PROJET DE FIN D'ANNÉE :

RÉFECTION DE LA SALLE INFORMATIQUE

Le projet que je vais vous présenter à lieu dans le cadre d'un BTS SIO option SISR, à l'IUMM de Beauzelle (31).

Il est porté par les 6 élèves de la promotion de 2024-2026 et a pour but la remise à niveau de la salle informatique.

Pour ce faire, il doit répondre à des conditions fixées par le rectorat mais aussi s'adapter aux besoins des élèves et enseignants et au matériel déjà présent sur place.

SOMMAIRE :

Table des matières

> *NB : Cette documentation a été complétée au fur et à mesure des 2 années de BTS. Pendant ce temps certains paramètres de l'infrastructure (IPs, ajout ou suppression de service, …) ont pu changer.*

I. Introduction

A. Les contraintes

Telle une simulation de ce que nous pourrons rencontrer lorsque nous travaillerons en entreprise, il faudra répondre aux contraintes imposées par le jury :

- Systèmes d'exploitation imposés : Linux et Windows
- Logiciel de virtualisation : HyperV, VMware
- Gestionnaire de base de données : MariaDB
- Authentification des utilisateurs : Active Directory
- Outil de supervision Réseau : Zabbix
- Outil de ticketing : GLPI
- Solution de redondance et de continuité de service
- Filtrage des flux : Pare-feu Fortinet et Switch Cisco
- Solution de sauvegarde : Ur-BackUp
- Logiciel de travail collaboratif : NextCloud
- Solution de répartition de charge : VLAN, redondance
- Solution de déploiement : WDS
- Automatisation : script de déploiement
- Solution de chiffrement : BitLocker
- Vlans
- Logiciel d'analyse de flux : Wireshark
- Prise de contrôle à distance sécurisé : IDrac, ILo, XClarity, BMC

Mais aussi aux contraintes liées au matériel présents sur place :

- Un serveur TERRA 7220 G3
- Un serveur HPE Gen 8
- Un serveur Lenovo
- Un serveur Dell R430
- Un switch Cisco
- Un pare-feu Fortinet

De plus, une problématique s'ajoute : nous devons travailler sur ce projet de façon discontinue (emploi du temps fixe) et nous ne pouvons pas interrompre les services mis en place et nécessaires au fonctionnement de la salle.

B. Les enjeux

La réfection de la salle informatique et plus précisément de la baie informatique, à pour enjeux de fournir aux futurs étudiants des services informatiques performants, sûrs, et optimisés.

Mais outre ce but principal, le projet nous permet de mettre en pratique les compétences et spécialités de chacun et de simuler une gestion de projet et un travail en équipe. Ces compétences sont nécessaires pour un futur technicien informatique et travailler ensemble nous permet de développer nos connaissances mais aussi nos capacités à enseigner ce que nous savons.

I. Hardware

A. Serveur Dell R430

CPU: XEON E5-2609 v4 1.70 GHz
RAM: 2x 32go + 2x 16go
DISK: 2x 120go + 2x 500go RAID 0

B. Serveur Lenovo

CPU: XEON E-2356G 3.20 GHz
RAM: 2x 32go
DISK: 480go + 2.4to RAID 0

C. Serveur HPE ProLiant DL380p Gen 8

CPU: XEON E5-2630 2.30 GHz x2
RAM: 2x 64go
DISK: 273 gib RAID 5 + 1788gib RAID 5

D. Serveur TERRA SERVER 7220 G3

CPU: Xeon Silver 4210R 2.40GHz x2
RAM: 4x 32go
DISK: RAID 0 1.36 tb + 1.3 tb

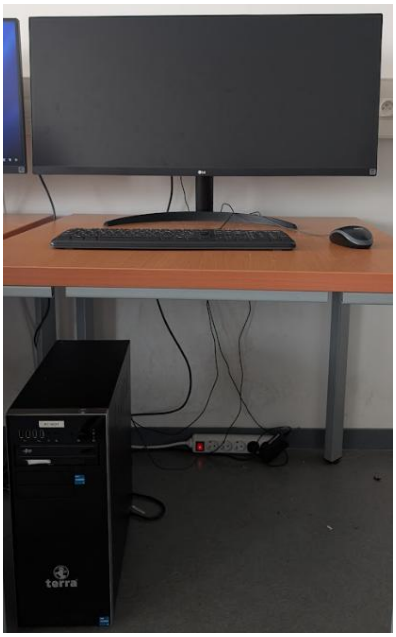
E. Switch Cisco

SG500X 48

F. Pare-feu Fortinet

FGT100D

G. Les postes



CPU: 11Gen Intel Core i5 11400 2.60go
RAM: 64go
DISK: 1to
Carte Graphique: NVDIA GeForce 4060

OS : Windows 11 éducation

H. IOT

1. Imprimante

Epson ET-5150

2. NAS

Synology DS923

III. Premiers constats

A. Brainstorming

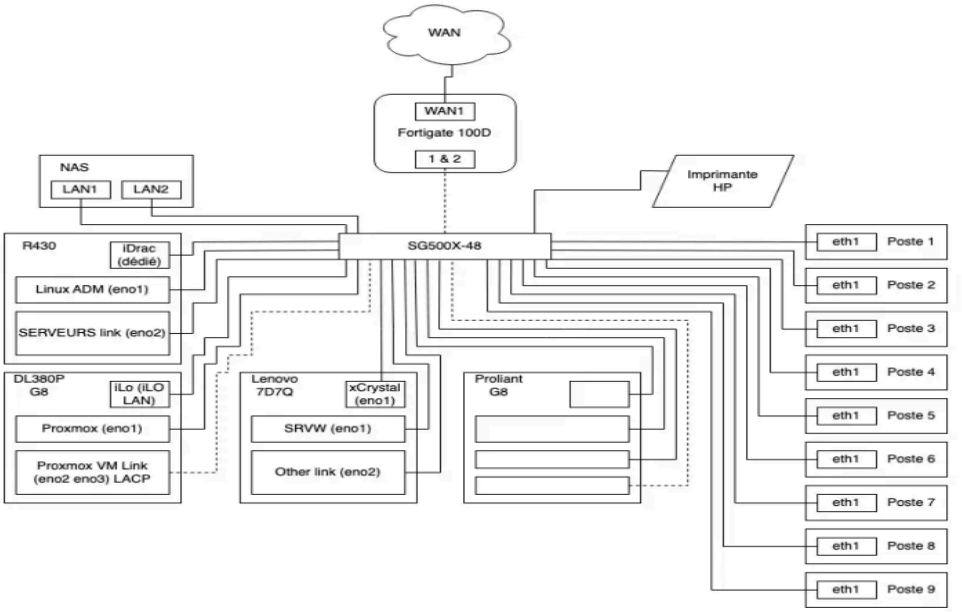
Depuis un an nous sommes dans cette salle près de 80% du temps. Nous avons éprouvé l'infrastructure réseau mais aussi les systèmes informatiques mis en place. C'est donc naturellement que nous avons opté pour un principe simple : mettre en place une infrastructure épurée, légère et avec une haute disponibilité.

De plus, nous devons faire face à un problème omniprésent dans ce domaine : la cybercriminalité. Bien que minimum dans notre contexte de salle informatique de l'IUMM de Beauzelle, la cybercriminalité est omniprésente et est perçue par certain comme un défi d'initiation en première année.

En gardant ces faits en tête (haute disponibilité, sécurité, légèreté), nos idées ont commencé à émerger : nous développerons notre infrastructure autour du Fortinet et grâce aux quatres serveurs que nous avons à disposition, nous en consacrerons un exclusivement pour assurer la redondance.

Pour concilier cette volonté de sécuriser la salle avec la praticité nécessaire au travail en équipe, nous avons fait le choix d'héberger un gestionnaire de mots de passe, Vaultwarden, sur un de nos serveurs. L'ensemble des identifiants et des clés sensibles y sont centralisés, ce qui nous permet d'utiliser des mots de passe robustes et distincts tout en les partageant de manière sécurisée entre les membres de l'équipe et les enseignants.

B. Schéma physique et adressage



1. Adressage VLAN ADMIN

NOM	HOSTNAME	GATEWAY	SUBNET	IP ADDRESS	VLAN
Fortigate 100D	CFAI-FW-100D	WAN	WAN	WAN	NONE
Fortigate 100D	CFAI-FW-100D	WAN	255.255.255.0	172.18.1.254	100 (ADMIN)
Lenovo 7D7Q	CFAI-SRVW-HPV	172.18.1.254	255.255.255.0	172.18.1.15	100 (ADMIN)
Lenovo 7D7Q	CFAI-XCLARITY-N4	172.18.1.254	255.255.255.0	DHCP PIN (172.18.1.5)	100 (ADMIN)
Nas Synology	CFAI-NAS-1				100 (ADMIN)
Poweredge R430	CFAI-SRVL-AIO	172.18.1.254	255.255.255.0	172.18.1.13	100 (ADMIN)
Poweredge R430	CFAI-IDRAC-N1	172.18.1.254	255.255.255.0	DHCP PIN (172.18.1.3)	100 (ADMIN)
Proliant Gen8 DL380P	CFAI-ILO-N2	172.18.1.254	255.255.255.0	DHCP PIN (172.18.1.4)	100 (ADMIN)
Proliant Gen8 DL380P	CFAI-PROXMOX-N2	172.18.1.254	255.255.255.0	172.18.1.14	100 (ADMIN)
SG500X-48	CFAI-SW-MAIN	172.18.1.254	255.255.255.0	172.18.1.1	100 (ADMIN)
Terra Server 7220 Gen 3	CFAI-BMC-N3	172.18.1.254	255.255.255.0	DHCP PIN (172.18.1.6)	100 (ADMIN)
Terra Server 7220 Gen 3	CFAI-SRVL-BACKUP	172.18.1.254	255.255.255.0	172.18.1.16	100 (ADMIN)

2. Adressage VLAN IOT

NOM	HOSTNAME	GATEWAY	SUBNET	IP ADDRESS	VLAN
Fortigate 100D	CFAI-FW-100D	WAN	255.255.255.0	172.18.2.254	200 (IOT)
Imprimante Epson	CFAI-IMPR-EPSON1	172.18.2.254	255.255.255.0		200 (IOT)

3. Adressage VLAN POSTES

NOM	HOSTNAME	GATEWAY	SUBNET	IP ADDRESS	VLAN
Fortigate 100D	CFAI-FW-100D	WAN	255.255.255.0	172.18.3.254	300 (POSTES)
Poste de travail	CFAI-POSTE-1	172.18.3.254	255.255.255.0	DHCP	300 (POSTES)
Poste de travail	CFAI-POSTE-2	172.18.3.254	255.255.255.0	DHCP	300 (POSTES)
Poste de travail	CFAI-POSTE-3	172.18.3.254	255.255.255.0	DHCP	300 (POSTES)
Poste de travail	CFAI-POSTE-4	172.18.3.254	255.255.255.0	DHCP	300 (POSTES)
Poste de travail	CFAI-POSTE-5	172.18.3.254	255.255.255.0	DHCP	300 (POSTES)
Poste de travail	CFAI-POSTE-6	172.18.3.254	255.255.255.0	DHCP	300 (POSTES)
Poste de travail	CFAI-POSTE-7	172.18.3.254	255.255.255.0	DHCP	300 (POSTES)
Poste de travail	CFAI-POSTE-8	172.18.3.254	255.255.255.0	DHCP	300 (POSTES)
Poste de travail	CFAI-POSTE-9	172.18.3.254	255.255.255.0	DHCP	300 (POSTES)

4. Adressage VLAN SERVEURS

NOM	HOSTNAME	GATEWAY	SUBNET	IP ADDRESS	VLAN
Fortigate 100D	CFAI-FW-100D	WAN	255.255.255.0	172.18.5.254	500 (SERVEURS)
Lenovo 7D7Q	CFAI-SRVW-HPV	172.18.5.254	255.255.255.0	172.18.5.15	500 (SERVEURS)
Lenovo 7D7Q (AD-BDC)	SRV-AD-BDC	172.18.5.254	255.255.255.0	172.18.5.2	500 (SERVEURS)
Lenovo 7D7Q (AD-PDC)	SRV-AD-PDC	172.18.5.254	255.255.255.0	172.18.5.1	500 (SERVEURS)
Poweredge R430	CFAI-SRVL-AIO	172.18.5.254	255.255.255.0	172.18.5.13	500 (SERVEURS)
Poweredge R430 (GLPI)	CFAI-SRVL-GLPI	172.18.5.254	255.255.255.0	172.18.5.24	
Poweredge R430	CFAI-SRVL-NXTC	172.18.5.254	255.255.255.0	172.18.5.23	500 (SERVEURS)

(NextCloud)					
Poweredge R430 (Zabbix)	CFAI-SRVL-ZBX	172.18.5.254	255.255.255.0	172.18.5.25	500 (SERVEURS)
Proliant Gen8 DL380P	CFAI-PROXMOX-N2	172.18.5.254	255.255.255.0		500 (SERVEURS)

C. Reset et paramétrages

Pour le contrôle à distance des serveurs nous avons choisi d'utiliser le système de prise de contrôle natif des serveurs : iDrac, xClarity et iLo.

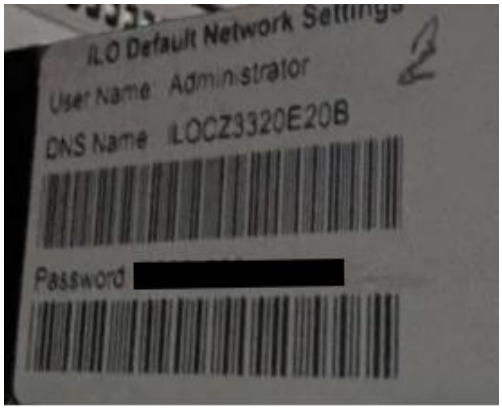
Cependant ces systèmes n'ont jamais été utilisés ou paramétrés, nous avons eu besoin de réinitialiser et de récupérer les IP pour pouvoir nous y connecter via une page web.

1. iLo

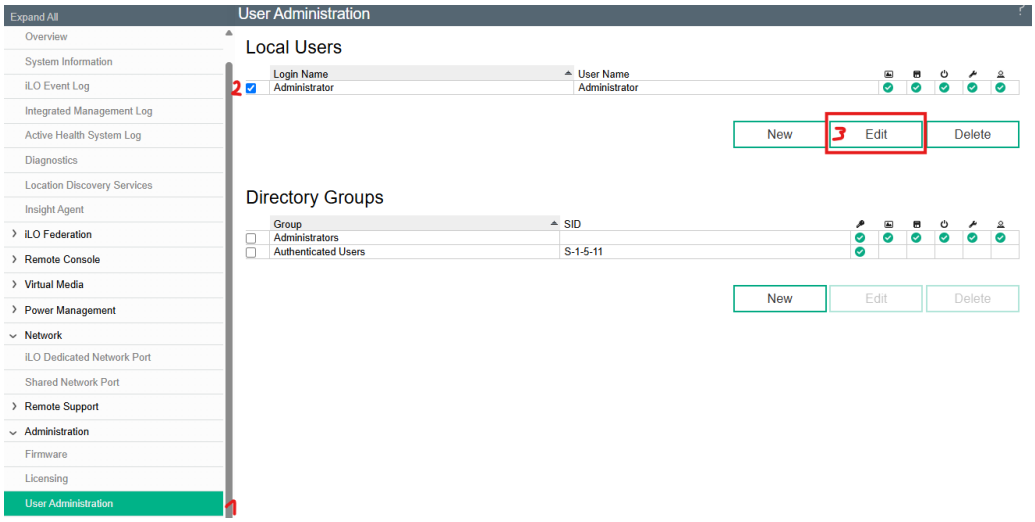
Pour configurer iLo, il faut aller aussi dans le BIOS, un message s'affiche en disant d'appuyer sur F8 pour entrer dans la configuration de iLo.

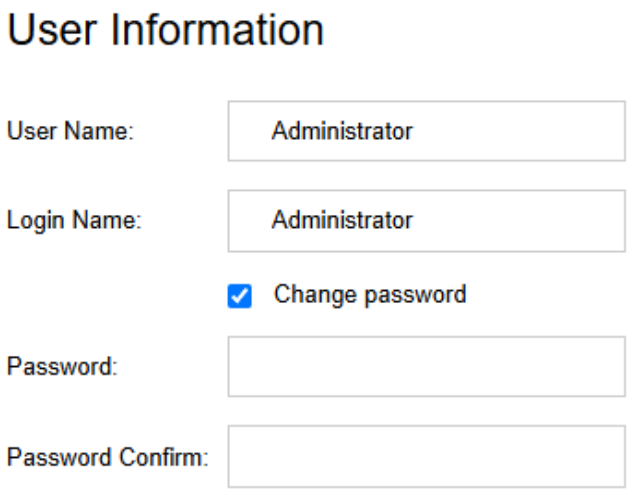
Mettre l'attribution d'IP par DHCP.

Une fois dedans nous avons réinitialisé le service car même une fois l'IP connue, le mot de passe n'était pas celui par défaut.



Sur le site nous pouvons maintenant changer le mot de passe et l'identifiant.



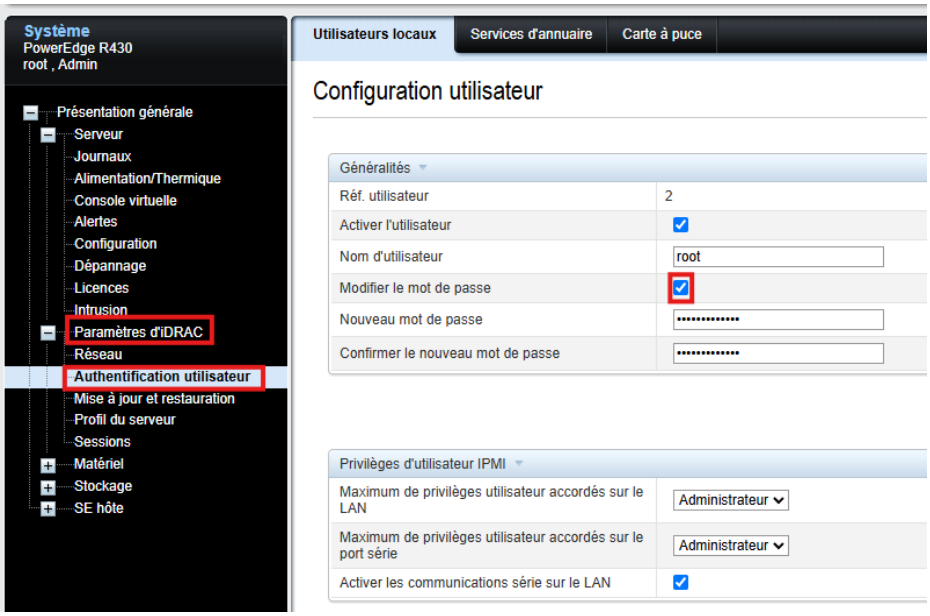


2. iDrac

Sur le serveur qui possède iDrac, la procédure est simple, tout se fait à partir de l'écran, naviguer dessus se fait avec les flèches "<" et ">" présentes dans l'image 4.

Nous sommes sur un IDRAC 8, les identifiants et mot de passe par défaut sont :

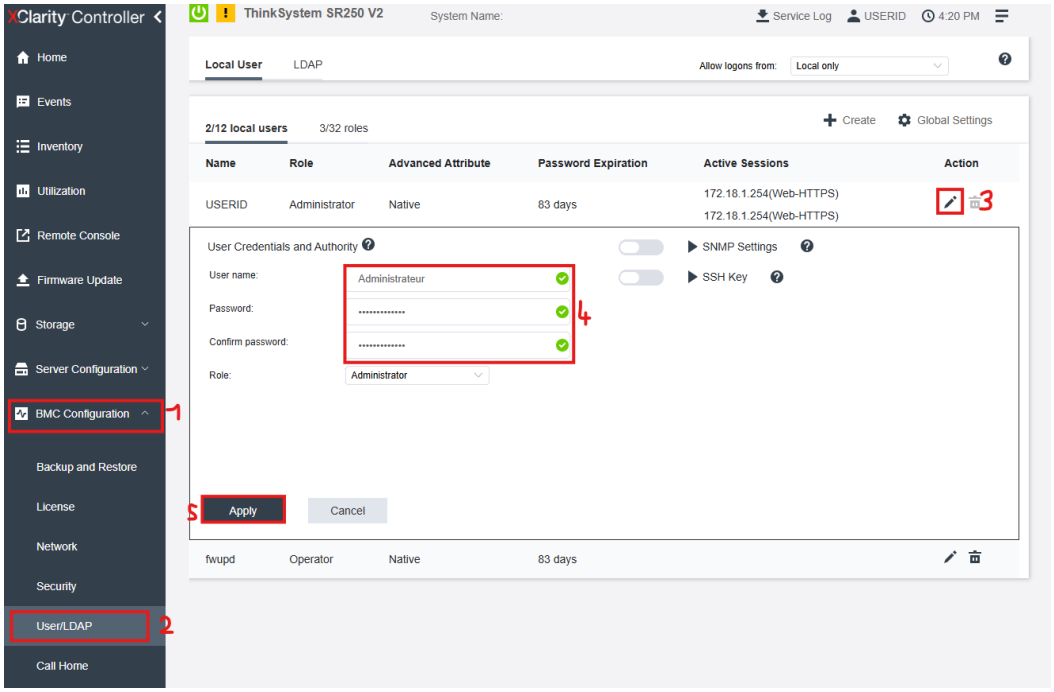
Nous pouvons donc aller sur l'interface WEB avec les identifiants par défaut et changer le mot de passe :



3. XClarity

Pour récupérer l'IP de xClarity nous avons dû aller dans le BIOS et faire une demande de récupération d'adresse par le DHCP.

Sur le site nous changeons le mot de passe et l'identifiant :



4. BMC

Comme pour les autres serveurs, pour configurer BMC nous avons dû aller dans le BIOS (F2) du serveur puis aller dans :

- Server Management,
- BMC LAN configuration.

Nous pouvons d'ici changer les paramètres IP.

Ensuite dans :

- User Configuration

User ID administrator (root) et ici nous avons pu modifier le mot de passe (attention : clavier en qwerty).

5. Switch

```
username sio password encrypted 1c6d099546a5b225358914bb535d6f5c488d2e0b privilege 15
username sio2 password encrypted 146006166e86b2d52fcd86e28e692f801fe9e741 privilege 15
username cisco password encrypted d50caa2bb3ef5bb6c8699db0f454c8cdce3a041d privilege 15
username orichet password encrypted 2a05237ed600ca26f1361402bb1c5121d49af501 privilege 15
username slottin password encrypted d65f24e0c2c2400f72f11bd9fd0d7b215a14266b privilege 15
ip ssh server
```

Nous avons créé plusieurs utilisateurs : les enseignants et les élèves (chaque année à un compte). L'utilisation de compte défini permet de tracer les actions et une meilleure lecture des logs.

NB : Nous n'avons pas eu besoin de réinitialiser le switch car Mr Richet notre enseignant nous a donné les identifiants. En cas de besoin, le switch SG500 se reset de cette façon :

- *Déconnecter le switch du réseau.*
- *Allumer le switch.*
- *Appuyer + de 10 secondes sur le bouton reset avec un trombone.*

Les vlans :

Au nombre de 5 avec chacun un but particulier :

- VLAN 100 : VLAN administrative
- VLAN 200 : VLAN pour IOT
- VLAN 300 : VLAN pour les ordinateurs élèves
- VLAN 400 : VLAN pour le déploiement (WDS)
- VLAN 500 : VLAN serveur

```
(config)#vlan 100
(config-vlan)#name ADMIN
(config-vlan)#exit
(config)#exit
```

Puis nous avons attribué des ports précis aux différents VLANs.

```
100        ADMIN            Po1-2        gi1/1/25-28,              S
                                         gi1/1/37-38
200         IOT             Po1-2                                  S
300       POSTES            Po1-2            gi1/1/1-12            S
400        ELSE             Po1-2                                  S
500      SERVEURS           Po1-2           gi1/1/13-14            S
```

Pour finir et permettre le passage des différents sous réseaux jusqu'à notre pare-feu et notre interface WAN, nous avons configuré le port du WAN en mode trunk.

```
interface Port-channel1
 switchport trunk allowed vlan add 100,200,300,400,500
!
interface Port-channel2
 description PROXMOX-N2
 switchport trunk allowed vlan add 100,200,300,400,500
!
```

Pour nous permettre de travailler sur le nouveau réseau tout en conservant l'ancien ou se situe encore l'Active Directory en production, nous avons, le temps de la transition, laisser l'ancien réseau en VLAN 1, ce qui nous permet de passer d'un réseau à l'autre en fonction de nos heures de classe. La transition se fait en deux lignes :

```
switch-sg500x(config)#interface range GigabitEthernet1/1/1-12
switch-sg500x(config-if-range)#$ccess vlan 1
```

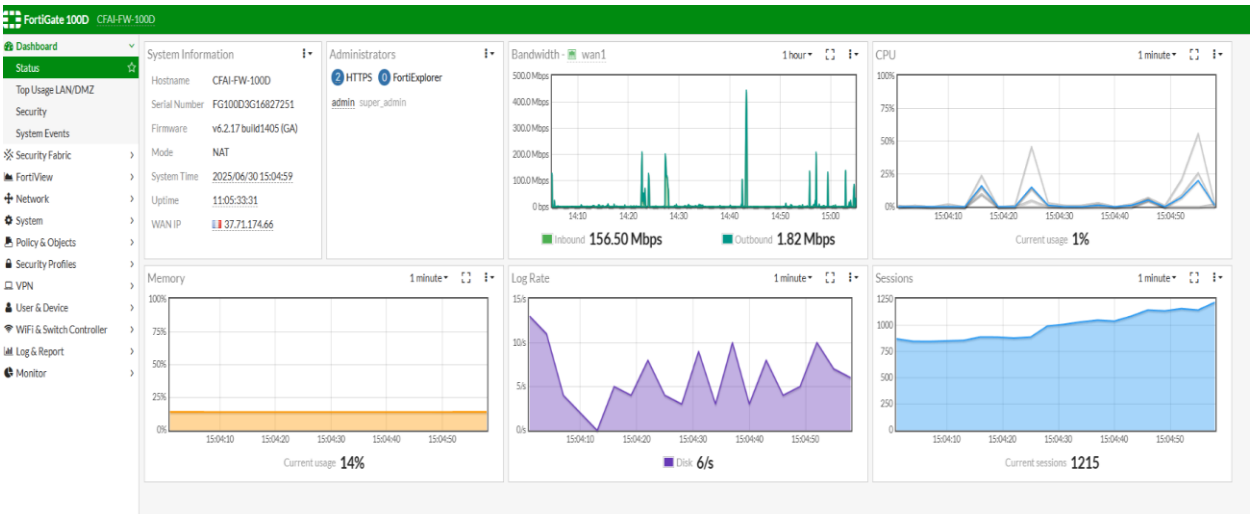
Et si un élève perd sa connexion internet à ce moment-là, un simple " #ipconfig /renew " sur l'invite de commande Windows permet de récupérer la nouvelle ip du réseau.

6. Pare-feu

Pour partir sur une configuration propre nous avons choisi de réinitialiser le fortigate. Pour cela il faut l'allumer, puis appuyer sur le bouton reset jusqu'à ce que la LED power clignote.

Une fois le reset fait, nous nous sommes branchés sur le pare-feu avec un câble ethernet sur le port management et nous avons passé l'ordinateur sur le même réseau que le FortiGate (= staging).

Une fois sur le même réseau et branché, nous pouvons accéder au pare-feu. D'ici nous ferons tous les paramétrages futurs, nous n'utiliserons pas de CLI.



IV. Les services

Pour répondre du mieux possible aux contraintes imposées et pour exploiter entièrement le matériel mis à disposition, nous avons réparti les différents services de la façon qui va suivre.

Ce choix a été fait en prenant en compte les besoins en ressources des services à installer :

- L'Active Directory : Le cœur de notre infrastructure.
  Authentification des utilisateurs, gestion des droits d'utilisateurs, DNS. Ce sont des services clés qui ont besoin d'une haute disponibilité et c'est pour cela que nous utiliserons le serveur Lenovo pour l'héberger.
- Gestion de parc et logiciels collaboratifs : Forte demande de stockage mais ils proposent des services qui ne sont pas essentiels au fonctionnement de notre parc.
  La surveillance du réseau avec Zabbix, la gestion du parc informatique avec GLPI et un service collaboratif avec Nextcloud entraîne une forte demande en RAM et du stockage pour accueillir du partage de fichier, bien que d'expérience nous pensons que le service NextCloud ne sera que peu utilisé.
- Serveur de back-up : crucial s'il arrive un problème sur les serveurs, le serveur de back-up est là dans le cas d'une panne matériel. Il prendra alors le relais. Il a besoin d'une grosse capacité de stockage et un processeur puissant pour pouvoir prendre le relais de n'importe quel serveur. Nous avons choisi de mettre ce service sur le serveur Terra qui est un serveur difficile à prendre en main et peu ergonomique : en cas de besoin il fera tourner ce qu'il faut, mais nous n'aurons pas besoin de l'utiliser quotidiennement.

A. Contrôle à distance

Dans le cadre de la gestion à distance des serveurs, nous avons mis en œuvre plusieurs solutions de prise de contrôle. Celles-ci sont indispensables pour assurer la maintenance préventive, le diagnostic rapide des incidents, ainsi que la gestion quotidienne des machines, même en dehors des heures d'ouverture ou en cas de panne critique.

1. Interfaces de gestion hors bande (OOB)

Chaque serveur dispose de sa propre interface de gestion hors bande (Out-Of-Band Management), indépendante du système d'exploitation :

- iDrac (Integrated Dell Remote Access Controller) pour le serveur Dell.

- iLo (Integrated Lights-Out) pour le serveur HP Proliant.
- XClarity Controller pour le serveur Lenovo.
- BMC (Baseboard Management Controller) pour le serveur Terra.

Ces interfaces permettent d'interagir directement avec le matériel du serveur, même lorsque celui-ci est éteint ou que le système d'exploitation est inopérant. Elles donnent accès à une console distante complète (équivalente à un écran physique), à la gestion de l'alimentation (allumage/extinction/forçage), ainsi qu'à des fonctionnalités avancées comme :

- Le montage à distance d'images ISO pour réinstaller un système d'exploitation sans support physique,
- La surveillance du matériel (températures, ventilateurs, alimentation, disques, etc.),
- La capture des logs matériels pour les analyses post-incident.

Afin de garantir la sécurité de ces accès critiques, chaque interface est configurée avec une adresse IP statique dédiée sur le VLAN ADMIN, totalement isolé du reste du réseau pédagogique et des VLAN utilisateurs. L'accès à leur interface nécessite une authentification dont les utilisateurs disposant des droits adéquats peuvent y accéder, via une liaison sécurisée.

2. Prise en main logicielle (in-band)

En complément des interfaces OOB, nous avons également mis en place une solution de prise de contrôle logicielle, principalement utilisée pour l'administration de l'environnement serveur et les démonstrations pédagogiques :

- RDP (Remote Desktop Protocol).

Cet accès est principalement utilisé pour :

- L'installation de rôles ou services.
- Les mises à jour logicielles,
- Les diagnostics système (journal d'événements, vérification de performances, etc.),
- Les sessions pédagogiques ou les manipulations par les étudiants en environnement virtualisé.

L'utilisation du RDP présente plusieurs avantages significatifs, notamment sa légèreté. Il optimise la bande passante en transmettant principalement les commandes d'affichage plutôt que le contenu graphique complet. Cela permet une prise en main fluide même sur des connexions réseau peu performantes ou instables, tout en minimisant la charge sur les serveurs et les postes clients.

L'accès RDP nécessite une authentification avec un compte ayant les droits d'administration. L'ensemble des connexions est journalisé, permettant une traçabilité complète des actions.

B. Windows Server 2025

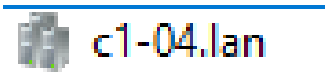
C. Active Directory

Active Directory (AD) est un service d'annuaire créé par Microsoft. Il permet une gestion centralisée, sécurisée et évolutive des ressources et des utilisateurs.
C'est une base de données centralisée qui nous permet de contrôler les droits des différents utilisateurs, gérer leurs mots de passe et leurs comptes. Il permet aussi de créer un domaine, ici nous avons choisi de nommer notre domaine "C1-04.lan" soit le nom de la salle où nous travaillons.

Pour conserver une haute disponibilité et une solution en cas de panne nous avons fait un AD primaire nommé PDC, et un AD secondaire nommé BDC. Les serveurs sont identiques et fonctionnent en même temps.

1. Domaine

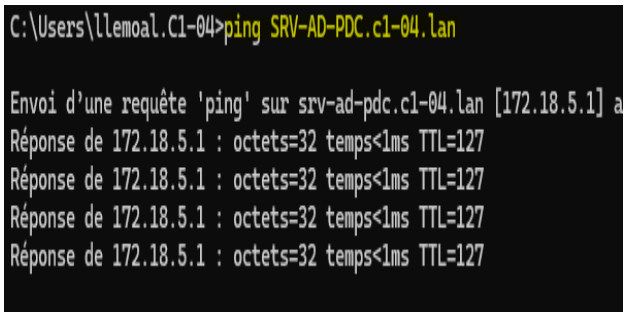
Un domaine donc est un groupe dans lequel sont rassemblés tous les ordinateurs. Toutes les informations liées à ce domaine seront stockées dans l'Active Directory.



Lorsque nous créons un domaine il faut aussi que nous créions un DNS. C'est le service qui va "associer" les adresses IP des différentes machines à leur nom.

Par exemple :

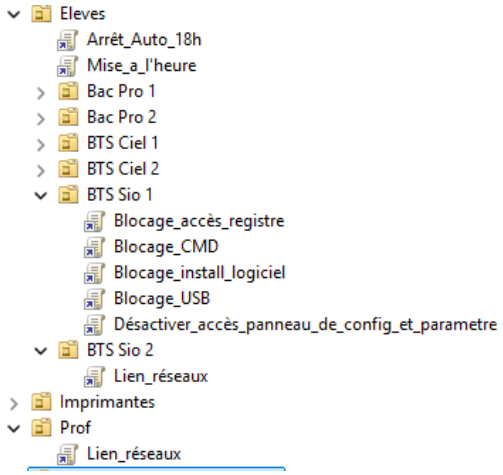
Nous pouvons ping la machine qui s'appelle SRV-AD-PDC aussi bien avec son nom (hostname) qu'avec son IP, c'est le service DNS qui permet cela.

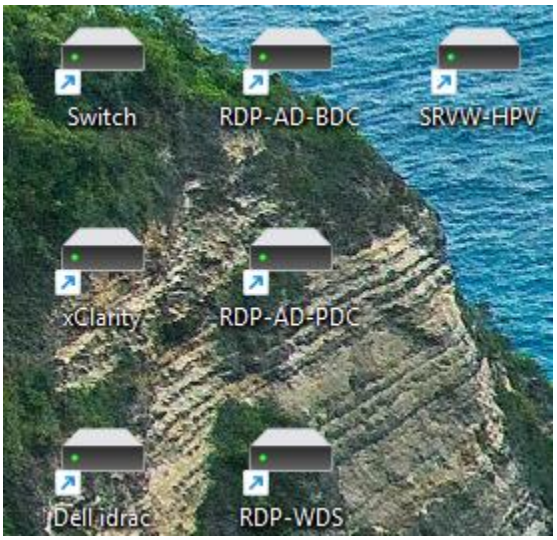


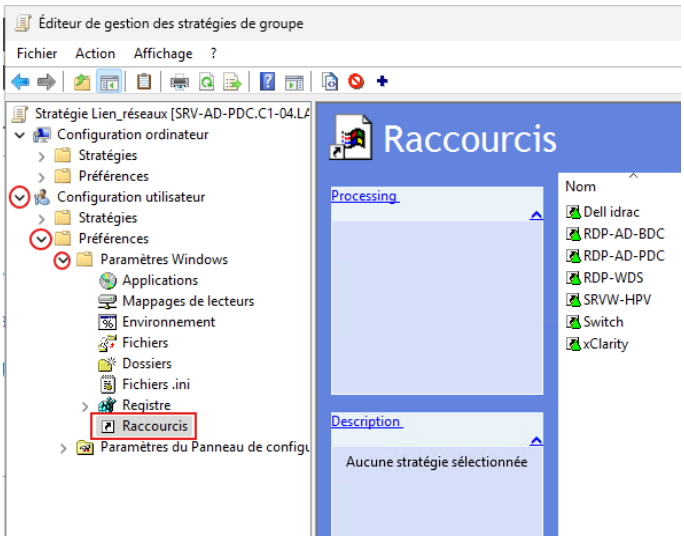
2. GPO

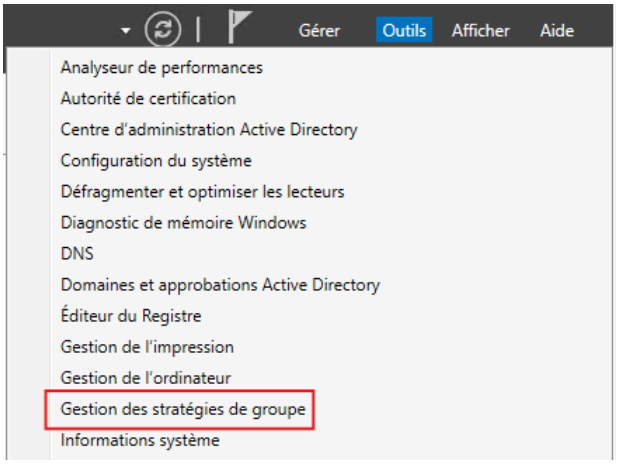
Les GPO (Group Policy Object), ou objet de stratégie de groupe sont des règles que nous définissons.
Grâce aux GPO nous pouvons interdire l'accès à l'invite de commande à certains utilisateurs, ou créer des raccourcis pour d'autres.

Nous avons défini les règles selon deux grands groupes : les premières années et les deuxièmes années. De plus, deux autres règles sont communes aux deux groupes : les ordinateurs s'éteignent à 18h après un message de prévention, et l'heure de tous les postes sont synchronisés au serveur qui héberge l'AD.



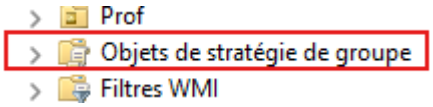




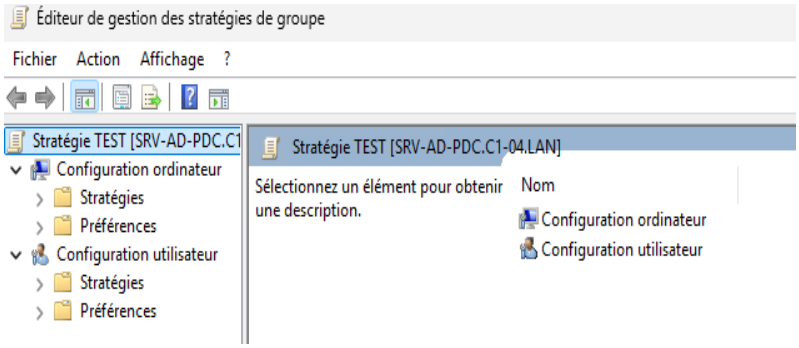


Pour créer une GPO :

- Outils.
- Gestion des stratégies de groupe.
- Défiler l'arborescence jusqu'à Objets de stratégie de groupe.



- Clic droit dans la fenêtre et faire "nouveau".
- Nommer la stratégie, faire "Ok", puis clic droit sur la stratégie et faire "Modifier".



- Une fois la GPO créer, faire clic droit sur l'OU (Unité d'Organisation) : lier une GPO.

Il existe plusieurs types de GPO : celles qui s'affectent aux utilisateurs ou celles s'affectent aux machines.

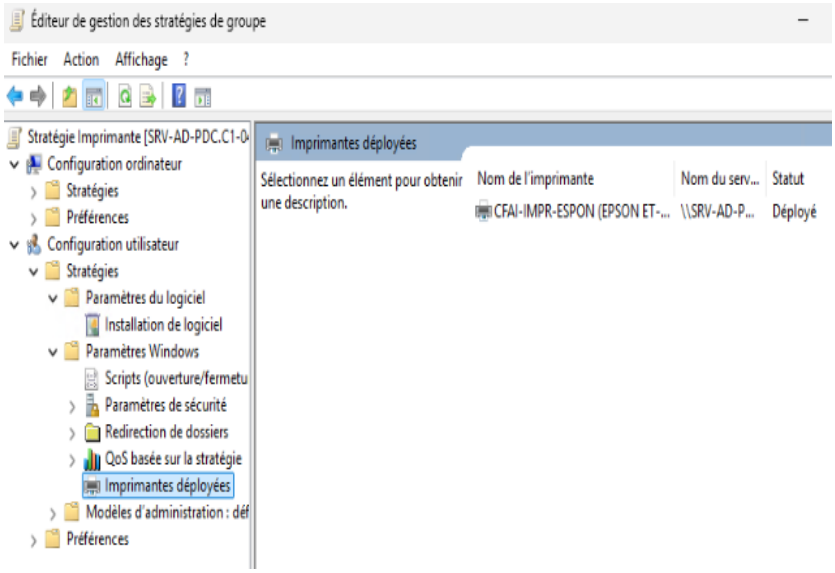
a. GPO machine

- Ne pas voir le dernier utilisateur
- Heure synchro avec l'AD

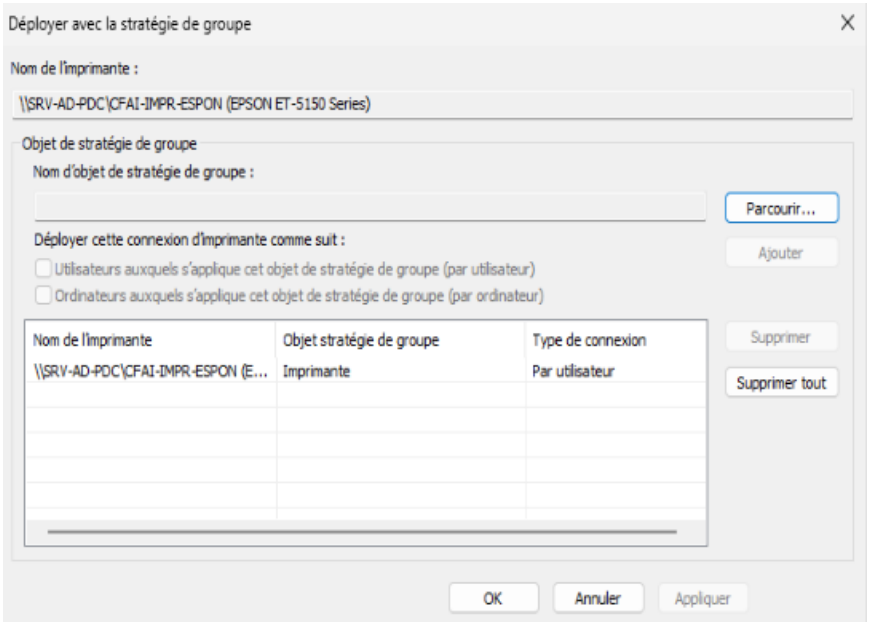
b. GPO utilisateur

Nous prendrons l'exemple de la GPO "imprimante" qui a besoin d'être utilisable sur tous les ordinateurs mais pas par tout le monde.

- Créer une GPO appelée "imprimante" comme vu précédemment et l'assigner à une OU (SIO 2 et Prof pour notre cas).
- Éditer la GPO et ajouter l'imprimante.



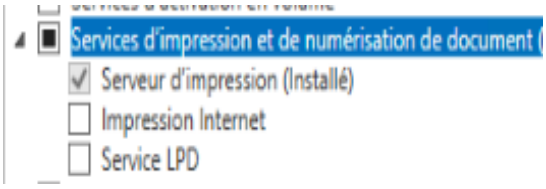
- Retourner sur printmanagement.msc.
- Clic droit sur l'imprimante, déployer avec la stratégie de groupe.



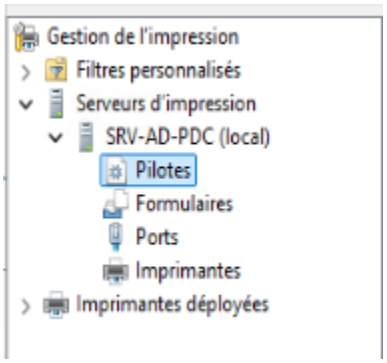
3. Autres services

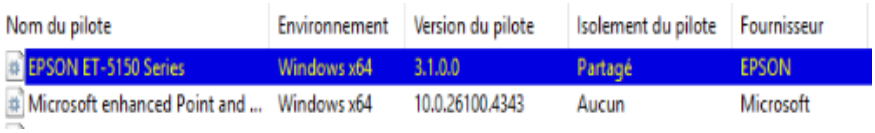
Services d'impression

Utile pour pouvoir ajouter une imprimante de façon généralisée et ne pas avoir à le faire sur chaque ordinateur du domaine, nous avons ajouté l'outil Services d'impression qui permet l'ajout automatique pour chaque utilisateur et qui permet la gestion des droits d'impression.



- Installer le pilote de l'imprimante sur le serveur (ici un pilote Epson trouvé sur le site officiel).
- Faire Win+R et rentrer : printmanagement.msc
- Ajouter le pilote.





Nom du pilote	Environnement	Version du pilote	Isolement du pilote	Fournisseur
EPSON ET-5150 Series	Windows x64	3.1.0.0	Partagé	EPSON
Microsoft enhanced Point and ...	Windows x64	10.0.26100.4343	Aucun	Microsoft

- Ajouter l'imprimante sur le serveur et sélectionner l'option ajouter une imprimante IPP, TCP/IP (2eme option).
- Cocher détecter automatiquement le pilote à utiliser

L'imprimante apparaît dans les périphériques ajoutés :

Nom de l'imprimante	Statut de la file...	Travau...	Nom du serveur	Nom du pilote
CFAI-IMPR-ESPON (EPSON ET-5150 Series)	Prêt	0	SRV-AD-PDC (l...	EPSON ET-5150 Series
CFAI-IMPR-ESPON (EPSON ET-5150 Series) sur SRV-AD-PDC (redirection de 3)	Prêt	0	SRV-AD-PDC (l...	EPSON ET-5150 Series

Maintenant il faut créer une GPO pour la déployer (cf GPO)

D. Ubuntu - Linux

Basé sur un noyau UNIX, Ubuntu est un OS libre de droit et léger. Nous avons choisi cet OS car nous avons eu un problème de compatibilité entre notre serveur et debian. Comme Ubuntu est basé sur Debian, les commandes ne changent que peu. Il est en revanche plus accessible pour les débutants, ce qui est un avantage pour un environnement de cours où des élèves peuvent ne jamais avoir travaillé sur du Linux.

1. Configuration

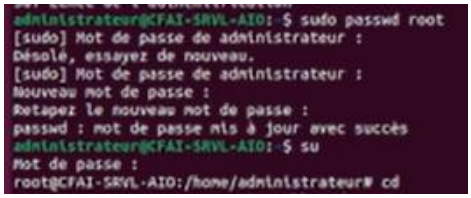
a. Root

Sur ubuntu, par défaut, le mot de passe root est le même que l'utilisateur que l'on a créé durant l'installation. Nous allons donc le changer.

Dans un terminal :

```
#sudo passwd root
```

-> entrer l'ancien mot de passe, puis entrer le nouveau mot de passe.



b. Configuration réseau

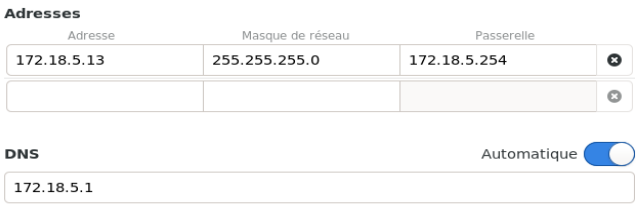
Comme Ubuntu sera accessible à la fois via la Vlan administrateur et via la Vlan Serveur, nous utilisons deux cartes réseau (deux interfaces). Cependant, Linux est incapable d'utiliser plusieurs passerelles. Dans notre cas ce n'est pas trop dérangeant car le réseau admin ne sert qu'à l'administration en local, nous utiliserons donc uniquement la passerelle du réseau serveur.

Carte réseau (eno 1), Vlan Admin :

- Pas de passerelle ni de DNS car nous utiliserons ceux du Vlan Serveur pour l'évasion internet.

Carte réseau (eno 2), Vlan Serveur :

- Passerelle du Vlan Serveur et ses DNS. L'évasion se fera via cette IP.



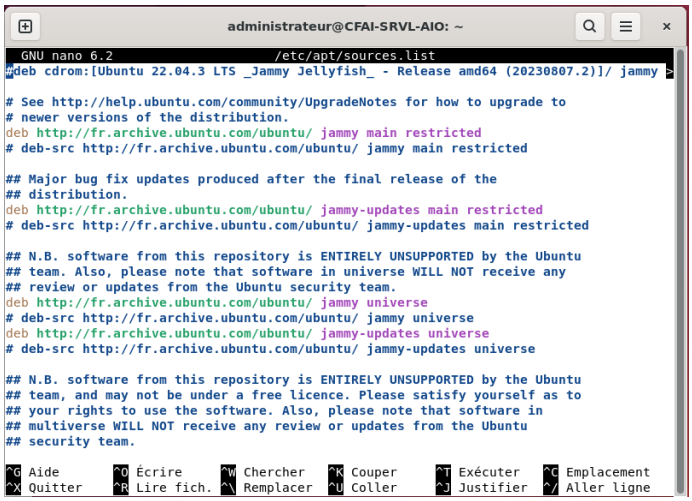
Une fois le réseau configuré, nous pouvons mettre à jour la machine :

```
#apt update -y && apt upgrade -y
```

En cas de problème vérifier la source liste :

```
#nano /etc/apt/source.list
```

Si vous n'avez pas installé les miroirs lors de l'installation vous devrez les ajouter à la main.



2. Activation du RDP

Le RDP (Remote Desktop Protocol) n'est pas natif sur linux. Pour pallier cela nous devons installer le logiciel xrdp :

```
#apt install xrdp -y
```

Xrdp n'autorise pas de s'identifier avec un utilisateur autre que root. Pour contourner cette règle, nous allons modifier le fichier de configuration *sesman.ini* :

```
#nano /etc/xrdp/sesman.ini
```

Commenter les lignes avec un # :

```
#TerminalServerUsers=tsusers
#TerminalServerAdmins=tsadmins
```

ctrl w + o pour sauvegarder et quitter

Maintenant le serveur est joignable en RDP.

/! Attention : En cas de connexion en root, il est nécessaire de désactiver toute mise en veille ou écran noir sous peine de voir sa session root déconnectée et bloquée sur l'écran de dévérouillage.

3. Installation de VMWare

Pour installer VMWare nous aurons besoin du ***bundle*** ici nous prenons celui de Mr Richet que nous avons mis sur une clé usb et que nous avons placé dans les documents.

Pour s'en servir :

- Le rendre exécutable :

```
#sudo chmod +x <file>
```

- L'exécuter :

```
#./<location>
```

Une fois démarré vous arriverez sur une fenêtre vous demandant d'indiquer la mise à jour du kernel.
Pour ce faire, dans un terminal :

```
#sudo apt install git build-essential linux-headers-$(uname -r)
```

- Fermer l'application et la rouvrir.

Une nouvelle fenêtre doit s'ouvrir avec un bouton ***install***. Après cela, l'installation se lance normalement.

Au moment de rentrer la licence entrez :

MC60H-DWHD5-H80U9-6V85M-8280D

L'installation va ensuite se finir et vous pourrez vous en servir normalement.

/! Attention : Si vous mettez à jour votre linux et que vous redémarrez la machine, il est probable que VMWare ne fonctionne plus car la version du kernel grub sera trop récente. Il faudra alors retourner sur l'ancienne.

Identifier la version la plus récente du grub :

```
#grep 'menuentry' /boot/grub/grub.cfg | cut -d "'" -f2
```

Une fois la version la plus récente identifier on la supprime :

```
#sudo apt remove linux-image-6.8.0-60-generic linux headers-6.8.0-60-generic
#sudo update-grub
```

Redémarrez votre machine.

Dans notre cas, nous utilisons plusieurs carte réseau. Dans le cas donc ou vous souhaitez mettre une VM en bridge il important de se rendre dans *edit -> virtual network editor* et ici selectionnez bien la carte reseau correspondant au réseau que vous souhaite utilisez

E. Masterisation

NB : cette documentation est tirée d'un TP réalisée plus tôt dans l'année et inclus donc des contraintes différentes de celles rencontrées pour la réfection de la salle. Cependant elle est applicable en production en adaptant et/ou enlevant certaines règles.

1. Pré-requis

Serveur WDS

- Windows Server 2025 avec le rôle WDS installé (SRV-WDS).
- Matériel : 8 Go RAM · 4 vCPU · 2 disques — OS (60 Go) + disque dédié WDS (50 Go minimum, formaté NTFS, volume E:).
- Un DHCP opérationnel sur le même réseau que les postes à déployer.
- SRV-WDS joint au domaine Active Directory C1-04.lan.

Poste de référence

- Un poste sous Windows 11, connecté au même réseau que SRV-WDS.
- ISO Windows 11 — présente sur le serveur interne de la classe.

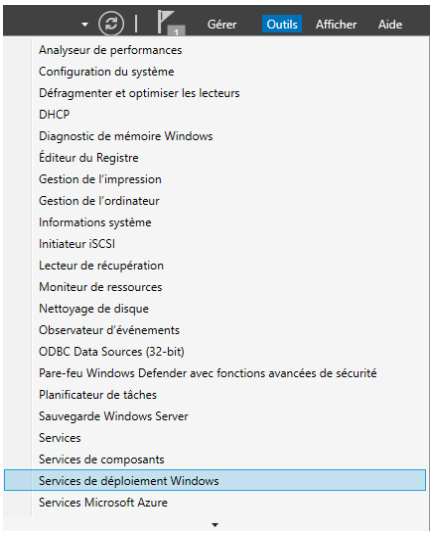
Infrastructure réseau

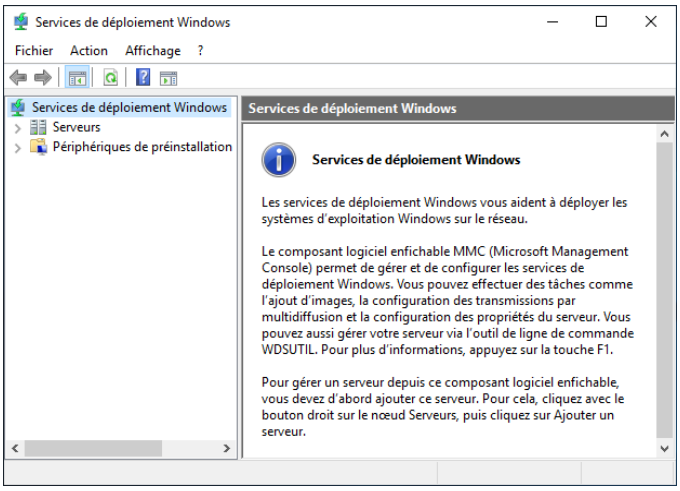
Composant	Rôle	Adresse
SRV-WDS	Serveur WDS + DHCP	172.18.4.x (VLAN 400 - DÉPLOIEMENT)
SRV-AD-PDC	Domaine Active Directory PDC	172.18.5.1
SRV-AD-BDC	Domaine Active Directory BDC	172.18.5.2
Postes salle C1-04	Cibles du déploiement	172.18.3.x (DHCP, VLAN POSTES)

2. Configuration du serveur WDS

a. Installation du rôle WDS

1. Gestionnaire de serveurs → Gérer → Ajouter des rôles et fonctionnalités.
2. Sélectionner « Services de déploiement Windows ». Dans la fenêtre contextuelle, cliquer sur « Ajouter des fonctionnalités ».

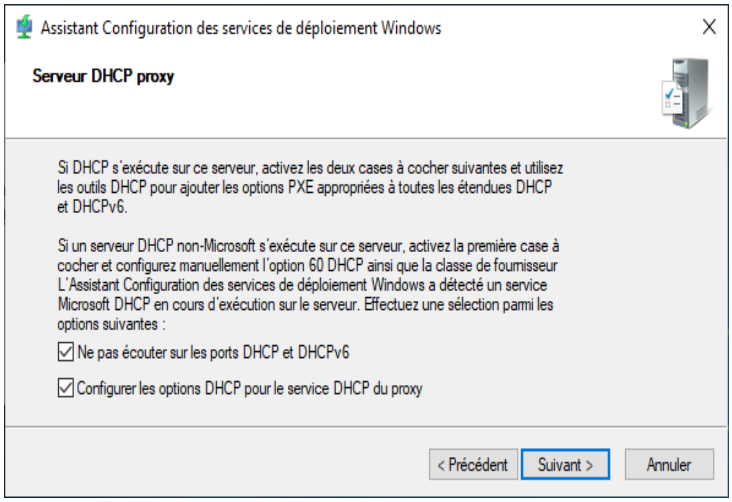


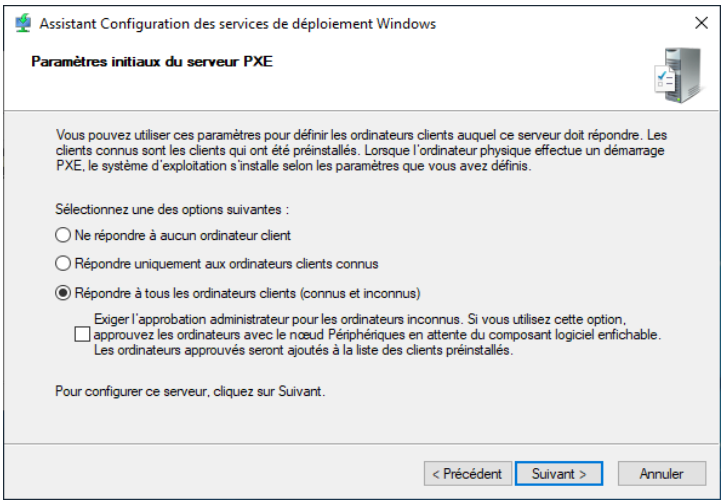


b. Configuration initiale

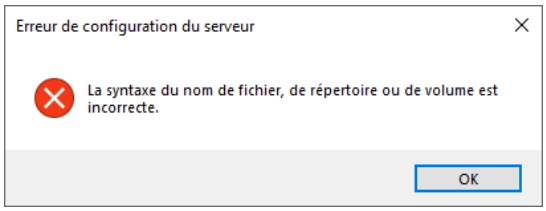
3. Outils → Services de déploiement Windows → clic droit sur le serveur → « Configurer le serveur ».
4. Sélectionner « Intégré à Active Directory » — le serveur est membre du domaine C1-04.lan.

5. Chemin d'installation à distance : E:\WDS.
6. Paramètres PXE : cocher « Répondre à tous les ordinateurs clients (connus et inconnus) ».
7. Laisser les deux cases DHCP cochées si le DHCP tourne sur le même serveur → Terminer.





/!\ Si vous obtenez une erreur « La syntaxe du nom est incorrecte » : aller dans les propriétés de la carte réseau et vérifier que « Partage de fichiers et d'imprimantes » est bien coché.



c. Images de démarrage et de capture

Copier boot.wim depuis l'ISO Windows 11 25H2 (D:\sources\boot.wim) vers C:\Documents.
Les fichiers dans l'ISO sont compressés et peuvent ralentir l'importation.

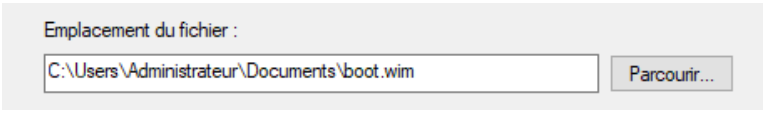
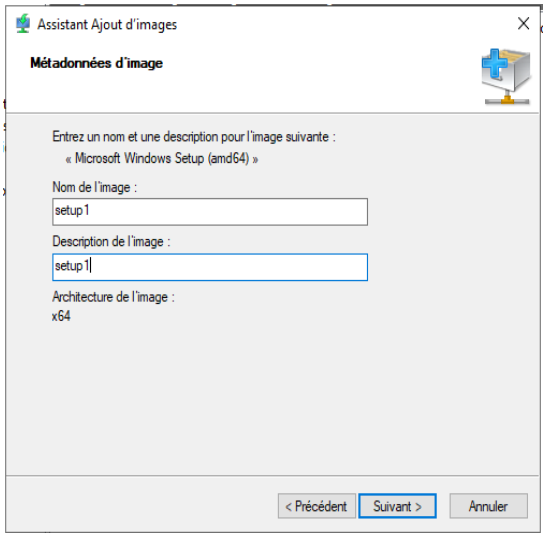


Image de démarrage :

8. Clic droit sur « Images de démarrage » → « Ajouter une image de démarrage ».
9. Sélectionner C:\Documents\boot.wim → Suivant.
10. Nommer l'image « setup1 » → Suivant → attendre la fin → Terminer.



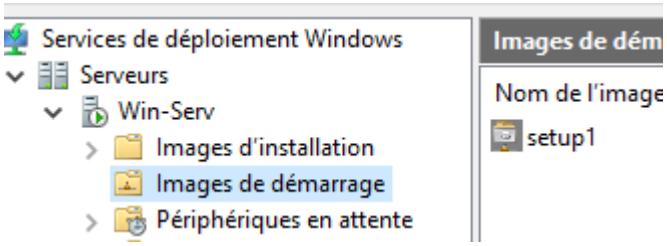
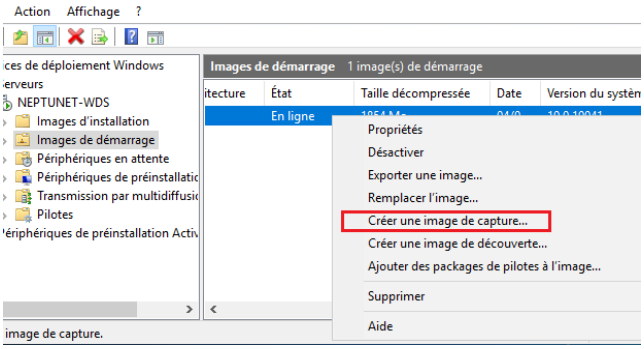
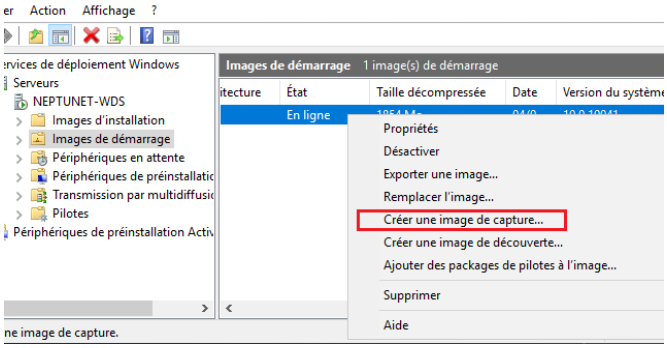


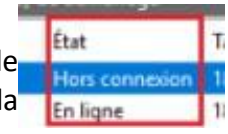
Image de capture : elle servira à capturer le poste de référence après Sysprep :

11. Clic droit sur l'image setup1 → « Créer une image de capture ».





12. Nom : capture · Emplacement : E:\WDS\boot\x64\images\capture.wim → Suivant.
13. Attendre la création → cocher « Ajouter une image au serveur de déploiement Windows » → Terminer.
14. Désactiver ensuite l'image setup1 : clic droit sur setup1 → Désactiver. Elle passe en état « Hors connexion ». Seule capture doit être active pendant la phase de capture.

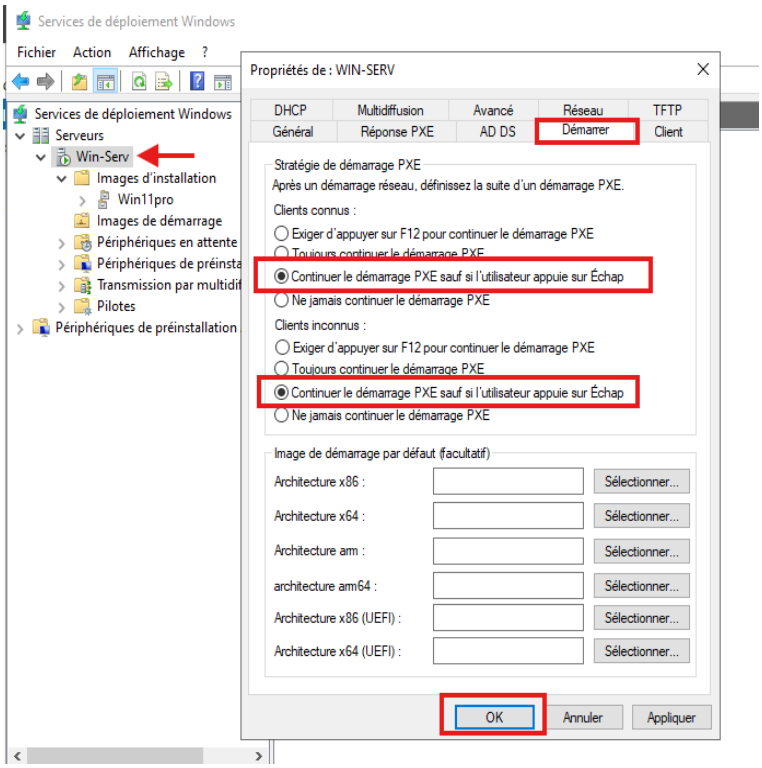


/!\ Avant chaque déploiement (après la capture), ne pas oublier de réactiver setup1 et de désactiver capture. C'est une erreur fréquente qui empêche le boot PXE de fonctionner.

15. Clic droit sur « Images d'installation » → « Ajouter un groupe d'images » → Nom : Win11pro → OK.

d. Paramètres Boot PXE

16. Clic droit sur le serveur WDS → Propriétés → onglet « Démarrer ».
17. Clients connus ET inconnus : sélectionner « Continuer le démarrage PXE sauf si l'utilisateur appuie sur Échap ».



Avant de lancer la capture, redémarrer le service WDS : clic droit sur le serveur → Toutes les tâches → Redémarrer.

3. Configuration du poste de référence Windows 11

Le poste de référence est un poste Windows 11 25H2 Éducation N entièrement configuré qui servira de modèle pour tous les déploiements. Il est connecté au même réseau que SRV-WDS.

À l'étape du choix de la région lors de l'installation initiale, appuyer sur Ctrl+Shift+F3 pour passer en mode Audit. Le poste redémarre avec la session Administrateur automatiquement ouverte et la fenêtre Sysprep au premier plan.

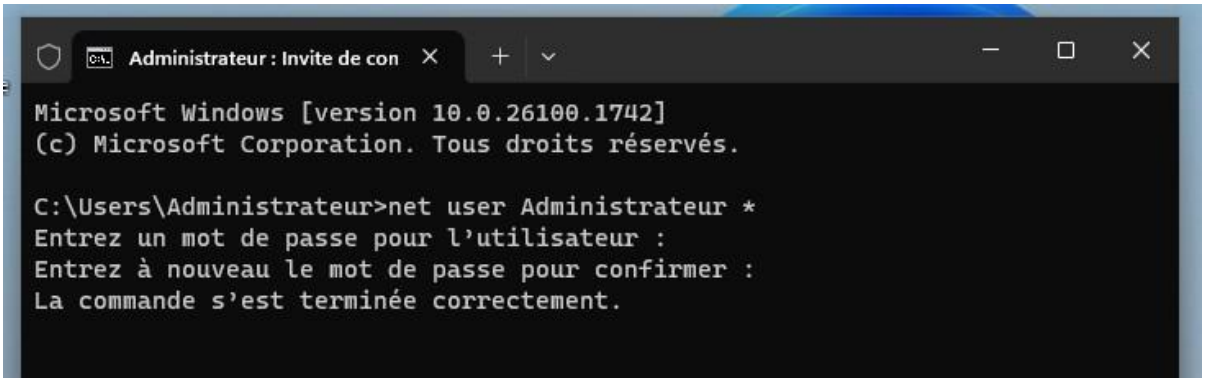
/!\ Ne pas fermer la fenêtre Sysprep qui s'ouvre au redémarrage. On s'en servira à l'étape F.

a. Installation des logiciels

18. Installer Google Chrome : google.com/intl/fr_fr/chrome/ → En faire le navigateur par défaut.
19. Installer GIMP : gimp.org/downloads → lancer l'installation.

b. Mot de passe Administrateur

Ouvrir le CMD en tant qu'Administrateur et saisir :

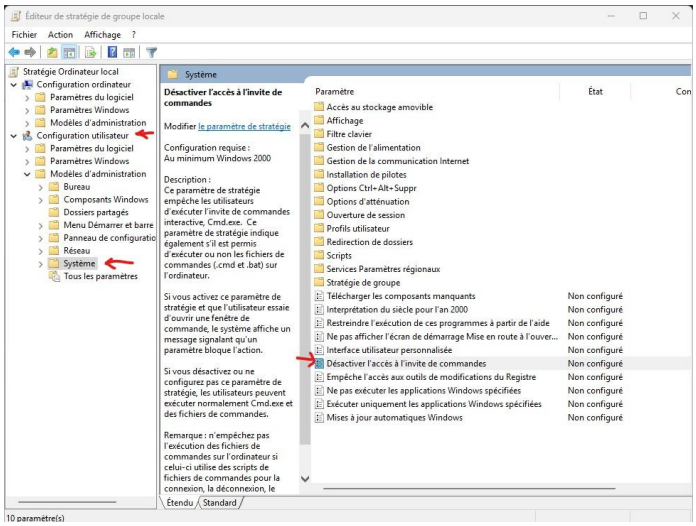


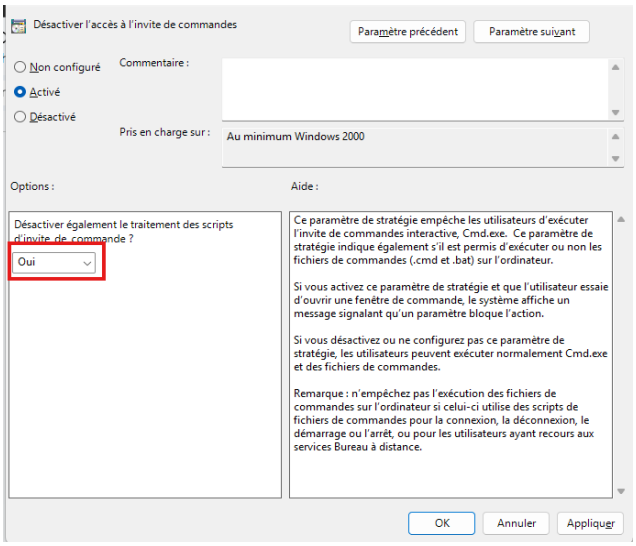
c. Fond d'écran noir

20. Télécharger une image noire et la placer dans C:\Windows\Web\Wallpaper\ avec le nom wallpaper.png.
21. Si les extensions ne sont pas visibles : Affichage → cocher « Extensions de noms de fichiers ».
22. Ouvrir gpedit.msc → Configuration utilisateur → Modèles d'administration → Bureau → Bureau → Papier peint du Bureau → Activé.
23. Saisir le chemin : C:\windows\web\wallpaper\wallpaper.png · Style : Ajuster → Appliquer → OK.

d. Désactiver l'invite de commande

24. gpedit.msc → Configuration utilisateur → Modèles d'administration → Système.
25. Double-cliquer sur « Désactivation de l'accès à l'invite de commande » → Activé.
26. Désactiver également le traitement des scripts ? → Oui → Appliquer → OK.





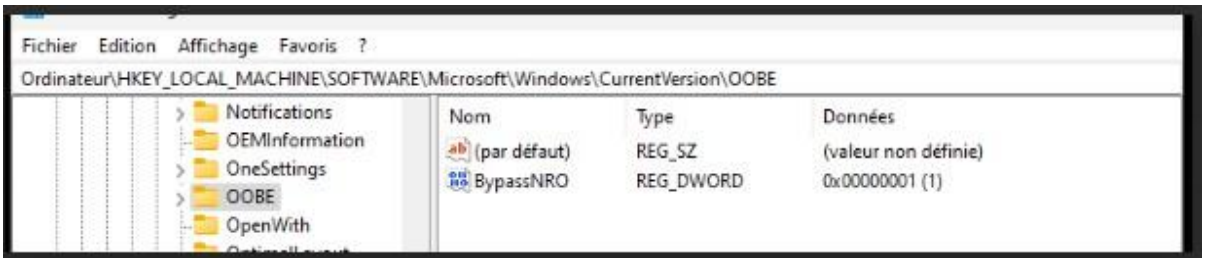
e. Bypass NRO

Sans cette étape, l'utilisateur sera bloqué à l'OOBE avec une obligation de créer un compte Microsoft.

Comme le CMD est désactivé, il ne pourra pas contourner cette étape — le poste sera inutilisable.

27. Ouvrir l'Éditeur de registre (regedit).
28. Naviguer vers: HKEY_LOCAL_MACHINE → SOFTWARE → Microsoft → Windows → CurrentVersion → OOBE.
29. Clic droit dans le dossier OOBE → Nouveau → Valeur DWORD 32 bits.

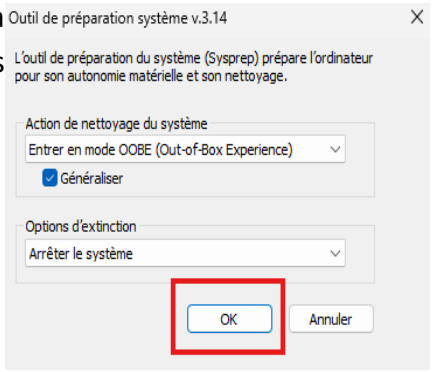
30. Nommer la valeur : BypassNRO · Données de la valeur : 1 → OK.



Lors du déploiement, l'utilisateur verra un bouton « Je n'ai pas internet » à l'écran de connexion réseau OOBE, ce qui lui permet de continuer vers la création d'un compte local.

f. Sysprep OOBE — capture finale

Le poste de référence est maintenant configuré. Retourner sur la fenêtre Sysprep laissée ouverte au démarrage (ou la relancer depuis C:\Windows\System32\Sysprep\sysprep.exe).



Configurer la fenêtre Sysprep comme suit et cliquer OK :

- Action de nettoyage du système : Entrer en mode OOBE
- Cocher Généraliser
- Options d'extinction : Arrêter le système

Le poste s'éteint automatiquement à la fin (10 à 15 minutes).

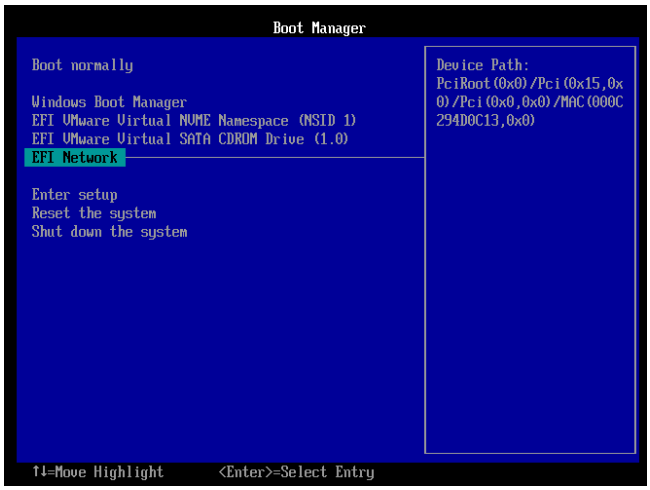
4. Capture de l'image via PXE

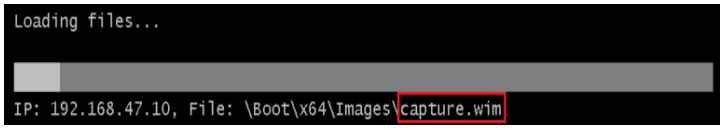
Le poste de référence est éteint. Sur SRV-WDS, s'assurer que « capture » est En ligne et « setup1 » est Hors connexion.

a. Boot PXE sur le poste de référence

31. Démarrer le poste de référence en bootant sur la carte réseau (F12 au démarrage ou via le BIOS — touche variable selon le matériel).

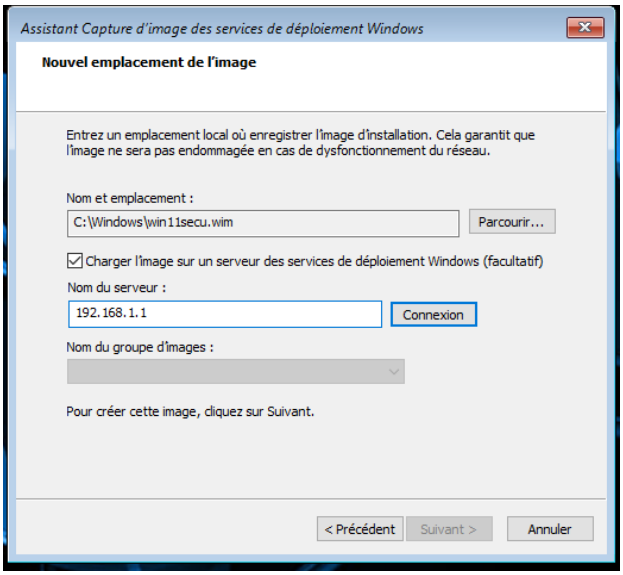
32. L'image capture.wim se charge depuis SRV-WDS.

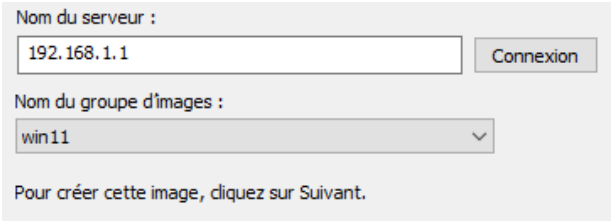


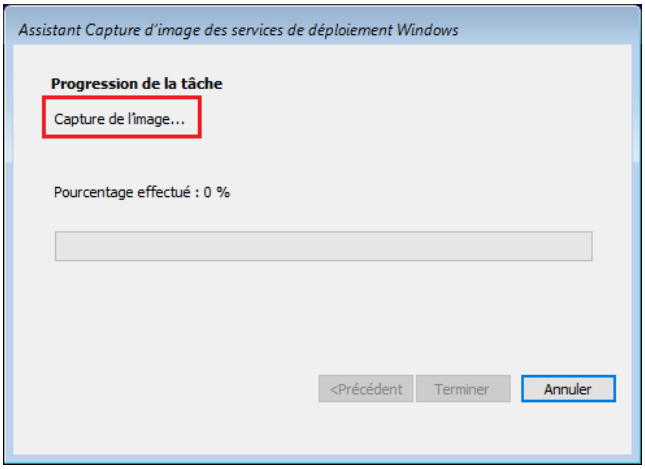


b. Assistant de capture

33. L'assistant « Capture d'image des services de déploiement Windows » s'ouvre → Suivant.
34. Volume à capturer : C:\ · Nom de l'image : WIN11 → Suivant.
35. Cocher « Charger l'image sur un serveur WDS » → Nom du serveur : SRV-WDS → Connexion.
36. Un CMD s'ouvre pour l'authentification. Se déplacer avec les flèches, saisir les identifiants du compte WDS → OK.







37. Le groupe WIN11 apparaît.

38. La capture commence (30 à 60 minutes). Une fois terminée → Terminer → éteindre le poste.

5. Chiffrement BitLocker du disque WDS

Le disque WDS (volume E:) contient les images système. Le chiffrer avec BitLocker protège ces données en cas d'accès physique non autorisé au serveur.

39. Gestionnaire de serveurs → Ajouter des rôles et fonctionnalités → Fonctionnalités → développer « Utilitaires d'administration du Chiffrement de lecteur BitLocker » → cocher les deux sous-options → Installer.
40. Rechercher « Gérer BitLocker » → ouvrir.
41. Dans « Lecteurs de données fixes », repérer E: (WDS) → « Activer BitLocker ».
42. Mode de déverrouillage : mot de passe → saisir et confirmer → Suivant.
43. Sauvegarde de la clé de récupération : « Enregistrer dans un fichier » → stocker dans Vaultwarden → Suivant.
44. Chiffrement : « Ne chiffrer que l'espace disque utilisé » → Nouveau mode de chiffrement → Démarrer le chiffrement.

/! À chaque redémarrage de SRV-WDS, le disque E: est verrouillé. Ouvrir l'Explorateur → double-clic sur E: → saisir le mot de passe BitLocker avant de démarrer le service WDS, sans quoi les images seront inaccessibles.

6. Déploiement des postes

Préparation avant chaque déploiement

- Si BitLocker est actif sur E: : double-clic sur E: dans l'Explorateur → saisir le mot de passe pour déverrouiller.
- Console WDS : s'assurer que setup1 est En ligne et capture est Hors connexion.

Procédure de déploiement :

- Mode UEFI obligatoire (requis pour Windows 11 et BitLocker TPM 2.0).
- Boot réseau (PXE) en priorité de démarrage.
- Sur les postes Lenovo de la salle : F1 → Configuration UEFI → Gestionnaire d'amorçage → Mode UEFI.

45. Démarrer le poste en bootant sur la carte réseau.
46. L'image setup1 se charge depuis SRV-WDS.

L'installation Windows démarre. Suivre l'assistant d'installation normalement.

F. GLPI

GLPI (Gestionnaire Libre de Parc Informatique) est une solution open source de gestion des services informatiques et de gestion des actifs. Développé pour aider les organisations à gérer efficacement leur infrastructure IT, GLPI offre des fonctionnalités variées telles que la gestion des incidents, la gestion des demandes de service, la gestion des actifs matériels et logiciels, ainsi que la planification des ressources. Grâce à son interface conviviale et à sa flexibilité, GLPI permet aux équipes informatiques d'optimiser leurs processus, d'améliorer la communication avec les utilisateurs et de garantir un meilleur suivi des opérations.

1. Prérequis

```
#apt install apache2 php mariadb-server -y
#apt install php-{mysql,mbstring,curl,gd,xml,intl,ldap,apcu,xmlrpc,zip,bz2,imap} -y
```

2. Installation de la base de données

```
#mysql_secure_installation
```

Entrer le mot de passe root puis :

```
#no
#no
#yes
#no
#yes  (remove database test)
#yes
```

MariaBD est installé, maintenant nous créons sa base de données :

```
#mysql -u root
```

```
#create database db_glpi;
```

La commande suivante va créer un utilisateur ici nommé « admindb_glpi », lui attribuer le mot de passe « votre-MDP » et lui donner tous les privilèges (3 commandes en une).

> /!\ Gardez les " " lorsque vous mettrez votre mot de passe.

```
#grant all privileges on db_glpi.* to admindb_glpi@localhost identified by "votre-MDP";
#flush privileges;
#exit;
```

3. Installation du service GLPI

```
#cd /tmp
#wget https://github.com/glpi-project/glpi/releases/download/10.0.17/glpi-10.0.17.tgz
```

Décompressez l'archive de GLPI directement dans le répertoire par défaut du service web (/var/www/html):

```
#tar -xvzf glpi-10.0.17.tgz -C /var/www/html
```

Rendez l'utilisateur des services web (nommé www-data) propriétaire de ces nouveaux fichiers :

```
#chown -R www-data /var/www/html
```

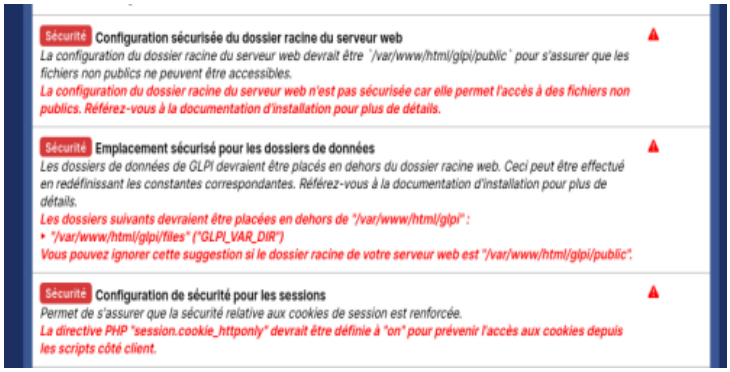
Vous pouvez vérifier que tout est OK en listant le contenu du répertoire avec la commande « ls -l /var/www/html ». Vous pourrez alors constater la présence du répertoire glpi et que le propriétaire est bien l'utilisateur nommé « www-data » :

```
root@GLPI:/tmp# ls -l /var/www/html
total 16
drwxr-xr-x 25 www-data administrateur  4096  6 nov.   2024 glpi
-rw-r--r--  1 www-data root          10701  4 juil. 11:27 index.html
```

Redémarrez apache2 :

```
#sudo systemctl restart apache2
```

Le serveur GLPI est prêt à l'emploi. Cependant si nous allons sur son interface web nous rencontrerons ces messages erreurs. Ils ne sont pas bloquants mais nous allons voir maintenant comment les résoudre.



4. Modification des emplacements fichiers

Créez un dossier nommé « glpi » dans /etc :

```
#mkdir /etc/glpi
```

Dans ce nouveau dossier, créez un fichier nommé « local_define.php » :

```
#nano /etc/glpi/local_define.php
```

```
<?php
define('GLPI_VAR_DIR', '/var/lib/glpi');
define('GLPI_LOG_DIR', '/var/log/glpi');
```

Sauvegarder et quitter (ctrl x puis o puis entrée).

Déplacez le dossier « config » situé actuellement dans /var/www/html/glpi dans /etc/glpi:

```
#mv /var/www/html/glpi/config /etc/glpi
```

Rendez www-data propriétaire de /etc/glpi et de son contenu :

```
#chown -R www-data /etc/glpi/
```

Poursuivons en déplaçant le dossier « files » de glpi dans /var/lib/glpi :

```
#mv /var/www/html/glpi/files /var/lib/glpi
```

Ensuite nous allons préparer le dossier de logs de GLPI et rendre, une fois encore, l'utilisateur www-data propriétaire avec les 2 commandes suivantes :

```
#mkdir /var/log/glpi
#chown www-data /var/log/glpi
```

Il va maintenant falloir faire comprendre à GLPI où il va devoir chercher les fichiers et ses configurations:

```
#nano /var/www/html/glpi/inc/downstream.php

        <?php
        define('GLPI_CONFIG_DIR', '/etc/glpi/');
        if (file_exists(GLPI_CONFIG_DIR . '/local_define.php')) {
        require_once GLPI_CONFIG_DIR . '/local_define.php';
        }
```

5. Configuration du serveur web

Nous allons modifier le fichier php.ini situé dans /etc/php/8.2/apache2:

```
        #nano /etc/php/8.2/apache2/php.ini
```

Recherchez la ligne « session.cookie_httponly = » et ajoutez « on » après le =.

Ensuite il faut créer un virtualhost (fichier configuré sur apache permettant de faire cohabiter plusieurs sites web différents sur la même machine).

Créez dans le dossier d'apache2 un fichier nommé « glpi.conf » :

```
        #nano /etc/apache2/sites-available/glpi.conf
```

Écrivez :

```
<VirtualHost *:80>
        # ServerName vm-glpi
        ServerAlias VOTRE-IP
        DocumentRoot /var/www/html/glpi
        Alias "/glpi" "/var/www/html/glpi/public"
        <Directory /var/www/html/glpi>
                Require all granted
                RewriteEngine On
                RewriteCond %{REQUEST_FILENAME} !-f
                RewriteRule ^(.*)$ index.php [QSA,L]
        </Directory>
</VirtualHost>
```

Une fois ceci fait, activez un module apache qui permet de faire de la redirection d'URL :

```
#sudo a2enmod rewrite
```

Désactivez la config par défaut d'Apache avec la commande suivante :

```
#sudo a2dissite 000-default.conf
```

Et enfin, activez le fichier de configuration web spécialement créé précédemment pour glpi :

```
#sudo a2ensite glpi.conf
```

Il ne reste plus qu'à redémarrer le service apache2 pour appliquer toutes les modifications apportées :

```
#sudo systemctl restart apache2
```

NB : Si lors du redémarrage d'apache vous avez un message d'erreur, il vous faudra commenter la ligne 225 du fichier annoncé lorsque vous faites la commande :

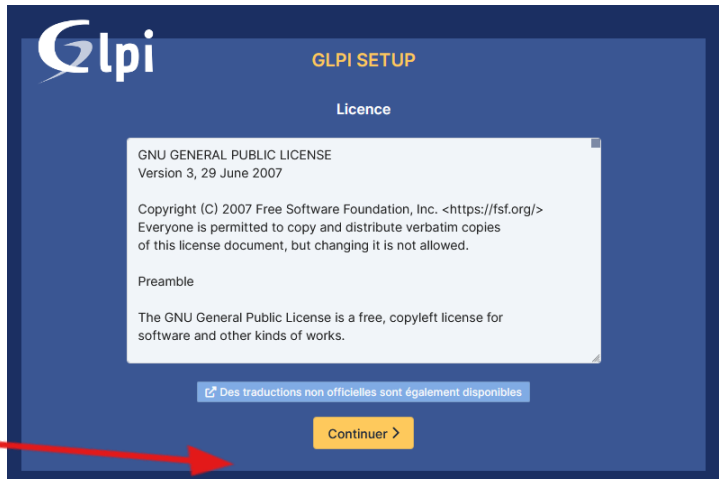
```
#systemctl status apache2
```

6. Configuration de GLPI

Votre serveur GLPI est prêt à être configuré, nous allons passer sur son interface web :
2 façons :
→ http://localhost/glpi
→ http://ipdelamachine/glpi et on met L'IP de la machine.

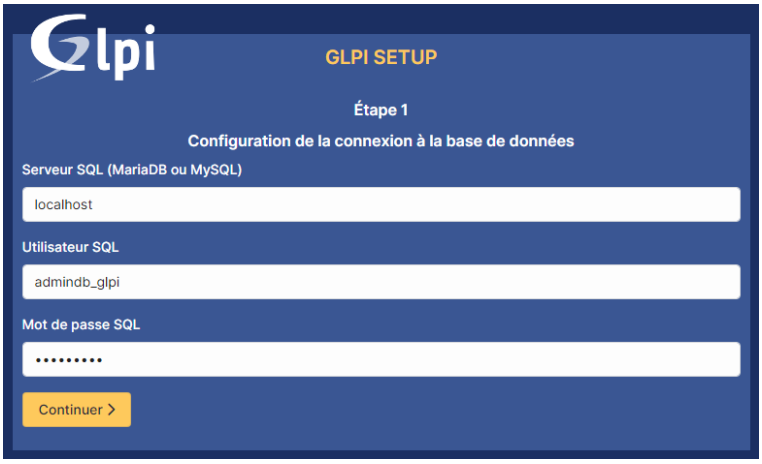
OK

Continuer



Installer

Saisissez localhost pour spécifier que la machine actuelle héberge à la fois le site web de GLPI et la base de données.



Rentrez ensuite le nom de l'utilisateur qui a tous les privilèges sur cette base de données et son mot de passe.

On sélectionne notre base de données.

Le service GLPI est maintenant installé et fonctionnel.

Se connecter en mode administrateur : **glpi/glpi**

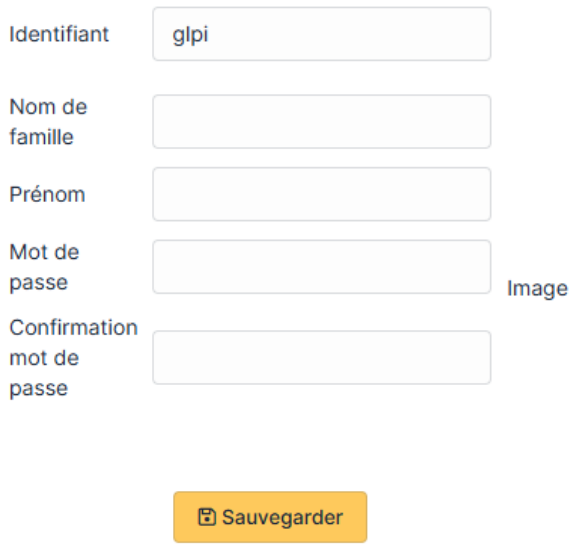
2 messages s'affichent :

- Changer les mots de passe des utilisateurs
- Supprimer le fichier install.php

a. Pour supprimer le fichier install.php

```
#rm -r /var/www/html/glpi/install/
```

b. Changez les mots de passes utilisateur



G. Zabbix

Dans le cadre de la réfection de la salle informatique, il était important de mettre en place une solution de supervision afin de garantir la stabilité et la performance de l'infrastructure. Le choix s'est porté sur Zabbix, une solution open-source reconnue pour sa fiabilité et sa flexibilité.
Zabbix permet de surveiller en temps réel l'état des équipements réseau, des serveurs et des services associés. Il centralise les informations issues des différents matériels, ce qui facilite la détection des anomalies et le suivi de l'ensemble du système.
Cette solution présente plusieurs avantages : une interface web claire, une compatibilité avec de nombreux types d'équipements et OS, et surtout gratuit.
Grâce à Zabbix, la supervision devient proactive : les incidents peuvent être anticipés, les interventions mieux ciblées, et la continuité de service assurée pour les utilisateurs.

1. Installer l'entrepôt Zabbix

```
#wget https://repo.zabbix.com/zabbix/7.4/release/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.4+debian12_all.deb
#dpkg -i zabbix-release_latest_7.4+debian12_all.deb
#apt update
```

2. Installer les paquets Zabbix

```
#apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
```

3. Créer la base de données et l'utilisateur

```
        #apt install mariadb-server -y
        #mysql -u root -p
password
        #create database zabbix character set utf8mb4 collate utf8mb4_bin;
        #create user zabbix@localhost identified by 'password';
        #grant all privileges on zabbix.* to zabbix@localhost;
        #set global log_bin_trust_function_creators = 1;
        #quit;
```

/! Garder les guillemets autour du mot de passe.

4. Importation du schéma de la base de données créée

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

Désactiver l'option « log_bin_trust_function_creators » après l'importation de la base de données :

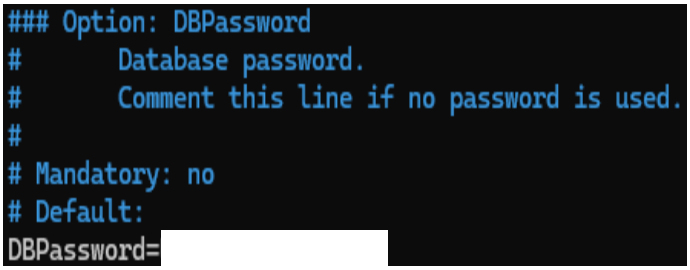
```
        #mysql -uroot -p
password
        #set global log_bin_trust_function_creators = 0;
        #quit;
```

5. Configurer la base de données pour le serveur Zabbix

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

Remplacer "password" par le mot de passe précédemment configuré.

DBPassword=password



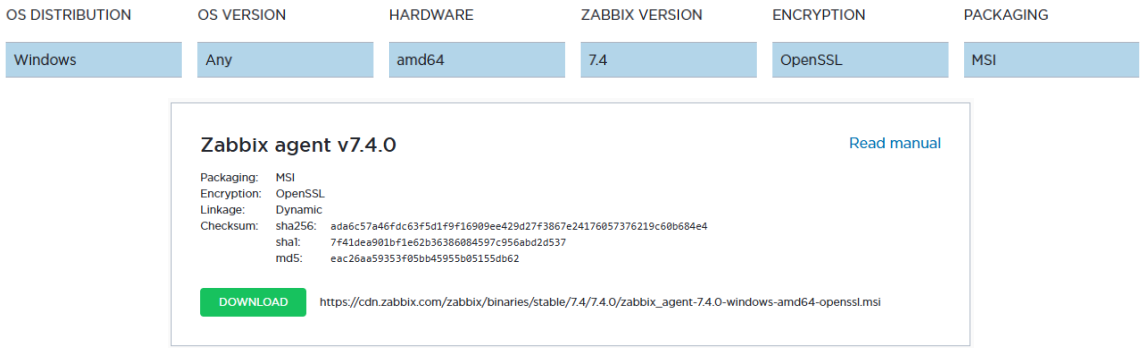
6. Démarrer Zabbix et faire en sorte qu'il démarre au démarrage du serveur

```
#systemctl restart zabbix-server zabbix-agent apache2
#systemctl enable zabbix-server zabbix-agent apache2
```

7. Ajouter un Agent Zabbix

https://www.zabbix.com/download_agents

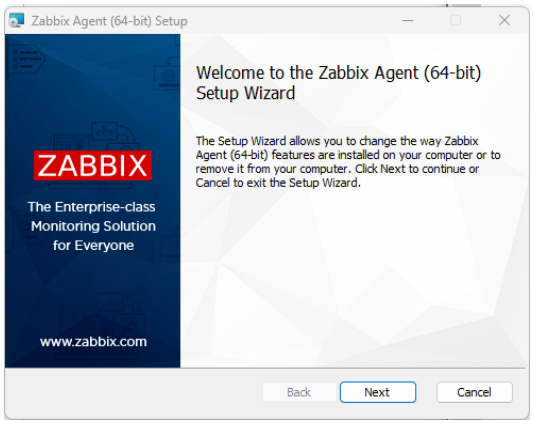
a. Windows



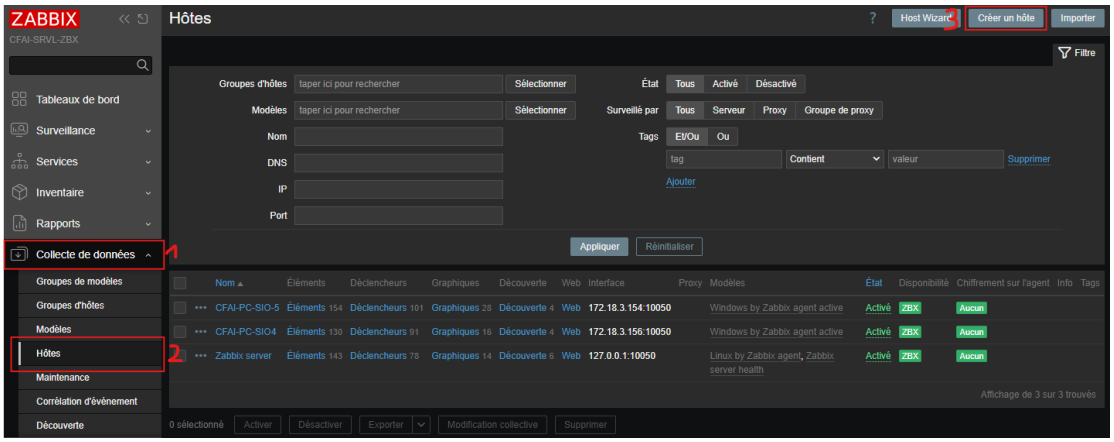
Télécharger l'agent Zabbix pour Windows.

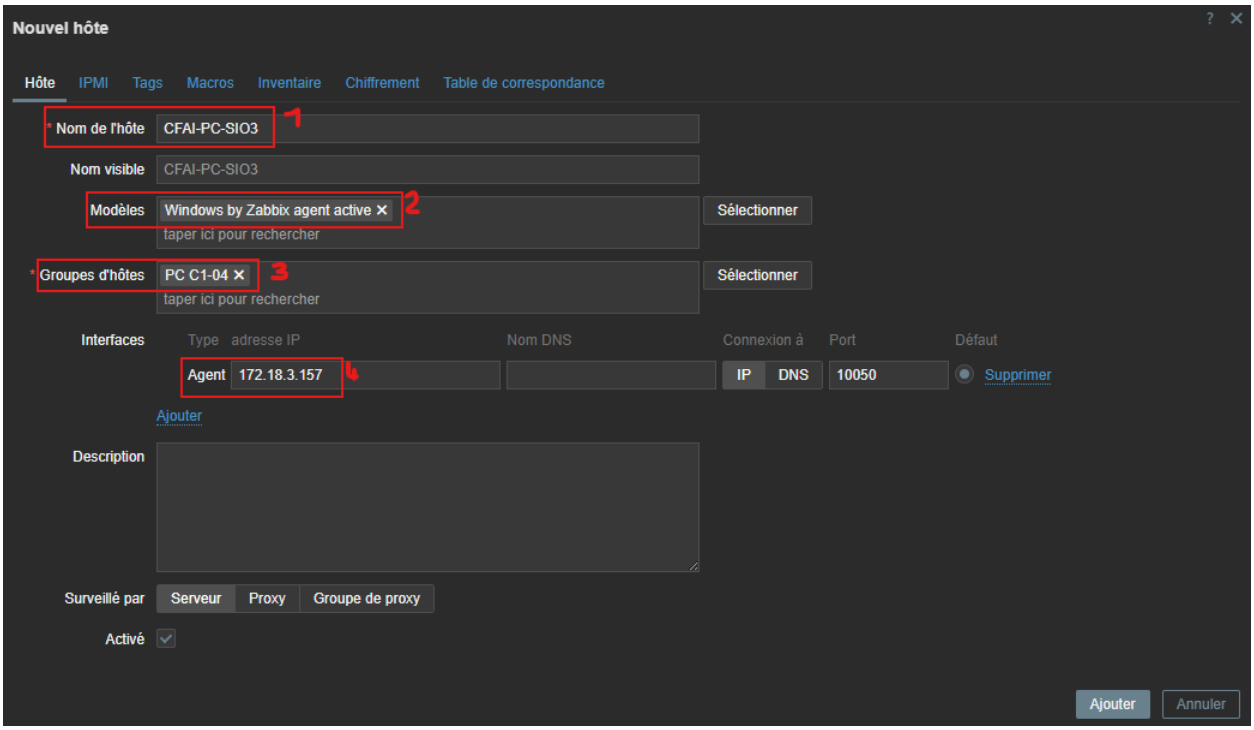
- Faire Next
- Cocher "Accepter" pour continuer
- Next

- Hostname : *Nom de l'ordinateur*
- Zabbix serveur : 172.18.5.25
- Server ou Proxy : 172.18.5.25
- Next
- Installer (avec les droits admin)
- Fin



Nous avons installé l'agent sur la machine à monitorer. Maintenant il faut l'ajouter sur le service Zabbix.
Cette procédure est la même que la machine soit sur windows ou sur linux.



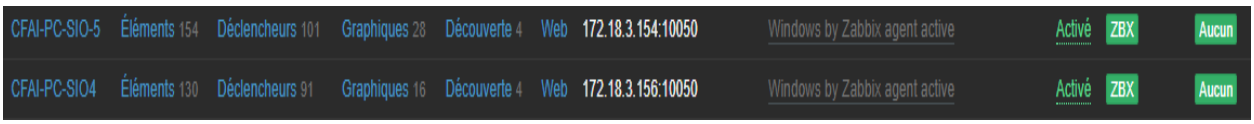


1 : Nom de la machine à monitorer.

2 : Type d'agent. Sera toujours actif.

3 : Groupe d'hôtes, ici nous prenons l'exemple d'un poste sur le domaine. Peut-être une VM, un serveur, etc.

4 : IP de la machine à monitorer.



H. Nextcloud

Nextcloud

Service en open source, Nextcloud propose, entre autres, des services de cloud computing, messagerie, stockage, partage et édition de fichier. Avec sa base de données installée en local, il permet de contrôler et sécuriser les données.
Il est compatible avec différents OS, gratuit et rapide à installer.

1. Prérequis

Installation du serveur web apache :

```
#sudo apt install apache2 -y
```

Installation de MariaDB :

```
#sudo apt install mariadb-server -y
```

Installation de PHP :

```
#sudo apt install php{,-gd,-mbstring,-xml,-zip,-curl,-mysql,-ldap} -y
```

Pour vérifier que tous les modules PHP sont bien installés :

```
#dpkg -l | grep 'php'
```

2. Installation de Nextcloud

Téléchargez la dernière version de Nextcloud :

```
#cd /tmp
```

```
#wget https://download.nextcloud.com/server/releases/latest.zip
```

Décompressez l'archive :

```
#unzip latest.zip
```

Déplacez les fichiers vers le répertoire du serveur web :

```
#mv nextcloud/ /var/www/html/nextcloud
```

Donnez les droits au serveur web :

```
#chmod 775 /var/www/html/nextcloud
#sudo chown -R www-data:www-data /var/www/html/nextcloud
```

3. Configuration de la base de données

Créez une base de données pour Nextcloud :

```
#mysql -u root
```

Dans MariaDB, exécutez :

```
#create database nextcloud;
#create user nextcloud@localhost identified by "yourPassword";
#grant all privileges on nextcloud.* to nextcloud@localhost;
#flush privileges;
#quit;
```

Cela va créer une base de données nommée « nextcloud », un utilisateur nommé « nextcloud » également avec un mot de passe que vous aurez renseigné.

4. Configuration du serveur web

Créez un fichier de configuration Nextcloud :

```
#nano /etc/apache2/sites-available/nextcloud.conf
```

Ajoutez le contenu suivant :

```
<Directory /var/www/html/nextcloud/>
Require all granted
AllowOverride All
Options FollowSymLinks MultiViews
        <IfModule mod_dav.c>
        Dav off
        </IfModule>
 </Directory>
```

Activez les modules requis :

```
#sudo a2ensite nextcloud
#sudo a2enmod rewrite headers env dir mime
```

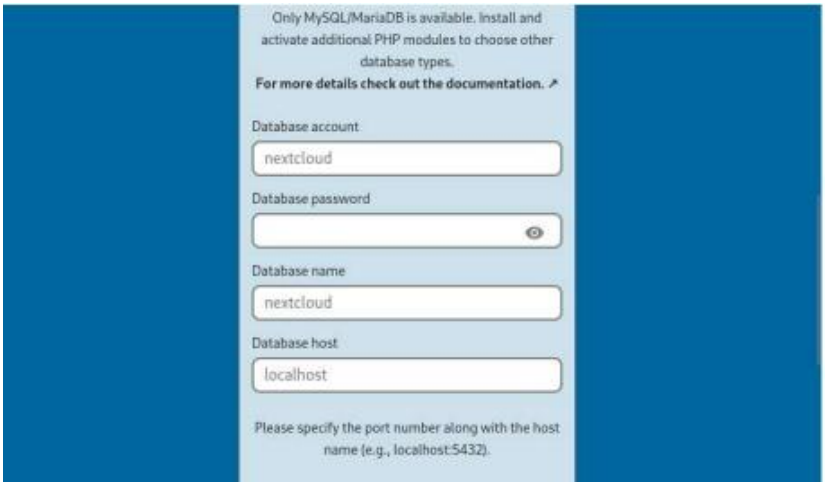
Redémarrer le serveur web :

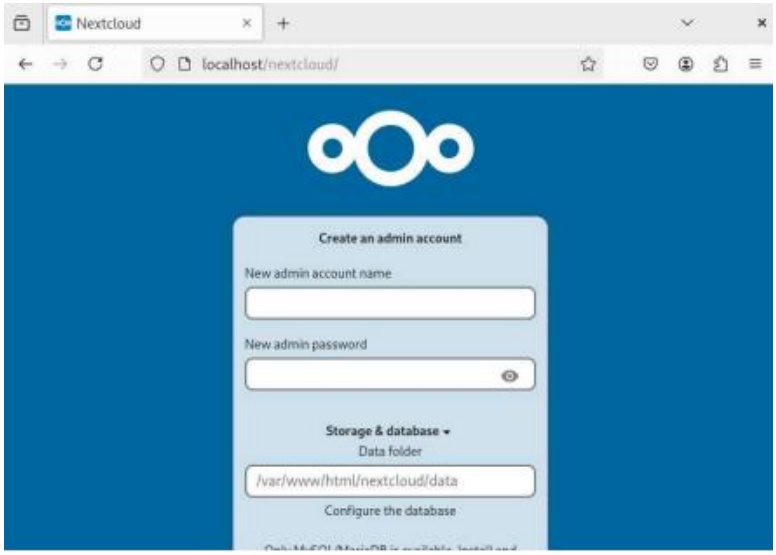
```
#sudo systemctl restart apache2
```

5. Finalisation de l'installation via l'interface web

Connectez-vous via votre navigateur sur l'interface web : http://localhost/nextcloud

Renseignez les informations (nom d'utilisateur/mot de passe) de l'utilisateur qui sera administrateur.
Entrez les informations de connexion de la base de données puis validez.





Vous avez maintenant fini l'installation de Nextcloud, la mise en route va se lancer et vous arriverez sur votre interface.

/! : S'il vous est impossible de se connecter sur votre Nextcloud sur une machine de votre réseau il se pourrait que cela vienne de la configuration de PHP.

Pour corriger cela :

- Éditer le fichier config php :

```
#sudo nano /var/www/html/nextcloud/config/config.php
```

- Trouvez la ligne « trusted_domains » :
  Ajouter une ligne avec l'ip de votre machine

```
'trusted_domains' =>
array (
  0 => 'localhost',
  1 => '127.0.0.1',
  2 => '192.168.50.16', #remplacer par L'IP privée de votre serveur
```

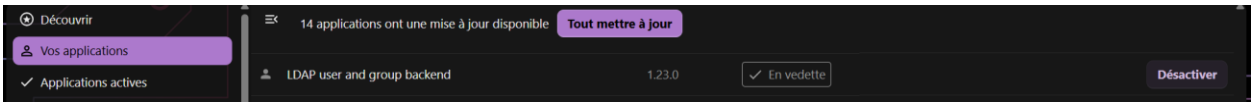
6. Ajout au LDAP Active Directory

Par défaut, Nextcloud gère ses propres comptes utilisateurs. Pour que les utilisateurs puissent se connecter avec leurs identifiants Windows (Active Directory), il faut activer l'application LDAP intégrée à Nextcloud et la configurer pour interroger notre AD.

NB : LDAP (Lightweight Directory Access Protocol) est le protocole utilisé par l'Active Directory pour exposer ses données. En configurant Nextcloud pour interroger l'AD via LDAP, les utilisateurs n'ont pas de compte Nextcloud séparé, ils utilisent leurs identifiants Windows habituels.

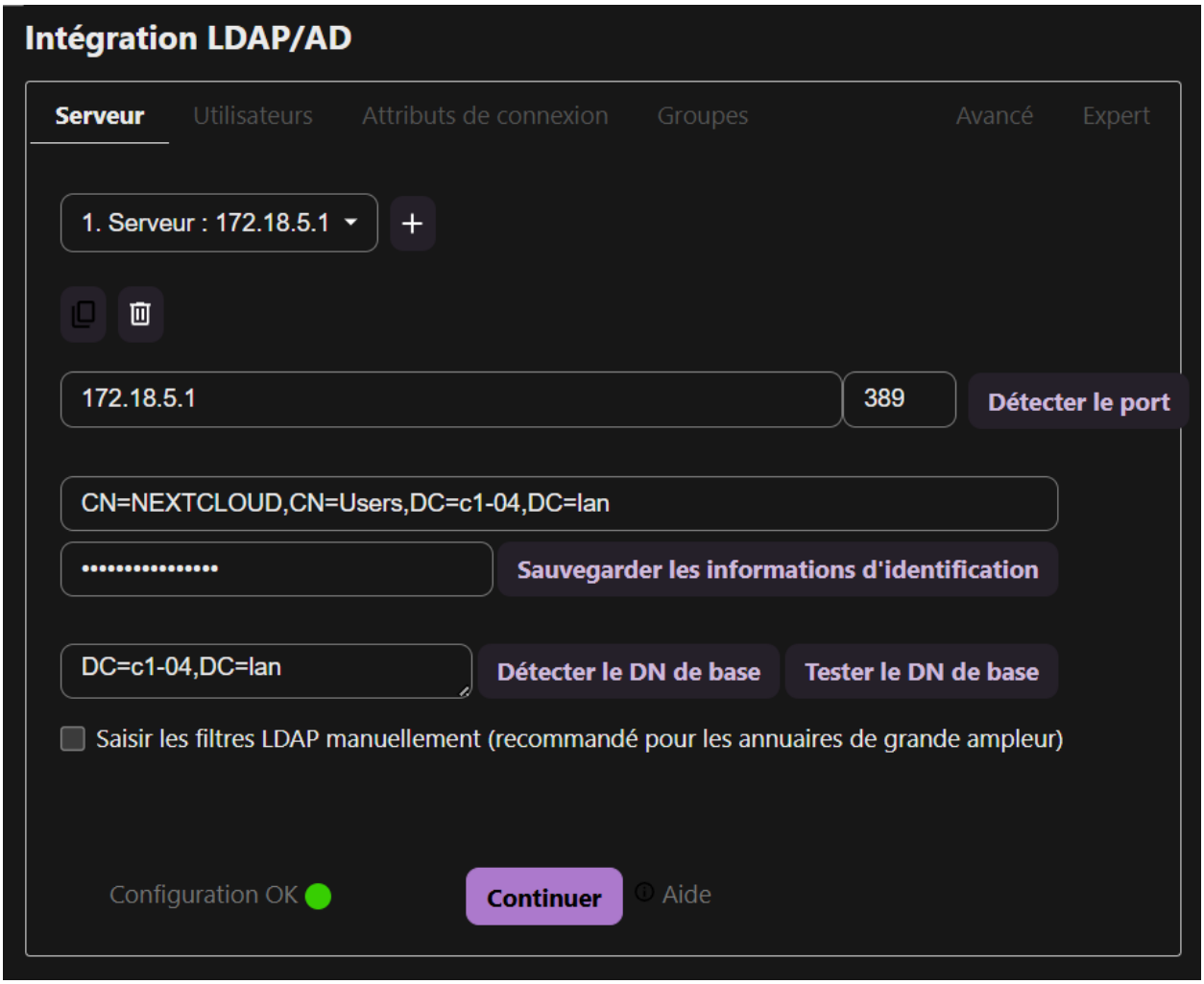
L'application LDAP est intégrée à Nextcloud mais désactivée par défaut. Pour l'activer :

Applications > Désactivées > LDAP user and group backend > Activer



Une fois l'application activée, se rendre dans :

Paramètres d'administration > Intégration LDAP / AD



Info : Le compte LdapService est un compte de service dédié dans l'AD, il a uniquement les droits de lecture sur l'annuaire. C'est lui que Nextcloud utilise pour vérifier si un utilisateur existe et récupérer ses informations, sans avoir besoin de droits admin.

Onglet Utilisateurs :

```
(&(|(objectclass=person)(objectclass=user)))
```

Info : Le filtre exclut les comptes désactivés (userAccountControl) et les comptes machine. Seuls les comptes utilisateurs actifs peuvent se connecter. L'attribut samaccountname correspond au login Windows habituel, c'est ce que l'utilisateur saisit pour se connecter.

Pour restreindre l'accès Nextcloud à certains groupes AD, on peut ajouter un filtre sur les groupes. Dans notre cas, on limite aux groupes suivants :

```
(&(objectClass=group)(|(cn=BTS SIO 2)(cn=Prof)))
```

Un bouton Test de connexion est disponible en bas de chaque onglet. Il permet de vérifier que Nextcloud contacte bien le PDC et récupère les utilisateurs correctement. En cas d'échec, vérifier :

- Que le port 389 est ouvert entre le serveur Nextcloud (VLAN 500) et le PDC (172.18.5.1)
- Que les credentials du compte LdapService sont corrects
- Que le DN de base est bien DC=c1-04,DC=lan

Première connexion utilisateur :

Lors de la première connexion d'un utilisateur AD sur Nextcloud, un compte Nextcloud est créé automatiquement et lié au compte AD. Les connexions suivantes utilisent directement les credentials Windows, l'utilisateur n'a rien à configurer de son côté.

À noter : Si un utilisateur existait déjà dans Nextcloud avec un compte local (créé avant l'activation LDAP) et que son login correspond à son samaccountname AD, les deux comptes peuvent entrer en conflit. Dans ce cas, il faut supprimer le compte local Nextcloud avant d'activer LDAP.

I. Proxmox

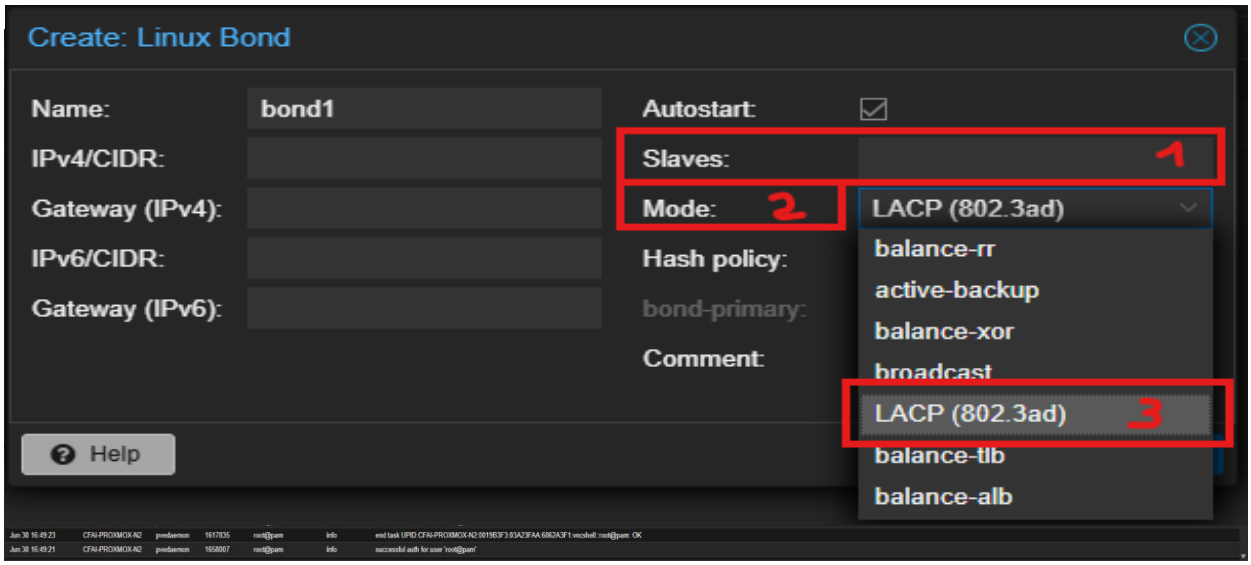
Afin de disposer d'un environnement stable, centralisé et capable d'héberger plusieurs services sur un seul serveur physique, nous avons choisi d'installer Proxmox VE comme système d'exploitation principal.

Ce choix s'appuie sur plusieurs critères :

- Compatibilité avec notre matériel : le serveur HPE ProLiant DL380p Gen8 (2015) est un serveur vieillissant mais il réussit à bien faire tourner Proxmox, et grâce à ses outils de monitoring faciles à prendre en main nous pouvons adapter les ressources allouées aux VM de façon précise.
- Simplicité d'installation et de gestion : il propose une interface web et permet une administration centralisée des machines virtuelles et du monitoring réseau et matériel. Bien que redondant avec xClarity pour le monitoring, son interface web nous sera pratique et nous permettra une bonne lisibilité des différents services proposés sur le serveur.
- Haute disponibilité et sauvegarde intégrée. Il permet une gestion des snapshots, des backups et facilite les restaurations rapides en cas de problème. En cas de besoin ou d'agrandissement, Proxmox permet une mise en cluster facile et à postériori à condition que le serveur à mettre en cluster tourne lui aussi sur cet OS.
- Coût nul : en tant que solution open source, Proxmox nous offre une solution de qualité, gratuite et avec une communauté riche qui permet d'apporter des solutions en cas de problème.

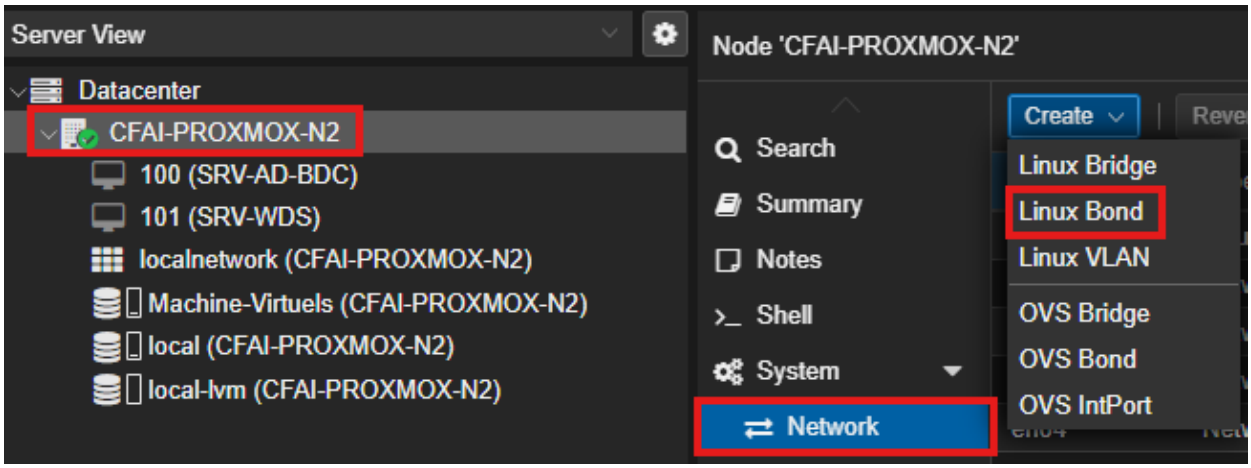
En résumé, Proxmox s'est imposé comme une solution fiable, légère et adaptée à nos objectifs, tout en maximisant les performances d'un serveur plus ancien qui peut souffrir de son obsolescence.

Pour aller sur l'interface WEB de proxmox il faut entrer l'IP du serveur et le port sur lequel Proxmox travaille.



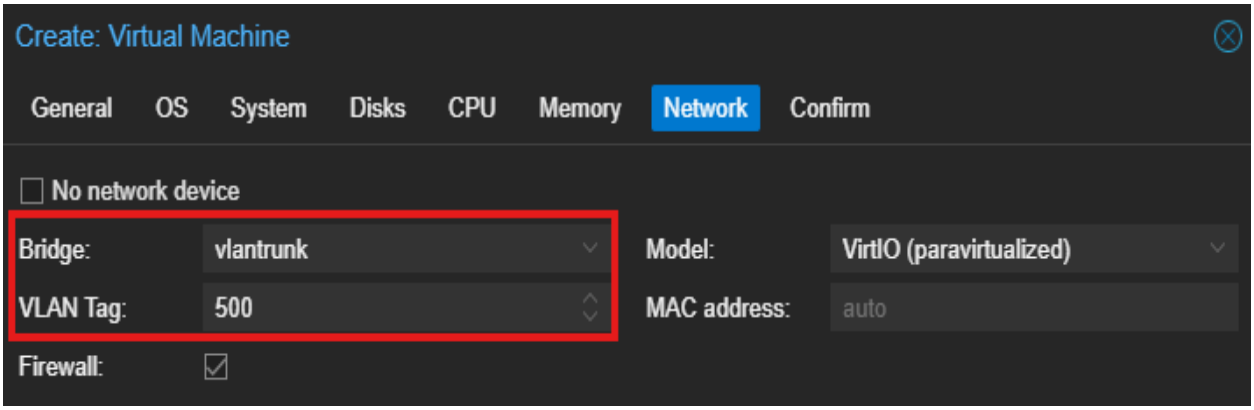
Nous avons créé un Bond entre les interfaces eno2 et eno3 qui servira d'agrégation pour permettre une meilleure répartition des charges et une haute tolérance aux pannes. La procédure est simple :

- On sélectionne le nœud que nous avons créé au préalable.
- Onglet “Network”, on clique sur “create” et on sélectionne “Linux Bond”

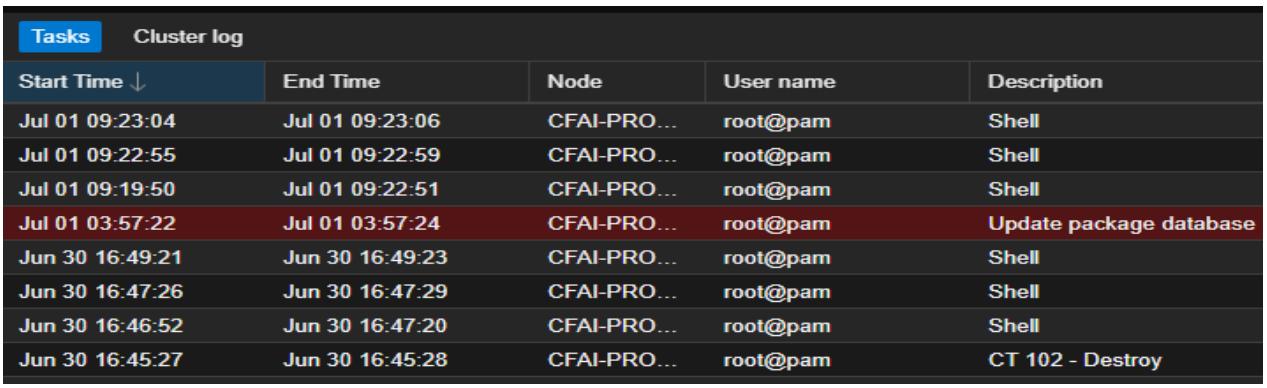


- On nomme notre bond, ici “bond0”.
- Dans l’onglet Slaves on écrit les ports que nous voulons agréger, ici eno2 et eno3.
- Dans l’onglet Mode on choisit **LACP**.

Comme nous travaillons sur différents réseaux (VLAN), lorsque nous créerons de nouvelles VM il ne faudra pas oublier de sélectionner le bon tag :



Le système de log de Proxmox nous permet une vision rapide des différentes actions effectuées récemment. Cela nous permet de surveiller ce qu'il se fait sur le serveur et permet aussi une communication rapide au sein de l'équipe car nous avons l'horodatage qui fournit des données importantes.



Start Time	End Time	Node	User name	Description
Jul 01 09:23:04	Jul 01 09:23:06	CFAI-PRO…	root@pam	Shell
Jul 01 09:22:55	Jul 01 09:22:59	CFAI-PRO…	root@pam	Shell
Jul 01 09:19:50	Jul 01 09:22:51	CFAI-PRO…	root@pam	Shell
Jul 01 03:57:22	Jul 01 03:57:24	CFAI-PRO…	root@pam	Update package database
Jun 30 16:49:21	Jun 30 16:49:23	CFAI-PRO…	root@pam	Shell
Jun 30 16:47:26	Jun 30 16:47:29	CFAI-PRO…	root@pam	Shell
Jun 30 16:46:52	Jun 30 16:47:20	CFAI-PRO…	root@pam	Shell
Jun 30 16:45:27	Jun 30 16:45:28	CFAI-PRO…	root@pam	CT 102 - Destroy

V. Annexe

Active Directory (AD) : Service d'annuaire développé par Microsoft permettant la gestion centralisée, sécurisée et évolutive des utilisateurs, des droits d'accès, des machines et des services (notamment le DNS) au sein d'un domaine.

BDC (Backup Domain Controller) : Contrôleur de domaine secondaire. Il duplique les données du contrôleur principal (PDC) et assure la continuité du service d'authentification en cas de panne de ce dernier.

BitLocker : Solution de chiffrement de disque intégrée à Windows, qui protège les données stockées en cas d'accès physique non autorisé au matériel.

BMC (Baseboard Management Controller) : Contrôleur matériel embarqué permettant la gestion hors bande d'un serveur (ici le serveur Terra), indépendamment du système d'exploitation.

Bond (agrégation de liens) : Regroupement logique de plusieurs interfaces réseau physiques en une seule interface virtuelle, afin d'augmenter la bande passante et d'assurer une tolérance aux pannes.

Bundle : Un fichier .bundle est le format officiel d'installation de VMware sur Linux, car il est universel et compatible avec toutes les distributions. Contrairement aux paquets .deb ou .rpm, il inclut tout le nécessaire : interface, services, et modules à compiler pour le noyau. C'est un script exécutable qui facilite une installation complète et fonctionnelle, sans dépendre du système de paquets des différentes distributions.

DHCP (Dynamic Host Configuration Protocol) : Protocole attribuant automatiquement les paramètres réseau (adresse IP, passerelle, DNS) aux machines d'un réseau.

DNS (Domain Name System) : Service de résolution de noms qui associe le nom d'une machine (hostname) à son adresse IP, et inversement.

Domaine : Regroupement logique de machines et d'utilisateurs administrés de façon centralisée, dont les informations sont stockées dans l'Active Directory.

GLPI (Gestionnaire Libre de Parc Informatique) : Solution open source de gestion de parc informatique et de ticketing (gestion des incidents, des demandes de service et des actifs matériels et logiciels).

GPO (Group Policy Object) : Objet de stratégie de groupe. Ensemble de règles appliquées aux utilisateurs ou aux machines d'un domaine Active Directory (restrictions, déploiements, configuration).

Hyper-V : Hyperviseur de virtualisation de Microsoft, permettant d'exécuter plusieurs machines virtuelles sur un même serveur physique.

iDRAC (Integrated Dell Remote Access Controller) : Interface de gestion hors bande propre aux serveurs Dell, permettant l'administration à distance indépendamment du système d'exploitation.

iLO (Integrated Lights-Out) : Interface de gestion hors bande des serveurs HPE, équivalent fonctionnel de l'iDRAC.

IoT (Internet of Things / Objets connectés) : Désigne les périphériques connectés au réseau autres que les serveurs et les postes de travail (ici l'imprimante et le NAS).

LACP : Protocole qui permet de combiner plusieurs interfaces réseau physiques afin d'augmenter la bande passante totale disponible, par exemple en agrégeant deux liens de 1 Gbit/s pour atteindre 2 Gbit/s. De plus, le protocole répartit de manière intelligente le trafic entre ces interfaces en utilisant un algorithme de hachage, ce qui permet d'optimiser l'utilisation de chaque lien et d'éviter la surcharge d'une seule interface.

LDAP : Lightweight Directory Access Protocol (LDAP) est un protocole qui permet de communiquer avec différents types d'annuaires (y compris Active Directory) et de les interroger.

Miroir : Serveur hébergeant une copie des dépôts de paquets d'une distribution Linux, à partir duquel le système télécharge et met à jour ses logiciels (apt). En contexte RAID, le terme désigne également la duplication intégrale d'un disque sur un autre (RAID 1).

NAS (Network Attached Storage) : Périphérique de stockage en réseau permettant le partage centralisé de fichiers (ici un Synology DS923).

Nextcloud : Solution open source de cloud privé (stockage, partage et édition de fichiers, messagerie), hébergée localement pour conserver la maîtrise des données.

OOB / Out-Of-Band Management : Gestion hors bande d'un serveur, c'est-à-dire un accès d'administration indépendant du système d'exploitation et du réseau de production (iDRAC, iLO, BMC, xClarity).

OOBE (Out-Of-Box Experience) : Phase de premier démarrage de Windows durant laquelle l'utilisateur configure la langue, le compte, etc.

OU (Organizational Unit / Unité d'Organisation) : Conteneur dans l'Active Directory servant à organiser les utilisateurs et les machines, et auquel on lie des GPO.

PDC (Primary Domain Controller) : Contrôleur de domaine principal, qui héberge l'Active Directory de référence.

Proxmox VE : Hyperviseur open source basé sur Linux, offrant virtualisation, gestion de conteneurs, snapshots, sauvegardes et mise en cluster via une interface web.

PXE (Preboot Execution Environment) : Mécanisme de démarrage d'un poste à partir du réseau, utilisé pour le déploiement d'images système via WDS.

RAID (Redundant Array of Independent Disks) : Technologie regroupant plusieurs disques pour améliorer les performances (RAID 0) ou la tolérance aux pannes (RAID 1, RAID 5).

RDP (Remote Desktop Protocol) : Protocole de prise de contrôle à distance d'un bureau, léger car il transmet principalement les commandes d'affichage plutôt que le contenu graphique complet.

Sysprep : Outil Windows préparant une image système (généralisation) avant sa capture et son déploiement sur d'autres postes.

TPM (Trusted Platform Module) : Composant matériel sécurisé stockant les clés de chiffrement, requis en version 2.0 pour Windows 11 et BitLocker.

Trunk : Mode de configuration d'un port de switch laissant passer simultanément le trafic de plusieurs VLAN.

UEFI (Unified Extensible Firmware Interface) : Micrologiciel de démarrage moderne remplaçant le BIOS, requis pour Windows 11 et le TPM 2.0.

Ur-Backup : Solution de sauvegarde open source assurant la sauvegarde et la restauration des données (ici hébergée sur le serveur Terra).

Vaultwarden : Gestionnaire de mots de passe open source et auto-hébergé, permettant de centraliser et de partager de manière sécurisée les identifiants et les clés sensibles de l'infrastructure.

VLAN (Virtual Local Area Network) : Réseau local virtuel permettant de segmenter logiquement un réseau physique afin d'isoler les flux (admin, serveurs, postes, IoT).

VMware : Éditeur et solution de virtualisation permettant d'exécuter des machines virtuelles.

WAN (Wide Area Network) : Réseau étendu ; désigne ici la liaison vers l'extérieur (Internet) au niveau du pare-feu.

WDS (Windows Deployment Services) : Rôle de Windows Server permettant le déploiement d'images système Windows sur le réseau via PXE.

xClarity (Lenovo XClarity Controller) : Interface de gestion hors bande des serveurs Lenovo, équivalent de l'iDRAC et de l'iLO.

Zabbix : Solution open source de supervision réseau permettant de surveiller en temps réel l'état des serveurs, des équipements et des services.