zabbix_server -c /etc/zabbix/zabbix_server.conf -T

5.6 Installation graphique via le navigateur

Ouvrir un navigateur depuis un poste d'administration et accéder à l'IP du serveur Zabbix. Accepter l'avertissement du certificat auto-signé (domaine interne .local).

```
https://172.18.20.10
```

L'assistant d'installation se déroule en 6 étapes :

Sélectionner la langue

Sélectionner la langue Français (fr_FR) dans le menu déroulant. Cliquer sur Prochaine étape.

Vérification des prérequis

Zabbix vérifie automatiquement que tous les prérequis PHP sont satisfaits. Tous les éléments doivent afficher OK avant de continuer :

Prérequis	Valeur requise	Résultat attendu
Version de PHP	>= 8.0.0	OK
Option PHP memory_limit	128M	OK
Option PHP post_max_size	16M	OK
Option PHP upload_max_filesize	2M	OK
Option PHP max_execution_time	300	OK

Prérequis	Valeur requise	Résultat attendu
Option PHP max_input_time	300	OK
Support MySQL par PHP	Actif	OK
bcmath pour PHP	Actif	OK
mbstring pour PHP	Actif	OK

Configurer la connexion à la base de données

Renseigner les paramètres de connexion MariaDB :

Champ	Valeur
Type de base de données	MySQL
Hôte base de données	localhost
Port de la base de données	0 (port par défaut : socket Unix)
Nom de la base de données	zabbix
Stocker les informations dans	Texte brut (ou Coffre HashiCorp / CyberArk si disponible)
Utilisateur	adm_zabbix
Mot de passe	Mot de passe défini lors de la création de l'utilisateur MariaDB

Chiffrement TLS de la base de données
L'interface affiche : 'La connexion ne sera pas chiffrée car elle utilise un fichier socket (sous Unix)'. C'est normal et attendu, la connexion entre Zabbix et MariaDB passe par socket local, le chiffrement TLS n'a de sens que pour une connexion réseau distante.

Paramètres

Configurer les paramètres généraux du serveur :

Champ	Valeur
Nom du serveur Zabbix	SRV-N-MTR (ou nom choisi affiché dans l'interface et les notifications)
Fuseau horaire par défaut	(UTC+02:00) Europe/Paris
Thème par défaut	Bleu (ou selon préférence)

Résumé pré-installation

Vérifier que tous les paramètres sont corrects avant de valider :

Paramètre	Valeur attendue
Type de base de données	MySQL
Serveur base de données	localhost
Port de la base de données	défaut
Nom de la base de données	zabbix
Utilisateur base de données	adm_zabbix
Chiffrement TLS	false (normal pour socket Unix)
Nom du serveur Zabbix	SRV-N-MTR

Si tout est correct, cliquer sur Prochaine étape pour lancer l'installation.

Installation

Zabbix crée automatiquement le fichier de configuration PHP conf/zabbix.conf.php. Le message suivant confirme le succès de l'installation :

> **Félicitations !**
> Vous avez installé l'interface Zabbix avec succès. Fichier de configuration conf/zabbix.conf.php créé.

Cliquer sur Terminé pour accéder à la page de connexion. Se connecter avec les identifiants par défaut :

Paramètre	Valeur
URL	https://172.18.20.10
Login par défaut	Admin
Mot de passe par défaut	zabbix

> **Action prioritaire**
> Le mot de passe 'zabbix' du compte Admin est connu publiquement. Le modifier immédiatement après le premier accès : Utilisateurs → Utilisateurs → Admin → Changer le mot de passe. Désactiver également le compte 'guest' : Utilisateurs → Utilisateurs → guest → décocher Activé → Mettre à jour.

5.7 Configuration de l'interface web

Une fois connecté, effectuer les réglages suivants avant tout ajout d'hôte.

Langue et fuseau horaire

Administration → Général → GUI :

- Langue par défaut : Français
- Fuseau horaire : Europe/Paris
- Thème : selon préférence

Rétention des données (Nettoyage)

Administration → Nettoyage. La rétention définit combien de temps Zabbix conserve l'historique des métriques en base de données. Les paramètres et leur signification :

Paramètre	Valeur recommandée	Description
Période de stockage des données de déclencheurs	365 jours	Historique de toutes les alertes : problèmes déclenchés, résolus, acquittés
Période de stockage des données de service	30 jours	Événements liés aux services IT Zabbix (SLA). 1 jour par défaut est insuffisant
Période de stockage des données internes	30 jours	Événements internes Zabbix (items non supportés, etc.)
Période de stockage des données de découverte réseau	30 jours	Résultats des scans de découverte automatique réseau
Période de stockage des données d'enregistrement automatique	30 jours	Historique des agents enregistrés automatiquement
Période de stockage des données : Services	365 jours	Historique des services IT pour calculs de disponibilité et SLA
Période de stockage des données : Sessions	365 jours	Sessions de connexion à l'interface web, utile pour l'audit
Historique : Période de stockage des données	31 jours	Valeur brute collectée toutes les X secondes. Le plus volumineux, adapté à 80 Go de stockage
Tendances : Période de stockage des données	365 jours	Moyennes horaires calculées, très peu volumineuses, garder un an

> **Surcharger la période des éléments**

> Les champs Historique et Tendances sont grisés par défaut, les valeurs sont définies dans chaque template. Cocher 'Surcharger' uniquement si tu veux imposer une valeur globale différente des templates, par exemple pour réduire la rétention sur tous les items d'un coup.

Rôles utilisateur et groupes d'utilisateurs

Dans Zabbix 7.0, la gestion des droits repose sur deux niveaux distincts et complémentaires.

Les rôles (Utilisateurs → Rôles utilisateur) définissent ce que l'utilisateur peut faire dans l'interface :

Rôle	Droits
Super admin role	Accès total, configuration, utilisateurs, toute l'interface sans restriction
Admin role	Configuration des hôtes, templates, triggers, pas de gestion des utilisateurs
User role	Surveillance uniquement : voir les données, graphiques, alertes, pas de configuration
Guest role	Accès en lecture seule minimal, encore plus restreint que User role correspond au compte guest désactivé

Les groupes d'utilisateurs (Utilisateurs → Groupes d'utilisateurs) définissent quels hôtes et données l'utilisateur peut voir :

Groupe	Description
Zabbix administrators	Groupe par défaut avec accès à tous les hôtes pour les administrateurs
Internal	Utilisateurs internes avec accès standard
Guests	Accès invité : lecture seule très limitée
No access to the frontend	Bloque complètement l'accès à l'interface web
Disabled	Désactive l'utilisateur sans le supprimer
Enabled debug mode	Active le mode debug dans l'interface pour le diagnostic

> **Résumé Rôle vs Groupe**
> Le rôle contrôle ce que l'utilisateur peut FAIRE (configurer, voir, administrer). Le groupe contrôle quels HÔTES et DONNÉES il peut voir. Un utilisateur avec le rôle Admin mais dans un groupe sans accès à certains hôtes ne verra pas ces hôtes du tout. Pour oasis.local avec une seule équipe, utiliser Zabbix administrators + Super admin role ou Admin role selon le niveau de responsabilité.

Canaux de notification

Zabbix supporte de nombreux canaux de notification : email (SMTP), Slack, Microsoft Teams, Telegram, webhooks personnalisés, etc. La configuration des notifications est à réaliser ultérieurement selon les ressources disponibles. Les canaux se configurent dans Administration → Général → Types de médias.

> **Sans notification active**
> Sans canal de notification configuré, Zabbix détecte et enregistre les pannes mais ne peut pas alerter activement. L'état des hôtes reste visible en temps réel dans l'interface (icône rouge si hôte injoignable) et dans Surveillance → Problèmes. Une surveillance régulière de l'interface est nécessaire en attendant la mise en place d'un canal d'alerte.

Tableau de bord opérationnel

Tableaux de bord → Créer un tableau de bord. Widgets recommandés :

- Problèmes : liste des alertes actives en temps réel
- Vue d'ensemble des hôtes : statut global (disponible / problème / inconnu)
- Graphique : CPU, RAM ou réseau des hôtes critiques
- Disponibilité des hôtes : synthèse par groupe
- Top 10 : hôtes avec le plus d'alertes récentes

5.8 Importer un template dans Zabbix

Zabbix propose des templates officiels qui ne sont pas inclus par défaut dans l'installation. Pour les utiliser, il faut les télécharger et les importer manuellement. Exemple avec le template OPNsense by SNMP :

Télécharger le template sur le serveur Zabbix

```
# Télécharger le template depuis GitHub officiel Zabbix
wget -O /tmp/opnsense_snmp.yaml
'https://raw.githubusercontent.com/zabbix/zabbix/release/7.0/templates/app/opnsense_snmp/templa

# Vérifier que c'est bien un fichier YAML Zabbix
head -3 /tmp/opnsense_snmp.yaml
# Résultat attendu : zabbix_export:

# Copier dans le répertoire web pour le télécharger depuis le navigateur
cp /tmp/opnsense_snmp.yaml /usr/share/zabbix/opnsense_snmp.yaml
```

Récupérer le fichier sur le poste d'administration

Ouvrir un navigateur et accéder à l'URL suivante pour télécharger le fichier YAML :

```
https://172.18.20.10/opnsense_snmp.yaml
```

Le navigateur propose de télécharger le fichier. L'enregistrer sur le poste d'administration.

Importer dans l'interface Zabbix

Dans l'interface web Zabbix :

- Collecte de données → Templates
- Cliquer sur le bouton Importer (en haut à droite)
- Cliquer sur Choisir un fichier → sélectionner le fichier YAML téléchargé
- Cliquer sur Importer

Le template apparaît dans la liste des templates et peut être appliqué à un hôte. La procédure est identique pour tout template officiel Zabbix non inclus par défaut.

6. Supervision

6.1 Supervision Linux

Agent Zabbix

Pour tous les serveurs Linux accessibles, l'agent Zabbix 2 est la méthode recommandée.
Elle offre plus de métriques et une communication bidirectionnelle.

Installer l'agent 2 de Zabbix

```
wget https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.0+debian13_all.deb

dpkg -i zabbix-release_latest_7.0+debian13_all.deb

apt update && apt install -y zabbix-agent2
```

Configuration de /etc/zabbix/zabbix_agent2.conf :

```
Server=172.18.20.10
ServerActive=172.18.20.10
Hostname=nom-du-serveur
DenyKey=system.run[*]
LogType=file
LogFile=/var/log/zabbix/zabbix_agent2.log
LogFileSize=50
```

Activer, démarrer et vérifier le service de l'agent Zabbix.

```
systemctl enable --now zabbix-agent2
systemctl status zabbix-agent2
```

Dans l'interface Zabbix, aller sur Collecte de données → Hôtes → Créer un hôte.

Champ	Valeur
Nom d'hôte	Identique au paramètre Hostname dans zabbix_agent2.conf
Groupes	Linux servers
Interface	Agent, IP de l'hôte, Port 10050
Templates	Linux by Zabbix agent

SNMP

La supervision Linux via SNMP est possible si l'installation de l'agent n'est pas envisageable. Elle nécessite l'installation du daemon SNMP sur l'hôte supervisé.

Installer snmpd sur l'hôte Linux à superviser.

```
apt install -y snmpd
```

Editer /etc/snmp/snmpd.conf.

```
# Autoriser les connexions depuis le serveur Zabbix uniquement
agentaddress udp:161

# Définir la communauté SNMP (remplacer public par une valeur secrète)
rocommunity MDP 172.18.20.10
```

Activer, démarrer et vérifier le service SNMP.

```
systemctl enable --now snmpd
systemctl status snmpd
```

Dans l'interface Zabbix, aller sur Collecte de données → Hôtes → Créer un hôte.

Champ	Valeur
Nom d'hôte	Nom de l'hôte
Groupes	Linux servers
Interface	SNMP, IP de l'hôte, Port 161
Version SNMP	SNMPv2
Communauté SNMP	{$SNMP_COMMUNITY}
Templates	Linux by SNMP

> **Agent recommandé pour Linux**
> La supervision SNMP Linux ne donne pas accès à tous les items disponibles via l'agent (processus détaillés, métriques applicatives, logs). Utiliser l'agent Zabbix 2 chaque fois que possible et SNMP uniquement si l'installation d'un agent est impossible.

6.2 Supervision Windows

Agent Zabbix

Télécharger l'installeur MSI depuis https://www.zabbix.com/download et choisir la version 7.0, Windows, Agent 2. Lors de l'installation, renseigner :

Paramètre	Valeur
Zabbix server IP	172.18.20.10
Host name	Nom du serveur Windows
Server active	172.18.20.10

L'agent s'installe en tant que service Windows et démarre automatiquement.

Dans l'interface Zabbix, aller sur Collecte de données → Hôtes → Créer un hôte.

Champ	Valeur
Nom d'hôte	Identique au Host name saisi lors de l'installation
Groupes	Windows servers
Interface	Agent, IP du serveur Windows, Port 10050
Templates	Windows by Zabbix agent

SNMP

Windows intègre un agent SNMP natif qui peut être activé sans installation tierce. Utile pour superviser des serveurs Windows sans déployer l'agent Zabbix.

Ouvrir PowerShell avec des privilèges et ajouter le service SNMP Windows.

```
# Dans PowerShell en administrateur :
Add-WindowsFeature SNMP-Service
```

Configurer le service SNMP dans les propriétés du service (services.msc) → onglet Sécurité.

Paramètre	Valeur
Nom de communauté	oasis-snmp-2026 (même valeur que la macro Zabbix)
Droits	LECTURE SEULE
Accepter les paquets SNMP de ces hôtes	172.18.20.10 (IP du serveur Zabbix uniquement)

Dans l'interface Zabbix, aller sur Collecte de données → Hôtes → Créer un hôte.

Champ	Valeur
Nom d'hôte	Nom du serveur Windows
Groupes	Windows servers
Interface	SNMP, IP du serveur, Port 161
Version SNMP	SNMPv2
Communauté SNMP	{$SNMP_COMMUNITY}
Templates	Windows by SNMP

Agent recommandé pour Windows

Comme pour Linux, l'agent Zabbix 2 Windows donne accès à bien plus de métriques que SNMP (services Windows, registre, WMI, performance counters). Utiliser SNMP uniquement si le déploiement de l'agent n'est pas possible.

6.3 Supervision pfSense

Agent Zabbix

Dans l'interface pfSense : Système → Gestionnaire de paquets → Paquets disponibles → rechercher zabbix → installer Zabbix Agent 7.

Après installation : Services → Zabbix Agent 7:

Paramètre	Valeur
Enabled	Cocher
Hostname	Nom du pare-feu
Server	172.18.20.10
Server Port	10051

Sauvegarder et démarrer le service.

Dans l'interface Zabbix, aller sur Collecte de données → Hôtes → Créer un hôte.

Champ	Valeur
Nom d'hôte	Identique au paramètre Hostname dans la config agent
Groupes	Firewalls (ou Network devices)
Interface	Agent, IP du firewall, Port 10050
Templates	FreeBSD by Zabbix agent

> **Métriques disponibles avec l'agent**
> CPU (utilisation par coeur), RAM, espace disque, interfaces réseau (trafic entrant/sortant, erreurs), processus actifs, charge système, uptime. Bien plus complet que SNMP qui ne remonte que le trafic des interfaces.

6.4 Supervision OPNsense

Agent Zabbix

Dans l'interface OPNsense : Système → Firmware → Plugins → activer Show community plugins → rechercher zabbix → installer os-zabbix7-agent.

> **Choix du paquet OPNsense**
> os-zabbix7-agent correspond à Zabbix 7.x (version utilisée dans ce projet). Ne pas utiliser os-zabbix6-agent (Zabbix 6.x), os-zabbix72-agent (7.2) ou os-zabbix74-agent (7.4). Ils sont incompatibles avec un serveur Zabbix 7.0 LTS.

Après installation : Services → Zabbix Agent → Settings :

Paramètre	Valeur
Enabled	Cocher
Hostname	Nom du pare-feu
Listen Port	10050
Listen IPs	0.0.0.0
Zabbix Servers	172.18.20.10

Dans l'interface Zabbix, aller sur Collecte de données → Hôtes → Créer un hôte.

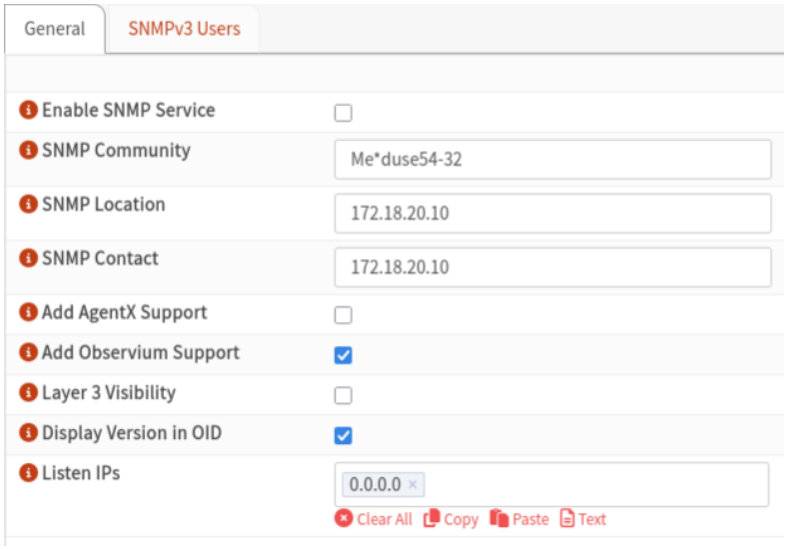
Champ	Valeur
Nom d'hôte	Identique au paramètre Hostname dans la config agent
Groupes	Firewalls (ou Network devices)
Interface	Agent, IP du firewall, Port 10050
Templates	FreeBSD by Zabbix agent

SNMP

Dans l'interface d'OPNsense : System → Firmware → Plugins → cocher afficher les plugins communautaires.

Rechercher Net-SNMP et l'installer.

Dans services → Neet-SNMP, renseigner le secret communauté, et l'IP du serveur Zabbix dans SNMP location et contact.



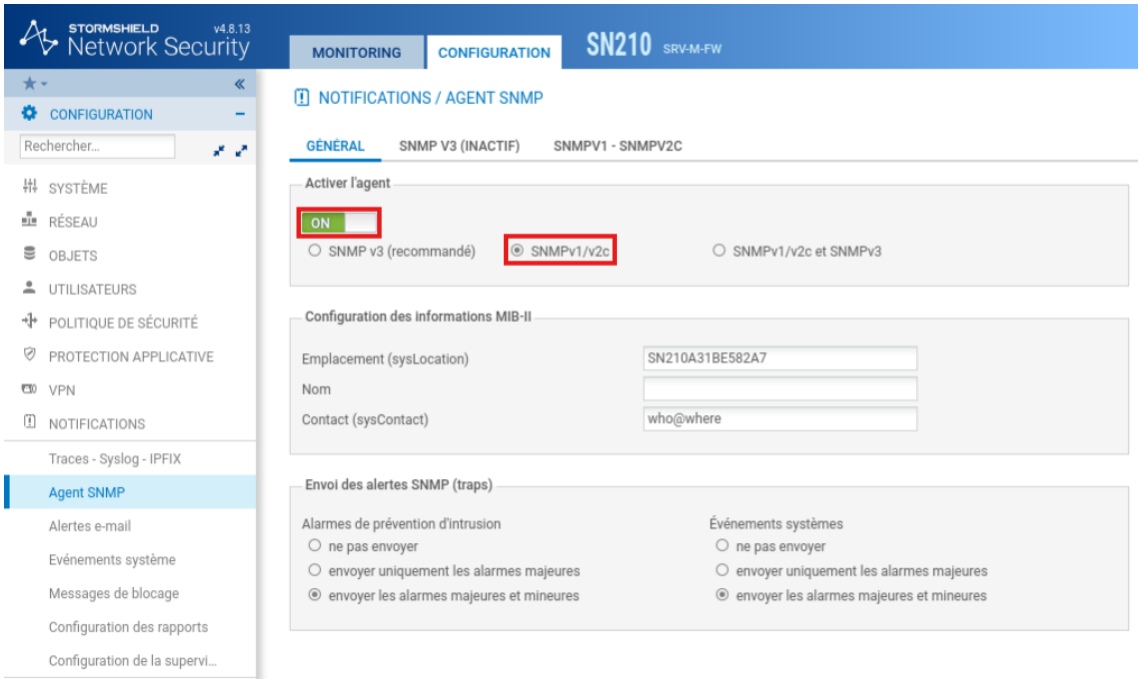
Dans l'interface Zabbix, aller sur Collecte de données → Hôtes → Créer un hôte.

Champ	Valeur
Nom d'hôte	Nom de l'hôte
Groupes	Firewalls
Interface	SNMP, IP de l'hôte, Port 161
Version SNMP	SNMPv2
Communauté SNMP	{$SNMP_COMMUNITY}
Templates	FreeBSD by SNMP

6.5 Supervision Stormshield

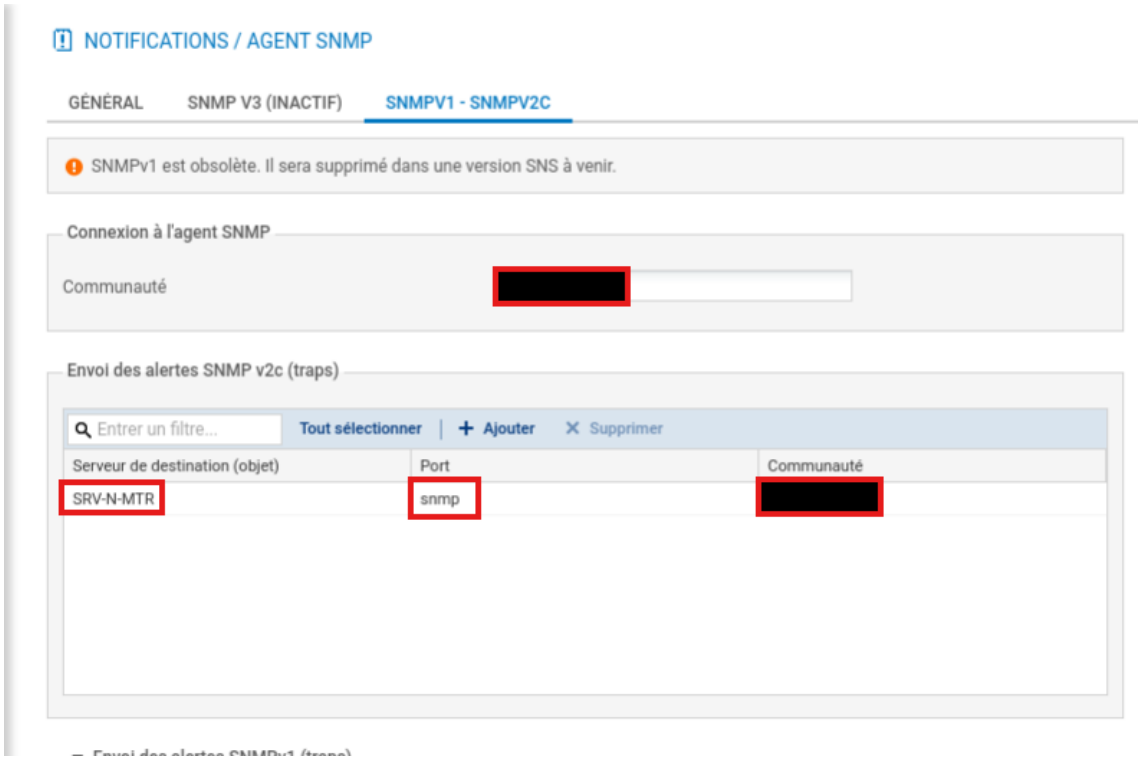
Dans l'interface Stormshield : Configuration → Notifications → Agent SNMP → activer l'agent SNMP.

Puis, cochez SNMPv1/v2c.



Dans l'onglet SNMPv1 – SNMPv2C, renseigner le secret communauté.

Ajouter un envoie d'alertes SNMP en saisissant l'objet (alias) du serveur Zabbix, le protocole et le secret communauté. Puis appliquer.



6.6 Supervision Pare-feu en CARP

Architecture réseau

Champ	Valeur
Serveur Zabbix (Nantes)	`172.18.20.10`
FW1 MASTER CARP (Paris)	`172.16.20.252`
FW2 BACKUP CARP (Paris)	`172.16.20.253`
IP CARP virtuelle WAN	`10.44.151.200`
IP CARP virtuelle ADMIN	`172.16.20.254`

> Le tunnel IPSEC est monté depuis l'IP CARP WAN (10.44.151.200) et géré uniquement par FW1 (MASTER). FW2 en mode BACKUP ne participe pas au tunnel.

Problème identifié

Lorsque Zabbix (Nantes) tente de joindre FW2 (172.16.20.253) via le tunnel IPSEC, le scénario suivant se produit :

1. Le paquet arrive dans le tunnel IPSEC sur FW1 (MASTER).
2. FW1 décapsule le paquet et le forward vers FW2 sur l'interface ADMIN.
3. FW2 reçoit le paquet mais ne connaît pas la route retour vers 172.18.20.0/24.
4. FW2 tente d'utiliser sa copie du tunnel IPSEC, qui est DOWN car il est en BACKUP.
5. La réponse est droppée, Zabbix ne reçoit rien.

> Ce comportement est documenté par Netgate (pfSense). La solution officielle est de configurer un Outbound NAT pour masquer l'IP source.

Solution appliquée

Trois actions ont été nécessaires pour résoudre le problème :

Règle Firewall ADMIN sur FW1

Depuis l'interface web de FW1 via l'IP CARP (172.16.20.254), ajouter une règle dans Firewall > Rules > ADMIN :

Champ	Valeur
Action	Pass
Protocol	Any
Source	NET_NAN (172.18.20.0/24)

Destination	GS_FIREWALLS (alias contenant 172.16.20.252 et 172.16.20.253)
Description	Accès Nantes vers FW

Cette règle se synchronise automatiquement sur FW2 via la réplication CARP. Elle permet à FW2 d'accepter le trafic venant de Nantes qui lui est destiné directement.

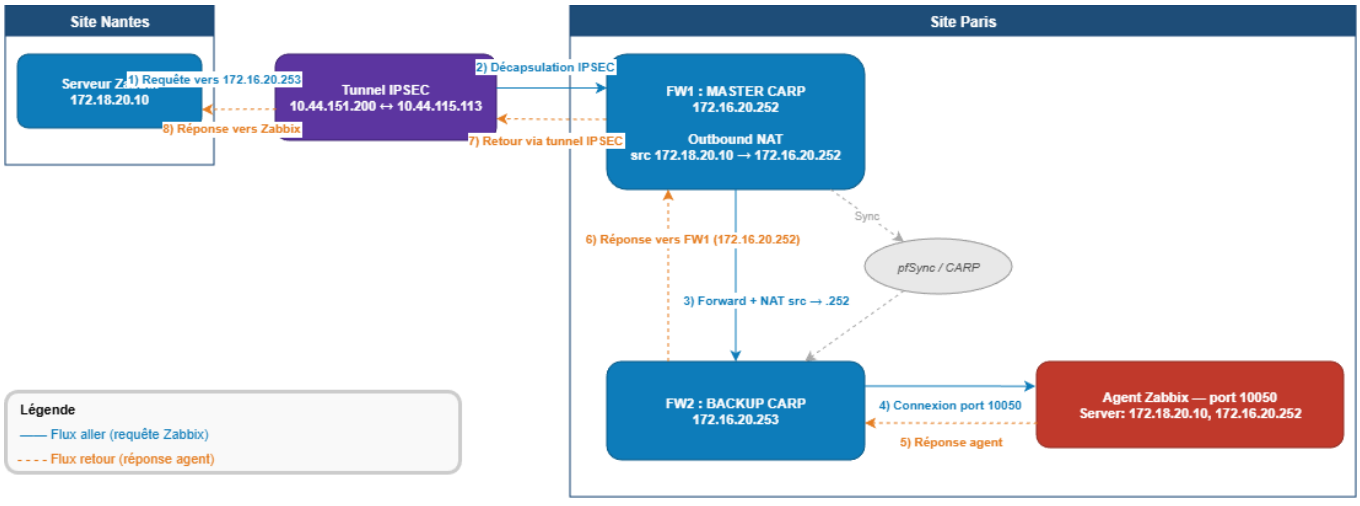
Outbound NAT sur FW1

Depuis Firewall > NAT > Outbound, passer en mode Hybrid puis ajouter la règle suivante :

Champ	Valeur
Interface	ADMIN
Address Family	IPv4
Protocol	Any
Source	NET_NAN (172.18.20.0/24)
Destination	`172.16.20.253/32`
Translation - Address	ADMIN address (172.16.20.252)

Cette règle masque l'IP source de Nantes (172.18.20.10) par l'IP physique de FW1 (172.16.20.252) lorsque le trafic est destiné à FW2. Ainsi, FW2 répond à FW1 qui retransmet via le tunnel IPSEC.

Schéma du flux après Outbound NAT



Attention ! Cette règle NAT n'affecte que le trafic de Nantes vers 172.16.20.253/32. Tout le reste du trafic inter-sites n'est pas impacté.

Configuration de l'agent Zabbix sur FW2

Après le NAT, FW2 reçoit les connexions avec l'IP source 172.16.20.252 (FW1) au lieu de 172.18.20.10 (Nantes). L'agent Zabbix refuse alors la connexion car FW1 n'est pas dans sa liste de serveurs autorisés.

Modifier le fichier de configuration de l'agent via Diagnostics > Edit File sur FW2 :

Fichier :

`/usr/local/etc/zabbix7/zabbix_agentd.conf`

Modifier la ligne Server :

`Server=172.18.20.10,172.16.20.252`

Laisser ServerActive inchangé :

`ServerActive=172.18.20.10`

Redémarrer l'agent depuis Status > Services > zabbix_agentd.

Vérification

Depuis le serveur Zabbix (172.18.20.10), tester la connectivité avec l'agent :

```
zabbix_get -s 172.16.20.253 -p 10050 -k agent.ping
```

Résultat attendu : 1

> Si le résultat est '1', la supervision est opérationnelle. FW2 devrait passer au vert dans l'interface Zabbix dans les minutes suivantes.

6.7 Supervision Switch HP

Configuration sur le switch HP

Configurer l'adresse IP du switch

```
# Configurer l'adresse IP du switch sur le vlan admin
configure
vlan 20
ip address 172.16.20.210 255.255.255.0
exit
ip default-gateway 172.16.20.254

# Vérifier la communication
ping 172.16.20.1

# Sauvegarder
write memory
```

Connectez-vous en console ou SSH sur le switch :

```
# Activer le community (secret) SNMP en lecture
snmp-server community "SECRET" Operator

# Définir le serveur Zabbix
snmp-server host 172.18.20.10 "SECRET"

# Vérifier la configuration
show snmp-server

# Vérifier la communication
ping 172.18.20.10

# Sauvegarder
write memory
```

Ajouter le switch dans Zabbix

Dans l'interface Zabbix, aller sur Collecte de données → Hôtes → Créer un hôte.

Champ	Valeur
Nom d'hôte	Nom du switch HP
Groupes	Switchs
Interface	SNMP, IP du switchs, Port 161
Version SNMP	SNMPv2
Communauté SNMP	{$SNMP_COMMUNITY}
Templates	HP Entreprise by SNMP

7. Vérification

7.1 Vérification des services

```
# Statut des services principaux
systemctl status zabbix-server zabbix-agent2 nginx mariadb

# Logs en temps réel
journalctl -u zabbix-server -f

# Valider la configuration sans redémarrer
zabbix_server -c /etc/zabbix/zabbix_server.conf -T
```

7.2 Test de collecte depuis le serveur

```
apt install -y zabbix-get

# Tester un agent local (VLAN 20)
zabbix_get -s 172.18.20.X  -p 10050 -k 'system.uptime'

# Tester un agent distant (site IPsec)
zabbix_get -s [IP-distante] -p 10050 -k 'system.uptime'

# Tester la charge CPU
zabbix_get -s [IP] -p 10050 -k 'system.cpu.load[all,avg1]'

# Lister les interfaces réseau
zabbix_get -s [IP] -p 10050 -k 'net.if.list'
```

Résultat attendu
La commande retourne une valeur numérique (ex : 12345 pour l'uptime en secondes). Un échec sur un agent distant indique un problème de tunnel IPsec ou de politique de sécurité, pas de Zabbix lui-même.

7.3 Vérification dans l'interface web

- Surveillance → Hôtes : tous les hôtes affichent l'icône ZBX verte
- Surveillance → Dernières données : valeurs collectées récentes pour chaque hôte

7.4 Consultation des journaux

```
# Zabbix Server / Agent2
tail -f /var/log/zabbix/zabbix_server.log
tail -f /var/log/zabbix/zabbix_agent2.log

# Nginx
tail -f /var/log/nginx/error.log
```

8. Améliorations

Voici quelques améliorations possibles pour ce projet :

- Utiliser un Zabbix proxy sur un site distant.
- Interface graphique remplacé par Grafana.
- Chiffrement des communications des agents Zabbix.
- Configurer des alertes par mail.
- Utiliser la fonction Maps de Zabbix pour avoir une vue visuelle de l'infrastructure.
- Utilisez un Vault comme HashiCorp ou CyberArk

9. Conclusion

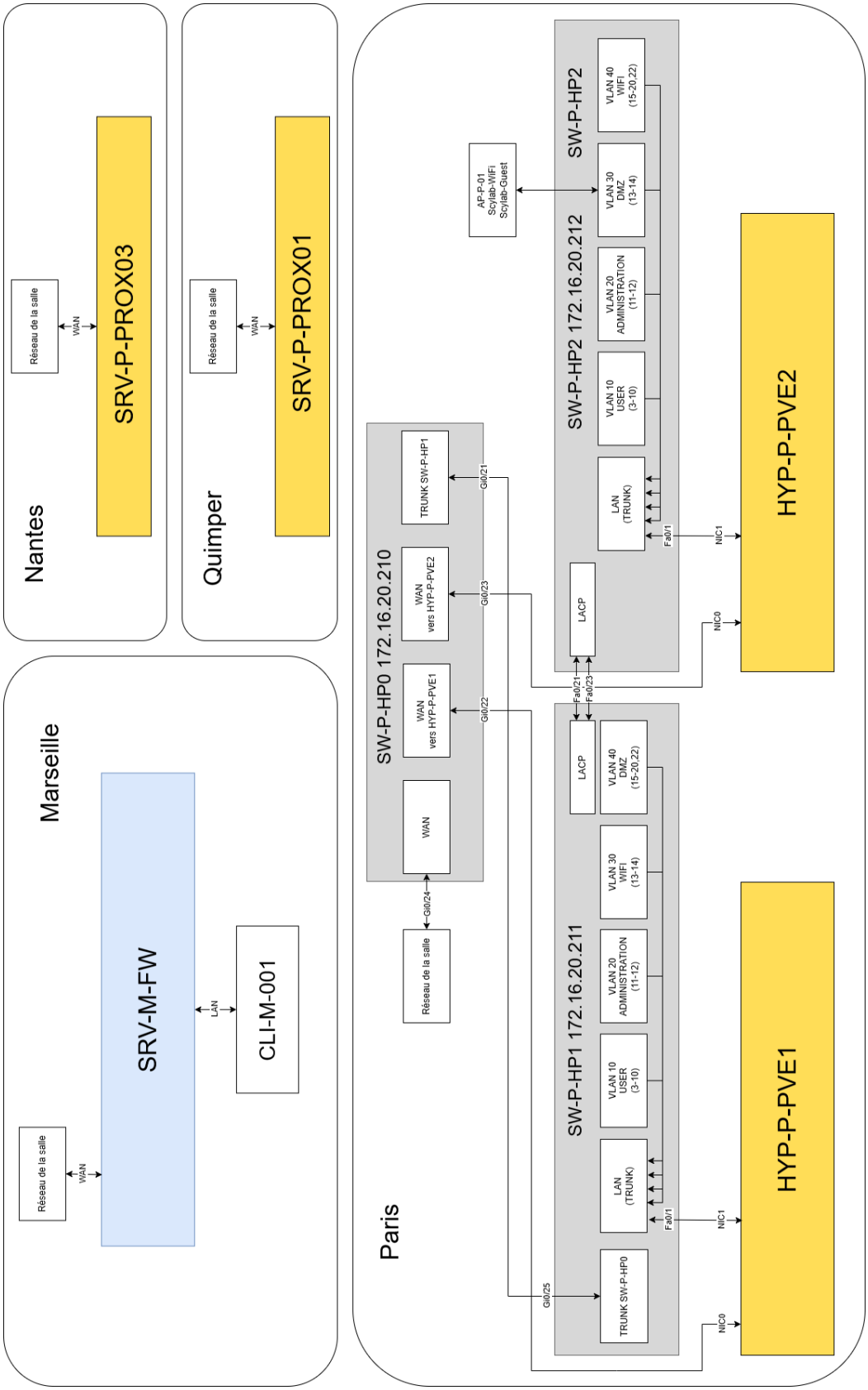
Ce projet m'a apporté énormément, aussi bien sur le plan de l'administration système que sur celui des réseaux. Il a nécessité une réflexion approfondie pour s'adapter à l'infrastructure existante, notamment avec la gestion du CARP ou encore les configurations des switches qui ont dû être revues et adaptées en conséquence.

Au-delà de quelque souci rencontré qui sont à présent corrigé due aux règles de pare-feu ou de configuration d'équipement à adapter, je n'ai pas eu de problème avec la solution en elle-même. Je la trouve complète et même presque prête à l'emploi grâce aux modèles déjà configurés et certains scripts intégrés sur l'interface Web, comme ping ou traceroute, seul l'interface WEB pourrait être à revoir.

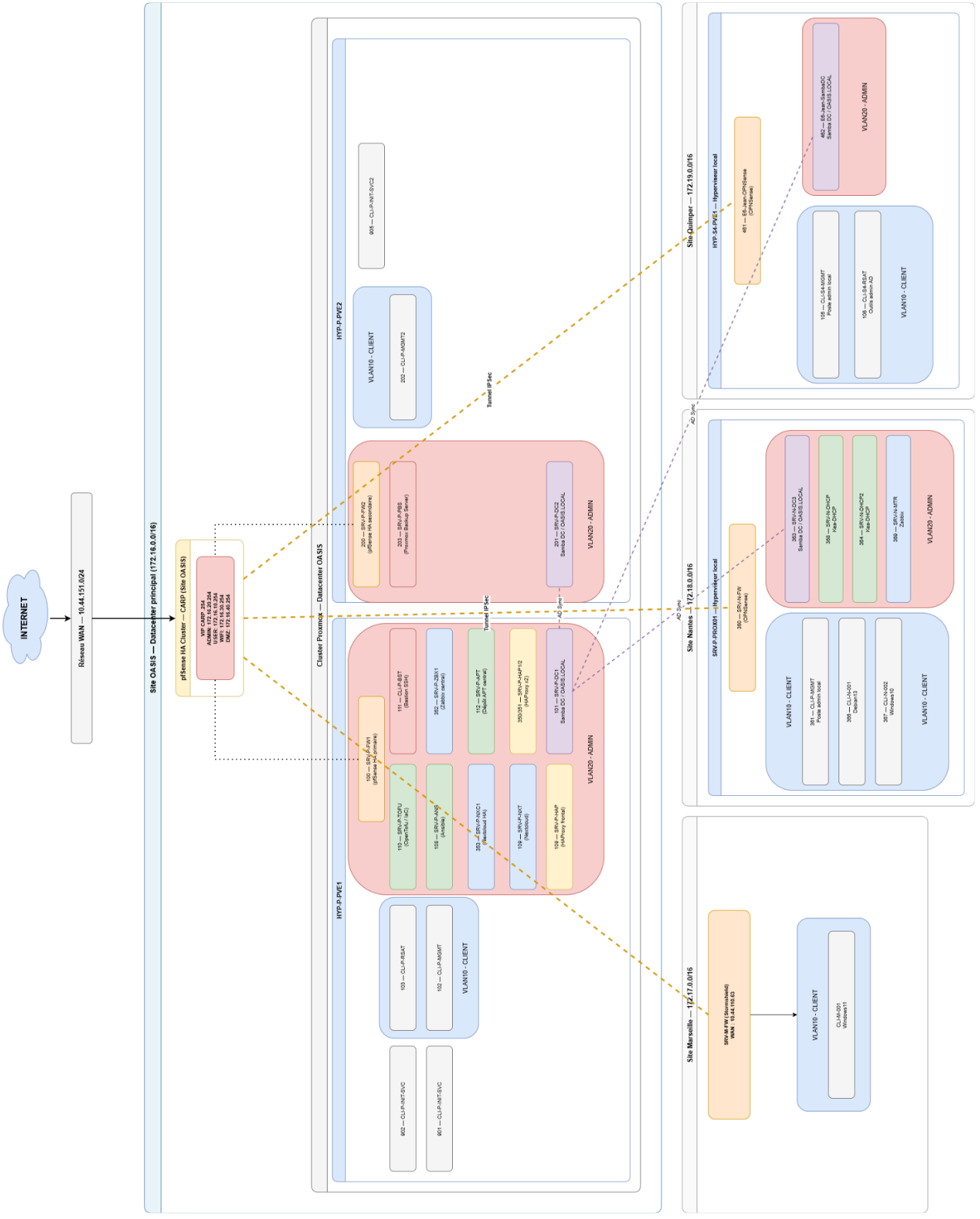
Je suis satisfait d'avoir pu déployer un service qui représente, selon moi, une composante essentielle de toute infrastructure professionnelle. La supervision permet en effet de détecter une panne au plus tôt et d'obtenir des informations précises sur sa nature, ce qui est indispensable pour garantir la continuité de service.

10. Annexes

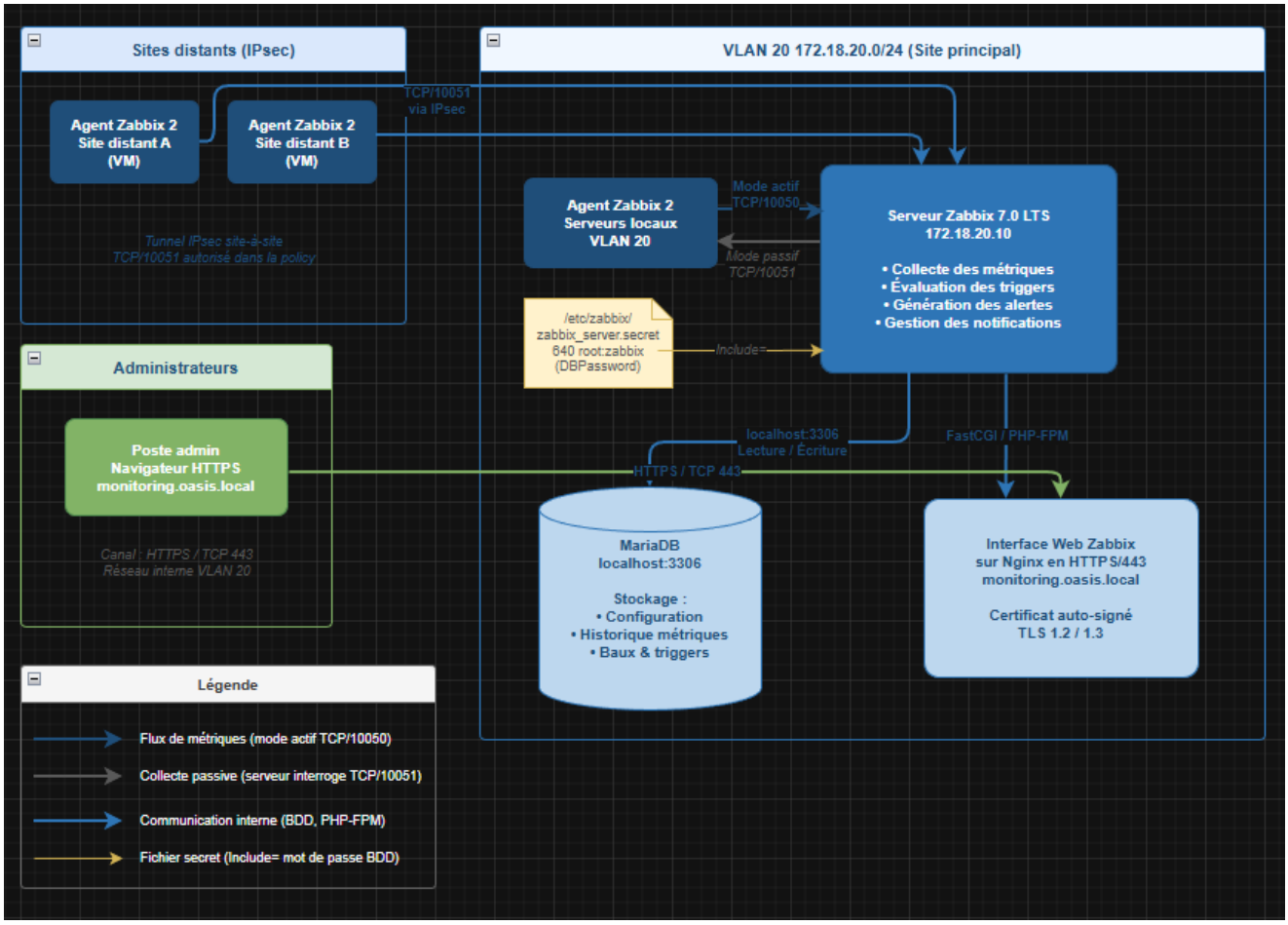
10.1 Schéma physique



10.2 Schéma logique



10.3 Schéma de flux de supervision



10.4 Référence des commandes de diagnostic

```
# Services
systemctl status zabbix-server
systemctl restart zabbix-server
systemctl reload nginx
zabbix_server -c /etc/zabbix/zabbix_server.conf -T

# Agent
zabbix_agent2 -t system.uptime
zabbix_get -s [IP] -p 10050 -k [clé]

# Base de données
mysql -u adm_zabbix -p -e 'SELECT COUNT(*) FROM zabbix.hosts;'

# Certificat
openssl x509 -in /etc/nginx/ssl/zabbix.crt -noout -dates

# Nginx
nginx -t

# SNMP - Tester la connectivité avec un switch
snmpwalk -v2c -c TEST 172.16.20.210

# SNMP - Récupérer le nom du switch
```

```
snmpget -v2c -c TEST 172.16.20.210 sysName.0

# SNMP - Lister toutes les interfaces du switch
snmpwalk -v2c -c TEST 172.16.20.210 ifDescr

# SNMP - État des interfaces (1=up, 2=down)
snmpwalk -v2c -c TEST 172.16.20.210 ifOperStatus

# SNMP - Trafic entrant par interface
snmpwalk -v2c -c TEST 172.16.20.210 ifInOctets

# SNMP - Trafic sortant par interface
snmpwalk -v2c -c TEST 172.16.20.210 ifOutOctets

# SNMP - Vérifier la version SNMP supportée par le switch
snmpget -v2c -c TEST 172.16.20.210 sysDescr.0

# Logs Zabbix en temps réel
tail -f /var/log/zabbix/zabbix_server.log

# Vérifier les erreurs SNMP dans les logs
grep -i snmp /var/log/zabbix/zabbix_server.log

# Tester la connectivité UDP 161 vers un switch
nmap -sU -p 161 172.16.20.210
```

10.5 Fichiers de configuration importants

Fichier / Répertoire	Rôle
/etc/zabbix/zabbix_server.conf	Configuration principale du serveur (paramètres en début de fichier)
/etc/zabbix/zabbix_server.secret	Mot de passe BDD (fichier secret séparé)
/etc/zabbix/zabbix_agent2.conf	Configuration de l'agent
/etc/nginx/conf.d/zabbix.conf	Configuration Nginx / HTTPS
/etc/nginx/ssl/	Certificat auto-signé (crt + key)
/var/log/zabbix/	Journaux Zabbix Server et Agent

10.6 Tableau des ports réseau

Service	Port	Protocole	Direction	Scope
Nginx HTTPS	443	TCP	Entrant	Admins → Serveur Zabbix (172.18.20.10)
Zabbix Agent2	10051	TCP	Entrant	Mode actif : l'agent envoie les données au serveur
Zabbix Serveur	10050	TCP	Sortant	Mode passif : le serveur interroge l'agent
MariaDB	3306	TCP	Local	Localhost uniquement