Rapport de fonctionnement d'infrastructure

Par Hugo LOURREIRO et
Alexandre BEROT-ARMAND
IUT Nord-Franche Comté - 2023

TABLE DES MATIERES

Contextualisation _____ 3
Schéma du réseau _____ 4
Test de fonctionnement _____ 5

CONTEXTUALISATION

Dans le but d'apprendre à installer et utiliser un IPS, nous devons mettre en place une infrastructure réseau simple pour avoir une base de travail où des données circulent.

Pour ce faire, nous avons commencé par choisir une solution pour faire tenir l'infrastructure. Pour ce projet, nous avons décidé d'utiliser Proxmox, un hyperviseur open source installé sur un serveur personnel.
Ce choix a été motivé pour plusieurs raisons :

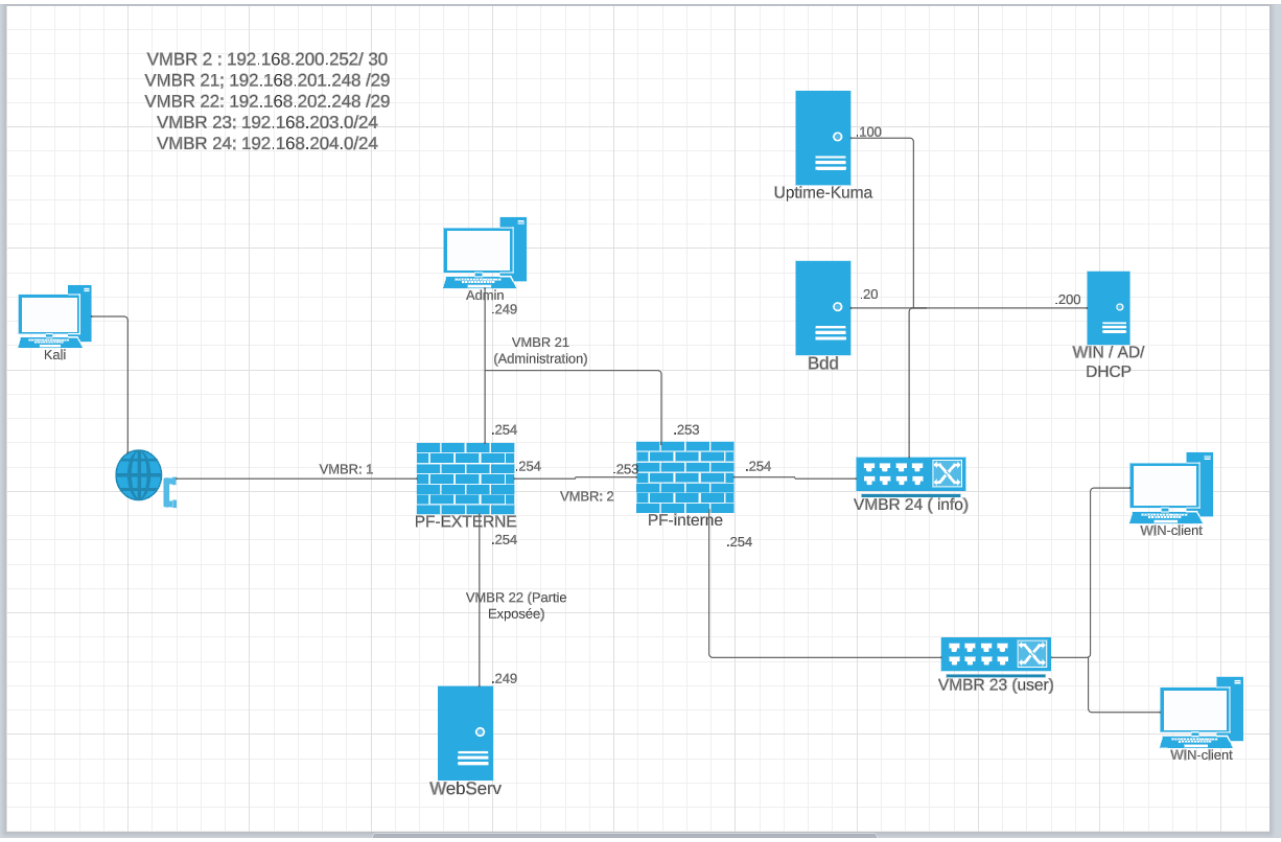
- Créer une infrastructure virtualisée pour réduire les coûts machines.
- Avoir une infrastructure centralisée en un point pour pouvoir mutualiser le travail et accélérer le processus.
- Avoir une infrastructure accessible en ligne pour pouvoir travailler efficacement depuis n'importe où.

Après avoir choisi la solution, nous avons décidé de mettre en place une infrastructure légère mais appropriée contenant :

- Un VLAN contenant le serveur AD/DNS/DHCP/Fileserver, la base de données du site et un serveur de monitoring.
- Un VLAN pour les usagers.
- Un VLAN pour administrer les Pare-feux.
- Un VLAN pour le serveur Web.

Nous avons ajouté à notre cahier des charges une division du réseau sur une DMZ multi-niveau en suivant les préconisations de l'ANSSI. Pour cela nous avons séparé le serveur Web de sa base de données en utilisant un protocole NAT/PAT pour permettre un accès sécurisé et protéger la base de données.

SCHEMA DU RESEAU

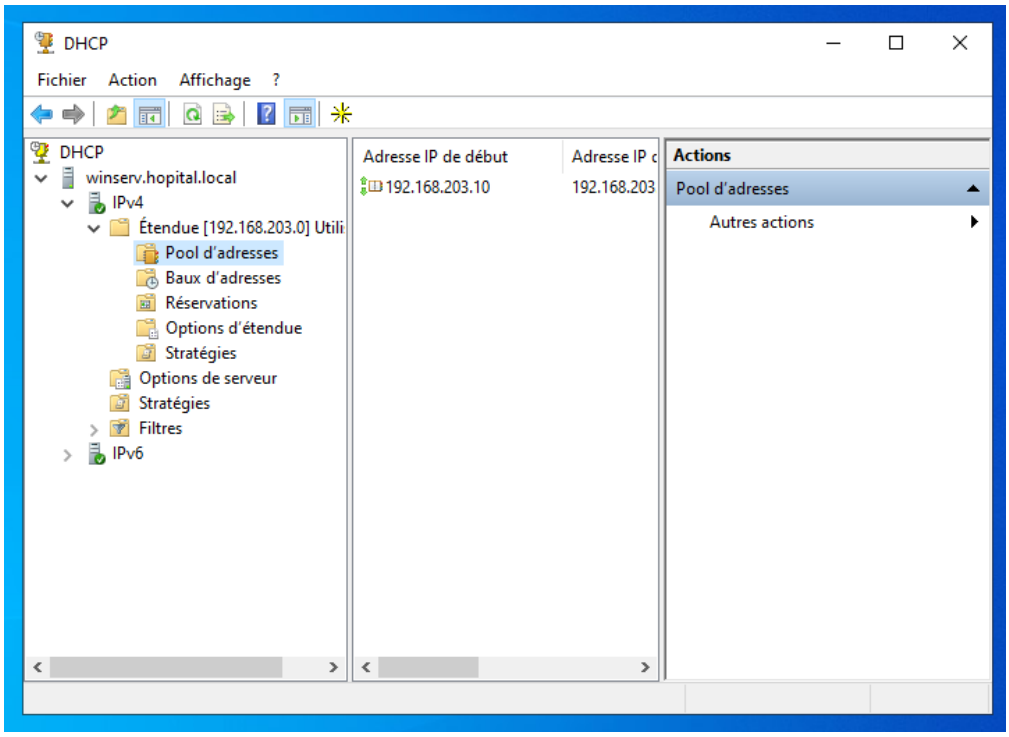


Voici le schéma réseau avec les différents VLAN (gérer par les VMBR de Proxmox)

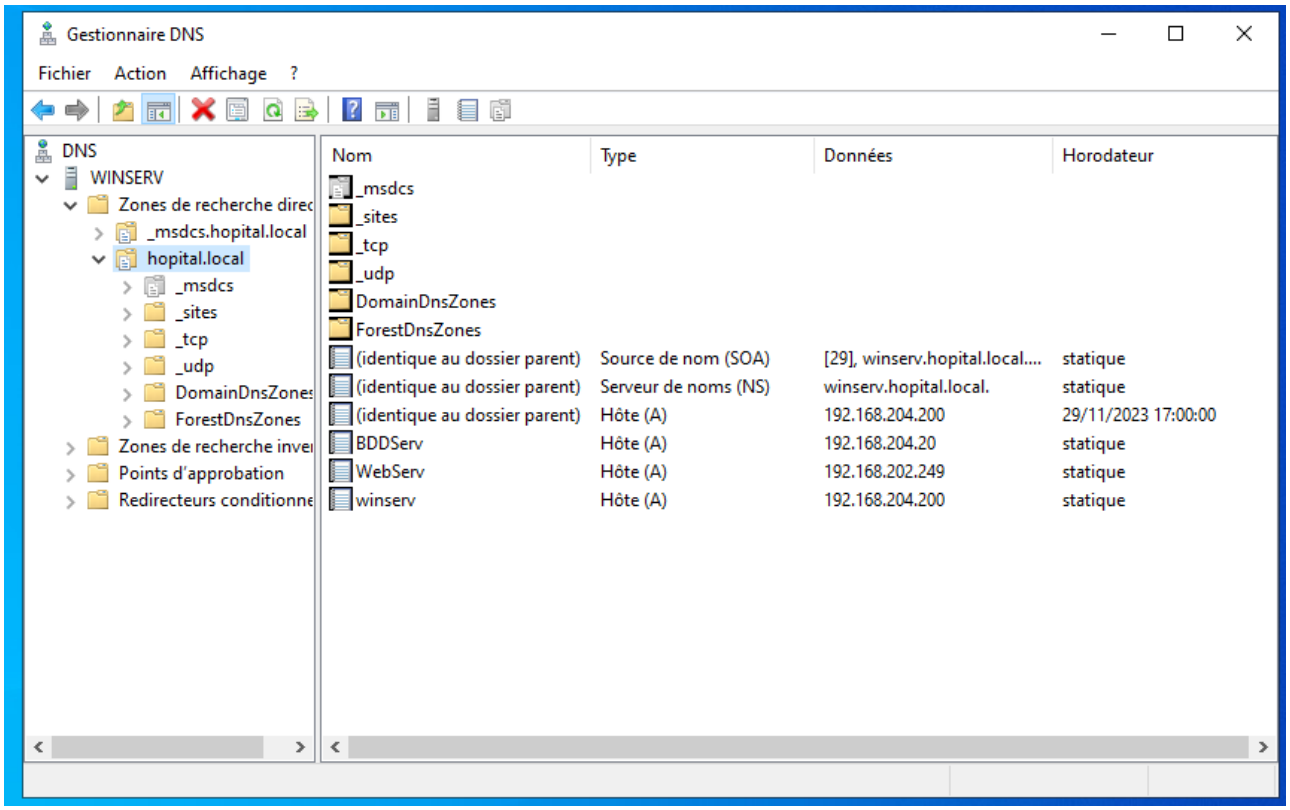
Nous pouvons voir que le réseau prend en compte les recommandations de l'ANSSI concernant les DMZ multi-niveau, la séparation des services par ordre de sensibilité et l'utilisation de rupture protocolaire via l'utilisation de pfSense avec des règles NAT/PAT.

TEST DE FONCTIONNEMENT

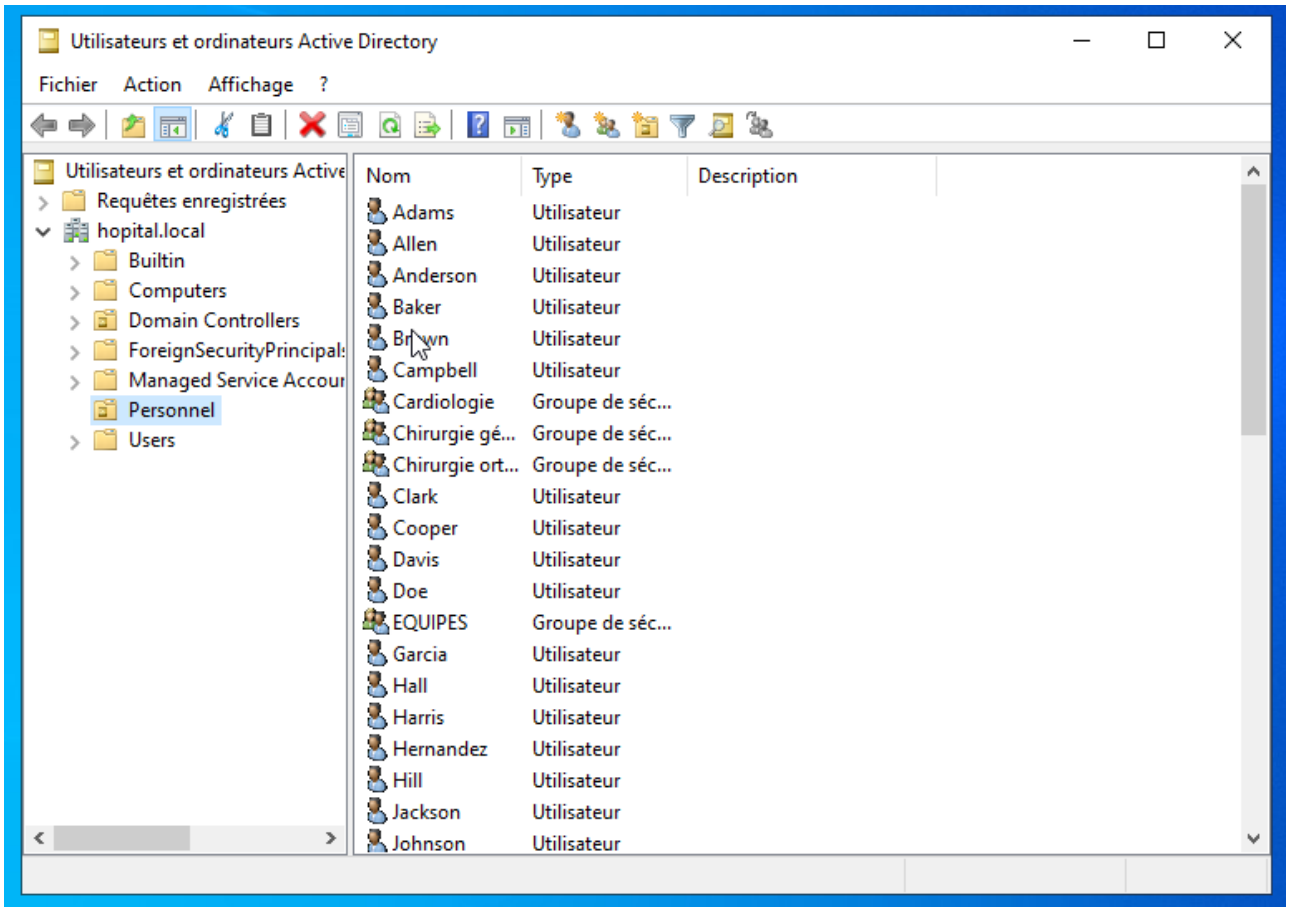
DHCP :



DNS :



Active Directory :



Serveur web joignant la BDD :

```
root@WebServ:~# ping BDDServ
PING BDDServ (192.168.204.20) 56(84) bytes of data.
64 bytes from BDDServ (192.168.204.20): icmp_seq=1 ttl=62 time=0.589 ms
64 bytes from BDDServ (192.168.204.20): icmp_seq=2 ttl=62 time=0.573 ms
64 bytes from BDDServ (192.168.204.20): icmp_seq=3 ttl=62 time=0.645 ms
64 bytes from BDDServ (192.168.204.20): icmp_seq=4 ttl=62 time=0.625 ms
64 bytes from BDDServ (192.168.204.20): icmp_seq=5 ttl=62 time=0.699 ms
^C
--- BDDServ ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4055ms
rtt min/avg/max/mdev = 0.573/0.626/0.699/0.044 ms
root@WebServ:~# _
```

L'infrastructure fonctionne donc avec les règles mises en place sur les firewall pour permettre uniquement le flux utile et interdisant le flux potentiellement malicieux.