

CUSTOMIZE



PROJET
EVOLUTION



YOUR

CAR





<https://www.cyc.com>

Table des matières

A- INTRODUCTION	2
A.1 Contexte	2
A.2 Cahier des charges	2
B – AXES DE DEVELOPPEMENT	3
B.1 Carte conceptuelle.....	3
B.2 Planning.....	4
C – HOMOGENEITE DE L'ESPACE DE TRAVAIL	5
D- ARCHITECTURE DU RESEAU	8
D.1 Accès à Internet.....	8
D.2 Topologie du réseau	8
D.3 Interconnexion	9
D.4 Stratégie d'adressage IP	12
D.5 Anticipation des risques	14
E- CHOIX DU MATERIEL RESEAU	16
F- SYSTEMES D'HYPERVISION ET DE SUPERVISION	18
F.1 Hypervision et virtualisation	18
F.2 Installation de la solution d'hypervision	19
F.3 Supervision	20
G- SERVEURS VIRTUALISES	22
G.1 Distributions Windows et GNU/Linux	22
G.2 Serveurs DNS	23
G.3 Serveurs DHCP.....	23
G.4 Serveur Active Directory	25
G.5 Serveur d'impression	26
G.6 Sauvegarde.....	27
G.7 Profil d'évolution du réseau	28



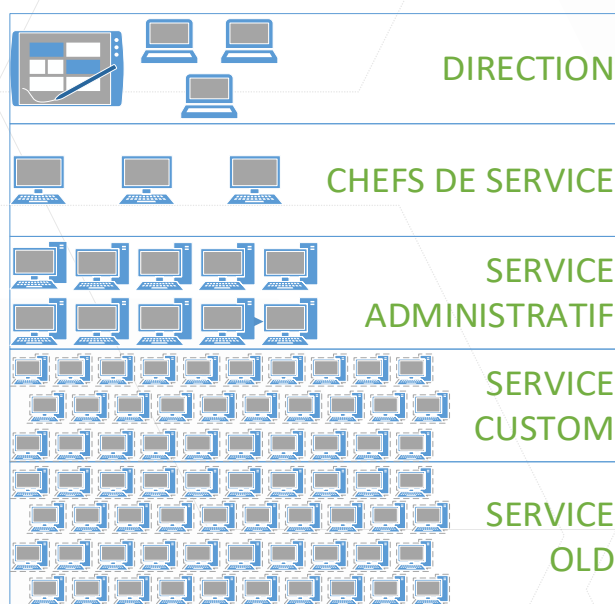
A- Introduction

A.1 Contexte

Recrutés récemment au sein de la société Customize Your Car pour rénover le système d'information de la structure, nous sommes en charge de simplifier les échanges entre les différents services de la société fonctionnant aujourd'hui par échanges sur support externe.

L'entreprise se décompose en 5 services qui sont les suivants :

- Service Direction (1 tablette Apple, 3 portables HP Spectre sous Windows 7)
- Service Chefs de services (3 portables HP Spectre sous noyau Linux)
- Service Administratif (10 postes fixes Dell Optiplex sous Windows 7)
- Service Old (40 portables Dell sous noyau Linux)
- Service Custom (30 portables Dell sous noyau Linux)



Légende		
Liste du matériel en utilisation		
Symbole	Total	Description
	1	Tablette Apple OS X
	3	HP Spectre Portable Windows 7
	3	HP Spectre Portable GNU/Linux
	10	Dell Optiplex Fixe Windows 7
	70	Ordinateur Portable Dell GNU/Linux

A.2 Cahier des charges

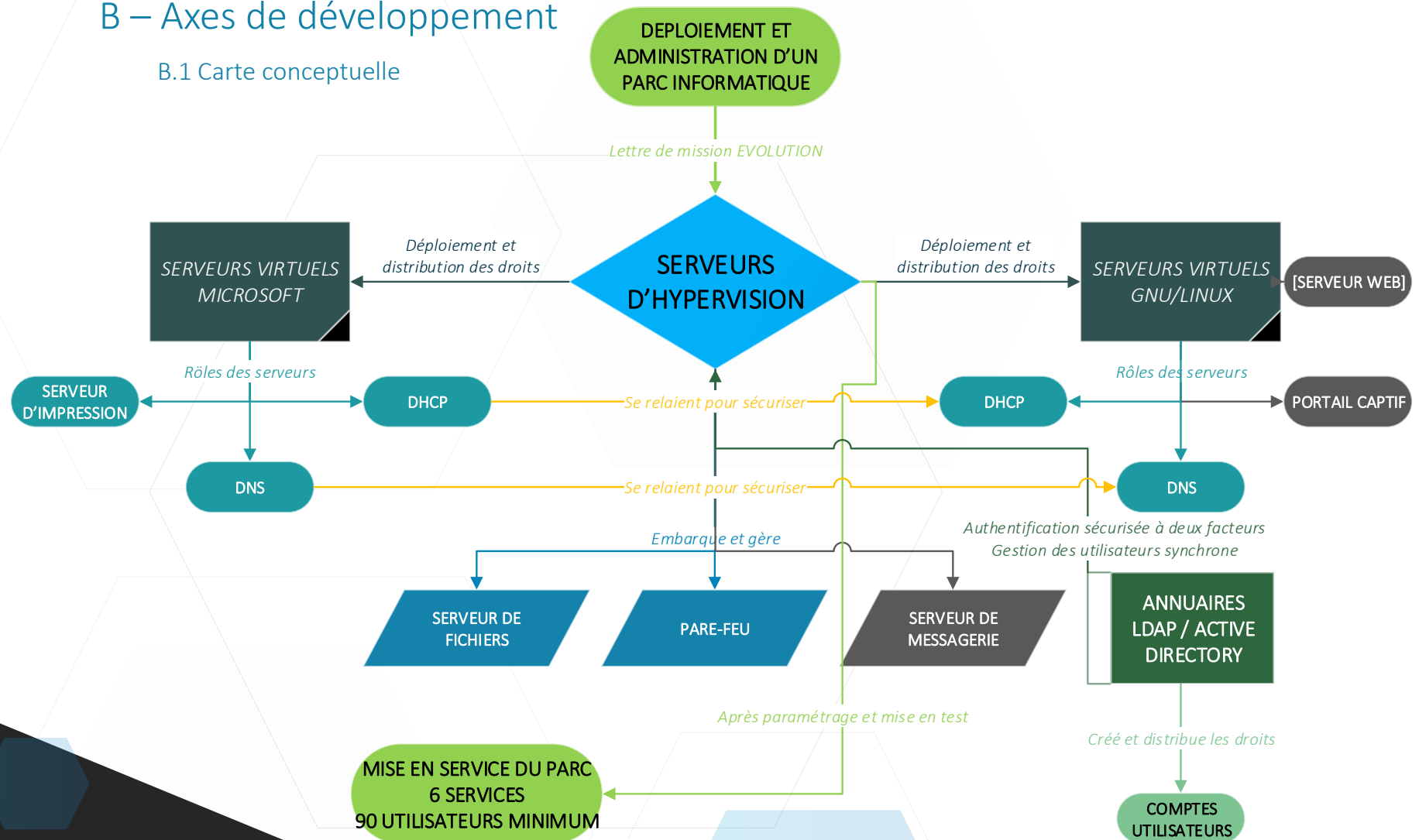
Lors de la réception de notre lettre de mission (Réf. [H.1 Lettre de mission](#)), il nous a été confié de valider les points suivants :

- Déployer un système d'information faisant cohabiter des serveurs DNS et DHCP Windows et GNU/Linux
- Garantir que ces serveurs puissent se relayer en cas de chute d'un d'entre eux
- Assurer au personnel de la société un espace de stockage sur le réseau
- Offrir un espace de partage sécurisé pour les salariés
- Mettre à disposition une solution de gestion des impressions via le réseau
- Garantir l'intégrité des données stockées ou transitant sur le réseau en assurant leur sauvegarde
- S'assurer de la supervision des solutions matérielles et systèmes mises en place



B – Axes de développement

B.1 Carte conceptuelle



B.2 Planning

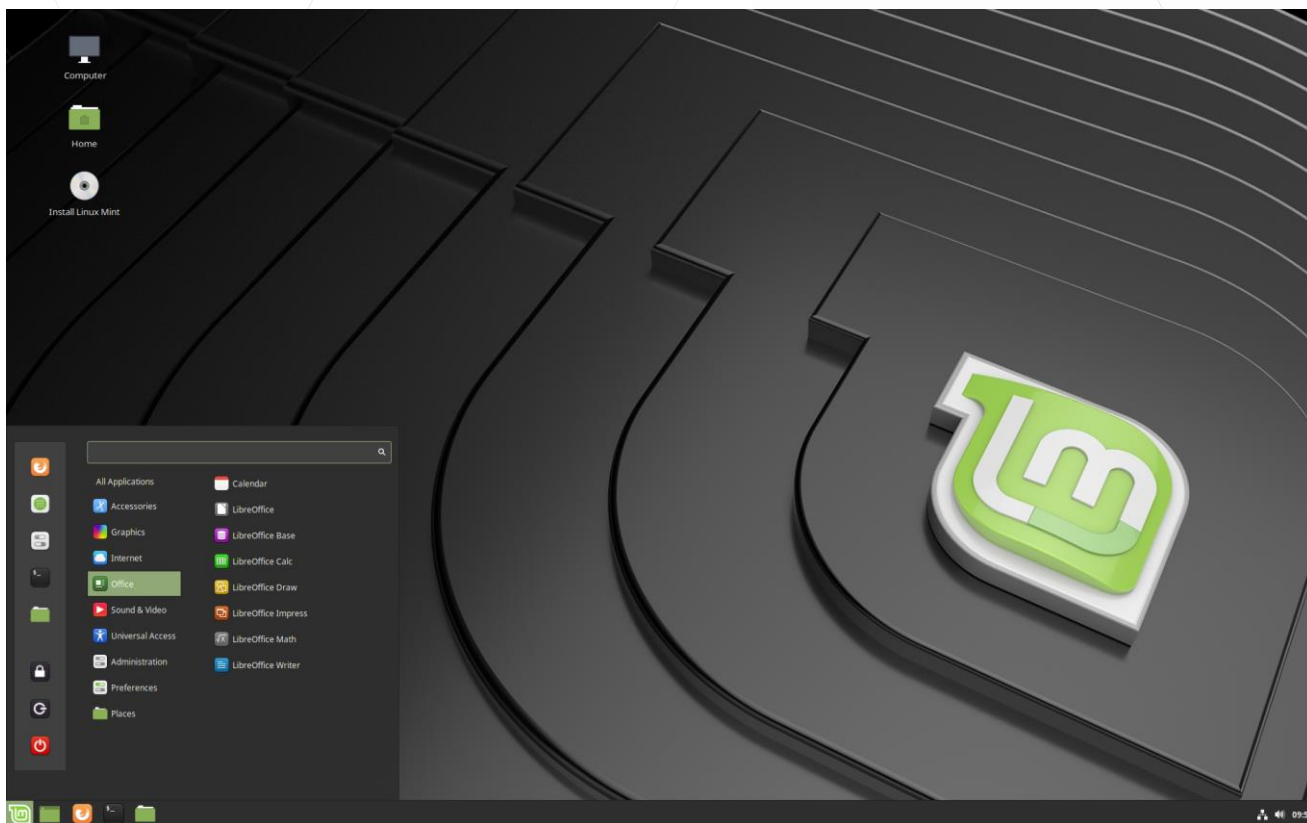
I - CONNEXION INTERNET		KOUVTANOVICH CORENTIN	
ADSL, VDSL ou FIBRE	VDSL + Fibre	OK	Orange + Numéricable
II - ARCHITECTURE RESEAU		KOUVTANOVICH CORENTIN	
Choix d'architecture ?	Maillé + Etoile	OK	Cœur maillé / Terminaisons étoile
Plan d'adressage ?		OK	
Plan générale ?	Répartition des locaux techniques	OK	
Plan des baies ?	Sous Visio	OK	
Supervision réseaux et des éléments actif ?	Obligatoire	OK	Hpe iLo
III - DHCP		HAUTEVELLE NATHAN	
Hardware ou software ?	Software	OK	
Procédure Linux	PFSense	OK	
Procédure Windows		OK	
IV - DNS		KOUVTANOVICH CORENTIN	
Hardware ou software ?	Software	OK	
Procédure Linux	PFSense	OK	
Procédure Windows		OK	
V - SYSTÈME D'INFORMATION		KOUVTANOVICH CORENTIN	HAUTEVELLE NATHAN
Postes de supervision	Hpe iLo + Accès distant	OK	
Solutions logiciel		OK	LibreOffice, Discord
Topologie du système	Sur 2 plans : Cable et Wifi	OK	
VI - SERVEURS		KOUVTANOVICH CORENTIN	HAUTEVELLE NATHAN
Hardware ou software ?	Hyperviseurs physiques / Système Niveau 1	OK	Solution Proxmox
Gestion du RAID ?	A prendre en charge	OK	Ceph - OSD + Pools
Gestion SMART ?	A prendre en charge	OK	Carte intégrée serveur + HDD SAS + Ceph
ActiveDirectory ?	Nécessité pour gérer les droits	OK	AD + LDAP
VII - PC CLIENTS		KOUVTANOVICH CORENTIN	
Remplacement ?	Non	OK	Passage système GNU/Linux
Attribution de l'espace de 20G ?		OK	
Espace Communs à tous les users ?		OK	
VIII - PARE-FEU + FLUX D'ECHANGE		KOUVTANOVICH CORENTIN	
Hardware ou software ?	Intégré à Proxmox	OK	3 couches d'action intégrées
Schéma d'échange		A finaliser	
IX - GESTION DES IMPRESSIONS		HAUTEVELLE NATHAN	
Oui ? Non ?	Serveur d'impression GUI gere par prestataire	OK	Prestataire certifie par Hpe
X - BACKUP		HAUTEVELLE NATHAN	
Système de Backup ?	Obligatoire	OK	Script sous Ceph pour serveurs
XI - MAINTENANCE		HAUTEVELLE NATHAN	
Prestation externe ?	Oui pour le hardware	OK	
XII - MAQUETTE		HAUTEVELLE NATHAN	
Packet tracer ?	Cluster non réalisable sous PT / Simplification	OK	
XIII - COUT FINANCIER		KOUVTANOVICH CORENTIN	HAUTEVELLE NATHAN
Bilan Financier ?	Appel d'offre et croisement des prestations	OK	
KOUVTANOVICH CORENTIN		8	
HAUTEVELLE NATHAN		8	



C – Homogénéité de l'espace de travail

Dans le cadre de la standardisation et l'optimisation des communications et des échanges entre les collaborateurs et leurs services, nous avons choisi de procéder à la migration des systèmes Microsoft Windows vers un système d'exploitation GNU/Linux. Ces derniers représentent 80% des systèmes d'exploitation actuellement déployés dans notre structure et s'avèrent être beaucoup plus économes en termes de ressources machine (Par exemple : seulement 1Gb de RAM utilisés contre 4Gb sous Windows pour utiliser une suite bureautique).

Afin de ne pas dépayser les services de Direction et d'Administration, nous avons décidé de leur fournir le système d'exploitation déjà en usage par les agents des services Old et Custom : Linux Mint. La raison de cette généralisation au site tient principalement à son l'interface, proche de celle de Windows (Réf. [H.16 Procédure d'installation de Linux Mint](#))

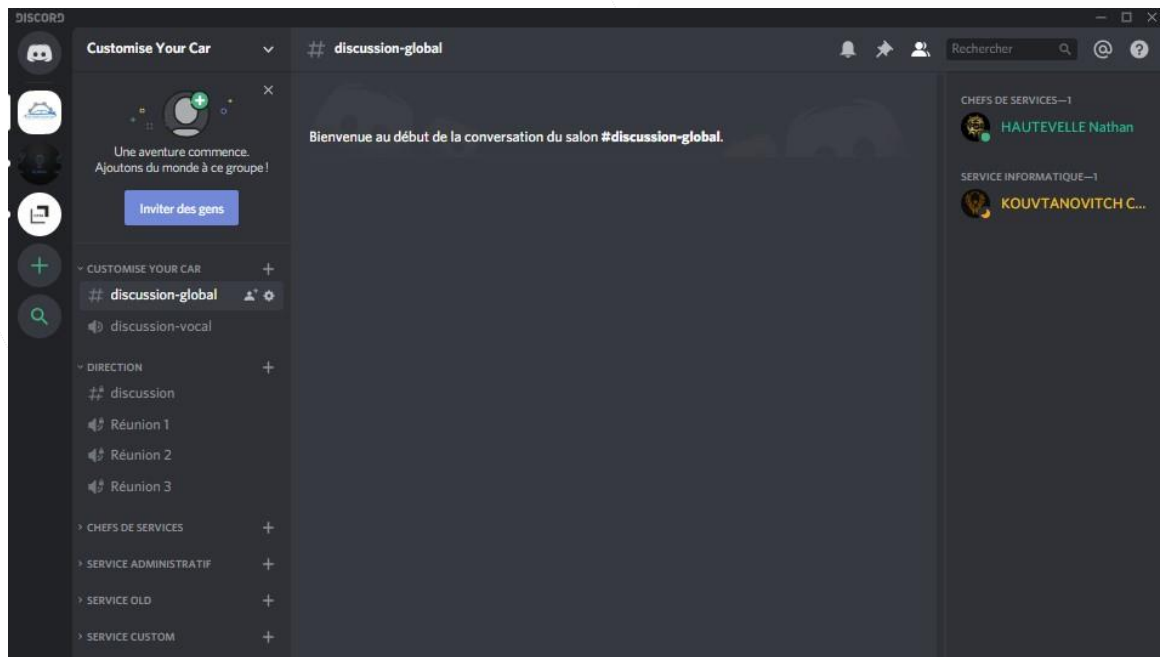


Nous avons aussi pris en considération les problèmes de comptabilité des applications de travail, la suite Microsoft Office du côté des utilisateurs Windows et Libre Office pour les utilisateurs Linux et Mac. Afin de pallier aux problématiques liées à la lecture des documents et à leur mise en forme d'un service à l'autre, nous travaillerons donc désormais avec Libre Office.

Le fonctionnement général de cette suite bureautique est similaire à celui de Microsoft Office sous Windows.

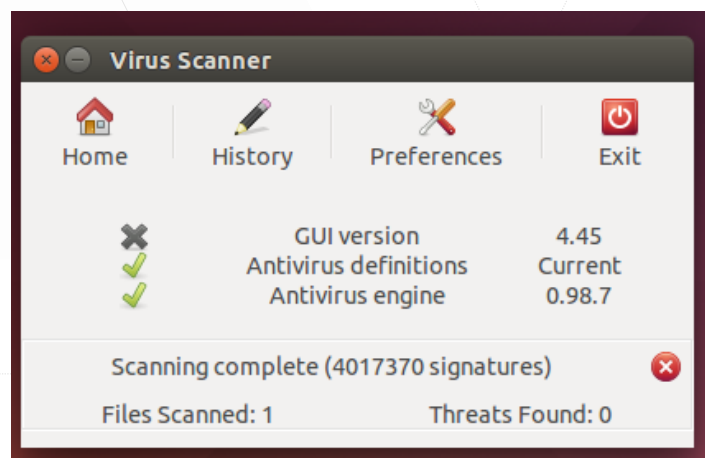
Afin de prévenir toute problématique éventuelle concernant leur utilisation, une période de formation de deux demi-journées sera observée pour les services Direction et Administration. Cette formation sera délivrée en interne par nos soins et pourra être renforcée au quotidien par les échanges de ces services avec nos utilisateurs chevronnés du système (Réf. [H.2 Planning de formation à l'environnement de travail GNU/Linux](#)).

La communication en interne et en externe sera assurée par le logiciel libre Discord, nous offrant les mêmes fonctionnalités que Skype Entreprise (Groupes de conversation et de réunion, vidéo conférence, chat et surtout échanges de fichiers). Le serveur Discord a été paramétré en fonction des différents services/secteurs d'activité de la société :



Les autres logiciels indispensables à nos équipes (Gimp, Blender) fonctionnant déjà en environnement GNU/Linux, aucun autre changement n'est à prévoir à ce stade.

Bien que nous déployions un environnement de travail moins exposé aux risques d'attaque, nous avons tout de même étudié les différentes solutions logicielles antivirus afin de nous assurer d'un risque minimal pour notre réseau.



Notre choix s'est alors arrêté sur ClamAV sur la base des critères suivants :

	ClamAV	RookKit Hunter	BitDefender
Fonctionnement cross platform	Oui	Non	Oui
Conforme POSIX	Oui	Oui	Oui
Mises à jour auto intégrées	Oui	Non	Oui
Scan des archives et fichiers compressés	Oui	Non	Oui
Tarif	Gratuit	Gratuit	250€/an

Hormis la gratuité de cette solution antivirus, deux critères ont particulièrement retenu notre attention. Tout d'abord, ClamAV fonctionne sur tous les systèmes d'exploitation et peut être paramétré à la fois par la console ou par une interface graphique.

Ensuite, ClamAV permet de scanner les menaces éventuelles contenues dans toute forme de fichier compressé ou compilé.

D- Architecture du réseau

D.1 Accès à Internet

Afin de nous assurer une disponibilité réseau optimale (HA) ainsi qu'une forte tolérance aux pannes (FT) ; nous avons choisi de nous engager auprès de deux fournisseurs d'accès Internet différents :

- Numericable pour une connexion fibre ultra haut débit
- Orange pour une connexion VDSL très haut débit

De ce fait, en cas d'interruption des services par l'un des fournisseurs d'accès, la société peut maintenir sa production via le réseau du second opérateur.

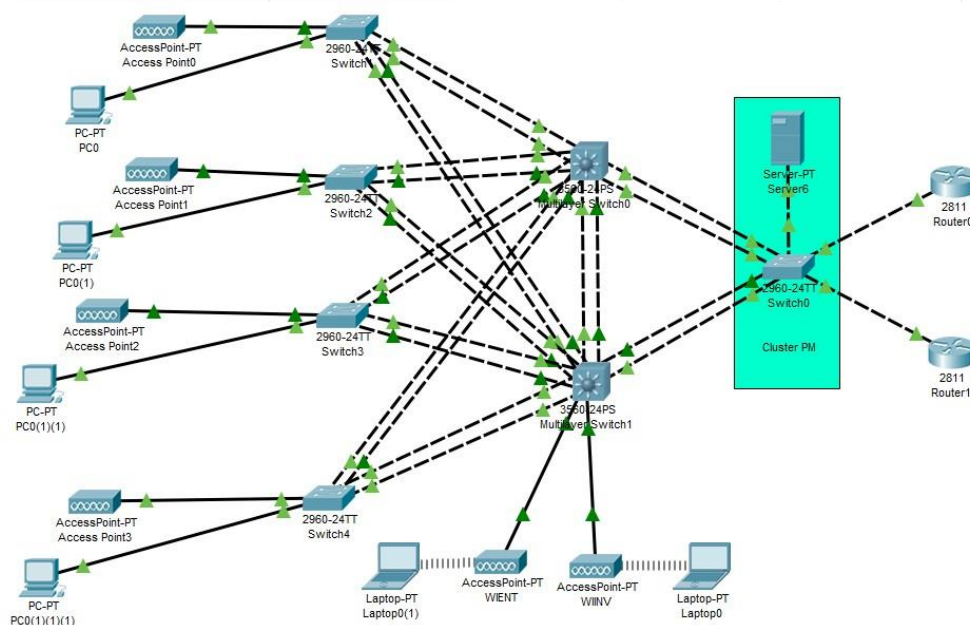
De plus, si l'un des deux circuits d'acheminement du réseau (Fibre ou VDSL) venait à être coupé ; lors de travaux de voirie par exemple ; la société pourra maintenir son niveau de service.

L'acheminement de la connexion sur la totalité de notre réseau sera assuré par des câbles Ethernet de catégorie 6a.

Enfin, dans le cadre de l'optimisation du débit entre notre réseau local et l'Internet, nous opérons à l'agrégation de la connexion de nos deux fournisseurs d'accès grâce à un routeur (Réf. [D.5 Anticipation des risques](#)).

D.2 Topologie du réseau

Au-delà de ces premiers éléments, nous avons adopté une topologie maillée en étoile dont la distribution du réseau est assurée par des commutateurs paramétrables HPe, au nombre de 7. Le schéma ci-dessous fait abstraction du nombre de serveurs en présence dans le cluster. En effet, Packet Tracer ne dispose pas de suffisamment d'options pour nous permettre d'illustrer l'architecture exacte que nous avons décidé de mettre en place.



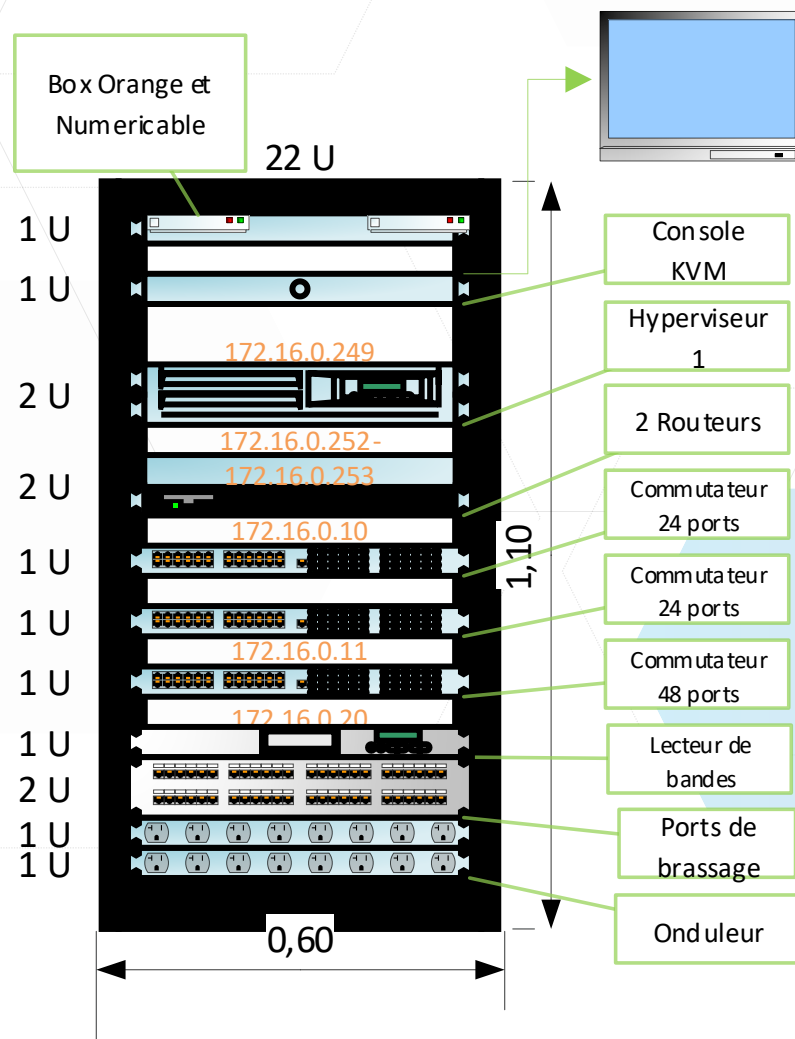
Au centre du réseau se trouve un cluster formé par nos trois serveurs hyperviseurs montés en redondance. Le stockage, la gestion du domaine, la distribution des adresses sur le réseau ainsi que les services d'impression y seront concentrés. La structure du noyau de notre réseau permettra donc, en cas de panne d'un de nos appareils de maintenir le niveau de service de la société. Cette dernière élimine donc les risques de perte de données, de connexion ou d'un des différents services, notamment, celui d'authentification.

Enfin, la majorité du parc informatique étant constituée d'ordinateurs portables ou appareils de type "mobiles", nous nous sommes aussi assurés de diffuser la connexion sur la totalité du site, via un réseau Wi-Fi, à l'aide de 5 points d'accès sans-fil HPe.

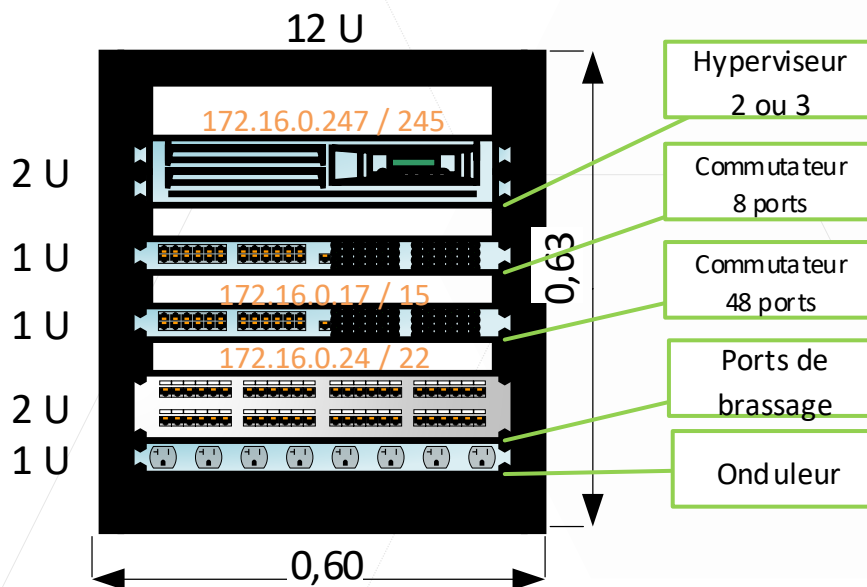
D.3 Interconnexion

Au sein du bâtiment principal se trouvera notre salle serveur principale ; respectant les normes d'installation (Réf. [H.3 Normes d'installation de salle réseau](#)) ; comportant un nœud de notre cluster ; les routeurs de nos opérateurs ; notre routeur permettant l'agrégation de liens ; notre console de management ainsi que le commutateur distribuant le réseau pour le bâtiment.

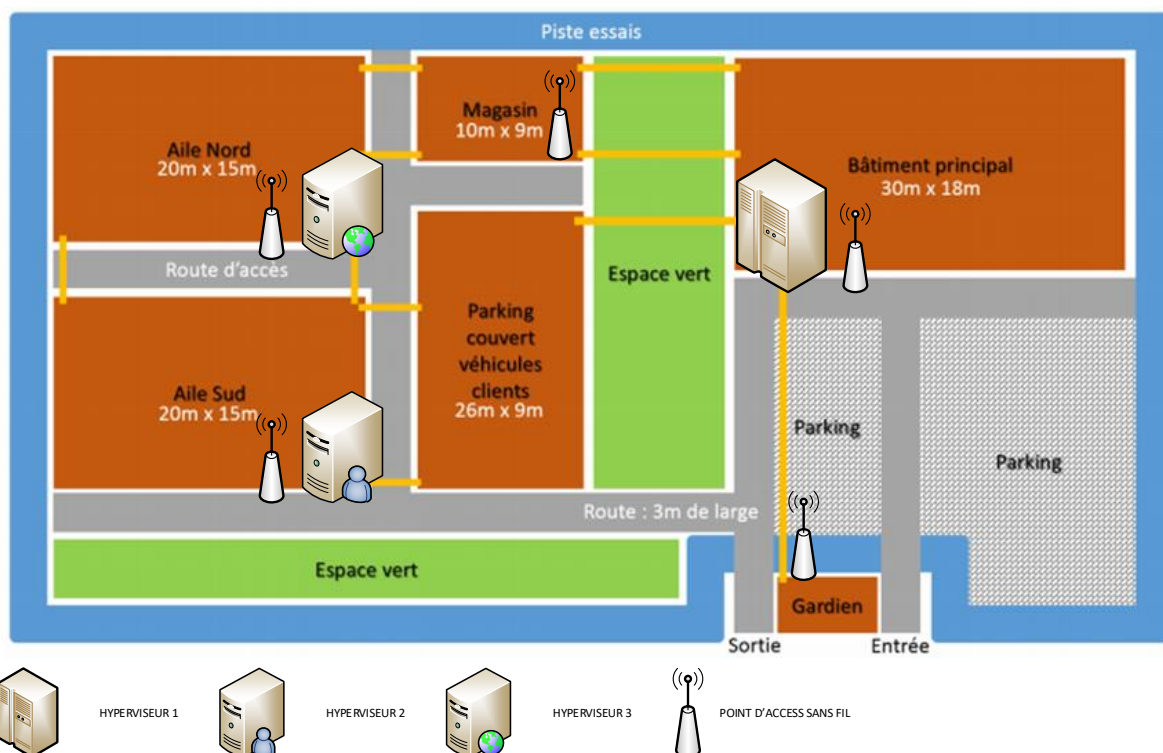
L'ensemble de ces équipements sera alors coffré dans une baie serveur de 22U ; suffisamment grande pour accueillir en tout confort un ajout futur d'équipement.



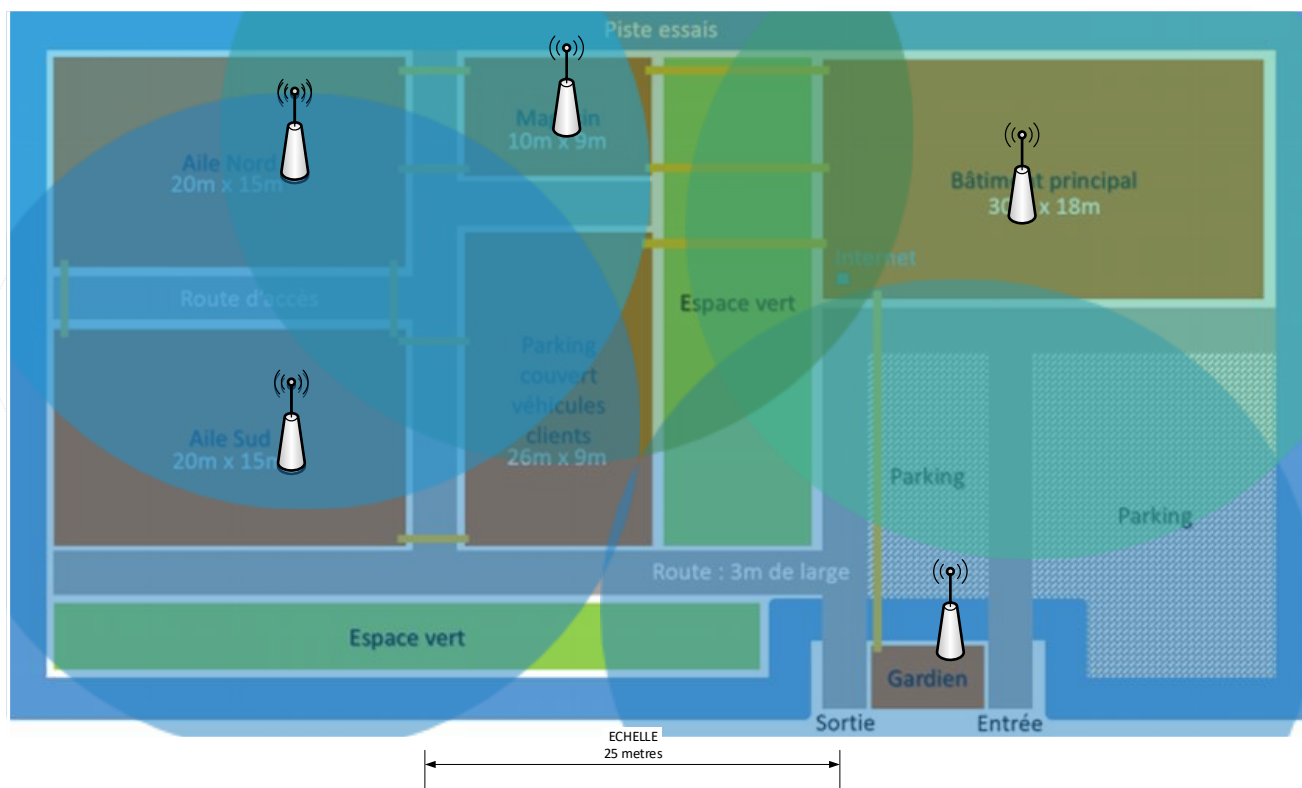
Nos deux autres nœuds (hyperviseurs) se situeront dans deux salles serveurs secondaires respectivement situées dans les ailes Nord et Sud. Elles sont accompagnées pour chacune d'elle d'un commutateur redistribuant le réseau dans les locaux concernés. Chacun de ces pôles est intégré à une baie réseau de taille plus restreinte comptant 12U.



Par conséquent, la répartition de nos locaux techniques est réalisée de la manière suivante :



Notre réseau câblé ne couvrant pas la totalité de l'espace d'activité de la société, nous avons alors réparti nos 5 points d'accès sans fil aux différents points stratégiques comme suit :



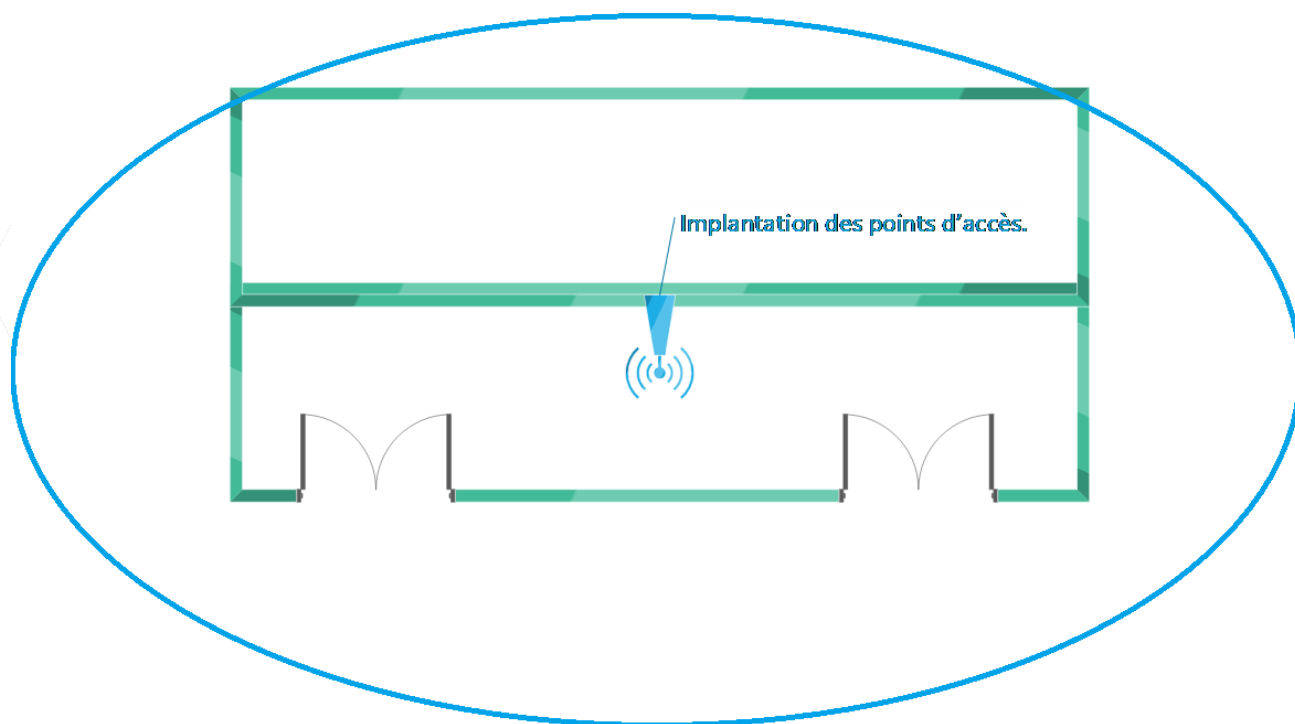
La portée théorique sans obstacle des points d'accès que nous avons choisi pour le réseau est de 100m. En considérant que ces dispositifs sont installés en intérieur et qu'un parking se trouve au cœur de notre site, nous avons considéré une portée efficace de nos bornes de 40m.

La communication étant indispensable entre tous les collaborateurs, un des points de distribution du réseau sans fil a été positionné dans la guérite d'accès à notre parking. Cela leur permettra de réaliser les devis en direct depuis les véhicules clients sans à devoir rejoindre les ports brassés dans les locaux.

Ce dispositif, bien qu'utile, n'est pas indispensable aux collaborateurs pour assurer leurs tâches au quotidien. Par conséquent, il a été décidé de ne pas créer de redondance au niveau du réseau sans fil (Aucune borne supplémentaire dans les bâtiments).

En cas d'incident, les collaborateurs bénéficieront toujours des points d'accès câblés de nos locaux et une intervention du service informatique sera menée pour rétablir le réseau sans-fil.

Enfin, nous avons veillé à positionner les bornes au plafond du rez-de-chaussée de nos bâtiments afin d'assurer une distribution efficace du réseau sans-fil :



Afin d'éviter toute perturbation sur le réseau liée à la superposition des canaux, nous avons placé chaque antenne des points d'accès sur des canaux différents (Ces derniers vont de 1 à 13 en considération du fait qu'aucun autre réseau Wifi ne se trouve aux alentours).

D.4 Stratégie d'adressage IP

Dans le but de limiter l'encombrement du réseau et les connexions non contrôlées sur ce dernier, nous avons choisi de l'inscrire dans des VLAN.

Les VLAN (Virtual LAN) consistent en des réseaux logiques indépendants pouvant coexister. L'utilisation des réseaux locaux virtuels réside dans :

- L'optimisation de la bande passante sur un réseau
- La segmentation des domaines de broadcast et la séparation des flux
- L'isolation des ensembles logiques vis-à-vis des réseaux externes. Seul le routage de ces réseaux logiques permettra alors de communiquer entre ces derniers

Pour plus de sécurité, nous avons procédé à la désactivation du VLAN par défaut, à savoir, le VLAN 1.

Afin de simplifier le contrôle des échanges sur notre réseau, nous avons alors choisi d'isoler les branches suivantes dans des VLAN spécifiques :

Identité du VLAN	Cible
VLAN 10	Réseau entrant du Cluster
VLAN 20	Réseau Ethernet local
VLAN 30	Réseau Wi-Fi Entreprise 2.4 GHz
VLAN 40	Réseau Wi-Fi Invité 5.0 GHz

Suite à la fragmentation de notre réseau, nous avons pu établir le plan d'adressage de ce dernier comme suit (La notation [x] renvoi aux initiales des bâtiments d'implantation du matériel) :

Matériel – Nom réseau	Début de plage	Fin de plage	Masque de sous-réseau - /CIDR	Adresse de broadcast
Routeur Orange – RTO	172.16.0.252		255.255.0.0 - /16	172.16.255.255
Routeur Numéricable – RTN	172.16.0.253		255.255.0.0 - /16	172.16.255.255
Routeur Interne - RTI	172.16.0.254		255.255.0.0 - /16	172.16.255.255
Hyperviseur 1 – SRVPM1	172.16.0.248	172.16.0.249	255.255.0.0 - /16	172.16.255.255
Hyperviseur 2 – SRVPM2	172.16.0.246	172.16.0.247	255.255.0.0 - /16	172.16.255.255
Hyperviseur 3 – SRVPM3	172.16.0.244	172.16.0.245	255.255.0.0 - /16	172.16.255.255
Adresses d'administration (iLo, Web interfaces...)	172.16.0.200	172.16.0.243	255.255.0.0 - /16	172.16.255.255
Serveur virtualisé Windows GUI – SRVGADS	172.16.0.103		255.255.0.0 - /16	172.16.255.255

Serveur virtualisé Windows – SRVADHNS	172.16.0.102		255.255.0.0 - /16	172.16.255.255
Serveur virtualisé GNU/Linux sécurité - SRVPF	172.16.0.100	172.16.0.101	255.255.0.0 - /16	172.16.255.255
Points d'accès sans fil – WFI[x] / WFE[x]	172.16.0.30	172.16.0.49	255.255.0.0 - /16	172.16.255.255
Imprimantes – PRNTR[x]	172.16.0.50	172.16.0.69	255.255.0.0 - /16	172.16.255.255
Switchs – SWD[x]	172.16.0.10	172.16.0.29	255.255.0.0 - /16	172.16.255.255
Plages de sécurité	172.16.0.1	172.16.0.9	255.255.0.0 - /16	172.16.255.255
	172.16.0.70	172.16.0.99	255.255.0.0 - /16	172.16.255.255
	172.16.0.104	172.16.0.199	255.255.0.0 - /16	172.16.255.255
Plage DHCP GNU/Linux	172.16.1.10	172.16.1.254	255.255.0.0 - /16	172.16.255.255
Plage DHCP Windows	172.16.2.10	172.16.2.254	255.255.0.0 - /16	172.16.255.255

D.5 Anticipation des risques

La forte redondance appliquée à notre réseau compense les risques importants pesant sur notre infrastructure.

En effet, en cas de pics de diffusion sur le réseau, le flux d'information peut habituellement conduire à la création de tempêtes de broadcast, la perte de données ou bien l'inscription de plusieurs copies d'une seule et même trame (Couche OSI n°2 – Réf. [H.5 Modèles OSI et TCP/IP](#)).

La redondance que nous avons mis en place réduit énormément ce risque.

Afin de renforcer l'efficacité de nos échanges sur le réseau, nous avons choisi de doubler nos raccords physiques entre nos serveurs.

Communément appelée Etherchannel par le fabricant Cisco ; cette pratique normée IEEE 802.3ad est un protocole consistant à créer un raccord logique sur la base de deux raccords physiques (Au minimum). Au-delà du renfort de la redondance sur notre réseau, ce protocole nous a permis d'augmenter la bande passante de notre réseau ; agrégeant celle de nos raccords physiques (Réf. [H.6 Protocole LACP](#)). De plus, cette pratique réduit le risque de créer des goulots d'étranglement sur le réseau lorsque certains utilisateurs le sollicitent constamment.

Afin d'assurer ce haut niveau de redondance sur notre réseau, nous avons fait usage des protocoles de spanning-tree pour nos différents VLAN.

Matériel	Ports physiques	VLAN	Protocole	Load-Balancing
Routeur HPe FlexNetwork MSR958 PoE	1-4	10	HSRP	Oui
Serveur HPe Proliant DL380 G7 configuré	1-4	10	HSRP	Oui
Serveur HPe Proliant DL380 G7 configuré	5	10	Access	Non
Commutateur HPe ProCurve 3500yl-48G-POE+	1-12	10, 20, 30, 40	Trunk	Oui
Commutateur HPe ProCurve 3500yl-48G-POE+	13-15	10, 20, 30, 40	Trunk	Non
Commutateur HPe ProCurve 3500yl-48G-POE+	16-48	20	Access	Oui
Commutateur HPe ProCurve 3500yl-24G-POE+	1-4	20, 30, 40	Trunk	Oui
Commutateur HPe ProCurve 3500yl-24G-POE+	5-22	20	Access	Oui
Commutateur HPe ProCurve 3500yl-24G-POE+	23-24	30, 40	Trunk	Oui
Commutateur HPe ProCurve 2530-8G-POE+	1-8	10	HSRP Access	Oui
Console KVM HPe LCD8500	1-3	10	Access	Non
Point d'accès sans fil HPe Aruba AP-303H	1	30, 40	Trunk	Oui



E- Choix du matériel réseau

Dans le cadre du déploiement d'un tel réseau sur le site, la société a besoin d'investir dans les éléments matériels suivants (Réf. [H.4 Détail technique du matériel](#)) :

- 3 serveurs rackables HPe Proliant DL380 G7 2U équipés d'alimentations 750W en redondance, de 2 processeurs Xeon 6 cœurs en 2.93 GHz, 128 Go de RAM, 4 disques SSD de 240 Go de capacité, 12 disques SAS 15K de 1.2 To chacun et 2 cartes Dual Port 10GbE
- 7 commutateurs rackables, manageables et empilables HPe de la gamme 3500yl dont 3 en 48 ports, 2 en 24 ports et 2 de 8 ports
- 2 routeurs HPe FlexNetwork MSR958 PoE de 8 ports
- 5 points d'accès sans fil HPe Aruba AP-303H (RW)
- 3 baies réseaux HPe dont 1 de 22U et 2 de 12U
- 1 tiroir de console de management rackable HPe LCD8500

Nos choix d'investissements se sont portés sur du matériel reconditionné dont le support fabricant vient tout juste d'être stoppé (2018). En effet, le rapport coût/performance des nouvelles générations de matériel serveur présente la nécessité de mobiliser un fort taux de ressources de la société vis-à-vis de notre plan de déploiement :

Élément matériel	Tarif neuf	Tarif reconditionné	Nombre d'unités	Total neuf	Total reconditionné
Serveur HPe Proliant DL380 G7 configuré	4500 €	560 €	3	13500 €	1680 €
Commutateur HPe ProCurve 3500yl-24G-POE+	1980 €	365 €	2	3960 €	1095 €
Commutateur HPe ProCurve 3500yl-48G-POE+	4695 €	540 €	3	14085 €	1620 €
Commutateur HPe ProCurve 2530-8G-POE+	180 €	80 €	2	360 €	160 €
Routeur HPe FlexNetwork MSR958 PoE	1275 €	560 €	2	2550 €	1120 €
Point d'accès sans fil HPe Aruba AP-303H	565 €	70 €	5	2825 €	350 €
Lecteur de bande HPe LTO-5 Ultrium 3000	3000€	400 €	1	3000€	400 €
Baie HPe 22U	700 €	150 €	1	700 €	150 €
Baie HPe 12U	640 €	120 €	2	1280 €	240 €
Console KVM HPe LCD8500 + Kit de rackage et commutateur KVM	2650 €	650 €	1	2650 €	650 €
Licence iLo 3 Advanced	240 €	10 €	3	720 €	30 €
Coût final du matériel			25	45630 €	6495 €

Comme inscrit dans notre tableau d'étude sur la page précédente, une économie de 85% est réalisée lorsque nous faisons appel à des revendeurs de matériel reconditionné certifiés par le fabricant. Il est d'ailleurs à souligner que la "Lifetime Guarantee" nous est transférée lors de l'achat de ce matériel, ce qui nous couvre malgré l'état d'usage du matériel.

HP 3500-24G-PoE YI Switch SN: SG630TF066

[View details](#)

Type	Identifier 	Service type	Start date	End date	Status
Base Warranty	SG630TF066	Wty: HPE Parts Exchange Support	Sep 1, 2006	Aug 31, 2105	Active
		Wty: HPE Support for Initial Setup	Sep 1, 2006	Aug 31, 2105	Active

De plus, bien que le support fabricant ait cessé pour le matériel, la communauté autour de ce matériel est particulièrement active et très peu de sujets ont des probabilités de rester sans réponse. Ainsi, de l'installation physique au changement de pièces en passant par les déploiements serveurs et logiciels, une documentation officielle et/ou communautaire complète existe et peut être consultée gratuitement (Réf. [H.4 Détail technique du matériel](#)).




My products

OR OR Aucun fichier choisi

[How to import my products](#)
[Template \(Max 50 serial number for spreadsheet\)](#)

Search by serial number or Product #

☐ Subscribe all registered products to software update notifications

	Product #	Product Description	Serial #	Friendly name	OpenCase/Support info	Action
	J8692A	HP 3500-24G-PoE yI Switch	SG630TF066	Switch Phoenixia	Open Case Download software Product Support Info	 

Du fait de notre haut niveau de disponibilité réseau, l'utilisation de matériel reconditionné est rendue possible. Si nous avions établi un niveau de disponibilité plus faible, il aurait été plus judicieux de porter les investissements matériels sur du neuf, ce qui augmenterait drastiquement nos coûts.

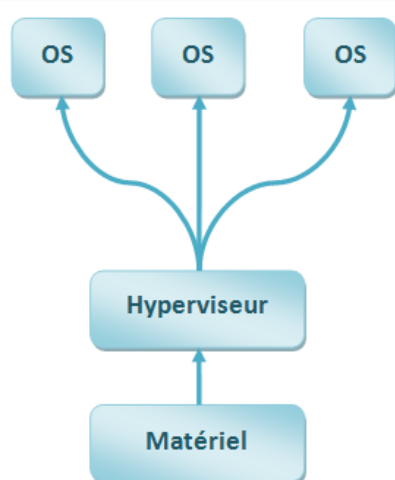
Nous avons par ailleurs contacté plusieurs sociétés certifiées auprès de HPe afin d'assurer la maintenance matérielle ainsi que la gestion de notre système d'impression (Réf. [G.5 Serveur d'impression](#)).



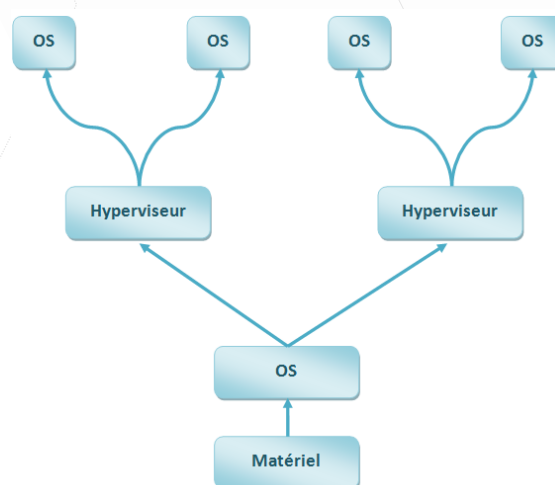
F- Systèmes d'hypervision et de supervision

F.1 Hypervision et virtualisation

Afin de créer le cœur de notre réseau, nous avons choisi de déployer une solution d'hypervision. Ce type de solutions consistent en des plates-formes de virtualisation qui offrent alors la possibilité de faire travailler plusieurs machines (virtuelles) en même temps, sur une seule machine physique. Il en existe aujourd'hui deux types ; les hyperviseurs natifs (Type 1) et les hyperviseurs hébergés (Type 2).



Hyperviseur Type 1



Hyperviseur Type 2

Notre objectif à travers l'adoption d'une solution d'hypervision réside dans la maîtrise des performances et des coûts du déploiement du réseau ; la virtualisation étant une technologie aux avantages certains :

- Un nombre restreint de dépenses en matériel et en surface (Moins de serveurs matériels à acheter, ce qui représente un gain d'espace conséquent)
- Une stabilité accrue du réseau avec un meilleur contrôle sur ce dernier (Moins de risques de failles liées à la multiplication de ports inutilisés, de pertes de données lors des échanges entre serveurs...)
- Une utilisation intelligente des ressources matérielles grâce à la répartition interne des charges de travail entre les différents serveurs virtuels
- Enfin, une économie d'énergie conséquente, la dépense énergétique d'un serveur seul ou d'un hyperviseur étant sensiblement la même lors de leur fonctionnement

Les solutions d'hypervision de Type 1 s'exécutant directement sur le matériel sont par conséquent très légères en termes d'espace de stockage et de performance matérielle.

Nous avons alors procédé à un comparatif des trois solutions d'hypervision de Type 1 les plus stables, suivies et documentées de ces dernières années afin d'adopter la plus efficace d'entre-elles pour la création de notre cœur de réseau.

	Hyper-V	VMWare	ProxMox
Cout de licence	Gratuit	11000 €	Gratuit
Niveau de documentation	Haut niveau éditeur et communautaire	Haut niveau éditeur	Haut niveau éditeur et communautaire
Support de virtualisation	Tous systèmes	Tous systèmes	Tous systèmes
Nested virtualisation	Activation via Powershell	Active	Active
Support éditeur	Gratuit	Gratuit	79 € par an
Pare-feu intégré	Non	Non	Sur 3 niveaux
Gestion du stockage intégré / RAID	Aucun serveur de stockage / RAID gere	Aucun serveur de stockage / RAID gere	Serveur de stockage Ceph / Gestion par pools
Gestion automatique des sauvegardes	Non	Oui	Oui
Gestion des accès par utilisateur	Non	Non	Oui
Outils de supervision intégrés	Oui	Oui	Oui
Serveur mail intégré	Non	Non	Oui
Chiffrement ZFS	Non	Oui	Oui

En dépit de son support payant, la solution d'hypervision ProxMox fait force de nombreux atouts et commençant par sa capacité à prendre en charge tous les environnements de travail ainsi que le nombre de fonctionnalités qu'elle offre en complément de son système de base. De plus, la documentation relative à la solution ProxMox étant extrêmement complète, nous estimons le nombre de contacts avec le support minime.

Enfin, les services de chiffrement des disques et des données, de serveur mail, de pare-feu de gestion du stockage poussés intégrés à la solution nous permettent de centraliser de nombreux services qui auraient engendré des dépenses matérielles et logicielles avec les deux autres solutions.

F.2 Installation de la solution d'hypervision

Afin d'installer notre solution d'hypervision, nous avons au préalable créé une clé USB bootable. Grâce à son environnement visuel, son installation est effectuée en quelques minutes (Réf. [H.7 Installation et configuration de ProxMox](#)).

Après avoir procédé à l'installation de ProxMox sur nos trois serveurs physiques et vérifié que ces derniers soient à jour, nous joignons le réseau de notre hyperviseur et accédons à son interface à l'adresse <https://172.16.0.249:8006> De cette adresse, nous ouvrons le terminal et débutons la création de notre cœur de réseau ; le cluster.

```
pvecm create cycluster
```

A ce stade, nous avons créé notre premier nœud. Il nous faut alors ajouter nos deux autres hyperviseurs à cycluster. Pour cela, nous joignons les adresses de nos serveurs l'une après l'autre et depuis le terminal de ces derniers, exécutons la commande d'ajout au nœud qui est la source de création du cluster.

```
pvecm add 172.16.0.249
```

Notre cluster est alors prêt à accueillir les différents serveurs et services que nous avons prévu de mettre en fonction au cours de la construction de notre réseau.

Après différents tests initiaux ; nous poursuivons le déploiement de notre cœur de réseau en déployant notre service de gestion de stockage, Ceph (Réf. [H.8 Installation et configuration de Ceph](#)).

Au cours du paramétrage de ce dernier, nous séparons nos disques destinés à héberger activement nos serveurs et nos données de ceux qui accueilleront les sauvegardes de la première partie. Pour y parvenir, nous avons, depuis le terminal, sélectionné nos disques cibles pour les faire repérer en tant que Object Storage Device (OSD) avant de les intégrer dans des pools ; des partitions logiques réparties sur nos trois nœuds.

```
pveceph createmon  
ceph osd pool create cycnetworking 64  
ceph osd pool create cycbackup 128
```

Afin d'anticiper tout risque de vol de données par l'intervention éventuelle d'un prestataire externe, nous appliquons alors les premières couches de sécurité à notre cluster en activant le service de chiffrement du système de fichiers ZFS (Réf. [H.9 Configuration du chiffrement ZFS](#)). Ce protocole nous offre l'assurance que toute donnée de notre réseau n'est lisible que sur ce dernier. Ainsi, si un ou plusieurs de nos disques durs sont connectés sur un serveur externe ou que les données sont copiées sur un système de stockage amovible (Type clé USB), ces derniers seront illisibles.

Enfin, nous renforçons la sécurité autour de notre cluster en paramétrant le pare-feu de ProxMox que nous couplons à notre serveur PFSense.

F.3 Supervision

Afin de nous assurer du bon fonctionnement de notre réseau, nous souhaitons garder le contrôle sur les différents mouvements matériels et logiciels sur notre réseau. Pour cela, nous profitons du fait que nos serveurs soient livrés avec leur outil de supervision ; HP iLO Advanced ; l'outil SNMP (Réf. [H.10 Protocole SNMP](#)) sous ProxMox ne nous offrant pas la possibilité d'observer tous les éléments que nous souhaitons sur nos serveurs.

Grâce à cet outil, nous aurons la possibilité de superviser l'état et l'activité sur nos trois hyperviseurs depuis notre console, et en particulier les éléments suivants :

- L'état de fonctionnement des hyperviseurs et des serveurs virtuels
- La température de nos hyperviseurs et l'état du système de refroidissement de ces derniers
- Le niveau d'encombrement du stockage des hyperviseurs et des serveurs virtuels
- Le niveau d'utilisation de la RAM des hyperviseurs et des serveurs virtuels
- Le niveau d'utilisation des CPU
- Le suivi du Event Log

En voici une capture faisant état de la température système d'un des hyperviseurs :

System Information - Temperature Information

Summary | Fans | **Temperatures** | Power | Processors | Memory | NIC Information | Drives

Show values in Fahrenheit

Temp	Location	Status	Reading	Thresholds
01-Inlet Ambient	Ambient	OK	17C	Caution: 42C; Critical: 46C
02-CPU	CPU	OK	50C	Caution: 74C; Critical: 75C
03-P1 DIMM 1-4	Memory	OK	33C	Caution: 87C; Critical: 92C

De plus, en cas de nécessité de redéployer le système de nos hyperviseurs ou de les relancer en cas d'interruption de service ; l'outil HP iLO Advanced nous permet d'effectuer ces actions à distance, depuis les adresses respectives des ports iLO de nos hyperviseurs <https://172.16.0.200/>; <https://172.16.0.201/>; <https://172.16.0.202/> .

Connect Virtual Floppy

Image Inserted: None

Scripted Media URL:

Boot on Next Reset: ☐

Connect CD/DVD-ROM

Image Inserted: None

Scripted Media URL:

Boot on Next Reset: ☐

Eject Media | Force Eject Media | Insert Media

Les adresses des ports iLO auront été paramétrées par nos soins lors du premier démarrage des serveurs comme suit :

Network Configuration

MAC Address: 3c-4a-92-79-17-3a

Network Interface Adapter: ON

Transceiver Speed Autoselect: ON

IP Address: 172.16.0.200

Subnet Mask: 255.255.0.0

Gateway IP Address: 172.16.0.254

[F10]=Save [ESC]=Cancel

Il est possible d'allouer un domaine au port afin de transformer l'adresse du portail d'accès en un format plus "User Friendly", ce que nous souhaitons éviter afin de limiter les possibilités d'intrusion (Soient-elles volontaires ou non).



G- Serveurs virtualisés

G.1 Distributions Windows et GNU/Linux

Notre volonté étant de déployer un réseau durable présentant un minimum de risques (Notamment liés aux failles de sécurité), nous avons choisi comme base pour nos serveurs les systèmes d'exploitation suivants :

- Windows Server 2019 pour nos serveurs Microsoft (Windows Server Nano n'étant plus maintenu par Microsoft bien que plus léger)
- PFSense pour nos serveurs GNU/Linux ; ce dernier système nous offrant tout le support nécessaire pour déployer la totalité des fonctionnalités souhaitées

Afin de ne pas exploiter inutilement les ressources de nos hyperviseurs et limiter les risques d'accès à nos serveurs virtuels, nous avons choisi de déployer la quasi intégralité de nos serveurs virtuels en mode core. Seul notre serveur SRVADSI incluant notre Active Directory secondaire couplé à notre serveur d'impression est déployé en mode GUI (Avec interface graphique).

	Windows Server 2019 GUI	Windows Server 2019 Core	Windows Server Nano	PFSense Server GUI	PFSense Server Core
Espace disque	32GB	28GB	16GB	4GB	
RAM	4GB ECC	800MB ECC	512MB ECC	512MB ECC	
Processeur	1,4GHz 64-bit			600MHz 32/64-bit	
Ports ouverts	20	9	2	2	
Patchs critiques	12	2		0	
Redémarrages	9	6	2	2	
Différence de performance	50%		75%	10%	

De par les performances observables par chacun des systèmes ainsi que le nombre de ports ouverts, un réseau établi uniquement autour des systèmes GNU/Linux aurait été idéal. La lettre de mission nous imposant d'intégrer les services Microsoft au réseau, nous utilisons ces derniers comme serveurs de secours visant à garantir notre qualité de service.

L'accès à nos différents serveurs se réalisera de deux manières différentes dépendant du degré d'intervention requis ; premièrement via l'interface web de nos hyperviseurs et enfin ; en RDP (Connexion Bureau à Distance) sur le serveur déployé en GUI ; ce qui nous offre une gestion centralisée de nos serveurs à différents niveaux. Afin de pouvoir paramétrer nos différents services à distance, nous déployons la solution openssh-server sur nos serveurs GNU/Linux.

G.2 Serveurs DNS

Le rôle DNS (Domain Name System) permet de faire correspondre une adresse IP à un nom de domaine. Dans notre cas, nous pourrions observer la correspondance suivante :

- SRVADHNS.network.cyc.com = 172.16.0.102

Décomposé en trois labels identifiables aux points qui les séparent, cet ensemble constitue un FQDN ; Fully Qualified Domain Name (Réf. [H.11 Structure d'un nom de domaine](#)).

Afin de garantir notre niveau de service en cas de défaillance de nos serveurs Windows ou GNU/Linux ; nous avons choisi de déployer deux zones DNS ; une primaire sur le serveur Windows SRVADHNS et une zone secondaire sur le serveur GNU/Linux SRVDHNSL. Ainsi, en cas d'attaque ou de bug étant orienté sur un seul des deux systèmes d'exploitation de nos serveurs ; seule une partie de nos serveurs s'en trouveront affectés sans que cela impacte les utilisateurs du réseau.

Le DNS primaire sera le premier à être interrogé par les postes des différents utilisateurs présents sur le réseau dans le but de connaître l'adresse IP qui répond à son nom (SRVADHNS.network.cyc.com). Si ce dernier ne répond pas dans le délai imparti ou s'avère défaillant ; les postes des utilisateurs tenteront alors de joindre le DNS secondaire.

Nos différents serveurs s'inscrivent automatiquement dans les zones de recherche directes de nos deux serveurs DNS. Le script de déploiement du service DNS pour le serveur Windows se résume aux commandes suivantes :

```
Install-WindowsFeature DNS -IncludeManagementTools
Add-DnsServerPrimaryZone -name cyc.local -ZoneFile cyc.local.DNS -DynamicUpdate
NonsecureAndSecure
```

En cas d'échec d'ajout des serveurs dans les zones de recherche, la commande suivante peut alors saisi en complément.

```
Add-DnsServerResourceRecordA -Name CYCADHNS -ZoneName cyc.local -AllowUpdateAny -
IPv4Address 172.16.0.2
```

Alors que les services de gestion DNS sont standardisés sous les systèmes serveur Microsoft ; un choix multiple s'est offert à nous pour le déploiement du serveurs DNS en GNU/Linux.

Recherchant à la fois la simplicité et la performance dans l'utilisation, à la fois côté serveur et client ; nous avons pris la décision d'utiliser le service DNS de PFSense sous GNU/Linux qui se présente en tant que dnsmasq (Réf. [H.12 Configuration des serveurs DNS](#)).

Bien que la pratique de sécurisation d'un serveur DNS Windows sous Linux soit rare ; il s'agit tout de même d'une association efficace lorsqu'il s'agit d'assurer la continuité d'un service essentiel et indispensable sur notre réseau.

Si notre serveur DNS primaire venait à tomber, une intervention rapide visant à rétablir ses fonctions sera cependant nécessaire. En effet ; le serveur secondaire n'est pas en capacité de transmettre les données acquises au serveur maître.

G.3 Serveurs DHCP

Le rôle serveur DHCP (Dynamic Host Configuration Protocole) nous permet d'allouer dynamiquement des adresses IP à la totalité des appareils qui se connectent sur un réseau. Cette attribution d'adresse est en réalité plus complexe puisque les appareils qui rejoignent le réseau reçoivent en réalité les quatre attributs suivants :

- Une adresse IP unique (sur le réseau ; il est fort probable qu'un réseau d'une autre société comporte un appareil possédant la même adresse IP)

- Un masque de sous-réseau (Unique pour tous les hôtes présents sur le réseau)
- Une adresse DNS afin d'être en mesure de résoudre les noms d'hôte et joindre nos serveurs
- L'adresse d'une passerelle qui permet de parcourir notre réseau et atteindre l'extérieur du réseau

Nos serveurs DHCP (Windows et GNU/Linux) cohabitent sur notre réseau de la manière qui suit :

	Plage Linux	Plage Windows
Adresses IP	172.16.1.10-254	172.16.2.10-254
Masque de sous-réseau	255.255.0.0	

Ainsi, chacun de nos serveurs peut distribuer librement des adresses aux hôtes sans empiéter sur la plage de distribution de l'autre.

Le script PowerShell suivant fait état des différentes étapes de déploiement de notre service DHCP sous Windows Server 2019 :

- Définition de l'adresse statique du serveur DHCP

```
New-NetIPAddress -IPAddress 172.16.0.102 -InterfaceAlias "Ethernet" -  
DefaultGateway 172.16.0.254 -AddressFamily IPv4 -PrefixLength 16
```

- Définition des adresses DNS

```
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses  
127.0.0.1, 172.16.0.102
```

- Définition du nom du serveur et redémarrage

```
rename-computer SRVADHNS  
restart-computer
```

- Installation du service DHCP

```
Install-WindowsFeature DHCP -IncludeManagementTools
```

- Ajout des groupes de sécurité

```
Netsh dhcp add securitygroups
```

- Redémarrage du service DHCP

```
restart-service dhcpserver
```

Une fois le serveur de domaine déployé sur le réseau, nous intégrons le serveur DHCP à ce dernier via la commande :

```
Add-DhcpServerInDC -DnsName SRVADHNS.cyc.local -IPAddress 172.16.0.102
```

Nous avons par ailleurs prévu des plages d'adresses suffisamment larges sur chacun d'entre eux afin qu'en cas d'interruption des services du côté Windows ou GNU/Linux, nos hôtes puissent toujours bénéficier de l'accès au réseau.

Par exemple, sous Windows Server 2019, nous retrouvons la partie de script suivante :

- Notification au gestionnaire de serveur pour valider et installer la configuration DHCP

```
Set-ItemProperty -Path registry ::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ServerManager\Roles\12 -Name ConfigurationState -Value 2
```

- Ajout de la plage DHCP

```
Add-DhcpServerv4Scope -name 'SRVADHNS' -StartRange 172.16.1.10 -EndRange 172.16.1.254 -SubnetMask 255.255.0.0 -State Active
```

- Ajout du serveur DNS et de la référence routeur par défaut dans le serveur DHCP.

```
Set-DhcpServerv4OptionValue -DnsServer 172.16.0.101,172.16.0.102 -Router 172.16.0.254
```

G.4 Serveur Active Directory

Le déploiement d'un serveur Active Directory au sein d'un réseau consiste à mettre en place un service d'annuaire LDAP qui nous permet par la suite de centraliser l'identification, l'authentification ainsi que la gestion et l'attribution de stratégies aux des éléments constitutifs d'un parc informatique (Utilisateurs finaux, imprimantes, ordinateurs, dossiers partagés, serveurs...).

Cet annuaire, respectant une hiérarchie stricte est bâtie autour d'unités organisationnelles (OU : Organisational Unit) visant à regrouper les éléments partageant les mêmes droits et stratégies sur le réseau (GPO : Group Policy Object). De fait, tout élément constituant notre réseau pouvant être inclus dans l'annuaire sera appelé objet dans cette section.

Au sein de cet annuaire, les utilisateurs et autres objets concernés par l'application des GPO sont instanciés dans des groupes (Réf. [H.13 Groupes et architecture Active Directory](#)).

Les annuaires LDAP ne pouvant fonctionner sans nom de domaine (Forêt) ; nous avons déployé le serveur Active Directory en mode core en incluant les rôles suivants :

- AD
- AD Domain Services
- DNS

Le script présent ci-dessous fait état des différentes étapes de déploiement des rôles nécessaires au bon fonctionnement de l'annuaire et la création de la forêt :

- Attribution de l'adresse IP au serveur et pointage vers les DNS

```
New-NetIPAddress -IPAddress 172.16.0.102 -InterfaceAlias "Ethernet" -DefaultGateway 172.16.0.254 -AddressFamily IPv4 -PrefixLength 16
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 127.0.0.1, 172.16.0.101
```

- Nommage du serveur virtuel

```
Rename-Computer SRVADHNS
Restart-Computer
```

- Déploiement des services Active Directory et des services associés

```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
Install-ADDSForest -DomainName "cyc.local" -DomainNetbiosName "CYC" -
InstallDns:$false -NoRebootOnCompletion:$false
```

- Création des Unités d'Organisation (OU)

```
New-ADOrganizationalUnit -Name "ADCYC" -Path "dc=CYC,dc=local"
New-ADOrganizationalUnit -Name "Groupes" -Path "ou=ADCYC,dc=CYC,dc=local"
New-ADOrganizationalUnit -Name "Utilisateurs" -Path "ou=ADCYC,dc=CYC,dc=local"
```

- Ajout des groupes de sécurité au domaine

```
New-ADGroup -Name "GS_Direction" -Path "OU=Groupes,OU=ADCYC,DC=CYC,DC=local" -
GroupCategory "Security" -GroupScope Global
New-ADGroup -Name "GS_ChefsService" -Path "OU=Groupes,OU=ADCYC,DC=CYC,DC=local" -
GroupCategory "Security" -GroupScope Global
New-ADGroup -Name "GS_Administratif" -Path "OU=Groupes,OU=ADCYC,DC=CYC,DC=local" -
GroupCategory "Security" -GroupScope Global
New-ADGroup -Name "GS_Old" -Path "OU=Groupes,OU=ADCYC,DC=CYC,DC=local" -
GroupCategory "Security" -GroupScope Global
New-ADGroup -Name "GS_Custom" -Path "OU=Groupes,OU=ADCYC,DC=CYC,DC=local" -
GroupCategory "Security" -GroupScope Global
```

Pour aller plus loin, nous avons établi un script d'inscription simplifiée des utilisateurs dans le domaine (Réf. [H.14 Script de creation des utilisateurs dans le domaine](#)).

G.5 Serveur d'impression

Comme mentionné dans la partie relative au choix matériel (Réf. [E – Choix du matériel réseau](#)), nous établissons un contrat de maintenance avec la société SCC, située à 200m de notre société.

3 résultats
Trier par Statut du partenaire ✓

SCC 4,13 km +33 3 80483800 info@fr.scc.com Visiter le site Web	PLATINUM Partenaire Spécialisations: 5 Compétences: 3 Plus d'informations
XEFI DIJON 2,98 km +33 3 80 72 00 10 dijon@xeflfr Visiter le site Web	GOLD Partenaire Spécialisations: 4 Plus d'informations
AMG INFORMATIQUE 21 3,71 km +33 3 80 74 24 44 amg@amg-informatique.com Visiter le site Web	GOLD Partenaire Spécialisations: 4 Plus d'informations

SCC
6 RUE DU CAP VERT
QUETIGNY, 21800
+33 3 80483800
info@fr.scc.com
[Visiter le site Web](#)

OBTENIR DES DIRECTIVES

Spécialisation Partner Ready
Support de stockage - Silver
Spécialiste prestataire de service - Silver
Spécialiste réseau - Platinum
Spécialiste ServiceOne Enterprise - Gold
Hybrid IT Specialist - Platinum

Partner Ready Competencies
ClearPass Policy Management
Services de location
Software Defined Infrastructure - VMware & Hyper-V Virtualization

Cette société, certifiée partenaire HPe et spécialisée dans la gestion matérielle, réseau et sécurité est à même d'intervenir en moins de 10 minutes, de gérer le déploiement d'un serveur d'impression et des imprimantes sur le site ainsi que d'assurer la sécurisation de nos sauvegardes sur leur Cloud.

G.6 Sauvegarde

Afin de pallier à tout risque de perte de nos données et/ou fonctionnalités serveur ; nous avons mis en place une routine de sauvegarde des différentes données en présence sur nos hyperviseurs (Serveurs, dossiers utilisateurs et dossier commun).

Le premier niveau de sauvegarde est observable sur nos hyperviseurs qui sont intégrés dans le cluster cyccluster. Ce dernier agit de manière équivalente au RAID 10 avec une perte de performances réduite par rapport à ce protocole.

Name	Size/min	# Placement Groups	CRUSH Rule		Used	
			ID	Name	%	Total
cycnetworking	2/2	64	0	replicated_rule	0.00%	0 B
cycbackup	2/2	64	0	replicated_rule	0.00%	0 B
					0.00%	0 B

De plus ; à l'aide de Ceph que nous avons introduit plus haut dans ce rapport (Réf. [H.8 Installation et configuration de Ceph](#)) ; nous bénéficions de deux pools de stockage :

- cycnetworking (Pool d'accueil de notre environnement de stockage utilisateur et commun)
- cycbackup (Pool d'accueil des sauvegardes de nos serveurs virtuels et du pool cycnetworking)

Nous avons alors établi que nous conservons les vingt-et-une dernières sauvegardes dans le pool cycbackup pour éviter à la fois un stockage de données trop important mais aussi, en cas d'incident, de rencontrer des problèmes de restauration en cas de corruption d'une sauvegarde.

Un script a été écrit dans ce but :

```
#!/bin/bash

#~ CONFIGURATION ~#
# Répertoire des fichiers
dossier="[répertoire de fichier : pool cycnetworking]"
# Répertoire de backup
backup="[répertoire de backup: pool cycbackup]"
# Nombre de backup a garder
nb=21
#~ NE PAS MODIFIER ~#
now=$(date +"%m_%d_%Y_%H%M%S")
tar czvf $backup/backup_$now.tar.gz --absolute-names $dossier > /dev/null &&
if [ ! -d "$backup/last" ]
```

```
then
    mkdir $backup/last > /dev/null
fi &&
for i in $(find $backup | ls -ltrF $backup | grep -v '/$' | tail -$nb)
do
    let y++
    tableau[$y]=$i
    mv "$backup/${tableau[$y]}" $backup/last > /dev/null
done &&
find $backup -maxdepth 1 -type f -delete &&
mv $backup/last/* $backup &&
rmdir $backup/last
```

Une version PowerShell du script est par ailleurs disponible en annexes (Réf. [H.15 Script de sauvegarde PowerShell](#)). ProxMox étant construit autour d'un noyau GNU / Linux, le script a été écrit en langage bash.

Conformément au cahier des charges qui nous a été communiqué avec la lettre de mission, nous donnons les autorisations d'exécution a notre script comme suit :

```
chmod +x backupscript
```

Ensuite, nous éditons le fichier crontab afin de créer une tâche planifiée pour notre script :

```
nano /etc/crontab
* 19 * * * root bash /home/backupscript
```

Afin d'éviter une saturation du pool, nous l'avons paramétré de sorte que son volume de stockage soit un peu plus de deux fois supérieur à celui du pool de stockage utilisateur, cycnetworking.

De plus, un lecteur de bande est présent dans notre salle réseau principale afin de créer des sauvegardes mobiles et sécurisées en cas d'incident environnemental sur site (Incendie, dégât des eaux...). Ces sauvegardes sont conservées sous coffre à l'étage du bâtiment principal.

Pour pallier à toute éventualité, la société SCC, notre prestataire en maintenance matérielle assurera en plus le stockage de nos sauvegardes sur leur Cloud.

G.7 Profil d'évolution du réseau

Au-delà de l'architecture détaillée au-dessus, le réseau en instance de déploiement pour notre société nous offre de multiples perspectives d'évolution.

En effet, comme représente sur la carte conceptuelle en début de ce rapport (Réf. [B.1 Carte conceptuelle](#)), il nous sera alors possible d'intégrer au réseau différents services sur les serveurs afin de faciliter la gestion de l'infrastructure interne du réseau, le management des utilisateurs finaux (Postes, matériel périphérique...), le rapatriement de certains services sur nos propres serveurs.

Ces évolutions pourront être menées à travers les points suivants :

- Déploiement d'un serveur mail sécurisé via le système ProxMox afin de s'affranchir de notre prestataire de messagerie
- Mise en place d'un portail captif via PFSense afin d'affiner le filtrage des réseaux des points d'accès
- Mise en place d'un serveur de déploiement PxE (Via iLo Advanced ou Fog entre autres)
- Déploiement de serveurs Apache, MariaDB, phpMyAdmin afin de rapatrier notre site web ou nos services de données actuellement gérés en externe (Comptabilité, datamining...)
- Déploiement d'un serveur HPeOneView afin de réaliser un mappage et une gestion globale des réseaux pour les sites appartenant au groupe Customize Your Car...