

SAE4D011 - Déployer des services

Infrastructure

Solution

Pour mener à bien notre mission, nous sommes parties sur la solution Open source Proxmox qui va nous permettre de déployer des solutions plus efficacement.

Proxmox

Tableau des IPs salle 202 :

Nom	IP	Service
IDRAC_px1	10.202.19.1/16	IDRAC
IDRAC_px2	10.202.19.2/16	IDRAC
IDRAC_px3	10.202.19.3/16	IDRAC
IDRAC_px4	10.202.19.4/16	IDRAC
px1	10.202.19.5/16	Proxmox
px2	10.202.19.6/16	Proxmox
px3	10.202.19.7/16	Proxmox
px4	10.202.19.8/16	Proxmox
Firewall_PatteExterne	10.202.0.136/16	Firewall/Router

Pour installer Proxmox, nous avons utilisé les ldracs que nous avons reconfigurées dans notre sous-réseau de la salle 202 -> 10.202.19.X/16. Nous avons utilisé la dernière version stable 7.4 de Proxmox qui a été installé sur les cartes SD en raid prévu à cet effet dans les serveurs.

Réseau

Pour la partie réseau, nous avons mis les cartes 10 Gigabit (Medzannine) sur le switch Gigabit de la salle afin d'avoir les meilleures performances possibles. La carte Gigabit à elle été branchée sur un switch externe au réseau de la salle, qui va servir à connecter les serveurs entre eux dans un réseau privé -> 192.168.20.X/24. Les serveurs sont interconnectés sur le switch 10 Gigabit dans le but de faire des migrations le plus rapide possible et de réduire la latence à l'accès aux partages.

Stockage

Pour la gestion du stockage et le partage entre nos VM, nous avons décidé de mettre les SSD de 500 Go situés en façade du serveur 1 et 2 sur le serveur 4 afin qu'il serve de serveur de stockage principal. La configuration finale est :

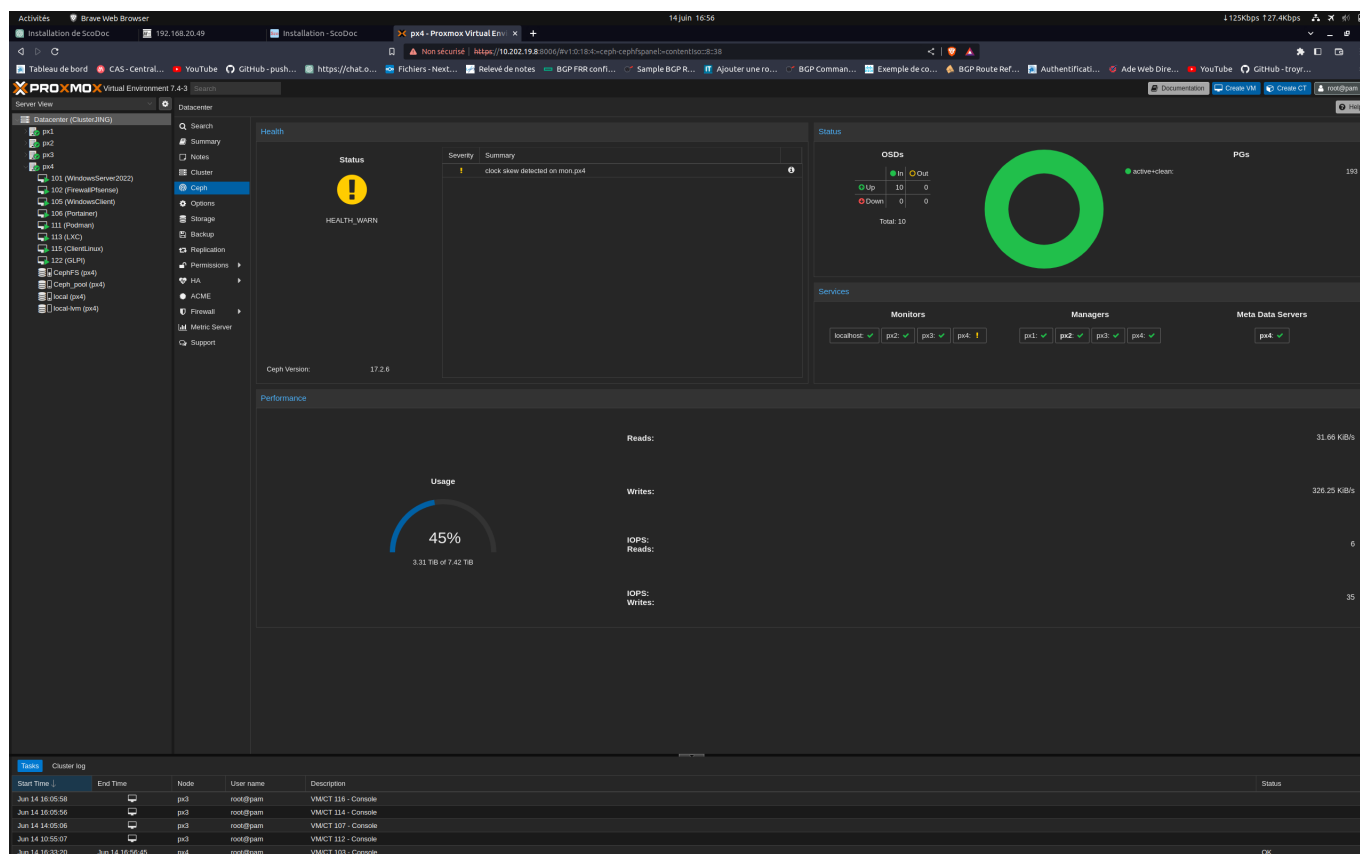
Sur les 4 serveurs les disques 2 To ont été divisés en 2 disques virtuels de 1To et 750 Go pour Ceph.

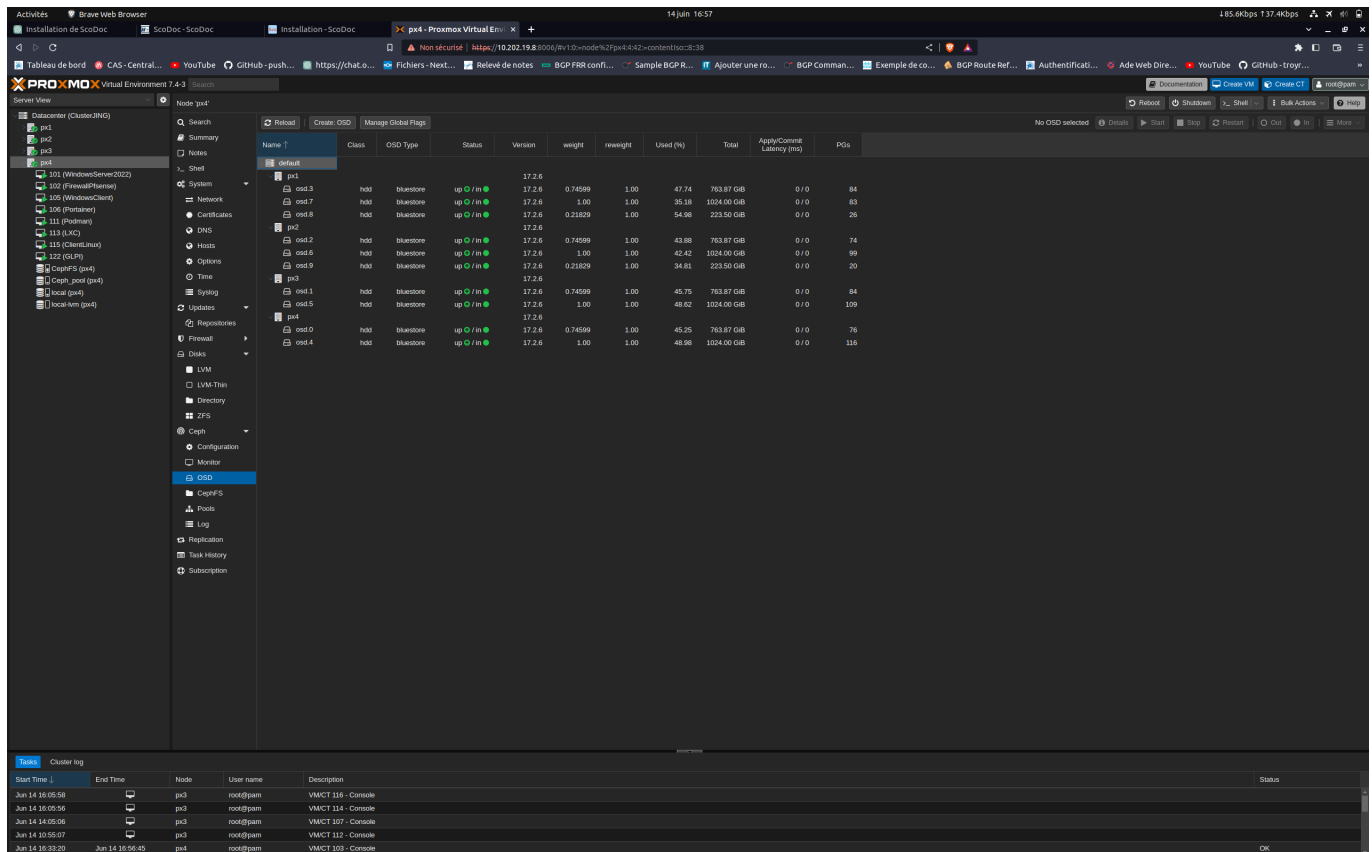
- Serveur 1 : 3 Disques physique SSD : 2 To et 2 * 250 Go en raid1 (1 disque virtuel de 500 Go).
- Serveur 2 : 3 Disques physique SSD : 2 To et 2 * 250 Go en raid1 (1 Disque virtuel de 250Go).
- Serveur 3 : 1 Disque physique SSD : 2 To.
- Serveur 4 : 3 Disque physique SSD : 2 To et 2 * 500 Go en raid1 (Disque virtuel de 500 Go).

Mise en place du Ceph et CephFS

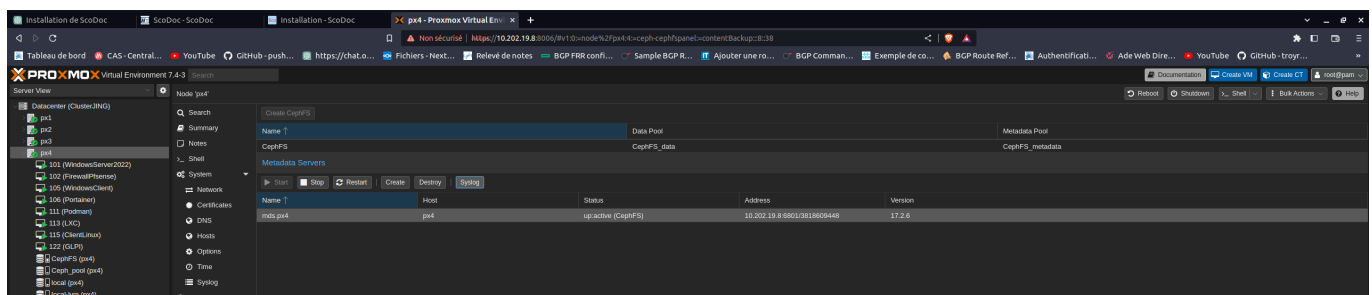
Pour utiliser le partage de fichier inter-noeud et inter-VM, j'ai utilisé tous les disques disponibles. Ce n'était pas prévu à l'origine, mais la fiabilité et la rapidité de Ceph, on suffit à mener à bien le projet.

Pour installer Ceph, il suffit de suivre la procédure habituelle et nous n'avons pas rencontré de problème. Voilà le résultat final après plusieurs jours d'utilisation et tous les disques affectés :





J'ai mis en place le CephFS, qui permet d'avoir en haute disponibilité, les backups, les ISOs, les Templates, lecture/écriture, et pleins d'autres options.



Windows Server

Installation

Installation d'un serveur Windows afin de déployer l'Active Directory et le partage de fichiers Samba. La version est un Windows Server 2022 en graphique.

Service AD

Le service a été installé via le menu de gestion du serveur et a été configuré :

- Nom de domaine jing.local
- Service DNS passif, pour aider les clients Windows à rejoindre le domaine.
- IP fixe 192.168.20.251
- Création de plusieurs comptes utilisateurs du domaine

Service Partage Samba

Installation du service via le gestionnaire du serveur et la configuration est la suivante :

- Partage d'un disque de 200 Go inter-clients.
- Attributions de droits en fonction du compte.

Assistant Nouveau partage

Sélectionner le serveur et le chemin d'accès au partage

Sélectionner un profil

Emplacement du partage

Nom de partage

Autres paramètres

Autorisations

Confirmation

Résultats

Serveur :

Nom du serveur	Statut	Rôle du cluster	Nœud propriétaire
WIN-5R9A1VBV63Q	En ligne	Non-cluster	

Emplacement du partage :

☒ Sélectionner par volume :

Volume	Espace libre	Capacité	Système de fichiers
C:	115 Go	127 Go	NTFS
D:	200 Go	200 Go	NTFS

L'emplacement du partage de fichiers sera un nouveau dossier du répertoire \Shares sur le volume sélectionné.

☐ Tapez un chemin personnalisé :

Windows Client

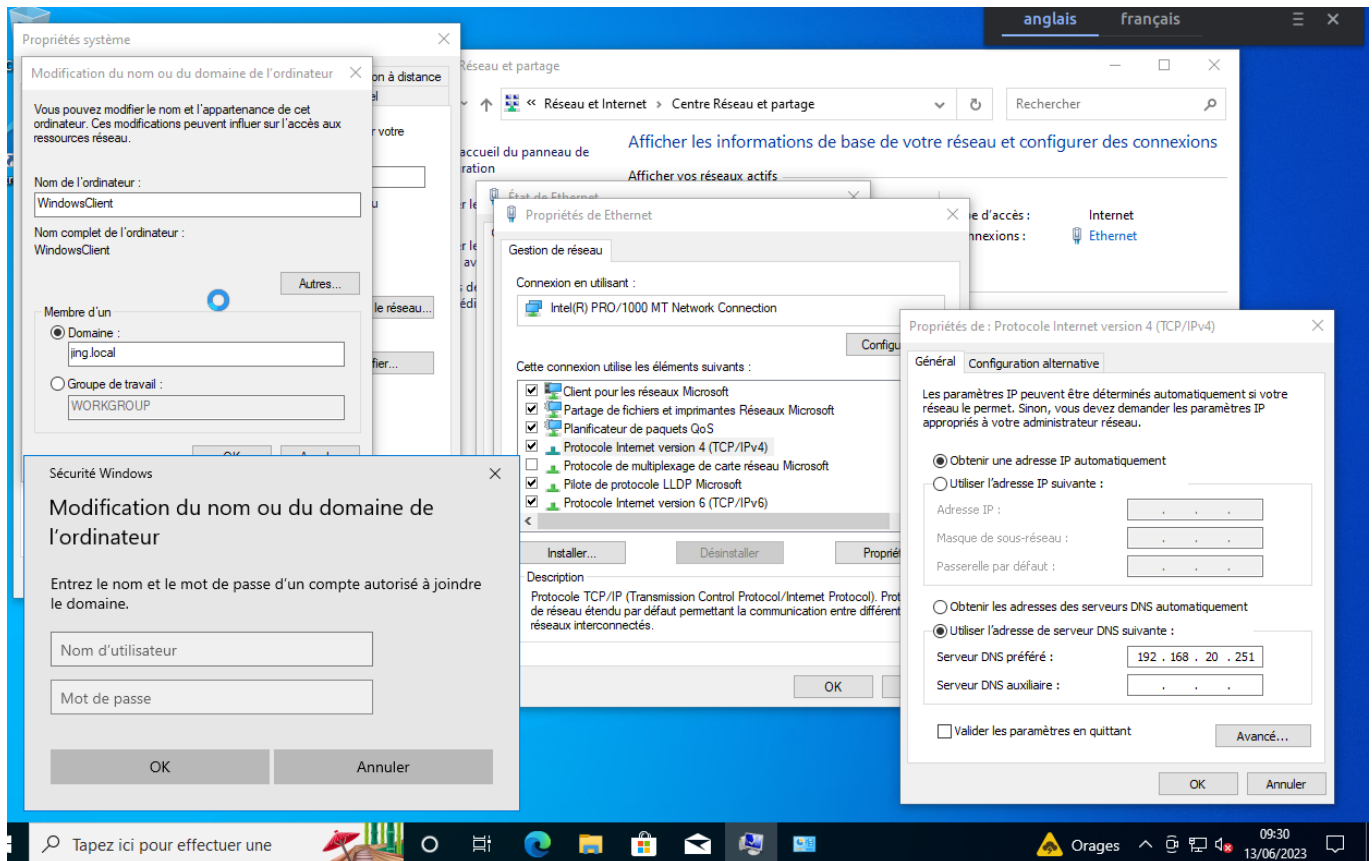
Installation

Installation de plusieurs clients Windows 10 configuré comme suit :

- Ajout au domaine 'jing.local'.
- Ajout du partage Samba.
- Blocage des comptes locaux clients.
- Gestion des droits dans l'AD.
- Adressage IP dynamique via DHCP.

Ajout à l'AD

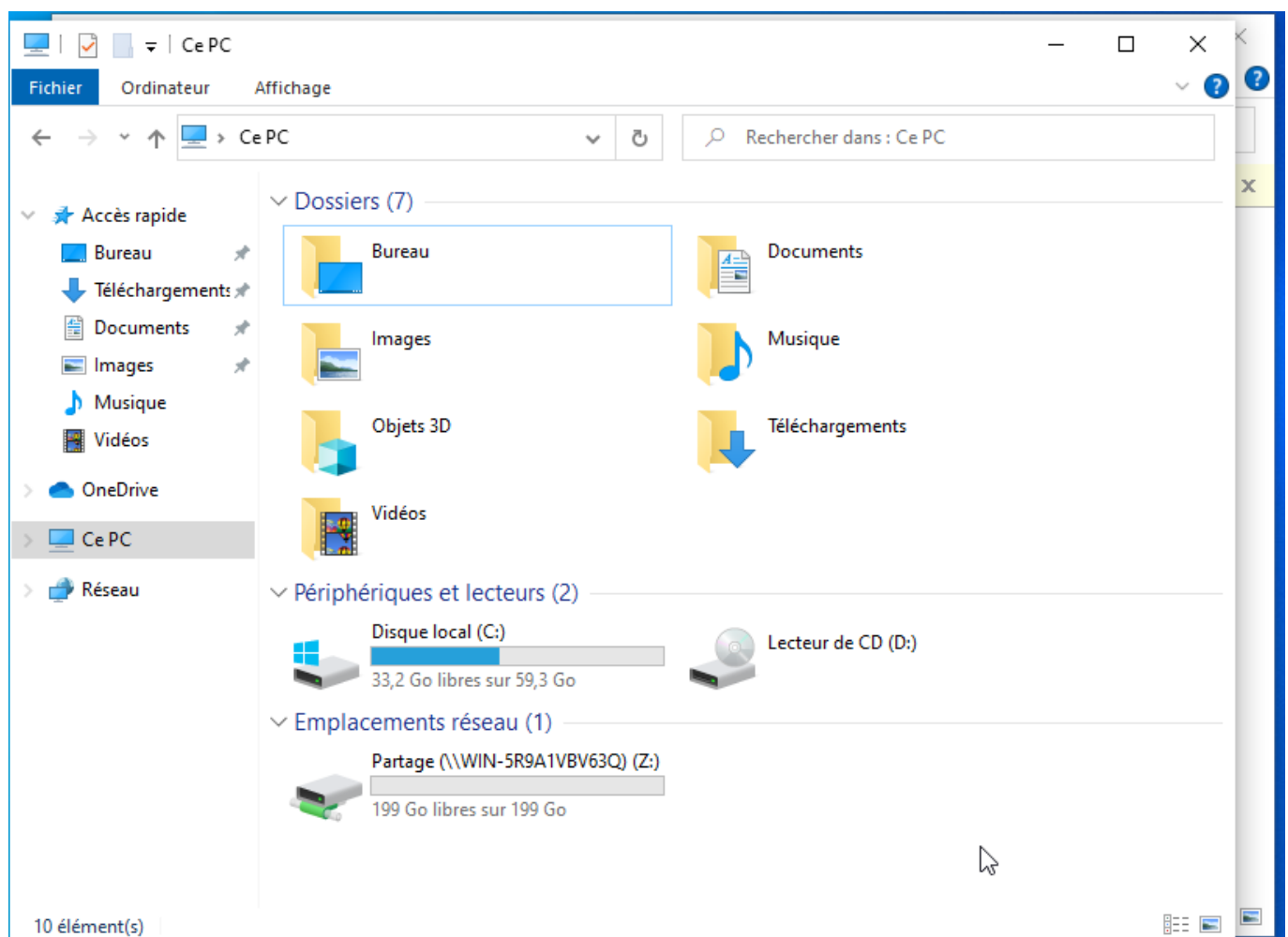
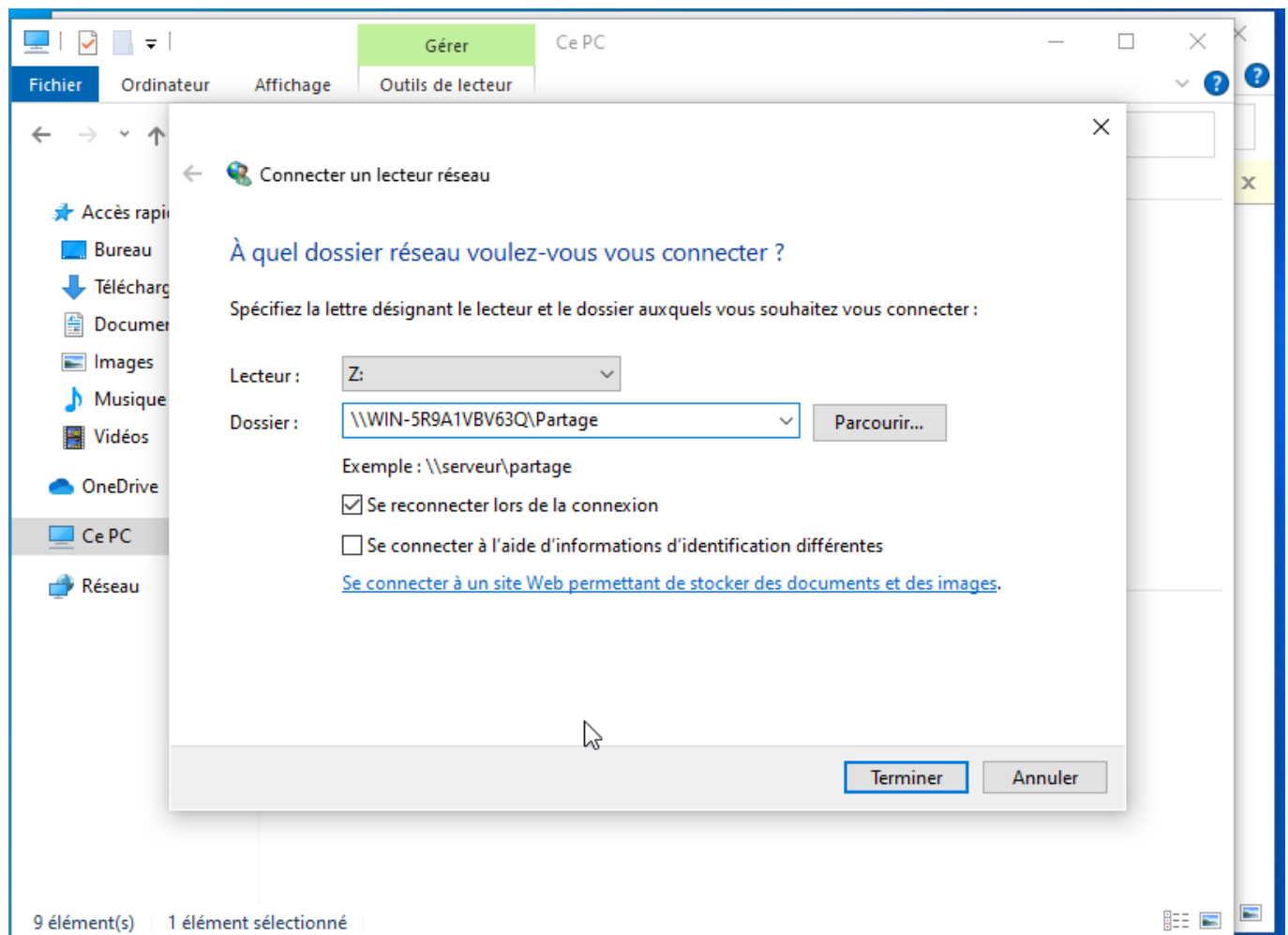
Pour joindre l'ordinateur au domaine j'ai été confronter à un problème ou le client ne pouvait pas atteindre le serveur AD. Pour résoudre le problème, j'ai dû mettre en tant que DNS privilégié l'IP du serveur AD :



Sur cette capture d'écrans, on peut voir l'adresse du DNS par défaut du client qui s'est changé par l'ip du serveur AD et par la suite le bon fonctionnement de la synchronisation.

Ajout du partage Samba

Pour ajouter le partage j'ai ajouté le lien vers le partage dans : Connecter un lecteur.



J'ai accès à tous les fichiers, je m'en suis par exemple servi plus tard pour mettre le fichier d'installation du GLPI Agent-Inventory pour Windows.

Portainer

Installation

Portainer a été containerisé à l'aide de docker dans une VM Debian 11. Son IP est -> 192.168.20.252.

```
sudo docker run -d -p 8000:8000 -p 9443:9443 --name portainer --restart=always -v /var/run/docker.sock:/var/run/docker.sock -v portainer_data:/data portainer/portainer-ce:latest
```

Je n'ai malheureusement pas pu ajouter de docker sur Portainer car il faut prévoir à l'avance l'ouverture de port pour pouvoir accéder au socket.

Podman

Installation

Installation d'un Podman debian11 accueillant un Scodoc :

```
1 sudo apt update
2 sudo apt install podman
3 podman run -d -it --name scodoc -p 80:80 -p 443:443 debian:11 /bin/bash
```

```
#Dans le container Scodoc
1 apt-get update
2 apt-get install -y nginx
3 echo "deb http://scodoc.org/repo bullseye main" >
/etc/apt/sources.list.d/scodoc.list
4 apt-get -y install gnupg
5 apt install wget
6 wget -O - https://scodoc.org/misc/scodoc-repo.gpg.key | apt-key add
-
7 apt-get update
8 apt-get install scodoc9
9 passwd scodoc
10 /opt/scodoc/tools/configure-scodoc9.sh
11 systemctl restart nginx
12 systemctl restart scodoc9
```

À la fin un crash apparaît en lien avec Postgres. Je n'ai pas le temps de résoudre le problème, mais le problème n'est pas en liens avec Podman.

LXC

Installation

Pour mettre en place une solution utilisant LXC, j'ai refait un serveur Scodoc :

Je me suis aidé de la doc officielle :

```
#Création container
1  sudo apt update
2  sudo apt install lxc
3  sudo lxd init
4  lxc launch images:debian/bullseye scodoc
5  lxc network attach ens18 scodoc eth0 eth0
6  lxc exec scodoc -- /bin/bash
```

```
#Dans le container Scodoc
1  apt-get update
2  apt-get install -y nginx
3  echo "deb http://scodoc.org/repo bullseye main" >
/etc/apt/sources.list.d/scodoc.list
4  apt-get -y install gnupg
5  apt install wget
6  wget -O - https://scodoc.org/misc/scodoc-repo.gpg.key | apt-key add
-
7  apt-get update
8  apt-get install scodoc9
9  passwd scodoc
10 /opt/scodoc/tools/configure-scodoc9.sh
11 systemctl restart nginx
12 systemctl restart scodoc9
```

GLPI

Installation

Installation d'un gestionnaire d'inventaire automatique j'ai choisi GLPI, car il permet une grande variété de choix, comme l'inventaire automatique natif (pas besoins de plugins tiers), supervisions, ticketing, etc.

```
services:
#MariaDB Container
mariadb:
  image: mariadb:10.7
  container_name: mariadb
  hostname: mariadb
  volumes:
    - /var/lib/mysql:/var/lib/mysql
```



```
env_file:
  - ./mariadb.env
restart: always

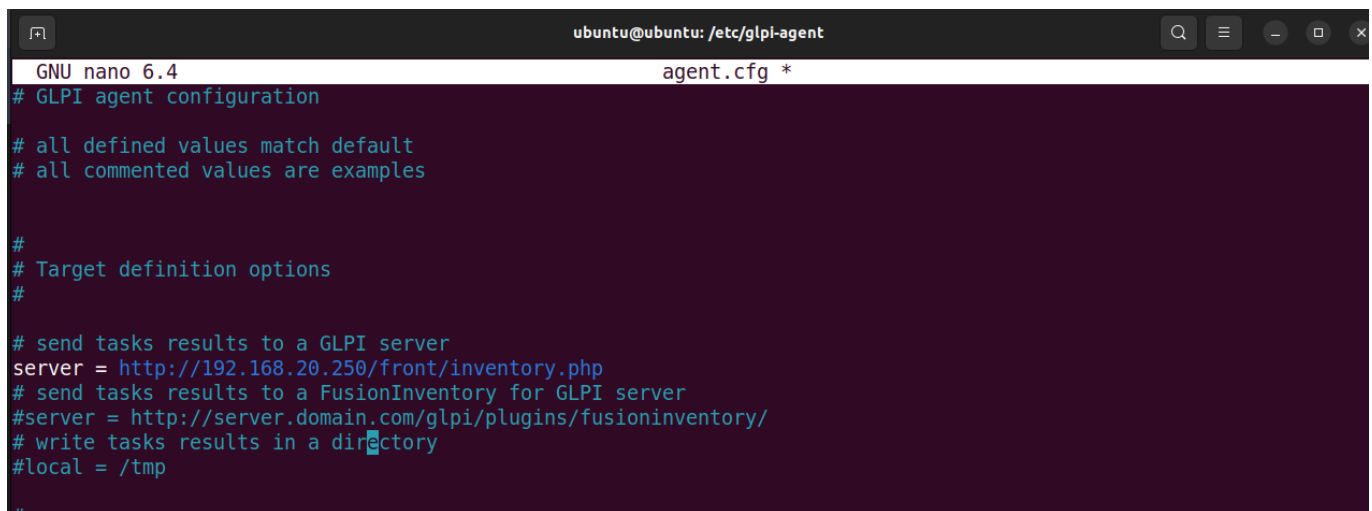
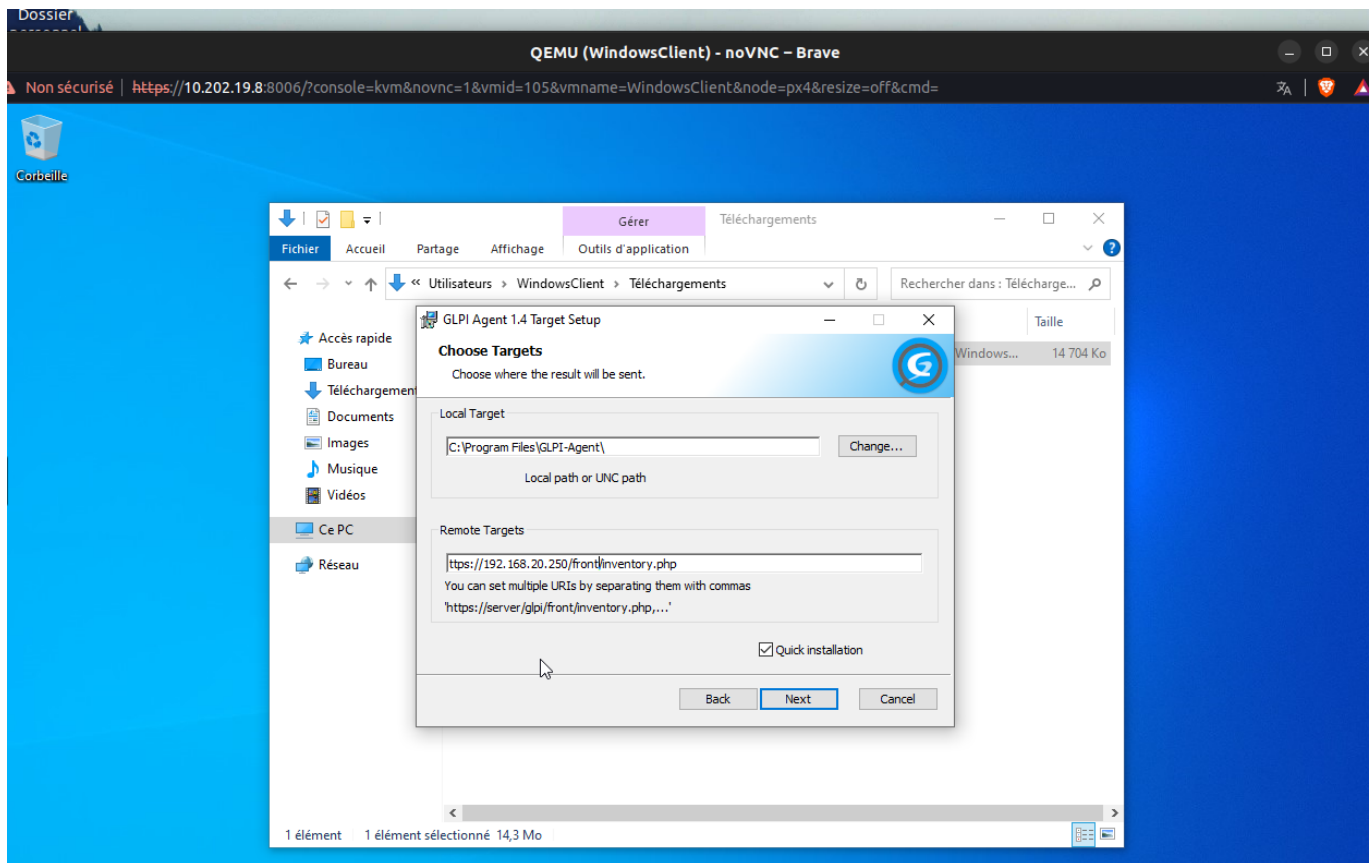
#GLPI Container
glpi:
  image: diouxx/glpi
  container_name : glpi
  hostname: glpi
  ports:
    - "80:80"
  volumes:
    - /etc/timezone:/etc/timezone:ro
    - /etc/localtime:/etc/localtime:ro
    - /var/www/html/glpi/:/var/www/html/glpi
  environment:
    - TIMEZONE=Europe/Paris
  restart: always
```

Utilisation d'un docker compose sur une VM Debian 11 pour la mise place du service. Il dispose du Container web GLPI et une base de donnée MariaDB.

Pour permettre de faire remonter les informations des VM automatiquement, j'ai du installé **GLPI-Inventory**.

```
#Connexion sur la machine via SSH
ssh machine@192.168.20.X
wget https://github.com/glpi-project/glpi-agent/releases/download/1.4/glpi-agent-1.4-linux-installer.pl #Téléchargement du packet
chmod +x glpi-agent-1.4-linux-installer.pl #Droit d'execution
./glpi-agent-1.4-linux-installer.pl #Installation de l'agent
#Lors de l'installation ajouter l'ip du serveur GLPI :
http://192.168.20.250/front/inventory.php
```

Installation des agents :



Une fois installer l'agent va remonter tous les jours.

GLPI

Accueil / Parc / Ordinateurs

Rechercher

Super-Admin
Entité racine (Arborescence)

Chercher dans le menu

Parc

Tableau de bord

Ordinateurs

Moniteurs

Logiciels

Matériels réseau

Périphériques

Imprimantes

Cartouches

Consommables

Téléphones

Baies

Châssis

PDU

Équipements passifs

Équipements non gérés

Câbles

Cartes SIM

Global

Assistance

Gestion

Outils

Administration

Configuration

Éléments visualisés

contient

régle

régle globale

groupe

Rechercher

Actions

NOM	STATUT	FABRICANT	NUMÉRO DE SÉRIE	TYPE	MODÈLE	SYSTÈME D'EXPLOITATION - NOM	LIEU	DERNIÈRE MODIFICATION	COMPOSANTS - PROCESSEUR
clientlinux-Standard-PC-i440FX-PIIX-1996		QEMU		QEMU	Standard PC (i440FX + PIIX, 1996)	Ubuntu 22.10		2023-06-14 10:32	Common KVM processor
glpi		QEMU		QEMU	Standard PC (i440FX + PIIX, 1996)	Ubuntu 22.10		2023-06-14 10:18	Common KVM processor
portainer		QEMU		QEMU	Standard PC (i440FX + PIIX, 1996)	Ubuntu 22.10		2023-06-14 10:18	Common KVM processor
ubuntu		QEMU		QEMU	Standard PC (i440FX + PIIX, 1996)	Ubuntu 22.10		2023-06-13 17:04	Common KVM processor
WIN-5R9A1VBV63Q		QEMU		QEMU	Standard PC (i440FX + PIIX, 1996)	Microsoft Windows Server 2022 Standard		2023-06-13 10:56	pc-i440fx-5.1
WindowsClient		QEMU		QEMU	Standard PC (Q35 + ICH9, 2009)	Microsoft Windows 10 Professionnel		2023-06-14 10:23	pc-q35-7.2

20 lignes / page

De 1 à 6 sur 6 lignes

Linux Client

Installation

Installation d'un client Linux, je lui ai fait rejoindre le domaine AD à l'aide du paquet : `realmd`

```
clientlinux@clientlinux-Standard-PC-i440FX-PIIX-1996:~$ sudo realm help
realm discover -v [realm-name]
Discover available realm

realm join -v [-U user] realm-name
Enroll this machine in a realm

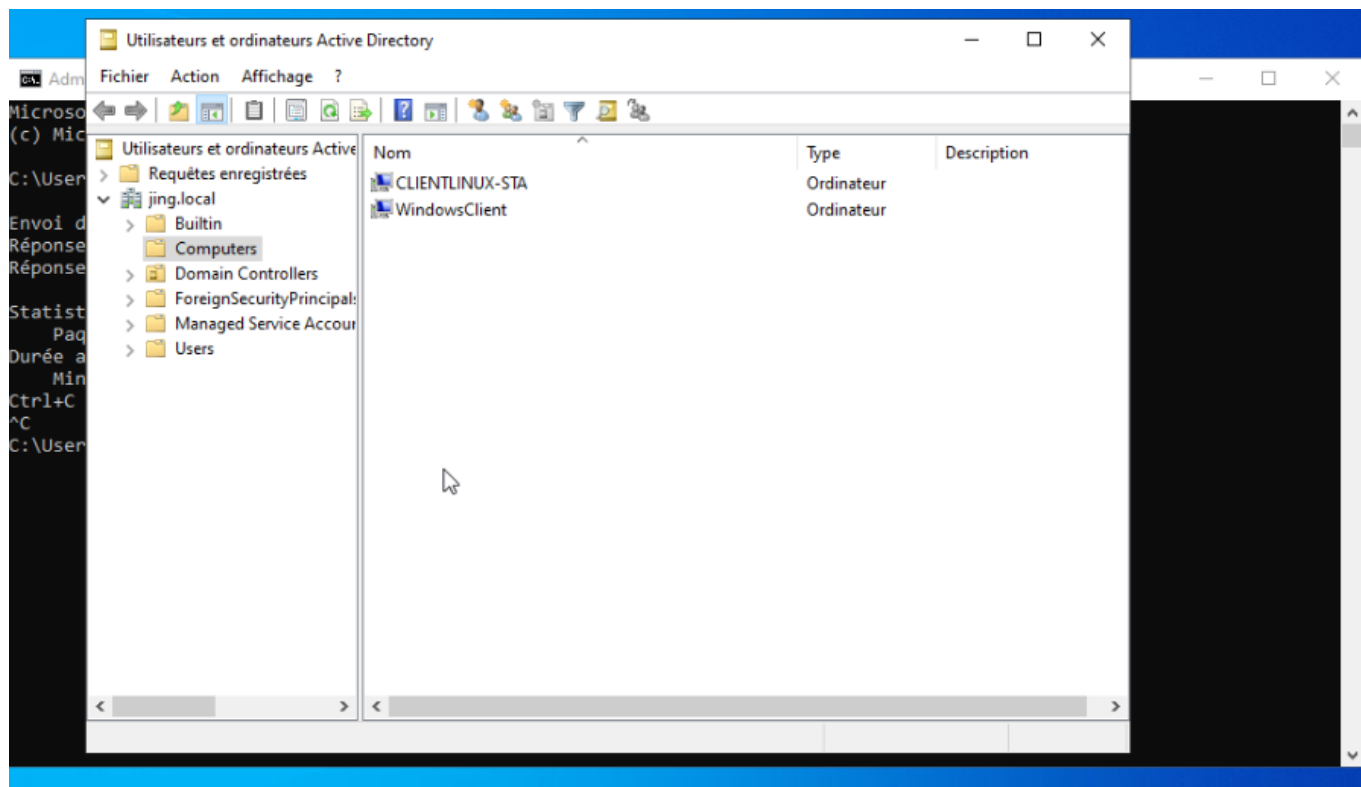
realm leave -v [-U user] [realm-name]
Unenroll this machine from a realm

realm list
List known realms

realm permit [-ax] [-R realm] user ...
Permit user logins

realm deny --all [-R realm]
Deny user logins
clientlinux@clientlinux-Standard-PC-i440FX-PIIX-1996:~$ sudo realm join jing.local -U administrateur
Password for administrateur:
```

Il est possible de voir sur le serveur AD le client linux qui remonte :



J'ai essayé de raccorder le partage samba au linux. Mais le système malgré la bonne configuration, car j'ai déjà réussi avec mon poste personnel.

Firewall Pfsense

Installation

Installation de la VM sur proxmox, il est en High Availability et me permet de séparer le réseau de la salle du réseau des proxmox afin d'éviter les mauvaises manipulations des autres groupes et d'isoler les serveurs du réseau initial. J'ai le configuré pour qu'il utilise le statique DHCP pour les serveurs principaux, et le reste des machines est sur le dhcp local du firewall. On a découvert qu'il fallait activer le DNS forwarder pour permettre au firewall de faire suivre les requêtes qu'ils recevaient de nos machines local vers le dns local ou cloud.

Gestion de projet

Nous avons eu différent type de problèmes comme des retards sur certaines composantes essentielles, par exemple :^

- Des problèmes comment savoir qu'elle tâche est le plus important au début, comme la mise en place de l'architecture réseau. Le firewall virtuel est arrivé 4 jours après le début de la SAE ce qui nous a fait perdre du temps dans l'adressage, dhcp et dns.
- Le firewall est virtualisé ce qui n'est pas la meilleure des choses, car si un nœud tombe est qu'il est dessus, il se coupe un cours temps avant de revenir ce qui isole les VM d'internet ce temps-là.
- J'ai déployé des services que je n'avais fait auparavant, donc on perd vite 1/2 jour à comprendre le fonctionnement et/ou comment l'installer proprement et fonctionnellement.

Sinon l'ambiance de groupe était bonne, lorsqu'il y avait besoins d'aide on s'entraidait le plus souvent.