Cahier des charges
Projet Hospitalier

Kenzi BOUGHADOU
Hugo GRILLET

Table des matières

1. Équipements actuels

1.1. Serveurs

- **Type et nombre** : Serveurs physiques (rack, tour) et/ou virtualisés.
- **Systèmes d'exploitation** : Windows Server (2022), distributions Linux (Debian).
- **Rôles** : Contrôleur de domaine, bases de données, applications métiers, serveurs de fichiers.
- **État matériel** : Processeurs, mémoire, stockage, ancienneté.
- **Niveau de maintenance** : Patches de sécurité, mises à jour logicielles, contrats de support.

1.2. Postes de travail

- **Nombre et répartition** : Bureaux administratifs, services médicaux, postes mobiles.
- **Systèmes d'exploitation** : Windows 10, Linux.
- **Applications installées** : Logiciels de bureautique, outils métiers, antivirus.
- **Politique de renouvellement** : Échéances de support, compatibilité matériel-logiciel.

1.3. Pare-feu et solutions de sécurité périmétrique

- **Dispositifs en place** : Pare-feu matériel (UTM, NGFW), OPNSense.
- **Configuration** : Segmentation (DMZ, VLAN), règles de filtrage, VPN.
- **Mises à jour** : Versions du firmware, correctifs de sécurité.

1.4. Outils de supervision

- **Technologies utilisées** : Zabbix, ou supervision basique via scripts.
- **Couverture** : Surveillance du réseau, des serveurs, des applications critiques.
- **Alerte** : Canal d'alerte (mail), seuils paramétrés, corrélations d'événements.

2. Analyse des forces, faiblesses et vulnérabilités

2.1. Forces

- **Matériel récent** : Serveurs et commutateurs bénéficiant encore de support constructeur.
- **Pare-feu déjà en place** : Filtrage et gestion du trafic (OPNSense ou solution professionnelle).
- **Supervision partielle** : Présence d'un outil de monitoring, même si peu exploité.

2.2. Faiblesses

- **Matériel obsolète** : Certains serveurs et postes de travail dépassés, hors support.
- **Mises à jour irrégulières** : Systèmes d'exploitation et applications non patchés.
- **Pare-feu mal configuré** : Règles trop permissives, absence de logs ou d'analyse approfondie.
- **Supervision limitée** : Surveillances incomplètes, absence d'historiques et de corrélations.

2.3. Vulnérabilités potentielles

- **Logiciels non conformes** : Versions anciennes exposées à des failles critiques.
- **Absence de segmentation réseau** : Risque de propagation rapide d'une infection.
- **Authentification faible** : Mots de passe simples, partage de comptes, gestion des droits insuffisante.
- **Manque de formation** : Personnel peu sensibilisé aux risques (phishing, ransomwares)

3. Liste des besoins techniques et métiers

1. **Continuité du service médical**
    - Disponibilité des systèmes 24h/24 et 7j/7.
    - Accès rapide et fiable aux dossiers patients et aux images médicales.
    - Tolérance aux pannes pour éviter toute interruption dans la prise en charge des patients.
2. **Protection des données sensibles**
    - Chiffrement des flux et des stockages contenant des données de santé.
    - Contrôle d'accès rigoureux (comptes, rôles, habilitations).
    - Traçabilité et journalisation des opérations sur les données.
3. **Conformité réglementaire**
    - Respect des obligations légales (RGPD, hébergement de données de santé, statut OIV).
    - Application des bonnes pratiques de sécurité (ISO 27001 ou autres référentiels).
    - Mise en place d'un Plan de Continuité d'Activité (PCA) et d'un Plan de Reprise d'Activité (PRA).
4. **Interopérabilité et évolutivité**
    - Capacité à intégrer des applications métiers hospitalières (gestion des patients, imagerie médicale, laboratoire, pharmacie).
    - Scalabilité pour absorber une augmentation du nombre d'utilisateurs et de données.
    - Compatibilité avec les systèmes de supervision et d'administration existants ou futurs.
5. **Efficacité opérationnelle**
    - Simplification de la gestion quotidienne (administration centralisée, automatisation des mises à jour).
    - Surveillance proactive pour détecter les anomalies et anticiper les incidents.
    - Processus d'installation et de maintenance documentés pour réduire le temps d'intervention.

4. Propositions de solutions adaptées

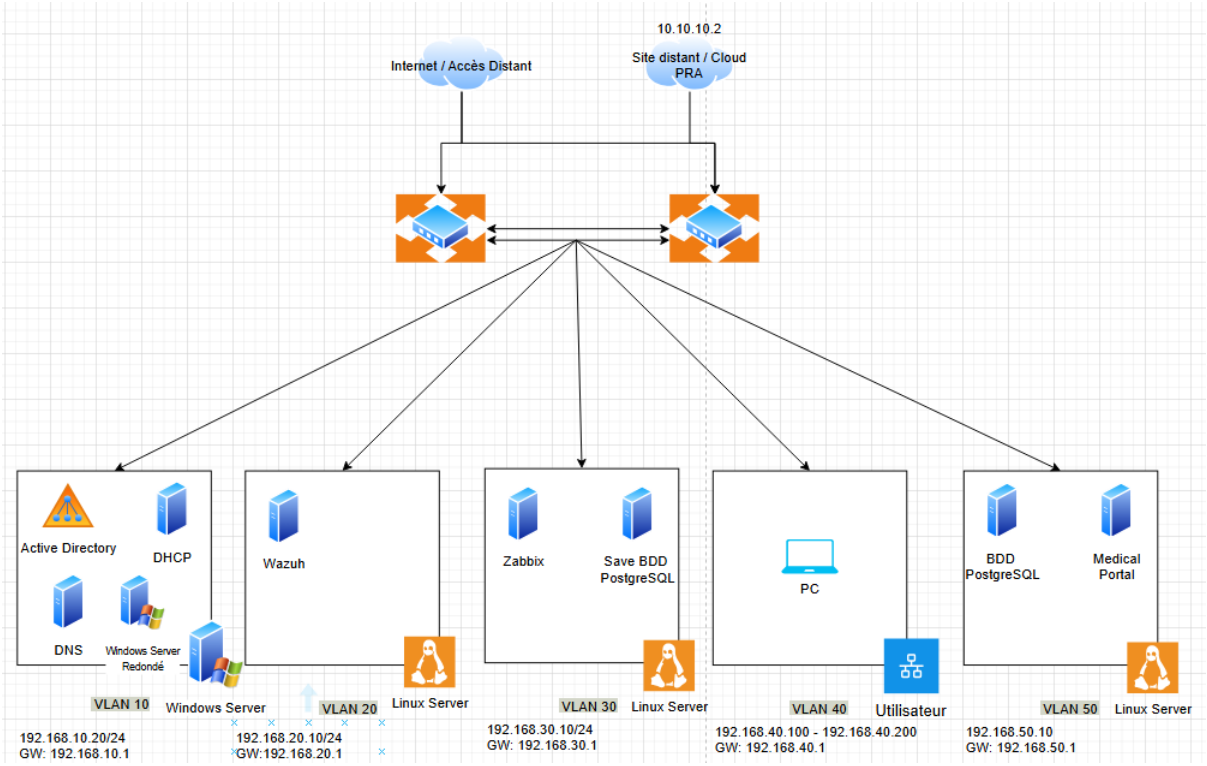
4.1. Matériel

- **Serveurs physiques ou virtualisés** :
    - Plateforme Proxmox on pour créer des machines virtuelles et faciliter la haute disponibilité.
    - Choix de serveurs x86 compatibles avec des processeurs récents, de la mémoire ECC et des disques SSD ou HDD configurés en RAID.
    - Dimensionnement selon la volumétrie des bases de données et le nombre d'utilisateurs simultanés.
- **Commutateurs et routeurs** :
    - Commutateurs managés pour la segmentation réseau (VLAN).
    - Routeurs ou pare-feu capables de gérer des protocoles de redondance si un lien tombe (exemple : CARP sur OPNSense).

4.2. Logiciel

- **Système d'exploitation serveur** :
    - Windows Server 2022 pour le rôle de contrôleur de domaine (Active Directory, DNS, DHCP).
    - Debian ou Ubuntu pour les serveurs applicatifs et de supervision (Zabbix).
- **Pare-feu et VPN** :
    - OPNSense pour filtrer les flux, configurer des VPN (IPsec ou OpenVPN) et gérer la détection d'intrusion (Snort ou Suricata).
    - Segmentation en VLAN (DMZ, LAN, réseau de supervision) avec des règles spécifiques et strictes.
- **SIEM et supervision** :
    - Wazuh ou une solution basée sur la suite Elastic pour la corrélation des logs.
    - Zabbix pour la supervision technique (CPU, mémoire, disponibilité des services) et l'alerte en temps réel.
- **Sauvegarde et redondance** :
    - Sauvegarde automatisée sur un NAS ou un serveur de stockage dédié.

- Réplication possible vers un second site ou un hébergement cloud certifié pour les données de santé.
- Tests réguliers de restauration afin de valider la procédure de reprise d'activité.



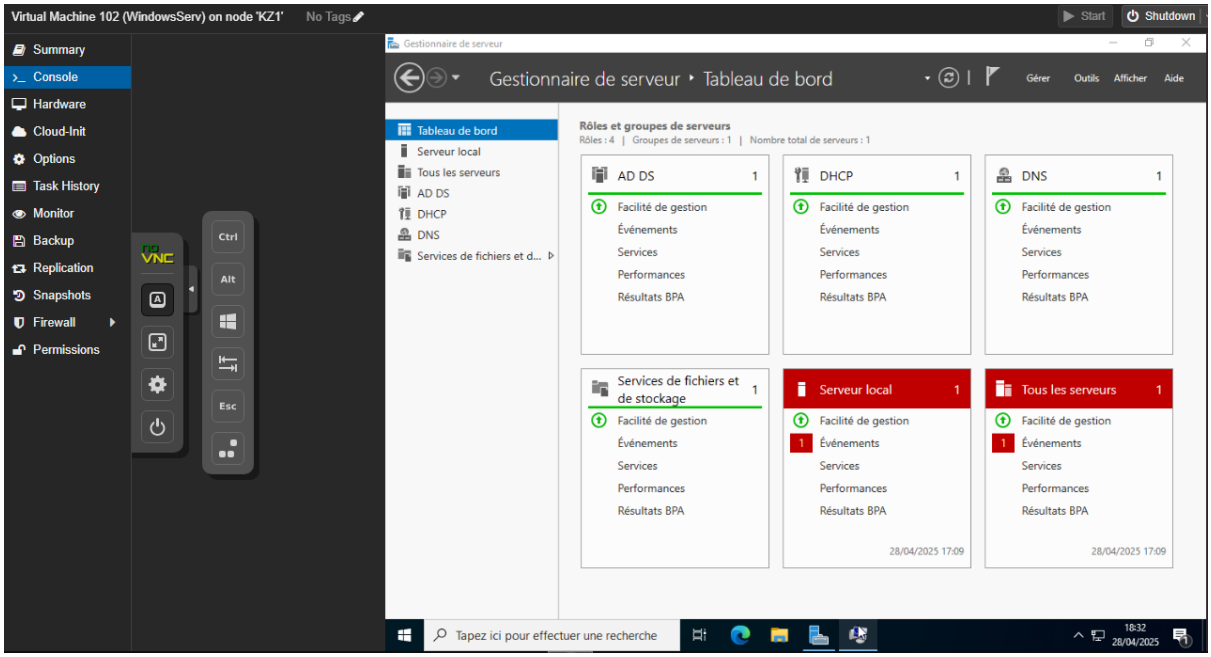
Machine	IP	VLAN	Rôle	Gateway	DNS
Windows Server 2022	192.168.10.20	VLAN 10	Active Directory, DNS, DHCP	192.168.10.1	192.168.10.20 / 1.1.1.1
Wazuh	192.168.20.10	VLAN 20	Sécurité	192.168.20.1	192.168.10.20 / 8.8.8.8
Zabbix Server	192.168.30.10	VLAN 30	Supervision	192.168.30.1	192.168.10.20 / 8.8.8.8
PC Utilisateurs	192.168.40.100 - 192.168.40.200	VLAN 40	Poste utilisateur	192.168.40.1	192.168.10.20 / 8.8.8.8
BDD	192.168.50.10	VLAN 50	DMZ, BDD	192.168.50.1	192.168.10.20 / 8.8.8.8

4.3. Organisationnel

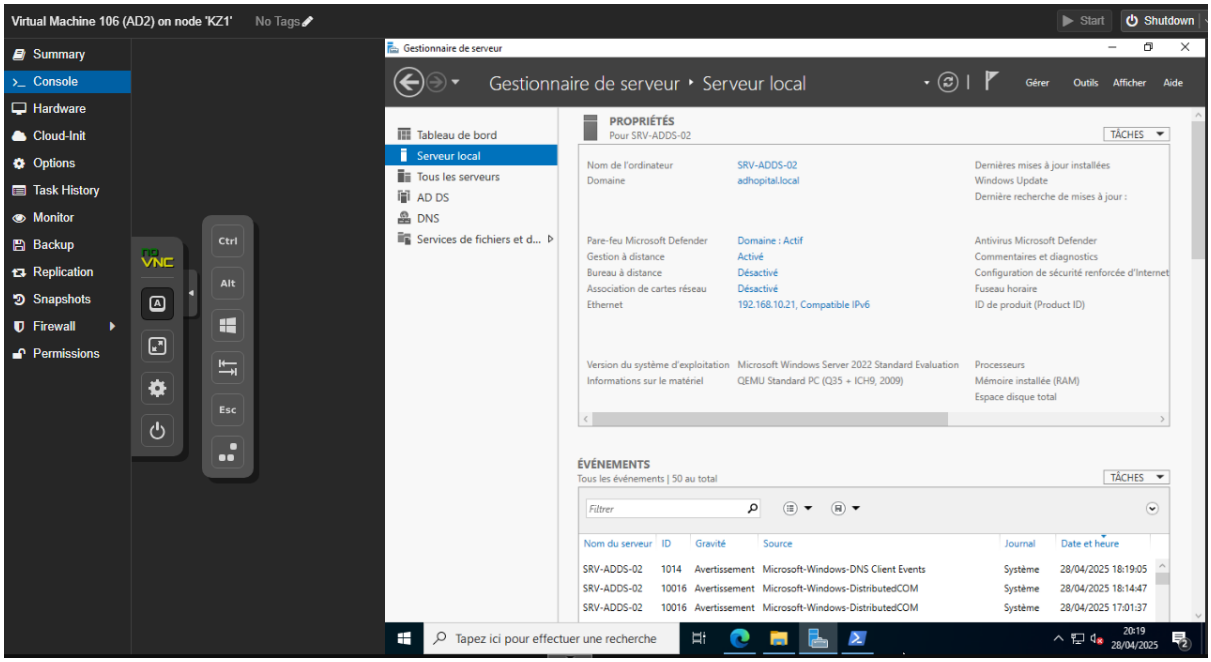
- **Gestion des identités et des accès** :
  - Contrôleurs de domaine avec comptes et groupes définis selon les rôles (médecins, infirmiers, administrateurs).
  - Authentification multifacteur pour les accès distants (VPN, administration).
  - Politique stricte de mots de passe (longueur, complexité, rotation).
- **Processus de sécurité** :
  - Chartes et politiques internes validées par la direction (usage des ressources informatiques, confidentialité).
  - Procédures de gestion des incidents et des changements.
  - Sessions de sensibilisation pour le personnel médical et administratif (hameçonnage, mots de passe partagés, clés USB non autorisées).
- **Coût et conformité** :
  - Limitation des coûts de licence grâce à l'utilisation de solutions libres (OPNSense, Debian, Wazuh, Zabbix).
  - Investissement ciblé sur la résilience et la protection des données (serveurs, sauvegardes, dispositifs de redondance).
  - Respect des obligations HDS et RGPD en stockant les données de santé dans des environnements conformes et en assurant la traçabilité.

5. Équipements installés

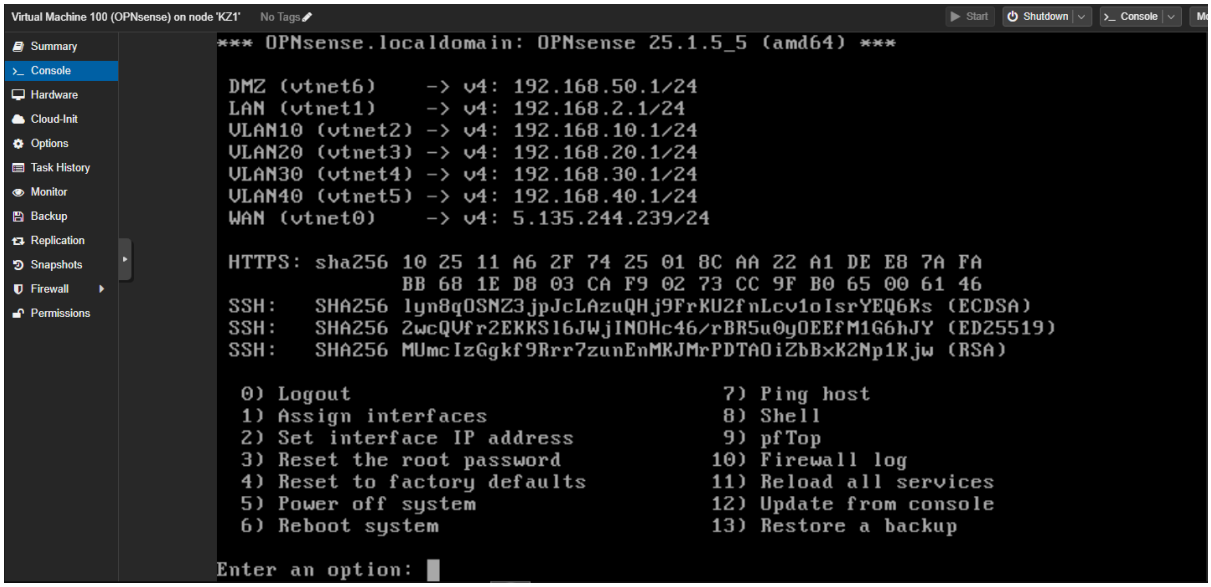
AD 1 :



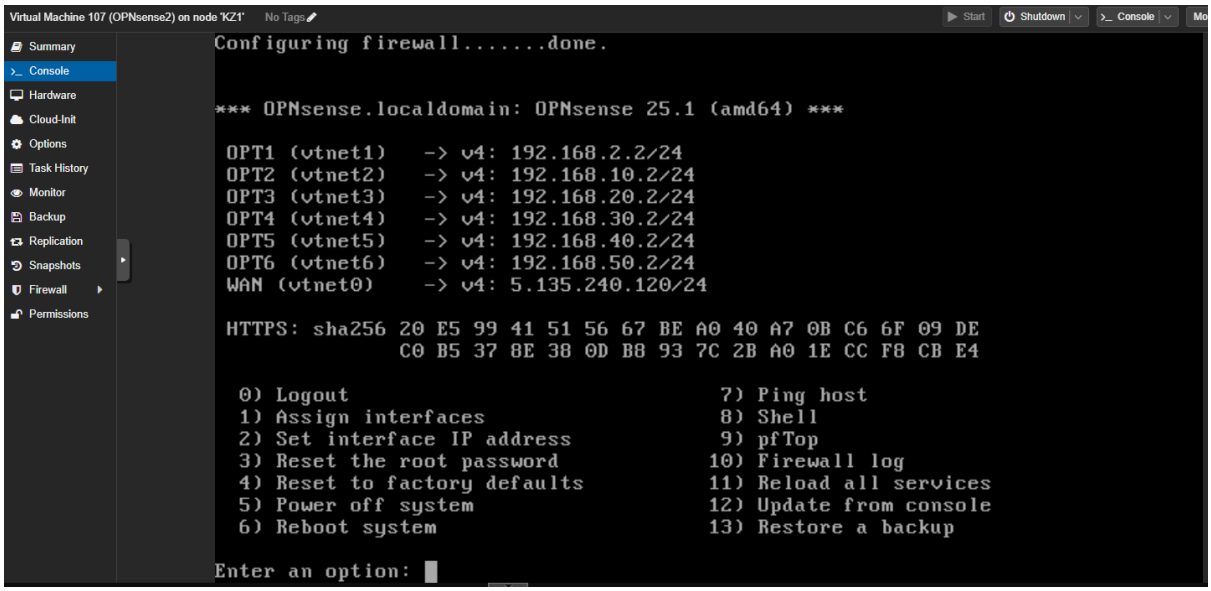
AD 2 :



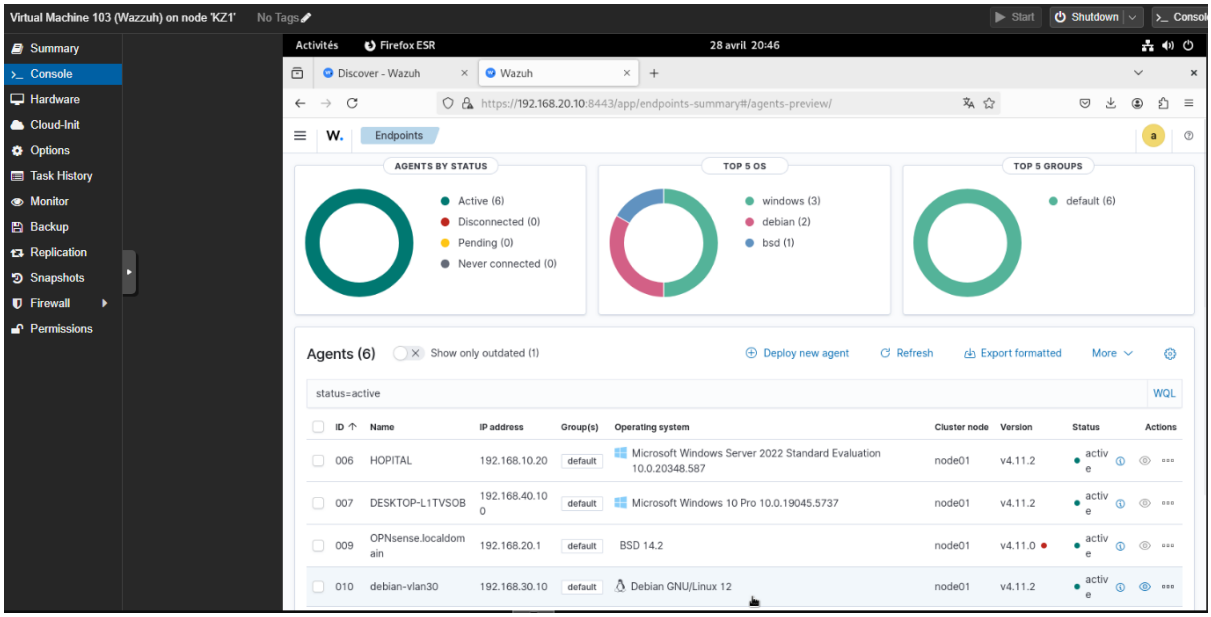
OPNSense 1 :



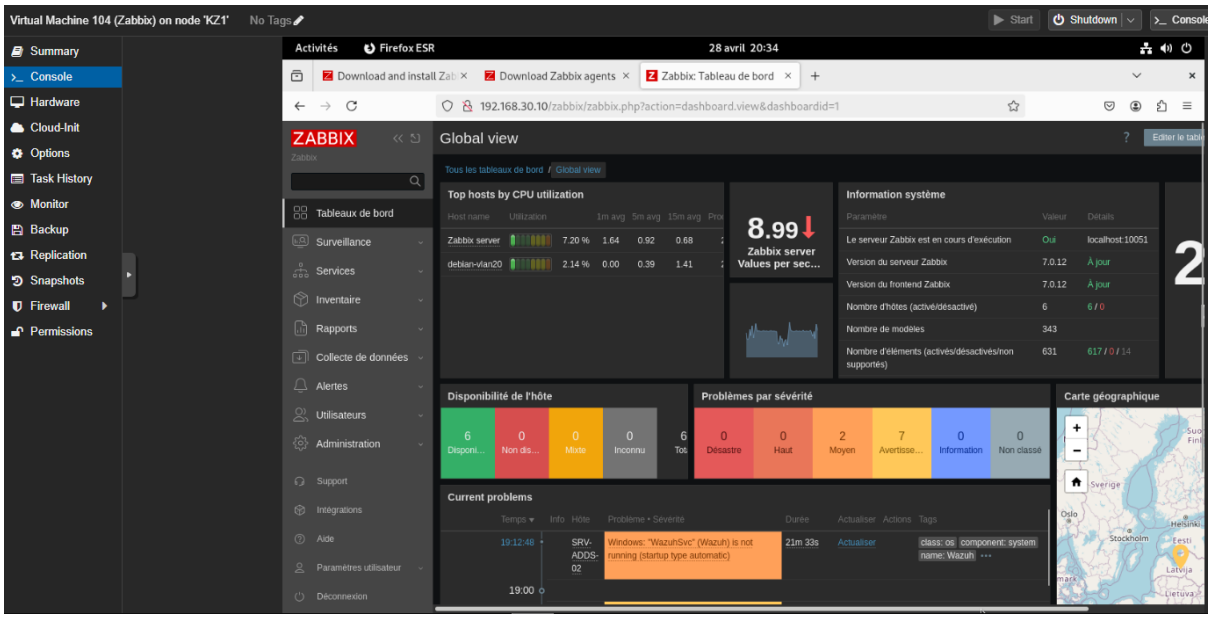
OPNSense 2 :



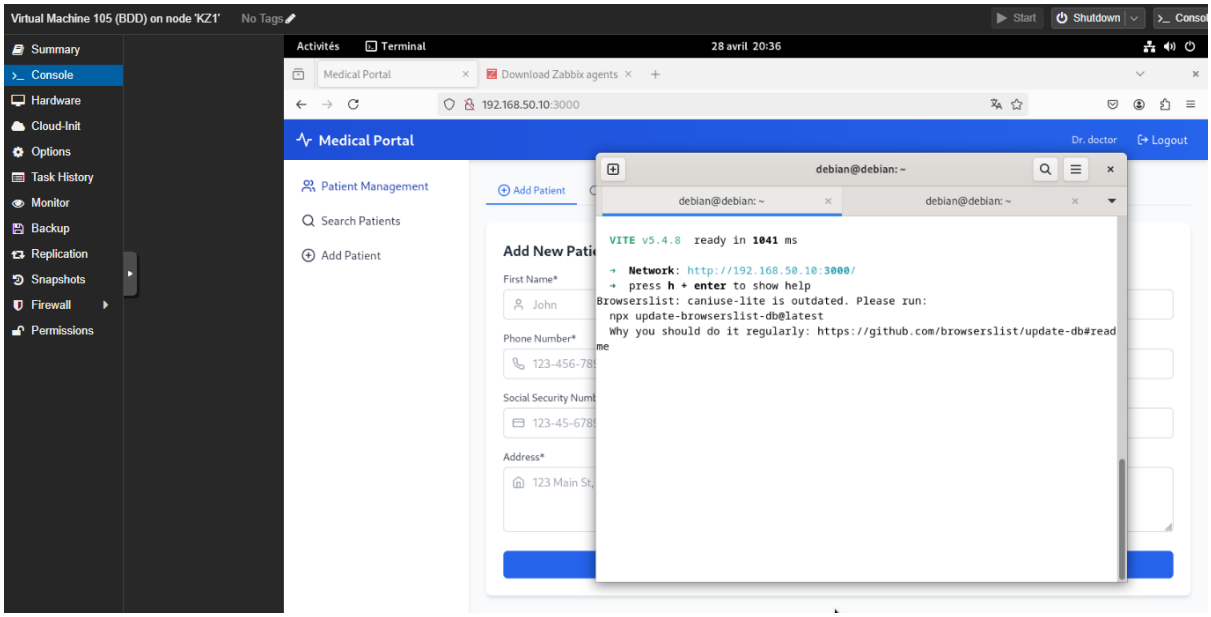
Wazzuh :


Virtual Machine 103 (Wazzuh) on node 'KZ1'
No Tags
Start
Shutdown
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Backup
Replication
Snapshots
Firewall
Permissions
Activités
Firefox ESR
28 avril 20:46
Discover - Wazuh
Wazuh
https://192.168.20.10:8443/app/endpoints-summary#/agents-preview/
Endpoints
AGENTS BY STATUS
Active (6)
Disconnected (0)
Pending (0)
Never connected (0)
TOP 5 OS
windows (3)
debian (2)
bsd (1)
TOP 5 GROUPS
default (6)
Agents (6)
Show only outdated (1)
Deploy new agent
Refresh
Export formatted
More
status=active
WQL
ID
Name
IP address
Group(s)
Operating system
Cluster node
Version
Status
Actions
006 HOPITAL 192.168.10.20 default Microsoft Windows Server 2022 Standard Evaluation 10.0.20348.587 node01 v4.11.2 active
007 DESKTOP-L1TVSOB 192.168.40.100 default Microsoft Windows 10 Pro 10.0.19045.5737 node01 v4.11.2 active
009 OPNsense.localdomain 192.168.20.1 default BSD 14.2 node01 v4.11.0 active
010 debian-vlan30 192.168.30.10 default Debian GNU/Linux 12 node01 v4.11.2 active

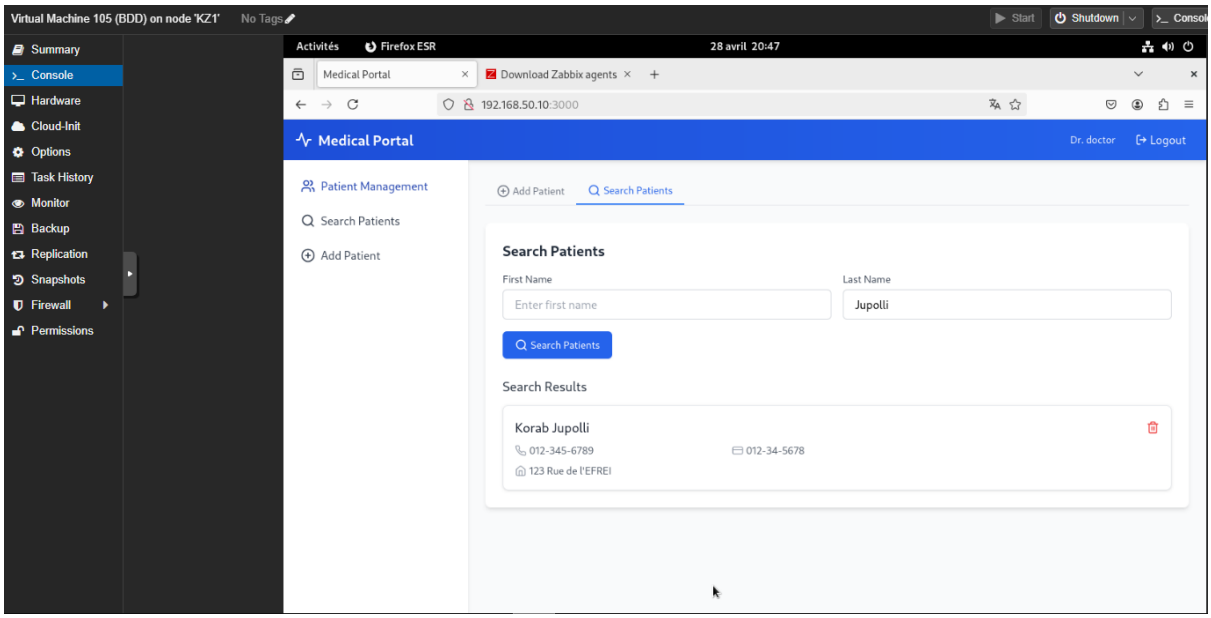
Zabbix :


Virtual Machine 104 (Zabbix) on node 'KZ1'
No Tags
Start
Shutdown
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Backup
Replication
Snapshots
Firewall
Permissions
Activités
Firefox ESR
28 avril 20:34
Download and install Zabbix agents
Download Zabbix agents
Zabbix: Tableau de bord
192.168.30.10/zabbix/zabbix.php?action=dashboard.view&dashboardid=1
ZABBIX
Global view
Tableau de bord
Surveillance
Services
Inventaire
Rapports
Collecte de données
Alertes
Utilisateurs
Administration
Support
Intégrations
Aide
Paramètres utilisateur
Déconnexion
Top hosts by CPU utilization
Zabbix server
debian-vlan20
8.99
Zabbix server Values per sec...
Information système
Le serveur Zabbix est en cours d'exécution
Version du serveur Zabbix
Version du frontend Zabbix
Nombre d'hôtes (activé/désactivé)
Nombre de modèles
Nombre d'éléments (activés/désactivés/non supportés)
Disponibilité de l'hôte
Problèmes par sévérité
Désastre
Haut
Moyen
Information
Non classé
Carte géographique
Current problems
SRV-ADDS-02
Windows: "WazuhSvc" (Wazuh) is not running (startup type automatic)
21m 33s
Actualiser
class: os
component: system
name: Wazuh

BDD :


Virtual Machine 105 (BDD) on node 'KZ1'
No Tags
Start
Shutdown
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Backup
Replication
Snapshots
Firewall
Permissions
Activités
Terminal
28 avril 20:36
Medical Portal
Download Zabbix agents
192.168.50.10:3000
Medical Portal
Dr. doctor
Logout
Patient Management
Search Patients
Add Patient
debian@debian: ~
VITE v5.4.8 ready in 1041 ms
Network: http://192.168.50.10:3000/
press h + enter to show help
Browserslist: caniuse-lite is outdated. Please run:
npx update-browserslist-db@latest
Why you should do it regularly: https://github.com/browserslist/update-db#readme

Save BDD :


Virtual Machine 105 (BDD) on node 'KZ1'
No Tags
Start
Shutdown
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Backup
Replication
Snapshots
Firewall
Permissions
Activités
Firefox ESR
28 avril 20:47
Medical Portal
Download Zabbix agents
192.168.50.10:3000
Medical Portal
Dr. doctor
Logout
Patient Management
Search Patients
Add Patient
Add Patient
Search Patients
Search Patients
First Name
Enter first name
Last Name
Jupolli
Search Patients
Search Results
Korab Jupolli
012-345-6789
012-34-5678
123 Rue de l'EFREI