Fuentes - Mise en place d'une infrastructure de supervision

> SIS 67 — Service Départemental d'Incendie et de Secours du Bas-Rhin

> **Période** : Janvier-Février 2026 — Stage de 2ème année

> **Réalisation** : Projet collectif — Alternant réseau, pilote architecture, Alessandro Fuentes, alternant applicatif.

> **Solution** : Zabbix 7.4 (Server + Proxy) sur Ubuntu 22.04 LTS

> ⚠️ *Pour des raisons de confidentialité, certains éléments réseau ont été rendus génériques.*

1. Contexte et problématique

Qu'est-ce que Zabbix ?

Zabbix est une solution de supervision et de monitoring **open-source de classe entreprise**, conçue pour surveiller en temps réel la disponibilité et les performances des infrastructures informatiques : serveurs, équipements réseau, machines virtuelles, services cloud, imprimantes, caméras IP, etc.

Son fonctionnement repose sur trois piliers :

1. **Collecte de données** — via des agents installés sur les machines supervisées, ou via des protocoles sans agent comme SNMP pour les équipements réseau.
2. **Traitement et stockage** — le serveur analyse les données reçues, les compare à des seuils définis (Triggers/Déclencheurs) et stocke l'historique en base de données MySQL.
3. **Visualisation et alerting** — tableaux de bord personnalisables, cartes d'état, envoi d'alertes par email selon des règles de criticité.

Composants déployés dans ce projet :

- **Zabbix Server** — le cœur du système. Il orchestre la collecte, évalue les déclencheurs et génère les alertes. Hébergé au siège du SIS 67 sur le VLAN

de supervision dédié.

- **Zabbix Proxy** — composant intermédiaire hébergé sur le VLAN passerelle. Il collecte les données des équipements des sites distants (casernes) et les transmet au serveur central. Cela évite des traversées WAN répétées pour chaque élément collecté, réduit la charge sur le serveur principal et sécurise les flux réseau.

Situation au SIS 67 avant le projet

Le SIS 67 gère une infrastructure informatique répartie sur plusieurs dizaines de sites dans le Bas-Rhin : casernes, centre de traitement des appels (CTA), états-majors et sites distants. Cette infrastructure est administrée par le département informatique interne (GSIC).

Problème identifié : il n'existait aucune supervision centralisée sans erreurs. Les pannes n'étaient détectées que par remontée des utilisateurs, sans aucune visibilité proactive sur certains équipements sur la disponibilité ou les performances du SI. Dans un organisme de secours où la continuité de service est critique, ce manque de visibilité juste représentait un risque opérationnel réel.

Besoin exprimé : déployer une solution open-source, évolutive et maintenable, capable de superviser plusieurs centaines d'équipements répartis sur tout le département, de détecter les incidents proactivement et d'alerter les équipes concernées avec un niveau de criticité défini.

2. Objectifs du projet

- Déployer un serveur Zabbix central pour la supervision unifiée du SI
- Déployer un Zabbix Proxy pour la collecte distante (sites hors siège)
- Superviser les serveurs Linux et Windows via Zabbix Agent 2
- Superviser les équipements réseau (switches, firewalls) via SNMP
- Mettre en place un système d'alertes email structuré, routé par équipe et par criticité
- Créer des tableaux de bord adaptés à chaque profil (opérateurs, techniciens réseau/système, DSI)

- Créer une carte géolocalisée interactive pour visualiser l'état en temps réel de toutes les casernes
- Chiffrer toutes les communications (PSK) entre agents, proxy et serveur
- Documenter l'ensemble pour assurer la maintenabilité après le stage

3. Environnement technique

> ⚠️ *Les valeurs réseau ci-dessous sont issues de la documentation interne et ont été rendues génériques pour la publication. L'architecture réelle est plus complexe.*

Élément	Détail
Hyperviseur	VMware — cluster de production
OS serveurs	Ubuntu 22.04 LTS
Solution de supervision	Zabbix 7.4 (Server + Proxy + Agent 2)
Base de données	MySQL
Firewalls	Firewalls
Protocoles de collecte	Zabbix Agent 2, SNMP v2c, ICMP (ping)
Chiffrement	PSK (Pre-Shared Key) entre agents, proxy et serveur
Synchronisation temps	NTP — fuseau Europe/Paris
Serveur Zabbix	VLAN de supervision dédié — Ubuntu 22.04 LTS — 2 vCPU / 8 Go RAM / 150 Go
Proxy Zabbix	VLAN passerelle inter-sites — Ubuntu 22.04 LTS — même dimensionnement
Équipements supervisés	Plusieurs centaines d'hôtes (serveurs, switches, PC, imprimantes, caméras…)

4. Mon rôle et ma contribution personnelle

> **Projet collectif** — L'alternant réseau a piloté l'architecture globale et la supervision SNMP des équipements. L'alternant applicatif a développé la

> carte interactive via l'API Zabbix. Ma contribution s'est concentrée sur la **partie système et infrastructure**.

Mes contributions personnelles :

- Installation et configuration partiels de Zabbix Server et du Zabbix Proxy.
- Création des deux VMs sur le cluster (déploiement depuis modèle Ubuntu 22.04 LTS, configuration Netplan, coordination avec l'administrateur réseau pour l'ouverture des flux firewall)
- Création des groupes d'hôtes et intégration des hôtes supervisés dans l'interface
- Configuration des comptes utilisateurs, groupes et droits dans Zabbix
- Mise en place du système d'alertes email (actions de déclencheur, routage par équipe et criticité)
- Création des tableaux de bord (Global View, Nexsis,...)
- Rédaction de la documentation technique complète pour la passation

5. Infrastructure virtuelle (VMware)

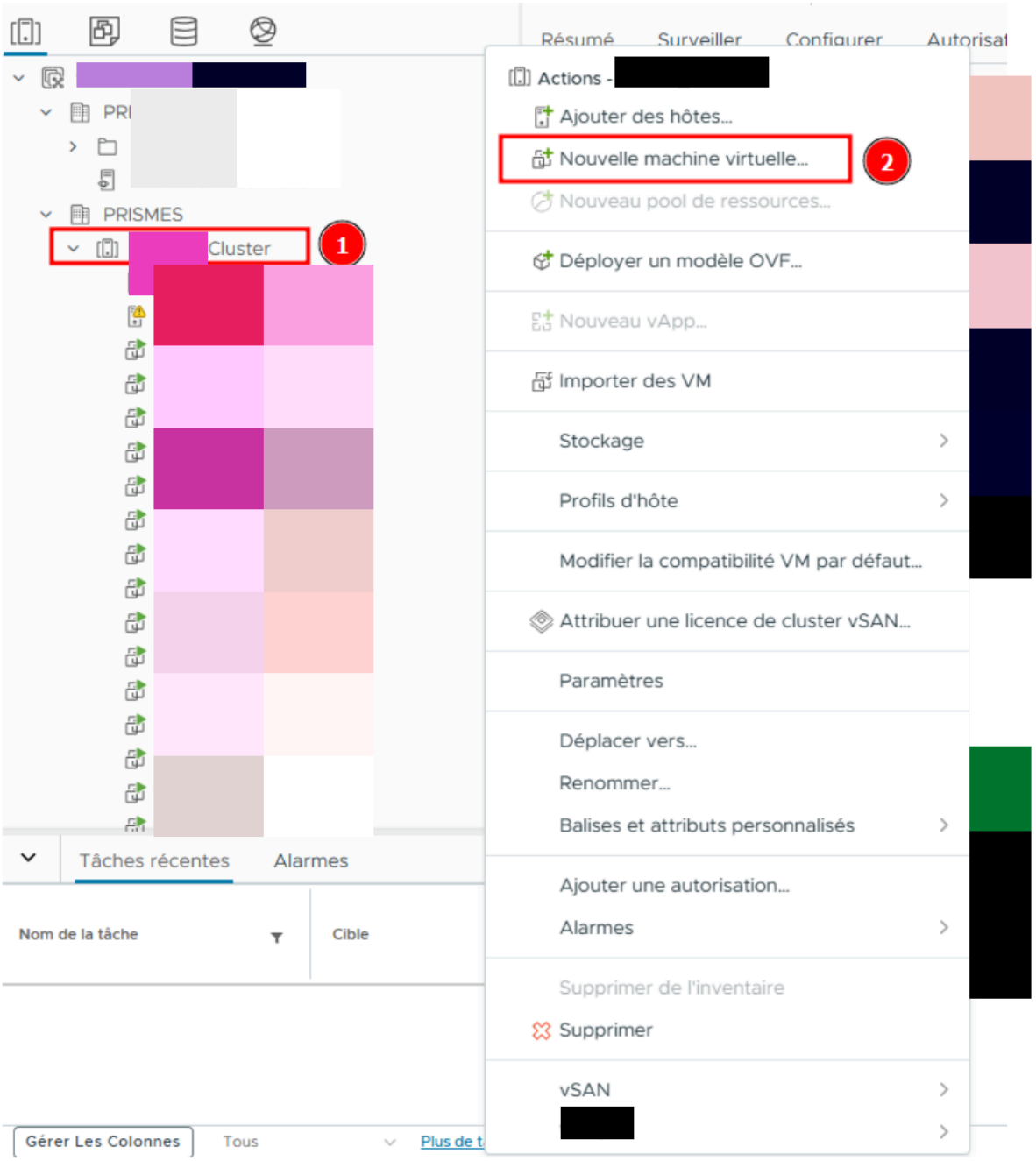
5.1 Localisation dans l'infrastructure

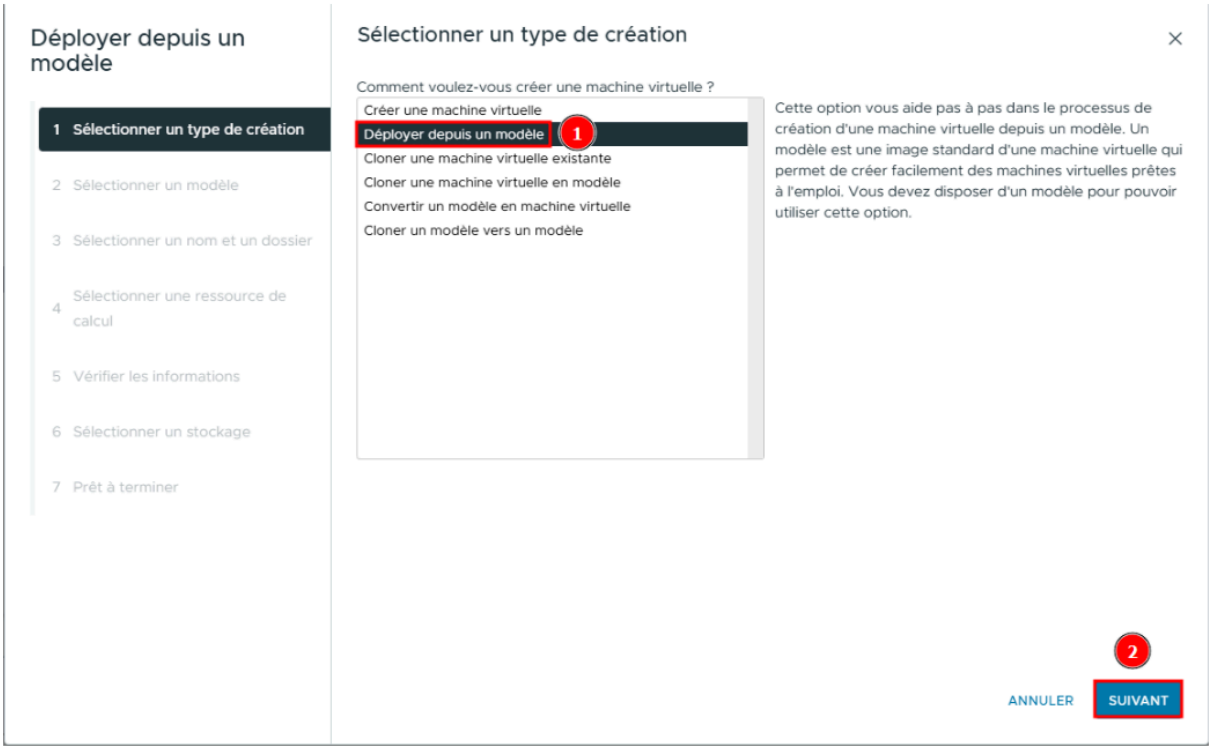
Les deux VMs Zabbix sont hébergées sur le **cluster de production** du SIS 67. L'accès nécessite une autorisation préalable auprès de l'administrateur réseau.

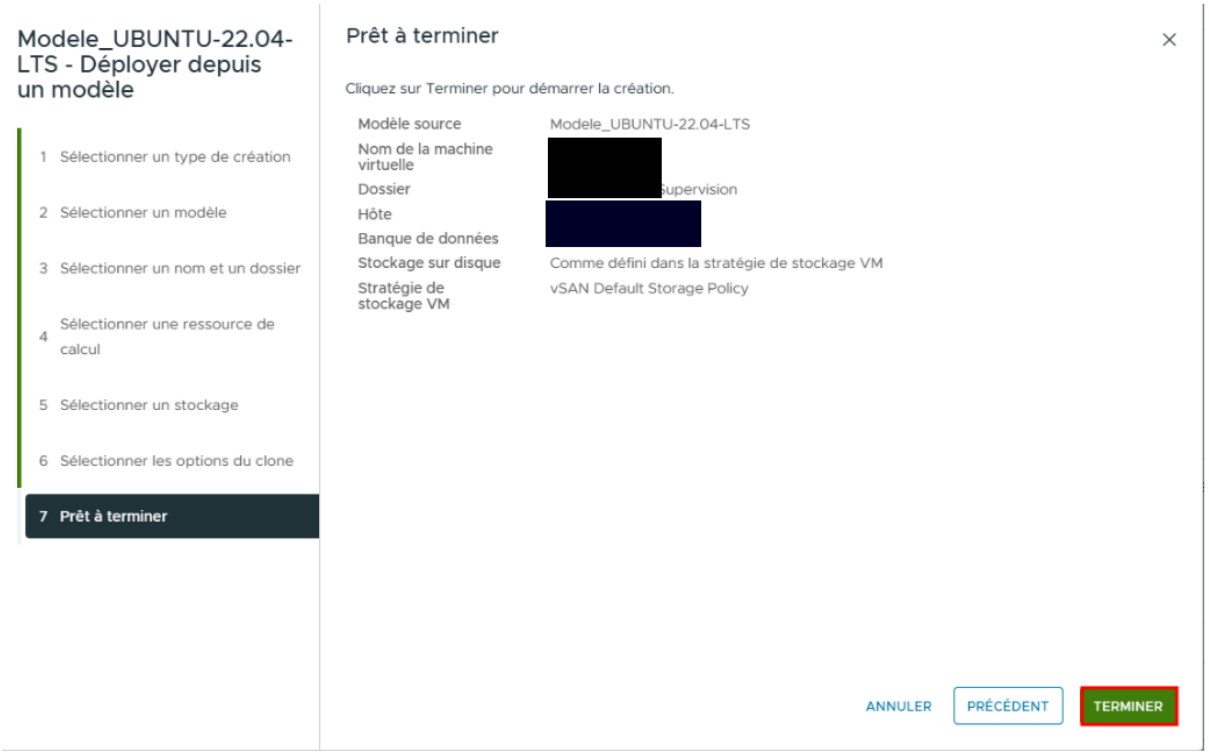
Procédure de création (identique pour le Server et le Proxy) :

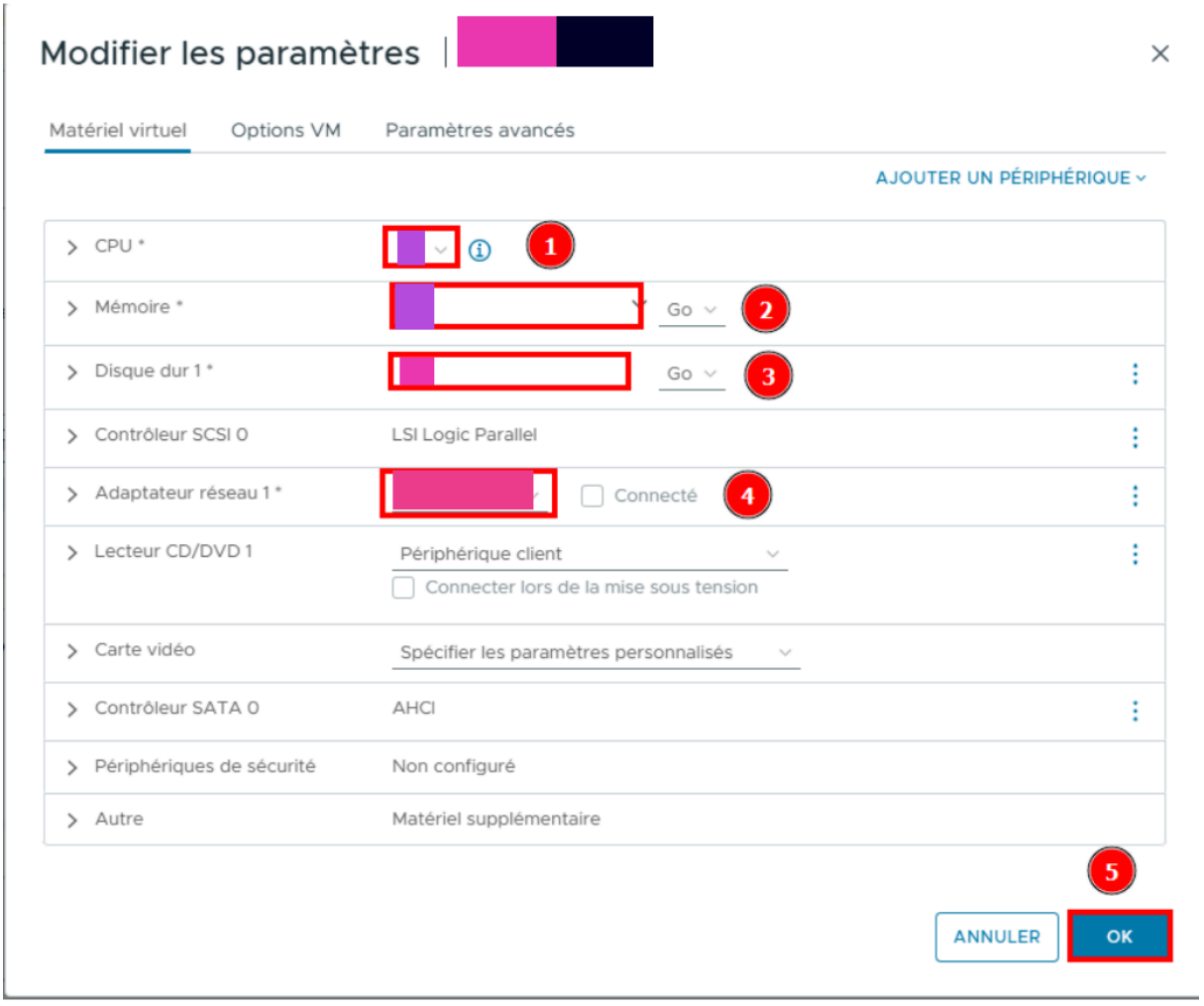
1. Dans vSphere, clic droit sur le cluster `Cluster` → *Nouvelle machine virtuelle*
2. Sélectionner **Déployer depuis un modèle**
3. Naviguer dans l'arborescence : `PRISMES → MODELES → LINUX` → sélectionner `Modele_UBUNTU-22.04-LTS`
4. Nommer la VM et la placer dans le dossier `Administration-Supervision`
5. Sélectionner un hôte de calcul (nœud du cluster)
6. Sélectionner la banque de données `Datastore`
7. Ne cocher **aucune** option de personnalisation du clone
8. Valider et terminer

Images de démonstration en exemple :




Déployer depuis un modèle
1 Sélectionner un type de création
2 Sélectionner un modèle
3 Sélectionner un nom et un dossier
4 Sélectionner une ressource de calcul
5 Vérifier les informations
6 Sélectionner un stockage
7 Prêt à terminer
Sélectionner un type de création
Comment voulez-vous créer une machine virtuelle ?
Créer une machine virtuelle
Déployer depuis un modèle
1
Cloner une machine virtuelle existante
Cloner une machine virtuelle en modèle
Convertir un modèle en machine virtuelle
Cloner un modèle vers un modèle
Cette option vous aide pas à pas dans le processus de création d'une machine virtuelle depuis un modèle. Un modèle est une image standard d'une machine virtuelle qui permet de créer facilement des machines virtuelles prêtes à l'emploi. Vous devez disposer d'un modèle pour pouvoir utiliser cette option.
2
ANNULER
SUIVANT


Modele_UBUNTU-22.04-LTS - Déployer depuis un modèle
1 Sélectionner un type de création
2 Sélectionner un modèle
3 Sélectionner un nom et un dossier
4 Sélectionner une ressource de calcul
5 Sélectionner un stockage
6 Sélectionner les options du clone
7 Prêt à terminer
Prêt à terminer
Cliquez sur Terminer pour démarrer la création.
Modèle source
Modele_UBUNTU-22.04-LTS
Nom de la machine virtuelle
Dossier
Supervision
Hôte
Banque de données
Stockage sur disque
Comme défini dans la stratégie de stockage VM
Stratégie de stockage VM
vSAN Default Storage Policy
ANNULER
PRÉCÉDENT
TERMINER



5.2 Configuration réseau et système

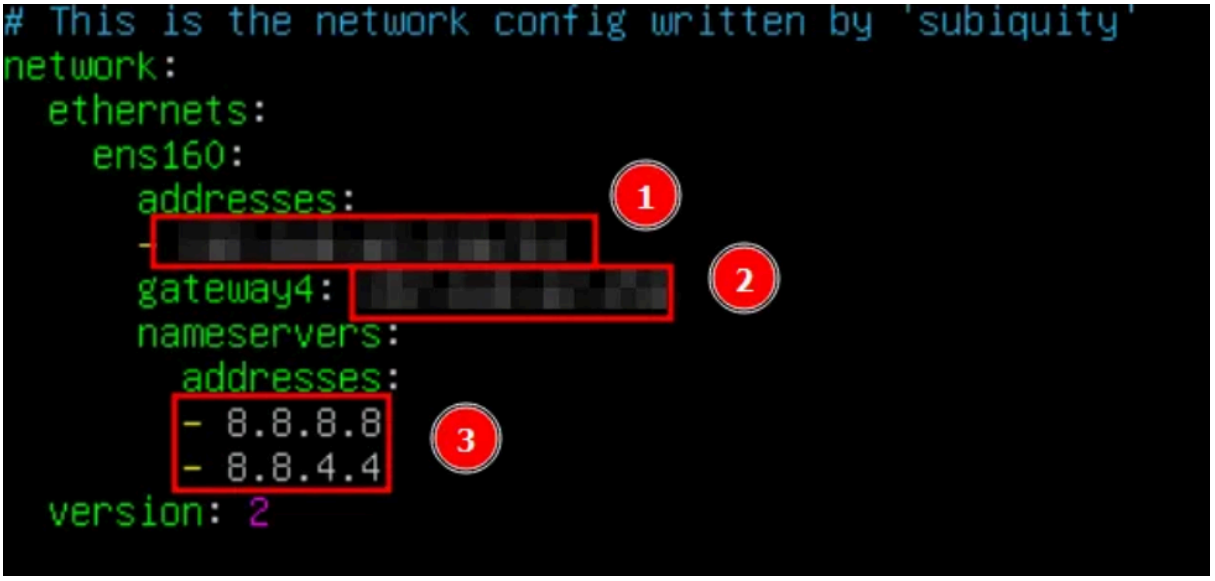
Depuis la console web vSphere, configurer l'IP statique via Netplan :

```
nano /etc/netplan/00-installer-config.yaml
```

```
network:
  version: 2
  ethernets:
    ens160:
      addresses:
        - <adresse_IP>/<masque>
      gateway4: <passerelle>
      nameservers:
```

```
        addresses: [8.8.8.8, 8.8.4.4]
      dhcp4: false
```

```
sudo netplan apply
# Vérifier la connectivité
ping google.com
sudo apt update && apt upgrade
```



Activer SSH pour la gestion à distance :

```
sudo apt install openssh-server
# Connexion depuis un poste : ssh <user>@<ip_vm>
```

Création des comptes Linux (principe du moindre privilège) :

```
# Compte de consultation sans privilèges
sudo useradd -m -k /etc/skel -s /bin/bash user
sudo passwd user

# Compte technique avec droits sudo restreints
sudo useradd -m -k /etc/skel -s /bin/bash admin
sudo passwd adminsys
sudo visudo -f /etc/sudoers.d/admin
```

Contenu du fichier sudoers restreint :

```
Defaults:adminsys !rootpw, logfile="/var/log/sudo.log"
adminsys ALL=(ALL:ALL) /usr/bin/systemctl, \
  /usr/bin/journalctl, \
  /usr/bin/apt, /usr/bin/apt-get, /usr/bin/dpkg, \
  /usr/bin/useradd, /usr/bin/usermod, \
  /usr/bin/ufw, /usr/bin/reboot, /usr/bin/shutdown, \
  /usr/bin/ls, /usr/bin/cat, /usr/bin/less, \
  /usr/bin/nano, /usr/bin/vim
```

```
sudo chmod 440 /etc/sudoers.d/admin
```

> L'accès Internet des VMs est autorisé temporairement pour les installations, puis révoqué. Ces serveurs ne doivent pas être exposés sur le réseau public.

6. Installation de Zabbix

6.1 Zabbix Server

```
# Ajout du dépôt officiel Zabbix 7.4
wget https://repo.zabbix.com/zabbix/7.4/release/ubuntu/poo
l/main/z/zabbix-release/zabbix-release_latest_7.4+ubuntu22.
04_all.deb
dpkg -i zabbix-release_latest_7.4+ubuntu22.04_all.deb
apt update

# Installation des paquets
apt install zabbix-server-mysql zabbix-frontend-php zabbix-
apache-conf zabbix-sql-scripts zabbix-agent2

# Paquets plugins optionnels (Agent 2)
apt install zabbix-agent2-plugin-mongodb zabbix-agent2-plug
in-mssql zabbix-agent2-plugin-postgresql
```

Base de données MySQL :

```
sudo apt install mysql-server
mysql_secure_installation

sudo mysql -uroot -p
```

```
CREATE DATABASE zabbixdb CHARACTER SET utf8mb4 COLLATE utf8
mb4_bin;
CREATE USER 'zabbixuser'@'localhost' IDENTIFIED BY 'VOTRE_M
OT_DE_PASSE_DB';
GRANT ALL PRIVILEGES ON zabbixdb.* TO 'redeyeuser'@'localho
st';
SET GLOBAL log_bin_trust_function_creators = 1;
FLUSH PRIVILEGES;
QUIT;
```

```
# Import du schéma initial (opération longue — NE PAS INTER
ROMPRE)
zcat /usr/share/zabbix/sql-scripts/mysql/server.sql.gz | my
sql --default-character-set=utf8mb4 -uredeyeuser -p redeyed
b

# Désactiver l'option activée pour l'import
mysql -uroot -p
# set global log_bin_trust_function_creators = 0; quit;
```

Configuration de `zabbix_server.conf` :

```
nano /etc/zabbix/zabbix_server.conf
# Paramètres à modifier :
# DBName=zabbixdb
# DBUser=zabbixuser
# DBPassword=<mot_de_passe>
# EnableGlobalScripts=1
```

Locale française + démarrage des services :

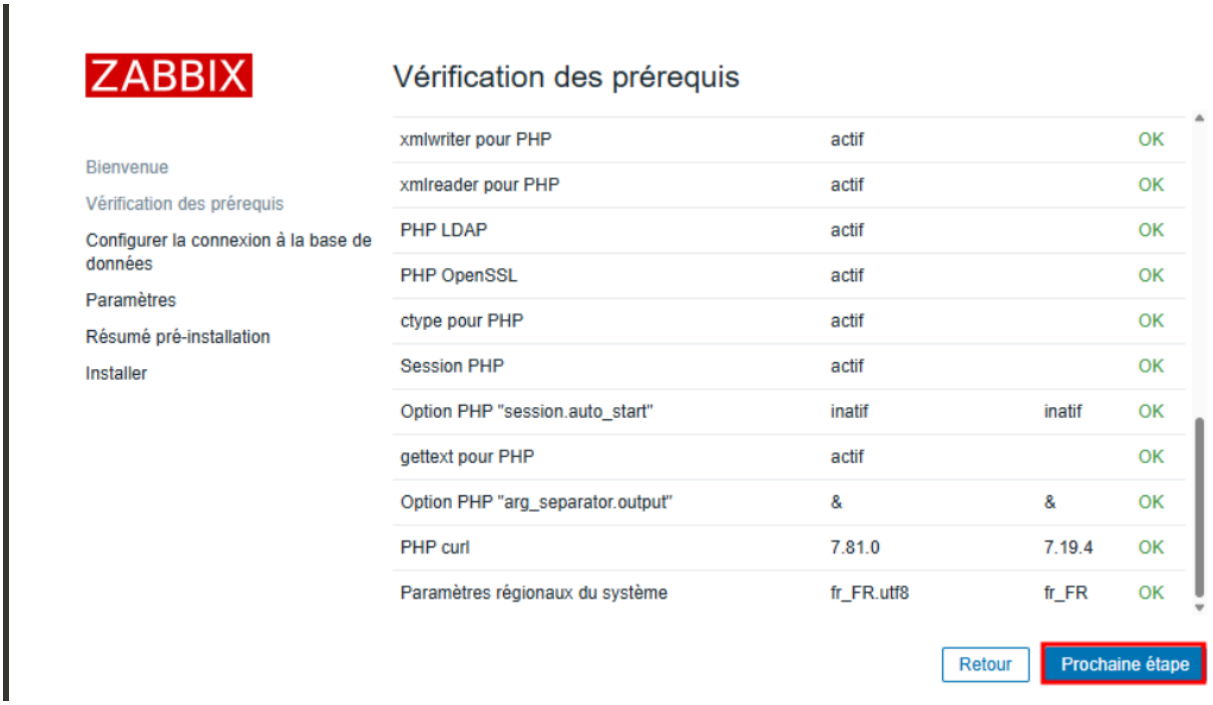
```
sudo apt install language-pack-fr
sudo locale-gen fr_FR.UTF-8
sudo update-locale LANG=fr_FR.UTF-8

systemctl restart zabbix-server zabbix-agent2 apache2
systemctl enable zabbix-server zabbix-agent2 apache2
```

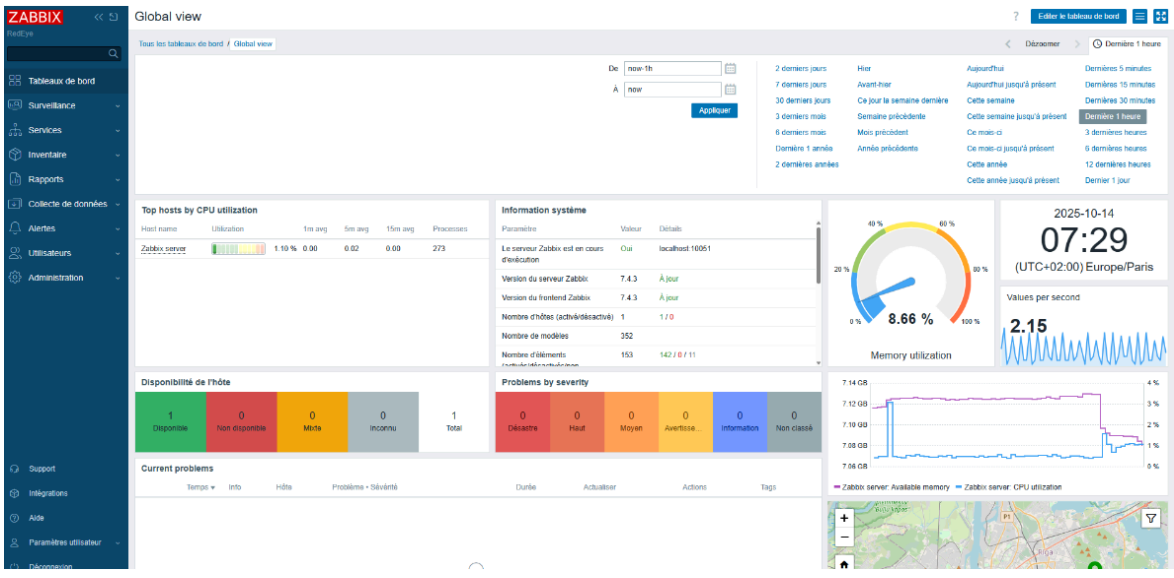
6.2 Initialisation de l'interface web

Accès via `http://<ip_serveur>/zabbix` :

1. Sélectionner la langue **Français (fr_FR)**
2. Vérifier que tous les prérequis PHP sont au statut **OK**
3. Renseigner les paramètres de connexion à la base de données
4. Définir le nom du serveur affiché dans l'interface
5. Valider — identifiants par défaut : **Admin / zabbix** (à changer immédiatement)




ZABBIX
1
Nom d'utilisateur
Admin
2
Mot de passe
••••••
Me rappeler toutes les 30 jours
3
S'enregistrer


ZABBIX
Global view
Tableaux de bord
Surveillance
Services
Inventaire
Rapports
Collecte de données
Alertes
Utilisateurs
Administration
Support
Intégrations
Aide
Paramètres utilisateur
Top hosts by CPU utilization
Information système
Disponibilité de l'hôte
Problems by severity
Current problems
8.66 %
Memory utilization
2025-10-14
07:29
(UTC+02:00) Europe/Paris
Values per second
2.15

6.3 Zabbix Proxy

Le proxy est installé sur une VM distincte pour collecter les données des sites distants sans traversée WAN répétée.

```
wget https://repo.zabbix.com/zabbix/7.4/release/ubuntu/poo
l/main/z/zabbix-release/zabbix-release_latest_7.4+ubuntu22.
04_all.deb
dpkg -i zabbix-release_latest_7.4+ubuntu22.04_all.deb
apt update
apt install zabbix-proxy-mysql zabbix-sql-scripts

sudo apt install mysql-server && mysql_secure_installation
mysql -uroot -p
```

```
CREATE DATABASE zabbixproxydb CHARACTER SET utf8mb4 COLLATE
utf8mb4_bin;
CREATE USER 'zabbixproxyuser'@'localhost' IDENTIFIED BY 'VO
TRE_MOT_DE_PASSE_DB';
GRANT ALL PRIVILEGES ON zabbixproxydb.* TO 'zabbixproxyuse
r'@'localhost';
SET GLOBAL log_bin_trust_function_creators = 1;
FLUSH PRIVILEGES; QUIT;
```

```
cat /usr/share/zabbix/sql-scripts/mysql/proxy.sql | mysql -
-default-character-set=utf8mb4 -uzabbix -p zabbix_proxy
```

Configuration de `zabbix_proxy.conf` :

```
nano /etc/zabbix/zabbix_proxy.conf
```

```
DBName=zabbixproxydb
DBUser=zabbixproxyuser
DBPassword=<motdepasse>
Server=<IP_du_serveur_Zabbix>
Hostname=zabbixProxy
ListenPort=10051
```

```
ProxyMode=0               # Mode actif : le proxy pousse les
données vers le serveur
ConfigFrequency=3600      # Synchronisation de la configurat
ion toutes les heures
DataSenderFrequency=5     # Envoi des données collectées tou
tes les 5 secondes
```

```
systemctl restart zabbix-proxy
systemctl enable zabbix-proxy
```

Déclarer le proxy dans l'interface Zabbix : Administration → Proxies → Créer un proxy → saisir le nom et le mode actif.

7. Configuration fonctionnelle

7.1 Groupes d'hôtes

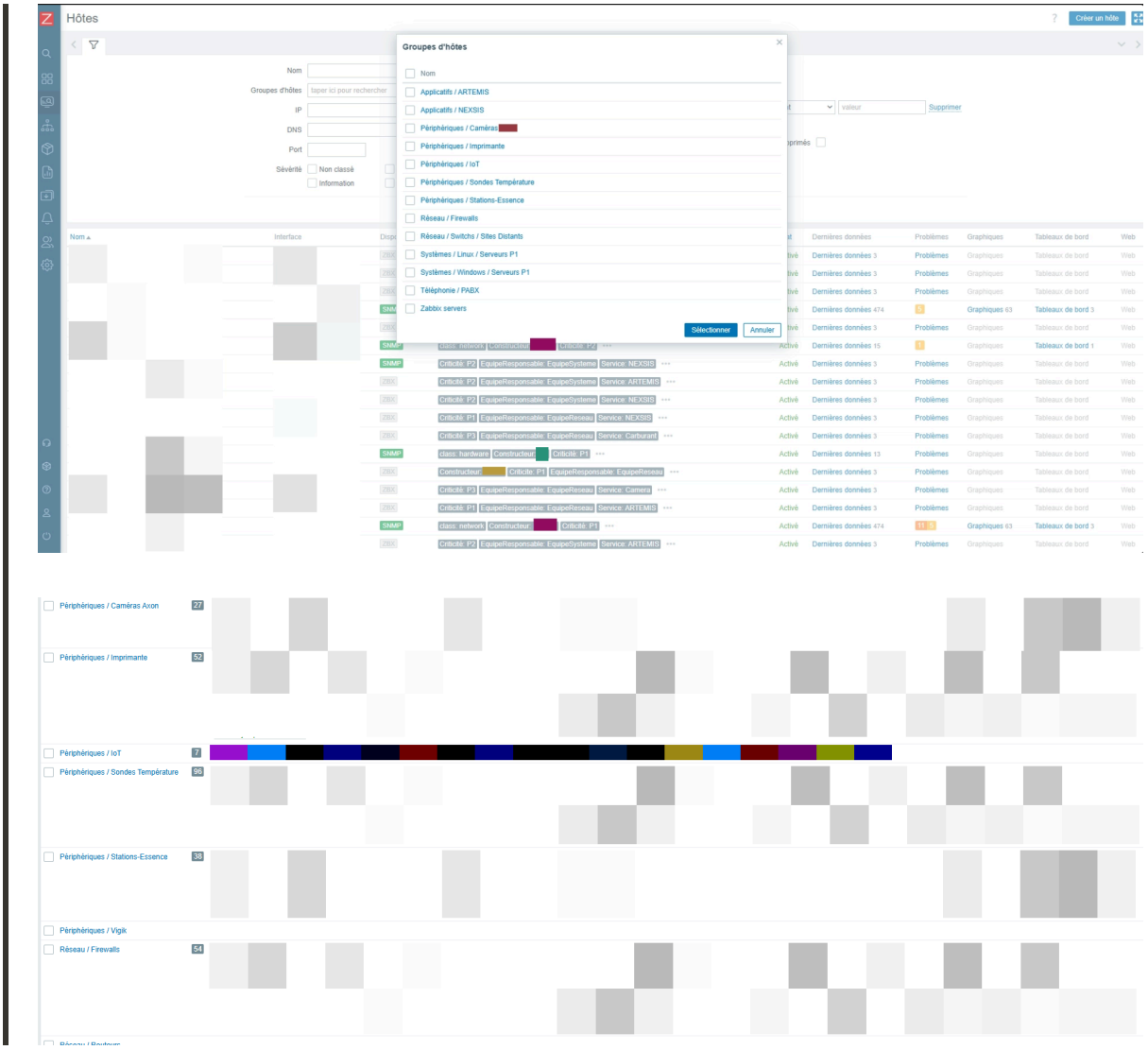
Les groupes d'hôtes permettent d'organiser le parc supervisé par catégorie, de filtrer les vues dans les dashboards et de router automatiquement les alertes vers la bonne équipe.

Chemin dans l'interface : Données → Hôtes → Groupes d'hôtes → Créer un groupe d'hôtes

Exemples de groupes créés *(nommage interne non publié)* :

Groupe	Contenu
Applications métier	Serveurs applicatifs internes
Périphériques / Imprimantes	Imprimantes réseau sur les sites
Périphériques / Caméras	Caméras IP sur les casernes
Réseau / Firewalls	Firewalls siège et sites
Réseau / Switchs / Sites distants	Switches sur les casernes
Systèmes / Linux / Serveurs critiques	Serveurs Linux de production
Systèmes / Windows / Serveurs critiques	Serveurs Windows de production

> **Capture de la liste des groupes d'hôtes dans l'interface Zabbix**



7.2 Ajout d'hôtes dans Zabbix

L'ajout d'un hôte dans Zabbix consiste à déclarer l'équipement dans l'interface et à lui associer un mode de collecte (agent ou SNMP).

Chemin : Données → Hôtes → Créer un hôte

Les champs principaux à renseigner :

Onglet Hôte :

- *Nom de l'hôte* : doit correspondre exactement au paramètre `Hostname` configuré dans l'agent sur la machine
- *Groupes* : rattacher au(x) groupe(s) approprié(s)
- *Interfaces* : définir le type de collecte (Agent Zabbix ou SNMP) et l'IP de l'équipement

- *Proxy* : sélectionner `zabbixproxy` pour les hôtes sur sites distants, laisser vide pour les hôtes locaux

Onglet Templates :

Appliquer un ou plusieurs templates selon le type d'équipement. Le template définit automatiquement tous les éléments collectés, les déclencheurs et les graphiques associés.

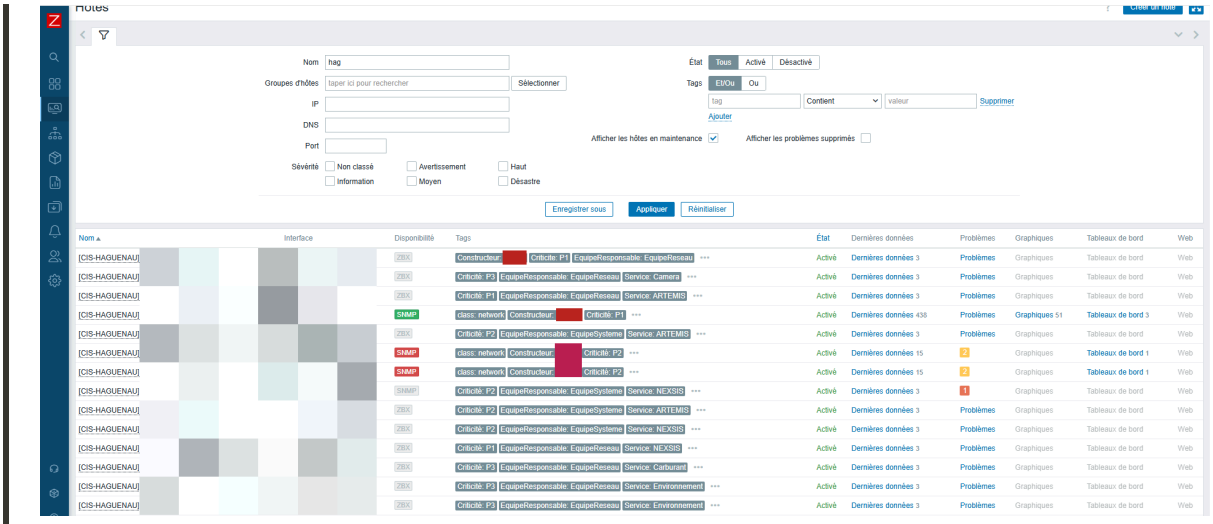
Exemples :

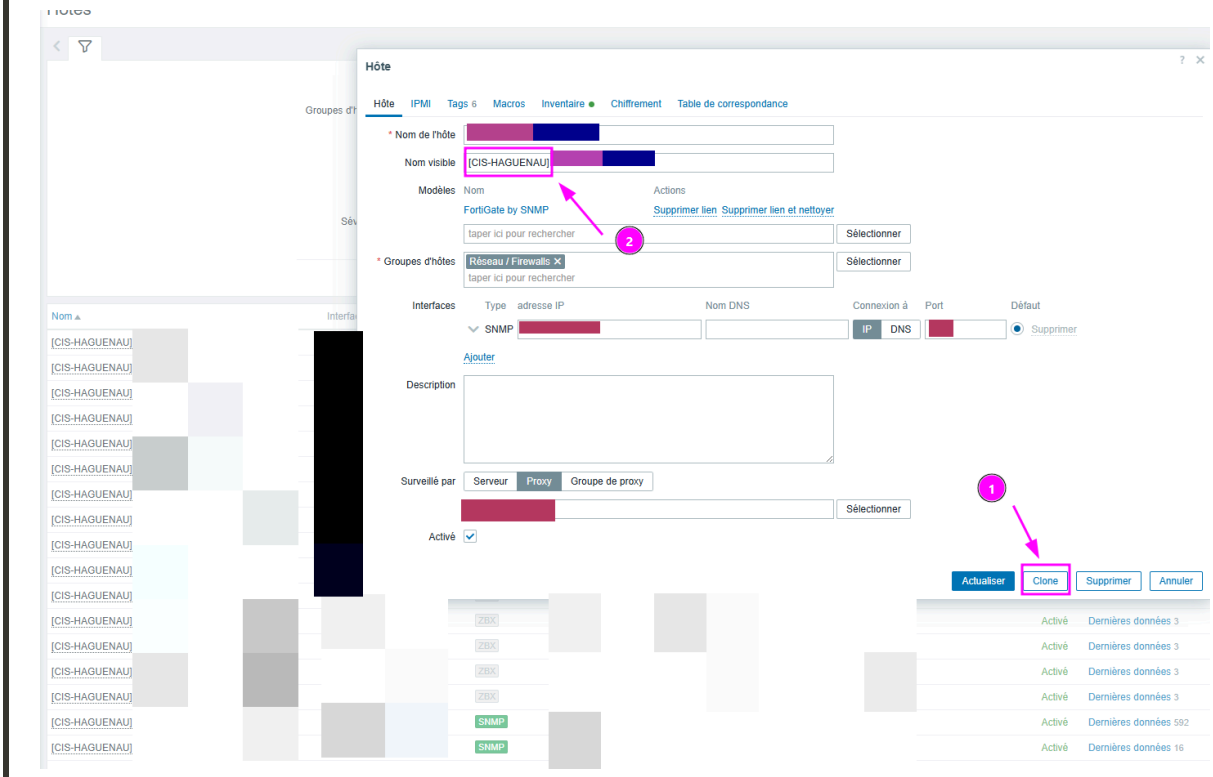
Type d'équipement	Template appliqué
Serveur Linux	`Linux by Zabbix Agent`
Serveur Windows	`Windows by Zabbix Agent`
Switch réseau	Template adapté au constructeur
Firewall	Template adapté au constructeur
Imprimante	`Printer by SNMP`

Onglet Tags :

Chaque hôte reçoit des tags structurés pour le filtrage et le routing des alertes :

Tag	Valeur exemple
`Constructeur`	Dell, Netgear, HP...
`Criticité`	P1, P2, P3
`EquipeResponsable`	EquipeReseau, EquipeSystème
`Service`	Firewall, ConnectivitéSite...
`Site`	*(nom de la caserne)*
`Type`	Switch, Serveur, Imprimante...




Hôte
Hôte
IPMI
Tags 6
Macros
Inventaire
Chiffrement
Table de correspondance
* Nom de l'hôte
Nom visible
[CIS-HAGUENAU]
Modèles
Nom
Actions
FortiGate by SNMP
Supprimer lien
Supprimer lien et nettoyer
taper ici pour rechercher
Sélectionner
* Groupes d'hôtes
Réseau / Firewalls
taper ici pour rechercher
Sélectionner
Interfaces
Type
adresse IP
Nom DNS
Connexion à
Port
Défaut
SNMP
IP
DNS
Supprimer
Ajouter
Description
Surveillé par
Serveur
Proxy
Groupe de proxy
Sélectionner
Activé
1
2
Actualiser
Clone
Supprimer
Annuler


Nouvel hôte
Hôte
IPMI
Tags 6
Macros
Inventaire
Chiffrement
Table de correspondance
Tags
Nom
Valeur
Constructeur
Criticité
P1
EquipeResponsable
EquipeReseau
Service
ConnectiviteSite
Site
CIS-HAGUENAU
Type
Firewall
Supprimer
Ajouter
Ajouter
Annuler

7.3 La supervision SNMP

Pourquoi SNMP pour les équipements réseau ?

Les switches et firewalls ne supportent pas l'installation d'un agent Zabbix. On utilise à la place le protocole **SNMP (Simple Network Management Protocol)**, qui permet d'interroger les équipements réseau à distance pour récupérer leurs métriques (charge CPU, utilisation des interfaces, table de routage, état des ports...).

SNMP repose sur une architecture **Manager / Agent** : Zabbix (ou son Proxy) joue le rôle de Manager et interroge l'agent SNMP intégré nativement dans l'équipement réseau.

Configuration côté Zabbix

Dans la fiche de l'hôte, onglet **Interfaces**, sélectionner le type **SNMP** :

- Adresse IP de l'équipement
- Port : **161** (UDP, port standard SNMP)
- Version SNMP : **v2c** pour la majorité des équipements

> ℹ️ La version SNMP v3 offre un chiffrement et une authentification renforcés mais nécessite une configuration plus complexe côté équipement. La version v2c, utilisée ici avec une community string dédiée, offre un bon compromis pour un environnement réseau interne maîtrisé.

Le template sélectionné (selon le constructeur) définit automatiquement les OIDs interrogés pour chaque métrique.

La collecte SNMP des équipements sur les **sites distants** est intégralement déléguée au **Proxy Zabbix**, ce qui évite que le serveur central traverse le WAN pour chaque item collecté.

7.4 Comptes utilisateurs et droits dans Zabbix

La gestion des accès à l'interface Zabbix repose sur un système de **groupes d'utilisateurs** liés à des **rôles** et à des **groupes d'hôtes**, conformément au principe du moindre privilège.

Chemin : Administration → Utilisateurs

Exemples de rôles disponibles :

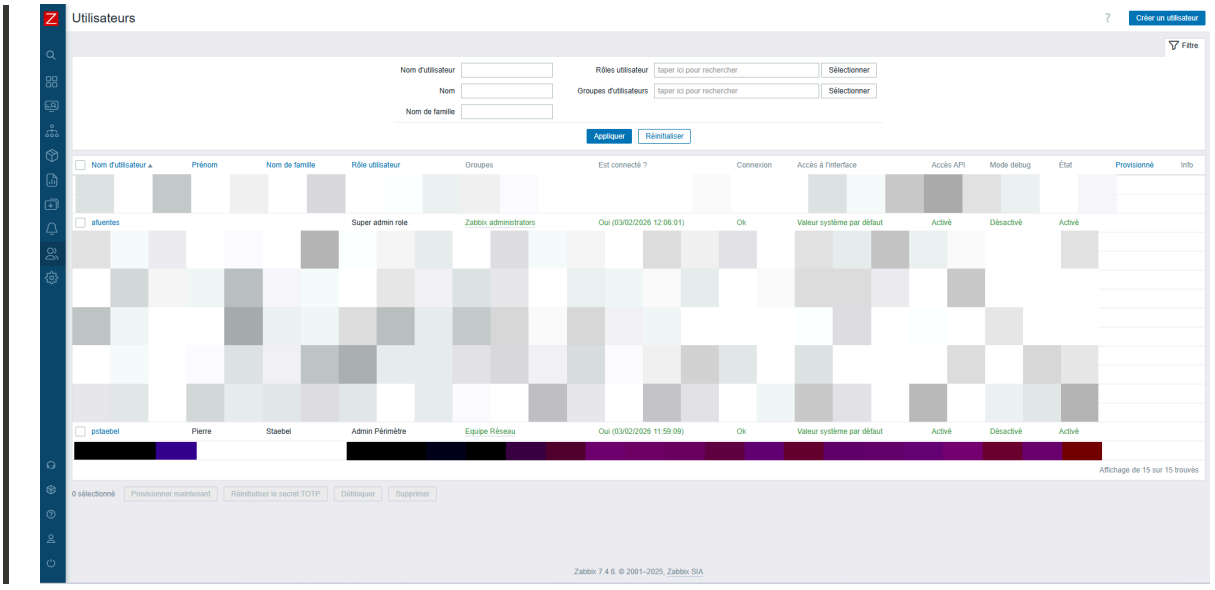
- **Super Admin** — accès complet à l'ensemble des paramètres, configuration globale
- **Admin** — peut gérer les hôtes, dashboards et alertes de son périmètre
- **Utilisateur (Readonly)** — consultation uniquement, aucune modification possible

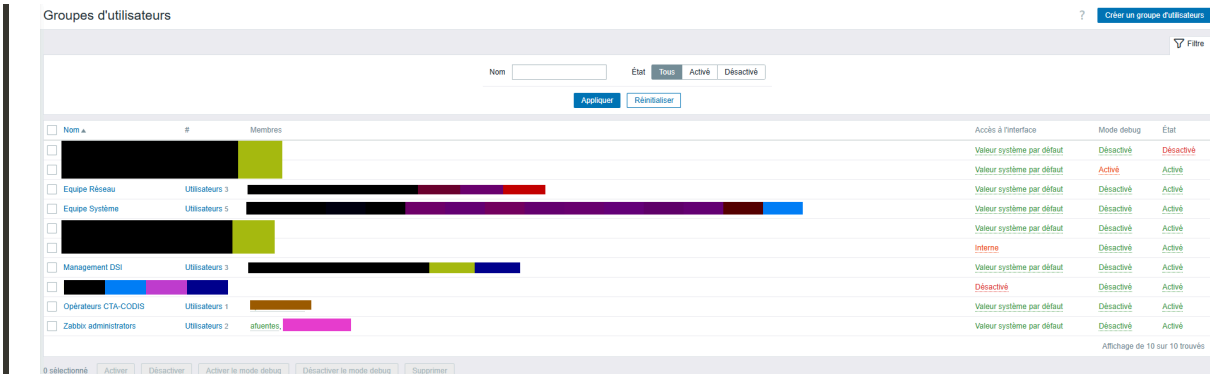
Groupes d'utilisateurs créés :

Groupe	Rôle Zabbix	Groupes d'hôtes visibles
Administrateurs DSI	Super Admin	Tous les hôtes
Équipe Réseau	Admin	Réseau / Firewalls, Réseau / Switchs
Équipe Système	Admin	Systèmes / Linux, Systèmes / Windows
Opérateurs terrain	Utilisateur (Readonly)	Vue carte + dashboards opérationnels

Créer un groupe d'utilisateurs : Administration → Groupes d'utilisateurs → Créer un groupe d'utilisateurs → définir le nom, les permissions sur les groupes d'hôtes, et le rôle.

Créer un utilisateur : Administration → Utilisateurs → Créer un utilisateur → renseigner le login, le groupe d'appartenance, et définir un mot de passe fort.





7.5 Système d'alertes

Principe de fonctionnement

Zabbix détecte les incidents via des **Déclencheurs (Triggers)** : chaque template définit des conditions d'alerte (ex. : "hôte injoignable depuis 5 minutes", "utilisation CPU > 90% pendant 10 minutes"). Lorsqu'un déclencheur passe à l'état PROBLEM, Zabbix exécute des **Actions** qui envoient des notifications.

Configuration du média email

Chemin : Administration → Types de médias → Email → configurer les paramètres SMTP vers le serveur Exchange interne.

Création des actions de déclencheur

Chemin : Alertes → Actions → Trigger actions → Créer une action

Chaque action définit :

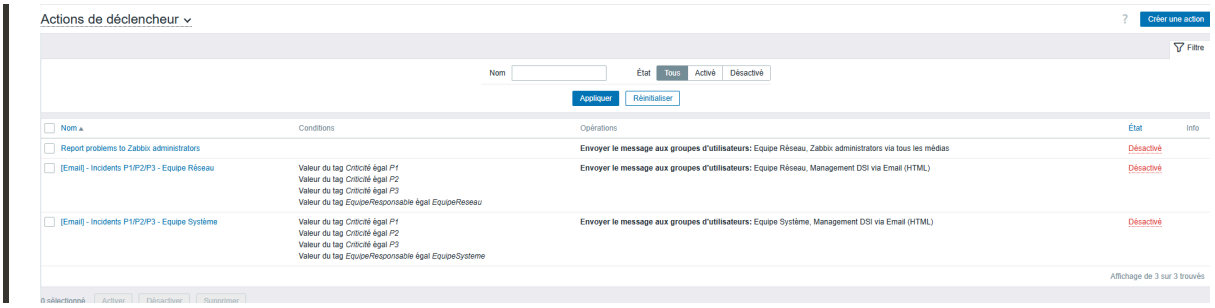
- **Conditions** : filtres sur le niveau de sévérité (Warning, Average, High, Disaster) et sur les tags de l'hôte concerné (ex. : `EquipeResponsable = EquipeReseau`)
- **Opérations** : qui notifier, via quel média, avec quel message

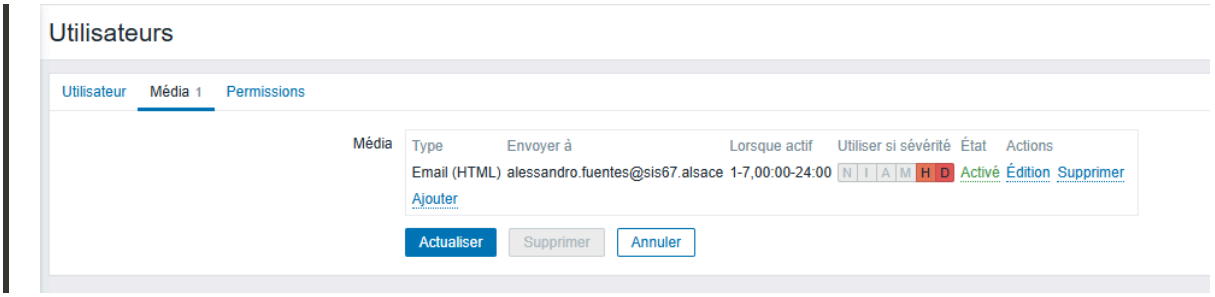
Trois actions créées, correspondant aux trois équipes :

Action	Filtre tag	Destinataires	Sévérités couvertes
Alertes Équipe Réseau	`EquipeResponsable = EquipeReseau`	Membres équipe réseau	High, Disaster (P1/P2)
Alertes Équipe Système	`EquipeResponsable = EquipeSystème`	Membres équipe système	High, Disaster (P1/P2)

Action	Filtre tag	Destinataires	Sévérités couvertes
Escalade DSI	Tous hôtes `Criticité = P1`	Responsables DSI	Disaster uniquement

Ce routage garantit que chaque équipe ne reçoit que les alertes de son périmètre, évitant les notifications intempestives.





7.6 Tableaux de bord (Dashboards)

Les dashboards Zabbix sont entièrement personnalisables et permettent d'afficher en temps réel les informations les plus pertinentes selon le profil de l'utilisateur. Chaque dashboard est composé de **widgets** (graphiques, compteurs, listes, cartes...) que l'on ajoute, redimensionne et configure individuellement.

Chemin : Tableaux de bord → Créer un tableau de bord

Dashboard Global View (DSI / Responsables)

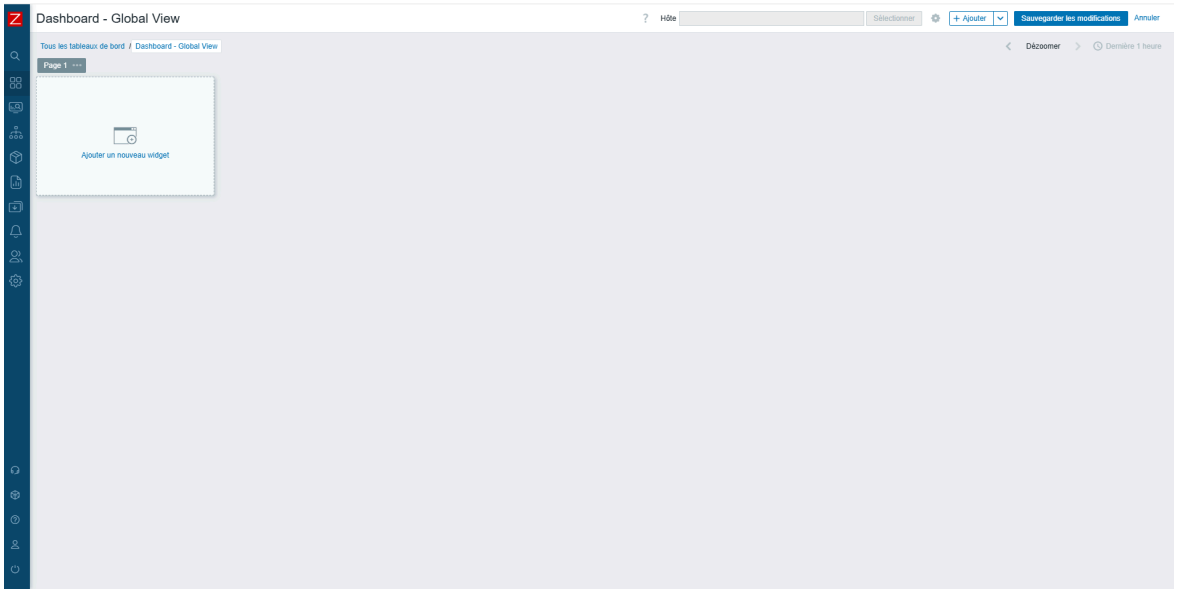
Destiné aux responsables et à la DSI, ce dashboard donne une vision synthétique de l'état global du SI.

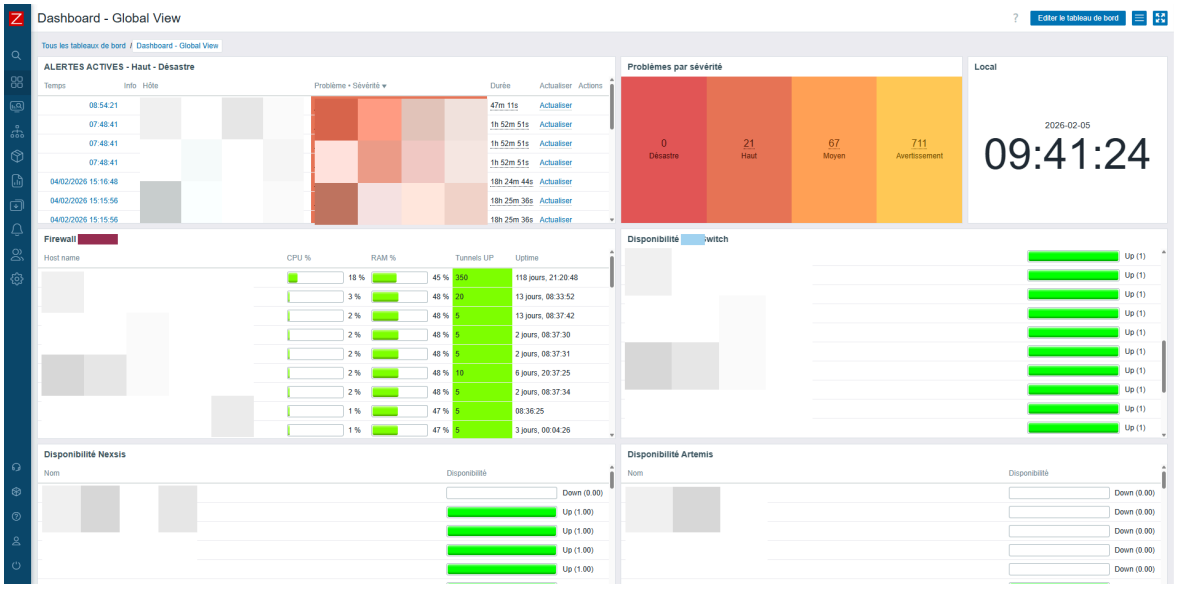
Widgets configurés :

- **Synthèse des problèmes** : liste des incidents actifs, triés par sévérité, avec le nom de l'équipement, la durée et la description

- **Disponibilité des hôtes** : compteur du nombre d'hôtes OK vs en problème vs inconnus
- **Top 10 hôtes par charge CPU** : graphique des serveurs les plus sollicités
- **Informations système Zabbix** : version du serveur, nombre d'hôtes supervisés, nombre d'éléments collectés, statut du serveur
- **Horloge** : affichage de l'heure locale (Europe/Paris) en temps réel
- **Memory utilization** : graphique de consommation mémoire du serveur Zabbix

Capture du dashboard Global View





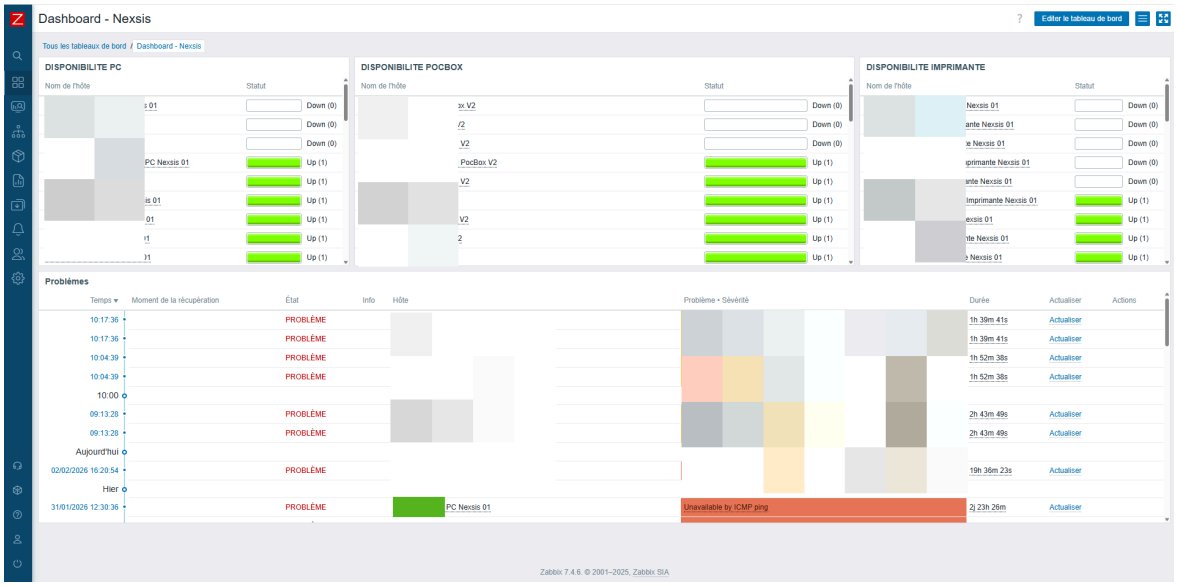
Dashboard Nexsis (Opérateurs terrain / CTA)

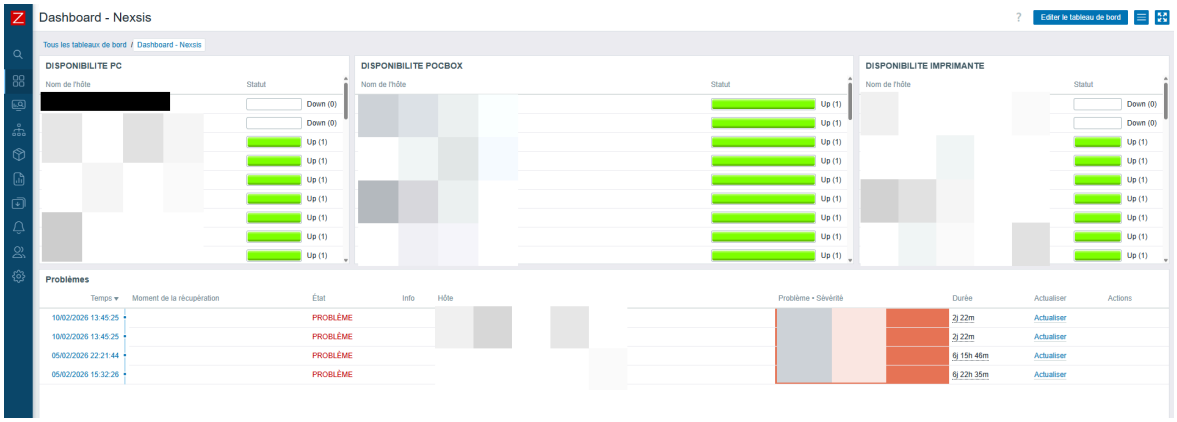
Conçu pour les opérateurs du Centre de Traitement des Appels, ce dashboard affiche l'état des équipements directement liés à l'infrastructure NexSIS (système de gestion des opérations de secours), déployée dans les casernes.

Widgets configurés :

- **État des PC Nexsis par caserne** : tableau de disponibilité des postes NexSIS site par site
- **État des POCBOX** : terminaux spécifiques Nexsis
- **État des imprimantes Nexsis** : disponibilité des imprimantes associées au système
- **Incidents actifs filtrés Nexsis** : liste des problèmes actifs uniquement sur les équipements Nexsis

Capture du dashboard Nexsis





Dashboard Firewalls / Réseau

Destiné à l'équipe réseau, ce dashboard donne une vue consolidée de l'état des firewalls et de la connectivité des sites.

Widgets configurés :

- **État des firewalls** : disponibilité de chacun (siège + sites distants)
- **Connectivité WAN des sites** : état des liens réseau vers chaque caserne
- **Topologie réseau** : vue par caserne avec état de chaque équipement réseau
- **Trafic interfaces** : graphiques de charge sur les interfaces WAN critiques

7.7 Carte interactive géolocalisée

> **Cette section décrit une réalisation réalisée à 100% par Jonas**, l'alternant applicatif du projet.

Présentation

Une **carte d'état géolocalisée** a été développée pour les opérateurs du CTA, permettant de visualiser en temps réel l'état de toutes les casernes du département Bas-Rhin sur fond de carte interactive.

Chaque caserne est représentée par un marqueur coloré dont la couleur évolue dynamiquement selon l'état des équipements supervisés sur ce site :

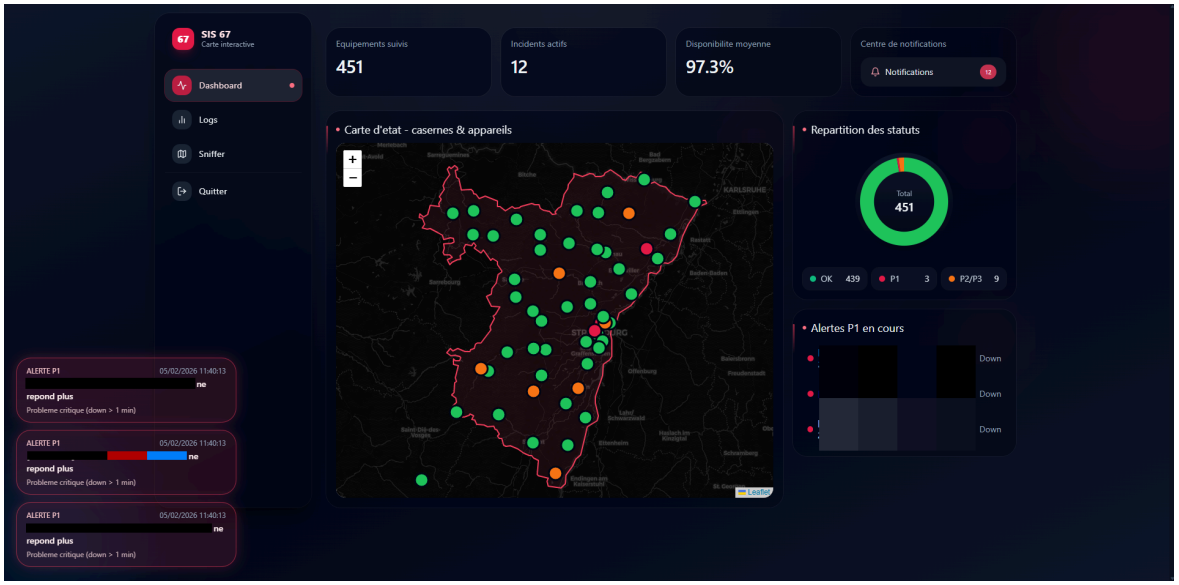
- 🟢 **Vert** : tous les équipements OK
- 🟠 **Orange** : au moins un problème non critique détecté
- 🔴 **Rouge** : au moins un incident critique actif

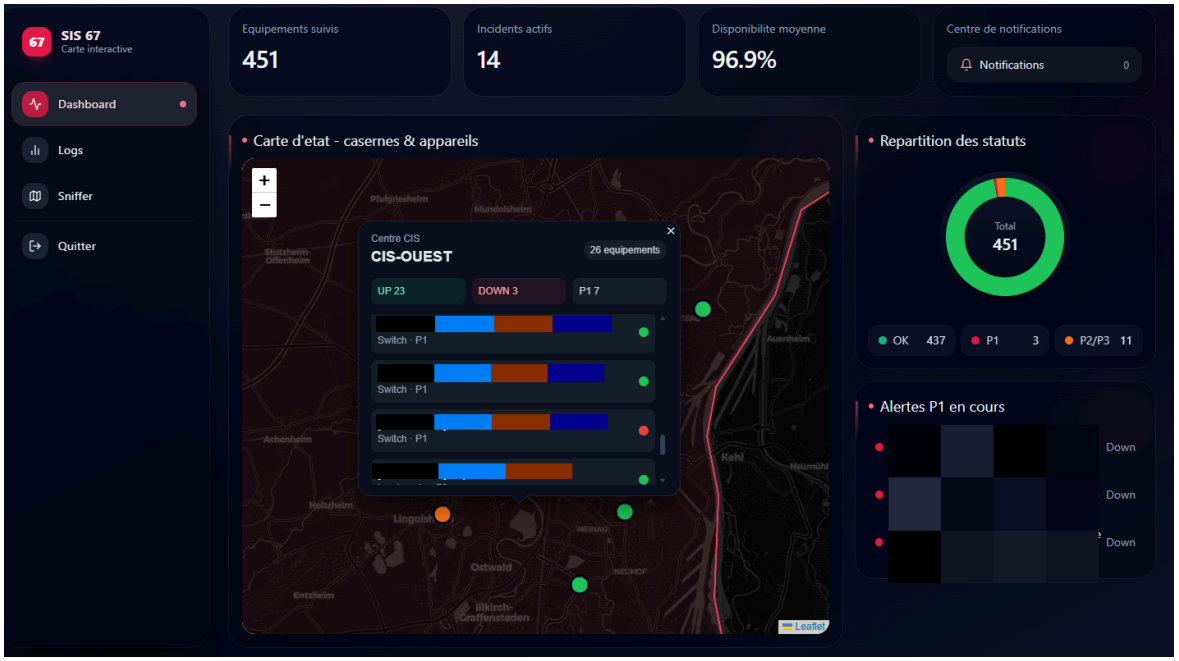
Fonctionnement technique

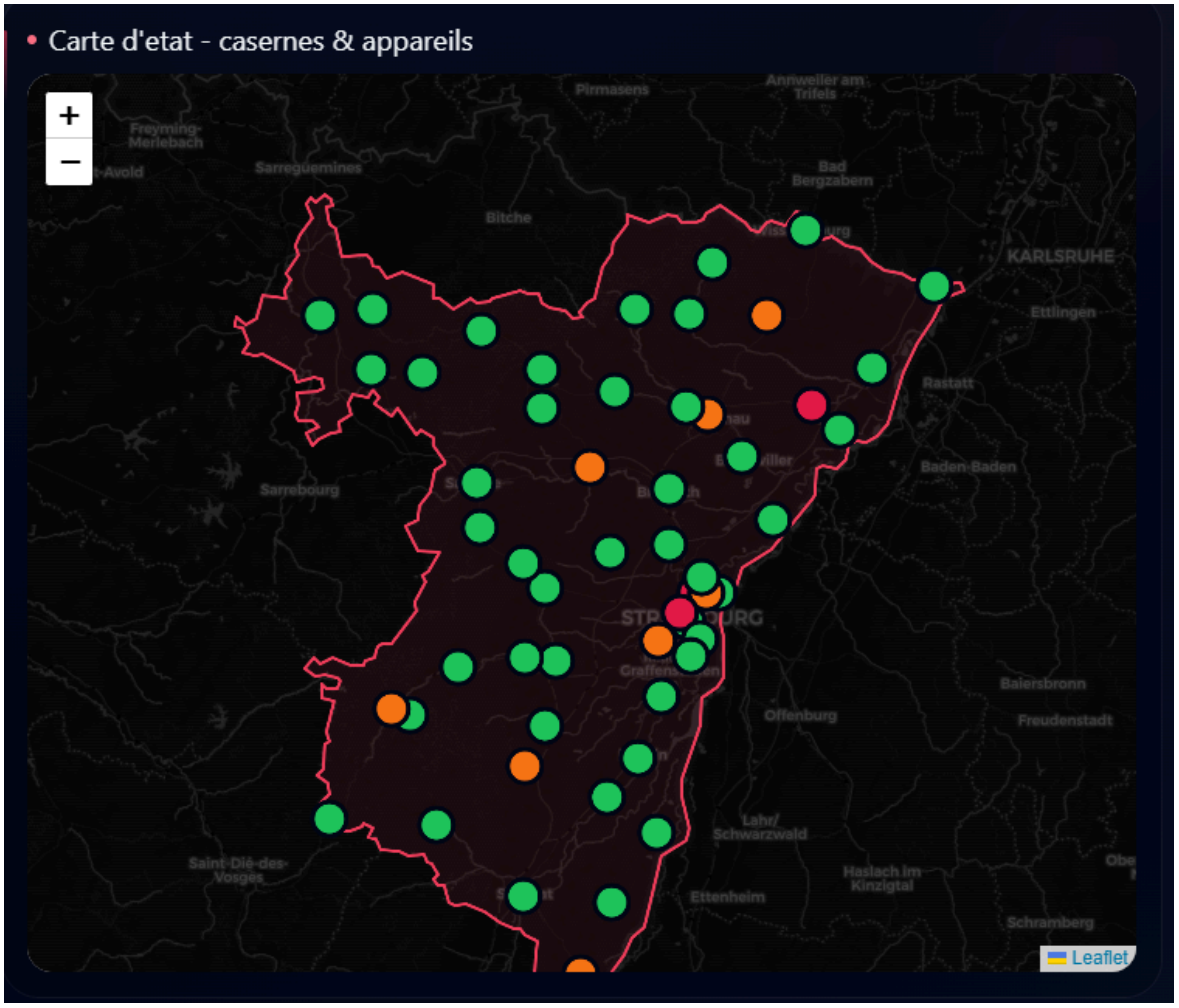
La carte interroge l'**API REST de Zabbix** à intervalle régulier pour récupérer l'état des hôtes par site. Les données sont superposées sur une carte Leaflet (bibliothèque JavaScript de cartographie open-source).

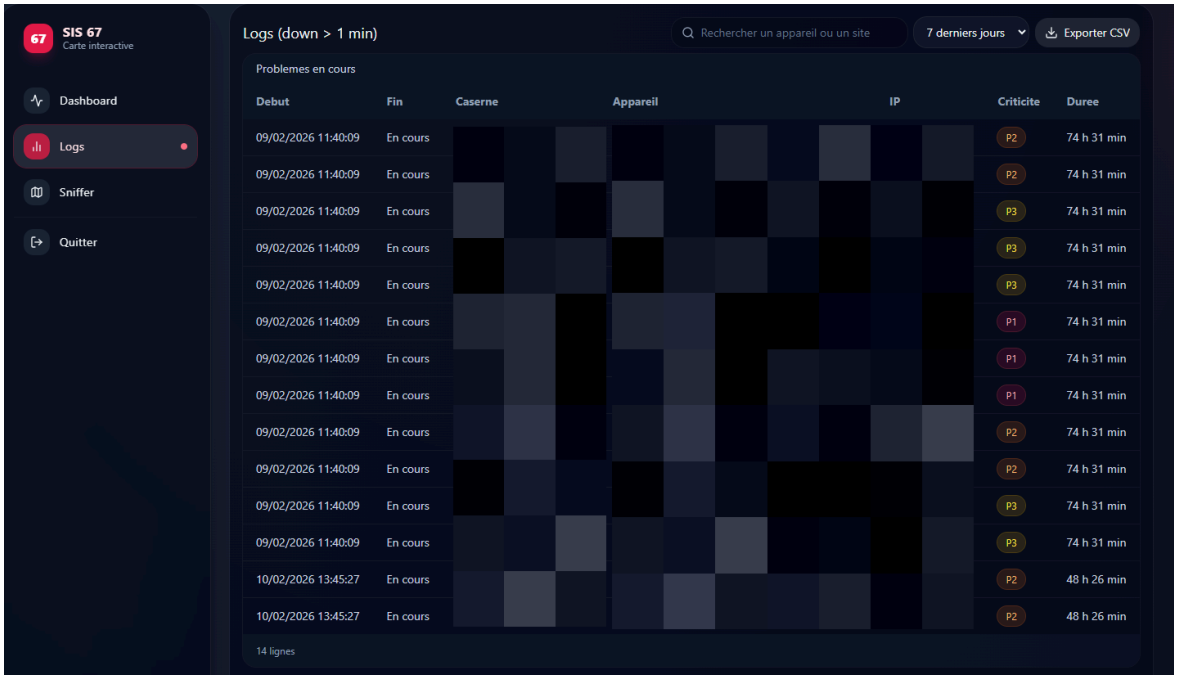
Un clic sur un marqueur affiche un résumé de l'état des équipements du site concerné.

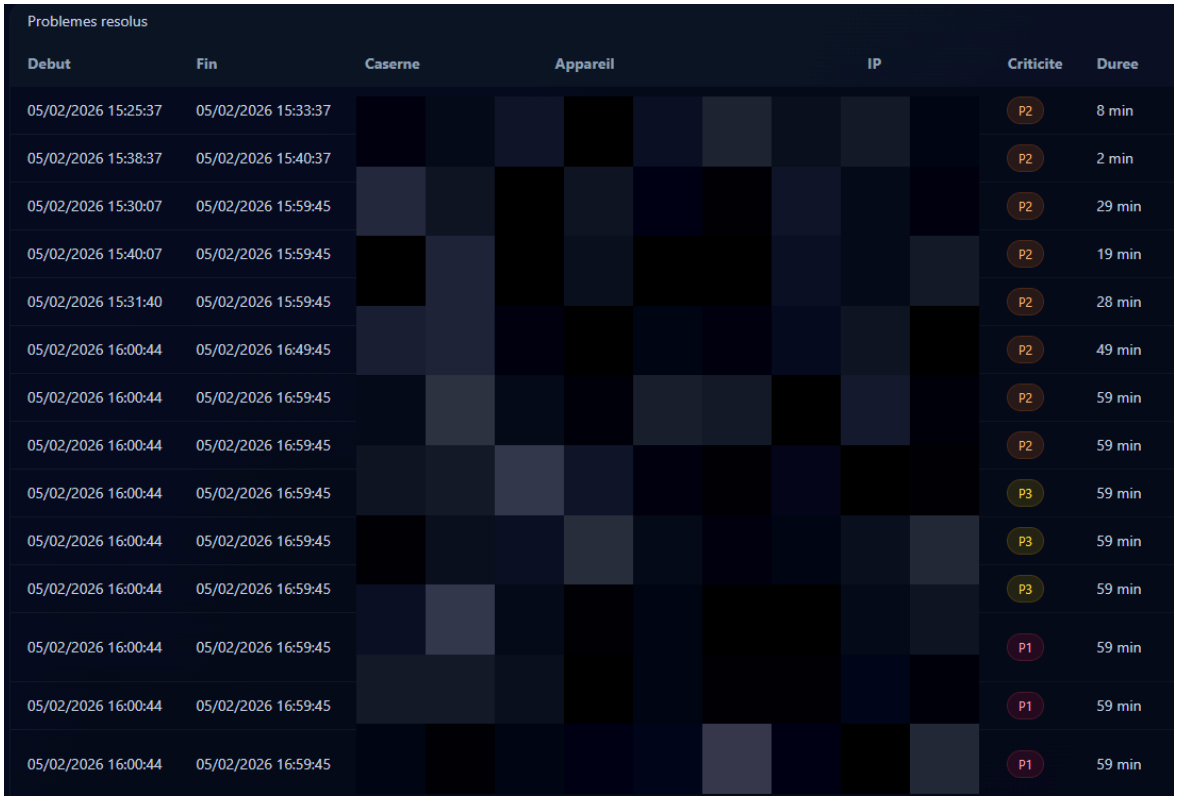
> **Captures de la carte géolocalisée**

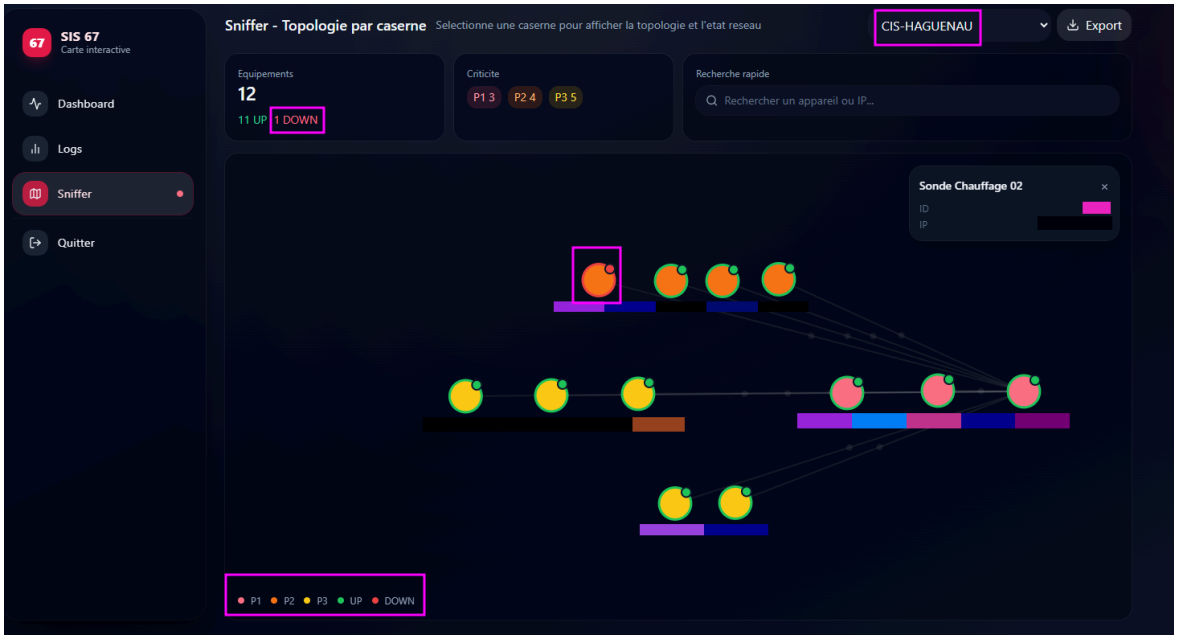

SIS 67
Carte interactive
Dashboard
Logs
Sniffer
Quitter
Equipements suivis
451
Incidents actifs
12
Disponibilite moyenne
97.3%
Centre de notifications
Notifications
Carte d'etat - casernes & appareils
Repartition des statuts
Total
451
OK 439
P1 3
P2/P3 9
Alertes P1 en cours
Down
Down
Down
ALERTE P1
05/02/2026 11:40:13
repond plus
Probleme critique (down > 1 min)
ALERTE P1
05/02/2026 11:40:13
repond plus
Probleme critique (down > 1 min)
ALERTE P1
05/02/2026 11:40:13
repond plus
Probleme critique (down > 1 min)


SIS 67
Carte interactive
Dashboard
Logs
Sniffer
Quitter
Equipements suivis
451
Incidents actifs
14
Disponibilite moyenne
96.9%
Centre de notifications
Notifications
0
Carte d'etat - casernes & appareils
Centre CIS
CIS-OUEST
26 equipements
UP 23
DOWN 3
P1 7
Switch · P1
Switch · P1
Switch · P1
Repartition des statuts
Total
451
OK 437
P1 3
P2/P3 11
Alertes P1 en cours
Down
Down
Down


Carte d'etat - casernes & appareils
Pirmasens
Annweiler am Trifels
Freyming-Merlebach
Sarreguemines
Bad Bergzabern
Bitche
KARLSRUHE
Ettlingen
Rastatt
Baden-Baden
Sarrebourg
Offenburg
Baiersbronn
Freudenstadt
Lahr/ Schwarzwald
Haslach im Kinzigtal
Ettenheim
Schramberg
Saint-Dié-des-Vosges
Leaflet


SIS 67
Carte interactive
Dashboard
Logs
Sniffer
Quitter
Logs (down > 1 min)
Rechercher un appareil ou un site
7 derniers jours
Exporter CSV
Problemes en cours
Debut
Fin
Caserne
Appareil
IP
Criticite
Duree
09/02/2026 11:40:09 En cours P2 74 h 31 min
09/02/2026 11:40:09 En cours P2 74 h 31 min
09/02/2026 11:40:09 En cours P3 74 h 31 min
09/02/2026 11:40:09 En cours P3 74 h 31 min
09/02/2026 11:40:09 En cours P3 74 h 31 min
09/02/2026 11:40:09 En cours P1 74 h 31 min
09/02/2026 11:40:09 En cours P1 74 h 31 min
09/02/2026 11:40:09 En cours P1 74 h 31 min
09/02/2026 11:40:09 En cours P2 74 h 31 min
09/02/2026 11:40:09 En cours P2 74 h 31 min
09/02/2026 11:40:09 En cours P3 74 h 31 min
09/02/2026 11:40:09 En cours P3 74 h 31 min
10/02/2026 13:45:27 En cours P2 48 h 26 min
10/02/2026 13:45:27 En cours P2 48 h 26 min
14 lignes





8. Matrice de flux réseau

Les flux ont été ouverts sur les firewalls du siège et des sites distants. Voici les flux principaux, présentés de façon générique :

Protocole	Source	Destination	Port	Objet
TCP	Serveurs supervisés (LAN)	Proxy Zabbix	10051	Agents vers proxy
TCP	Proxy Zabbix	Serveur Zabbix	10051	Synchronisation proxy → serveur
UDP	Proxy Zabbix	VLAN réseau	161 (SNMP)	Interrogation switchs/firewalls siège
TCP	Serveur Zabbix	Serveur Exchange	SMTP	Envoi d'alertes email
TCP	Poste technicien	Serveur Zabbix	80/443	Accès interface web
UDP	Proxy Zabbix	Sites distants (WAN)	161 (SNMP)	Collecte sur casernes distantes
UDP	Proxy Zabbix	Sites distants (WAN)	ICMP/PING	Vérification disponibilité

9. Tests et validation

Test réalisé	Résultat
Connectivité serveur ↔ proxy	✅ OK
Remontée de données	✅ OK
Interrogation SNMP d'un switch	✅ OK
Réception d'une alerte email lors d'un hôte down	✅ OK
Disponibilité de l'interface web Zabbix	✅ OK
Affichage de la carte géolocalisée	✅ OK
Filtrage des alertes par équipe responsable	✅ OK
Synchronisation NTP	✅ OK
Restriction des droits par groupe d'utilisateurs	✅ OK

10. Difficultés rencontrées et solutions

Ouverture des flux réseau : la matrice de flux a nécessité plusieurs allers-retours avec l'administrateur réseau pour identifier l'ensemble des ports à ouvrir

(10051 TCP pour les agents, 161 UDP pour SNMP, SMTP pour les alertes email). Certains flux vers les sites distants étaient encore en attente de validation en fin de stage, ce qui a temporairement limité la couverture SNMP aux équipements du siège.

Import du schéma SQL : l'importation du schéma initial est une opération longue qui ne doit sous aucun prétexte être interrompue, au risque de corrompre la base de données et de devoir recommencer l'installation from scratch. Une surveillance active du terminal pendant toute la durée de l'import était indispensable.

Configuration SNMP sur équipements existants : certains switches étaient déjà en production avec une configuration SNMP partielle ou non standard. Il a fallu reconfigurer les community strings et vérifier l'accessibilité depuis le proxy avant de pouvoir les intégrer dans Zabbix, en coordination avec l'équipe réseau.

Ajout manuel des hôtes : les premiers hôtes intégrés ont nécessité plusieurs ajustements avant d'obtenir une remontée de données propre — notamment la cohérence entre le `Hostname` déclaré dans l'agent et celui saisi dans l'interface, le choix du bon template, et la vérification que le proxy était bien sélectionné pour les hôtes distants. Un processus d'intégration standardisé a ensuite été formalisé pour accélérer les ajouts suivants.

11. Présentation à la DSI

En fin de stage, une **présentation de restitution** a été organisée devant la DSI et les responsables d'équipes pour valider le déploiement.

Points présentés :

- Architecture déployée et justification des choix techniques (Server + Proxy, Ubuntu 22.04, MySQL)
- Démonstration live de l'interface Zabbix (dashboards, carte, alertes)
- Nombre d'hôtes supervisés et répartition par type d'équipement
- Logique du système d'alertes et du routage par équipe
- Perspectives d'évolution (extension SNMP sur les sites distants, supervision applicative, hardening des serveurs)
- Remise de la documentation technique pour la prise en main par les équipes