UNIRAIL

Rapport individuel

BLOC 3 : MAINTENIR ET SECURISE LES INFRASTRUCTURES INFORMATIQUES

ETUDIANT : BERNOIS DAMIEN

PROMOTION : ADMINISTRATEUR SYSTEMES ET RESEAUX 2024-25

CESI
ÉCOLE D'INGÉNIEURS

Table des matières

1. Contexte

i. Reformule des besoins

Dans le cadre d'un audit, UNIRAIL a mis à niveau l'infrastructure systèmes et réseaux de son système d'information afin de mettre à disposition des salariés des équipements plus performants. Pour ce faire, les équipements tels que les commutateurs et serveurs ont été implantés dans les nouveaux locaux et une salle serveur a été aménagée.

À la suite de la mise en œuvre de ce précédent projet et afin d'assurer le maintien et la sécurité de la nouvelle infrastructure du système d'information, l'équipe IT se doit d'étudier la mise en place de solution de gestion, de supervision et de sécurisation du parc informatique.

ii. Exigences du client

FT / FC	Fonction	Critères d'acceptation	Niveaux	Flex	Réponse
FT1	Les utilisateurs se connectent de façon sécurisée	Ils se connectent par mot de passe	6	F0	Portail d'authentification avec identifiants (login + mdp) LDAPS hébergé sur le serveur AD1 et AD2
		Une session non utilisée pendant cinq minutes est automatiquement déconnectée	4	F2	GPO qui règle la veille sur 5 minutes
FT2	Les utilisateurs déclarent des incidents	Les utilisateurs déclarent les incidents auprès du service informatique en précisant le problème, ses identifiants, la date et l'heure où il est apparu	6	F1	Mise en place d'un serveur GLPI avec une interface Web, connexion à partir des mêmes identifiants du portail d'authentification, possibilité de renseigner les incidents avec détail (identifiants, date, heure, lieu/équipements concernés)
FT3	L'Administrateur Système et Réseau gère les incidents	L'administrateur diagnostique, met en œuvre la mesure corrective et informe en correspondance avec la procédure établie	6	F0	Diagnostique de l'infrastructure à partir d'un serveur de supervision ZABBIX, procédure de maintenance
		L'administrateur analyse et rapporte à la hiérarchie les indices de performance sur lesquels il est engagé	4	F2	Supervision de l'infrastructure
FT4	Les fichiers sont sauvegardés	Un support de sauvegarde est présent	6	F0	Sauvegarde sur baie de stockage SAN
		La sauvegarde des fichiers est planifiée et optimisée	5	F0	Plan de sauvegarde, backup, planifié à partir d'un serveur VEEAM

		Une sauvegarde externalisée est réalisée			Sauvegarde externalisée sur un hébergeur cloud Leviaa externe français et certifié
FT5	Les applications sont sauvegardées	Un support de sauvegarde est présent	6	F0	Sauvegarde sur baie de stockage SAN
		La sauvegarde des fichiers est planifiée et optimisée	5	F0	Plan de sauvegarde, backup, planifié à partir d'un serveur VEEAM
FT6	Les serveurs sont sauvegardés	Un support de sauvegarde est présent	6	F0	Sauvegarde sur baie de stockage SAN
		La sauvegarde des fichiers est planifiée et optimisée	5	F0	Plan de sauvegarde, backup, planifié à partir d'un serveur VEEAM
FT7	L'Administrateur Système et Réseau effectue une restauration granulaire	L'administrateur peut restaurer systèmes, applications et données	6	F0	Service licence VEEAM backup et restauration
		Il peut définir un ordre de priorité en fonction du tableau annexe 4.1	5	F2	Plan de priorité de sauvegarde défini
FT8	L'Administrateur Système et Réseau répertorie, met à jour, déploie les stations de travail	L'administrateur à un inventaire en temps réel de l'état et caractéristiques de chacun des composants du SI	4	F2	Gestion du parc informatique via GLPI et supervision via ZABBIX
		L'administrateur assure la compatibilité et la mise à jour des composants du SI	6	F0	Plan de maintenance, veille et plan de mise à jour des systèmes
		L'administrateur déploie ou restaure des stations de travail à distance sur la base des profils métier	4	F1	Prise en main à distance via TeamViewer
FT9	L'Administrateur Système et Réseau supervise le réseau en temps réel	L'administrateur peut visualiser les charges réseau, l'état des équipements	4	F2	Supervision via ZABBIX
		L'administrateur peut intervenir pour optimiser les bandes passantes	3	F2	Accès aux configurations des routeurs, commutateurs, de la salle serveur via la machine d'administration
FT10	L'Administrateur Système et Réseau supervise les	L'administrateur peut visualiser l'état des serveurs,	6	F0	Supervision via ZABBIX

	serveurs en temps réel	la charge des baies de stockages			
FC1	Une politique de mot de passe doit être appliquée	Le mot de passe doit être d'authentification forte	6	F1	Politique de mot de passe via PSO (GPO de mot de passe)
		Le mot de passe doit être renouvelé à échéances régulières	6	F0	Politique de mot de passe via PSO (GPO de mot de passe)
		Un mot de passe ne doit pas être défini à l'identique d'un ancien	4	F2	Politique de mot de passe via PSO (GPO de mot de passe)
FC2	Les utilisateurs doivent respecter les bonnes pratiques de cybersécurité	Les utilisateurs ne doivent pas ouvrir des mails de provenance inconnue	6	F0	Politique de cybersécurité (charte)
		Les utilisateurs ne doivent pas communiquer leur adresse professionnelle en dehors de l'exercice de leur fonction	6	F0	Politique de cybersécurité (charte)
		Les utilisateurs ne peuvent ajouter une adresse personnelle dans leur messagerie	6	F0	Politique de cybersécurité (charte)
FC3	Les stations de travail doivent être disponibles en spare	Chaque type de station de travail doit être disponible en spare	4	F2	Plan de sparing des équipements réseaux et d'utilisateurs
FC4	Les incidents doivent être traités sur la base d'une procédure définie	Une procédure doit être établie pour définir les responsabilités et délais à respecter en fonction niveau de maintenance nécessaire (niveau 1 à3).	5	F1	Plan de maintenance défini
FC5	Les sauvegardes doivent être dupliquées sur un site externe	Une sauvegarde externalisée est réalisée	6	F0	Sauvegarde externalisée sur un hébergeur cloud Leviaa externe français et certifié
		La sauvegarde peut être réinternalisée dans un délai maximum de 2 heures	5	F2	Rapidité de réplication des données vers le LAN
FC6	Le réseau doit être protégé	Seuls les terminaux déclarés de l'entreprise	6	F0	Administration uniquement via machine d'administration

	contre les intrusions	peuvent se connecter au réseau			sur les terminaux des équipements réseaux définis par le VLAN "Admin"
		Garantir la sécurité des connexions nomades sur des réseaux publics	6	F0	Mise en place d'un serveur VPN/agent VPN, d'un VLAN "Distant", ainsi que d'ACL pour ce réseau distant
FC7	L'accès à la salle serveur doit être sécurisé	L'accès à la salle serveur doit faire l'objet d'une authentification	6	F1	carte d'accès + digicode
		Les ouvertures extérieures doivent être sécurisées	5	F1	Badge d'accès
FC8	L'ensemble du système d'information doit être protégé par antivirus	L'administration doit être centralisée	6	F0	Antivirus centralisé sur un serveur
		La solution doit être à faible consommation de ressources sur les tous les terminaux	5	F1	Etude d'une antivirus à faible consommation de ressources
		La solution doit être résiliente face aux menaces avancées	5	F2	Antivirus efficace, rapide, puissant

iii. Plan budgétaire

- Coût matériel :

Référence	Quantité	Durée	Prix UHT	Prix HT
VCenter VMware pour ESXI	1	∞	6 500€	6 500 €
Licence de support pour VCenter	1	3 ans	3 400 €	3 400 €
VMware vSphere 7 entreprise Plus (par CPU)	6 +2	∞	3 600 €	28 800 €
Licence support vSphere (par CPU)	6 +2	3 ans	1 600 €	12 800 €
Licence Windows Server 2022 standard	6	∞	600 €	3 600 €
Commutateur Cisco C9200-24P-E	1	∞	1 965,26 €	1 965,26 €
Commutateur Cisco C9200-8P-E	1	∞	965,4 €	965,4 €
Routeur Cisco C891F-K9	1	∞	925 €	925 €
Pare-feu Stormshield SN-S-Series 320	1	∞	2 036,4 €	2 036,4 €
Borne Wi-Fi Cisco Catalyst 9115AXI-E	2	∞	470 €	940 €
Imprimante HP LaserJet Ent MFP 137fnw	1	∞	780,22 €	780,22 €
Traceur HP DesignJet T230	1	∞	632,8 €	632,8 €
Serveur physique DELL PowerEdge R750xs	1	∞	3 583 €	3 583 €
Carte contrôleur RAID 6 Areca ARC-1883ix-12	1	∞	1 620 €	1 620 €
Disques durs WD SATA Gold 20 To	5	∞	486,99 €	2 434,95 €
Kit clavier et souris bureautique Logitech Desktop MK120	15	∞	22,41 €	336,15 €
Ecran IIYAMA XUB2463HSU-B1	10	∞	120 €	1 200 €
Station de travail Lenovo Thinkstation P2 Tower	6	∞	715,9 €	4 295,4 €
Ordinateur portable Lenovo ThinkBook T16	5	∞	498 €	2 490 €

- Coût humain :

Référence	Durée	Prix UHT	Prix HT
Directeur général	5 mois	4 500 €	22 500 €
Directeur technique	5 mois	3 200 €	16 000 €
Administrateur système et réseau	5 mois	3 000 €	15 000 €
Responsable paie	1 mois	2 800 €	2 800 €
Déploiement de la commande de matériel à la formation des utilisateurs	1 mois	4 360 €	4 360 €

- Coût total :

L'estimation du coût total de la mise en œuvre de ce projet est estimé à 139 964,6 € (comprenant les coûts humains et matériels), dont 16 200 € seront à renouveler tous les 3 ans.

iv. Pilotage du projet

- Indicateur de suivi :

Les indicateurs de suivi sont un outil de gestion du projet qui permet de suivre l'avancement de différentes étapes du projet tout au long de ce dernier, tels que :

- Suivi des coûts des différentes ressources par rapport au plan budgétaire étudié en amont : (coûts estimés – coûts réels).
- Suivi de l'avancement des différentes étapes et respect des jalons par rapport au planning organisationnel prévu initialement : (durées estimées – durées réelles).
- Les risques et niveaux de priorités de chacune des tâches du projet : (utilisation d'une matrice des risques).
- Suivi de la disponibilité des ressources humaines tout au long du projet par rapport aux besoins exprimés en amont : (% de disponibilité et de temps de réponse).

- Indicateur de réussite/performance (KPI) :

Les indicateurs de réussite sont aussi un outil de gestion du projet qui permet d'assurer l'atteinte des objectifs de ce dernier, tels que :

- Les résultats de la recette de tests et des bons fonctionnements de la mise en place des services et équipements réseaux : (% des résultats prédis par rapport au % des résultats obtenus).
- La satisfaction des parties prenantes internes et externes au projet par rapport à leurs attentes des fonctionnalités et services fournis par l'entreprise : (% de satisfaction obtenue).
- Une plus-value en termes d'efficacité et de vitesse de production et de performance des services : (% de latence du trafic minimisé et %).
- Le calcul du retour sur investissement (ROI) à partir des coûts totaux du projet par rapport aux bénéfices financiers : (% de retour sur l'investissement).

2. Maintenance SI

A. Ticketing

i. Solution retenue

La solution de ticketing retenue est celle fournie par le service OpenSource "GLPI". Cet outil permet de centraliser la remonter d'incident à l'aide d'un système de tickets rédiger par l'utilisateur concerné et une plateforme de gestion de ces derniers pour le service informatique afin de pouvoir y répondre et corriger ces incidents efficacement. De plus, GLPI peut nous permettre de faire de l'inventaire de parc informatique à l'aide d'un agent "GLPI Inventory" ("FusionInventory" n'étant plus maintenu) installer sur les équipements concernés.

Son interface est intuitive et complet, que cela soit pour les utilisateurs, mais aussi pour les administrateurs.

Les utilisateurs et administrateurs communiquent avec l'interface WEB du serveur GLPI en HTTPS.

GLPI est une solution de ticketing très modulable permettant de mettre en place une grande variété de plugins afin de répondre à un grand nombre de besoins, mais ainsi peu coûteuse en ressources (ressources de trafic réseau et ressources systèmes du serveur) contrairement à d'autres solutions telles que "OTRS". De plus, son interface WEB est complète et permet une gestion des tickets, du parc et de l'inventaire du SI.

Etant un service OpenSource, et donc gratuit, aucun support n'est garanti. Cependant, beaucoup de communautés et de forums actifs sont formés autour de ce logiciel permettant la veille et l'information accessibles à tout le monde.

ii. Ressources allouées

Serveur physique	Nom de VM	Service/Fonctionnalité	CPU	RAM	Stockage
ESXI 2	UR-V-SUP-001	Ticketing et gestion du parc informatique	6 vCPU	16 Go	Système : 150 Go Reste : 2 To

Le trafic réseau qu'engendrera le serveur de ticketing et de gestion du parc informatique GLPI devra être de priorité moyenne afin d'assurer l'inventaire du parc informatique, ainsi que la remontée des incidents.

iii. Politique de réponse des incidents

- Matrice priorité/impact des incidents :

		Impact				
		Très haute	**Haute**	**Moyen**	**Bas**	**Très bas**
Priorité	**Très haute**					
	Haute					
	Moyenne					
	Basse					
	Très basse					

- Réponse à l'échelle de criticités des incidents :

Criticité	Délais	Responsabilité
	1 mois maximum	Equipe support informatique / prestation de support
	3 semaines maximum	Equipe support informatique / prestation de support Délégation à l'Administrateur système et réseau en cas de blocage
	1 semaines et ½ maximum	Administrateur système et réseau
	6 jours maximum	Administrateur système et réseau et le reste de l'équipe IT si besoin
	3 jours maximum	Administrateur système et réseau et le reste de l'équipe IT si besoin

B. Supervision

i. Solution retenue

La solution de supervision retenue est celle fournie par le service OpenSource "ZABBIX". Cet outil permet de superviser, de surveiller et d'alerter l'entièreté de notre infrastructure réseau et système à l'aide d'une communication directe et privée (chiffrement TLS 1.3 disponible à partir de la version 6.X de ZABBIX et n'est pas configuré par défaut) entre le serveur et ses agents.

Pour ce faire, un agent ZABBIX est installé sur la machine destination de la supervision, le serveur et l'agent communiqueront sur le protocole 10050 et 10051 en mode PULL/PUSH tel que :

- Le serveur PULL sur les agents : le serveur interroge le client.
- Les agents PUSH sur le serveur : l'agent envoie les données au serveur.

L'interface Web est accessible en HTTPS et permet de configurer les différents points de supervision, ainsi que les alertes.

ZABBIX est une solution de supervision très peu coûteuse en ressources (ressources de trafic réseau, ressources système des agents, ressources systèmes du serveur) contrairement à d'autres solutions telles que "Prometheus". De plus, son interface de configuration est complète et permet une supervision totale de l'infrastructure réseau et système du SI.

Etant un service OpenSource, et donc gratuit, aucun support n'est garanti. Cependant, beaucoup de communautés et de forums actifs sont formés autour de ce logiciel permettant la veille et l'information accessibles à tout le monde.

ii. Ressources allouées

Serveur physique	Nom de VM	Service/Fonctionnalité	CPU	RAM	Stockage
ESXI 2	UR-V-SUP-001	Supervision de l'infrastructure	6 vCPU	16 Go	Système : 150 Go Reste : 1 To

Le trafic réseau qu'engendrera le serveur de supervision Zabbix devra être de priorité haute afin d'assurer sa communication en temps réel avec l'entièreté de l'infrastructure.

C. Politique de mise à jour des systèmes

i. Solution retenue

Il est nécessaire d'étudier un plan de mises à jour des systèmes Windows étant donné le parc informatique majoritairement sous Windows. Pour assurer ces dernières, une solution de mise à jour système est retenue, celle du service « WAPT », pour les composantes suivantes :

- Déploiement rapide de paquets logiciels, mises à jour et licences sur un environnement Windows.
- Historique des actions effectuées par le serveur WAPT (cycle de vie, mises à jour poussées, paquets supprimés, etc.).
- Certifier « Sécurité de Premier Niveau » (CSPN) par l'ANSSI, assurant sa fiabilité.
- Scripting de paquet possible permettant d'automatiser les déploiements.
- Vérification de la conformité des logiciels et mises à jour avant l'éteignement de la machine agent (pas de pop-up sur le bureau de l'utilisateur lors de l'utilisation de la machine).
- Moins demandeur en ressources que la solution WSUS déployable sur un Windows Server.
- Possibilité pour les utilisateurs de déployer les logiciels à disposition.

Le déploiement des paquets sur le réseau, du serveur WAPT à l'agent, se fait de façon chiffré à partir du protocole HTTPS (443).

Les utilisateurs pourront déployer des logiciels à leur disposition autorisés par le SI à l'aide de la fonctionnalité « WAPT Self Service », une interface graphique sur laquelle se retrouver tous les logiciels, pouvant être installés rapidement.

De plus, le service Windows Server Update Services (WSUS) permet de centraliser la gestion du déploiement des mises à jour des produits Microsoft sur le réseau.

ii. Ressources allouées

Serveur physique	Nom de VM	Service/Fonctionnalité	CPU	RAM	Stockage
ESXI 1	UR-V-WW-001	Déploiement et mises à jour système	4 vCPU	8 Go	Système : 150 Go Reste : 2 To

Le trafic réseau qu'engendrera le serveur de déploiement WAPT devra être de priorité haute afin d'assurer le déploiement rapide des paquets logiciels et mises à jour vers les hôtes obsolètes.

iii. Politique de déploiement

- Le déploiement d'un logiciel par un utilisateur sur son propre poste pourra être assuré grâce à l'interface « WAPT Self Service », sur laquelle les utilisateurs pourront sélectionner les logiciels voulant être installés sur leur poste, qui seront évidemment étudiés, vérifiés, configurés et autorisés en amont par l'équipe IT.
- Le délai du déploiement des paquets pour les nouvelles mises à jour se fera 1 mois après la sortie de cette dernière au grand public afin de laisser le fournisseur corriger les failles de sécurité de sa version.

- La vérification des versions des logiciels se fait lors de l'éteignement de la machine. Si une version est obsolète, le serveur WAPT enverra un paquet de la version à jour de ce dernier à la machine cible.

iv. Exemple de l'architecture d'un déploiement

Paquet : « Windows Update »

- Windows10.0.-XXXXXX-x64.msu
- setup.py
- control

```python
from setuphelpers import
#Windows 10 22H2.
min_version_nb = 19045

def windows_version_ok ():
    #Récupère la version Windows de la machine.
    version_info = get_windows_version()
    version_nb = int(version_info['version_nb'])
    #Si version machine > version minimale autorisée, alors 0, sinon 1.
    return version_nb > min_version_nb

def install ()
    #Si 0, alors continu.
    if not windows_version_ok():
        print ("Version Windows obselète. Une mise à jour est nécessaire. Veuillez ne pas éteindre la station ! Merci.")
        #Récupère la dernière version fournie dans le paquet "Windows Update".
        update = makepath(basedir, 'Windows10.0.-XXXXX-x64.msu')
        #Installe la dernière version.
        run('wusa "{}" /quiet /norestart'.format(update))
```

D. Politique de maintenance

i. Plan préventif

Tâche	Fréquence	Action	Responsabilité	Criticité
Mise à jour des OS et logiciels	Hebdomadaire / Mensuelle	Correction des failles de sécurité, ajout de fonctionnalité	Administrateur Systèmes et Réseaux	2
Sauvegardes automatiques	Quotidienne incrémentielle (22h à 6h) Hebdomadaire complète (dimanche)	Sauvegarde des données en cas de besoin de restauration ou perte de données	Administrateur Systèmes et Réseaux	3
Supervision	Quotidien	Mise en place d'alerte sur les équipements réseaux, les serveurs, les services, saturation des disques et des performances	Administrateur Systèmes et Réseaux	2
Contrôle des logs	Quotidien	Vérification des sauvegardes et du réseau (trafic, conformité, consommation et sécurité)	Administrateur Systèmes et Réseaux	2
Support informatique (ticketing GLPI)	Quotidien	Support informatique à disposition des utilisateurs, possibilité de reporter les incidents	Administrateur Systèmes et Réseaux OU Prestation de support informatique N1	1

ii. Plan correctif

Tâche	Fréquence	Action	Responsabilité	Criticité
Intrusion ou cyberattaque	Détection en -1h	Isolation de la cible, vérification des serveurs/services/sauvegardes/logs, contact avec les autorités compétentes (judiciaires, ANSSI, CNIL)	Administrateur Systèmes et Réseaux Directeur Technique	3
Panne serveur et/ou service	Remise en service -4h	Détection par les alertes de supervision ou le retour des utilisateurs. Remise en service sous 1 jour (1 semaine maximum cas exceptionnel/contact avec le fournisseur)	Administrateur Systèmes et Réseaux Directeur Technique	3
Saturation de l'espace de stockage (baie de stockage/baie de sauvegarde)	Détection en -1j	Nettoyage des volumes, ajout de volumes physique	Administrateur Systèmes et Réseaux Directeur Technique	2
Saturation des performances des services/applications	Détection en -1j	Révision des priorités de flux, augmentation de la bande passante, retravailler le programme	Administrateur Systèmes et Réseaux Directeur Technique	2

3. Plan de continuité informatique (PCI/PCA)

L'objectif du Plan de Continuité des Activités est de mettre en place une stratégie permettant de garantir la continuité des activités critiques de l'entreprise en cas de sinistre affectant le SI. Il est essentiel pour minimiser les interruptions et assurer la résilience de l'entreprise.

Ce plan couvre la totalité des ressources systèmes et réseaux de l'infrastructure du SI (serveurs physiques/virtuels, équipements réseaux, services, etc.).

Le PCA intervient immédiatement lors d'une perturbation. Il s'agit d'une réponse en temps réel pour garantir que les opérations critiques ne soient pas interrompues.

A. Audit de l'existant

i. Machine virtuelle

Nom	Service	vCPU	RAM	Volume	Carte réseau
UR-V-DC-001	AD / DNS / DHCP	6	8	150Go	2G
UR-V-DC-002	AD / DNS / VEEAM	6	16	150Go / 250Go	4G
UR-V-FS-001	Fichier (DFS) / Imprimantes	4	32	150Go / 2*4To	8G
UR-V-WW-001	WSUS / NTP / WAPT	4	8	150Go / 2To	4G
UR-V-PXE-001	PXE / FTP	2	8	150Go / 250Go	2G
UR-V-ERP-001	Sage / Project	14	32	150Go / 2*4To	8G
UR-V-VPN-001	OpenVPN	4	8	150Go / 250Go	8G
UR-V-SUP-001	GLPI / ZABBIX	6	16	150Go / 1To	8G

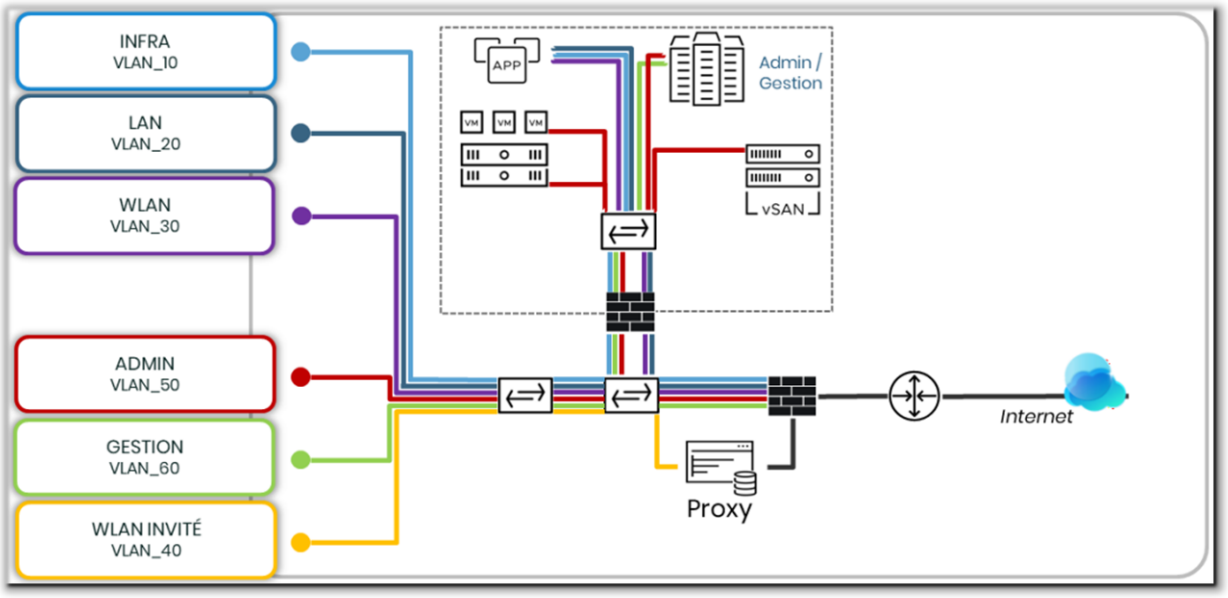
ii. VLAN

Numéro	Nom	Réseau	Réservations	Première IP	Dernière IP	Passerelle
10	Infra	192.168.1.0	Toute la plage	S/O	S/O	192.168.1.254
20	LAN	192.168.2.0	1-10 / 240-254	192.168.2.11	192.168.2.239	192.168.2.254
30	WLAN	192.168.3.0	1-25 / 240-254	192.168.3.26	192.168.3.239	192.168.3.254
40	WLAN invité	192.168.4.0	1-25 / 240-254	192.168.4.26	192.168.4.239	192.168.4.254
50	Admin	192.168.5.0	1-10 / 240-254	192.168.5.11	192.168.5.239	192.168.5.254
60	Gestion	192.168.6.0	1-10 / 240-254	192.168.6.11	192.168.6.239	192.168.6.254
70	Distant	192.168.7.0	1-10 / 240-254	192.168.7.11	192.168.7.239	192.168.7.254

iii. Equipements réseaux

Equipements	Quantité
Commutateur Cisco C9200-24P-E	2
Commutateur Cisco C9200-8P-E	2
Routeur Cisco C891F-K9	2
Pare-feu Stormshield SN-S-Series 320	2
Borne Wi-Fi Cisco Catalyst 9115AXI-E	4
Imprimante HP LaserJet Ent MFP 137fnw	3
Traceur HP DesignJet T230	2
Serveur physique DELL PowerEdge R750xs	2
Baie de stockage Synology SAN UC3200	1

iv. Flux réseau



v. Règles d'accès

- INFRA :
  - ALLOW : 192.168.1.0 to "internet"
  - ALLOW : 192.168.1.0 to UR-V-DC-001
  - ALLOW : 192.168.1.0 to UR-V-DC-002
  - ALLOW : 192.168.1.0 to UR-V-FS-001
  - ALLOW : 192.168.1.0 to UR-V-WW-001
  - ALLOW : 192.168.1.0 to UR-V-PXE-001
  - ALLOW : 192.168.1.0 to UR-V-ERP-001
  - ALLOW : 192.168.1.0 to UR-V-VPN-001
  - ALLOW : 192.168.1.0 to UR-V-SUP-001
  - DENY : ALL ANY

- LAN :
  - ALLOW : 192.168.2.0 to "internet"
  - ALLOW : 192.168.2.0 to UR-V-DC-001 eq 636 (LDAPS)
  - ALLOW : 192.168.2.0 to UR-V-DC-001 eq 67 (DHCP)
  - ALLOW : 192.168.2.0 to UR-V-DC-001 eq 68 (DHCP)
  - ALLOW : 192.168.2.0 to UR-V-DC-001 eq 53 (DNS)

- ALLOW : 192.168.2.0 to UR-V-DC-002 eq 636 (LDAPS)
- ALLOW : 192.168.2.0 to UR-V-DC-002 eq 67 (DHCP)
- ALLOW : 192.168.2.0 to UR-V-DC-002 eq 68 (DHCP)
- ALLOW : 192.168.2.0 to UR-V-DC-002 eq 53 (DNS)
- ALLOW : 192.168.2.0 to UR-V-FS-001 eq 445 (SMB)
- ALLOW : 192.168.2.0 to UR-V-FS-001 eq 631 (IPP)
- ALLOW : 192.168.2.0 to UR-V-FS-001 eq 69 (TFTP)
- ALLOW : 192.168.2.0 to UR-V-WW-001 eq 8531 (WSUS)
- ALLOW : 192.168.2.0 to UR-V-WW-001 eq 123 (NTP)
- ALLOW : 192.168.2.0 to UR-V-WW-001 eq 443 (WAPT)
- ALLOW : 192.168.2.0 to UR-V-PXE-001 eq 67 (PXE : DHCP)
- ALLOW : 192.168.2.0 to UR-V-PXE-001 eq 68 (PXE : DHCP)
- ALLOW : 192.168.2.0 to UR-V-PXE-001 eq 69 (PXE : TFTP)
- ALLOW : 192.168.2.0 to UR-V-PXE-001 eq 4011 (PXE : BINL)
- ALLOW : 192.168.2.0 to UR-V-PXE-001 eq 20 (FTP)
- ALLOW : 192.168.2.0 to UR-V-PXE-001 eq 21 (FTP)
- ALLOW : 192.168.2.0 to UR-V-ERP-001 eq 443 (HTTPS : ERP et Project)
- ALLOW : 192.168.2.0 to UR-V-SUP-001 eq 443 (HTTPS : GLPI)
- DENY : ALL ANY

➢ WLAN :

- ALLOW : 192.168.3.0 to "internet"
- ALLOW : 192.168.3.0 to UR-V-DC-001 eq 636 (LDAPS)
- ALLOW : 192.168.3.0 to UR-V-DC-001 eq 67 (DHCP)
- ALLOW : 192.168.3.0 to UR-V-DC-001 eq 68 (DHCP)
- ALLOW : 192.168.3.0 to UR-V-DC-001 eq 53 (DNS)
- ALLOW : 192.168.3.0 to UR-V-DC-002 eq 636 (LDAPS)
- ALLOW : 192.168.3.0 to UR-V-DC-002 eq 67 (DHCP)
- ALLOW : 192.168.3.0 to UR-V-DC-002 eq 68 (DHCP)
- ALLOW : 192.168.3.0 to UR-V-DC-002 eq 53 (DNS)
- ALLOW : 192.168.3.0 to UR-V-FS-001 eq 445 (SMB)

- ALLOW : 192.168.3.0 to UR-V-FS-001 eq 631 (IPP)
- ALLOW : 192.168.3.0 to UR-V-FS-001 eq 69 (TFTP)
- ALLOW : 192.168.3.0 to UR-V-WW-001 eq 8531 (WSUS)
- ALLOW : 192.168.3.0 to UR-V-WW-001 eq 123 (NTP)
- ALLOW : 192.168.3.0 to UR-V-WW-001 eq 443 (WAPT)
- ALLOW : 192.168.3.0 to UR-V-PXE-001 eq 67 (PXE : DHCP)
- ALLOW : 192.168.3.0 to UR-V-PXE-001 eq 68 (PXE : DHCP)
- ALLOW : 192.168.3.0 to UR-V-PXE-001 eq 69 (PXE : TFTP)
- ALLOW : 192.168.3.0 to UR-V-PXE-001 eq 4011 (PXE : BINL)
- ALLOW : 192.168.3.0 to UR-V-PXE-001 eq 20 (FTP)
- ALLOW : 192.168.3.0 to UR-V-PXE-001 eq 21 (FTP)
- ALLOW : 192.168.3.0 to UR-V-ERP-001 eq 443 (HTTPS : ERP et Project)
- ALLOW : 192.168.3.0 to UR-V-SUP-001 eq 443 (HTTPS : GLPI)
- DENY : ALL ANY

➢ WLAN Invité :

- ALLOW : 192.168.4.0 to "internet"
- DENY : ALL ANY

➢ ADMIN :

- ALLOW : 192.168.5.0 to ALL ANY
- DENY : ALL ANY

➢ GESTION :

- ALLOW : 192.168.6.0 to "internet"
- ALLOW : 192.168.6.0 to UR-V-ERP-001 eq 443 (HTTPS : ERP et Project)
- DENY : ALL ANY

➢ DISTANT :

- ALLOW : 192.168.7.0 to UR-V-DC-001 eq 636 (LDAPS)
- ALLOW : 192.168.7.0 to UR-V-DC-001 eq 67 (DHCP)
- ALLOW : 192.168.7.0 to UR-V-DC-001 eq 68 (DHCP)

- ALLOW : 192.168.7.0 to UR-V-DC-001 eq 53 (DNS)
- ALLOW : 192.168.7.0 to UR-V-DC-001 eq 636 (LDAPS)
- ALLOW : 192.168.7.0 to UR-V-DC-002 eq 67 (DHCP)
- ALLOW : 192.168.7.0 to UR-V-DC-002 eq 68 (DHCP)
- ALLOW : 192.168.7.0 to UR-V-DC-002 eq 53 (DNS)
- ALLOW : 192.168.7.0 to UR-V-FS-001 eq 69 (TFTP)
- ALLOW : 192.168.7.0 to UR-V-ERP-001 eq 443 (HTTPS : ERP et Project)
- ALLOW : 192.168.7.0 to UR-V-FS-001 eq 69 (TFTP)
- ALLOW : 192.168.7.0 to UR-V-VPN-001 eq 443 (HTTPS)
- DENY : ALL ANY

➢ Matrice de communication VLAN vers Serveurs :

		DEPUIS						
	VLAN /Srv	INFRA	LAN	WLAN	WLAN Invité	ADMIN	GESTION	DISTANT
VERS	UR-V-DC-001							
	UR-V-DC-002							
	UR-V-FS-001							
	UR-V-WW-001							
	UR-V-PXE-001							
	UR-V-ERP-001							
	UR-V-SUP-001							
	UR-V-VPN-001							

- Matrice de communication VLAN vers Ports/Protocoles :

		DEPUIS						
	VLAN /Srv	INFRA	LAN	WLAN	WLAN Invité	ADMIN	GESTION	DISTANT
VERS	LDAPS							
	DHCP							
	DNS							
	SMB							
	IPP							
	TFTP							
	WSUS							
	NTP							
	BINL							
	FTP							
	HTTP							
	HTTPS							
	Internet							

vi. Gestion de l'infrastructure

La stratégie de gestion de l'infrastructure système et réseau du SI adoptée est celle d'une gestion centralisée.

Pour ce faire, un VLAN "ADMIN" a été mis en place et a un accès permissif complet sur la totalité de l'infrastructure.

Cette gestion se fera à partir d'une machine d'administration branchée directement sur des terminaux dédiés à l'administrateur des éléments sensibles de l'infrastructure.

Cette machine d'administration se trouve dans la salle serveur (sécurisée par une carte d'authentification à badger, ainsi qu'un digicode à 6 chiffres (réinitialisation du code tous les 3 mois, effectuer par le directeur technique), mais aussi d'un mot de passe robuste sur la machine, ainsi qu'une connexion à double facteur à disposition uniquement du Directeur Technique, ainsi que de l'Administrateur Système et Réseau).

vii. VPN

Les utilisateurs nomades se voient attribuer un agent VPN "OpenVPN" qui permettra la communication avec le serveur OpenVPN hébergé sur le LAN UNIRAIL. De ce fait, le serveur VPN attribuera une IP privée du réseau 192.168.7.0) à l'utilisateur du VLAN « Distant », ce qui permettra à ce dernier de pouvoir communiquer avec les différentes composantes de l'infrastructure à l'aide des règles de filtrage.

viii. Sécurisation du SI

La sécurisation du SI se fait avant tout à l'aide du cluster de pare-feu mis en place en barrière des modems FAI d'accès à internet, ces derniers ont une configuration très stricte des trafics entrants et sortants autorisés. De plus, des alertes et des logs sont mis en place afin de remonter les informations en cas de sinistre ou de cyberattaque.

En somme, un antivirus est déployé sur le parc informatique du SI, sécurisant la totalité des équipements utilisateurs et des serveurs à l'aide de la solution « Sophos Intercept X Advanced ».

Ces deux derniers détectent et préviennent contre les intrusions grâce à une stratégie IDS et IPS.

Pour finir, la mise en place d'alerte de supervision à l'aide de la solution ZABBIX permet d'assurer la remontée des problèmes sur l'entièreté du SI.

ix. Plan de sauvegarde / restauration

- Solution de sauvegarde :
    - Solution interne :
        - Baie de stockage SAN
        - Redondance de l'alimentation de la baie
        - Plan de stockage RAID6
        - Redondance de la carte RAID6
        - Volume de stockage réel de 240To

- Volume de stockage exploitable de 120To
- Sauvegarde incrémentielle journalière à 1h
- Sauvegarde complète hebdomadaire le dimanche, à 1h
- Rétention des sauvegardes incrémentielles de 10j
- Rétention des sauvegardes complètes de 28j

Alimentation et carte du contrôleur redondante pour la baie de stockage (prévoir d'en racheter lorsque la première ne fonctionnera pas, pour garder une redondance de secours à tout instant).

- Solution externe :
  - Stockage externalisé sur un Cloud extérieur à l'entreprise
  - Volume de stockage réel de 40To
  - Ré-internalisation des données externalisées en moins de 2h
  - Sauvegarde incrémentielle journalière à 1h du LAN au Cloud
  - Sauvegarde complète hebdomadaire le dimanche, à 1h
  - Rétention des sauvegardes incrémentielles de 10j
  - Rétention des sauvegardes complètes de 28j

Nous optons pour une seconde solution de stockage à distance, externe à l'entreprise, mais basée en France afin d'assurer l'application des lois et normes RGPD françaises quant aux données. De plus, Leviaa est certifiée ISO 27001 et HDS par le ministère de la santé et des accès aux soins comme étant un hébergeur de confiance pour la sauvegarde de données de santé à caractère personnel.
Cette seconde solution est assurée par Leviia, un service de stockage 100 % et soucieux de l'environnement. Fondée en 2020, elle offre un espace de stockage de haute disponibilité sur son Cloud. De plus, elle s'engage à compenser ses émissions de carbone à 200 % en optimisant l'utilisation de ses serveurs, en finançant l'association Reforest'Action.

➢ Equipements :

Equipements	Référence	PHT €	Quantité	PTHT €
Baie de stockage	Synology SAN UC3200	5 930 €	1	5 930 €
Disques durs	WD SATA Gold 20 To	486,99 €	12	5 843.88 €
Stockage Cloud	Cloud Leviaa		Abonnement 120 To	15 000 € / an

➢ Granulation des sauvegardes :

« Veeam Backup & Recovery » est une solution de restauration granulaire des fichiers d'une machine sans avoir à restaurer l'ensemble des données d'un système ou d'une VM.

Solution	Quantité	PTHT €
Veeam Backup & Recovery	6 VM + 18,4 To	1 020 € /mois 12 240 € /an

➢ Plan de sauvegarde :

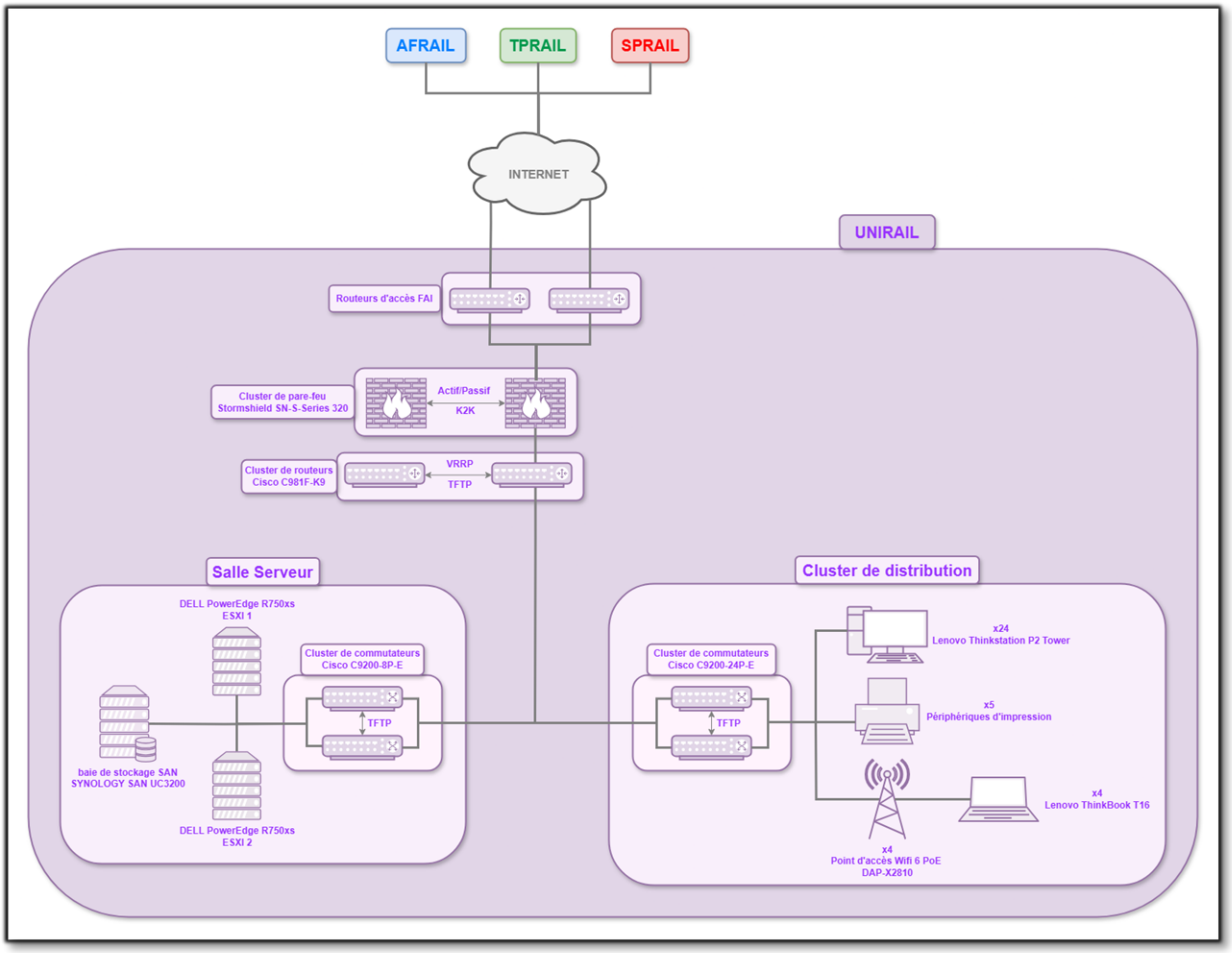
Nous mettons en place un plan de sauvegarde incrémentielle, étant donné son fonctionnement, il assure une récupération rapide et facile tout en optimisant l'utilisation du stockage de la sauvegarde.

La sauvegarde incrémentielle enregistre qui copie uniquement les fichiers modifiés depuis la dernière sauvegarde.

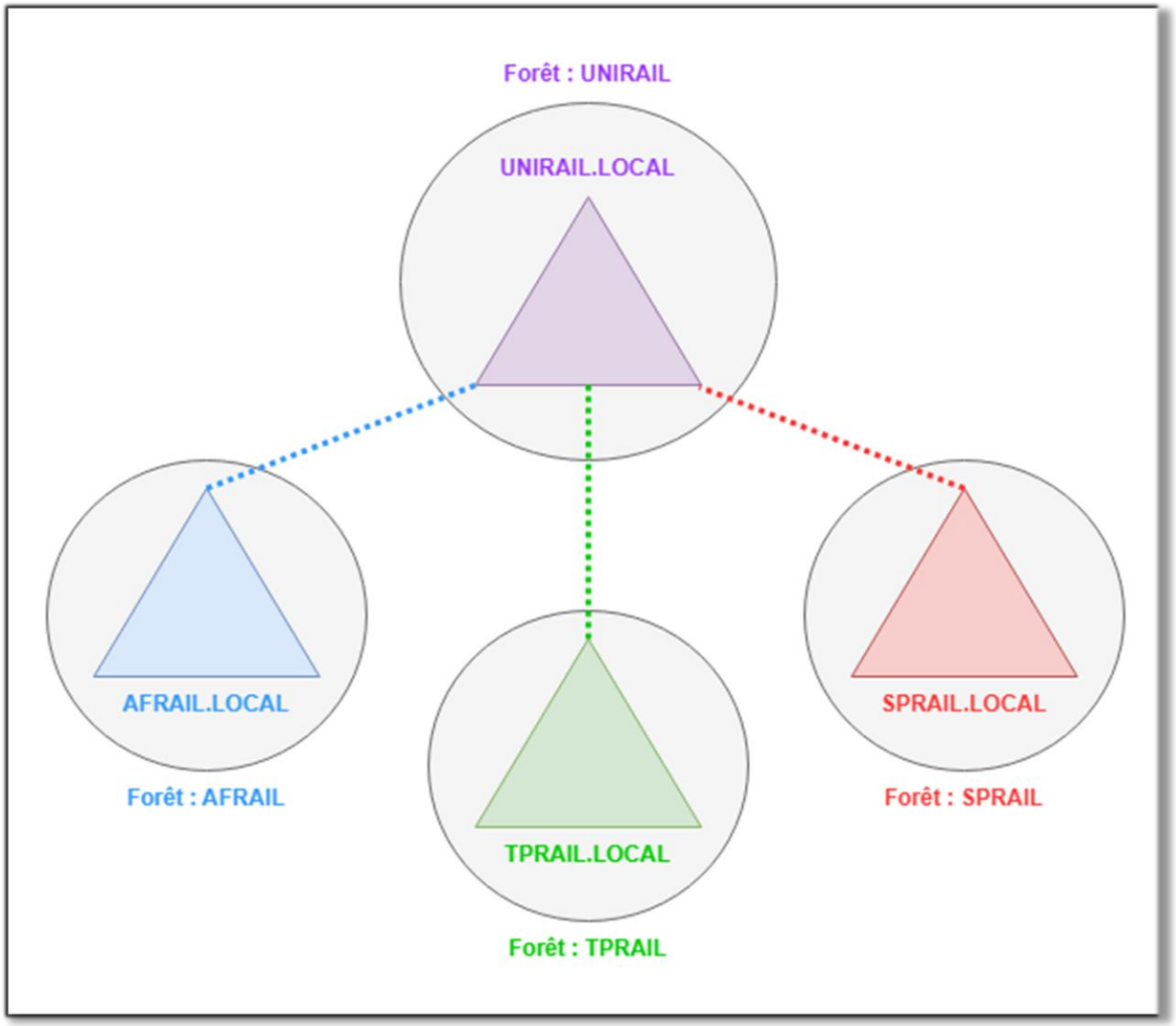
- La sauvegarde complète sera effectuée tous les dimanches à 1 H.
- La sauvegarde incrémentielle sera effectuée tous les jours à 1 H (excluant le dimanche).

x. Cartographie

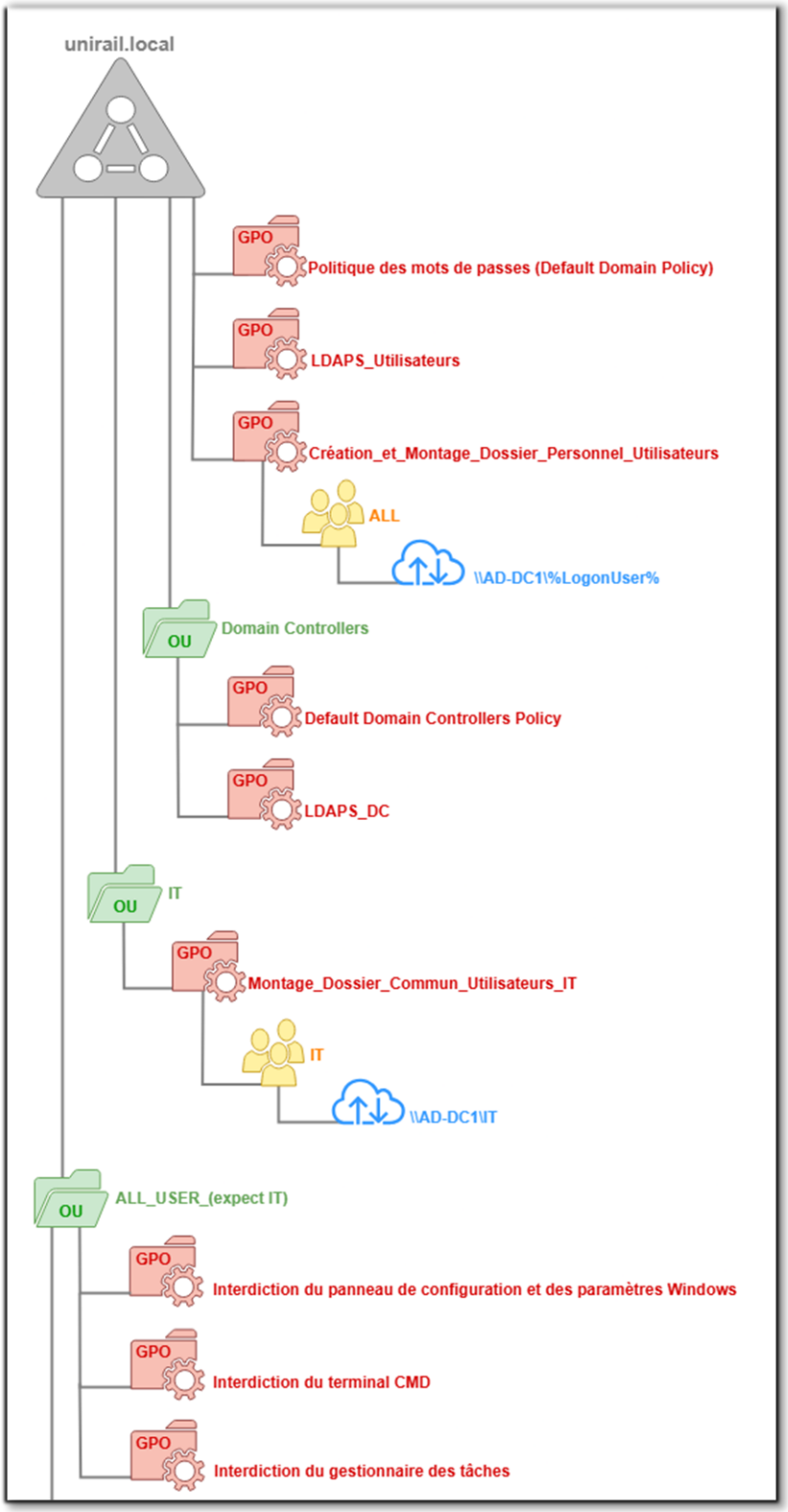
➢ Réseau :

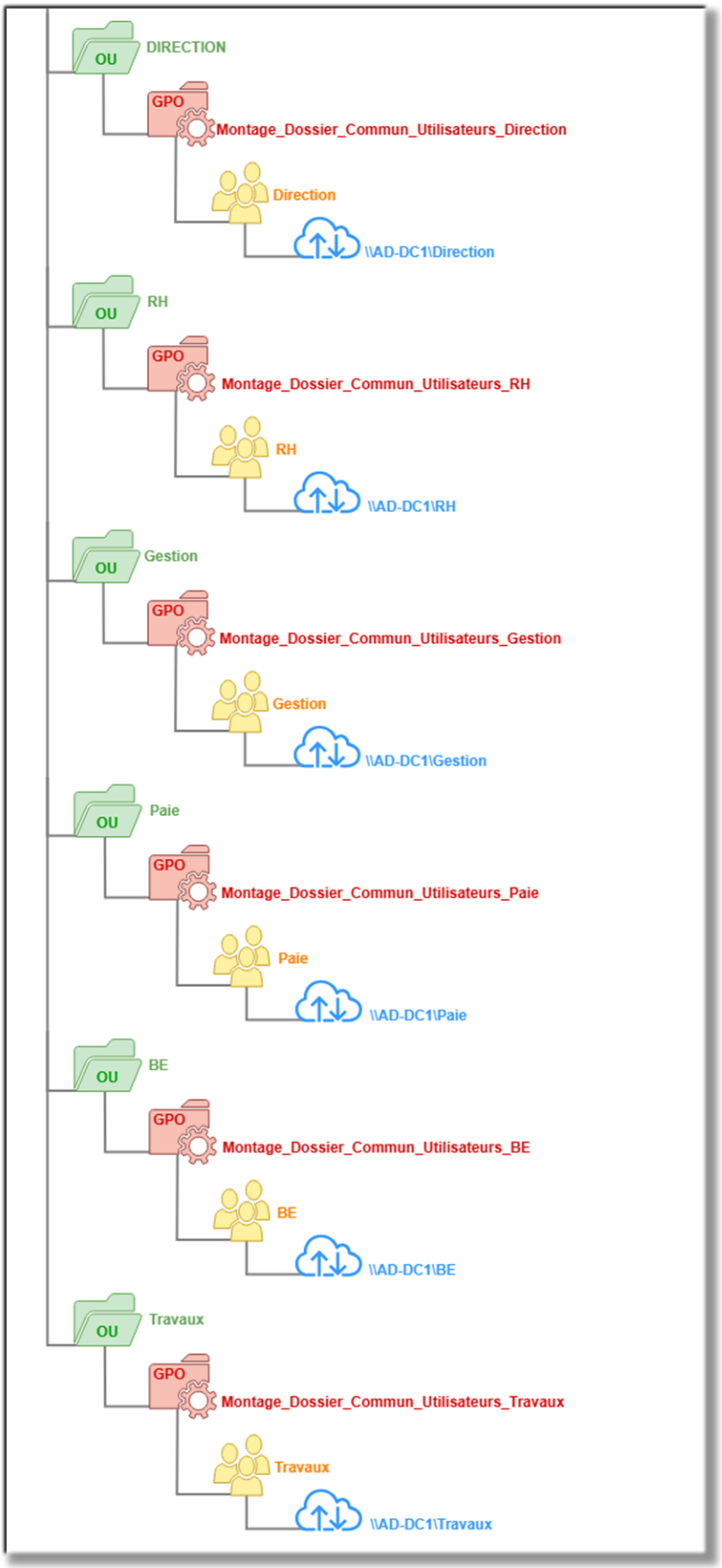


- Domaine :


Forêt : UNIRAIL
UNIRAIL.LOCAL
AFRAIL.LOCAL
Forêt : AFRAIL
SPRAIL.LOCAL
Forêt : SPRAIL
TPRAIL.LOCAL
Forêt : TPRAIL

➢ Arborescence du domaine unirail.local :




OU
DIRECTION
GPO
Montage_Dossier_Commun_Utilisateurs_Direction
Direction
\\AD-DC1\Direction
OU
RH
GPO
Montage_Dossier_Commun_Utilisateurs_RH
RH
\\AD-DC1\RH
OU
Gestion
GPO
Montage_Dossier_Commun_Utilisateurs_Gestion
Gestion
\\AD-DC1\Gestion
OU
Paie
GPO
Montage_Dossier_Commun_Utilisateurs_Paie
Paie
\\AD-DC1\Paie
OU
BE
GPO
Montage_Dossier_Commun_Utilisateurs_BE
BE
\\AD-DC1\BE
OU
Travaux
GPO
Montage_Dossier_Commun_Utilisateurs_Travaux
Travaux
\\AD-DC1\Travaux

B. Etude de criticité / des risques du SI

i. Analyse des risques

➢ Matrices définitives:

Vulnérabilité	Définition
Mineur	Vulnérabilité négligeable et improbable aux attaques.
Moyenne	Vulnérabilité légère et peu probable aux attaques.
Majeure	Vulnérabilité importante et probable aux attaques.
Critique	Vulnérabilité critique et récurrentes aux attaques.

Impact	Définition
Mineur	Pas de conséquences directes sur la sécurité du Système d'Information. Pas de conséquences sur la confidentialité et l'intégrité des données.
Moyen	Conséquences isolées sur un point précis du Système d'Information. Peu/pas de conséquences sur la confidentialité et l'intégrité des données.
Majeur	Conséquences restreintes sur une partie du Système d'Information. Conséquences moyenne sur la confidentialité et l'intégrité des données.
Critique	Conséquences généralisées sur l'ensemble du Système d'Information. Conséquences importantes sur la confidentialité et l'intégrité des données.

➢ Criticité des processus :

Processus	Vulnérabilité aux attaques	Impact de l'interruption
Service Active Directory (UR-V-DC-001 et UR-V-DC-002)	Critique	Critique
Service DNS (UR-V-DC-001 et UR-V-DC-002)	Critique	Majeur
Service DHCP (UR-V-DC-001)	Critique	Majeur
Service VEEAM (UR-V-DC-002)	Majeur	Critique
Service de Fichier/DFS (UR-V-FS-001)	Majeur	Majeur
Service d'impression (UR-V-FS-001)	Mineur	Mineur
Service de mise à jour Microsoft/WSUS (UR-V-WU-001)	Mineur	Moyen
Service de temps/NTP (UR-V-WU-001)	Mineur	Majeur
Service de déploiement/PXE (UR-V-PXE-001)	Mineur	Mineur
Service de transfert de fichier/FTP (UR-V-PXE-001)	Majeur	Critique
Service de ressources humaines et gestion/ERP Sage (UR-V-ERP-001)	Moyen	Critique
Service Microsoft Project (UR-V-ERP-001)	Mineur	Majeur
Service VPN/OpenVPN (UR-V-VPN-001)	Critique	Majeur

- Criticité des équipements :

Equipements	Vulnérabilité aux attaques	Impact de l'interruption
Routeur Cisco C891F-K9	Moyen	Critique
Pare-feu Stormshield SN-S-Series 320	Critique	Critique
Commutateur Cisco C9200-24P-E	Moyen	Critique
Commutateur Cisco C9200-8P-E	Moyen	Critique
Baie de stockage Synology SAN UC3200	Moyen	Critique
Borne Wi-Fi Cisco Catalyst 9115AXI-E	Majeur	Moyen
Imprimante HP LaserJet Ent MFP M527f Printer	Moyen	Mineur
Serveur physique DELL PowerEdge R750xs	Moyen	Critique
Station de travail Lenovo Thinkstation P2 Tower	Critique	Majeur
Ordinateur portable Lenovo ThinkBook T16	Critique	Majeur

ii. Etude des risques

Afin de pouvoir identifier la priorité de récupération, ainsi que la nécessité de supervision et de mise à jour d'une composante de l'infrastructure, une échelle est mise en place par la somme de deux variables (Vulnérabilité et Impact), permettant de placer cette dernière sur une échelle de risque allant de 1 à 10 :

- Vulnérabilité :
  - Critique : 5
  - Majeur : 3
  - Moyen : 1,5
  - Mineur : 0,5
- Impact :
  - Critique : 5
  - Majeur : 3
  - Moyen : 1,5
  - Mineur : 0,5
- Echelle :
  - 8 - 10 : Haute supervision (complète des ressources, performances et service, logs), haute sécurité (réseau et système, mise à jour très régulière, trafic réseau, restriction réseau, antivirus)
  - 5 - 8 : Supervision majeur (complète des ressources, performances et service, logs), haute sécurité (réseau et système, mise à jour régulière, trafic réseau, restriction réseau, antivirus)
  - 3 - 5 : Supervision standard (ressources et service logs), sécurité importante (réseau et système, trafic réseau, restriction réseau, antivirus)
  - 1 - 3 : Supervision minime (logs), sécurité standard (trafic réseau, restriction réseau, antivirus)

Composante	Valeur
Service Active Directory (UR-V-DC-001 et UR-V-DC-002)	10
Service DNS (UR-V-DC-001 et UR-V-DC-002)	8
Service DHCP (UR-V-DC-001)	8
Service VEEAM (UR-V-DC-002)	8
Service de Fichier/DFS (UR-V-FS-001)	6
Service d'impression (UR-V-FS-001)	1
Service de mise à jour Microsoft/WSUS (UR-V-WU-001)	2
Service de temps/NTP (UR-V-WU-001)	3,5
Service de déploiement/PXE (UR-V-PXE-001)	1
Service de transfert de fichier/FTP (UR-V-PXE-001)	8
Service de ressources humaines et gestion/ERP Sage (UR-V-ERP-001)	6,5
Service Microsoft Project (UR-V-ERP-001)	3,5
Service VPN/OpenVPN (UR-V-VPN-001)	8
Routeur Cisco C891F-K9	6,5
Pare-feu Stormshield SN-S-Series 320	10
Commutateur Cisco C9200-24P-E	6,5
Commutateur Cisco C9200-8P-E	6,5
Baie de stockage Synology SAN UC3200	6,5
Borne Wi-Fi Cisco Catalyst 9115AXI-E	4,5
Imprimante HP LaserJet Ent MFP M527f Printer	2
Serveur physique DELL PowerEdge R750xs	6,5
Station de travail Lenovo Thinkstation P2 Tower	8
Ordinateur portable Lenovo ThinkBook T16	8

iii. Procédure en cas de sinistre

Valeur	Procédure	Responsabilité
8 - 10	Communication avec les autorités compétentes (ANSSI, CNIL), Communication avec les fournisseurs, Remise à niveau maximal de 24h, Prise de prestation supplémentaire en cas de besoin	Directeur général, Directeur Technique, Administrateur systèmes et réseaux
5 - 8	Communication avec les fournisseurs, Remise à niveau maximal de 3j, Prise de prestation supplémentaire en cas de besoin	Directeur technique, Administrateur systèmes et réseaux
3 - 5	Communication avec les fournisseurs en cas de besoin, Remise à niveau maximal de 7j, Prise de prestation supplémentaire en cas de besoin	Administrateur systèmes et réseaux
1 - 3	Communication avec les fournisseurs, en cas de besoin, Remise à niveau maximal de 20j	Administrateur systèmes et réseaux

C. Etude de perte / indisponibilité

i. RPO et RTO

Composante	RPO	RTO
Service Active Directory (UR-V-DC-001 et UR-V-DC-002)	0	0
Service DNS (UR-V-DC-001 et UR-V-DC-002)	0	0
Service DHCP (UR-V-DC-001)	0	0
Service VEEAM (UR-V-DC-002)	0	1 heure
Service de Fichier/DFS (UR-V-FS-001)	0	30 minutes
Service d'impression (UR-V-FS-001)	acceptable	6 heures
Service de mise à jour Microsoft/WSUS (UR-V-WU-001)	peu	+ 1 jour
Service de temps/NTP (UR-V-WU-001)	peu	1 heure
Service de déploiement/PXE (UR-V-PXE-001)	peu	6 heures
Service de transfert de fichier/FTP (UR-V-PXE-001)	0	30 minutes
Service de ressources humaines et gestion/ERP Sage (UR-V-ERP-001)	0	0
Service Microsoft Project (UR-V-ERP-001)	0	1 heure
Service VPN/OpenVPN (UR-V-VPN-001)	peu	1 heure
Routeur Cisco C891F-K9	0	0
Pare-feu Stormshield SN-S-Series 320	0	0
Commutateur Cisco C9200-24P-E	0	0
Commutateur Cisco C9200-8P-E	0	0
Baie de stockage Synology SAN UC3200	0	15 minutes
Borne Wi-Fi Cisco Catalyst 9115AXI-E	peu	1 heure
Imprimante HP LaserJet Ent MFP M527f Printer	acceptable	6 heures
Serveur physique DELL PowerEdge R750xs	0	0
Station de travail Lenovo Thinkstation P2 Tower	acceptable	0
Ordinateur portable Lenovo ThinkBook T16	acceptable	0

- Le RPO est un outil de mesure permettant d'estimer de façon théorique combien de données le SI peut-il se permettre de perdre pour chacune de ses composantes sans encourir des effets de bord dit à risque (perte, coût, image). L'étude est faite indépendamment pour chacune d'entre elles, n'ayant pas la même criticité et donc le même besoin d'intégrité des données.

  Il en découle donc aussi une volonté de mettre en place une solution de backup plus ou moins efficace permettant de récupérer ces données perdues.

- Le RTO, quant à lui, est un outil de mesure permettant d'estimer de façon théorique combien de temps le SI peut-il se permettre d'avoir un service/processus indisponible parmi chacune de ses composantes sans encourir des effets de bord dit à risque (perte, coût, image). L'étude est aussi faite indépendamment pour chacune d'entre elles, n'ayant pas la même criticité et donc le même besoin de disponibilité du processus.

  Il est donc important de définir à quelle vitesse le SI peut-il restaurer son système et quel coût l'indisponibilité de ce dernier engendrera.

ii. Coût du sinistre

Afin de pouvoir estimer le coût engendré par l'interruption ou bien de la perte de données d'une ou plusieurs composantes du SI, il est nécessaire de calculer (le plus précisément possible) les 5 points suivants :

- Perte CA == CA hebdo / 35 * h interruption
- Perte productivité == salaire horaire moyen * nb employer affecter * h indisponibilité
- Coût restauration == coût prestation + coût matériel/licence à renouveler
- Frais indirect == déclaration légal + communication + etc.
- Impact sur l'image == perte contrats + perte clients

Total == Perte CA + Perte productivité + Coût restauration + Frais indirect + Impact sur l'image

D. Continuité du SI

La redondance des équipements et des services est nécessaire afin d'assurer la continuité du service (même hors sinistre). C'est pour cela qu'il est important de définir la stratégie de redondance de chacune des composante du si comme défini ci-dessous :

➢ Réseau :

Equipements	Solution	Plus-values
Commutateur Cisco C9200-24P-E	Stacking des commutateurs	Possibilité de mettre les commutateurs en stack : redondance du trafic, augmentation des ressources/performances, redondance de l'alimentation
Commutateur Cisco C9200-8P-E	Stacking des commutateurs	
Routeur Cisco C891F-K9	Unification des routeurs	Mise en place d'un IP virtuelle, répartition des charges, redondance du trafic ; partage des configurations
Pare-feu Stormshield SN-S-Series 320	Haute disponibilité des pare-feu	Mise en place du mode Actif/Passif, redondance du trafic, partage des configurations
Borne Wi-Fi Cisco Catalyst 9115AXI-E	Sommes des bornes	Redondance de la plage réseau Wi-Fi
Serveur physique DELL PowerEdge R750xs	Redondance du serveur physique	Redondance de l'hébergement physique des VM, redondance de l'alimentation, partage des données et configurations
Baie de stockage Synology SAN UC3200	Redondance du stockage des données Redondance des sauvegardes	Redondance des données, haute disponibilité des données, redondance de la carte contrôleur, redondance de l'alimentation, plan de sauvegarde

- Système :

Processus	Solution	Plus-values
AD (LDAPS)	Redondance du service AD	Redondance du service vers le deuxième environnement VMSphere ESXI du deuxième serveur physique
DHCP	Redondance du service DHCP	
DNS	Redondance du service DNS	
UR-V-DC-001	Redondance de la VM UR-V-DC-001	
UR-V-DC-002	Redondance de la VM UR-V-DC-002	
UR-V-FS-001	Redondance de la VM UR-V-FS-001	
UR-V-WW-001	Redondance de la VM UR-V-WW-001	
UR-V-PXE-001	Redondance de la VM UR-V-PXE-001	
UR-V-ERP-001	Redondance de la VM UR-V-ERP-001	
UR-V-VPN-001	Redondance de la VM UR-V-VPN-001	
UR-V-SUP-001	Redondance de la VM UR-V-SUP-001	

E. Plan de reprise informatique (PRI/PRA)

L'objectif du Plan de Reprise des Activités est de permettre à l'entreprise de retrouver un fonctionnement normal le plus rapidement possible après un incident en mettant en place une procédure de restauration des systèmes et des opérations après une interruption.

Cette procédure assure la récupération des données, la réparation des systèmes et la réactivation des processus métier.

i. Sparing des équipements

Equipements réseaux	PHT €	Quantité	PTHT €
Commutateur Cisco C9200-24P-E	1 965,26 €	1	1 965,26 €
Commutateur Cisco C9200-8P-E	965,4 €	1	965,4 €
Routeur Cisco C891F-K9	925 €	1	925 €
Pare-feu Stormshield SN-S-Series 320	2 036,4 €	1	2 036,4 €
Borne Wi-Fi Cisco Catalyst 9115AXI-E	470 €	2	940 €
Imprimante HP LaserJet Ent MFP 137fnw	780,22 €	1	780,22 €
Traceur HP DesignJet T230	632,8 €	1	632,8 €
Serveur physique DELL PowerEdge R750xs	3 583 €	1	3 583 €
Carte contrôleur RAID 6 Areca ARC-1883ix-12	1 620 €	1	1 620 €
Disques durs WD SATA Gold 20 To	486,99 €	5	2 434,95 €

Equipements utilisateurs	PHT €	Quantité	PTHT €
Kit clavier et souris bureautique Logitech Desktop MK120	22,41 €	15	336,15 €
Ecran IIYAMA XUB2463HSU-B1	120 €	10	1 200 €
Station de travail Lenovo Thinkstation P2 Tower	715,9 €	6	4 295,4 €
Ordinateur portable Lenovo ThinkBook T16	498 €	5	2 490 €

ii. Procédure type en cas de sinistre

- Détection :
  - Remonter de l'incident par les utilisateurs.
  - Remonter de la faille ou d'une anomalie par l'antivirus et les logs des équipements réseaux (pare-feu, routeurs, commutateurs).
  - Remonter des alertes à l'aide de la supervision.

- Déclaration :
  - Communication à la direction.
  - Communication avec les fournisseurs (possibilité de support lors de l'intervention de reprise).
  - Communication aux autorités compétentes.

- Résolution du sinistre :
  - Analyse du sinistre.
  - Isolation du sinistre.
  - Résolution du sinistre.

- Restauration des pertes :
  - Récupération des pertes par les backups.
  - Reconfiguration (si besoin).
  - Re-vérification du fonctionnement.

- Communication :
  - Communication aux utilisateurs du type de sinistre et de son impact.
  - Communication des possibles failles aux fournisseurs.
  - Sensibilisation des utilisateurs sur ce type de sinistre.

iii. Automatisation

La reprise d'un processus informatique peut prendre un certain temps non négligeable, étant souvent une étape récurrente (mise en place de l'OS, configuration réseau, configuration service, etc.), ce dernier peut facilement être automatisé afin d'apporter un réel gain de temps au SI et permettre une reprise plus rapide du processus.

Cette automatisation se fera à l'aide du service Ansible, ce dernier permet à l'équipe informatique de mettre en place une procédure d'automatisation des configurations type lors de la restauration et la reprise d'un processus.

De plus, quant à la création de comptes utilisateurs en cas de perte ou bien lorsqu'il est nécessaire dans un cas normal, 3 scripts ont été mis en place afin d'automatiser ce dernier, ils sont les suivants :

```powershell
# Variables
$domain = "UNIRAIL.LOCAL"
$domainUser = "nom_utilisateur_domaine"
$domainPassword = "mot_de_passe_domaine"
$computerName = "Nom_Ordinateur"
$installerPath0 = " \\UR-V-PXE-001\applications\DA-apps\sharepoint.exe"
$installerPath1 = " \\UR-V-PXE-001\applications\DA-apps\SAGE100.exe"
$installerPath2 = " \\UR-V-PXE-001\applications\DA-apps\Mysql.exe"

# Convertir le mot de passe en SecureString
$securePassword = ConvertTo-SecureString $domainPassword -AsPlainText -Force

# Créer les informations d'identification
$credential = New-Object System.Management.Automation.PSCredential($domainUser, $securePassword)

# Ajouter l'ordinateur au domaine
Add-Computer -DomainName $domain -Credential $credential -ComputerName $computerName -Restart

# Attendre le redémarrage et la connexion de l'utilisateur
Start-Sleep -Seconds 60

# Installer SharePoint
Start-Process -FilePath $installerPath0 -ArgumentList "/sAll /msi /norestart /quiet" -Wait

# Installer ERP Sage 100 Paie et RH
Start-Process -FilePath $installerPath1 -ArgumentList "/sAll /msi /norestart /quiet" -Wait

# Installer Client Serveur MySql Gestion des relevés d'heures de chantier
Start-Process -FilePath $installerPath2 -ArgumentList "/sAll /msi /norestart /quiet" -Wait

# Message de fin
Write-Host "L'ordinateur a été ajouté au domaine et les logiciels ont été installés."
```

```powershell
# Variables
$domain = "UNIRAIL.LOCAL"
$domainUser = "nom_utilisateur_domaine"
$domainPassword = "mot_de_passe_domaine"
$computerName = "Nom_Ordinateur"
$installerPath0 = " \\UR-V-PXE-001\applications\BE-apps\sharepoint.exe"
$installerPath1 = " \\UR-V-PXE-001\applications\BE-apps\Autocad.exe"

# Convertir le mot de passe en SecureString
$securePassword = ConvertTo-SecureString $domainPassword -AsPlainText -Force

# Créer les informations d'identification
$credential = New-Object System.Management.Automation.PSCredential($domainUser, $securePassword)

# Ajouter l'ordinateur au domaine
Add-Computer -DomainName $domain -Credential $credential -ComputerName $computerName -Restart

# Attendre le redémarrage et la connexion de l'utilisateur
Start-Sleep -Seconds 60

# Installer SharePoint
Start-Process -FilePath $installerPath0 -ArgumentList "/sAll /msi /norestart /quiet" -Wait

# Installer AutoCad
Start-Process -FilePath $installerPath1 -ArgumentList "/sAll /msi /norestart /quiet" -Wait

# Message de fin
Write-Host "L'ordinateur a été ajouté au domaine et les logiciels ont été installés."
```

```powershell
# Variables
$domain = "UNIRAIL.LOCAL"
$domainUser = "nom_utilisateur_domaine"
$domainPassword = "mot_de_passe_domaine"
$computerName = "Nom_Ordinateur"
$installerPath0 = " \\UR-V-PXE-001\applications\DT-apps\sharepoint.exe"
$installerPath1 = " \\UR-V-PXE-001\applications\DT-apps\MSProject.exe"
$installerPath2 = " \\UR-V-PXE-001\applications\DT-apps\Mysql.exe"

# Convertir le mot de passe en SecureString
$securePassword = ConvertTo-SecureString $domainPassword -AsPlainText -Force

# Créer les informations d'identification
$credential = New-Object System.Management.Automation.PSCredential($domainUser, $securePassword)

# Ajouter l'ordinateur au domaine
Add-Computer -DomainName $domain -Credential $credential -ComputerName $computerName -Restart

# Attendre le redémarrage et la connexion de l'utilisateur
Start-Sleep -Seconds 60

# Installer SharePoint
Start-Process -FilePath $installerPath0 -ArgumentList "/sAll /msi /norestart /quiet" -Wait

# Installer MS Prpject
Start-Process -FilePath $installerPath1 -ArgumentList "/sAll /msi /norestart /quiet" -Wait

# Installer Client Serveur MySql Gestion des relévés d'heures de chantier
Start-Process -FilePath $installerPath2 -ArgumentList "/sAll /msi /norestart /quiet" -Wait

# Message de fin
Write-Host "L'ordinateur a été ajouté au domaine et les logiciels ont été installés."
```

iv. Planification

Afin d'assurer et de finaliser la reprise des activités informatiques à la suite d'un sinistre quelconque, il est important de prendre en compte ces 2 points :Rém

- La documentation/procédure pour chacune des composantes du SI en cas de sinistre.
  Cela assure à l'équipe informatique une étape point par point (servant évidemment de base et pouvant être adapter sur le moment), guidant ces derniers tout au long du processus (de la détection à la restauration) afin d'assurer au mieux la reprise et dans les plus brefs délais.

- Tester et mettre à jour régulièrement les procédures de reprise en simulant un sinistre type.
  Cela assure à l'équipe informatique d'avoir une procédure à jour répondant au mieux à l'évolution des sinistres dans le temps, mais aussi la familiarisation de ces derniers à la mise en position d'une gestion de crise et à l'efficace de la mise en œuvre de cette dernière.

4. Sécurisation du SI

A. Politique de cybersécurité

Tous les salariés :

- Les utilisateurs ne doivent utiliser l'accès à internet et aux ressources (équipements et services) mises à disposition par le système d'information strictement dans le cadre de leur travail.
  Aucun écart et utilisation à intérêt personnel et privé ne sera toléré.
- Les utilisateurs ne doivent pas communiquer leur adresse professionnelle en dehors de l'exercice de leur fonction.
- Les utilisateurs ne peuvent ajouter une adresse personnelle dans leur messagerie.
- Les utilisateurs ne doivent pas ouvrir des mails de provenance inconnue. En cas de doute, ils devront contacter le service informatique.
- Les utilisateurs devront enregistrer leurs mots de passe sur le coffre-fort de mots de passe "Keepass", qui sera installé sur chacune des sessions.
- Mise en place d'un Chocoblast (le fait de devoir ramener des pâtisseries en cas de non-verrouillage de sa session et qu'un collègue est allé envoyer un mail pour le signaler) afin de sensibiliser les utilisateurs de façon plus "euphorique" pour que ces derniers puissent prendre le réflexe tout en ne ressentant pas cette pratique comme un fardeau.
- Sensibilisation des utilisateurs sur le verrouillage de leur session à partir du moment où ils quittent leur bureau, même pour une courte durée.
- Porte d'entrée sécurisée par une badgeuse, tous les salariés se voient attribuer un badge unique et personnel leur de lors première journée.

  Dans le cas de visites externes, un digiphone est mis en place et les visiteurs devront s'authentifier avant qu'un salarié vienne leur ouvrir.

Direction et Service Informatique :

- Utilisation du logiciel "PrivateBin", qui permet de partager des données sensibles à l'aide d'un lien temporaire et sécurisé.

Service Informatique :

- Accès à la salle serveur à l'aide d'une carte d'authentification à badger, ainsi qu'un digicode à 6 chiffres (réinitialisation du code tous les 3 mois, effectuée par le directeur technique).

B. Politique de mot de passe

Cette politique serait mise en œuvre et appliquée sur l'ensemble de l'environnement AD à l'aide d'une PSO (GPO pour les mots de passe).

- Premier mot de passe temporaire avec le modèle : « NOMprénomdate! »
- Création du mot de passe dès la première connexion (à la suite du mot de passe temporaire):
    - Minimum 12 caractères
    - Minimum 1 majuscule
    - Minimum 1 minuscule
    - Minimum 1 chiffre
    - Minimum 1 caractère spécial
- Durée de vie du mot de passe : 30 jours minimum / 60 jours maximum (impossibilité de se connecter après 60 jours tant que le mot de passe n'a pas été changé).
- Empêcher la réutilisation des 10 derniers mots de passe.
- Déconnexion automatique de la session après 5 minutes d'inactivité.
- Compte bloqué 30 minutes après 5 tentatives de connexion.

C. Politique d'authentification

Cette politique pourra être mise en place à l'aide d'un serveur RADIUS qui assurera la communication entre l'utilisateur et l'annuaire LDAP de l'AD. RADIUS récupère les informations d'authentification du LDAP et vérifie la cohérence de ces derniers avec les entrées de l'utilisateur et accepte ou non la connexion.

- L'authentification se fait à partir du service LDAPS mis en place sur l'AD.
- Chaque utilisateur est intégré à un/des groupe(s) d'utilisateurs et à une/des unité(s) d'organisation afin de pouvoir leur appliquer les réglementations imposées à travers les GPO.
- Un portail d'authentification est mis en place et permettra aux utilisateurs de pouvoir interagir avec les applications (leur étant concernées, à l'aide des OU) à l'aide de leur authentification LDAPS.
- Verrouillage de la session automatique après 10 minutes d'inactivité.

D. Antivirus

Le choix de l'antivirus "Sophos Intercept X Advanced" est un choix pertinent car il permet de couvrir les points essentiels et prioritaires quant à la sécurisation de l'infrastructure du Système d'Information.

Protection multicouche complète :

- Sophos Endpoint Protection combine antivirus, anti-malware, détection comportementale, et prévention des exploitations de vulnérabilités.
- Protection contre les ransomwares via "CryptoGuard", efficace même contre les variantes inconnues.

Centralisation via Sophos Central :

- Possibilité d'évoluer vers une console cloud unifiée pour la gestion de tous les terminaux, serveurs, et pare-feux agents du l'antivirus Sophos.

Intégration avec XDR et MDR :

- Sophos XDR (Extended Detection & Response) permet de visualisation les événements réseau, e-mail, etc.
- Possible d'ajouter Sophos MDR (Managed Detection and Response) pour une surveillance 24/7 par des analystes dans le cas d'une PME avec des effectifs et des moyens du domaine informatique insuffisants.

Facilité de déploiement et d'administration :

- Possibilité de déploiement par des scripts, Active Directory, ou GPO.
- Console intuitive, facile d'utilisation et ergonomique.

Conformité RGPD et normes ISO :

- Des fonctions de contrôle de données (DLP), chiffrement et audit.
- ISO 27001, ISO 27017 et ISO 27018 (spécifiquement pour la console cloud

Consommation des ressources :

- Le moteur de protection ne surcharge pas le système en permanence. Il agit surtout lorsqu'une menace potentielle est détectée.
- Sophos utilise une technologie de **protection basée sur le cloud**, ce qui signifie que certaines analyses sont effectuées à distance, réduisant la charge locale.

Situation	Impact
Utilisation de RAM	Faible à modérée
Utilisation CPU (en veille)	Faible
Utilisation CPU (en analyse)	Moyenne
Temps de démarrage système	Peu impacté
Navigation / tâches bureautiques	Peu impactées

Prix :

- Pour 40 licences : 102,60 € unitaire == 4 104 € /an

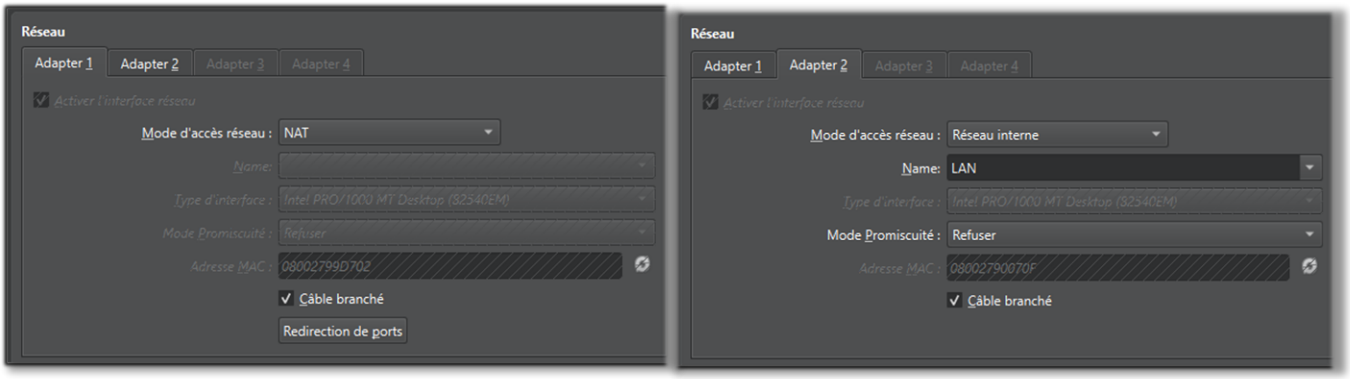
5. Mise en œuvre

A. Environnement Active Directory

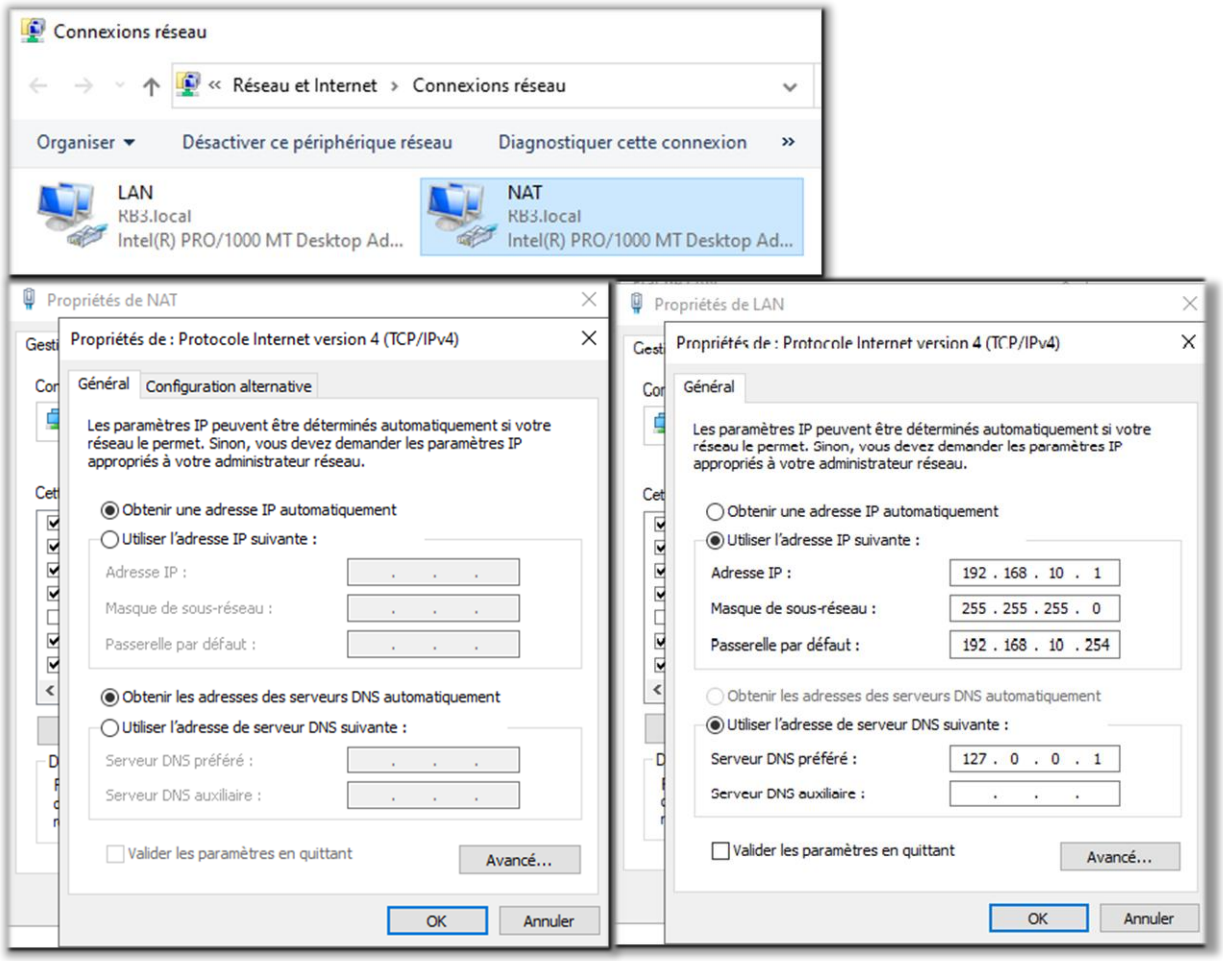
L'AD est le regroupement de nombreux services et fonctionnalités qui permet de gérer, sécuriser les différentes composantes d'un environnement réseau Windows.

i. Configuration de la VM

- Configuration réseau de la VM :

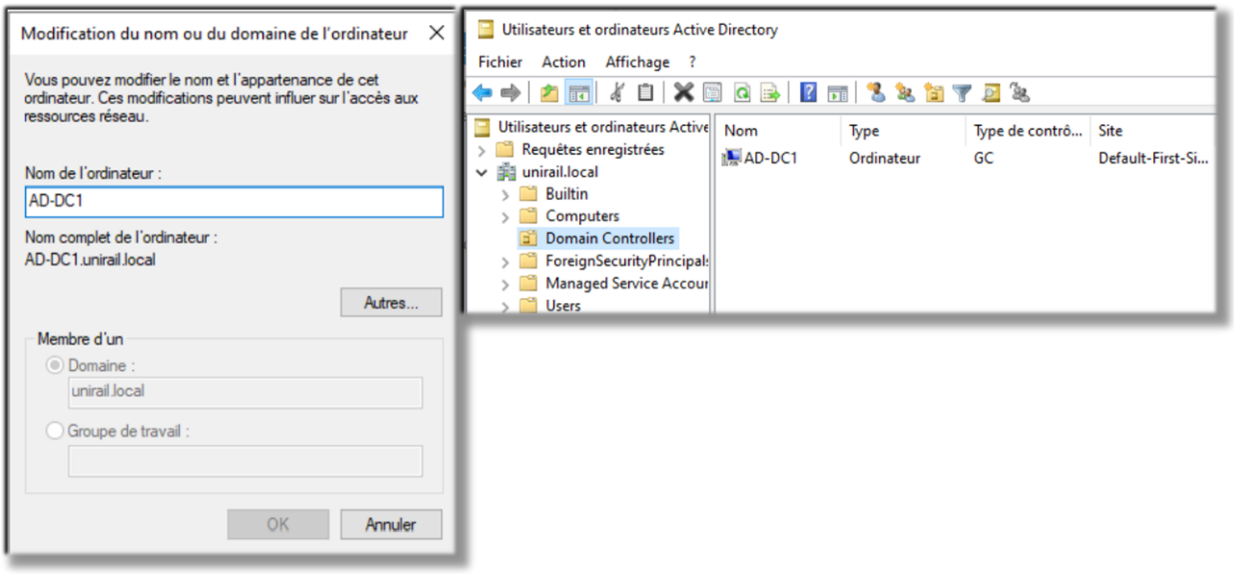


- Configuration des cartes réseaux :



ii. Service AD

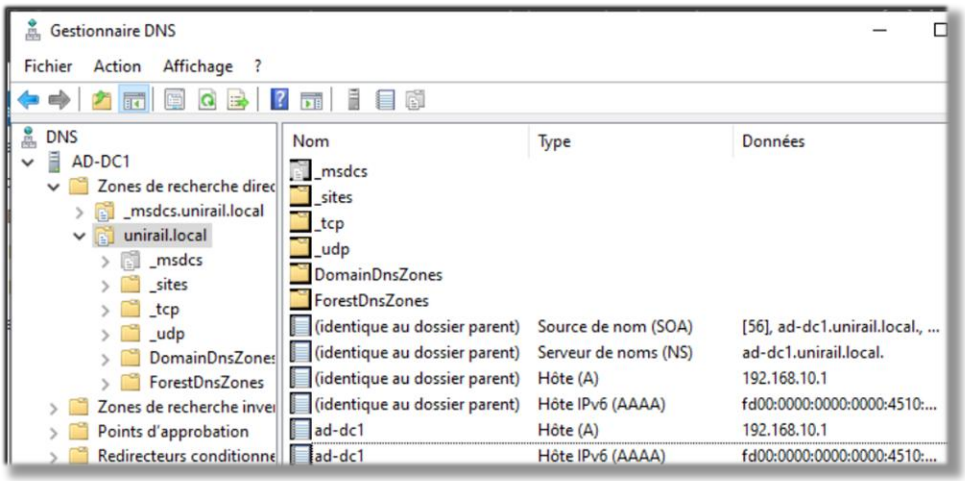
➢ Création du DC :



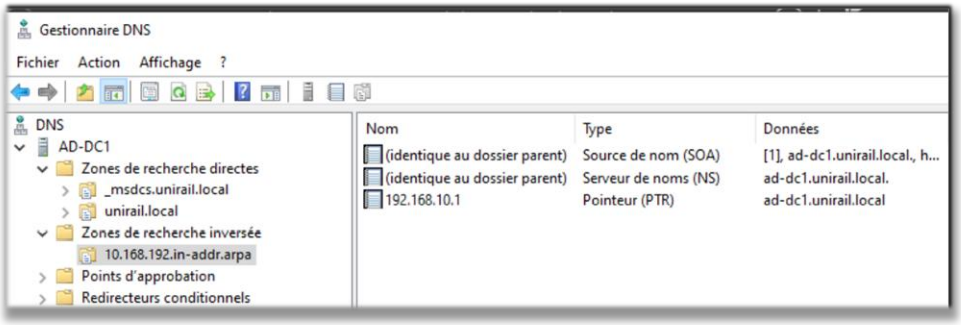
iii. Service DNS (Domain Name Server)

Le DNS permet d'associer le nom de domaine d'une entité à une adresse IP, cela facilite la navigation des utilisateurs vers les applications de l'infrastructure.

➢ Configuration des zones de recherches directes :



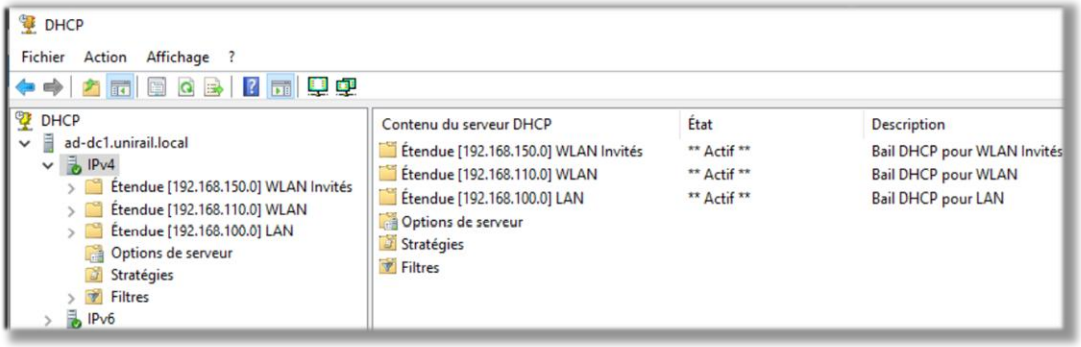
➢ Configuration des zones de recherches indirectes :



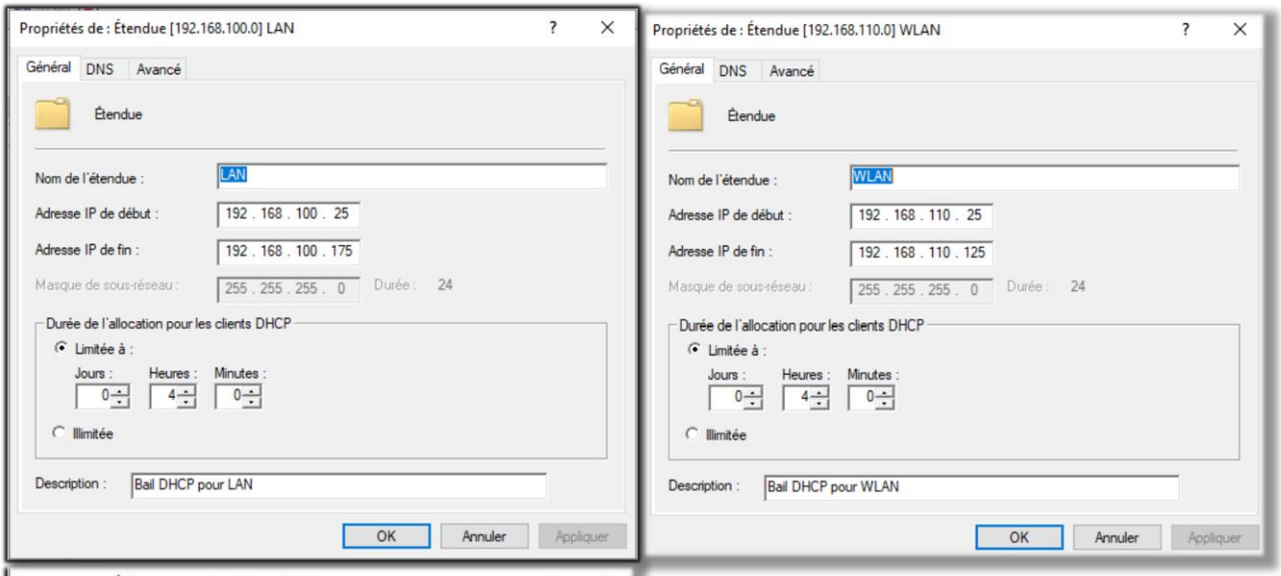
iv. Service DHCP (Dynamic Host Configuration Protocol)

Le DHCP permet d'attribuer des baux de configurations réseaux aux machines faisant partie du domaine, de ce fait, il assure la cohérence des configurations et donc la bonne intégration de la machine au réseau ainsi que sa communication avec le reste des composantes de ce dernier.

- Création des étendues :



- Configurations des étendues :

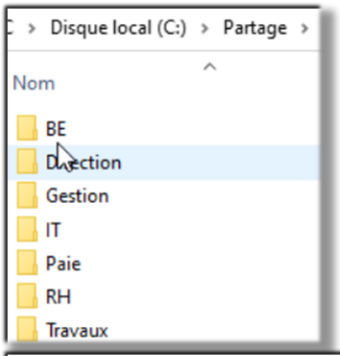


VLAN « INFRA », « Gestion », et « ADMIN » seront en statique

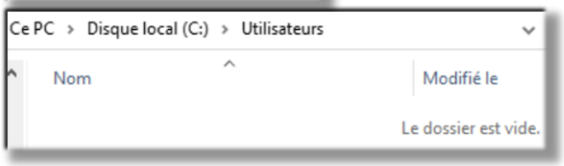
v. Service DFS (Distributed File System)

Le DFS est un système de fichiers distribué qui permet de structurer les fichiers partagés sur différents serveurs de fichiers Windows. Cela rend l'emplacement réel des données et le chemin d'accès à ces derniers indépendants.

- Création du DFS du dossier « partage » commun pour les départements de travail :

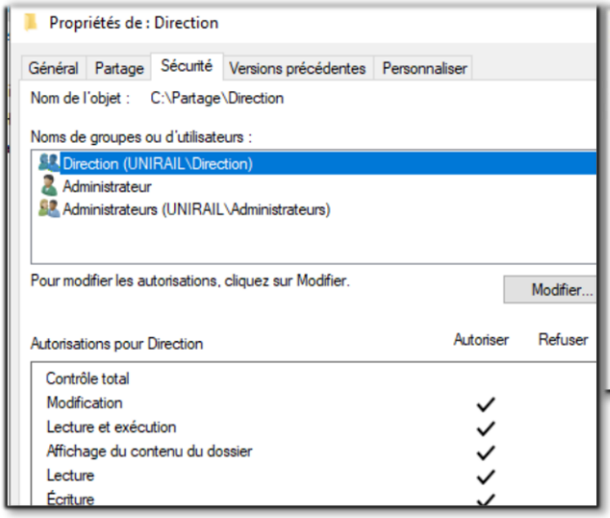


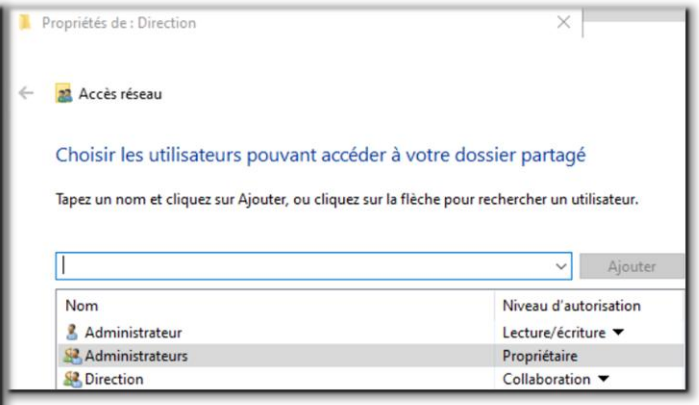
Création du dossier « Partage » hébergeant les différents dossiers partagés par département de travail.



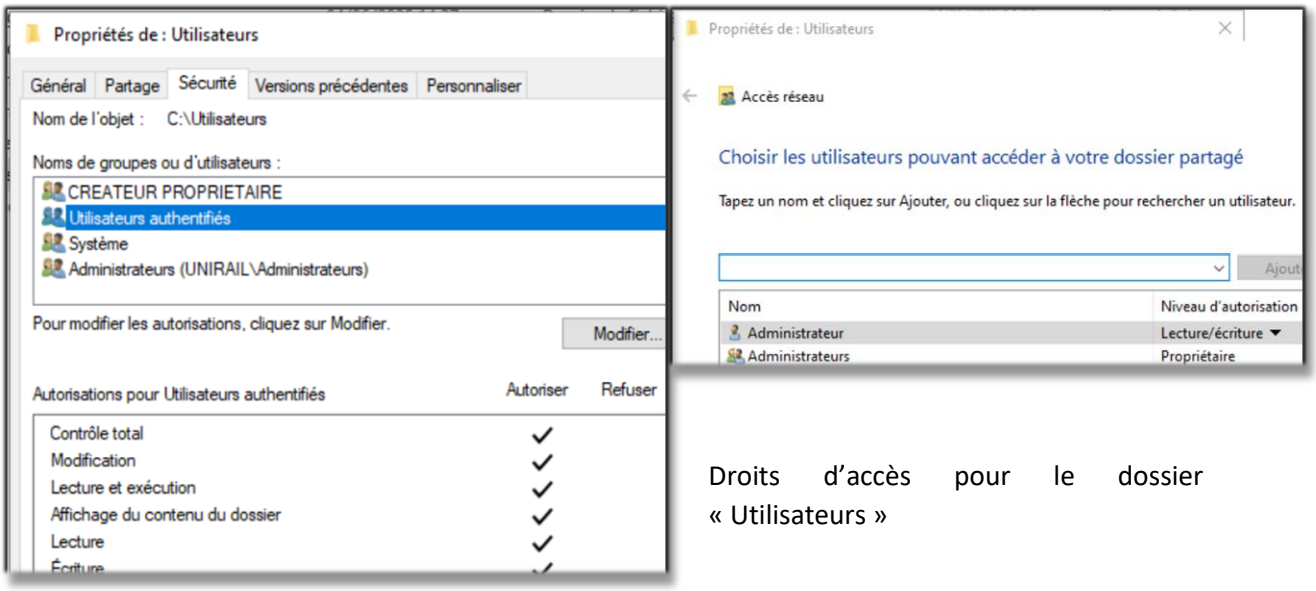
Création du dossier « Utilisateurs » hébergeant tous les dossiers personnels des utilisateurs.

- Configurations des droits d'accès aux dossiers (exemple « Direction ») :





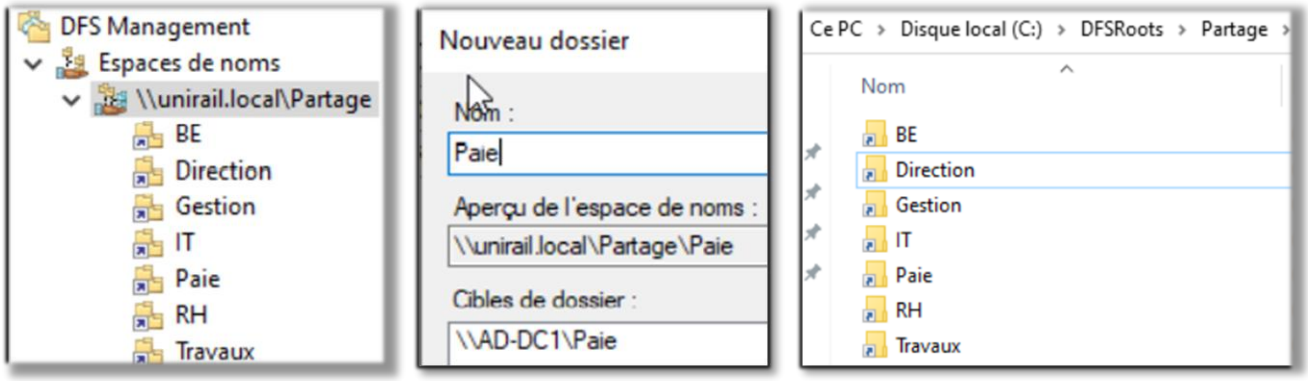
Droits d'accès pour le dossier « Partage »



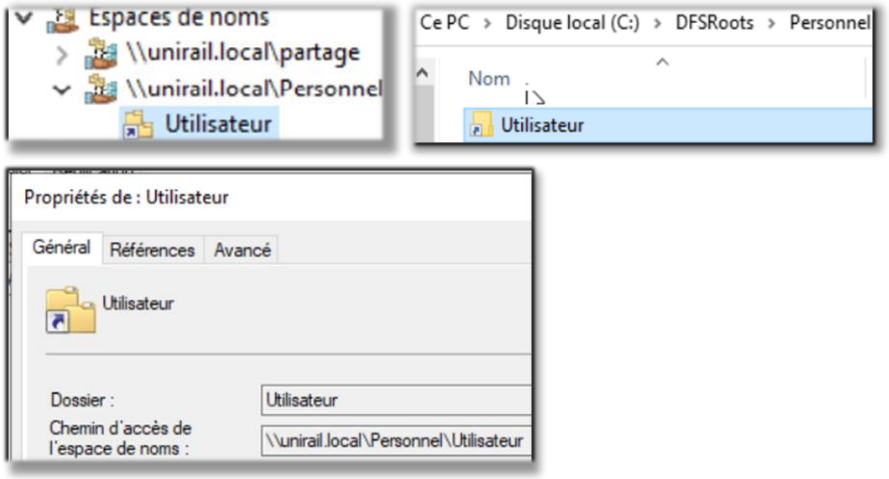
Droits d'accès pour le dossier « Utilisateurs »

- Création des dossiers DFS :

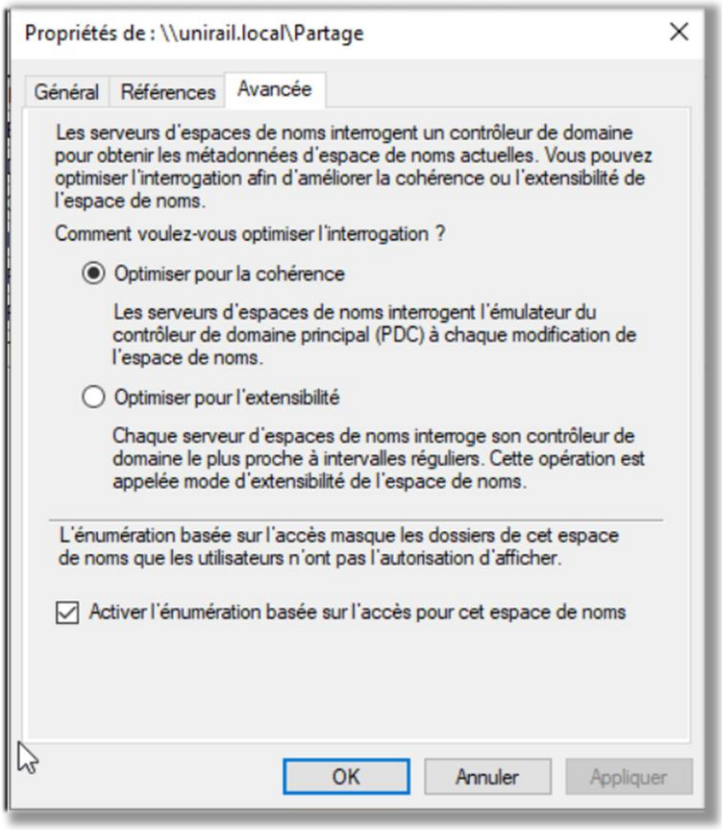
DFS crée des dossiers virtuels (dans « DFSRoots ») ciblant sur les dossiers physiques hébergés sur le serveur de fichiers (ici lui-même).



Création des dossiers pour le dossier « Partage »



- Activation de l'ABE (énumération basée sur l'accès) sur les deux espaces de noms créés:

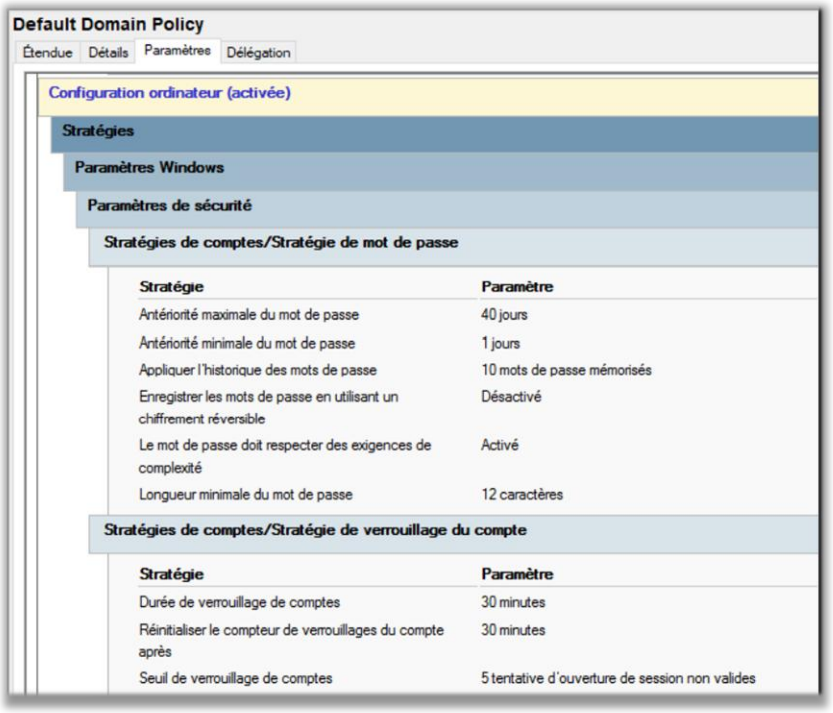


Les utilisateurs ne verront que le dossier auquel ils ont le droit d'accès, configurés précédemment.

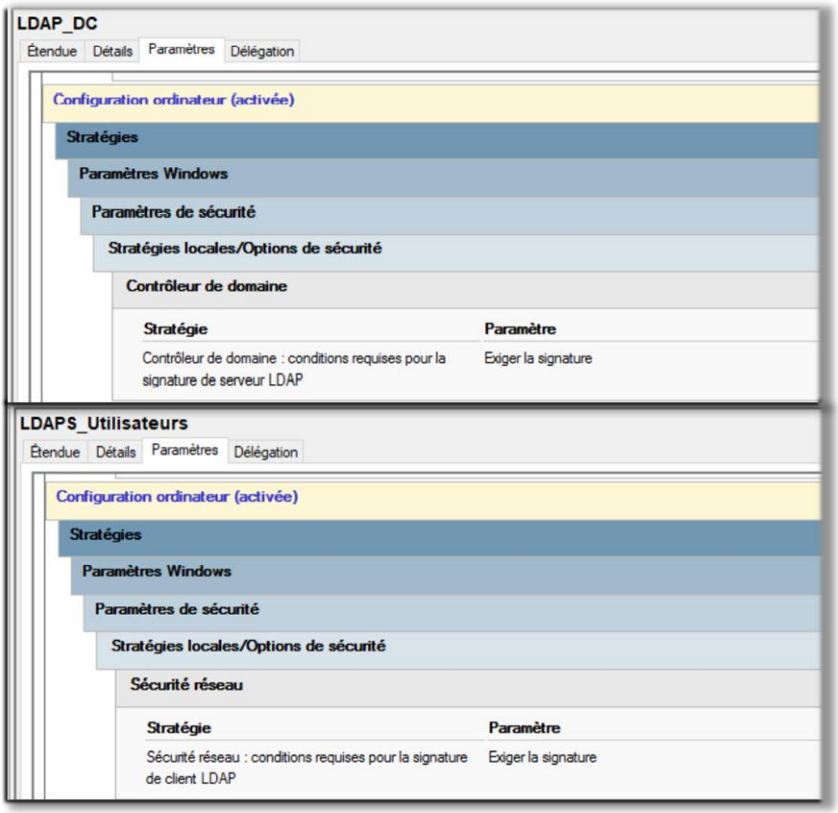
vi. GPOs (Groupe Policy Object)

Les GPOs sont des outils qui permettent de gérer, de façon centralisée sur le DC, tout l'environnement AD afin de contrôler les différents paramètres ordinateurs et utilisateurs des composantes de ce dernier.

- Création des GPOs :

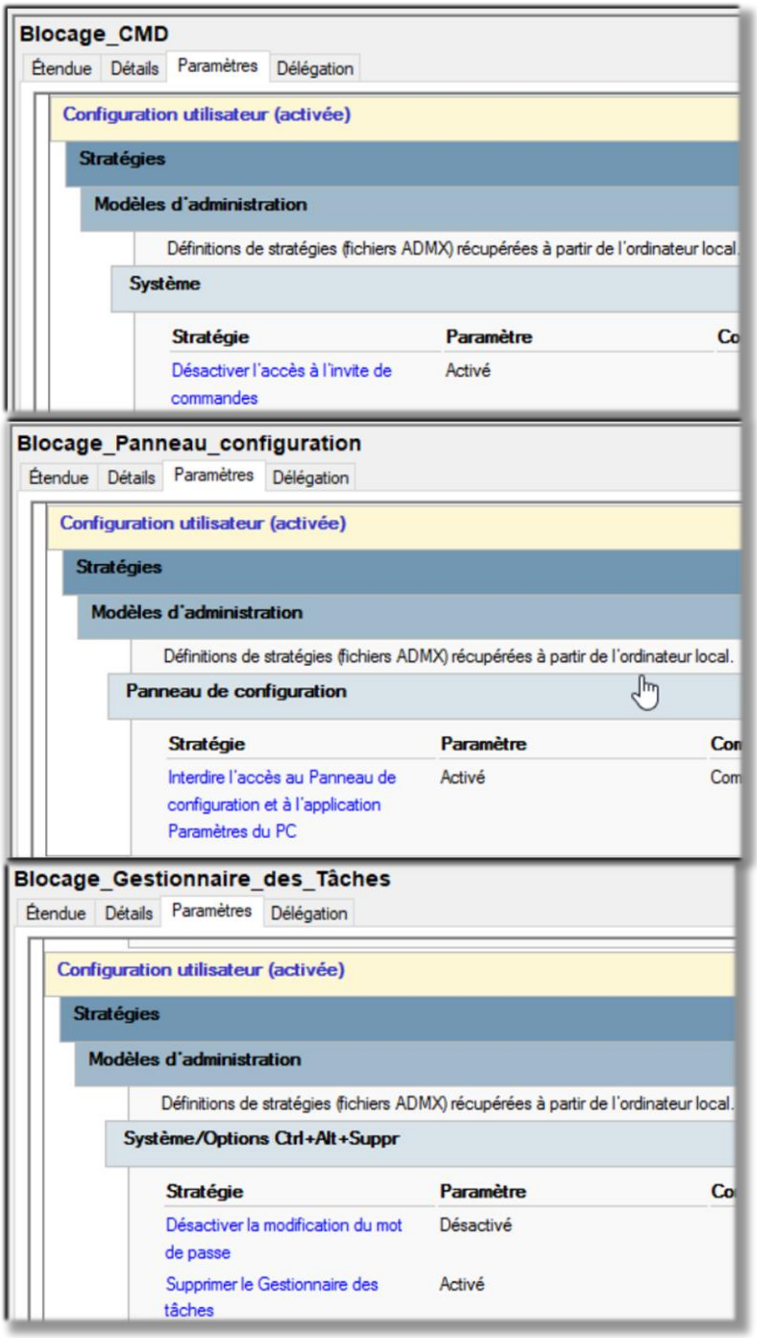


Afin d'assurer la politique de mot de passe exigée par le client.



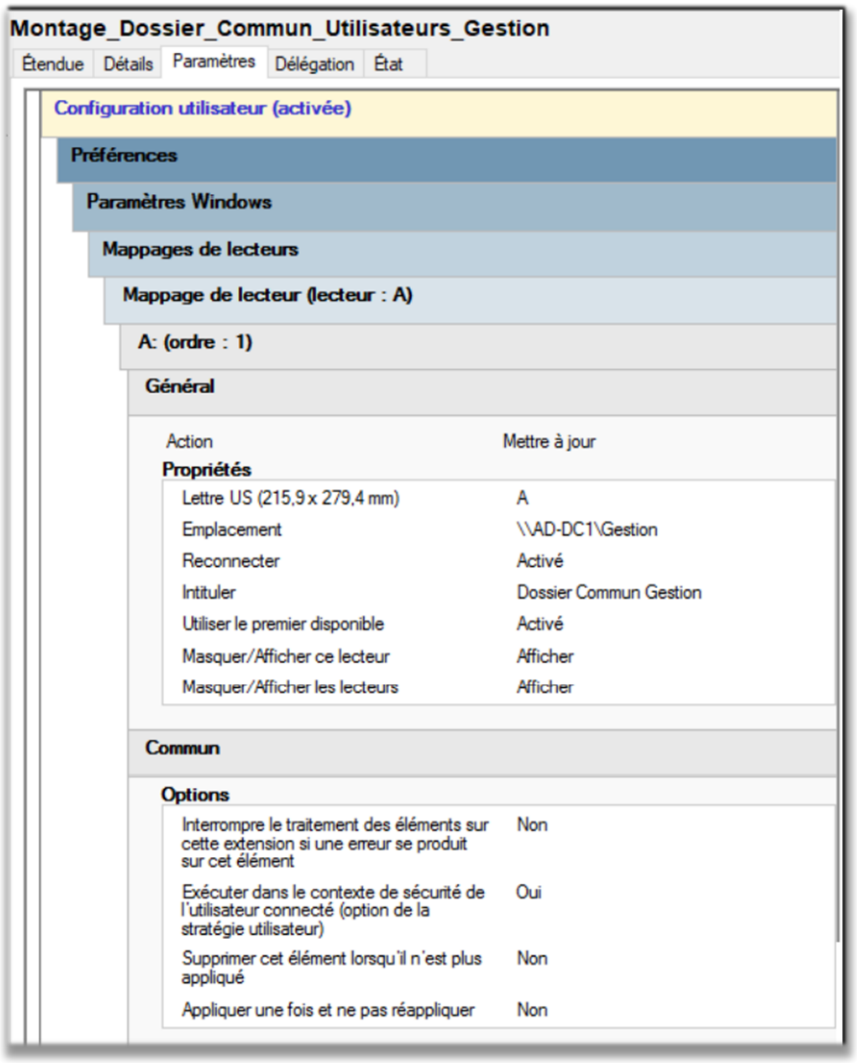
Afin de bloquer la communication par le protocole LDAP entre le serveur AD et les utilisateurs.

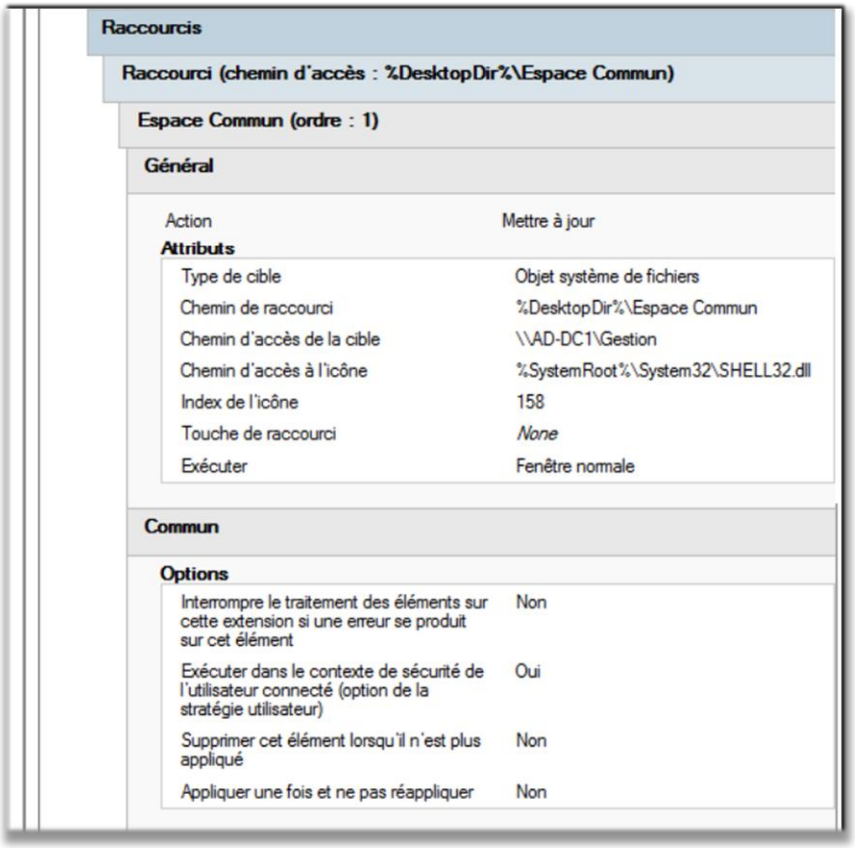
Force l'utilisation du protocole LDAPS pour cette communication, assurant le chiffrage des données.



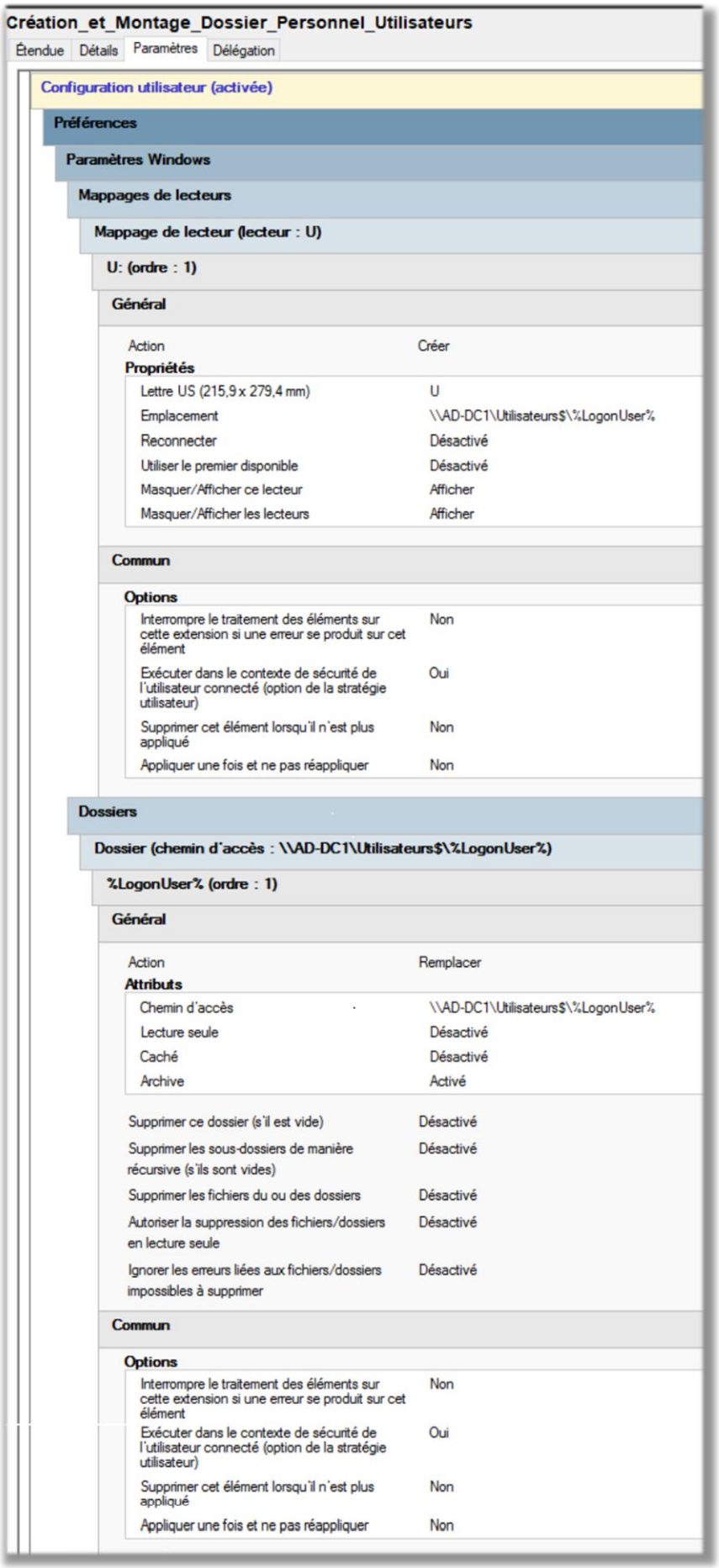
Afin d'assurer l'intégrité des configurations système et machine, ainsi que le masquage des informations sensibles (@MAC, @IP, version OS, etc.) des utilisateurs.

Assure le non-changement et la non-divulgation de ces derniers par l'utilisateur.


Montage_Dossier_Commun_Utilisateurs_Gestion
Étendue
Détails
Paramètres
Délégation
État
Configuration utilisateur (activée)
Préférences
Paramètres Windows
Mappages de lecteurs
Mappage de lecteur (lecteur : A)
A: (ordre : 1)
Général
Action
Mettre à jour
Propriétés
Lettre US (215,9 x 279,4 mm)
A
Emplacement
\\AD-DC1\Gestion
Reconnecter
Activé
Intituler
Dossier Commun Gestion
Utiliser le premier disponible
Activé
Masquer/Afficher ce lecteur
Afficher
Masquer/Afficher les lecteurs
Afficher
Commun
Options
Interrompre le traitement des éléments sur cette extension si une erreur se produit sur cet élément
Non
Exécuter dans le contexte de sécurité de l'utilisateur connecté (option de la stratégie utilisateur)
Oui
Supprimer cet élément lorsqu'il n'est plus appliqué
Non
Appliquer une fois et ne pas réappliquer
Non



Permet de monter et d'inscrire un raccourci sur le bureau le dossier commun par département de travail (créé et partagé en amont) pour chaque utilisateur en fonction de leur groupe de travail (hébergé sur le dossier partagé « Partage » avec un espace de noms DFS).



Création_et_Montage_Dossier_Personnel_Utilisateurs

Étendue | Détails | Paramètres | Délégation

Configuration utilisateur (activée)

Préférences

Paramètres Windows

Mappages de lecteurs

Mappage de lecteur (lecteur : U)

U: (ordre : 1)

Général

Action	Créer

Propriétés

Lettre US (215,9 x 279,4 mm)	U
Emplacement	\\AD-DC1\Utilisateurs$\%LogonUser%
Reconnecter	Désactivé
Utiliser le premier disponible	Désactivé
Masquer/Afficher ce lecteur	Afficher
Masquer/Afficher les lecteurs	Afficher

Commun

Options

Interrompre le traitement des éléments sur cette extension si une erreur se produit sur cet élément	Non
Exécuter dans le contexte de sécurité de l'utilisateur connecté (option de la stratégie utilisateur)	Oui
Supprimer cet élément lorsqu'il n'est plus appliqué	Non
Appliquer une fois et ne pas réappliquer	Non

Dossiers

Dossier (chemin d'accès : \\AD-DC1\Utilisateurs$\%LogonUser%)

%LogonUser% (ordre : 1)

Général

Action	Remplacer

Attributs

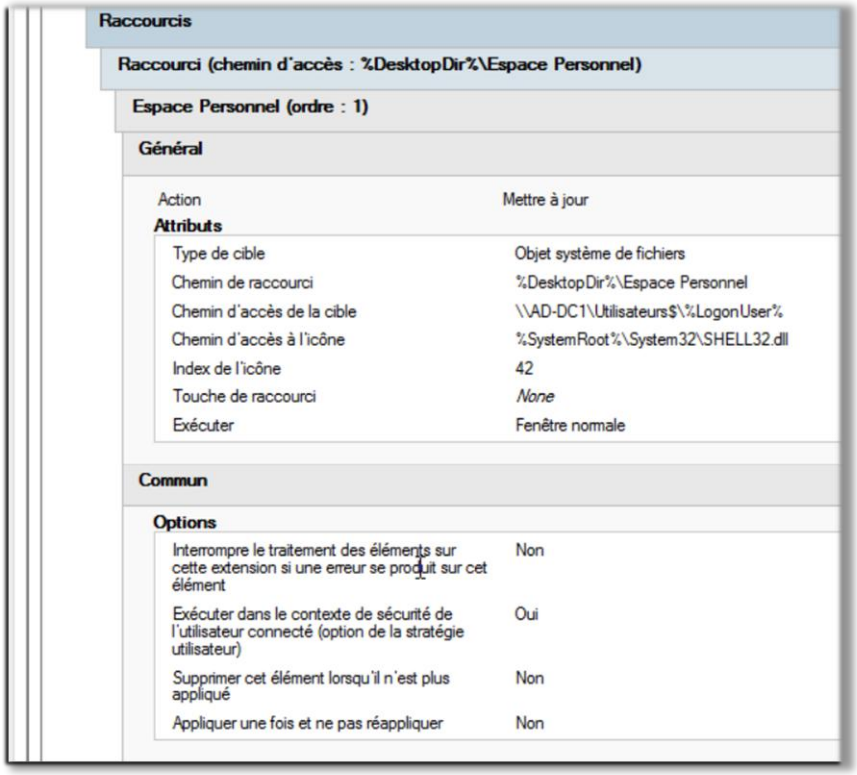
Chemin d'accès	\\AD-DC1\Utilisateurs$\%LogonUser%
Lecture seule	Désactivé
Caché	Désactivé
Archive	Activé

Supprimer ce dossier (s'il est vide)	Désactivé
Supprimer les sous-dossiers de manière récursive (s'ils sont vides)	Désactivé
Supprimer les fichiers du ou des dossiers	Désactivé
Autoriser la suppression des fichiers/dossiers en lecture seule	Désactivé
Ignorer les erreurs liées aux fichiers/dossiers impossibles à supprimer	Désactivé

Commun

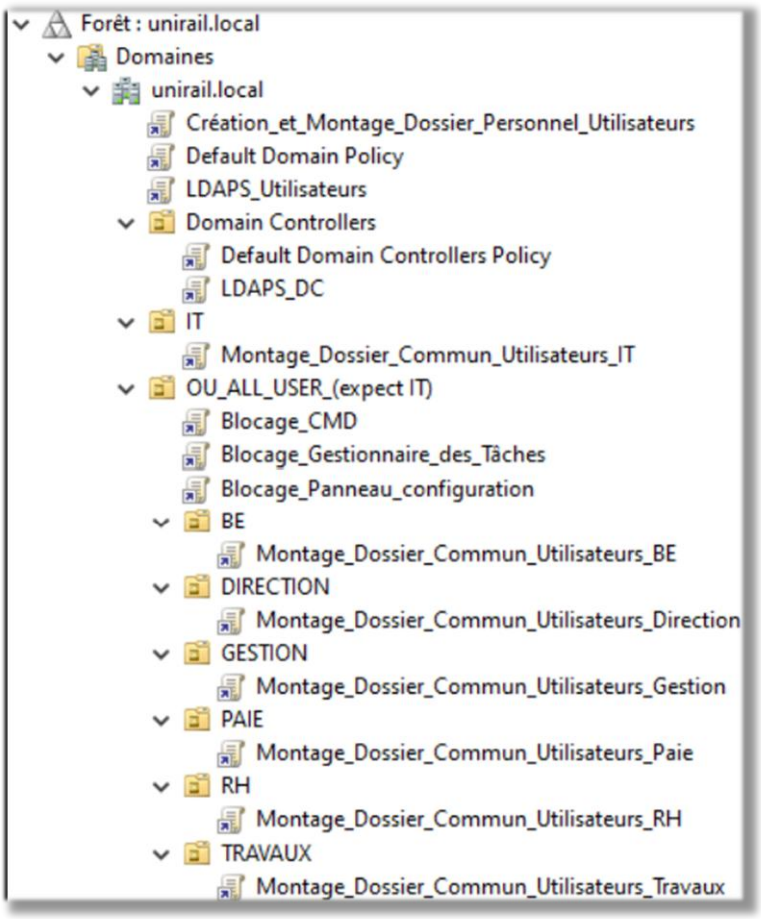
Options

Interrompre le traitement des éléments sur cette extension si une erreur se produit sur cet élément	Non
Exécuter dans le contexte de sécurité de l'utilisateur connecté (option de la stratégie utilisateur)	Oui
Supprimer cet élément lorsqu'il n'est plus appliqué	Non
Appliquer une fois et ne pas réappliquer	Non



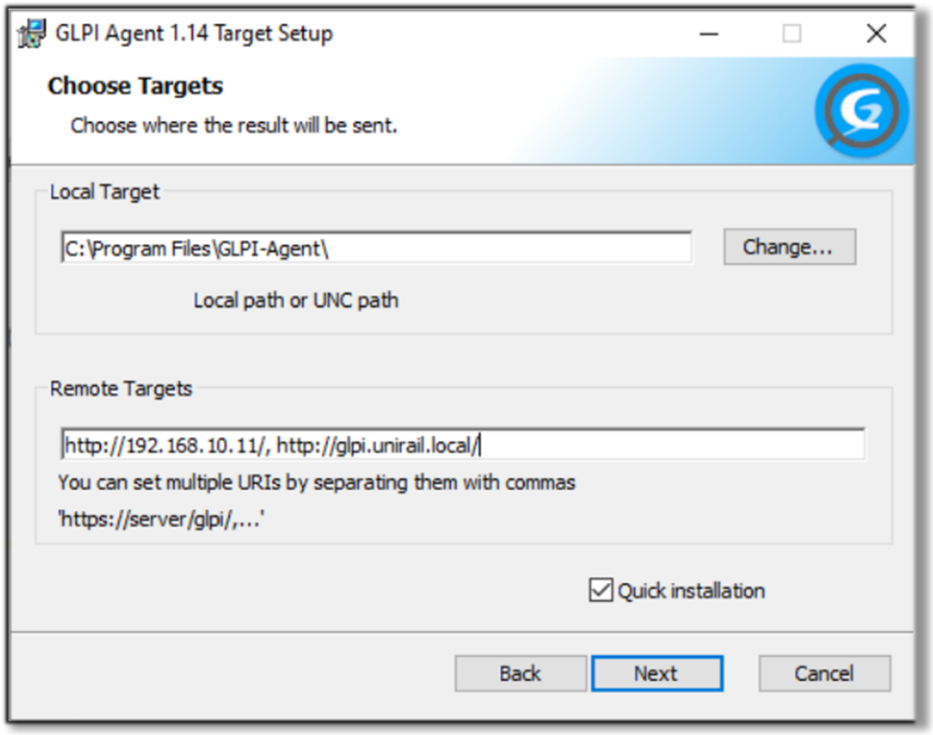
Permet de créer, de monter et d'inscrire un raccourci sur le bureau le dossier personnel de l'utilisateur (hébergé sur le dossier partagé « Utilisateurs » avec un espace de noms DFS).

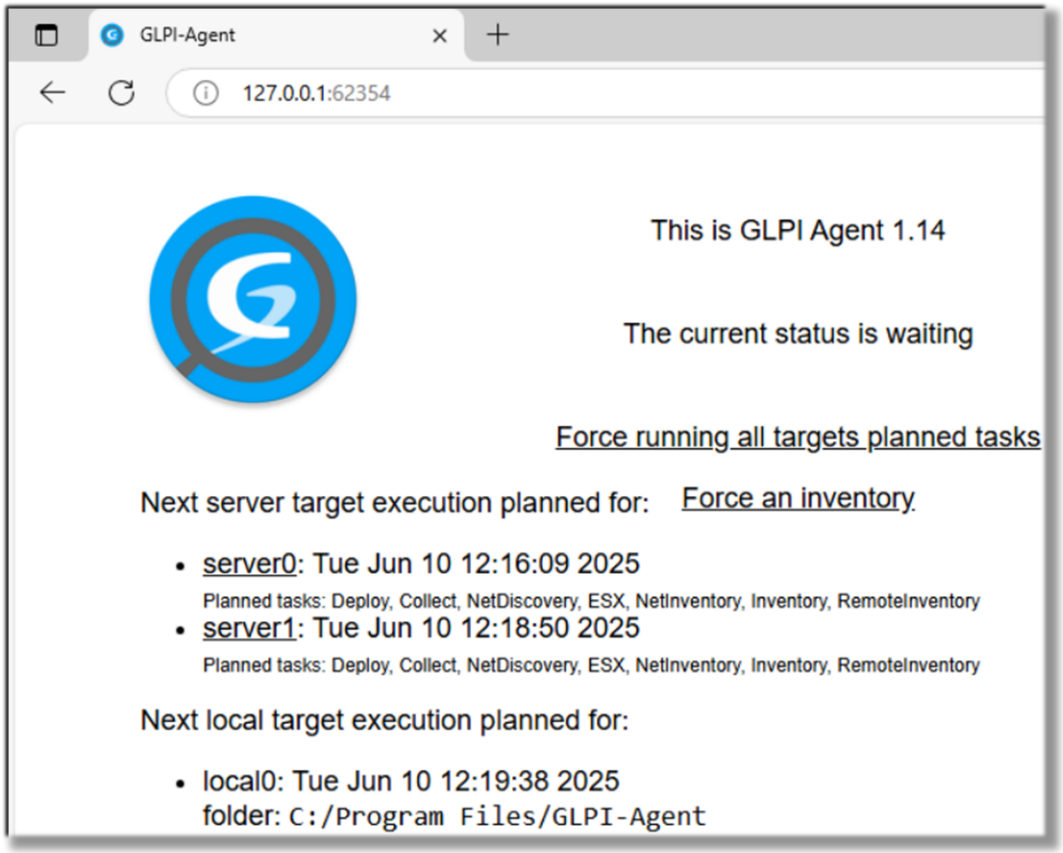
- Arborescence des GPOS :



vii. GLPI

- Installation de GLPI Inventory :

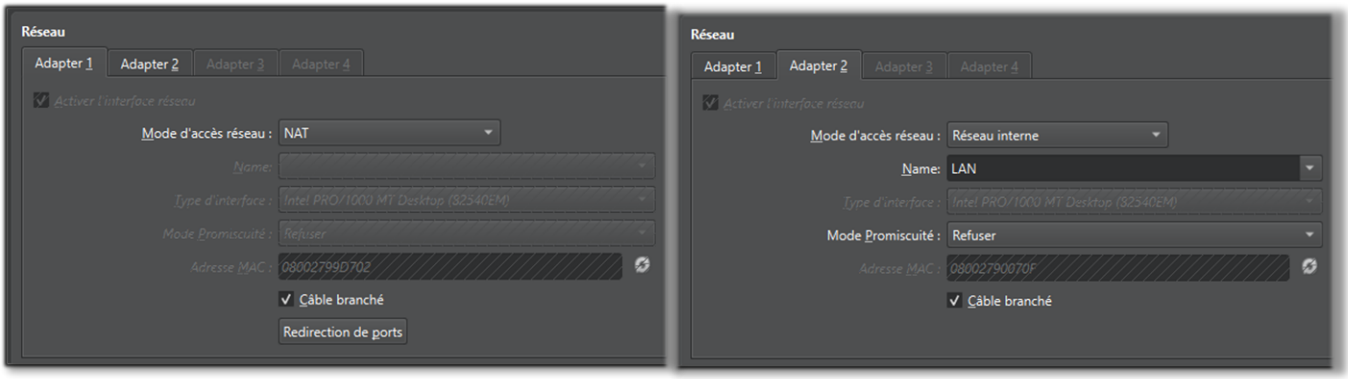




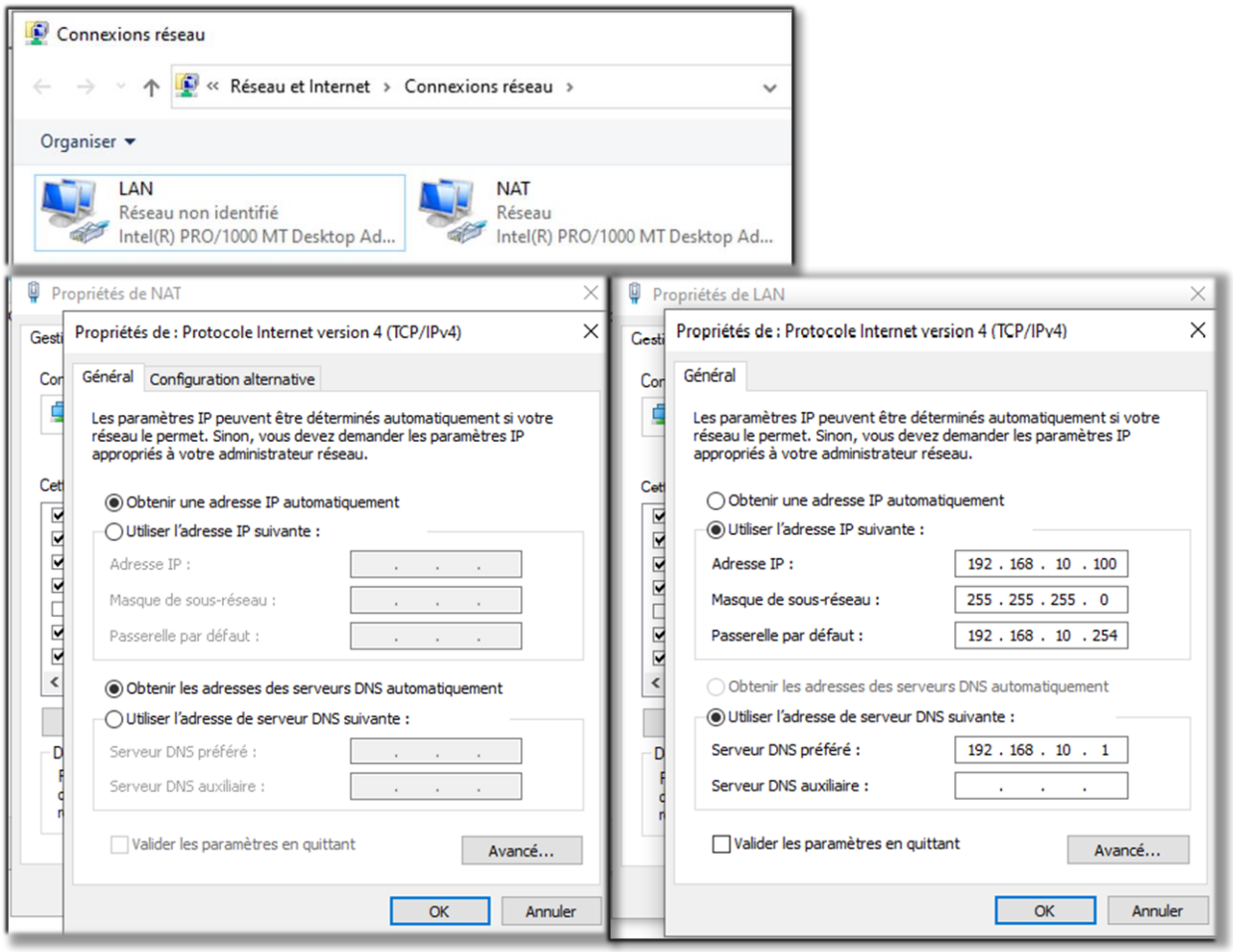
B. Client Windows 10

i. Configuration de la VM

➢ Configuration réseau de la VM :

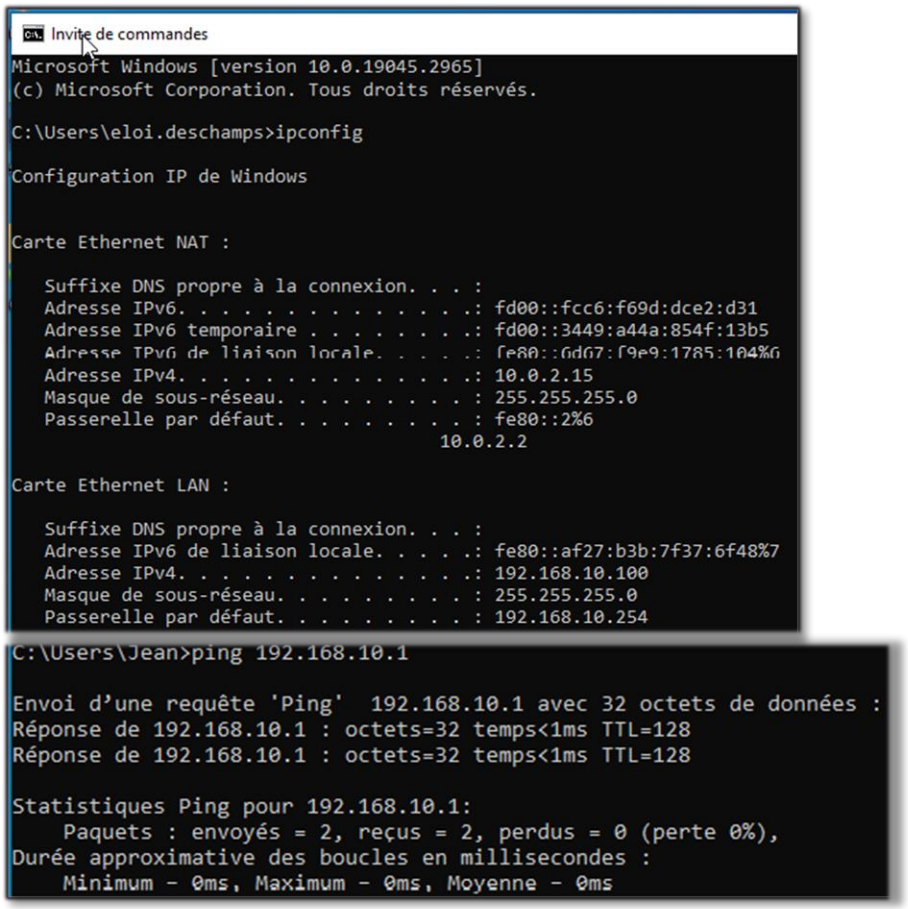


➢ Configuration des cartes réseaux :

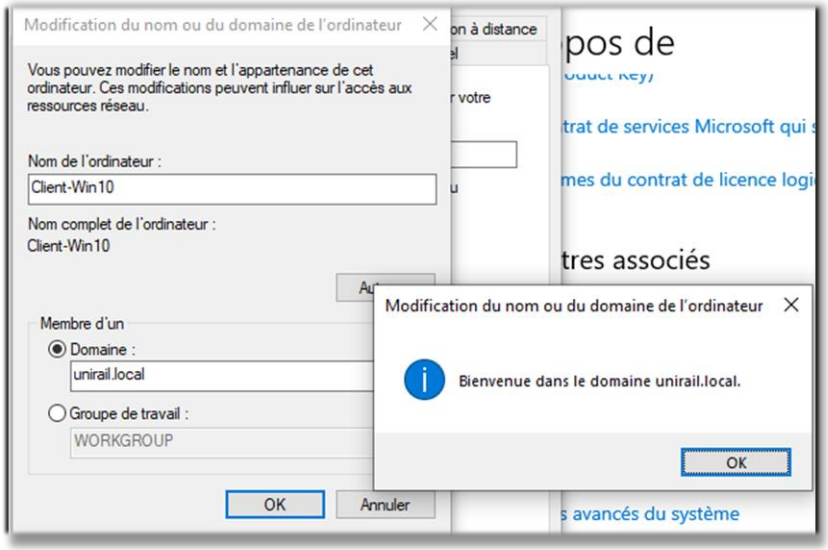


ii. Intégration au domaine

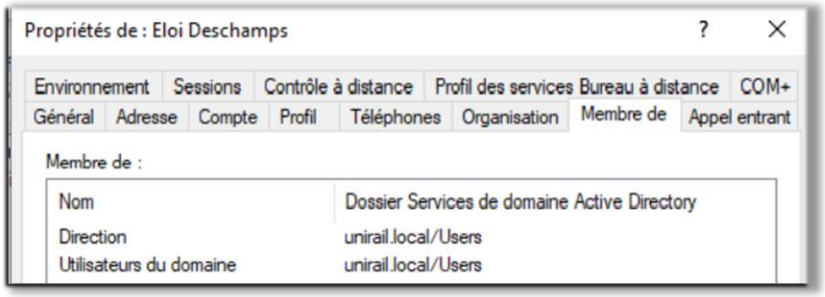
- Vérification de la communication réseau :



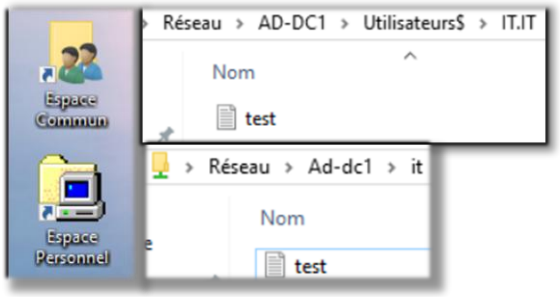
- Intégration au domaine :



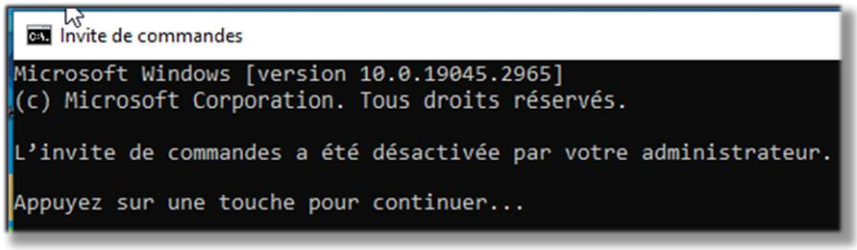
- Intégration du groupe « Direction » :

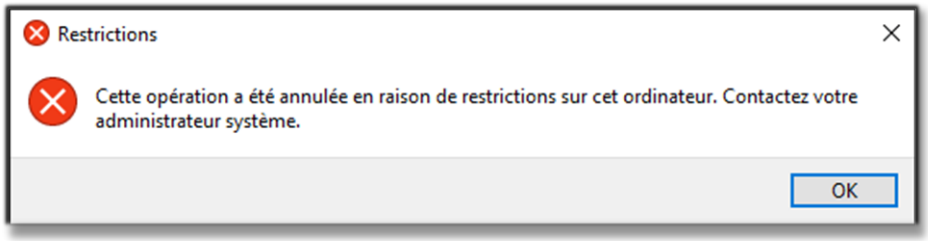


- Vérification de l'accès au dossier partage DFS :



- Vérification des GPOs :

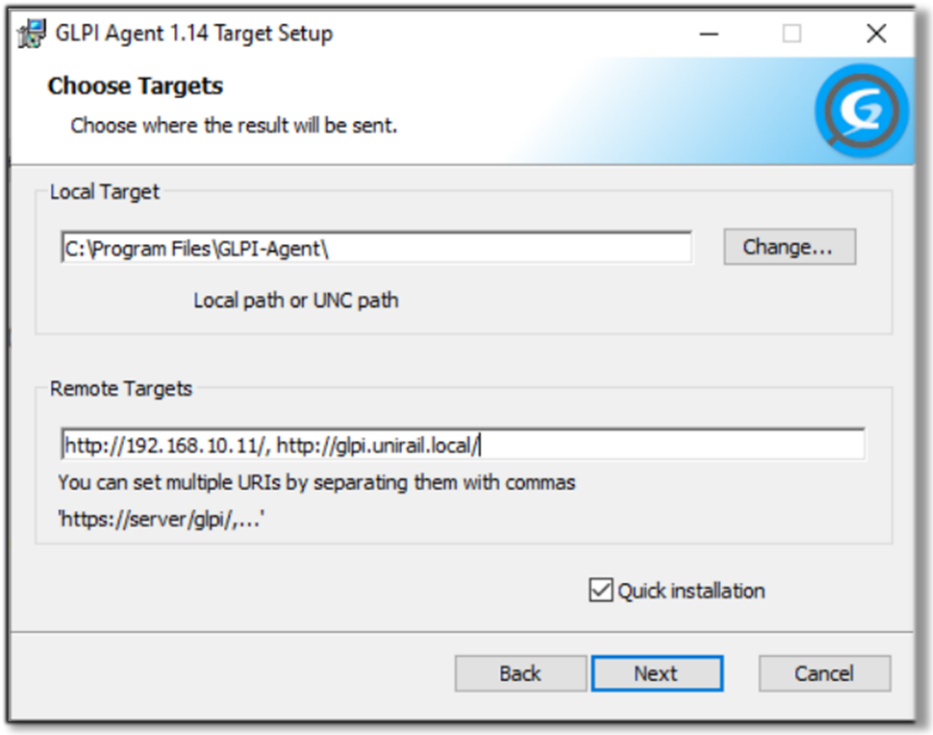


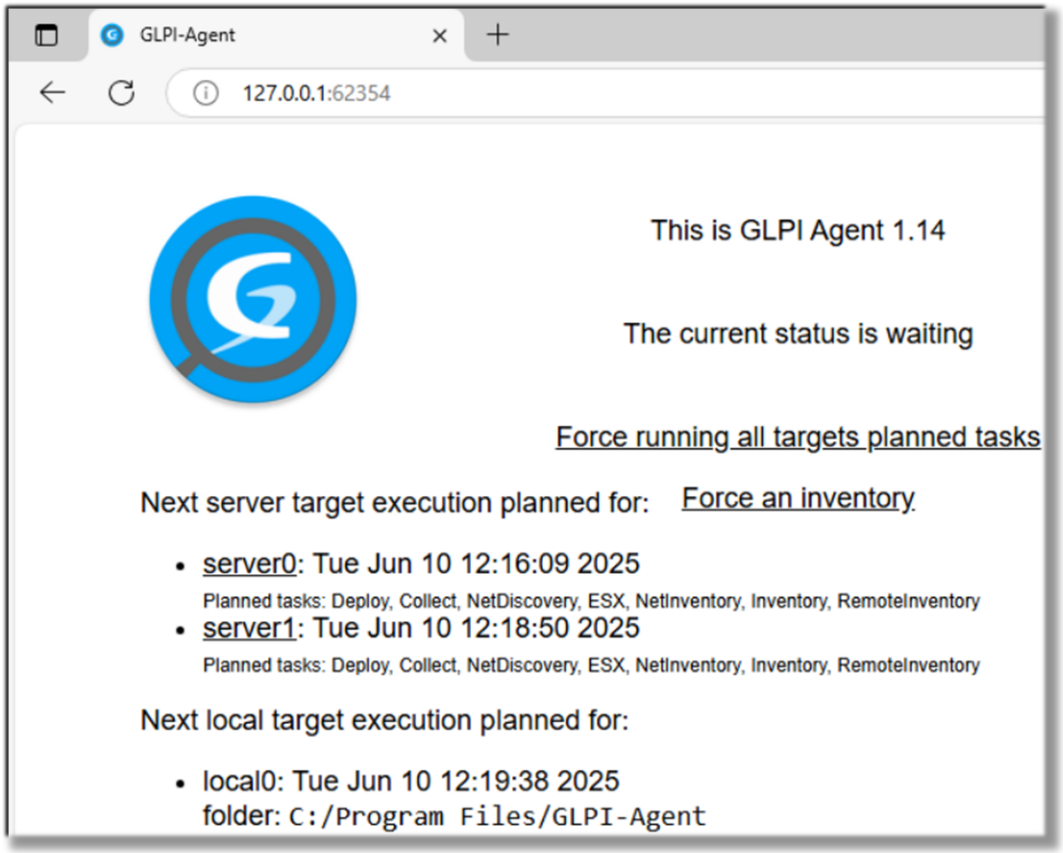


Panneau de configuration

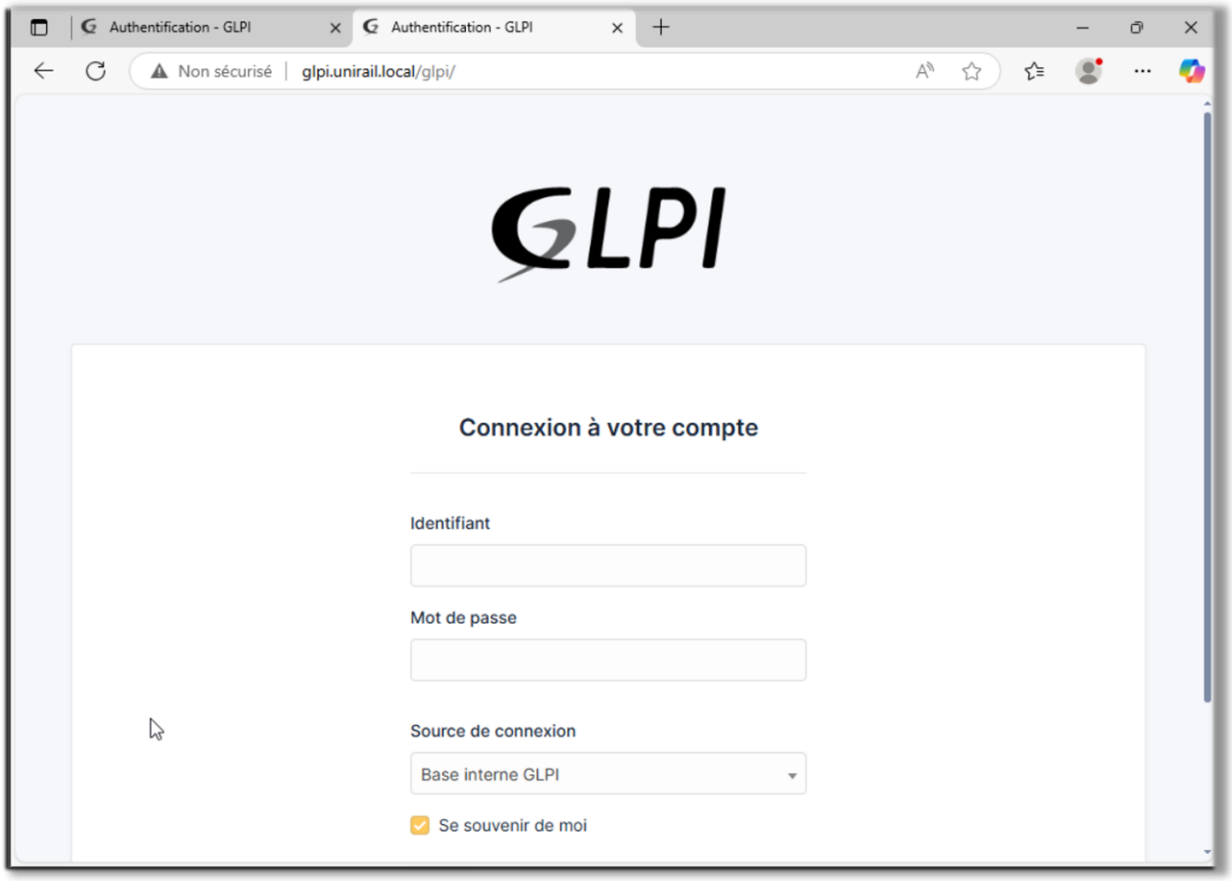
iii. GLPI

- Installation de GLPI Inventory :





- Accès à l'interface Web GLPI :



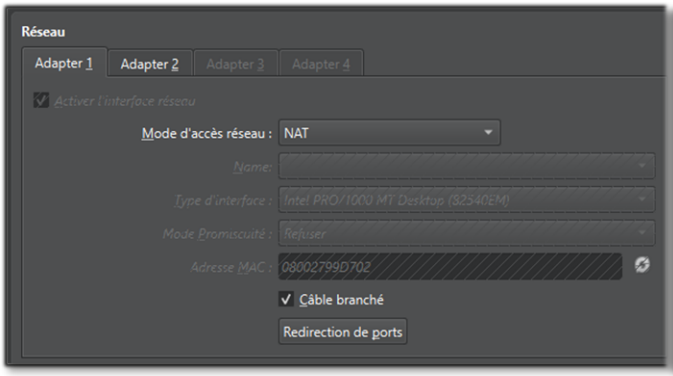
- Simulation de ticketing :

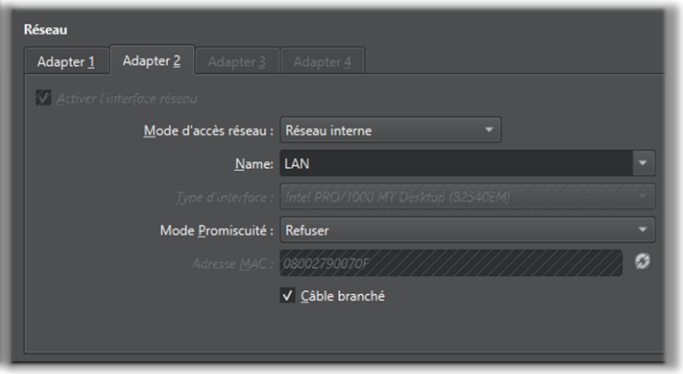
ID	TITRE	STATUT	DERNIÈRE MODIFICATION	DATE D'OUVERTURE	PRIORITÉ	DEMANDEUR - DEMANDEUR	ATTRIBUÉ À - TECHNICIEN	CATÉGORIE
2	Demande mise à jour logiciel KEEPASS	Nouveau	2025-06-10 12:04	2025-06-10 12:04	Basse	Deschamps Eloi		Logiciels
1	Remplacement écran poste de travail	Nouveau	2025-06-10 12:00	2025-06-10 12:00	Haute	Deschamps Eloi		Equipements

C. GLPI

i. Configuration de la VM

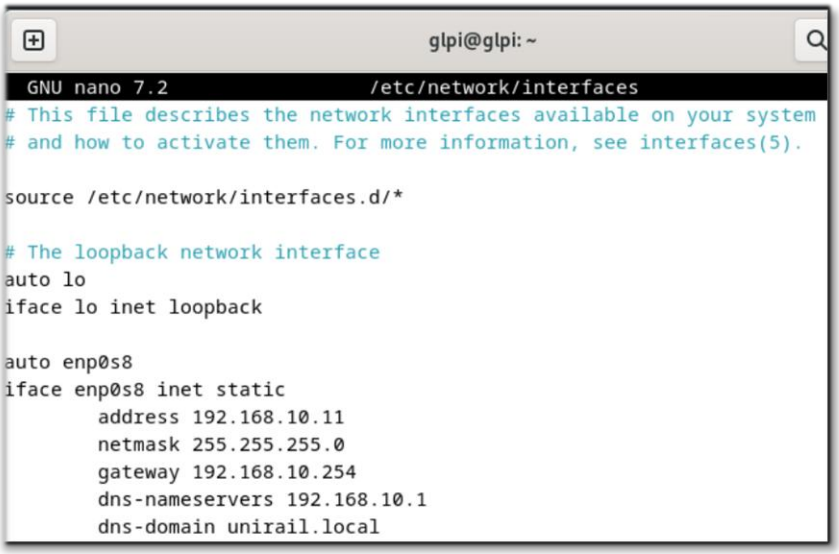
➢ Configuration réseau de la VM :





➢ Configuration des cartes réseaux :

- nano /etc/network/interfaces :



ii. Création et configuration BDD

➢ Installation d'apache :

- apt install apache2 php php-common libapache2-mod-php php-cli php-mysql php-xml php-xmlreader php-xmlwriter php-curl php-gd php-intl php-ldap php-zip php-bz2 unzip wget
- systemctl enable apache2
- systemctl start apache2

➢ Installation de la BDD :

- apt install mariadb-server
- mysql_secure_installation : no / no / yes / yes / yes / yes

➢ Configuration de la BDD :

- MySQL -u root -p :
  - create database glpi_db;
  - create user 'admin'@'localhost' identified by 'Admin1*';
  - grant all privileges on glpi_db.* to 'admin'@'localhost';
  - flush privileges;
  - exit;

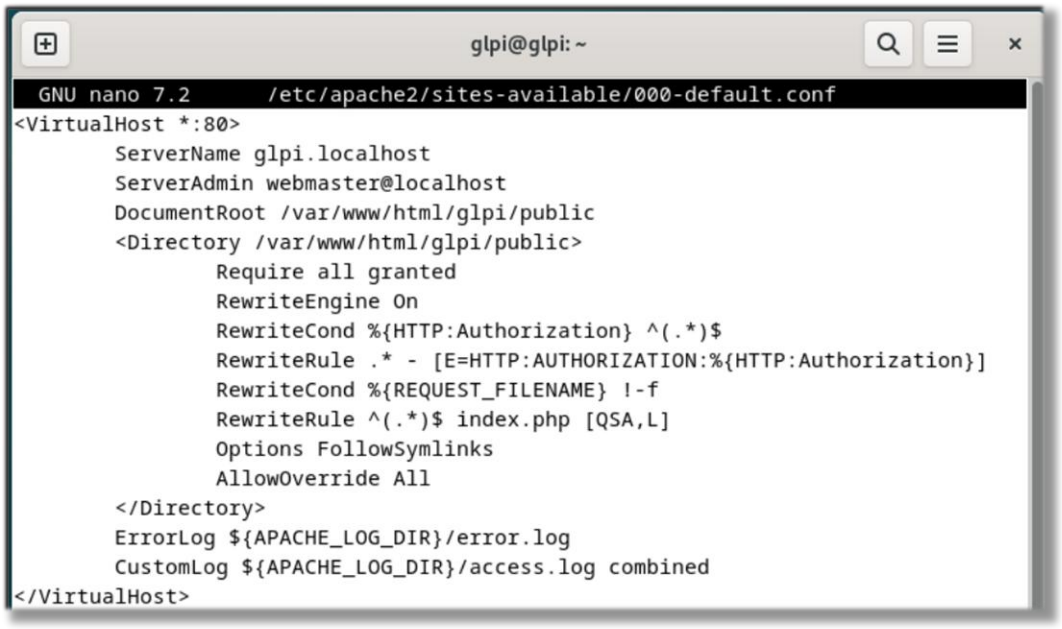
iii. Création et configuration de GLPI

➢ Téléchargement de GLPI :

- cd /var/www/html
- wget https://github.com/glpi-project/glpi/releases/download/10.0.17/glpi-10.0.17.tgz
- tar -xvzf glpi-10.0.17.tgz
- rm glpi-10.0.17.tgz

➢ Configuration de l'URL :

- nano /etc/apache2/sites-available/000-default.conf :



- systemctl restart apache2
- a2enmod rewrite
- systemctl restart apache2

- Configuration des permissions :
  - chown -R www-data:www-data /var/www/html/glpi
  - chmod -R 755 /var/www/html/glpi

- Configuration
  - nano /etc/php/8.2/apache2/php.ini :

- Installation de GLPI :
  - http://localhost/
  - http://glpi.unirail.local/
  - http://192.168.10.11/

- Suppression du dossier d'installation de GLPI :
  - rm /var/www/html/glpi/install/install.php

- Installation du plugin glpi-inventory :
  - cd /var/www/html/glpi/plugins/
  - wget https://github.com/glpi-project/glpi-inventory-plugin/releases/download/15.3/glpi-glpiiventory-1.5.3.tar.bz2
  - tar -xvf glpi-glpiinventory-1.5.3.tar.bz2
  - rm glpi-glpiinventory-1.5.3.tar.bz2

- Activation du plugin glpi-inventory :
  - Configuration : Plugins : GLPI Inventory : Actions : Installer
  - Configuration : Plugins : GLPI Inventory : Actions : Activer

iv. Gestion du parc

AD-DC1	innotek GmbH	VirtualBox-d9c927f0-fbd8-4256-8582-35f5bd9493fb	VirtualBox	VirtualBox	Microsoft Windows Server 2022 Standard
Client-Win10	innotek GmbH	VirtualBox-c7923cda-7f6f-4c73-967b-97d911c2e553	VirtualBox	VirtualBox	Microsoft Windows 10 Professionnel

v. Supervision des tickets