CESi
ENSEIGNEMENT
SUPÉRIEUR
ET FORMATION
PROFESSIONNELLE

Projet Evolution

CYC

« Customize Your Car »

M. Fabien DAUVERGNE
M. Jérémy DUPIN

19/12/2018

Table des matières

I. Introduction

1. Contexte

Nouvellement embauché au sein de l'entreprise CYC (Customize Your Car), nous devons mettre en place un ensemble d'outils d'administration de parc tout en implantant des solutions de sécurité et de tolérances aux pannes.

Le système d'information a été monté il y a plusieurs années par une connaissance du PDG.

Le parc se compose d'équipements informatiques dans un environnement sans serveurs.

2. Cahier des charges

Nous présenterons une maquette Cisco Packet Tracer fonctionnelle de l'architecture réseau choisie.

Une maquette opérationnelle sera mise en place pour effectuer une démonstration devant la Direction de l'établissement.

Il nous a été également demandé de respecter les points suivants :

- ✓ Faire cohabiter un serveur Windows DHCP et un serveur Linux DHCP sur le même réseau
- ✓ Installer un serveur Windows DNS et un serveur Linux DNS en cas de panne de l'un, l'autre doit prendre le relais.
- ✓ Effectuer une sauvegarde régulière des différents serveurs
- ✓ Mettre en place une solution de supervision
- ✓ Installer un serveur de fichiers
- ✓ Créer un dossier personnel par utilisateur
- ✓ Mettre à disposition un dossier commun avec archivage tous les jours à 19h et suppression du dossier d'archivage datant de plus de 3 semaines
- ✓ Décrire une solution de gestion des impressions
- ✓ Budgétiser l'intégralité des solutions proposées

II. Architecture réseau

1. Topologie réseau

Afin de distribuer le réseau sur l'intégralité du site, les choix suivants ont été fait :

Une topologie en étoile a été adoptée, nous prenons des commutateurs CISCO de distribution paramétrable essentiels pour les VLANs. Il y aura un commutateur par bâtiments.

Nous prévoyons des commutateurs de secours en cas de panne pour un changement rapide.

Des points d'accès sans fil seront répartis sur le site, afin de diffuser dans chaque bâtiment un réseau Wi-Fi (ISO 802.11), permettant aux ordinateurs portables et aux tablettes une connectivité optimale et mobile. Cisco Aironet 1850 Series Access Points

Le cœur de réseau sera lui composé de deux commutateurs en redondance. Ce dispositif permet lors d'une panne d'un des deux appareils de prendre l'intégralité de la charge du travail grâce à un câblage en redondance.

Les connectiques entre les commutateurs se feront grâce à des câbles Ethernets cuivrés 1 GB/s de catégorie 6.a. Les liens entre les matériels réseaux seront redondés.

Une baie de stockage sera connectée directement au serveur pour gérer les données de l'entreprise.

Les sauvegardes seront effectuées avec un serveur que nous appellerons « backup » et un lecteur de bande sera utilisé pour externaliser nos données.

2. Connexion Internet

L'accès internet arrivera par Fibre optique sur un routeur situé dans la salle serveur, et sera ensuite distribué à l'ensemble des employés. En cas de panne nous prévoyons une connexion de secours 4G chez notre opérateur afin que les utilisateurs puissent continuer de travailler. Si toutefois il y a une panne de la connexion principale, le relais avec la connexion secondaire 4G entrainera une faible perte de performance sur le débit internet.

Un pare-feu physique sera mis en place il se situera juste après le routeur. Pour des raisons de sécurité nous préférons faire intervenir des prestataires extérieurs afin de configurer le système de pare-feu. Nous estimons que nous manquons de compétence pour intervenir sur ce point critique de la sécurité informatique de notre entreprise. Le coût du pare-feu, ainsi que son installation et son administration est de 12000€. Il aura pour rôle en plus de sécuriser notre accès internet, de servir de proxy, et de serveur VPN si besoin futur.

3. Localisation du matériel informatique et interconnexion

A. La salle serveur

Elle contient les serveurs, les commutateurs « backbones », le routeur, le pare-feu, et le commutateur pour le bâtiment principal. Cette salle devra être dans une pièce fermée avec un accès se limitant aux informaticiens, avec une climatisation, sans fenêtre, et non accolée à un mur extérieur.

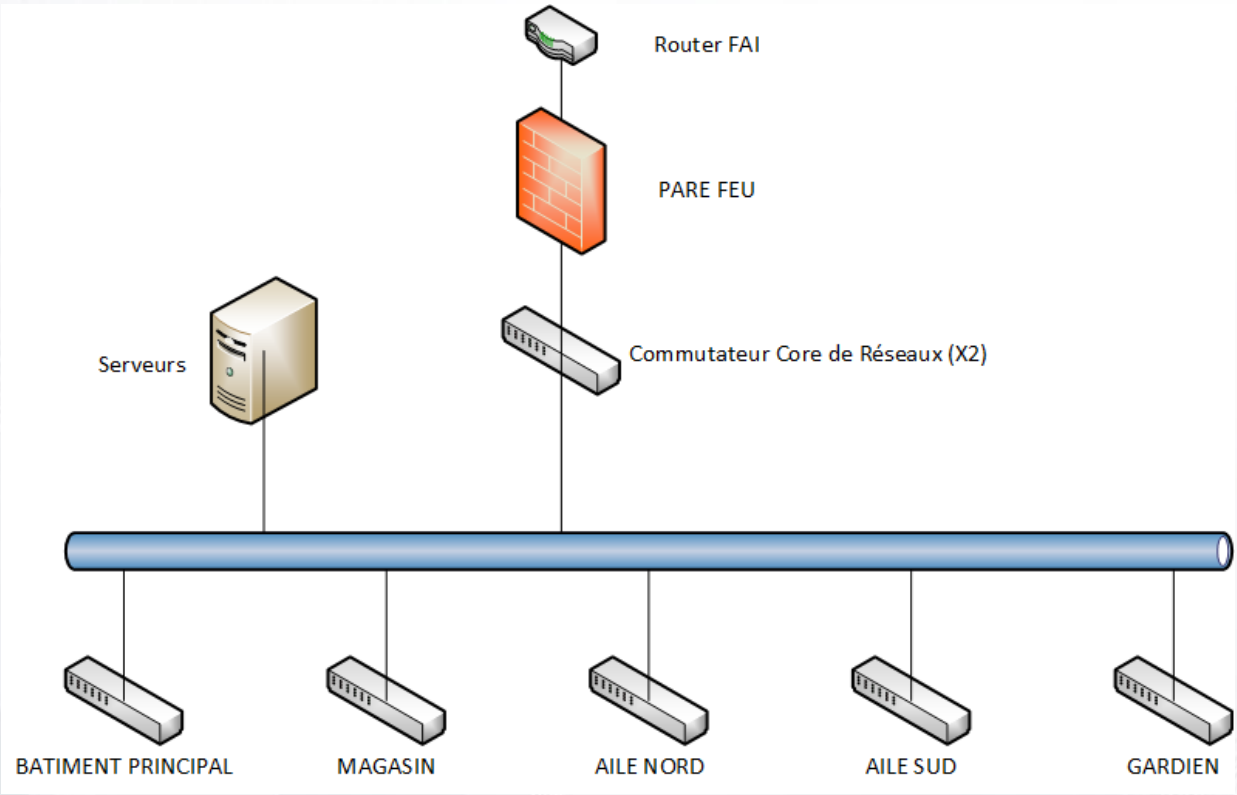
Le matériel informatique sera rangé dans une armoire type baie de brassage assez grande (28U minimum). L'idéal serait de la placer au milieu de la pièce pour permettre une facilité d'accès et une meilleure organisation des câbles.

B. Les baies de brassage

Il y aura six baies de brassage, une par étage de chaque bâtiment. Elles seront reliées par des câbles cuivre catégorie 6.a permettant de distribuer un débit pouvant atteindre jusqu'à 10Gb/s. Nous comptons un commutateur et un relais sans fil par baie.

Chaque baie se situera dans un local technique fermé, elle se composera d'une petite armoire suspendue. Nous avons décidé de prendre des armoires de 6U minimum, nous prévoyons ainsi les différents besoins que nous aurons dans le futur.

Même s'il n'y a, pour le moment, qu'un seul poste dans le bâtiment gardien nous avons préféré mettre un commutateur afin d'anticiper un besoin futur.

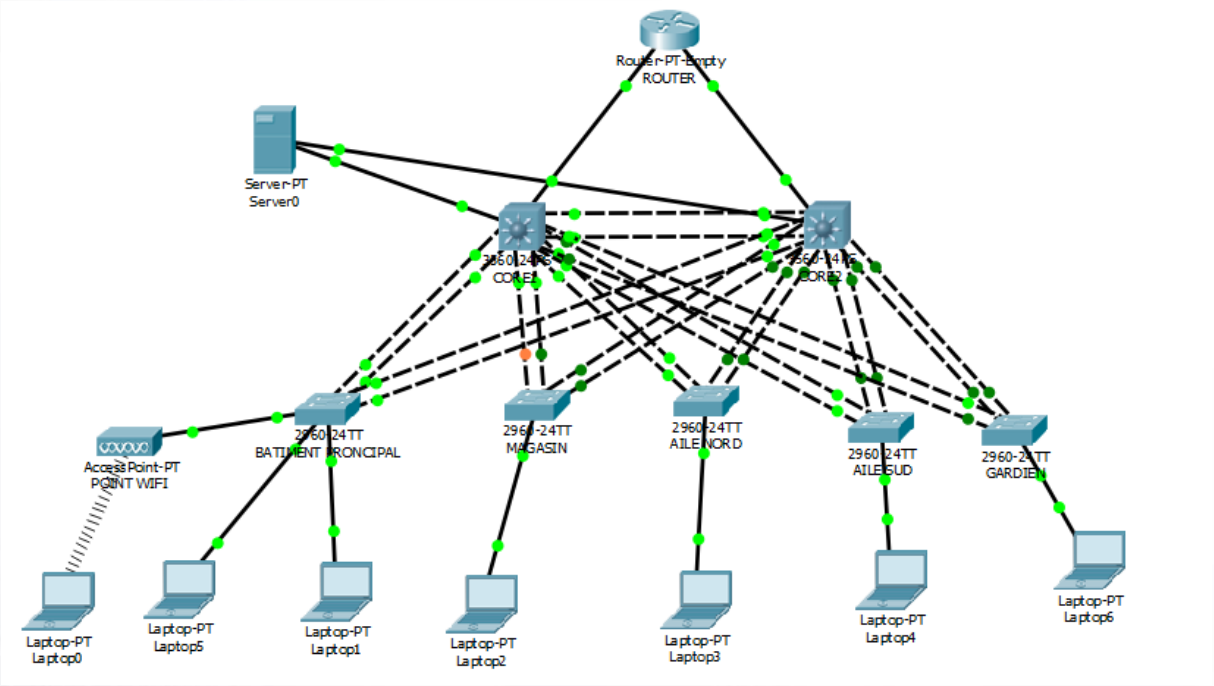


Récapitulatif de la topologie réseau

Nous avons effectué sur le logiciel CISCO Packet Tracer une maquette de notre infrastructure réseau.

Nous pouvons observer que tous les postes sont reliés au réseau, que le serveur DHCP leur attribue une adresse IP.

Tous les postes ou serveurs connectés au réseau avec cette configuration peuvent communiquer entre eux les requêtes ICMP (ping) sont réussies.



Capture d'écran de la maquette CISCO Packet Tracer

C. VLAN et adressage IP

Un VLAN est un réseau local (LAN) virtuel indépendant. Il permet de sécuriser le réseau sur la couche 2 du modèle OSI, de limiter le domaine de broadcast et ainsi d'optimiser la bande passante.

La configuration des VLANs s'effectue au niveau des commutateurs, et les routes, pour permettre de les faire communiquer, au niveau du routeur.

Nous organisons le réseau avec les VLANs suivants :

VLAN ID	Nom	Réseaux	Domaine d'application
10	Serveur	192.168.10.0	Tous les serveurs
20	Management	192.168.20.0	Matériel Réseau (Commutateurs, relais WIFI)
30	Informatique	192.168.30.0	Poste service informatique
40	Direction	192.168.40.0	Services : Direction, administratif
50	Old	192.168.50.0	Service : Old
60	Custom	192.168.60.0	Service : Custom
70	Imprimante	192.168.70.0	Imprimante et télécopieur
80	Wifi	192.168.80.0	WIFI

Le VLAN 1 qui est le VLAN par défaut et servira de VLAN natif ne sera pas utilisé, cela permet d'augmenter la sécurité de notre réseau interne.

Pour les commutateurs de niveau 3 (cœurs de réseaux) nous allons créer des routes afin que le VLAN 10 et 30 puissent communiquer avec tous les autres VLANs excepté le VLAN 1. Dans notre maquette Cisco Packet Traceur nous feront ces routes avec le routeur.

Nous utiliserons un masque de sous réseaux 255.255.255.0 qui nous permet d'avoir 254 machines par VLAN

Les serveurs, les commutateurs, et les imprimantes ont une adresse IP statique tandis que les postes utilisateurs ont une adresse dynamique alloué par un serveur DHCP.

Nom de la Machine virtuelle	Nom du serveur	Adresse IPV4	Masque de sous-réseau	Passerelle
Pfsense	Pfsense	192.168.10.254	255.255.255.0	192.168.1.50
Windows Manager	WINMANAGER	192.168.10.243	255.255.255.0	192.168.10.254
Windows Server DHCP	WINDHCP	192.168.10.252	255.255.255.0	192.168.10.254
Linux Server DHCP	LINDHCP	192.168.10.251	255.255.255.0	192.168.10.254
Windows Server AD / DNS	WINAD	192.168.10.250	255.255.255.0	192.168.10.254
Linux Server DNS	LINDNS	192.168.10.249	255.255.255.0	192.168.10.254
Windows Server Impression	WINPRINT	192.168.10.246	255.255.255.0	192.168.10.254
Windows Server Répertoire Partagé	WINREP	192.168.10.245	255.255.255.0	192.168.10.254
Serveur Backup	WINBACKUP	192.168.10.247	255.255.255.0	192.168.10.254
Serveur Déploiement	WINDEPLOY	192.168.10.248	255.255.255.0	192.168.10.254

Adressage IP des serveurs

Nom	Localisation	Adresse IPV4	Masque de sous-réseau	Passerelle
CORE1	Baie 1	192.168.20.11	255.255.255.0	192.168.20.254
CORE2	Baie 1	192.168.20.12	255.255.255.0	192.168.20.254
BATIMENT PRICIPAL	Baie 1	192.168.20.13	255.255.255.0	192.168.20.254
WIFI BP	Baie 1	192.168.20.14	255.255.255.0	192.168.20.254
MAGASIN	Baie 2	192.168.10.21	255.255.255.0	192.168.20.254
WIFI MAG	Baie 2	192.168.10.22	255.255.255.0	192.168.20.254
AILE NORD	Baie 3	192.168.10.31	255.255.255.0	192.168.20.254
WIFI NORD	Baie 3	192.168.10.32	255.255.255.0	192.168.20.254
AILE SUD	Baie 4	192.168.10.41	255.255.255.0	192.168.20.254
WIFI SUD	Baie 4	192.168.10.42	255.255.255.0	192.168.20.254
GARDIEN	Baie 5	102.168.20.51	255.255.255.0	192.168.20.254

Adressage IP des commutateurs

D. VTP

Protocole agissant sur la couche 2 du modèle OSI. Il est utilisé pour configurer et administrer les VLANs sur les commutateurs. Il permet d'ajouter, renommer ou supprimer un ou plusieurs VLANs sur le seul commutateur « serveur ». Grace au protocole les autres commutateurs « client » dans un même domaine VTP auront l'information et changeront leur table de VLAN. VTP permet d'homogénéiser les IDs des VLAN ainsi que leurs noms dans tout le domaine VTP. Un commutateur « serveur » agit aussi comme un « client » Dans notre cas nous choisissons de mettre les deux commutateurs cœur de réseau « serveur » et les autres « client »

Nous pouvons observer sur tous les commutateurs grâce au VTP :

```
10   Server                         active
20   Management                     active
30   Informatique                   active
40   Direction                      active
50   old                            active
60   Custom                         active
70   Imprimantes                    active
80   Wifi                           active
1002 fddi-default                   active
1003 token-ring-default             active
1004 fddinet-default                active
1005 trnet-default                  active
```

Capture d'écran de la commande : « show vlans » sur un commutateur dans CISCO Packet Tracer

E. Optimisation du réseau.

La redondance appliquée sur notre infrastructure réseau peut créer un problème de boucle. Une boucle implique tempête de diffusion (broadcast), l'instabilité de la table MAC, ainsi que plusieurs copies de la même trame. Ces évènements rendent le réseau indisponible.

STP (spanning-tree protocol) est un protocole réseau sur la couche liaison du modèle OSI, permettant au commutateur de communiquer entre eux afin de fermer des ports pour éviter de faire des boucles dans le réseau.

PVTP+ (per VLAN spanning tree protocol) est le protocole propriétaire CISCO permettant d'administrer les priorités des commutateurs par VLAN sur le réseau. Nous avons décidé de sélectionner nos deux commutateurs cœur de réseau prioritaire afin de mieux partager les trames Ethernet. Un load-balancing (partage de charge) est effectué. Nous pouvons observer sur notre maquette que CORE1 est « root bridge » sur les VLANs 10, 30, 50, 70 et CORE2 est « root bridge » sur les VLANs 20, 40, 60, 80. Cela veut dire que les trames Ethernet seront dirigées en priorité sur leur VLAN concerné, cette opération permet de mieux utiliser les ressources réseaux.

L'Etherchannel consiste à raccorder deux câbles réseaux physiques entre deux commutateurs pour en former un seul logiquement. Pour cela nous utilisons le mode LACP (commun à tous les constructeurs de commutateur, « norme IEEE 802.3ad ») pour créer un agrégat de liens entre les commutateurs. Augmentant la redondance donc la disponibilité du réseau, nous pouvons aussi augmenter la vitesse de la bande passante, si nous avons deux liens de 1Gb/s chacun, nous avons une bande passante théorique de 2Gb/s, en revanche le débit ne sera pas doublé, l'Etherchannel ne permet pas d'améliorer celui-ci.

III. Système d'information

1. Virtualisation serveur

Pourquoi virtualisé ?

La virtualisation est un ensemble d'outils techniques permettant de faire tourner plusieurs systèmes d'exploitation sur une machine Physique.

Les avantages :

La virtualisation devient omniprésente en entreprise, en effet cette technologie permet plusieurs avantages en comparaison avec une installation physique :

- ✓ Une économie matérielle, deux serveurs (le deuxième pour la redondance) suffise pour faire fonctionner toutes les machines virtuelles que nous aurons besoin. Comparé à une installation par système pour des installation physique uniquement.
- ✓ Une économie d'énergie, moins de serveur donc moins d'Energie nécessaire pour permettre leur fonctionnement

- ✓ Une utilisation matérielle optimisé, grâce à l'hyperviseur nous pouvons allouer les ressources processeur et mémoire. Sur un serveur physique l'utilisation des ressources est fixe
- ✓ Une fiabilité plus importante. Une redondance peut être fait avec un « transfère d'un serveur physique à l'autre en cas de panne sans pertes de disponibilités. Si un serveur physique ne fonctionne plus, les services s'arrêterons sans possibilité de reprise. De plus nous pouvons cloner une machine virtuelle, la transférer, la restaurer à partir un point précèdent, ceux qui peut permettre de migrer de serveur physique plus facilement et de corriger une erreur ou un incident grave plus rapidement

Quels hyperviseurs choisir :

Nous choisissons d'utiliser un hyperviseur de type 1 :

Installé directement, il dialogue directement avec la couche matérielle : c'est la solution la plus performante. Et celle utilisé majoritairement dans les entreprises.

Comparatif :

Nous nous sommes intéressés à 3 systèmes de virtualisation, Hyper v produit par Microsoft, ESX produit par VMWare, et Proxmox (Open Source) solution largement implantée dans le monde de l'informatique en entreprise

Hyper-V (Microsoft) : Solution gratuite appelée « Hyper-V Core » sans interface graphique.

Avantages :

Développé par Microsoft donc idéal pour un parc informatique déjà équipé de Windows, pas de problème de compactibilité. Console d'administration disponible sur un poste Windows 10 Pro (uniquement)

Inconvénients :

Domaine Windows recommandé, impossibilité de faire un cluster de serveur avec un domaine autre que Windows

Solution récente moins utiliser que VMWare qui est fortement attacher en entreprises.

ESX et ESXi (VMWare) : Solution gratuite pour ESXi, payante pour ESX

Avantages ***:***

Console d'administration V-Sphère très complète

Inconvénients :

Version gratuite avec peu d'options

ESX est une solution couteuse

Proxmox :

Avantages :

Utilisable pour tous environnement,

Open Source installation et utilisation gratuite

Inconvénients :

Support payant

Solution de virtualisation adoptée :

Nous avons fait le choix du produit Hyper-V. Nous préférons utiliser le budget pour d'autres domaines, et nous pensons que la version gratuite ESXi comporte trop peu d'option.

Avec un parc et des serveurs majoritairement sous environnement Microsoft, Hyper-V semble être la meilleure solution pour le long terme en manière de fiabilité en comparaison avec Proxmox qui est plus destiné aux environnement linux.

De plus le matériel personnel utilisé pour la conception de la maquette, possède un processeur Intel incompatible avec VMWare.

2. Choix du matériel Informatique

A. Poste de travail

Nous avons décidé de changer entièrement nos postes de travail du parc informatique.

Les ordinateurs déjà sur site sont estimés trop vieux. Afin de prévenir des pannes et d'assurer une continuité des services proposés par les postes de travail sur le long terme, nous décidons de remplacer les postes de travail par des nouveaux grâce à un contrat de location.

Le contrat de location durera trois ans. Ces trois années correspondent à la durée de vie d'une garantie acquise lors de l'achat d'un matériel neuf. Cela nous permet d'avoir des ordinateurs neuf tous les trois ans avec un coût mensuel fixe.

Station de travail mobil HP ZBook 14u G5

Le prix mensuel d'une Station de travail mobile HP ZBook 14u G5, comprenant, un processeur Intel® Core™ i7-8550U, une carte graphique Carte graphique dédiée AMD Radeon™ WX 3100 (2 Go de mémoire GDDR5 dédiée), 8Go de RAM (possibilité d'augmenter à 16Go) est environ de 70€. Une durée de 36 mois revient à 2520€ TTC le poste seul lui coûte 2000€.

Un ordinateur portable comme celui-ci permet d'avoir une utilisation confortable sur les logiciels Blender et GIMP.

Tous les trois ans nous auront des ordinateurs de nouvelle génération à un tarif similaire.

Cela nous permet aussi de ne pas avoir à gérer le recyclage des anciens matériels donc quelques économies seront réalisées sur le traitement des déchets électroniques.

Pour les ordinateurs portables achetés récemment nous attendrons une durée de trois ans et ainsi les remplacer par la même méthode.

Cette décision nous permet d'avoir un parc complètement homogène vu qu'il y aura une parfaite correspondance matérielle de tous les postes informatiques du parc.

Afin d'améliorer la qualité de service, il sera proposé à l'utilisateur des formations Windows 10 et bureautique office.

B. Choix des commutateurs

Il existe beaucoup de commutateurs différents, pour la couche Access nous avons besoin de 24 ports minimum pour les bâtiments de production et de 8 ports minimum pour le gardien. Le modèle C2960L-24TS (24 ports) et le modèle C2960L-8TS (8 ports) suffise pour notre usage. De plus ils sont plutôt économiques (600€ pour le premier 350€ pour le deuxième). Pour le cœur de réseau nous choisissons le modèle C9200L-24T-4X, commutateur de niveau 3 comprenant 24 ports 1Gb/s pour se connecter aux autres commutateurs, et 4 ports 10Gb/s pour se connecter au serveur.

C. Serveurs physiques

Nos machines virtuelles sont principalement sans interface graphique donc il demande peu de ressource. Pour la production, les serveurs : « Serveur Performance HPE ProLiant DL325 Gen10 7401P, monoprocesseur, 32 Go de RAM, P408i-a, 8 lecteurs SFF, alimentation redondante 1x800W », sont intéressant. Actuellement notre maquette fait 32Go de Ram et on peut constater quelques ralentissements, grâce à ce choix nous avons donc 64 Go de RAM et 48 cœurs disponibles pour toutes machines virtuelles. Nous pouvons assurer une évolution de nos serveurs (il est possible de rajouter de la mémoire vive, un processeur ou plusieurs disques durs), au cas où notre système d'information serait trop gourmand en ressources nous prenons en option deux cartes réseaux 10Gb/s ainsi que 3 disques dur 1To par serveur. Ils coûtent 8800.00€

Serveur Performance HPE ProLiant DL325 Gen10

Nous prévoyons un serveur de sauvegarde (que nous appelons backup), celui-ci a besoin de beaucoup moins de ressources par rapport aux serveurs de productions, mais il doit avoir suffisamment d'espace disque pour pouvoir enregistrer toutes les informations sur ses disques ou en écritures sur bandes un serveur entrée de gamme HPE ProLiant DL325 Gen10 7251,

monoprocesseur, 8 Go de RAM, alimentation redondante 500 W, suffit largement à nos besoins. Nous rajoutons 3 disques durs 1TO 7200tr/min pour le stockage. Le coût de ce serveur et de 4000€. Un lecteur de bandes sera rajouté, celui-ci accepte la technologie LTO-7 et ne peut contenir qu'une seule cassette, afin de pouvoir externaliser nos données pour prévenir des incidents majeurs imprévisibles.

Une armoire 24U est nécessaire afin d'installer tous les composants ainsi que deux onduleurs pour protéger notre système d'une éventuelle coupure réseaux. Le prix de cette armoire et de 500€

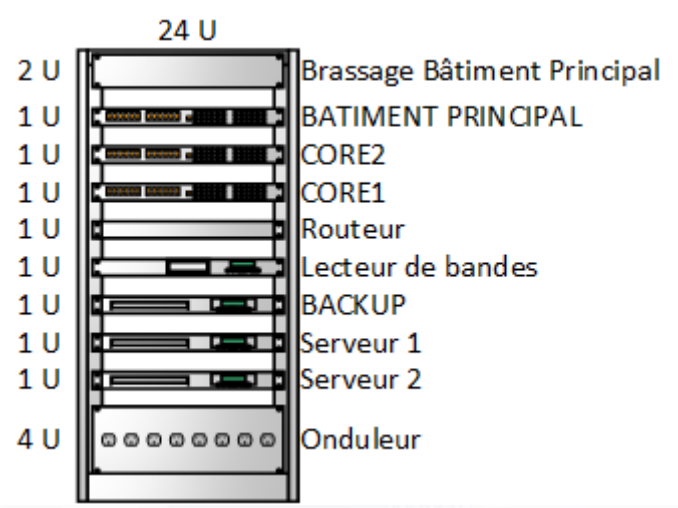


Schéma de l'armoire situé en salle serveur dans le bâtiment principal

IV. Supervision

Afin d'assurer la continuité du système informatique, un technicien informatique effectue quotidiennement les relevés d'informations des évènements et les rapports d'erreurs (logs) sur les différents serveurs.

Le logiciel de surveillance de disque dur SMART « HDD Health » est installé sur chaque serveur afin d'obtenir diverses informations comme la température, la capacité et encore l'état de santé.

Le technicien observe également le bon état de marche des équipements dans la salle serveur en vérifiant le clignotement des LED sur les baies.

Ces informations sont notifiées dans le tableau suivant :

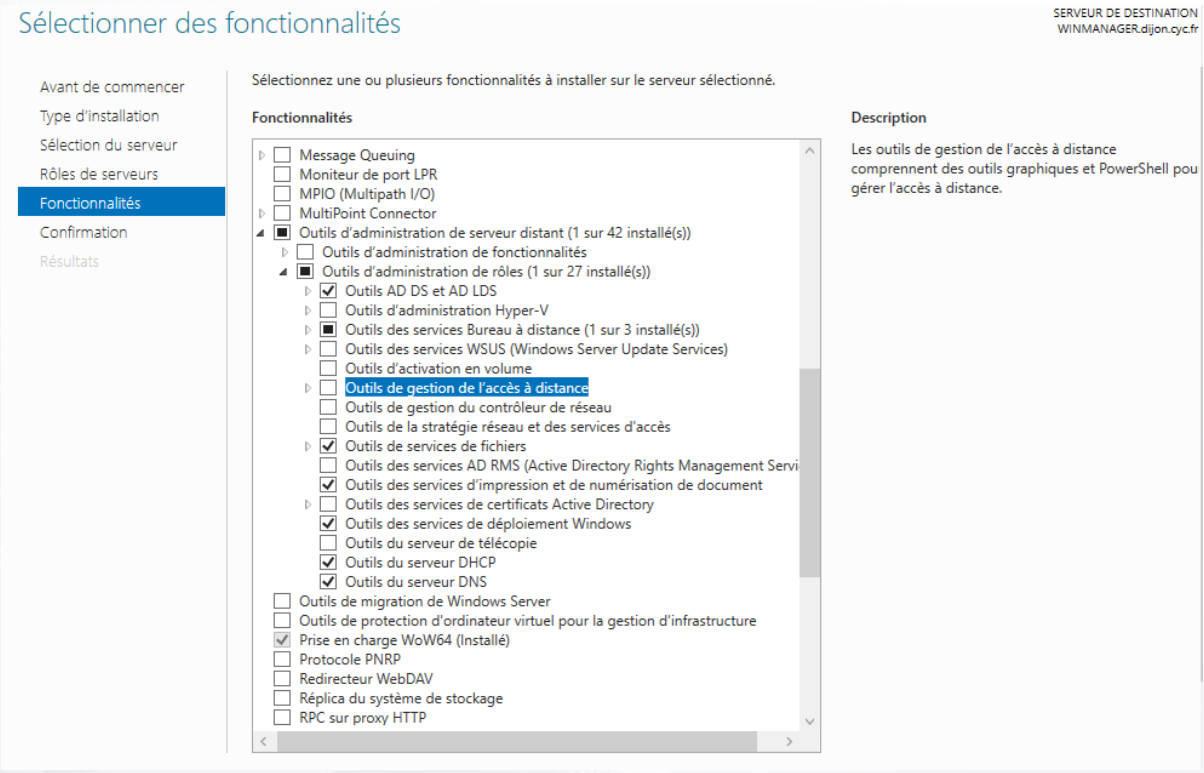
Nom du serveur	***Date***	lun 30 avril	mar 01 mai	mer 02 mai	jeu 03 mai	ven 04 mai
	Technicien	Jérémy DUPIN	Fabien DAUVERGNE	Jérémy DUPIN	Fabien DAUVERGNE	Fabien DAUVERGNE
Serveur 1	*Température*	35°C	35°C	35°C	35°C	35°C
	Etat de santé	Excellent	Excellent	Excellent	Excellent	Excellent
	Espace libre	46%	47%	47%	50%	52%
	Logs					
	Leds	Éteinte	Éteinte	Éteinte	Éteinte	Éteinte
Serveur 2	*Température*	35°C	35°C	35°C	35°C	35°C
	Etat de santé	Excellent	Excellent	Excellent	Excellent	Excellent
	Espace libre	65%	65%	65%	66%	67%
	Logs					
	Leds	Éteinte	Éteinte	Éteinte	Éteinte	Éteinte

Tableau des relevés d'information des serveurs

V. Serveurs

1. Windows Management

Pour administrer tous les serveurs nous avons choisi d'installer sur un seul serveur Windows Server 2016 en interface graphique avec l'installation des rôles des autres serveurs.

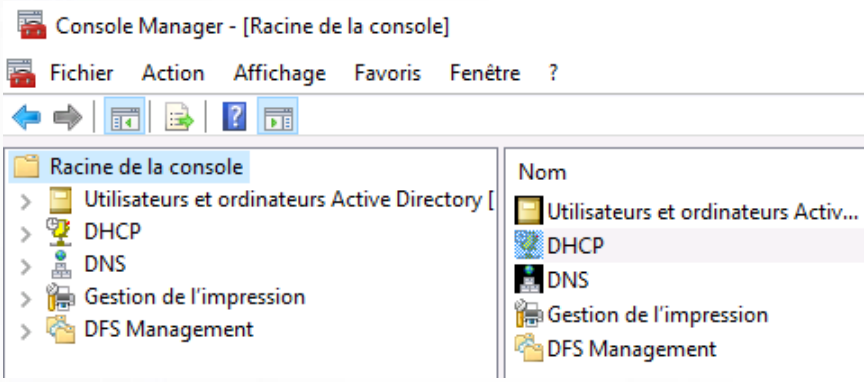


Les autres serveurs Windows sont en mode Core, ce qui permet d'avoir un système d'exploitation plus léger. En conséquence, le système requiert moins d'espace disque et moins de mémoire vive donc un faible coût. La surface d'attaque logicielle se trouve réduite puisqu'il y a moins de composants d'installer, donc moins de points d'entrées.

Serveur	Taille VHD (GB)	Temps de démarrage (s)	Nbre de ports ouverts	Redémarrage	Patchs critiques	Mémoire RAM Min.
Windows Server 2016 Full	10,4	1140	34	11	23	2 Go
Windows Server 2016 Core	6,5	300	26	6	8	512 Mo
Différence GUI vs Core	-63%	-26%	-76%	-55%	-35%	-26%

Comparatif entre Windows Server 2016 Desktop Expérience et Core

L'accès des différents serveurs se fera uniquement en Connexion Bureau à distance (RDP) sur le serveur 'WINMANAGER' ce qui permet de centraliser le management des serveurs. Une console MMC est configurée sur le bureau avec les différents rôles des serveurs.



Console MMC avec les rôles des différents serveurs

2. Serveurs Linux

Pour le serveur Linux, nous avons choisi d'installer Debian car c'est une distribution maintenue par la communauté en permanence. Elle nécessite peu de ressources donc un moindre coût. L'installation est simple et rapide.

Par ailleurs, nous l'installerons en mode console parce que les fichiers de configuration s'éditent facilement avec l'outil « Nano ». Cela nous permet également de l'administrer à distance avec des logiciels comme « PuTTY » ou « WinSCP ».

PuTTY permet de d'afficher une console à distance sur le serveur linux afin de le configurer.

WinSCP est un logiciel facilitant la manipulation de dossier et de fichiers grâce à une arborescence.

Pour communiquer avec ces logiciels, il faut laisser le port FTP (21) ouvert le temps des manipulations.

3. Active Directory

A. Définition

C'est la mise en œuvre de service annuaire LDAP, il offre une solution centralisée d'authentification, d'identification et de gestion de l'ensemble des objets d'un parc. On entend par objet, l'ensemble des ressources (imprimantes, ordinateurs, dossiers partagés), des services (serveur de messagerie) et des utilisateurs du parc. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs. Il fonctionne de manière hiérarchique.

Pour se faire on utilise des OU.

OU (Organisational Unit) unité organisationnelle, elle permet de regrouper un ensemble d'objets (utilisateurs, groupes, ressources) et de leur attribuer des droits ainsi qu'une politique de sécurité GPO (Group Policy Object).

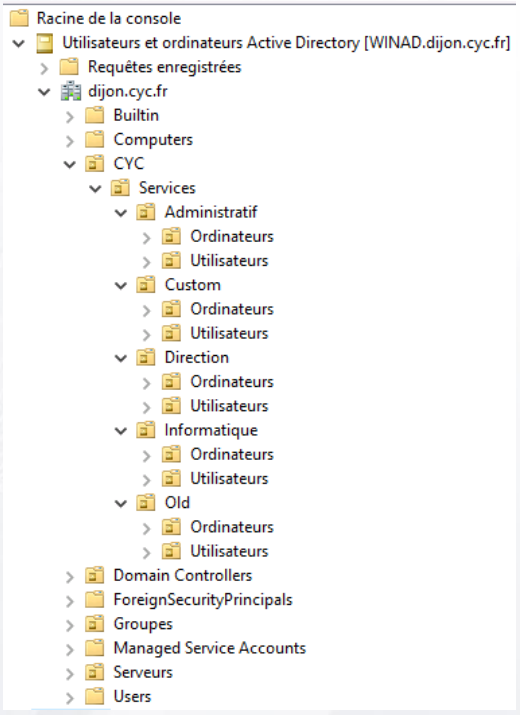
Des Groupes peuvent être créés dans l'AD, ils sont employés généralement à établir une liste d'utilisateurs et à leur attribuer des droits d'accès ou des services.

On distingue trois types de groupes :

Le groupe global : il peut contenir des utilisateurs de tous les domaines mais ne peut être placé que sur des ressources de son domaine.

Le groupe local : au sein d'un domaine, il est principalement utilisé pour affecter des droits à des ressources dans un domaine. Il peut comprendre des utilisateurs, des groupes globaux ou universels, issus du même domaine.

Le groupe universel : disponible depuis la version 2000, permet d'inclure des groupes et utilisateurs d'autres domaines.



Arborescence de l'Active Directory

B. Architecture de l'Active Directory

Pour créer le domaine sur Windows Server en mode Core, nous avons besoin d'installer les différents rôles : AD, AD Domain Services, DNS et de créer la nouvelle forêt en PowerShell.

Le script ci-dessous permet d'installer tous les rôles nécessaires pour l'AD et le DNS avec les outils d'administration à distance (RSAT AD Tools).

```
# Installation du rôle RSAT AD Tools
Add-WindowsFeature -Name RSAT-AD-Tools -IncludeManagementTools -IncludeAllSubFeature

# Installation du rôle AD Domain Services
Add-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools -IncludeAllSubFeature

# Installation du rôle DNS
Add-WindowsFeature -Name DNS -IncludeManagementTools -IncludeAllSubFeature

# Création de la nouvelle forêt
Import-Module ADDSDeployment
Install-ADDSForest -CreateDnsDelegation $false -DatabasePath "C:\Windows\NTDS" -DomainMode Default -DomainName "dijon.cyc.fr"
-DomainNetbiosName "CYC" -ForestMode Default -InstallDns:$true -LogPath "C:\Windows\NTDS" -NoRebootOnCompletion:$false
-SysvolPath "C:\Windows\SYSVOL" -Force:$true
```

Sur le serveur Windows Active Directory 'WINAD', nous avons créé une OU par service, avec à l'intérieur deux OU : *Ordinateurs* et *Utilisateurs* pour faciliter la mise en place de GPO au sein des différents services de l'entreprise. Une OU *Groupes* et *Serveurs* sont également crées pour gérer respectivement les documents partagés et les équipements réseaux.

C. Script PowerShell

Afin de faciliter la création des groupes dans l'Active Directory, nous avons élaboré un script PowerShell.

Celui-ci mettra automatiquement les groupes globaux pour les fichiers communs par service dans la bonne OU.

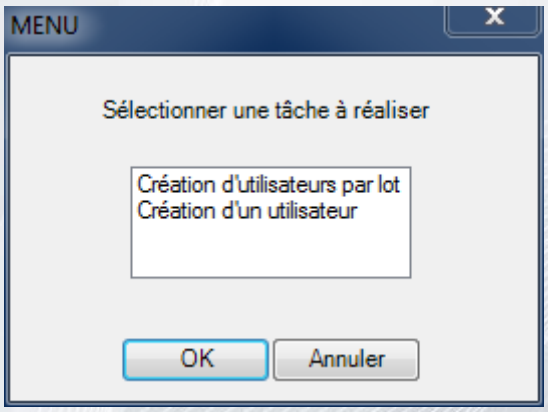
```powershell
# Importation des modules Active Directory et Microsoft Powershell Security
Import-Module ActiveDirectory
Import-Module Microsoft.PowerShell.Security

# Création des OU
New-ADOrganizationalUnit -Name CYC -Path "dc=dijon,dc=cyc,dc=fr"
New-ADOrganizationalUnit -Name Serveurs -Path "dc=dijon,dc=cyc,dc=fr"
New-ADOrganizationalUnit -Name Groupes -Path "dc=dijon,dc=cyc,dc=fr"

New-ADOrganizationalUnit -Name Services -Path "ou=CYC,dc=dijon,dc=cyc,dc=fr"

New-ADOrganizationalUnit -Name Direction -Path "ou=Services,ou=CYC,dc=dijon,dc=cyc,dc=fr"
New-ADOrganizationalUnit -Name Ordinateurs -Path "ou=Direction,ou=Services,ou=CYC,dc=dijon,dc=cyc,dc=fr"
New-ADOrganizationalUnit -Name Utilisateurs -Path "ou=Direction,ou=Services,ou=CYC,dc=dijon,dc=cyc,dc=fr"

New-ADOrganizationalUnit -Name Informatique -Path "ou=Services,ou=CYC,dc=dijon,dc=cyc,dc=fr"
New-ADOrganizationalUnit -Name Ordinateurs -Path "ou=Informatique,ou=Services,ou=CYC,dc=dijon,dc=cyc,dc=fr"
New-ADOrganizationalUnit -Name Utilisateurs -Path "ou=Informatique,ou=Services,ou=CYC,dc=dijon,dc=cyc,dc=fr"

New-ADOrganizationalUnit -Name Administratif -Path "ou=Services,ou=CYC,dc=dijon,dc=cyc,dc=fr"
New-ADOrganizationalUnit -Name Ordinateurs -Path "ou=Administratif,ou=Services,ou=CYC,dc=dijon,dc=cyc,dc=fr"
New-ADOrganizationalUnit -Name Utilisateurs -Path "ou=Administratif,ou=Services,ou=CYC,dc=dijon,dc=cyc,dc=fr"

New-ADOrganizationalUnit -Name Old -Path "ou=Services,ou=CYC,dc=dijon,dc=cyc,dc=fr"
New-ADOrganizationalUnit -Name Ordinateurs -Path "ou=Old,ou=Services,ou=CYC,dc=dijon,dc=cyc,dc=fr"
New-ADOrganizationalUnit -Name Utilisateurs -Path "ou=Old,ou=Services,ou=CYC,dc=dijon,dc=cyc,dc=fr"

New-ADOrganizationalUnit -Name Custom -Path "ou=Services,ou=CYC,dc=dijon,dc=cyc,dc=fr"
New-ADOrganizationalUnit -Name Ordinateurs -Path "ou=Custom,ou=Services,ou=CYC,dc=dijon,dc=cyc,dc=fr"
New-ADOrganizationalUnit -Name Utilisateurs -Path "ou=Custom,ou=Services,ou=CYC,dc=dijon,dc=cyc,dc=fr"

# Création des groupes
New-ADGroup -Name GG_Direction -GroupScope Global -GroupCategory Security -Path "ou=Groupes,dc=dijon,dc=cyc,dc=fr"
New-ADGroup -Name GG_Informatique -GroupScope Global -GroupCategory Security -Path "ou=Groupes,dc=dijon,dc=cyc,dc=fr"
New-ADGroup -Name GG_Administratif -GroupScope Global -GroupCategory Security -Path "ou=Groupes,dc=dijon,dc=cyc,dc=fr"
New-ADGroup -Name GG_Old -GroupScope Global -GroupCategory Security -Path "ou=Groupes,dc=dijon,dc=cyc,dc=fr"
New-ADGroup -Name GG_Custom -GroupScope Global -GroupCategory Security -Path "ou=Groupes,dc=dijon,dc=cyc,dc=fr"
```

Script PowerShell de création d'OU et de Groupes

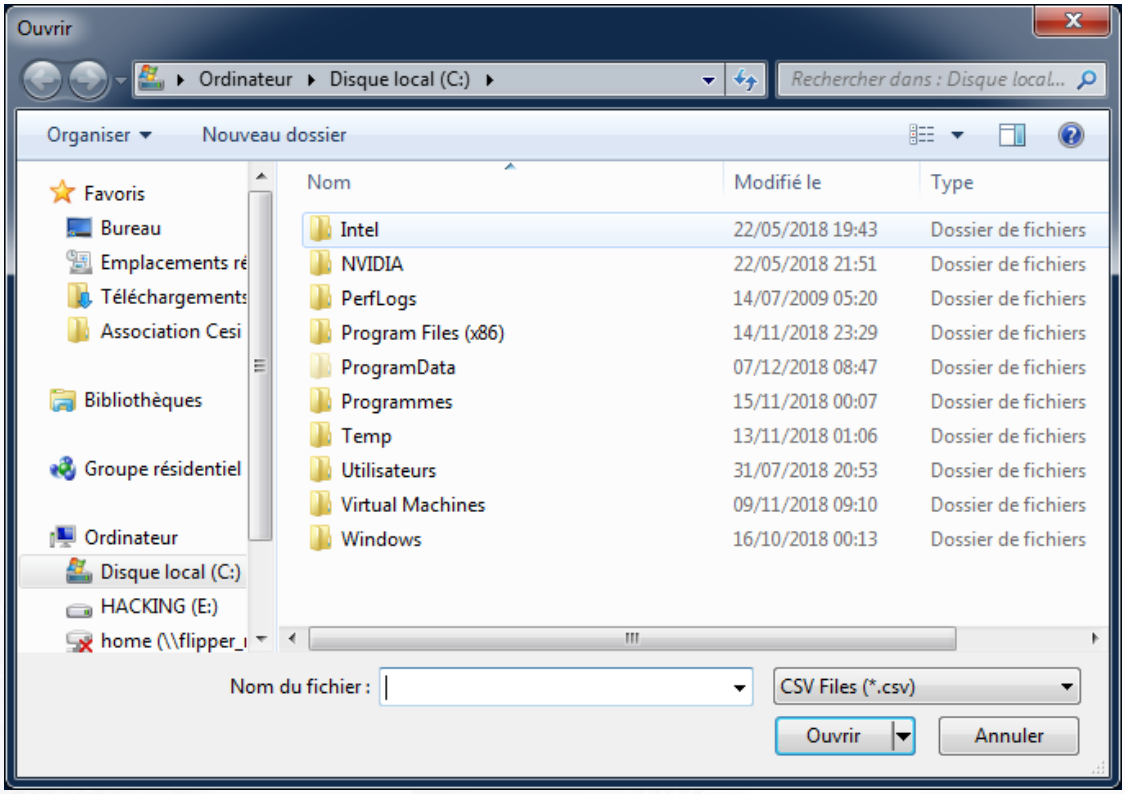
Pour permettre une meilleure administration dans l'Active Directory, un deuxième script PowerShell a été créé. Il permet soit d'intégrer plusieurs utilisateurs avec un fichier CSV, soit de créer un nouvel utilisateur en entrant les différents champs proposés.

Une interface graphique a été implémentée dans le script pour que la gestion soit administrée par une personne n'ayant pas de connaissance en PowerShell.

Dans un premier temps, un menu est proposé pour choisir la tâche à réaliser :

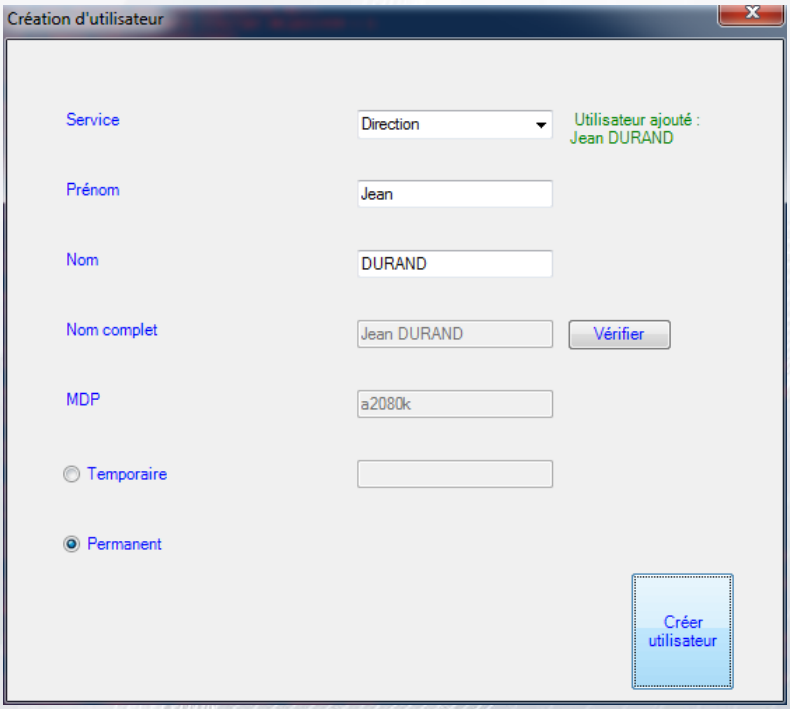


Pour la création d'utilisateurs par lot, un fichier csv sera demandé.



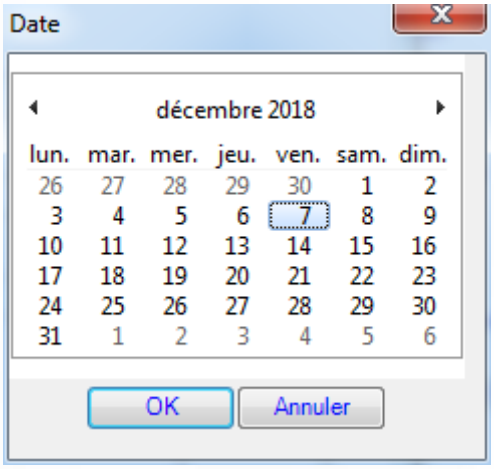
Une fois le fichier sélectionné, la création des utilisateurs sera effectuée automatiquement.

Pour la création d'un nouvel utilisateur, une fenêtre s'ouvre permettant de remplir les différents champs.



Nous pouvons vérifier si l'utilisateur est déjà dans l'AD à l'aide du bouton « Vérifier ».

S'il s'agit d'un utilisateur ayant une date de fin de contrat le bouton « Temporaire » affichera un calendrier afin de sélectionner une date de fin de contrat.



4. DNS

A. Définition

Domain Name System (Système de noms de domaine)

Le rôle DNS permet la correspondance entre un nom de domaine et une adresse IP.

Ex. : WINDHCP.dijon.cyc.fr = 192.168.10.252

Un nom de domaine se décompose en trois parties et se finit par un point.

Chaque partie, séparée par un point, est appelée Label et l'ensemble des labels constitue un FQDN : Fully Qualified Domain Name

Dans l'exemple « WINDHCP.dijon.cyc.fr »

« .fr » est le TLD : Top Level Domain (Domaine de premier niveau).

Il existe des TLD nationaux (fr, it, de, au, etc.) et les TLD génériques (com, org, biz, etc.)

« cyc.fr » est le SLD : Second-Level Domain (Domaine de deuxième niveau).

C'est un sous-domaine d'un domaine de premier niveau.

« dijon. » est appelé hôte, elle correspond à une machine ou une entité sur le réseau.

- ✓ Une zone de recherche directe se base sur la résolution de noms vers une adresse IP.
- ✓ Une zone de recherche inversée s'appuie sur l'adresse IP pour résoudre le nom.

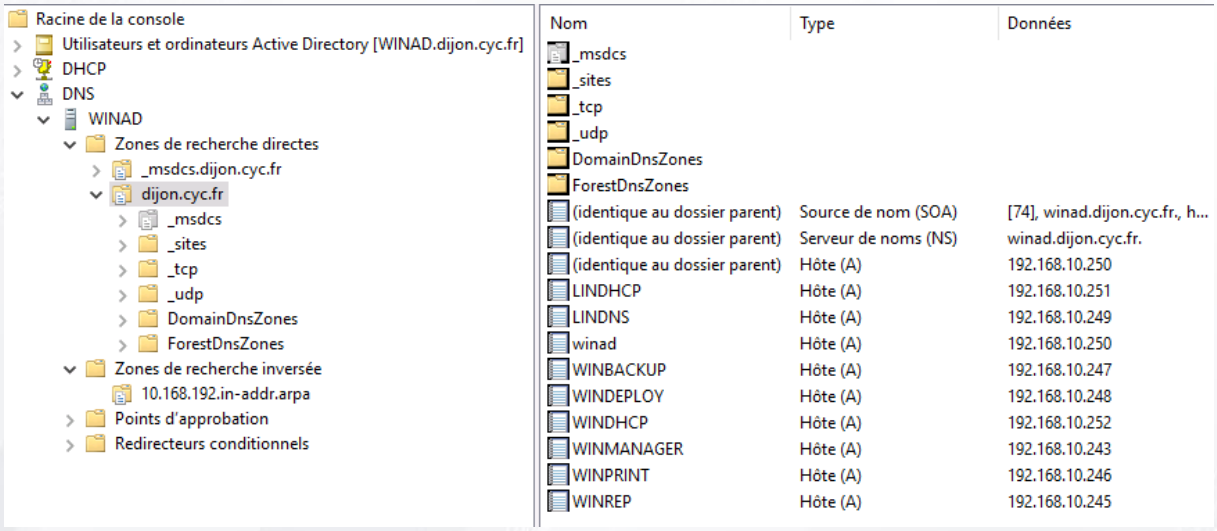
B. Serveurs Windows et Linux

La zone primaire du DNS est installée sur le serveur Windows 'WINDNS' avec un contrôleur de domaine nommé « dijon.cyc.fr ». Le DNS primaire est le premier serveur que le poste informatique va interroger pour connaitre l'adresse IP associée à un nom. Si le poste n'arrive pas à contacter le DNS primaire, il essayera alors de joindre le secondaire.

Pour assurer le bon fonctionnement du serveur Windows en cas de défaillance, nous installons une zone secondaire du DNS sur un serveur Linux.

Lors d'une panne du serveur Windows, le serveur Linux prend automatiquement le relais et n'entraîne aucune perte d'exploitation. Un serveur DNS secondaire est une sauvegarde (backup) de ce serveur DNS primaire. Les données qui se trouvent sur le serveur secondaire sont les mêmes que celles sur le serveur DNS primaire.

Sur le serveur Windows, nous renseignons les adresses des différents serveurs dans la zone de recherche directes et inversée.



Zones de recherches sur le serveur DNS

Sur le serveur Linux 'LINDNS', nous installons « bind9 » pour avoir le service DNS et « openssh-server » pour pouvoir configurer notre serveur à distance.

Nous configurons le serveur Linux comme la procédure se trouvant en annexe.

La réplication d'un serveur DNS Windows sous Linux, se justifie par la gratuité et la faible consommation d'un système Linux. C'est une solution qui semble peu utilisée mais c'est une équipe qui fonctionne et permet d'assurer la continuité d'un service indispensable pour communiquer. Si le serveur primaire tombe, le secondaire prend le relais mais ne communique pas les nouvelles données acquises à son serveur maître. Il est donc nécessaire de rétablir rapidement le fonctionnement du serveur DNS primaire qui est le seul capable de mettre à jour le cache sur le serveur secondaire.

5. DHCP

A. Définition

Dynamic Host Configuration Protocol (Protocole de configuration dynamique des hôtes)

Le rôle DHCP permet de distribuer dynamiquement des adresses IP à tout appareil qui se connecte sur le réseau en lui attribuant :

- ✓ Une adresse IP unique
- ✓ Un masque de sous-réseau qui est le même pour tous les hôtes du réseau
- ✓ Une adresse DNS pour pouvoir résoudre les noms d'hôtes
- ✓ L'adresse de la passerelle qui permet de se sortir du LAN et ainsi de se connecter à l'extérieur du réseau

B. Serveurs Windows et Linux

Afin d'avoir une tolérance aux pannes et de faire cohabiter les deux environnements sur le parc informatique, nous avons décidé de distribuer des adresses IP différentes selon les serveurs.

Le serveur Windows 'WINDHCP' distribuera une plage d'adresses pour chaque service, tandis que le serveur Linux 'LINDHCP' attribuera des adresses IP différentes sur le même réseau.

Cela nous permet d'avoir simultanément un DHCP Windows et un DHCP Linux sur le même réseau en évitant les conflits d'adressage.

Nous avons prévu une plage d'adresses assez grande sur chaque serveur. En cas de panne d'un des deux serveurs, l'autre pourrait prendre le relais aisément.

Les adresses IP seront distribuées de la manière suivante :

Catégorie	Plage d'adresse IPV4 Windows	Passerelle	Masque de sous-réseaux	Plage d'adresse IPV4 Linux
Equipement réseau	192.168.20.1 à 192.168.20.100	192.168.10.254	255.255.255.0	192.168.20.101 à 192.168.20.201
Service Informatique	192.168.30.1 à 192.168.30.100	192.168.10.254	255.255.255.0	192.168.30.101 à 192.168.30.201
Service Direction	192.168.40.1 à 192.168.40.100	192.168.10.254	255.255.255.0	192.168.40.101 à 192.168.40.201
Service Old	192.168.50.1 à 192.168.50.100	192.168.10.254	255.255.255.0	192.168.50.101 à 192.168.50.201
Service Custom	192.168.60.1 à 192.168.60.100	192.168.10.254	255.255.255.0	192.168.60.101 à 192.168.60.201
Imprimantes	192.168.70.1 à 192.168.70.100	192.168.10.254	255.255.255.0	192.168.70.101 à 192.168.70.201
Wifi	192.168.80.1 à 192.168.80.100	192.168.10.254	255.255.255.0	192.168.80.101 à 192.168.80.201

Plages d'adressage IP dédiées par VLAN

6. Impression

Le serveur d'impression est installé sous Windows 'WINPRINT' en attribuant le rôle Serveur d'impression et numérisation de documents.

Les pilotes des différentes imprimantes sont installés sur le serveur. Les copieurs sont dans un VLAN dédié (70) avec leurs adresses IP correspondantes.

Elles sont ensuite ajoutées sur le serveur d'impression grâce au port tcp/ip puis on les ajoute à l'annuaire.

Afin d'imprimer des plans créer sous Blender et tous les autres documents standards, nous louons un copieurs multifonctions RICOH par bâtiment. Pour les données sensibles il est possible de prévoir des imprimantes laser ou jet d'encre suivant l'utilité.

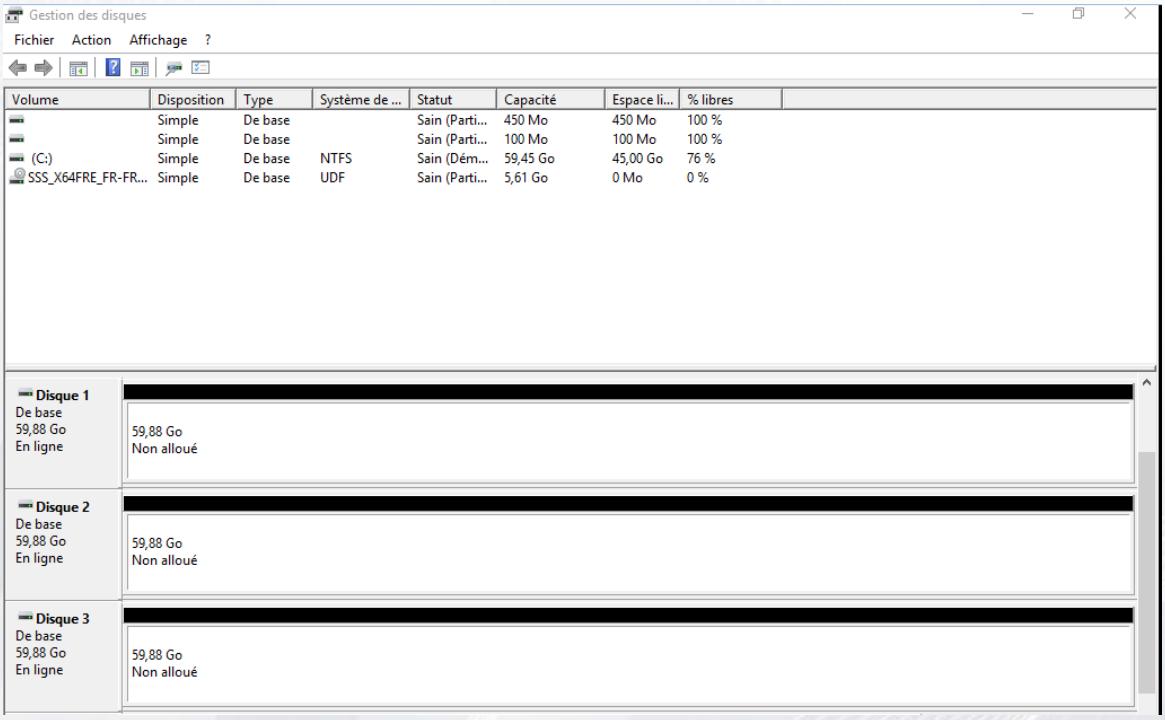
Les copieurs seront ensuite déployés sur les postes grâce à une GPO.

7. Sauvegarde

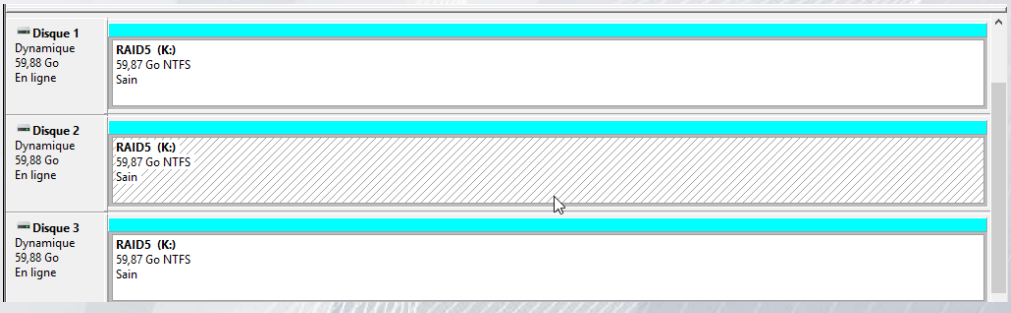
A. *Configuration RAID 5*

Le serveur Backup et les serveurs productions sont montés en RAID 5 :

Ex : Trois disques (dans notre maquette 60Go)



On configure le RAID 5 sur les trois disques afin d'avoir une sécurité en cas de dysfonctionnement d'un disque.



Nous choisissons un RAID 5 parce que nous estimons que cela nous apporte une sécurité suffisante pour nos données, le RAID 6 pourrait être envisagé mais cela augmenterait significativement le budget (un disque dur supplémentaire).

B. *Serveur Backup*

Nous installons le logiciel Veeam Backup & Replication.

Grâce au logiciel il est possible de faire des « Snapshots » de nos machines virtuelles et ainsi faire une copie sur disques ou sur bandes.

En production, nous effectuerons un Snapshot de toutes les machines virtuelles toutes les trois heures lors de la journée de travail.

Chaque soir après 19h nous effectuerons une mise sur bandes de la dernière sauvegarde de la journée afin de pouvoir récupérer ces bandes le lendemain matin en même temps que nos tâches quotidiennes de supervision.

8. Serveur de fichiers

Ce service permet de centraliser l'espace de stockage de différents utilisateurs sur un même serveur dédié. Cet accès à plusieurs dossiers peu importe leur localisation sur le réseau sera disponible sur chaque poste grâce à l'authentification de l'utilisateur. Il permet l'équilibrage des charges et la tolérance aux pannes si un serveur n'est pas disponible, l'autre prend le relais pour l'accès au dossier. Pour se faire, on crée un groupe de serveurs de réplication, la réplication permettra la synchronisation entre chaque membres et toutes modifications sur un dossier sera immédiatement répercutée sur l'autre.

Afin d'optimiser la réplication et la bande passante durant la journée, nous effectuerons une planification de réplication sur jour ouvrés de 21H30 à 00H00.

Donc nous avons un serveur avec 2 espaces disques : un volume pour le système, et un grand volume de 3 To (E:)

Après configuration du serveur (IP fixe, nom du serveur), nous créons des dossiers partagés sur le volume E.

Nous créons un dossier par service, les droits de modification, lecture et exécution seront attribuer par rapport au groupe de l'Active Directory.

9. Déploiement

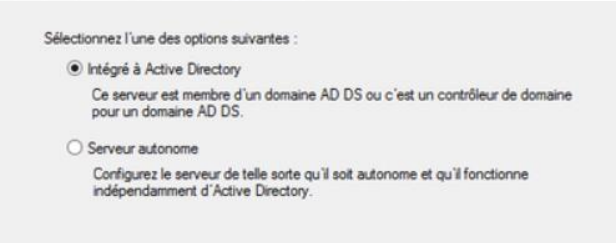
A. *MDT WDS*

Le serveur de déploiement est installé sur 'WINDEPLOY'. Nous l'installons sur Windows Server 2016 avec interface graphique car le rôle utilisé pour le déploiement n'est pas inclus en mode Core.

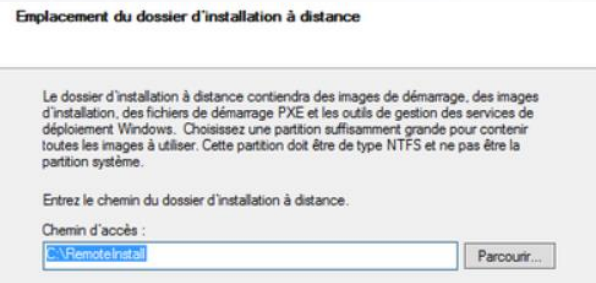
WDS (Windows Deployment Services)

Le rôle Services de déploiement Windows est installé sur le serveur, ce qui permet de déployer des images sur le réseau.

Pour la configuration, il faut lui renseigner qu'il fait partie d'un domaine avec un AD en sélectionnant « Intégré à l'Active Directory »



Choisir l'emplacement où seront stockés les images de boot et les fichiers qui permettront le boot PXE.



MDT (Microsoft Deployment Toolkit)

Dans un premier temps, nous installons « Windows ADK », outils de déploiement et Windows PE.

Ensuite nous installons MDT 2016 sur le serveur afin de créer nos masters à déployer sur les postes clients.

B. Pc Clients

Un script PowerShell mappera des lecteurs réseaux à chaque connexion sur un poste informatique. Ces lecteurs permettent d'accéder aux dossiers partagés :

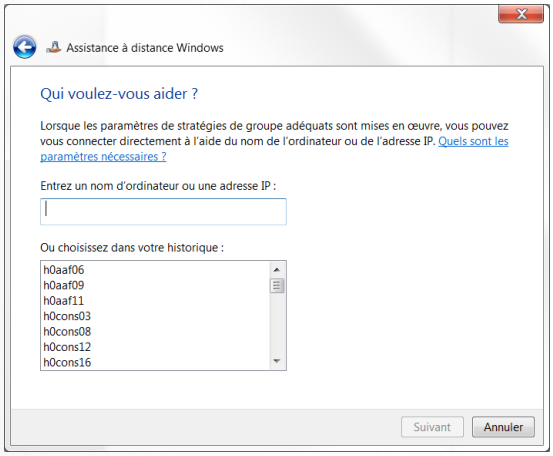
- ✓ Un dossier en fonction du service : Groupe Direction ;
  Groupe Informatique ;
  Groupe Administratif ;
  Groupe Old ;
  Groupe Custom ;
- ✓ Un répertoire personnel qui est dédié à chaque utilisateur avec quota de 20Go, ce dernier sera le seul à y avoir accès.
- ✓ Un dossier « Tout_le_monde » commun à tous les employés.

```powershell
# Chemins des lecteurs réseaux
$Direction = "\\WINREP\Direction"
$Administratif = "\\WINREP\Administratif"
$Informatique = "\\WINREP\Informatique"
$Old = "\\WINREP\Old"
$Custom = "\\WINREP\Custom"
$Tml = "\\WINREP\Tout_le_monde"
$Users = "\\WINREP\Users"

# Déconnexion des lecteurs : S=Service T=Tout_le_monde U=Utilisateur
Remove-PSDrive S -Force
Remove-PSDrive T -Force
Remove-PSDrive U -Force

# Mappage du lecteur réseau Tout le monde
New-PSDrive -Name T -Root $Tml -PSProvider FileSystem -Persist

# Mappage des lecteurs réseaux en fontion du service
# Récuperation des groupes auquel appartient l'utilisateur
$ID = ([Security.Principal.WindowsIdentity]::GetCurrent())
$Groupes = $ID.Groups | foreach-object {
 $_.Translate([Security.Principal.NTAccount])
}
if ($Groupes -contains $env:USERDOMAIN + "\" + "GG_Direction") {
 New-PSDrive -Name S -Root $Direction -PSProvider FileSystem -Persist
}
if ($Groupes -contains $env:USERDOMAIN + "\" + "GG_Administratif") {
 New-PSDrive -Name S -Root $Administratif -PSProvider FileSystem -Persist
}
if ($Groupes -contains $env:USERDOMAIN + "\" + "GG_Informatique") {
 New-PSDrive -Name S -Root $Informatique -PSProvider FileSystem -Persist
}
if ($Groupes -contains $env:USERDOMAIN + "\" + "GG_Old") {
 New-PSDrive -Name S -Root $Old -PSProvider FileSystem -Persist
}
if ($Groupes -contains $env:USERDOMAIN + "\" + "GG_Custom") {
 New-PSDrive -Name S -Root $Custom -PSProvider FileSystem -Persist
}

# Chemin du dossier Utilisateur
$UserShare = $Users + "\" + $env:UserName

# Nom de domaine + Nom de l'utilisateur
$Domuser = $env:USERDOMAIN + "\" + $env:UserName
# Ajout du controle totale à l'utilisateur
# (Nom du compte, Droits d'accès, Héritage enfant, Propagation ACE uniquement aux enfants, Autorise l'accès)
$UserAccess=New-Object security.AccessControl.FileSystemAccessRule($Domuser,"FullControl",1,2,"Allow")

$UserAcl=Get-Acl -Path $UserShare
$UserAcl.addAccessRule($UserAccess)

Set-Acl -Path $UserShare $UserAcl
```

L'espace commun « Tout_le_monde » sera vidé et archivé tous les jours à 19h00 grâce à une tâche planifiée qui exécutera un script PowerShell. Ces archives seront conservées 3 semaines dans un dossier nommé « Sauvegarde » puis détruites automatiquement.

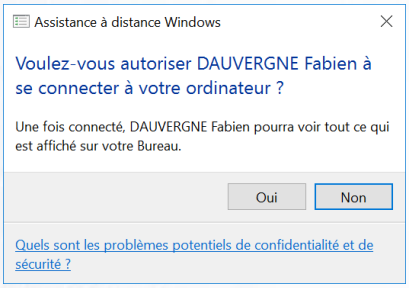
```powershell
#Chemin de la sauvegarde
$Path = "\\WINREP\Tout_le_monde"
#Date du jour au format jour.mois.année
$fileName = Get-Date -format dd.MM.yyyy

#Création du dossier avec la date du jour
New-Item -Name "Backup - $fileName" -ItemType directory -Path $Path -Force | Out-Null
#Déplacer le contenu du dossier commun dans le dossier "Sauvegarde"
Move-Item -Path "\\WINREP\Tout_le_monde\*" -Destination "\\WINREP\Sauvegarde\Backup - $fileName" -Force | Out-Null

#Chemin des fichiers de logs
$LogFilePath = "\\WINREP\Sauvegarde\Logs"
#Liste les éléments présents dans le dossier
$items = Get-ChildItem $Path
#Date de moins de 3 semaines
$DaysToCheck = (Get-Date).AddDays(-22)

#Création du fichier texte des Fichiers supprimés
$fileLog = $LogFilePath + "Fichiers supprimés.txt"

#Compare si la date de création du dossier et supérieur à 3 semaines
#Si c'est le cas, suppression du dossier et génération de logs
foreach ($item in $items) {
    if($item.GetType().Name -eq "DirectoryInfo") {

        $fileCreationTime = $item.CreationTime

        if($fileCreationTime -lt $DaysToCheck) {
            Remove-Item -Path $item.FullName -Recurse -Force
            Write-Output "Fichier supprimé : $($item.FullName)" | Out-File $fileLog -Append
        }
    }
}
```

Afin d'aider l'utilisateur le plus rapidement possible, un technicien informatique peut envoyer une assistance à distance. Cette demande d'aide doit être validé par l'utilisateur une première fois pour pouvoir visualiser l'écran distant, puis une deuxième pour interagir avec l'utilisateur.

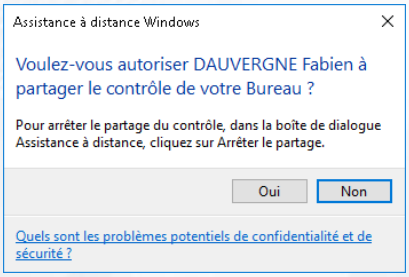


Nous lançons l'assistance grâce à la commande :

C:\Windows\System32\msra.exe /offerRA



Sur l'écran distant une fenêtre apparait afin de valider la demande par l'utilisateur.



Une fois la demande validée, une deuxième fenêtre apparait pour demander le contrôle à distance.

C. Master

Choix logiciel :

Gimp et blender sont les application métier disponible pour un système d'exploitation Microsoft, donc obligatoire. Ils seront intégrés au master client Windows 10.

Mozilla Firefox pour le navigateur internet.

Adobe Acrobat Reader pour la lecture des PDF.

La suite Office sera installée avec des comptes offices 365 comprenant :

- ✓ Un traitement de texte (WORD)
- ✓ Un tableur (EXCEL)
- ✓ Un client de messagerie (OUTLOOK)
- ✓ Un logiciel de visioconférence (SKYPE ENTERPRISE)

D. Politique de sécurité (GPO)

Les GPO (Group Policy Object) ou stratégies de groupe permettent la gestion des ordinateurs et des utilisateurs dans un environnement Active Directory. Elles peuvent agir notamment sur des clés de registre, les droits NTFS, la politique de sécurité et d'audit, l'installation de logiciel, les scripts de connexion et de déconnexion ou encore la connexion de lecteur réseau.

Les GPO peuvent être appliquées par OU, ou groupe, ou par utilisateur de l'Active Directory.

Pour les imprimantes multifonctions nous créons dans l'AD un groupe par matériel (par zone géographique).

Par exemple dans le groupe « IMP copieur Aile Nord » nous appliquerons la stratégie suivante :

Ajout de l'imprimante copieur Aile Nord dans les préférences utilisateurs. Nous appliquerons cette GPO une seule fois.

- GPO communes à tous :

  - Supprimer l'application ajouter ou supprimer des programmes
  - Paramétrage de l'écran de veille à 10 min
  - Empêcher l'accès aux outils pouvant modifier la base de registre
  - Autoriser l'accès à distance avec demande par l'utilisateur
  - Effacer l'historique des programmes récemment ouvert
  - Faire de www.google.fr, la page d'accueil par défaut d'Internet Explorer
  - Mappage de l'imprimante commune à tous
  - Autoriser les scripts PowerShell à s'exécuter sur les postes clients

- GPO de sécurité :

  - Longueur du mot de passe 8 caractères minimum et devra respecter les critères de complexité
  - Durée maximale du mot de passe 60 jours
  - Durée minimale du mot de passe 30 jour
  - Nombre de mots de passe gardés en mémoire 3

VI. Coût du projet

Ci-dessous le tableau récapitulatif du cout d'investissement nécessaire pour la réalisation initial du projet :

	Prix unitaire	Nombre	Description	Prix total
Réseaux				
C2960L-24TS	600,00 €	5	Commutateur Access (4+1)	3 000,00 €
C2960L-8TS	350,00 €	1	Commutateur Gardien	350,00 €
C9200L-24T-4X	3 000,00 €	2	Core de réseau	6 000,00 €
Cisco Aironet 1850 Series Access Points	250,00 €	4	Accès Wifi avec alimentation externe	1 000,00 €
Licences				
W2016 Datacenter	6 000,00 €	2	Pour serveur production	12 000,00 €
Cal	35,00 €	100	Un par utilisateur	3 500,00 €
W2016 serveur standard	800,00 €	1	Pour serveur Backup	800,00 €
Serveurs				
Armoire 24	500,00 €	1	Stockage salle serveur (Rack)	500,00 €
HPE ProLiant DL325 Gen10 7401P	8 800,00 €	2	24 cœurs 32 Go double alimentation 2 carte réseaux 10Gb/s Data : 3To	17 600,00 €
HPE ProLiant DL325 Gen10 7251	4 000,00 €	1	16 cœurs 16 Go double alimentation Data : 3To	4 000,00 €
HPE StoreEver LTO-7 Ultrium 15000	4 300,00 €	1	Débit écriture 300Mo/s	4 300,00 €
Cassette LTO7	75,00 €	20	Capacité 15To	1 500,00 €
Onduleur 2 U	1 200,00 €	2	2200VA ; 230V	2 400,00 €
Pare-feu				
Sophos G230	4 000,00 €	2	Pare-feu	8 000,00 €
Licence	2 000,00 €	1	Pare-feu	2 000,00 €
Installation	1 000,00 €	1	Pare-feu	1 000,00 €
Total				**67 950,00 €**

Ci-dessous le tableau récapitulatif du coût de fonctionnement annuel :

Services	Par mois	Par années	Nombre	Total
Location PC	70,00 €	840,00 €	100	84 000,00 €
Office 365	8,80 €	105,60 €	100	10 560,00 €
Veaam		600,00 €	1	600,00 €
Copieur multifonction	80,00 €	960,00 €	4	3 840,00 €
Total	**158,80 €**	**2 505,60 €**		**99 000,00 €**

VII. Conclusion

Les décisions successives présentées dans ce projet permet de répondre au cahier des charges. Nous assurons des postes de travail suffisamment performant pour l'utilisation des logiciels métiers de nos utilisateurs, ainsi qu'une connectivité au serveur fiable. Le risque de panne est relativement bas, nous offrons une haute disponibilité au serveur DHCP, DNS, AD et fichier. Le système de sauvegarde données prévient d'une éventuelle perte de données. Les scripts permettent une automatisation et un gain de temps significatif pour l'administration des serveurs de ficher et ADDS. Quant au budget, il est peu élevé lors de la mise en place de la nouvelle infrastructure, malgré le cout fonctionnel important cela permet d'économiser des ressources humaines du services informatique. En effet il suffit d'un seul technicien pour maintenir le parc une fois installé.