

PizzaCraft France



Installation du parc informatique

-

Mise en place de serveurs Windows et Linux

Kovacic Karine

Leveque Kevin

Sion John

GMSIA 2013

PizzaCraft France

Installation du parc Informatique

Mise en place de serveurs Windows et Linux

Table des matières

I – Présentation.....	5
A. PIZZACRAFT FRANCE au service de KING PIZZA	5
B. Le système informatique de PIZZA CRAFT FRANCE.....	6
C. L'équipe du service informatique.....	6
II – Projet.....	7
A. Description du projet, équipe projet et planning	7
A.1. Contexte et Cahier des charges.....	7
A.2. Partage des tâches	7
A.3. Planning d'avancement du projet.....	10
III – Étude des besoins en serveurs et logiciels	11
A. Étude des besoins en serveurs	11
A.1. Dimensionnement des serveurs.....	11
A.2. Choix des serveurs	12
A.4. Bilan financier matériel.....	13
B. Étude des besoins en Logiciels	13
B.1. Windows Server et Licences d'Accès Clients (CALs Users)	13
B.2. Licences d'Accès Terminal Serveur (CALs TSE).....	14
B.4. Antivirus serveur	15
B.5. Choix de la distribution Linux	15
B.6. Bilan financier logiciel.....	16
C. Bilan financier Global	16
IV – Plan d'adressage réseau	17
A. Choix de l'adresse réseau et distribution des adresses IP	17
B. Convention de nommages des machines	18
C. Schéma infrastructure système.....	18
V – Installation et configuration des Serveurs Windows	19
A. L'Active Directory	19
A.1. L'intérêt du déploiement d'un Active Directory ?	19
A.2. Présentation du domaine	19
A.3. Arborescence du domaine	19

A.4. Unité organisation – OU (Organizational Units)	20
A.5. Groupes	21
A.6. Comptes Utilisateurs et modèles.....	21
A.7. Convention de nommage des OU, groupes et utilisateurs :	22
A.8. Profils itinérants.....	23
A.9. VBScript.....	23
B. Le service DNS	25
B.1. Intérêt d'un service DNS	25
B.2. Fonctionnement d'un DNS	26
B.3. Enregistrement de ressources (SOA, NS, A, PTR) et Zones	28
C. La réplication des services Active Directory et DNS	31
C.1. Intérêt de la réplication.....	31
C.2. Fonctionnement de la réplication	31
C.3. Transfert de Zone	32
D. Scripts	35
D.1. Intérêt des scripts.....	35
D.2. Fonctionnement des scripts	35
D.3. Sauvegarde des scripts	36
E. Le Service Terminal Serveur.....	36
E.1. Intérêt d'un Service Terminal Serveur.....	36
E.2. Fonctionnement d'un Service Terminal Serveur	36
F. Serveur d'impression.....	38
F.1. Intérêt d'un serveur d'impression	38
F.2. Convention de nommage des imprimantes	38
F.3. Organisation + implantation des imprimantes	38
G. GPO ou Stratégies de Groupe	39
G.1. Intérêt des GPO.....	39
G.2 Mise en place des GPO.....	39
G.3. Résultats des GPO	40
VI – Installation et configuration des Serveurs Linux	42
A. Le service DHCP.....	42
A.1. Intérêt d'un DHCP	42
A.2. Fonctionnement d'un DHCP	42
A.3. Étendue, exclusion, réservation, durée du bail	42
A.4. Tolérance de panne	43
A.5. Installation et configuration	43
B. Le serveur de fichiers Samba (partage de fichiers interne)	46
B.1. Intérêt d'un serveur de fichiers	46

B.2. Arborescence du serveur de fichier.....	46
B.3. Intégration du serveur SAMBA au domaine	48
B.4. Gestion des permissions.....	50
B.5. Quotas	53
C. Le serveur FTP	54
C.1. Intérêt d'un serveur FTP	54
C.2. Installation et Configuration	54
C.3. Création d'utilisateurs virtuels	55
C.4. Utilisation en mode sécurisé	55
C.5. Utilisation en mode anonyme.....	58
VII– Le logiciel de gestion de parc informatique.....	60
A. Les besoins	60
B. MCD : Modèle conceptuel de base de donnée	60
C. MPD : Modèle physique de base de données.....	62
D. Réalisation / Maquette	63
D.1. Page d'accueil	63
D.2. Mode de Gestion.....	64
D.3. Mode de Consultation	65
VIII – La tolérance de panne	65
IX – La gestion des sauvegardes.....	66
A. Sauvegarde du contrôleur de domaine :	67
B. Sauvegarde du serveur de fichiers (profils itinérants, données de l'entreprise)	68
X – Planning prévisionnel.....	69
XI – Bilan Personnel	70
XII – Pour aller plus loin	72
A. Mise en place d'un server OCS et GLPI.....	72
A.1. Intérêt d'un server OCS et GLPI	72
A.2. Principe de fonctionnement.....	72
A.3. Installation et configuration	73
A.4. Déploiement de l'agent OCS Inventory sous linux	73
A.5. Déploiement de l'agent OCS Inventory sous Windows	74
A.6. Remontée des informations dans OCS.....	74
A.7. Interfaçage OCS – GLPI	76
B. Mise en place de serveur et client NFS – Sauvegarde du serveur de fichiers	77
B.1. Intérêt d'un serveur et client NFS.....	77
B.2. Principe de fonctionnement.....	78
B.3. Installation et configuration	79
B.4. Sauvegarde du serveur de partage de fichiers	80

PizzaCraft France

Installation du parc Informatique

Mise en place de serveurs Windows et Linux

I – Présentation

A. PIZZACRAFT FRANCE au service de KING PIZZA



KING PIZZA est une franchise internationale spécialisée dans le domaine de la restauration rapide autour de la pizza.

Implantée en France depuis 1989, le développement de notre franchise n'a cessé de croître jusqu'à atteindre un réseau de 215 points de vente en 2013.

Pour faciliter la logistique d'approvisionnement de ses points de ventes, **KING PIZZA** a créé parallèlement lors de son implémentation en France; l'entreprise **PIZZACRAFT France**.



PIZZACRAFT France est une centrale d'achat unique qui négocie et fournit 2 lignes de produits à l'ensemble des franchisés :

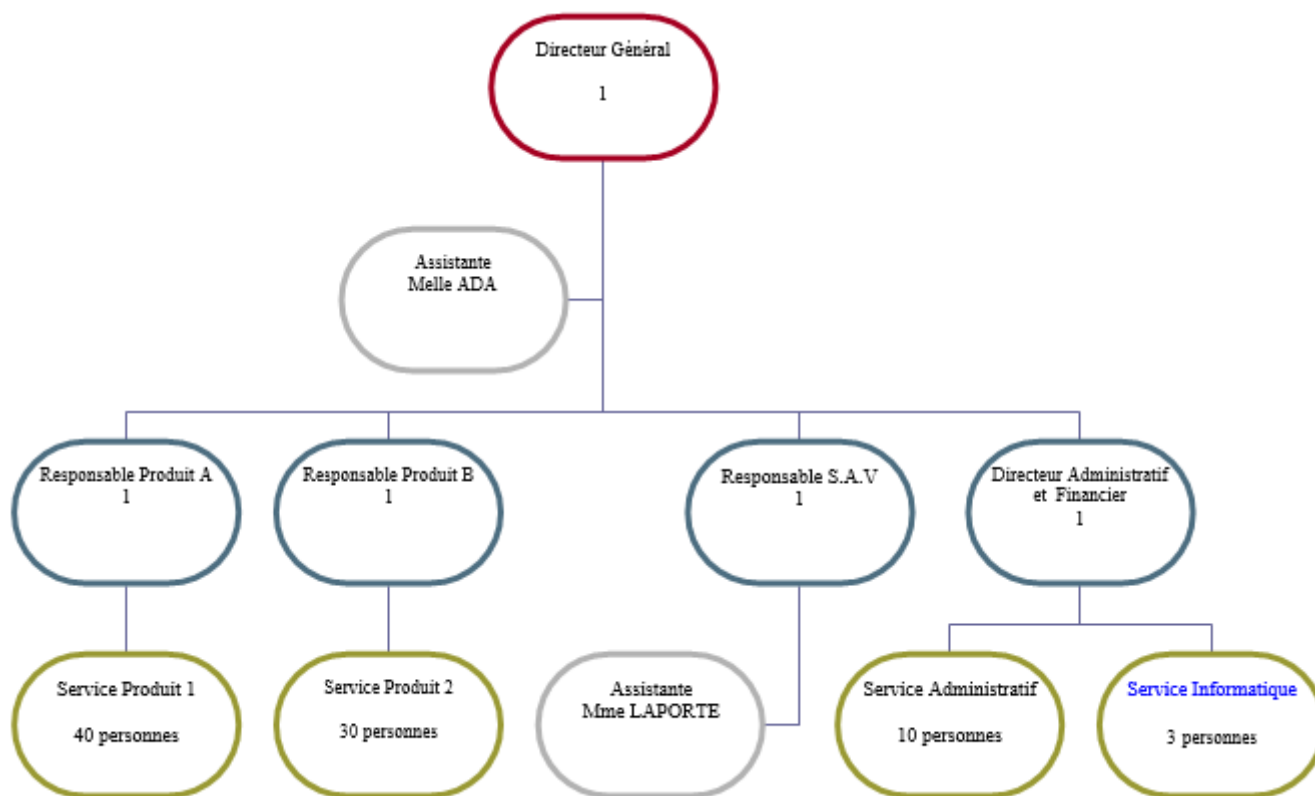
- **Une ligne de produits alimentaires** représentée par l'ensemble des éléments constituant les pizzas, ainsi que les entrées, desserts et boissons :

- Pâte, sauce tomate, fromages.
- Légumes, viande.
- Glaces, pâtisseries.
- Boissons (soda, eaux minérales etc...).

- **Une ligne de produits non alimentaires** constituée de l'ensemble du matériel nécessaire pour stocker, réaliser, vendre et acheminer les pizzas, par exemple :

- Réfrigérateurs, fours de cuisson.
- Boîtes à pizza, gobelets, serviettes, couverts en plastique.
- Comptoirs de vente, caisses, enseignes, signalétiques, éclairages.

L'entreprise **PIZZACRAFT FRANCE** compte aujourd'hui 90 salariés répartis selon l'organigramme ci-dessous :



B. Le système informatique de PIZZA CRAFT FRANCE

Le système informatique de **PizzaCraft** France est composé d'une trentaine d'ordinateurs (postes fixes et ordinateur portables). La majorité de ces ordinateurs se situent dans le bâtiment principal répartis sur deux étages.

On trouve aussi quatre postes fixes pour le service de production de la ligne Alimentaire dans le bâtiment Ouest et enfin 3 autres postes fixes dans le bâtiment Est pour la ligne de production Non Alimentaire.

Le parc informatique comporte aussi dix imprimantes, une pour chaque service (Direction, Compta, RH, SAV, Informatique, Accueil, 2 pour la Ligne Produit A et 2 pour la Ligne Produit B)

Ces postes ont pour système d'exploitation le logiciel Windows 7 Professionnel de Microsoft, sauf le responsable du service SAV et son assistante qui travaillent tous les deux sous Ubuntu afin de faire fonctionner une application métier dédiée.

C. L'équipe du service informatique

Le service informatique est composé de 3 personnes :

- M. Sion John, diplômé du CESI, spécialisé dans la gestion du réseau, chef de projet.
Interlocuteur privilégié entre les différents services pour les problématiques informatiques

(amélioration du système, étude des besoins).

- Mme. Kovacic Karine, diplômée du CESI, en charge de la gestion des serveurs Windows, notamment de l'annuaire de l'entreprise Active Directory.

- M. Leveque Kevin, diplômé du CESI, en charge des serveurs Linux.

II – Projet

A. Description du projet, équipe projet et planning

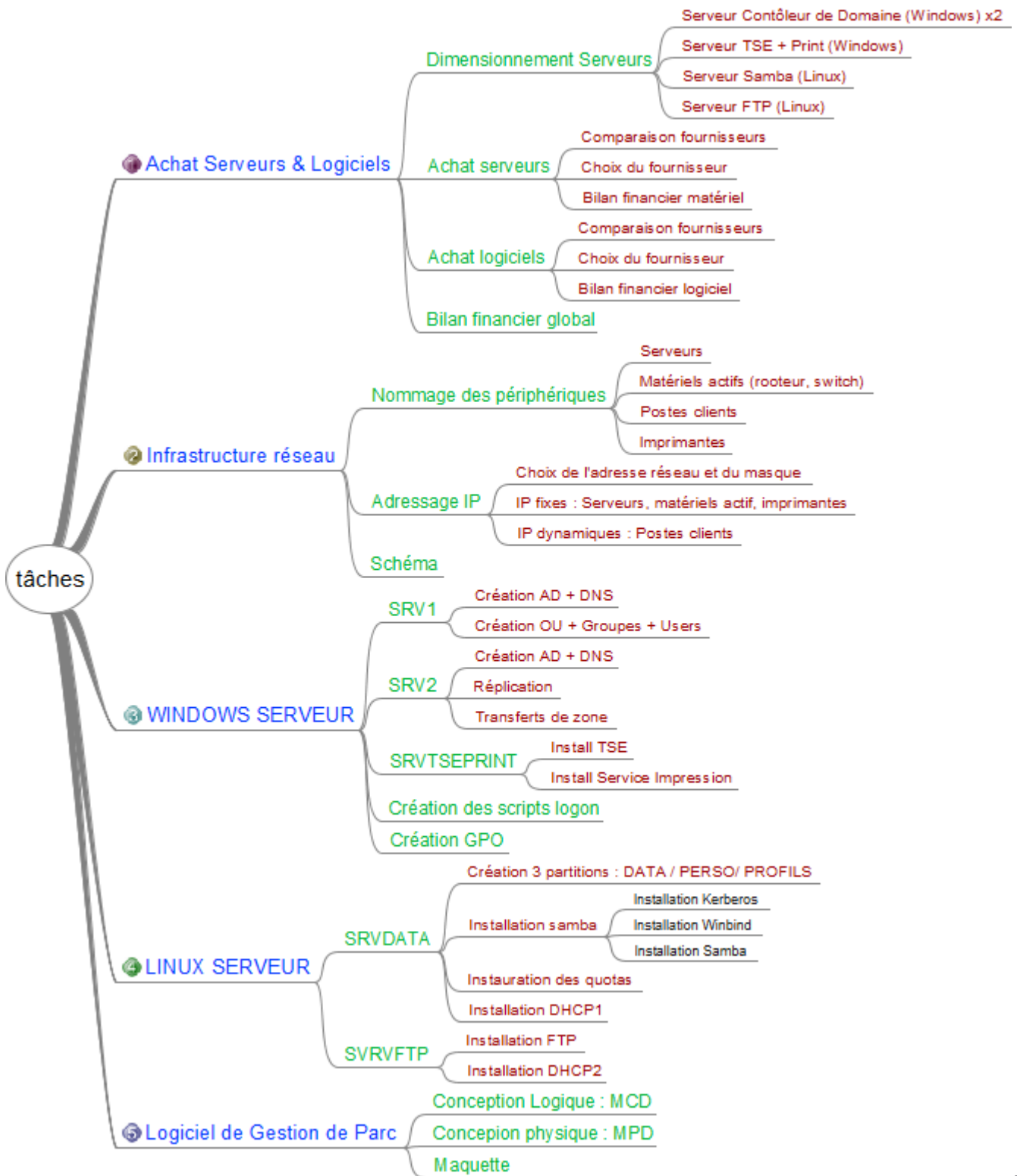
A.1. Contexte et Cahier des charges

Suite au déménagement de l'entreprise **PizzaCraft** dans ses nouveaux locaux et à l'installation de son nouveau parc informatique, un audit de ce dernier a été effectué et plusieurs axes d'améliorations ont été proposés :

- **Mise en place de plusieurs serveurs Windows avec différents services dont :**
 - **un annuaire d'entreprise : Active Directory.**
Il n'y a pas de gestions des droits utilisateurs, pas de règles de sécurité concernant les mots de passe. L'accès au système d'impression n'est pas réglementé et il n'existe pas de stratégie locale de sécurité sur les postes.
 - **Un service DNS (Domain Name System)**
Pour le moment, les postes sont en réseaux mais ne sont pas aisément identifiables. De plus il n'y a pas la possibilité de prise en main à distance de ces derniers.
 - **Un service Terminal Serveur (TSE)**
Les applications métiers hébergées sur les serveurs doivent être accessibles à distance depuis un certain nombre de poste.
 - **Un serveur d'impression**
Afin de faciliter la gestion des imprimantes.
- **Mise en place de plusieurs serveurs Linux dont :**
 - Un service DHCP afin d'attribuer automatiquement des adresses IP aux postes et de faire des réservations d'IP.
 - Un serveur de partage de fichiers internes (SAMBA)
 - Un serveur FTP en accès libre et identification sécurisée.
- **Réalisation d'un logiciel de gestion de parc.**
En effet, l'équipe informatique court partout...et se trompe souvent de lieu pour dépanner les utilisateurs. En plus, il n'y a pas d'informations stockées quelque part sur le parc (Nom d'hôtes, type de machines...)

A.2. Partage des tâches

A partir du cahier des charges, nous avons établis une liste des tâches :



L'organisation a été la suivante :

- Un chef de projet (Sion John) qui aura la tâche de superviser l'ensemble du projet, de veiller au respect des délais, et d'animer les réunions de travail, et qui s'occupera de la création du logiciel de gestion de parc.
- Un assistant projet qui gérera le déploiement des serveurs Windows (Karine Kovacic)
- Un assistant projet qui gérera le déploiement des serveurs Linux (Kevin Leveque)

Nous nous sommes ensuite réparties les tâches de la manière suivante :

Tâches	Affectations
Présentation	John
Entreprise / Service Info	John
Projet	John
Partage des tâches	John
Planning avancement projet	John
Charte Graphique	John
Etude Serveurs	Karyn
Choix d'une solution	Karyn
Choix d'un fournisseur	Karyn
Bilan financier matériel	Karyn
Etude Logiciels	Karyn
Windows Serveur	Karyn
CALs Users	Karyn
CALSTSE	Karyn
Antivirus	Karyn
Distribution Linux	Karyn
Bilan financier logiciel	Karyn
Bilan financier global	Karyn
Install. & Config. Win. Server	Karyn
Service DNS	Karyn
Service Active Directory	Karyn
Service Terminal Server	Karyn
Tolérance de panne	Karyn
Install. & Config. Linux Server	Kevin
Service DHCP	Kevin
Serveur SAMBA	Kevin
Seveur FTP	Kevin
Tolérance de panne	Kevin
Application Gestion de Parc	John
Analyse	John
MCD	John
MPD	John
Réalisation	John
Planning de faisabilité	John
Bilan personnel	John

Les outils utilisés pour mener à bien le projet :

- La suite [Microsoft Office](#) pour générer les documents
- Un dossier partagé [DROPBOX](#) pour le partage des documents
- [Skype](#) pour la tenue de réunion hebdomadaire (le Vendredi)

À chaque fin d'étape et lors des bilans, une réunion de concertation sera programmée.

A.3. Planning d'avancement du projet

En fonction du partage des tâches précédent et du délai pour rendre le projet, nous avons estimé le planning d'avancement suivant :

Tâches	Affectations	Mars				Avril				Mai				Juin				Juillet				
		Semaine	Semaine	Semaine	Semaine	Semaine	Semaine	Semaine	Semaine	Semaine	Semaine	Semaine	Semaine	Semaine	Semaine	Semaine	Semaine	Semaine				
		10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Présentation	John																					
Entreprise / Service Info	John																					
Projet	John																					
Partage des tâches	John																					
Planning avancement projet	John																					
Charte Graphique	John																					
Etude Serveurs	Karyn																					
Choix d'une solution	Karyn																					
Choix d'un fournisseur	Karyn																					
Bilan financier matériel	Karyn																					
Etude Logiciels	Karyn																					
Windows Serveur	Karyn																					
CALs Users	Karyn																					
CALs TSE	Karyn																					
Antivirus	Karyn																					
Distribution Linux	Karyn																					
Bilan financier logiciel	Karyn																					
Bilan financier global	Karyn																					
Install. & Config. Win. Server	Karyn																					
Service DNS	Karyn																					
Service Active Directory	Karyn																					
Service Terminal Server	Karyn																					
Tolérance de panne	Karyn																					
Install. & Config. Linux Server	Kevin																					
Service DHCP	Kevin																					
Serveur SAMBA	Kevin																					
Seveur FTP	Kevin																					
Tolérance de panne	Kevin																					
Application Gestion de Parc	John																					
Analyse	John																					
MCD	John																					
MPD	John																					
Réalisation	John																					
Planning prévisionnel	John																					
Bilan personnel	John																					

Nous avons prévu deux semaines de marge afin d'apporter les dernières modifications éventuelles.

En fonction de ces deux impératifs, le projet doit être achevé avant la fin de la semaine 26, c'est-à-dire le 27 Juin 2014.

III – Étude des besoins en serveurs et logiciels

A. Étude des besoins en serveurs

A.1. Dimensionnement des serveurs

Nous avons besoin de 5 serveurs.

Les serveurs **SRV1** et **SRV2** hébergeront l'Active directory et le DNS (le SRV2 étant une réplication du SRV1).

La configuration matérielle de ces serveurs tiendra compte des prérequis Microsoft, mais sera aussi pensée pour assurer la pérennité du matériel en fonction de l'accroissement de l'entreprise et de son activité.

Ainsi les prérequis Microsoft pour un serveur hébergeant un Active Directory sont :

Composant	Recommandation
Processeur	2 GHz ou plus
Mémoire	2 Go de RAM ou plus
Espace disque disponible	40 Go ou plus

Le 3^{ème} serveur, **SRVTSEPRINT**, hébergera quant à lui le service TSE et fera aussi office de serveur d'impression.

Le service TSE est un service exigeant en terme de ressources matériels car il virtualise un environnement complet Windows pour chaque utilisateur.

Ainsi la quantité de mémoire RAM est fonction du nombre d'utilisateurs du service mais aussi et surtout fonction de la quantité de mémoire vive nécessaire pour faire fonctionner l'application à virtualiser.

Nous prévoyons d'acquérir une licence par utilisateur du service TSE.

Les 4^{ème} et 5^{ème} serveurs, sont des serveurs de fichiers ayant pour système d'exploitation la distribution **Linux Debian**. Si la configuration matérielle pour faire fonctionner cette distribution peut être modeste, c'est le système de stockage de fichiers qu'il faut bien dimensionner. Nous opterons ici pour un système de RAID 5 qui allie à la fois sécurité et performance.

Ainsi le dimensionnement de nos serveurs sera le suivant :

Serveur	OS	Processeur	RAM	RAID	Taille disque	Nbre de disque	Taille Totale	Partition système	Partitions Fichiers / Bdd AD
SRV1	Win. Serv. 2008	3,0 Ghz	4 Go	RAID 1	500 Go	2	500 Go	100 Go	400 Go
SRV2	Win. Serv. 2008	3,0 Ghz	4 Go	RAID 1	500 Go	2	500 Go	100 Go	400 Go
SRVTSEPRINT	Win. Serv. 2008	3,0 Ghz	16 Go	RAID 10	500 Go	4	1 To	500 Go	500 Go
SRVDATA	Linux DEBIAN	3,0 Ghz	8 Go	RAID 5	500 Go	4	1,5 To	100 Go	400 Go -500 Go -500 Go
SRVFTP	Linux DEBIAN	3,0 Ghz	8 Go	RAID 5	500 Go	4	1,5 To	100 Go	1,4 To

A.2. Choix des serveurs

Lors du déménagement des locaux, nous avons dimensionné les baies de brassage afin de pouvoir y insérer du matériel « rackable ».

Après plusieurs recherches et comparatifs avec d'autres fabricants, notamment HP, nous avons retenue DELL car lui seul est capable de proposer une configuration personnalisée, adaptée à nos besoins.

Il est notamment possible de vérifier la compatibilité des cartes contrôleurs RAID avec les systèmes d'exploitation (distributions Linux), choisir la quantité de RAM et la configuration des disques avec précision.

Il est en outre possible grâce au site d'obtenir une estimation rapide du coût prévisionnel avant de passer à une étape de négociation avec le service commercial.

La rapidité du support et les prix compétitifs de ce fabricant, en font un choix judicieux pour équiper l'entreprise de serveurs.

Parallèlement, nous avons aussi souscrit un contrat de maintenance. Ce contrat sera composé d'une garantie matérielle de 3 ans, avec une intervention sur site dans les 4 heures.

Pour les serveurs [SRV1](#) et [SRV2](#) qui hébergeront l'Active directory et le DNS nous avons choisi la référence suivante : [Dell PowerEdge R210 II](#)

Ce serveur est équipé comme suit :

	Dell PowerEdge R210 II
Chassis	PowerEdge R210 II Chassis, 2x3.5" Cabled HDDs, LED Diagnostics
Processeur	Intel® Pentium® Processor G2120, 2C/2T, 3.10GHz, 3M Cache, 55W TDP
RAM	4GB Memory (1x4GB), 1600MT/s, Single Ranked, Low Volt UDIMM
OS	No Operating System
Controleur RAID	PERC H200 RAID Controller - RAID 1, Requires 2 SAS/SATA/SSD Drives
Disques durs	2 x 500GB, SATA, 3.5-in, 7.2K RPM Hard Drive (Cabled)
Lecteurs	16X DVD+/-RW ROM Drive SATA with SATA Cable
TOTAL HT	1 124,00 €

Pour le serveur [TSE/ Impression](#), la référence choisie est le serveur : [Dell PowerEdge R415](#)

Ce serveur est équipé comme suit :

	Dell PowerEdge R415
Chassis	PowerEdge R415 Rack Chassis for AMD Opteron 42xx, Up to 4x 3.5" Hot Plug HDDs, LCD
Processeur	AMD Opteron 4334, 6C, 3.1GHz, 6M L2/8M L3 Cache, Turbo CORE, 95W TDP, DDR3-1600MHz
RAM	16 GB Memory for 1CPU (1x16GB Dual Rank LV RDIMMs) 1600MHz, Running at 1333MHz
OS	No Operating System
Controleur RAID	PERC H200A RAID Controller - RAID 10, Requires 4 SAS/SATA/SSD Drives
Disques durs	4 x 500GB, SATA, 3.5-in, 7.2K RPM Hard Drive (Cabled)
Lecteurs	16X DVD+/-RW ROM Drive SATA with SATA Cable
TOTAL HT	2 260,00 €

Pour les serveurs de fichiers [SRVDATA](#) et [SRVFTP](#), nous choisirons la référence suivante : [Dell PowerEdge R415](#).

Ce serveur est équipé comme suit :

Dell PowerEdge R415	
Chassis	PowerEdge R415 Rack Chassis for AMD Opteron 42xx, Up to 4x 3.5" Hot Plug HDDs, LCD
Processeur	AMD Opteron 4334, 6C, 3.1GHz, 6M L2/8M L3 Cache, Turbo CORE, 95W TDP, DDR3-1600MHz
RAM	8GB Memory,(1x8GB) 1600MT/s, Single Rank LVRDIMMs
OS	No Operating System
Controleur RAID	RAID 5 for PERC H700A, 3-4 SAS/SATA/SSD Hot Plug HDDs
Disques durs	4 x 500GB, SATA, 3.5-in, 7.2K RPM Hard Drive (Cabled)
Lecteurs	16X DVD+/-RW ROM Drive SATA with SATA Cable
TOTAL HT	1 903,00 €

A.4. Bilan financier matériel

Objet	Référence	Prix HT
SRV 1	Dell PowerEdge R210 II	1 124,00 €
SRV 2	Dell PowerEdge R210 II	1 124,00 €
SRVTSEPRINT	Dell PowerEdge R415	2 260,00 €
SRVDATA	Dell PowerEdge R415	1 903,00 €
SRVFTP	Dell PowerEdge R415	1 903,00 €
Dell	Contrat de maintenance	2 312,00 €
TOTAL HT		10 626,00 €

B. Étude des besoins en Logiciels

B.1. Windows Server et Licences d'Accès Clients (CALs Users)

Il est désormais difficile de se procurer Windows Server 2008 R2 chez Microsoft, car ce dernier ne propose que la dernière version de Windows Server, à savoir la 2012 R2.

Pour obtenir la version 2008, nous devons passer par des vendeurs tiers ou acheter la version 2012 et procéder à un downgrade.

L'authentification des utilisateurs se fera par l'intermédiaire de CALs utilisateurs plutôt qu'à travers de CALs périphériques. Cela permettra à un utilisateur de se connecter sur n'importe quel poste grâce à ses identifiants et de retrouver son environnement de travail.

Windows Server 2012 R2 n'étant pas disponible chez DELL, nous avons choisi après comparaison, le fournisseur [Inmac](#) afin d'acquérir nos licences Windows Server 2012 R2 ainsi que nos CALs utilisateurs.

Nous avons donc comparé 2 offres :

- 1) Tout acheter (licences serveurs et CALs utilisateurs) en version 2008.
- 2) Tout acheter (licences serveurs et CALs utilisateurs) en version 2012 puis procéder à un downgrade vers la version 2008 R2.

Le nombre de licences d'accès clients (CALs) sera fonction du nombre de collaborateurs / postes informatiques. Nous avons une trentaine de postes informatiques, nous achèterons donc 30 licences d'accès client.

Windows Serveur 2008 R2				
Fournisseur	Produit	Prix unitaire	Quantité	Prix Total HT
Inmac	Windows Server 2008 R2 Standard Edition + 5 licences d'accès client	635,26 €	3	1 905,78 €
LDLC.com	Pack de 5 licences d'accès client pour Windows Server 2008 R2	154,95 €	3	464,85 €
				2 370,63 €

Windows Serveur 2012 R2				
Fournisseur	Produit	Prix unitaire	Quantité	Prix Total HT
Inmac	Windows Server 2012 R2 Standard Edition	638,86 €	3	1 916,58 €
Inmac	Pack de 5 licences d'accès client pour Windows Server 2012 R2	120,41 €	6	722,46 €
				2 639,04 €

Pour des raisons de disponibilité, nous nous orienterons vers la version 2012 de Windows serveur. Cela nous permettra dans un premier temps de basculer en version 2008 via un downgrade et plus tard de migrer vers la version 2012.

Dell propose l'installation de Windows Server sauf qu'à ce jour, il ne permet l'acquisition que de la version 2008 R2, et à un prix plus élevé que l'achat chez un autre fournisseur de la version 2012 R2. De plus, acheter la version 2008 R2 chez Dell va impliquer une restriction lors de l'upgrade vers 2012 R2 : il faudra acheter les licences 2012 R2.

B.2. Licences d'Accès Terminal Serveur (CALs TSE)

Une Licence d'Accès Terminal Serveur (CALs TSE), permet à un utilisateur de se connecter sur un ordinateur faisant tourner Windows Server, et rend possible la virtualisation d'un poste : l'utilisation d'une application ou d'un bureau complet de n'importe où, tout en garantissant un contrôle et une administration centralisée.

Comme pour les CALs utilisateurs plus haut, nous avons choisi les CALs TSE utilisateurs plutôt que périphériques.

CALs TSE - Windows Serveur 2012 R2				
Fournisseur	Produit	Prix unitaire	Quantité	Prix Total HT
Microsoft	5 CALs TSE - Windows Serveur 2012 R2	665,98 €	6	3 995,88 €
Materiel.net	1 CALs TSE - Windows Serveur 2012 R2	150,49 €	30	4 514,70 €

Pour des raisons de commodité, nous avons choisi www.materiel.net, qui est le plus proche distributeur européen.



B.4. Antivirus serveur

Nous avons comparé plusieurs fournisseurs d'antivirus serveur :

Fournisseur	Nom du logiciel	Nombre de licences (besoin = 30)	Administrable à distance	Adapté pour les serveurs	Prix HT / an
Kaspersky	ENDPOINT SECURITY FOR BUSINESS Core	25	Oui	Non	507,00 €
Kaspersky	ENDPOINT SECURITY FOR BUSINESS Core	50	Oui	Non	910,50 €
ESET	Endpoint Security	30	Oui	Non	742,40 €
Trend Micro	Worry-Free Business Security Standard	30	Oui	Oui	1 366,20 €
AVG	Antivirus Business Edition	30	Oui	Non	613,18 €
Avast	Endpoint Protection Plus	30	Oui	Non	779,70 €
Avira	Endpoint Security	30	Oui	Oui	1 098,00 €
Microsoft	Security Essential	N/A	Non	Non	Gratuit

Suite à ce comparatif, nous avons choisi l'antivirus **Avira**, qui offre flexibilité (choix du nombre exact de licences), un prix compétitif, ainsi que la possibilité d'une administration à distance et l'installation sur serveur Windows.



B.5. Choix de la distribution Linux

Une étude portant sur la répartition des distributions Linux utilisées dans le monde des serveurs web, nous indique que la distribution **DEBIAN** est la plus utilisée.

Distribution	Taux de répartition	Support	Prix HT / an
Debian	29,50%	Communauté	Gratuit
CentOs	29,32%	Communauté	Gratuit
Ubuntu	17,80%	Communauté	952,00 €
Red Hat	12,60%	RedHat Enterprise Linux	1 766,64 €
Fedora	5,20%	Communauté	Gratuit

Avantages de Debian :

- Il s'agit d'une distribution orientée serveur
- Le système d'exploitation est libre et gratuit
- Nouvelles versions régulières, afin de corriger d'éventuels bogues

Nous choisirons donc la distribution **DEBIAN** pour équiper nos serveurs sous Linux afin de profiter de la richesse du support assuré par la communauté.



B.6. Bilan financier logiciel

Description	Prix HT
Windows Server 2012 R2 Standard Edition + 30 CALs users	2 639,04 €
30 CALs Windows Server 2012 R2 Remote Desktop Services	4 514,70 €
Avira - Endpoint Security - 30 PC + Serveurs	1 098,00 €
Distribution Linux Debian	Gratuit
TOTAL	8 251,74 €

C. Bilan financier Global

Bilan financier global	
Prix HT	
Coût Matériel	10 626,00 €
Coût Logiciel	8 251,74 €
Coût Total	18 877,74 €

IV – Plan d’adressage réseau

A. Choix de l’adresse réseau et distribution des adresses IP

L’entreprise est donc actuellement équipée de 30 ordinateurs pour les collaborateurs, de 5 serveurs, de 6 imprimantes, de 6 switches et d’un routeur.

Pour le moment donc, l’entreprise ne possède que très peu de matériel nécessitant une adresse IP.

Or, il est prévu à terme de relier chaque franchise et leurs terminaux à un ERP hébergé au sein de l’entreprise.

Compte tenu de la croissance de la société, une adresse de classe B avec un masque en /16 nous garantira une évolution sereine de l’infrastructure réseau.

Nous avons donc choisi une adresse réseau du type 172.16.0.0 avec masque en /16 (255.255.0.0) qui nous permettra d’adresser 65534 machines.

Les serveurs, imprimantes et matériels réseau (switches, routeurs) auront des IP fixes tandis que les ordinateurs auront des IP dynamiques.

Ces adresses seront gérées par un serveur DHCP et distribuées de la manière suivante :

Equipements	Statiques	DHCP 1	DHCP 2
Serveurs	172.16.0.1 à 172.16.0.10	N/A	N/A
Switches et routeurs	172.16.0.11 à 172.16.0.21	N/A	N/A
Imprimantes	172.16.0.22 à 172.16.0.32	N/A	N/A
Postes clients	N/A	172.16.0.33 à 172.16.0.254	172.16.1.33 à 172.16.1.254

NB : le DHCP 2 ne sera utilisé qu’en cas de dysfonctionnement du 1^{er} serveur DHCP.

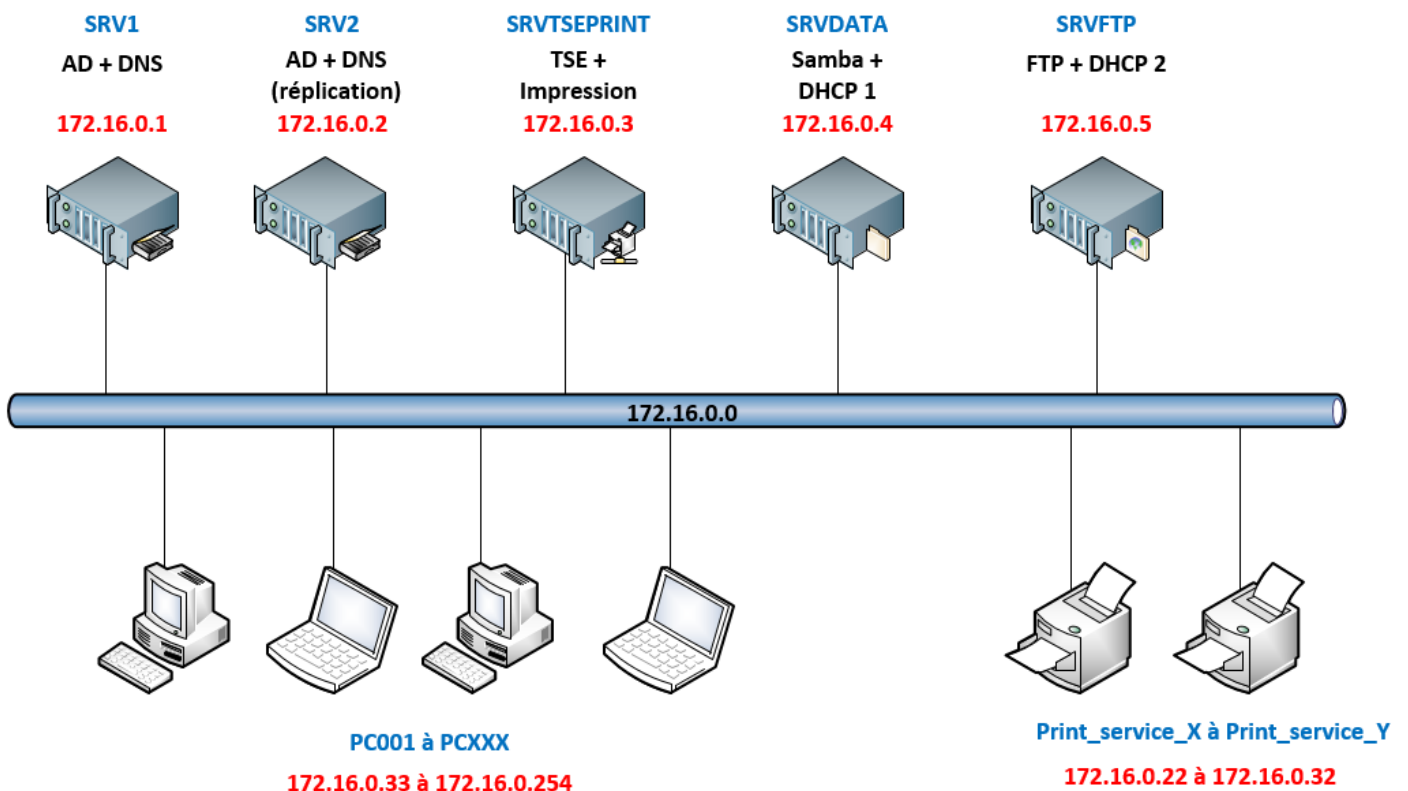
B. Convention de nommage des machines

L'ensemble du matériel sera nommé de la manière suivante :

Matériel	Nommage	Description
Serveurs	srv1	AD + DNS
	srv2	AD + DNS
	srvtseprint	Serveur TSE + impression
	srvdata	Serveur de fichiers + DHCP primaire
	srvftp	Serveur FTP + DHCP secondaire
Postes clients	pc001	Postes clients
	pc002	
	pcxxx	
Matériel actif	sw01	Switches
	sw02	
	swxx	
	root01	Routeurs
	rootxx	
	print_service_X	Printers
	print_service_Y	

C. Schéma infrastructure système

INFRASTRUCTURE RESEAU ENTREPRISE PIZZACRAFT



V – Installation et configuration des Serveurs Windows

A. L'Active Directory

A.1. L'intérêt du déploiement d'un Active Directory ?

Active Directory (AD) est la mise en œuvre, par Microsoft, des services d'annuaire LDAP (Lightweight Directory Access Protocol) pour les systèmes Windows.

L'objectif principal d'Active Directory est de fournir des services d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows.

Il permet également l'attribution et l'application de stratégies, la distribution de logiciels et l'installation de mise à jour critiques par les administrateurs.

Il répertorie les éléments d'un réseau administré : les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc.

Ainsi les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation des accès aux ressources répertoriées.

A.2. Présentation du domaine

Active Directory introduit la notion de hiérarchie. Sous la forme d'une arborescence cette organisation comporte plusieurs niveaux.

Le plus haut niveau de l'Active Directory est la forêt, elle-même constituée de domaines.

Un domaine est un environnement permettant de rassembler tous les utilisateurs et machines au sein d'une même architecture. Compte tenu de la taille de notre société, nous ne déploieront qu'un seul domaine. Le nom de ce domaine sera : [pizza.local](#)

A.3. Arborescence du domaine

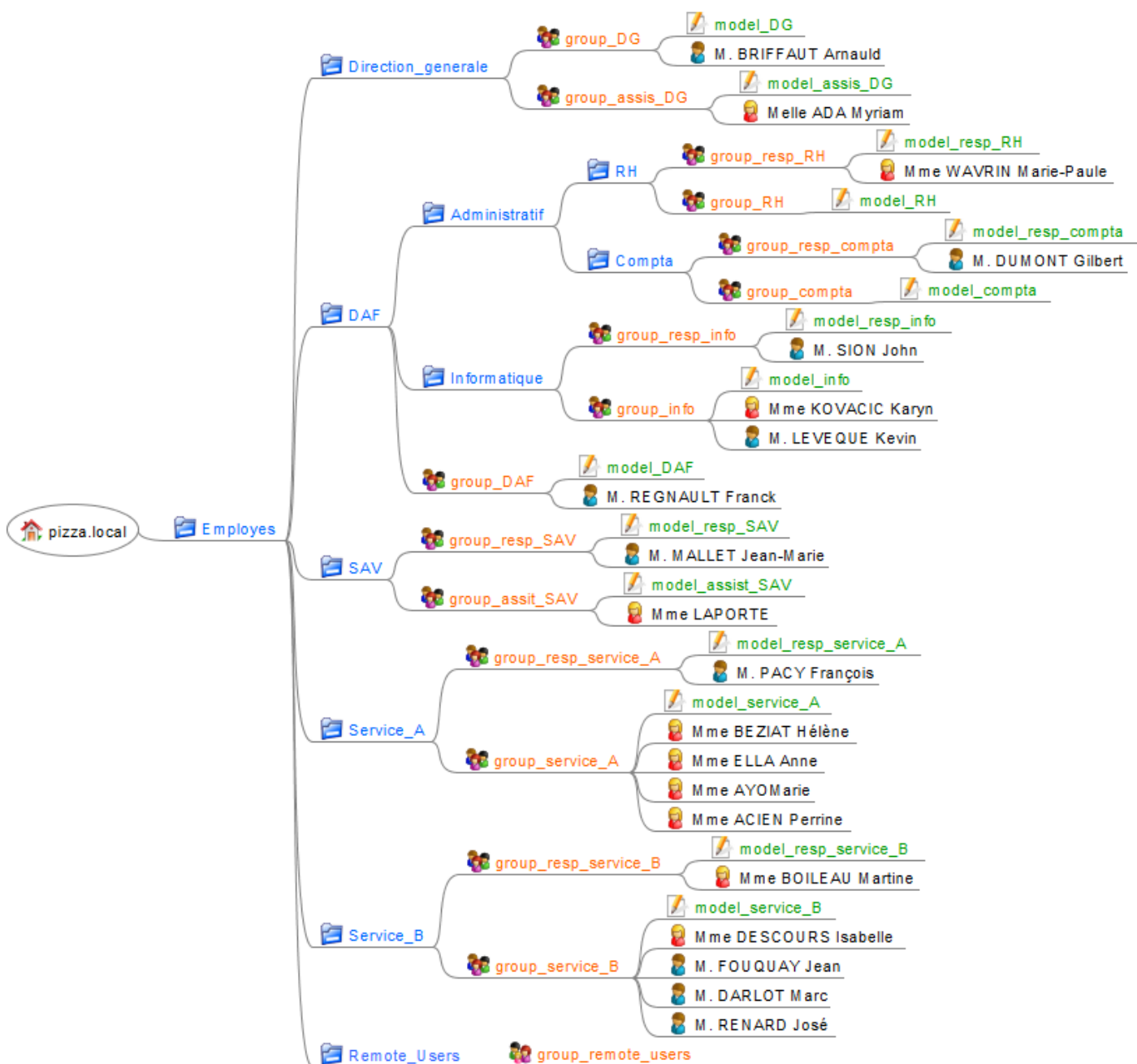
Un domaine peut être à son tour subdivisé en Unité Organisationnelle (par convention, nommé en anglais OU pour « Organizational Units »).

Ces OU sont des objets conteneurs qui permettent de hiérarchiser l'Active Directory.

En effet à l'intérieur de ces OU pourront être déclarés des utilisateurs, réunis par groupes. Des droits pourront être attribués de façon collective ou individuelle à ces utilisateurs ou groupes afin de faciliter l'administration des ressources informatiques de l'entreprise.

Les OU permettant de hiérarchiser les ressources informatiques d'une entreprise, nous avons décidé de les organiser en fonction de l'organigramme de la société.

Voici l'arborescence du domaine :

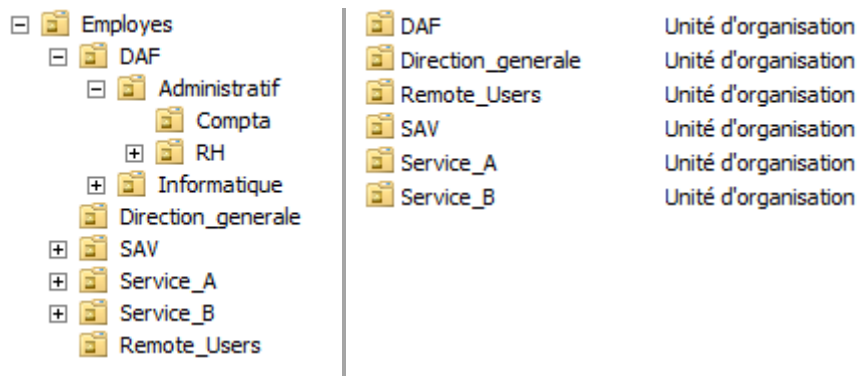


A.4. Unité organisation – OU (Organizational Units)

Comme indiqué précédemment, on crée les OU en respectant l'organigramme de la société, c'est-à-dire que l'on a autant d'OU que de services (Direction générale, DAF, SAV, Service A, Service B). On créera un dernier OU qui regroupera l'ensemble des utilisateurs du service bureau à distance (Remote_Users).

Le service du Directeur Administratif et Financier (DAF) a sous sa tutelle les services « Administratif » et « Informatique », on représentera ces derniers sous la forme de deux sous OU.

De la même manière, on trouvera à l'intérieur du sous OU « Administratif » les OU « RH » et « Compta ».



A.5. Groupes

Dans un OU, on trouvera à chaque fois un groupe représentant les fonctions des collaborateurs, par exemple :

- Le groupe responsable pour la fonction de responsable de service
- Le groupe directeur pour la fonction de directeur
- Le groupe assistante pour la fonction d'assistante
- Le groupe « nom du service » pour les employés n'ayant pas de titre

Ces groupes seront utiles pour l'attribution de droits à un collaborateur ou à un ensemble de collaborateurs. Par exemple si le DAF venait à être remplacé par un autre collaborateur, il suffira de déclarer ce collaborateur dans le groupe DAF, afin que ce dernier récupère ses droits et autorisations.

 group_assis_DG	Groupe de sécurité - Global
 group_DG	Groupe de sécurité - Global
 group_info	Groupe de sécurité - Global
 group_resp_info	Groupe de sécurité - Global

A.6. Comptes Utilisateurs et modèles






Ensuite on trouvera dans chaque groupe :

- Un modèle de compte utilisateur qui permettra de créer rapidement d'autres utilisateurs ayant les mêmes caractéristiques de profils (chemin de profil, script de démarrage, coordonnées de service)
- L'ensemble des utilisateurs appartenant au groupe.



 Arnauld BRIFFAUT	Utilisateur
 model_assis_DG	Utilisateur
 model_DG	Utilisateur
 Myriam ADA	Utilisateur

A.7. Convention de nommage des OU, groupes et utilisateurs :




OU : 1^{ère} lettre en majuscule, le reste en minuscule, pas d'accent, pas d'espace, deux mots doivent être séparés par un tiret bas. Des abréviations comme DAF ou SAV, en majuscule, peuvent être employées.

 DAF	Unité d'organisation
 Direction_generale	Unité d'organisation
 SAV	Unité d'organisation
 Service_A	Unité d'organisation
 Service_B	Unité d'organisation


Groupe : le nom d'un groupe commencera toujours par les lettres « group » en minuscule suivies d'un tiret bas et de la fonction/service.

 group_assis_DG	Groupe de sécurité - Global
 group_DG	Groupe de sécurité - Global

Utilisateur : son prénom sera écrit en minuscule avec la première lettre en majuscule suivi de son nom en majuscule. Ses identifiants de connexion seront la 1^{ère} lettre de son prénom suivi d'un point puis de son nom de famille

 Arnauld BRIFFAUT	Utilisateur
 model_assis_DG	Utilisateur
 model_DG	Utilisateur
 Myriam ADA	Utilisateur

Copier l'objet - Utilisateur ✕

 Créer dans : pizza.local/Employes/Direction_generale

Prénom : Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur :

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

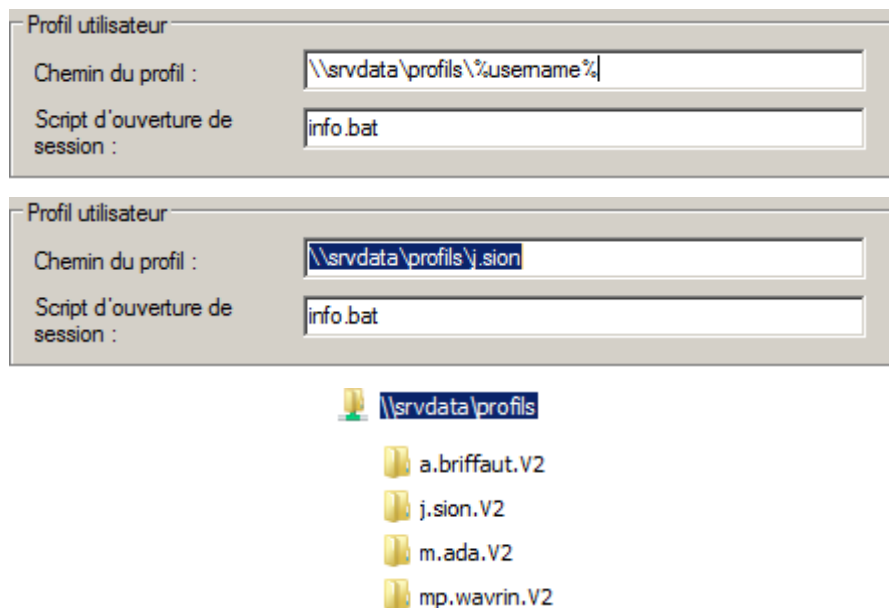
A.8. Profils itinérants

Un profil itinérant permet à un utilisateur de retrouver ses documents, ses paramètres et son environnement de travail (favoris Internet Explorer, arrière-plan du bureau, menu démarrer classique/normal, raccourcis), quelque soit l'ordinateur sur lequel il ouvre une session.

Il est possible d'effectuer une sauvegarde de ces profils sur un serveur distant afin d'éviter toute perte de documents. Lorsque les utilisateurs se connectent depuis un ordinateur Windows 7, le nom du profil sera automatiquement terminé par « .V2 ».

Les profils itinérants seront sauvegardés sur le serveur de fichier SRVDATA, sur une partition dédiée appelée « PROFILS ».

Le chemin UNC (Universal Naming Convention) des profils sera : <\\srvdata\profils>



A.9. VBScript

Pour faciliter la gestion de l'Active Directory, il est possible d'automatiser certaines tâches comme notamment la création d'unités d'organisations, de groupes et même d'utilisateurs.



L'automatisation de ces tâches peut se faire à l'aide d'un script codé en langage **VBscript** qui est un langage interprété et compréhensible par un ordinateur fonctionnant sous Windows. En effet sur ce dernier, il existe un interpréteur capable de comprendre le script et d'effectuer les actions demandées.

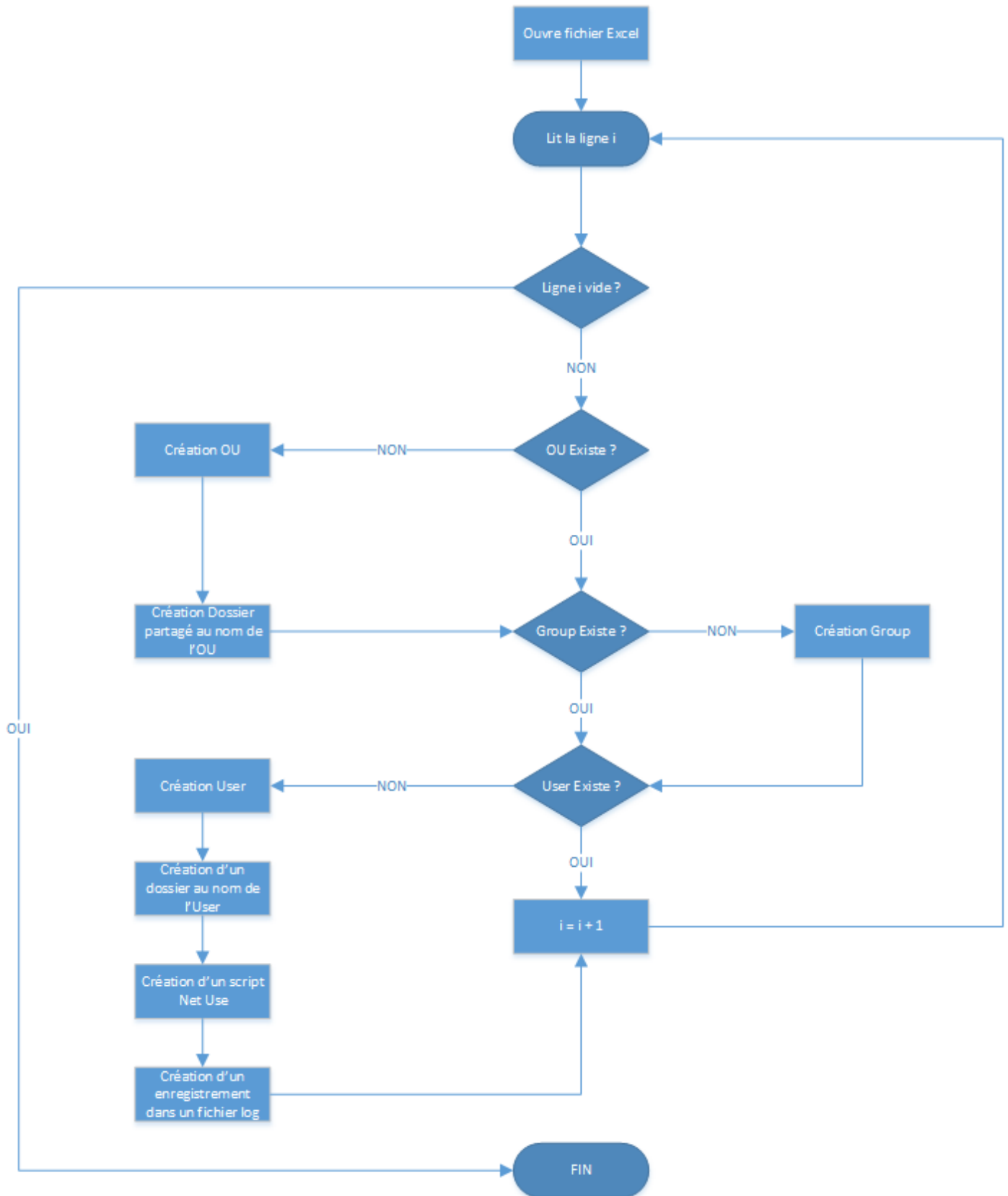
Le script que nous allons réaliser ouvrira un fichier Excel dans lequel seront répertoriées toutes les informations relatives aux collaborateurs (nom, prénom, service, fonction).

A la lecture de ces informations, le script créera automatiquement au sein de notre Active Directory les unités d'organisations, les groupes et les utilisateurs.

Il placera automatiquement les groupes dans les bonnes unités d'organisations, les utilisateurs dans les bons groupes et générera les scripts d'ouverture de session.

Ce script devra être capable de gérer les éventuels doublons pour ne pas créer deux unités d'organisations ou deux groupes identiques, ce qui provoquerait une erreur dans son exécution.

Voici un exemple d'Algorithme expliquant le fonctionnement de ce script :



Ainsi, à l'avenir à chaque arrivée d'un nouveau collaborateur, il suffira de renseigner le fichier Excel puis d'exécuter le script afin de créer automatiquement le compte de ce collaborateur et les droits associés.

Le fichier Excel sera stocké sur le serveur de fichier de l'entreprise, dans le répertoire de travail du service informatique.

Il aura la forme suivante :

Nom Complet	Prenom	Nom du compte	Description	Nom de l'O.U.	Compte de groupe
BRIFFAUT	Arnauld	a.briffaut	PDG	Direction_generale	group_DG
ADA	Myriam	m.ada	Assist DG	Direction_generale	group_assis_DG
WAVRIN	Marie-Paule	mp.wavrin	Resp. RH	RH	group_resp_RH
DUMONT	Gilbert	g.dumont	Resp. Compta	Compta	group_resp_compta
SION	John	j.sion	Resp. Info	Informatique	group_resp_informatique
LEVEQUE	Kévin	k.leveque	Tech. Info	Informatique	group_info
Kovacic	Karyne	k.kovacic	Tech. Info	Informatique	group_info
REGNAULT	Franck	f.regnault	DAF	DAF	group_DAF
MALLET	Jean-marie	jm.mallet	Resp. SAV	SAV	group_resp_SAV
LAPORTE	Danielle	d.laporte	Assist SAV	SAV	group_assis_SAV
PACY	François	f.pacy	Resp. Service A	Service A	group_resp_service_A
BEZIAT	Hélène	h.beziat	Tech. Service A	Service A	group_service_A
ELLA	Anne	a.ella	Tech. Service A	Service A	group_service_A
AYO	Marie	m.ayo	Tech. Service A	Service A	group_service_A
ACIEN	Perrine	p.acien	Tech. Service A	Service A	group_service_A
BOILEAU	Martine	m.boileau	Resp. Service B	Service B	group_resp_service_B
DESCOURS	Isabelle	i.descours	Tech. Service B	Service B	group_service_B
FOUQUAY	Jean	j.fouquay	Tech. Service B	Service B	group_service_B
DARLOT	Marc	m.darlot	Tech. Service B	Service B	group_service_B
RENARD	José	j.renard	Tech. Service B	Service B	group_service_B

B. Le service DNS

B.1. Intérêt d'un service DNS

Les machines sont identifiées et communiquent entre elles sur le réseau grâce à leur adresse IP qui est une série de plusieurs chiffres difficiles à retenir.

Pour faciliter cette identification, un service **DNS (Domain Name System)** peut être mis en place. Il s'agit d'un système qui établit une correspondance entre les adresses IP et les noms des machines.

Un service DNS permet donc d'identifier une machine sur le réseau grâce à :

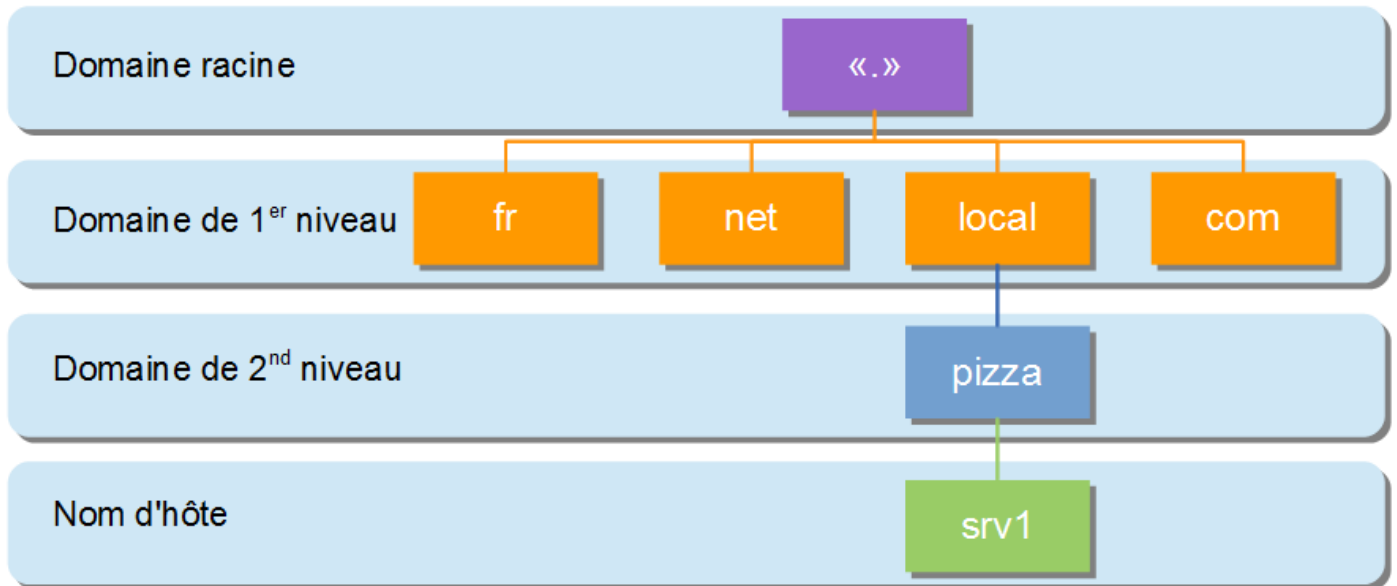
- son nom, on parle alors de **résolution de nom**.
- son adresse IP, on parle alors de **résolution inverse**.

B.2. Fonctionnement d'un DNS

B.2.1. Nommage des machines

Comme indiqué précédemment, un service DNS associe une adresse IP à un nom de machine et inversement.

Le nommage des machines doit répondre à une structure précise qui peut être symbolisée sous la forme d'une arborescence renversée.



Le point d'origine, appelé racine (ou « root » en anglais), est représenté par un **point** « . ».

Puis vient le 1^{er} niveau de domaine, ici ce sera « **local** ».

Ensuite intervient le 2^{ème} niveau de domaine ou le sous-domaine, ici « **pizza** ».

L'assemblage de ces 3 éléments séparés par un point forme ce que l'on appelle le **suffixe DNS**, ici donc : « **pizza.local.** »

L'association de ce suffixe DNS avec le nom d'un ordinateur, appelé aussi **nom d'hôte**, forme ce que l'on appelle le **FQDN** pour « **Fully Qualified Domain Name** ».

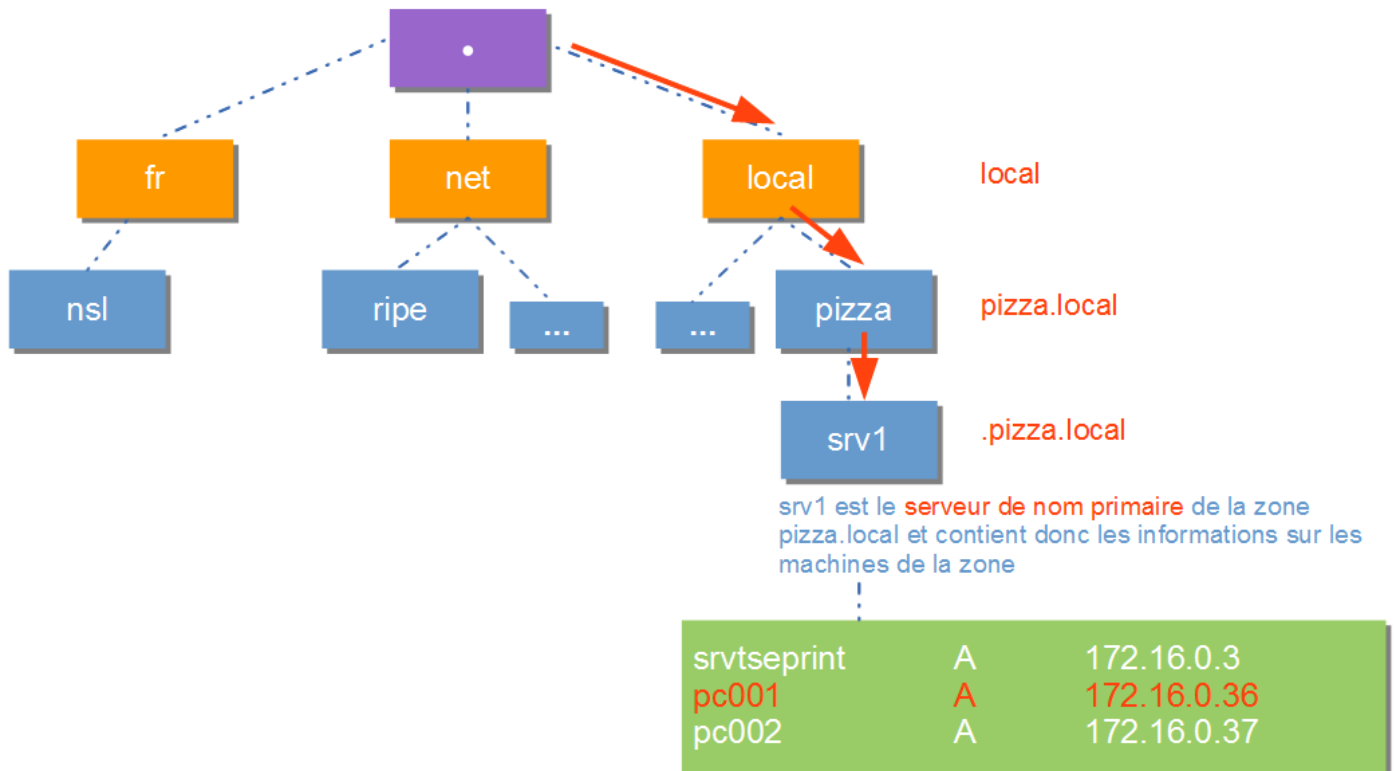
Ainsi pour le serveur 1, dont le nom d'hôte est **srv1**, le nommage « **srv1.pizza.local.** » correspond à la dénomination exacte de cette machine au sein du réseau, il s'agit de son **FQDN**.

B.2.2. Résolution de nom

Afin de trouver l'IP de la machine au sein du réseau, il suffira de lire son **FQDN** de la droite vers la gauche jusqu'à atteindre le nom d'hôte.

À ce stade, un **serveur de nom de domaine** se chargera d'indiquer l'adresse IP car lui seul connaît l'association : nom d'hôte ⇔ adresse IP.

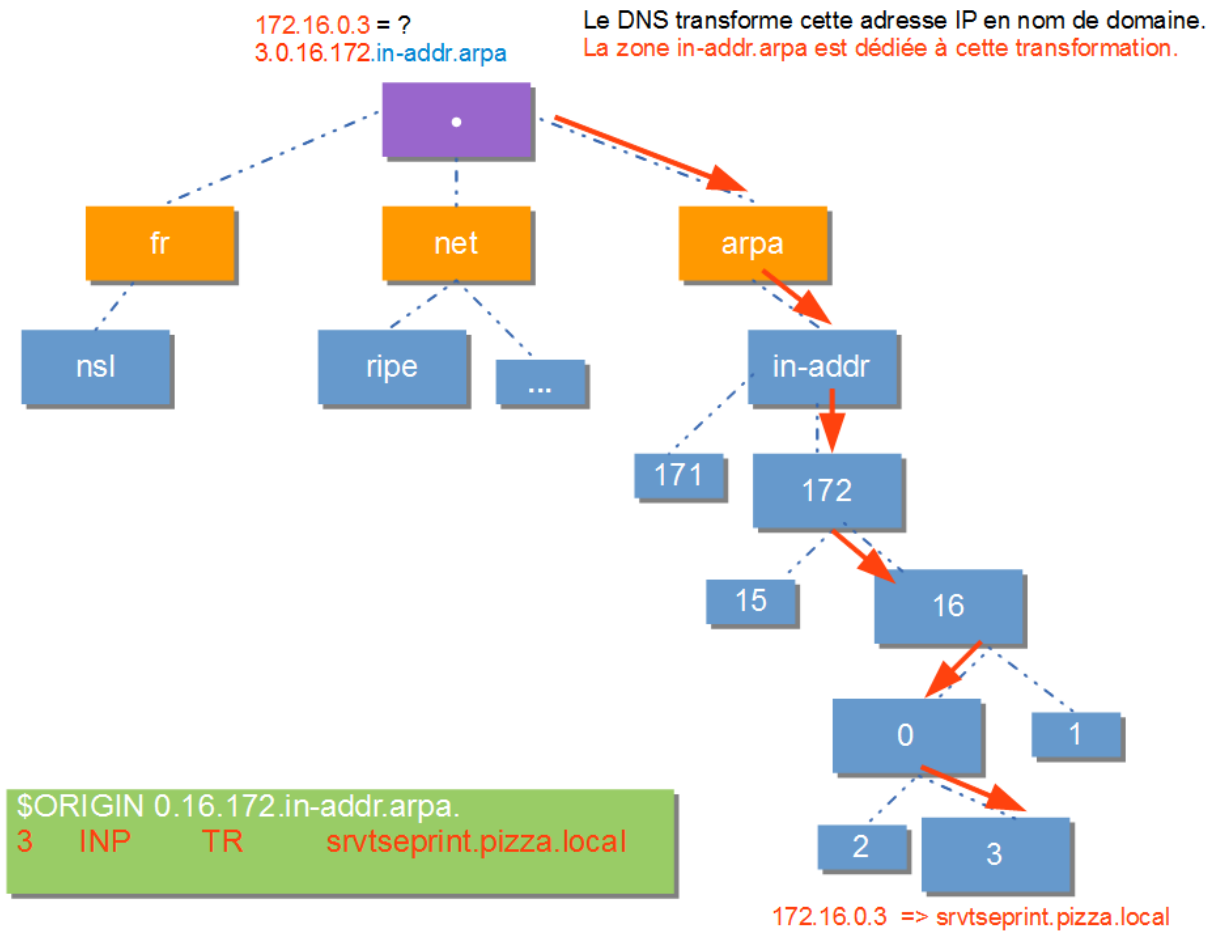
Exemple pour la résolution de la machine dont le **FQDN** est **pc001.pizza.local**



B.2.3. Résolution de nom inverse

La résolution inverse permet de retrouver le **FQDN** d'une machine à partir de son adresse IP. Pour cela la résolution inverse s'appuie aussi sur un système en arborescence qui a pour origine le domaine particulier « **in-addr.arpa** ». Ce domaine permet la transformation de l'adresse IP en nom de domaine.

Exemple je dois retrouver le **FQDN** de l'adresse IP 172.16.0.3



B.3. Enregistrement de ressources (SOA, NS, A, PTR) et Zones

Un service DNS peut être divisé en plusieurs zones. Une zone stocke l'ensemble des informations relatives à un domaine (adresses IP du domaine, nom du serveur de nom de domaine, nom des hôtes, etc.)

Ces informations sont appelées aussi « Entrées » ou « Enregistrements »

Il existe plusieurs types d'enregistrements :

- l'enregistrement de type SOA (Start Of Authority)
- l'enregistrement de type NS (Name Server)
- l'enregistrement de type A (Address)
- l'enregistrement de type PTR (Pointer Record)

Nom	Type	Données
(identique au dossier parent)	Source de nom (SOA)	[36], srv1.pizza.local,
(identique au dossier parent)	Serveur de noms (NS)	srv1.pizza.local.
(identique au dossier parent)	Hôte (A)	172.16.0.1
PC001	Hôte (A)	172.16.0.36
srv1	Hôte (A)	172.16.0.1
srvdata	Hôte (A)	172.16.0.3

B.3.1. Enregistrement de type SOA (Start Of Authority)

Cet enregistrement est obligatoire au début de toutes les zones DNS. Il permet d'indiquer le serveur de nom maître (primaire).

Il désigne l'autorité (Start Of Authority) ou le responsable de la zone dans la hiérarchie DNS.

Il contient des informations qui vont notamment aider les autres serveurs DNS à faire leur mise en cache. Il est possible, entre autre, de suggérer une fréquence de rafraîchissement.

C'est notamment sur cet enregistrement SOA que va baser la réplication entre serveurs DNS.

B.3.2. Enregistrement de type NS (Name Server)

À chaque enregistrement NS correspond un serveur de nom de domaine. Ici notre serveur de nom est [srv1.pizza.local](#), c'est cette entrée que l'on retrouvera dans l'enregistrement NS.

B.3.3. Enregistrement de type A (Address)

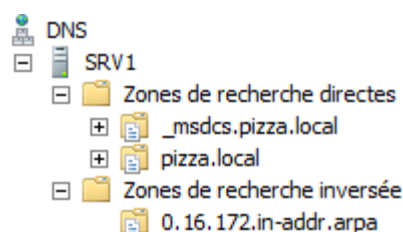
L'enregistrement de type A fait correspondre un nom d'hôte à une adresse IPv4 de 32 bit distribués sur quatre octets ex : 172.16.0.0

B.3.4. Enregistrement de PTR (Pointer Record)

Un enregistrement PTR (Pointer Record) associe une adresse IP à un nom d'hôte. Un enregistrement PTR s'appelle aussi enregistrement DNS inversé puisqu'un PTR convertit une adresse IP en un nom.

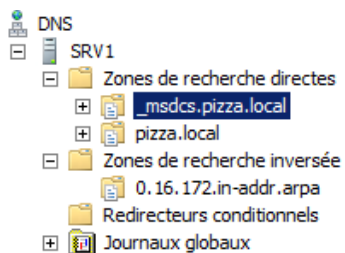
B.3.4. Nombre de Zones

Nous avons deux zones, [une zone de recherche directe](#), qui permet de trouver l'adresse IP d'un ordinateur à partir de son FQDN et [une zone de recherche inverse](#) qui permet de trouver le nom d'un ordinateur à partir de son adresse IP.



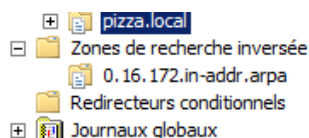
La zone de recherche directe est divisée en deux sous-domaines :

- le sous-domaine « **_msdcs** » qui rassemble les enregistrements DNS spécifiques aux services d'annuaires Microsoft, principalement les enregistrements des deux serveurs de noms (NS) et le SOA.



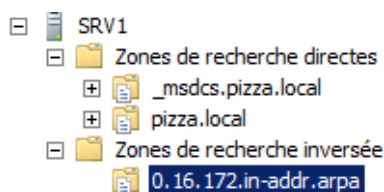
Nom	Type	Données
dc		
domains		
gc		
pdcc		
(identique au dossier parent)	Source de nom (SOA)	[36], srv1.pizza.local.
(identique au dossier parent)	Serveur de noms (NS)	srv2.pizza.local.
(identique au dossier parent)	Serveur de noms (NS)	srv1.pizza.local.
ced08ad7-e5ee-4c05-8fdb-2f...	Alias (CNAME)	srv2.pizza.local.
de881e0b-be62-443f-90a3-f0...	Alias (CNAME)	srv1.pizza.local.

- le sous-domaine « **pizza** » qui rassemble tous les enregistrements relatifs au domaine pizza (SOA, A, NS)



_udp		
DomainDnsZones		
ForestDnsZones		
(identique au dossier parent)	Source de nom (SOA)	[105], srv1.pizza.local.,
(identique au dossier parent)	Serveur de noms (NS)	srv2.pizza.local.
(identique au dossier parent)	Serveur de noms (NS)	srv1.pizza.local.
(identique au dossier parent)	Hôte (A)	172.16.0.1
(identique au dossier parent)	Hôte (A)	172.16.0.2
PC001	Hôte (A)	172.16.0.49
srv1	Hôte (A)	172.16.0.1
SRV2	Hôte (A)	172.16.0.2
srvdata	Hôte (A)	172.16.0.3
srvtseprint	Hôte (A)	172.16.0.4
test1	Hôte (A)	172.16.0.50
test2	Hôte (A)	172.16.0.51

La zone de recherche inverse renfermera le sous domaine **0.16.172.in-addr.arpa** dans lequel on trouvera les enregistrements PTR principalement.



(identique au dossier parent)	Source de nom (SOA)	[2], srv1.pizza.local.,
(identique au dossier parent)	Serveur de noms (NS)	srv1.pizza.local.
172.16.0.3	Pointeur (PTR)	srvdata.pizza.local.

C. La réplication des services Active Directory et DNS

C.1. Intérêt de la réplication

Nous allons installer un second serveur ([srv2](#)) sur lequel seront répliqués les services Active Directory et DNS.

La réplication est un processus qui permet de synchroniser les données entre contrôleurs de domaine afin d'assurer le bon fonctionnement d'Active Directory.

En effet, grâce à la réplication, l'intégrité et la cohérence des données stockées dans la base d'annuaire Active Directory est continuellement maintenue et les modifications sont rapidement mises à jour sur l'ensemble des contrôleurs du domaine.

Cela permet d'avoir une forte tolérance de pannes car tous les contrôleurs de domaine disposent de la même information.

C.2. Fonctionnement de la réplication

Une réplication intervient lorsque la base d'annuaire Active Directory sur un contrôleur de domaine est modifiée. Les modifications pouvant donner lieu à une réplication sont les suivantes :

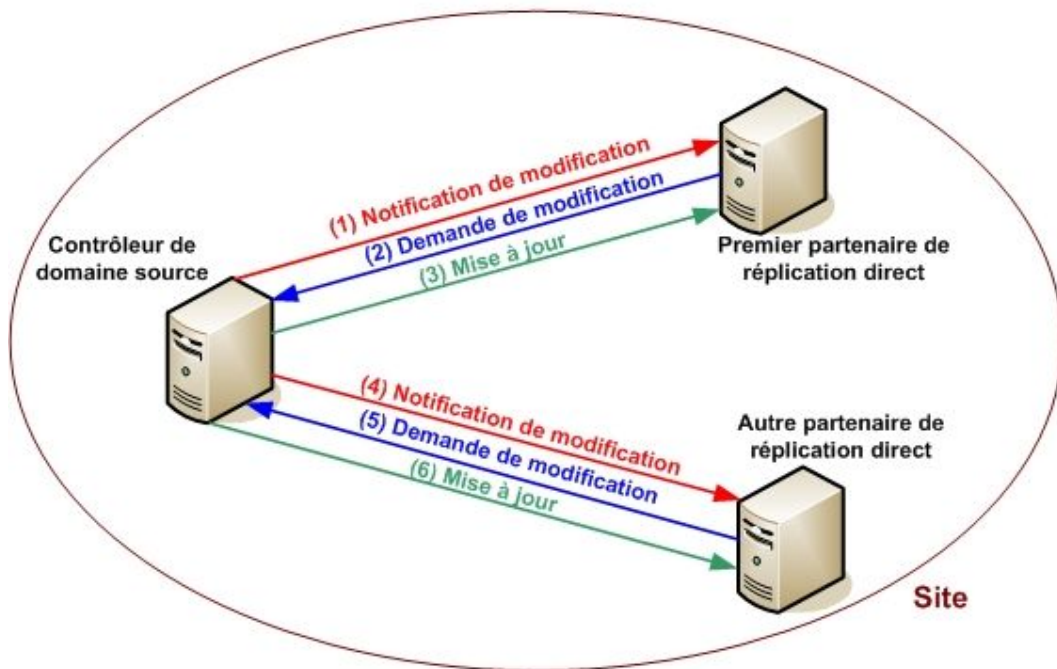
- Ajout d'un objet à Active Directory (ex. : création d'un compte utilisateur).
- Modification des valeurs d'attribut d'un objet (ex. : modification du prénom d'un utilisateur).
- Modification du nom d'un conteneur d'objet (ex. : modification du nom d'une unité d'organisation).
- Suppression d'un objet de l'annuaire Active Directory (ex. : suppression d'un compte utilisateur).

Suite à une modification de la base d'annuaire sur un contrôleur de domaine, un temps de latence (par défaut 5 minutes) est observé avant que ce dernier envoie un message de notification de modification aux autres contrôleurs de domaine (partenaires de réplication directe) du même site.

Lorsque les partenaires de réplication reçoivent la notification, ils demandent les modifications auprès du contrôleur de domaine.

Le contrôleur de domaine, à partir duquel la mise à jour d'origine a eu lieu, envoie alors les modifications à ses partenaires de réplication.

Il est à noter qu'après le temps de latence de 5 minutes, tous les partenaires de réplication ne sont pas notifiés en même temps : un des partenaires de réplications directs sera notifié en premier de la modification puis les autres seront notifiés à leurs tours à intervalles de 30 secondes. Cela permet de ne pas saturer le contrôleur de domaine source lors de demandes de mises à jour simultanées de la part de plusieurs partenaires de réplication.



Exemple du fonctionnement de la réplication avec 3 serveurs

Lors d'une modification pouvant affecter la sécurité, comme par exemple la désactivation d'un compte utilisateur, aucun temps de latence n'est observé. Dans ce cas, une réplication urgente est déclenchée (la notification de modification et la duplication sont appliquées immédiatement).

Si aucune modification n'est survenue pendant une heure, un processus de réplication est déclenché par les contrôleurs de domaine, afin de s'assurer que chaque réplique possède bien une copie identique de la base d'annuaire Active Directory.

C.3. Transfert de Zone

L'un des nombreux mécanismes disponibles pour répliquer les bases de données distribuées contenant les données DNS au travers d'un ensemble de serveurs DNS est le transfert de zone.

Le transfert de zone fonctionne sur une transaction en mode client-serveur. Le client (dit serveur secondaire) requiert les informations d'une partie de la base de données distribuée (zone) auprès d'un serveur (le maître) qui les fournit.

Le transfert de zone débute par la vérification de l'enregistrement DNS SOA de la zone considérée.

L'un des paramètres utilisés lors du processus de transfert de zone est le numéro de série (ou serial number) qui détermine la version des données.

Nom	Type	Données
(identique au dossier parent)	Source de nom (SOA)	[36] srv1.pizza.local.

Durant cette vérification, si le numéro de série (la version) de la zone du maître est identique (ou plus petit) à celui de la dernière copie de la zone en possession du serveur secondaire, le transfert s'arrête car aucun changement n'a eu lieu.

Si cette version est plus récente (numéro de série de la zone du maître plus grand que celui de la copie de zone du serveur secondaire), le serveur secondaire effectue la demande de transfert de zone en tant que telle.

Avant le transfert de zone, les deux contrôleurs de domaine ne sont pas synchronisés :

Les zones « _msdsc » n'ont pas le même nombre de serveur NS :

SRV	Nom	Type	Données
SRV1	dc		
	domains		
	gc		
	pdcc		
SRV1	(identique au dossier parent)	Source de nom (SOA)	[21] srv1.pizza.local.
	(identique au dossier parent)	Serveur de noms (NS)	srv1.pizza.local.
SRV2	dc		
	domains		
	gc		
	pdcc		
	(identique au dossier parent)	Source de nom (SOA)	[21] srv2.pizza.local.
	(identique au dossier parent)	Serveur de noms (NS)	srv1.pizza.local.
(identique au dossier parent)	Serveur de noms (NS)	srv2.pizza.local.	

Les zones « pizza.local » n'ont pas le même nombre de serveur NS, ni le même numéro d'enregistrement SOA :

SRV	Nom	Type	Données
SRV1	_msdcs		
	_sites		
	_tcp		
	_udp		
	DomainDnsZones		
	ForestDnsZones		
	(identique au dossier parent)	Source de nom (SOA)	[82] srv1.pizza.local
	(identique au dossier parent)	Serveur de noms (NS)	srv1.pizza.local.

		<table border="0"> <tr> <td>(identique au dossier parent)</td> <td>Source de nom (SOA)</td> <td>[81], srv2.pizza.local.</td> </tr> <tr> <td>(identique au dossier parent)</td> <td>Serveur de noms (NS)</td> <td>srv1.pizza.local.</td> </tr> <tr> <td>(identique au dossier parent)</td> <td>Serveur de noms (NS)</td> <td>srv2.pizza.local.</td> </tr> </table>	(identique au dossier parent)	Source de nom (SOA)	[81], srv2.pizza.local.	(identique au dossier parent)	Serveur de noms (NS)	srv1.pizza.local.	(identique au dossier parent)	Serveur de noms (NS)	srv2.pizza.local.
(identique au dossier parent)	Source de nom (SOA)	[81], srv2.pizza.local.									
(identique au dossier parent)	Serveur de noms (NS)	srv1.pizza.local.									
(identique au dossier parent)	Serveur de noms (NS)	srv2.pizza.local.									

Après le transfert de zone (voir procédure), les deux contrôleurs de domaine sont synchronisés, le nombre de serveurs NS et les numéros d'enregistrement SOA sont identiques pour toutes les zones :

		<table border="0"> <tr> <td>(identique au dossier parent)</td> <td>Source de nom (SOA)</td> <td>[24], srv1.pizza.local.</td> </tr> <tr> <td>(identique au dossier parent)</td> <td>Serveur de noms (NS)</td> <td>srv1.pizza.local.</td> </tr> <tr> <td>(identique au dossier parent)</td> <td>Serveur de noms (NS)</td> <td>srv2.pizza.local.</td> </tr> </table>	(identique au dossier parent)	Source de nom (SOA)	[24], srv1.pizza.local.	(identique au dossier parent)	Serveur de noms (NS)	srv1.pizza.local.	(identique au dossier parent)	Serveur de noms (NS)	srv2.pizza.local.
(identique au dossier parent)	Source de nom (SOA)	[24], srv1.pizza.local.									
(identique au dossier parent)	Serveur de noms (NS)	srv1.pizza.local.									
(identique au dossier parent)	Serveur de noms (NS)	srv2.pizza.local.									

		<table border="0"> <tr> <td>(identique au dossier parent)</td> <td>Source de nom (SOA)</td> <td>[24], srv2.pizza.local.</td> </tr> <tr> <td>(identique au dossier parent)</td> <td>Serveur de noms (NS)</td> <td>srv2.pizza.local.</td> </tr> <tr> <td>(identique au dossier parent)</td> <td>Serveur de noms (NS)</td> <td>srv1.pizza.local.</td> </tr> </table>	(identique au dossier parent)	Source de nom (SOA)	[24], srv2.pizza.local.	(identique au dossier parent)	Serveur de noms (NS)	srv2.pizza.local.	(identique au dossier parent)	Serveur de noms (NS)	srv1.pizza.local.
(identique au dossier parent)	Source de nom (SOA)	[24], srv2.pizza.local.									
(identique au dossier parent)	Serveur de noms (NS)	srv2.pizza.local.									
(identique au dossier parent)	Serveur de noms (NS)	srv1.pizza.local.									

		<table border="0"> <tr> <td>(identique au dossier parent)</td> <td>Source de nom (SOA)</td> <td>[87], srv1.pizza.local.</td> </tr> <tr> <td>(identique au dossier parent)</td> <td>Serveur de noms (NS)</td> <td>srv1.pizza.local.</td> </tr> <tr> <td>(identique au dossier parent)</td> <td>Serveur de noms (NS)</td> <td>srv2.pizza.local.</td> </tr> </table>	(identique au dossier parent)	Source de nom (SOA)	[87], srv1.pizza.local.	(identique au dossier parent)	Serveur de noms (NS)	srv1.pizza.local.	(identique au dossier parent)	Serveur de noms (NS)	srv2.pizza.local.
(identique au dossier parent)	Source de nom (SOA)	[87], srv1.pizza.local.									
(identique au dossier parent)	Serveur de noms (NS)	srv1.pizza.local.									
(identique au dossier parent)	Serveur de noms (NS)	srv2.pizza.local.									

		<table border="0"> <tr> <td>(identique au dossier parent)</td> <td>Source de nom (SOA)</td> <td>[87], srv2.pizza.local.</td> </tr> <tr> <td>(identique au dossier parent)</td> <td>Serveur de noms (NS)</td> <td>srv1.pizza.local.</td> </tr> <tr> <td>(identique au dossier parent)</td> <td>Serveur de noms (NS)</td> <td>srv2.pizza.local.</td> </tr> </table>	(identique au dossier parent)	Source de nom (SOA)	[87], srv2.pizza.local.	(identique au dossier parent)	Serveur de noms (NS)	srv1.pizza.local.	(identique au dossier parent)	Serveur de noms (NS)	srv2.pizza.local.
(identique au dossier parent)	Source de nom (SOA)	[87], srv2.pizza.local.									
(identique au dossier parent)	Serveur de noms (NS)	srv1.pizza.local.									
(identique au dossier parent)	Serveur de noms (NS)	srv2.pizza.local.									

D. Scripts

D.1. Intérêt des scripts

Avoir plusieurs ordinateurs en réseau implique souvent la création de partages pour accéder aux ressources d'un autre PC. Si le groupe résidentiel de Windows facilite la connexion à ces dossiers, un réseau d'entreprise se gère différemment et les scripts ont tout leur intérêt pour que les utilisateurs se connectent automatiquement aux partages des serveurs auxquels ils ont accès.

La mise en place de scripts permet donc d'automatiser la connexion aux répertoires et ressources partagées de l'entreprise en fonction de chaque service.

D.2. Fonctionnement des scripts

Un script est un fichier batch portant l'extension « .bat ». C'est en fait une ligne (ou un ensemble de lignes) de commande ms-dos « codées » sous forme de fichier texte dont on a changé l'extension.

L'ouverture de ce fichier exécutera les commandes écrites dans ce fichier.

- Pour connecter un lecteur réseau, la commande ms-dos utilisée est :

```
net use X: \\nom de l'ordinateur\nom du partage
```

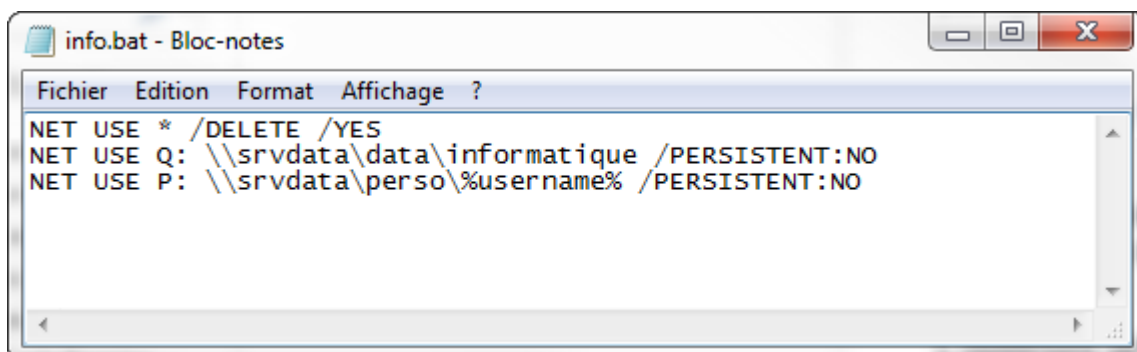
Où X: est la lettre de lecteur que vous souhaitez affecter à la ressource partagée.

- Pour déconnecter un lecteur, la commande utilisée est :

```
net use X: /delete
```

Où X: est la lettre de lecteur de la ressource partagée.

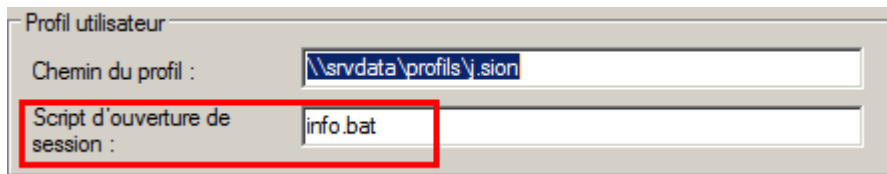
Voici un exemple de script :



```
info.bat - Bloc-notes
Fichier  Edition  Format  Affichage  ?
NET USE * /DELETE /YES
NET USE Q: \\srvdata\data\informatique /PERSISTENT:NO
NET USE P: \\srvdata\perso\%username% /PERSISTENT:NO
```

D.3. Sauvegarde des scripts

Dans l'Active Directory, les scripts sont déclarés pour chaque utilisateur au niveau de leur profil :



Profil utilisateur

Chemin du profil : \\srvdata\profils\j.sion

Script d'ouverture de session : info.bat

Le chemin par défaut de stockage de ces scripts se situe sur la partition système où est hébergé l'AD, ici :

```
C:\Windows\SYSTEM32\sysvol\pizza.local\scripts
```

Il est tout à fait possible de stocker ces scripts dans un autre répertoire, qui sera placé sur une autre partition que celle du système.

Ce répertoire pourra être sauvegardé par copie et envoyé vers un autre serveur, ou sur un disque externe par l'intermédiaire d'un logiciel de sauvegarde tel que Cobian Backup.

E. Le Service Terminal Serveur

E.1. Intérêt d'un Service Terminal Serveur

Les services Bureau à distance, anciennement Services Terminal Server (TSE), intègrent des technologies qui permettent aux utilisateurs d'accéder à des programmes Windows installés sur un serveur Hôte de session Bureau à distance, d'accéder à tout le Bureau Windows d'un serveur hôte de session Bureau à distance ou d'accéder à un ordinateur virtuel. Grâce aux services Bureau à distance, les utilisateurs peuvent accéder à un serveur Hôte de session Bureau à distance ou à un ordinateur virtuel à partir du réseau d'entreprise ou d'Internet.

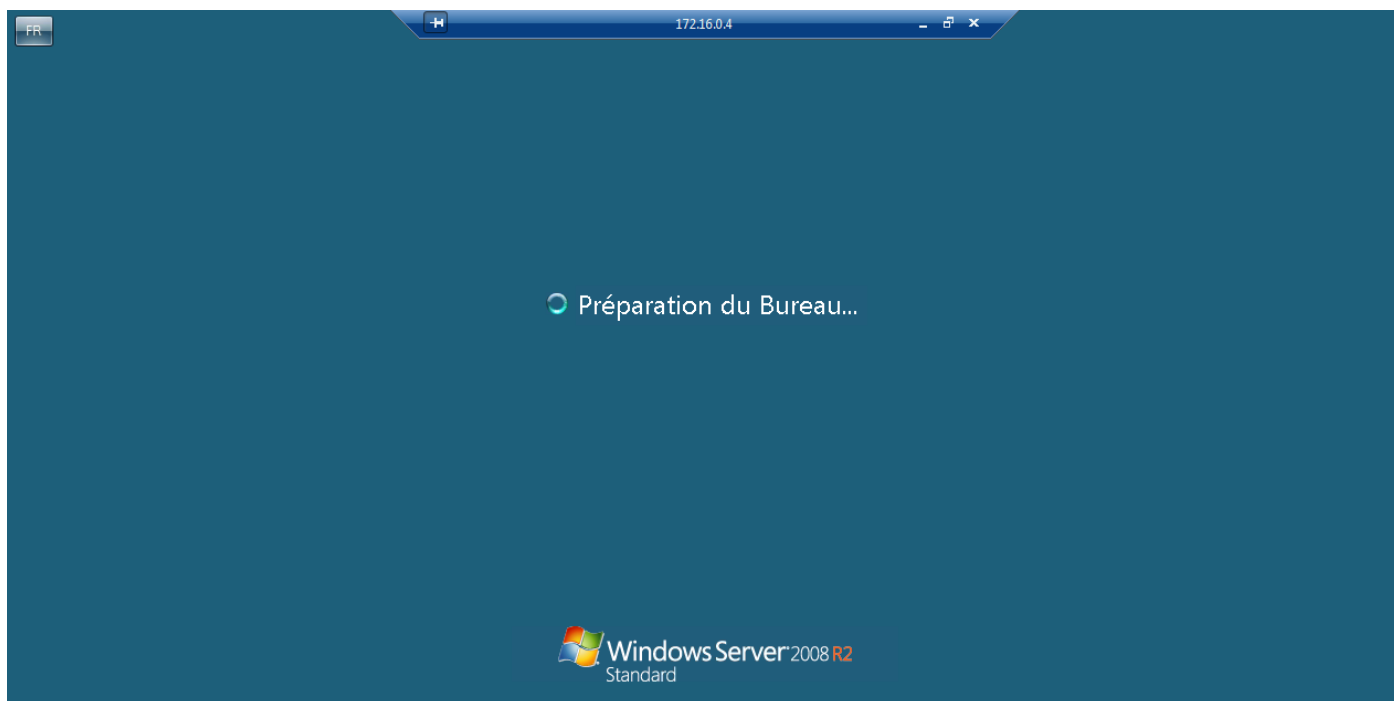
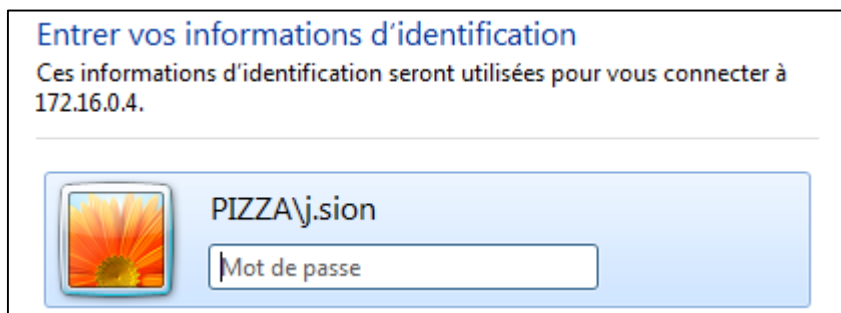
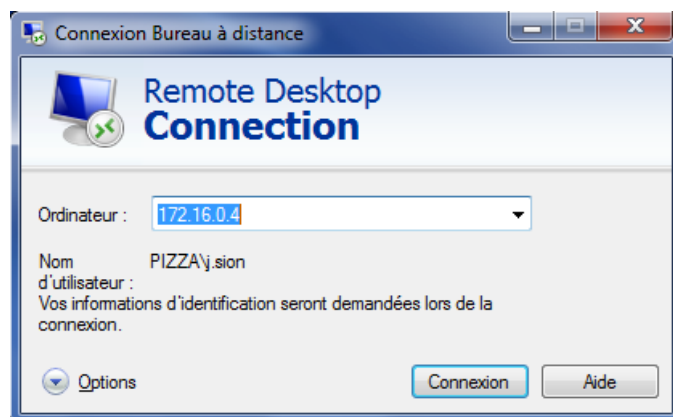
E.2. Fonctionnement d'un Service Terminal Serveur

Après l'installation du service terminal serveur, il faut procéder à une série d'étapes de configuration afin d'activer le service.

Parmi toutes ces étapes, on peut dégager 4 grandes étapes importantes :

- La création au sein de l'Active Directory d'un groupe d'utilisateurs autorisés à se connecter au bureau à distance.
- Autoriser sur le serveur TSE, au niveau de la stratégie locale, le groupe d'utilisateur du bureau à distance à ouvrir des sessions TSE.
- Autoriser ce même groupe, à ouvrir des connexions distantes dans les propriétés du serveur.
- Autoriser sur le poste client, les connexions distantes au niveau des propriétés de l'ordinateur.

Une fois ces 4 étapes importantes réalisées, un collaborateur pourra ouvrir une session de bureau à distance de la manière suivante :



F. Serveur d'impression

F.1. Intérêt d'un serveur d'impression











Un serveur d'impression et de numérisation de documents permet de centraliser les tâches de gestion des imprimantes et scanners réseau. Avec ce rôle, il est possible de recevoir des documents numérisés à partir de scanners réseau et d'acheminer les documents vers une ressource réseau partagée.

F.2. Convention de nommage des imprimantes

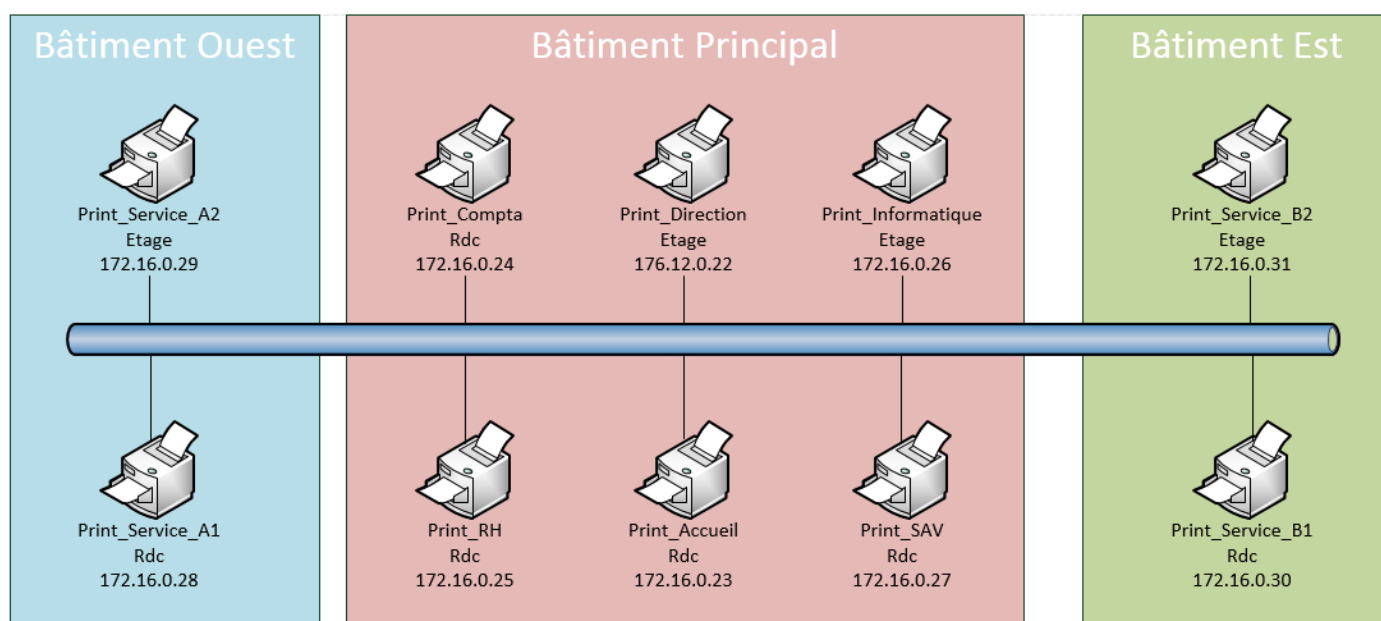
Le nom des imprimantes sera composé comme suit :

« **Print_nom_du_service** »

Par exemple : **Print_Accueil**, **Print_Direction**, **Print_Informatique**

-  Print_Accueil
-  Print_Compta
-  Print_Direction
-  Print_Informatique
-  Print_RH
-  Print_SAV
-  Print_Service_A1
-  Print_Service_A2
-  Print_Service_B1
-  Print_Service_B2

F.3. Organisation + implantation des imprimantes



G. GPO ou Stratégies de Groupe

G.1. Intérêt des GPO

Les stratégies de groupe (ou GPO pour Group Policy Object) sont des fonctions de gestion centralisée. Elles permettent la gestion des ordinateurs et des utilisateurs dans un environnement Active Directory.

Les stratégies de groupe incluent la gestion des ordinateurs déconnectés, la gestion des utilisateurs itinérants ou la gestion de la redirection des dossiers ainsi que la gestion des fichiers en mode déconnecté.

Bien que les stratégies de groupe soient régulièrement utilisées dans les entreprises, elles sont également utilisées dans les écoles ou dans les petites organisations pour restreindre les actions et les risques potentiels comme le verrouillage du panneau de configuration, la restriction de l'accès à certains dossiers, la désactivation de l'utilisation de certains exécutables, etc.

G.2 Mise en place des GPO

La mise en place d'une GPO respecte toujours un cycle de 3 phases :

1) La création et l'édition des stratégies de groupe :

Au travers de deux outils : le Group Policy Object Editor (gpedit.msc) et la Group Policy Management Console (gpmc.msc).

2) La liaison des stratégies de groupe :

La stratégie de groupe peut être liée à un site Active Directory, à un domaine ou à une unité d'organisation (UO).

3) L'application des stratégies de groupe :

Le poste client récupère la configuration de stratégie de groupe et l'applique en tenant compte des différents critères de filtres, de sécurité et d'héritages.

La liste des GPO mise en place dans le domaine sont les suivantes :

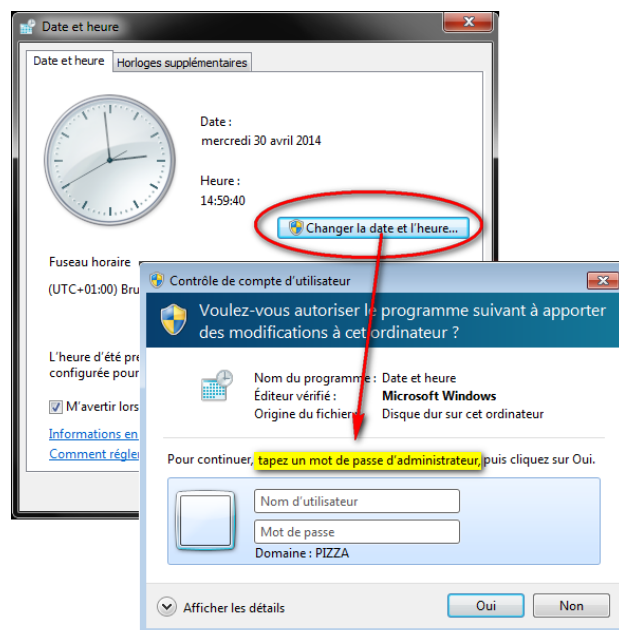
- Un Papier peint par service [Wallpaper_service_X](#)
- Interdiction d'installer des logiciels et de modifier l'heure système pour tous les services sauf Informatique et Direction : [Install_Soft_Disabled](#)
- Ports USB et lecteur CD désactivés sur les postes des services Produit A, B et SAV : [External_Drive_Disabled](#)
- Montage des différentes imprimantes par service : [Print_Service_X](#)

G.3. Résultats des GPO

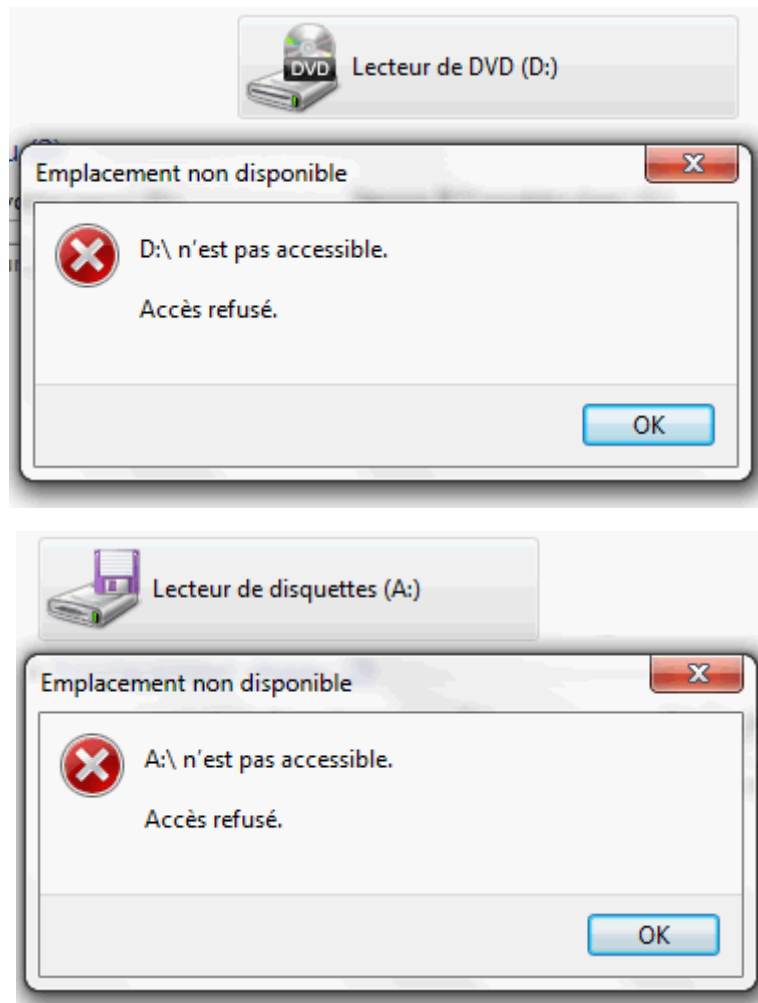
Un papier peint service :



Interdiction d'installer des logiciels et de modifier l'heure système :



Ports USB et lecteur CD désactivés :



Une imprimante dédiée par service :



VI – Installation et configuration des Serveurs Linux

A. Le service DHCP

A.1. Intérêt d'un DHCP

DHCP est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut et les adresses des serveurs de noms DNS.

A.2. Fonctionnement d'un DHCP

- L'ordinateur équipé de carte réseau, mais dépourvu d'adresse IP, envoie en diffusion Broadcast un datagramme (DHCP DISCOVER) qui s'adresse au port 67 de n'importe quel serveur à l'écoute sur ce port. Ce datagramme comporte entre autres l'adresse physique (MAC) du client.
- Tout serveur DHCP ayant reçu ce datagramme, s'il est en mesure de proposer une adresse sur le réseau auquel appartient le client, envoie une offre DHCP (DHCP OFFER) à l'attention du client (sur son port 68), identifié par son adresse physique. Cette offre comporte l'adresse IP du serveur, ainsi que l'adresse IP et le masque de sous-réseau qu'il propose au client. Il se peut que plusieurs offres soient adressées au client.
- Le client retient une des offres reçues (la première qui lui parvient), et diffuse sur le réseau un datagramme de requête DHCP (DHCP REQUEST). Ce datagramme comporte l'adresse IP du serveur et celle qui vient d'être proposée au client. Elle a pour effet de demander au serveur choisi l'assignation de cette adresse, l'envoi éventuel des valeurs des paramètres, et d'informer les autres serveurs qui ont fait une offre qui n'a pas été retenue.
- Le serveur DHCP élabore un datagramme d'accusé de réception (DHCP ACK pour acknowledgement) qui assigne au client l'adresse IP et son masque de sous-réseau, la durée du bail de cette adresse (dont découlent deux valeurs T1 et T2 qui déterminent le comportement du client en fin de bail), et éventuellement d'autres paramètres :
 - adresse IP de la passerelle par défaut,
 - adresses IP des serveurs DNS,

A.3. Étendue, exclusion, réservation, durée du bail

Une **étendue** représente la plage d'adresses IP qui peut être distribuée par le serveur DHCP à l'ensemble des postes clients au sein du réseau local.

L'adresse réseau retenue étant 172.16.0.0 /16, la plage d'adresses IP distribuable va de 172.16.0.1 à 172.16.255.254.

Compte tenu du peu de machines composant le parc actuellement, la dernière adresse allouée dynamiquement sera 172.16.0.254.

Au sein de cette plage, certaines adresses IP ne seront pas distribuées dynamiquement par le serveur DHCP, on parle alors d'**exclusion**.

Ce sera le cas pour les adresses IP des serveurs, des imprimantes et de l'ensemble des appareils actifs tels que les switch et routeurs. Ici nous excluons les 30 premières adresses IP, c'est-à-dire de 172.16.0.1 à 172.16.0.32.

Ensuite parmi les adresses distribuées dynamiquement, il sera parfois utile de toujours allouer la même adresse IP à une station de travail précise. On parle alors de **réservation**.

Lors d'une réservation, on indique au serveur DHCP, l'adresse MAC du poste client pour laquelle on souhaite que le serveur DHCP fournisse toujours la même adresse.

Enfin, pour des raisons d'optimisation des ressources réseau, les adresses IP délivrées dynamiquement par le serveur DHCP sont distribuées avec une date de début et une date de fin de validité. C'est ce qu'on appelle un **bail**.

Ici, la durée du bail sera définie par défaut, soit 8 jours.

A.4. Tolérance de panne

Pour parer à une éventuelle panne, il peut être judicieux de mettre en place un second serveur DHCP qui prendrait le relais du 1^{er} serveur en cas de défaillance de ce dernier.

En fonctionnement normal, il coexistera donc deux serveurs DHCP. Pour éviter un conflit d'adresse IP, la plage d'adresse IP allouées par le 2^{ème} serveur DHCP sera différente du 1^{er}, ici de 172.16.1.1 à 172.16.1.254.

De plus, le 1^{er} serveur DHCP sera déclaré comme serveur DHCP « autoritaire », c'est-à-dire que tant que ce serveur est en fonction, lui seul est habilité à distribuer des adresses IP.

A.5. Installation et configuration

Le serveur DHCP retenu pour nos serveurs tournant sous la distribution Linux DEBIAN est `isc-dhcp-server`.

L'installation se fait via la commande classique :

```
root# apt-get install isc-dhcp-server
```

Le fichier de configuration d'un serveur DHCP s'appelle /etc/dhcp/dhcpd.conf. Il suffit de l'éditer avec un éditeur de texte pour renseigner les paramètres de notre réseau.

Voici un exemple de fichier de configuration d'un serveur DHCP sous Linux Debian : dhcpd.conf

```
ddns-update-style none;

# on indique le nom du domaine
option domain-name "pizza.local";

# on précise l'adresse IP ou le nom du serveur de noms
option domain-name-servers srv1.pizza.local;

#on renseigne la durée minimale et maximale des baux
default-lease-time 600;
max-lease-time 7200;

# on indique que c'est ce serveur qui sera "autoritaire"
authoritative;

log-facility local7;

# on indique l'adresse réseau, le masque et la plage d'adresse a distribuer
subnet 172.16.0.0 netmask 255.255.0.0 {
    range 172.16.0.33 172.16.0.254;
    option routers srv1.pizza.local;
}

# on fait une réservation, en attribuant à une adresse mac une adresse IP
host print {
    hardware ethernet 00:0c:29:d4:83:91;
    fixed-address 172.16.0.36;
}
```

Exemple d'adressage d'IP dynamique :

Un poste client configuré en adresse IP dynamique :

Obtenir une adresse IP automatiquement

Utiliser l'adresse IP suivante :

Adresse IP :

Masque de sous-réseau :

Passerelle par défaut :

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré :

Serveur DNS auxiliaire :

Son adresse IP attribuée par le serveur est :

```
C:\Users\j.sion>ipconfig
```

Configuration IP de Windows

Carte Ethernet Connexion au réseau local :

```
Suffixe DNS propre à la connexion. . . : pizza.local
Adresse IPv4. . . . . : 172.16.0.21
Masque de sous-réseau. . . . . : 255.255.0.0
Passerelle par défaut. . . . . : 172.16.0.1
```

On libère l'adresse IP :

```
C:\Users\j.sion>ipconfig /release
```

Configuration IP de Windows

Carte Ethernet Connexion au réseau local :

```
Suffixe DNS propre à la connexion. . . :
Passerelle par défaut. . . . . :
```

On redemande une nouvelle adresse au serveur DHCP

```
C:\Users\j.sion>ipconfig /renew
```

Configuration IP de Windows

Carte Ethernet Connexion au réseau local :

```
Suffixe DNS propre à la connexion. . . : pizza.local
Adresse IPv4. . . . . : 172.16.0.21
Masque de sous-réseau. . . . . : 255.255.0.0
Passerelle par défaut. . . . . : 172.16.0.1
```

Exemple de réservation d'adresse IP :

On note l'adresse mac du poste client dont on souhaite réserver l'adresse IP

```
Adresse physique . . . . . : 00-0c-29-d4-83-91
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv4. . . . . : 172.16.0.21<préféré>
```

On renseigne cette adresse dans le fichier de configuration du serveur DHCP (dhcpd.conf)

```
host j.sion {
hardware ethernet 00:0c:29:d4:83:91;
fixed-address 172.16.0.49;
}
```

On remarque que le poste client prend cette adresse IP

```
C:\Users\j.sion>ipconfig /renew
```

Configuration IP de Windows

Carte Ethernet Connexion au réseau local :

```
Suffixe DNS propre à la connexion. . . : pizza.local  
Adresse IPv4. . . . . : 172.16.0.49  
Masque de sous-réseau. . . . . : 255.255.0.0  
Passerelle par défaut. . . . . : 172.16.0.1
```

B. Le serveur de fichiers Samba (partage de fichiers interne)

B.1. Intérêt d'un serveur de fichiers

Un serveur de fichiers permet de partager des données à travers un réseau. Le terme désigne souvent l'ordinateur (serveur) hébergeant le service applicatif. Il possède généralement une grande quantité d'espace disque où sont déposés des fichiers. Les utilisateurs peuvent ensuite les récupérer au moyen d'un protocole de partage de fichier (par exemple le protocole SMB Server Message Block)

Un serveur de fichiers propose de nombreux avantages. Par exemple :

- Si le serveur met en œuvre un protocole de sécurisation des données de type RAID ou de sauvegarde régulière par un système d'archivage (généralement sur bande), les données peuvent être davantage à l'abri d'une destruction que lorsque le disque dur d'un ordinateur local devient défectueux. En outre, le coût est relativement faible.
- Dans le milieu professionnel, il peut exister un lecteur réseau commun à toute l'entreprise, un autre spécifique à un service ou un projet, et un « privé » où seul l'utilisateur peut se connecter.

Notre serveur de fichier étant hébergé sur une solution Linux, nous déploieront un serveur de type SAMBA pour partager les ressources informatiques de l'entreprise.

Samba est un logiciel d'interopérabilité qui permet à des ordinateurs sous Linux de mettre à disposition des imprimantes et des fichiers dans des réseaux Windows, en mettant en œuvre le protocole SMB de Microsoft Windows.

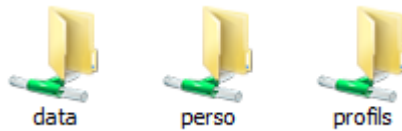
Samba donne donc la possibilité aux ordinateurs Windows d'accéder aux imprimantes et aux fichiers des ordinateurs Linux en permettant aux serveurs Linux de se substituer à des serveurs Windows.

B.2. Arborescence du serveur de fichier

Notre serveur de fichiers stockera sur 3 partitions distinctes du système d'exploitation, 3 types de données :

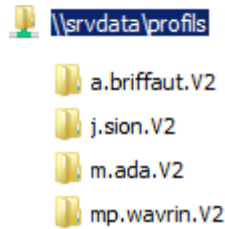
- Les profils itinérants des utilisateurs, dans un dossier racine appelé « ./profils »
- Les répertoires personnels des utilisateurs, dans un dossier racine appelé « ./perso »

- Les données et fichiers interne de l'entreprise, dans dossier racine appelé « « ./data » »



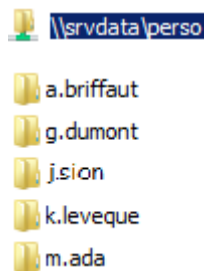
Arborescence du dossier profil :

Dans ce répertoire, on trouve les profils itinérants des utilisateurs. Ces répertoires sont créés automatiquement à la 1^{ère} connexion d'un utilisateur. La mention « .V2 » à la fin d'un nom d'utilisateur indique qu'il se connecte à partir d'un poste client équipé de Windows 7.



Arborescence du dossier perso :

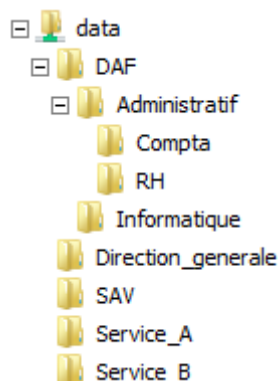
Dans ce répertoire, on trouve les dossiers personnels des utilisateurs. Ces répertoires sont créés automatiquement à la 1^{ère} connexion d'un utilisateur.



Arborescence du dossier data :

Dans ce répertoire, on trouvera l'ensemble des dossiers et fichiers partagés au sein de l'entreprise.

Chaque service aura son propre dossier. Ainsi l'arborescences du dossier « data » reprend l'organigramme de l'entreprise et se présente de la manière suivante :



B.3. Intégration du serveur SAMBA au domaine

Un serveur SAMBA peut être intégré de manière totalement transparente dans un environnement Windows Serveur grâce à un service (daemon) : Winbind.

Les paramètres à renseigner pour configurer ce service se situent dans la première partie du fichier de configuration générale du serveur SAMBA : smb.conf

```
[global]
workgroup=PIZZA
security=ads
realm=PIZZA.LOCAL
domain logons=no
domain master=no
local master=no
prefered master=no
os level=0
template homedir=/home/%D/%U
template shell=/bin/bash
winbind enum groups=yes
winbind enum users=yes
idmap config *:backend=tdb
idmap config *:range=11000-20000
idmap config PIZZA:backend=rid
idmap config PIZZA:range=10000000-19000000
```

Une fois paramétré, il suffit de redémarrer les services SAMBA et WINBIND, puis d'intégrer le serveur au domaine via la commande suivante :

```
>net ads join -U administrateur@pizza.local
```

On peut vérifier que le serveur SAMBA a bien intégré le domaine :

Du coté de Linux, en listant les utilisateurs de l'Active Directory via la commande :

```
>wbinfo -u
```

```

root@srvdata:~# wbinfo -u
PIZZA\administrateur
PIZZA\invité
PIZZA\krbtgt
PIZZA\model_dg
PIZZA\model_assis_dg
PIZZA\a.briffaut
PIZZA\m.ada
PIZZA\model_resp_info
PIZZA\model_info
PIZZA\j.sion
PIZZA\model_resp_rh
PIZZA\mp.wavrin
PIZZA\model_rh
PIZZA\model_resp_compta
PIZZA\model_compta
PIZZA\g.dumont
PIZZA\k.kovacic
PIZZA\k.leveque
PIZZA\model_daf
PIZZA\f.regnault
root@srvdata:~# _

```

Ou en listant les groupes, toujours du côté Linux avec la commande :

```
>wbinfo -g
```

```

PIZZA\group_dg
PIZZA\group_assis_dg
PIZZA\group_resp_rh
PIZZA\group_rh
PIZZA\group_resp_compta
PIZZA\group_compta
PIZZA\group_resp_info
PIZZA\group_info
PIZZA\group_daf
PIZZA\group_resp_sav
PIZZA\group_assis_sav
PIZZA\group_resp_service_a
PIZZA\group_service_a
PIZZA\group_resp_service_b
PIZZA\group_service_b
root@srvdata:~# _

```

Du côté de Windows, on peut vérifier que notre serveur de fichier est bien intégré au domaine car il apparaît dans l'OU « Computers » de l'Active Directory d'une part.



Et d'autre part, on trouve un enregistrement de type A (hôte IPv4) dans notre zone DNS

srvdata

Hôte (A)

172.16.0.3

B.4. Gestion des permissions

Nous avons vu grâce à la commande « `wbinfo -g` » que notre serveur Linux connaît la liste des groupes déclarés dans l'Active Directory.

```
PIZZA\group_dg
PIZZA\group_assis_dg
PIZZA\group_resp_rh
PIZZA\group_rh
PIZZA\group_resp_compta
PIZZA\group_compta
PIZZA\group_resp_info
PIZZA\group_info
PIZZA\group_daf
PIZZA\group_resp_sav
PIZZA\group_assis_sav
PIZZA\group_resp_service_a
PIZZA\group_service_a
PIZZA\group_resp_service_b
PIZZA\group_service_b
root@srvdata:~# _
```

Pour donner des permissions d'accès aux répertoires partagés, nous allons associer ces groupes à ces répertoires toujours au travers de notre fichier de configuration SAMBA : `smb.conf`

Exemples :

Pour le service Informatique :

```
[Informatique]
path=/data/DAF/Informatique
browseable = no
writeable = yes
read only = no
valid users = @"admins du domaine", @group_info, @group_resp_info, @group_DAF
```

Pour les autres services :

[Compta]

```
path=/data/DAF/Administratif/Compta
browseable = no
writeable = yes
read only = no
valid users = @"admins du domaine", @group_compta, @group_resp_compta, @group_DAF
```

[RH]

```
path=/data/DAF/Administratif/RH
browseable = no
writeable = yes
read only = no
valid users = @"admins du domaine", @group_rh, @group_resp_rh, @group_DAF
```

[Administratif]

```
path=/data/DAF/Administratif
browseable = no
writeable = yes
read only = no
valid users = @"admins du domaine", @group_DAF
```

[DAF]

```
path=/data/DAF
browseable = no
writeable = yes
read only = no
valid users = @"admins du domaine", @group_DAF
```

[Direction generale]

```
path=/data/Direction_generale
browseable = no
writeable = yes
read only = no
valid users = @"admins du domaine", @group_DG, @group_assis_DG
```

[SAV]

```
path=/data/SAV
browseable = no
writeable = yes
read only = no
valid users = @"admins du domaine", @group_resp_SAV, @group_assis_SAV
```

[Service_A]

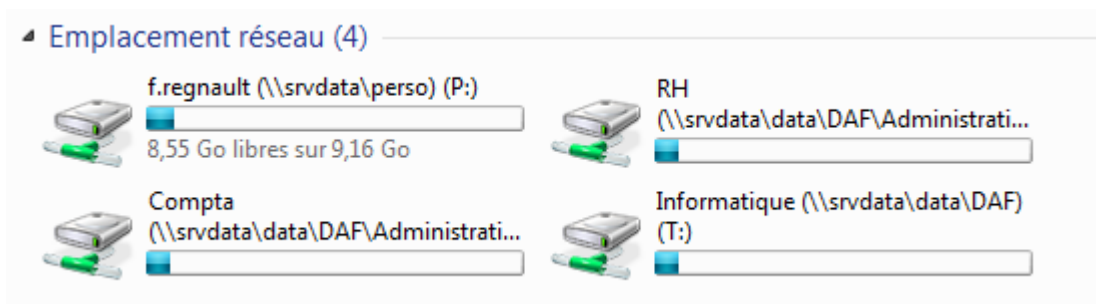
```
path=/data/Service_A
browseable = no
writeable = yes
read only = no
valid users = @"admins du domaine", @group_resp_service_A, @group_service_A
```

[Service_B]

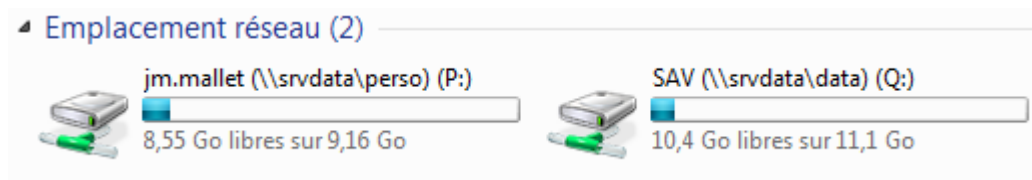
```
path=/data/Service_B
browseable = no
writeable = yes
read only = no
valid users = @"admins du domaine", @group_resp_service_B, @group_service_B
```

Exemple de connexion à un répertoire réseau :

L'utilisateur F.Regnault en qualité de DAF a accès à tous les répertoires des services sous sa direction, c'est-à-dire Administratif (RH et Compta) et Informatique ainsi qu'à son répertoire personnel :

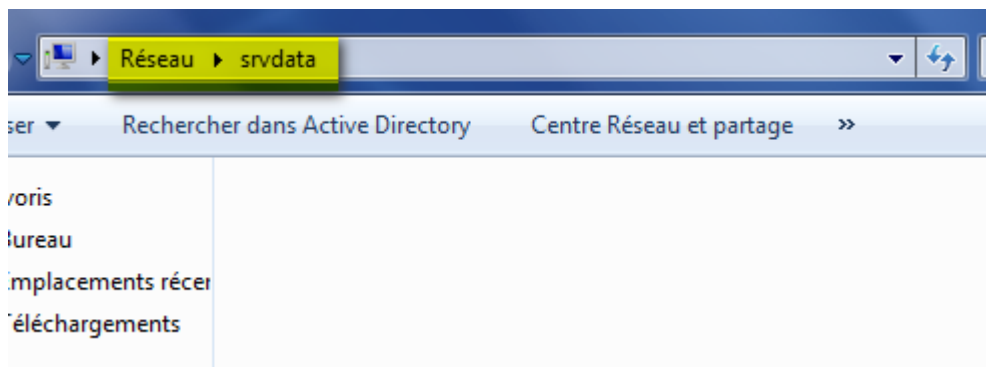


L'utilisateur JM.Mallet en qualité de responsable SAV ne devrait avoir accès qu'au répertoire SAV et à son répertoire personnel :

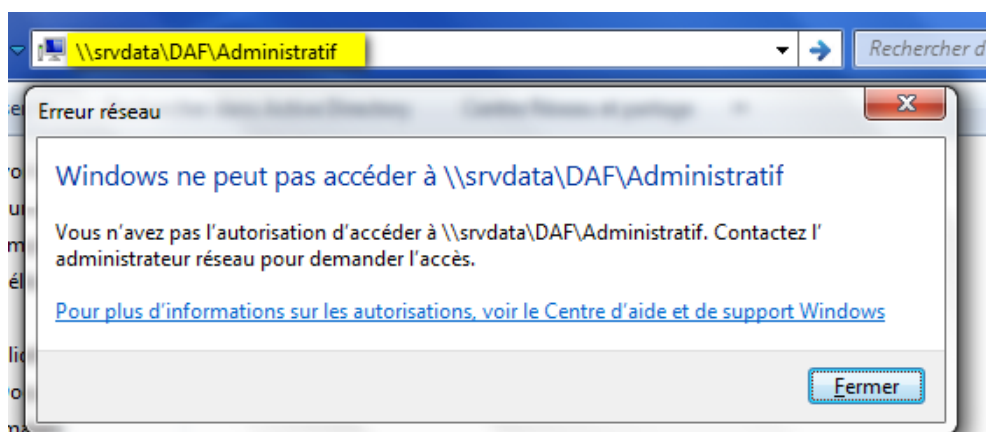


Il n'est pas possible pour un utilisateur d'un service de voir et d'accéder au répertoire d'un autre service.

D'une part en renseignant le chemin UNC (Universal Naming Convention), aucun répertoire ne s'affiche :



Et d'autre part, si on saisit l'adresse exacte d'un répertoire, une autorisation est requise :



B.5. Quotas

Les quotas permettent de limiter l'espace de stockage alloué à un volume, dossier ou à un utilisateur. Le cahier des charges indique que chaque utilisateur bénéficie de 5 go d'espace de stockage.

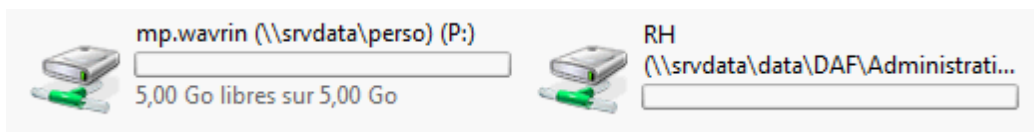
Un fois l'installation du paquet de gestion de quotas sous linux effectué et la configuration de ce service renseignée (voir procédure), il faut allouer l'espace de stockage à l'ensemble des utilisateurs.

L'attribution des quotas peut se faire par utilisateur ou par groupe. Ici nous utiliserons l'attribution par utilisateur.

```
root@srvdata:/# edquota -u mp.wavrin_
```

```
GNU nano 2.2.6      Fichier : /tmp//EdP.aI7Zs7F

Quotas disque pour user mp.wavrin (uid 11011) :
Système de fichiers      blocs      souple      stricte      inodes      souple$
/dev/sdb5                 0      5242880      5242880      0      0$
/dev/sdb6                 0      5242880      5242880      0      0$
```



Pour attribuer automatiquement les quotas à l'ensemble de nos utilisateurs, nous allons créer un script shell dans lequel nous allons employer la commande setquota.

```
1  #!/bin/bash
2  wbinfo -u | while read user
3  do
4      setquota -u $user 5242880 5242880 0 0 -a /dev/sdb5
5      setquota -u $user 5242880 5242880 0 0 -a /dev/sdb6
6  done
```

Le fonctionnement de ce script est simple.

Nous récupérons la liste des utilisateurs via la commande « wbinfo -u ». Chaque ligne retournée par cette commande correspond à un utilisateur que l'on va assigner à une variable « user » grâce à la fonction « read »

C'est sur cette variable que nous allons appliquer la commande « setquota »

C. Le serveur FTP

C.1. Intérêt d'un serveur FTP

Il est facile d'envoyer des fichiers par e-mail en les mettant en pièces jointes dans des messages. Mais ce moyen n'est pas du tout adapté à l'échange de données lourdes (vidéos, photos en haute définition, fichier CAO, etc.) : le poids des pièces jointes est souvent limité par le serveur et, quand ils sont acceptés, de tels fichiers sont longs à transférer.

Pour échanger des fichiers volumineux, la meilleure solution est d'installer un serveur FTP (File Transfer Protocol).

Les transferts de fichiers seront plus rapides que par e-mail et surtout, aucune limite de taille ne sera imposée. Le principe consiste à mettre un ou plusieurs dossiers sur un serveur en libre-service pour que les salariés, collaborateurs ou clients externes puissent y récupérer des fichiers ou en déposer.

Bien sûr, il n'est pas question de laisser les fichiers accessibles à n'importe qui. Pour cette raison, un identifiant et un mot de passe seront attribués à chaque personne habilitée à consulter ou à déposer des fichiers sur le serveur FTP.

C.2. Installation et Configuration

Le service FTP retenu sera « pure-ftpd » et sera installé sur notre second serveur Linux.

L'installation se fait par ligne de commande :

```
# aptitude install pure-ftpd
```

Ensuite il convient de configurer le serveur FTP en rajoutant quelques options sous forme de fichiers dans le dossier « conf » de pure-ftpd

Fichiers	Contenu
/etc/pure-ftpd/conf/ChrootEveryone	Yes
/etc/pure-ftpd/conf/CreateHomeDir	Yes
/etc/pure-ftpd/conf/MaxDiskUsage	80

La première option permet de « Chrooter » l'ensemble des utilisateurs du FTP. Cela signifie que le dossier créé sur le FTP pour chaque utilisateur sera considéré comme la racine « ./ » du système.

Cette manipulation a pour but d'empêcher un utilisateur d'accéder au dossier d'un autre utilisateur.

La seconde option indique qu'il faut créer un répertoire par utilisateur. Ce répertoire est créé dès sa première connexion.

Enfin la dernière option interdit de déposer (uploader) des fichiers sur le FTP si la partition de stockage utilisée est chargée au-delà des 80%.

C.3. Création d'utilisateurs virtuels

Pour des questions de sécurité, nous souhaitons distinguer les utilisateurs ayant accès au système hébergeant le FTP (administrateur du domaine, techniciens informatiques) ; des utilisateurs utilisant le service FTP (salariés, collaborateurs, ou clients externes).

Nous allons donc créer un compte système sans accès à ce dernier

```
# groupadd ftpgroup
# useradd -g ftpgroup -d /dev/null -s /etc ftpuser
```

Ensuite nous pouvons créer des utilisateurs virtuels

```
root@srvftp:/# groupadd ftpgroup
root@srvftp:/# useradd -g ftpgroup -d /dev/null -s /etc/ ftpuser
root@srvftp:/# pure-pw useradd userftp1 -u ftpuser -d /userftp1
Password: _
```

Après chaque création ou modification d'un utilisateur, il faut générer la base de données avec la commande suivante :

```
# pure-pw mkdb
```

Puis, il faut créer un lien symbolique pour activer l'authentification des utilisateurs virtuels :

```
# ln -s /etc/pure-ftpd/conf/PureDB /etc/pure-ftpd/auth/60pure
```

Enfin, il faut relancer le serveur FTP avec cette commande :

```
# /etc/init.d/pure-ftpd restart
```

C.4. Utilisation en mode sécurisé

On peut vérifier le bon fonctionnement de notre serveur FTP en mode sécurisé, avec identifiant et mot de passe :

Du côté de linux en listant les utilisateurs du FTP et leurs données d'utilisation grâce à la commande :


```
# pure-pw show test
```

Ce qui donne :

```
root@srvftp:/# pure-pw show userftp1

Login           : userftp1
Password        : $1$m10I4KG0$o208gopYiqWN9F53qVBQx1
UID             : 1001 (ftpuser)
GID             : 1001 (ftpgroup)
Directory       : /userftp1/./
Full name       :
Download bandwidth : 0 Kb (unlimited)
Upload  bandwidth : 0 Kb (unlimited)
Max files       : 0 (unlimited)
Max size        : 0 Mb (unlimited)
Ratio           : 0:0 (unlimited:unlimited)
Allowed local  IPs :
Denied  local  IPs :
Allowed client IPs :
Denied  client IPs :
Time restrictions : 0000-0000 (unlimited)
Max sim sessions : 0 (unlimited)
```

Toujours du côté de Linux en se connectant au serveur FTP par la commande :

```
# ftp 192.168.1.214
```

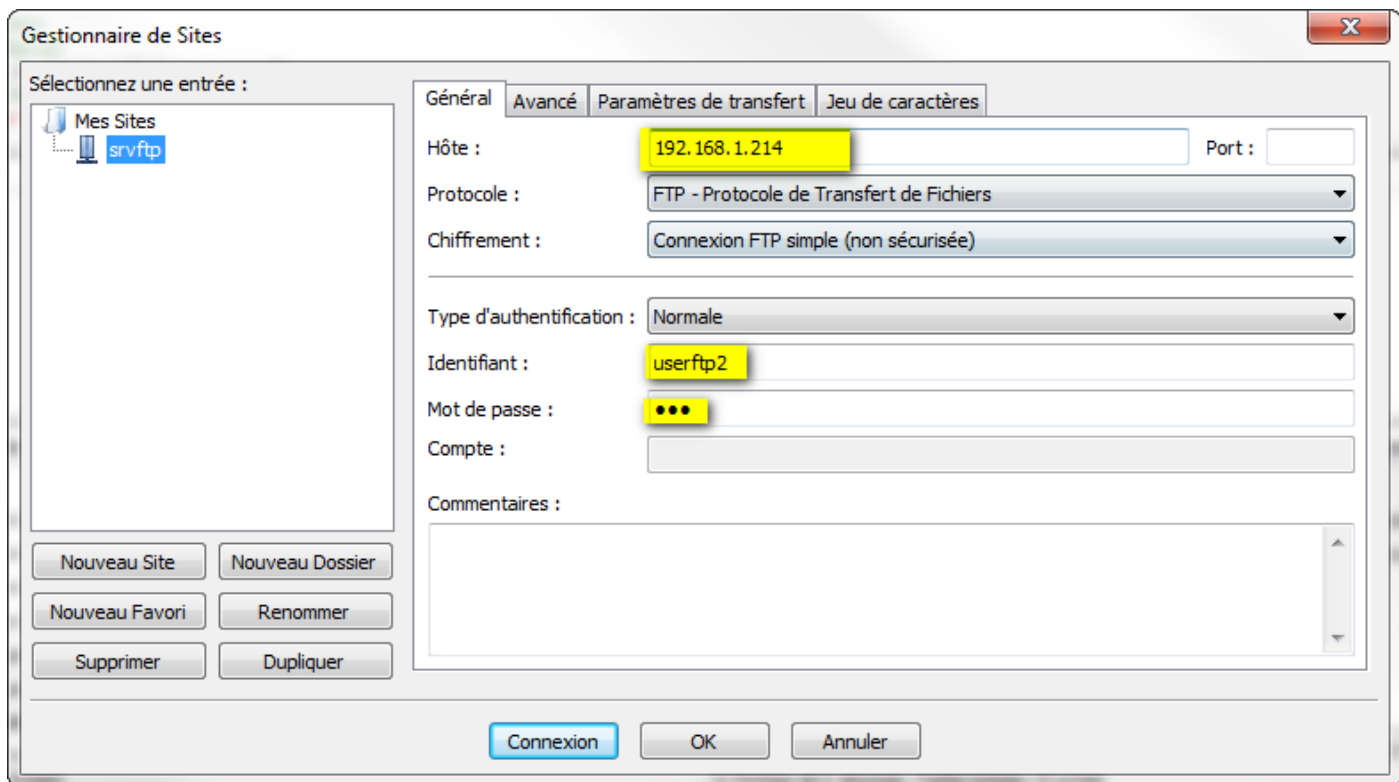
Ce qui donne :

```
root@srvftp:/# ftp 192.168.1.214
Connected to 192.168.1.214.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 50 allowed.
220-Local time is now 11:54. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (192.168.1.214:root): userftp1
331 User userftp1 OK. Password required
Password:
230 OK. Current directory is /
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> _
```

D'un point de vue Windows en utilisant un logiciel client FTP comme FILEZILLA



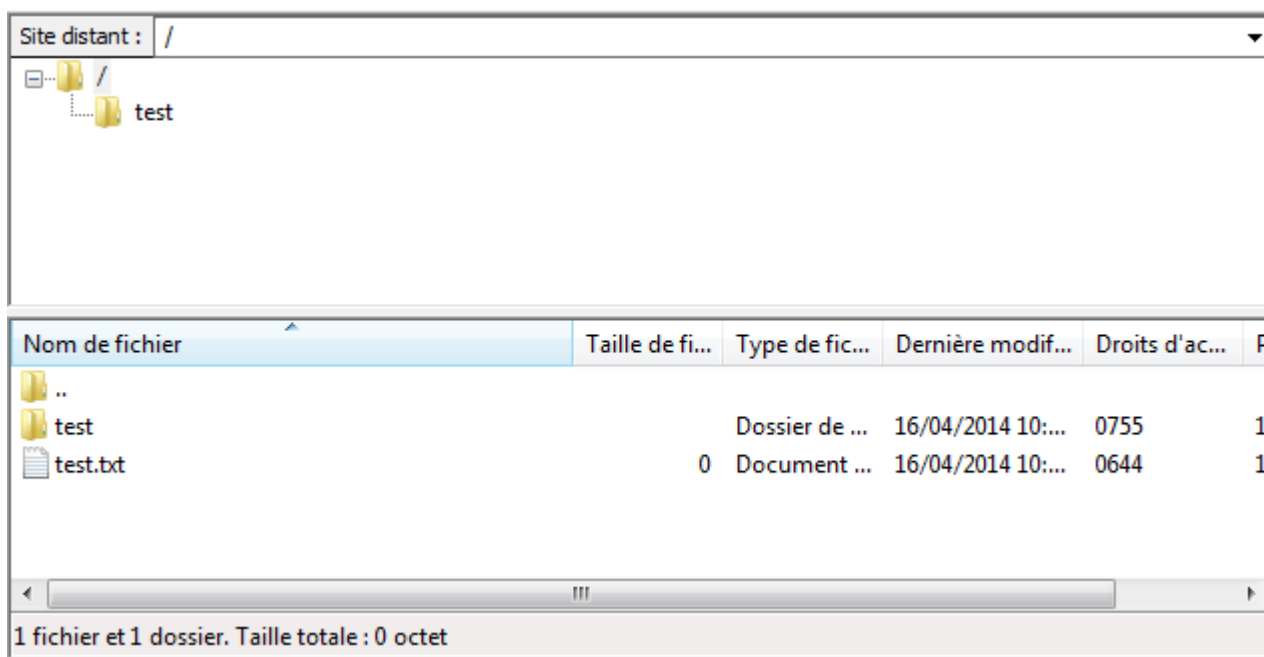
Dans le gestionnaire de site, on indique l'adresse IP du serveur FTP, l'identifiant utilisateur et le mot de passe. Puis on se connecte.



```

Statut : Connexion à 192.168.1.214:21...
Statut : Connexion établie, attente du message d'accueil...
Réponse : 220----- Welcome to Pure-FTPd [privsep] [TLS] -----
Réponse : 220-You are user number 3 of 50 allowed.
Réponse : 220-Local time is now 12:06. Server port: 21.
Réponse : 220-This is a private system - No anonymous login
Réponse : 220-IPv6 connections are also welcome on this server.
Réponse : 220 You will be disconnected after 15 minutes of inactivity.
Commande : USER userftp2
Réponse : 331 User userftp2 OK. Password required
Commande : PASS ***
Réponse : 230 OK. Current directory is /

```



C.5. Utilisation en mode anonyme

Pour accéder au FTP en mode anonyme, c'est-à-dire sans avoir besoin de saisir un mot de passe, nous allons :

Créer un utilisateur "anonyme" qui n'a pas besoin de mot de passe et son répertoire dédié. On place cet utilisateur dans le groupe ftpgroup

```
useradd -g ftpgroup -d /home/anonymous -s /usr/sbin/nologin anonymous
```

On change le propriétaire de ce répertoire

```
# chown ftpuser anonymous
```

On autorise l'écriture dans ce répertoire pour le groupe ftpgroup

```
# chmod 775 anonymous
```

Puis on ajoute quelques paramètres dans la configuration de pureftpd à savoir

```
# echo "no" > /etc/pure-ftpd/conf/NoAnonymous
# echo "yes" > /etc/pure-ftpd/conf/AnonymousCantUpload
# echo "yes" > /etc/pure-ftpd/conf/AnonymousCanCreateDirs
# echo "yes" > /etc/pure-ftpd/conf/AntiWarez
```

- Noanonymous : Autorise uniquement les utilisateurs authentifiés. Les utilisateurs anonymes sont interdits.
- AnonymousCantupload : Interdit l'accès en écriture sur le serveur (upload) pour les utilisateurs anonymes.
- AnonymousCanCreateDirs : Autorise les utilisateurs anonymes à créer des répertoires.
- Antiwarez : Interdit aux utilisateurs anonymes de télécharger des fichiers

Maintenant on peut se connecter au serveur FTP sans mot de passe.

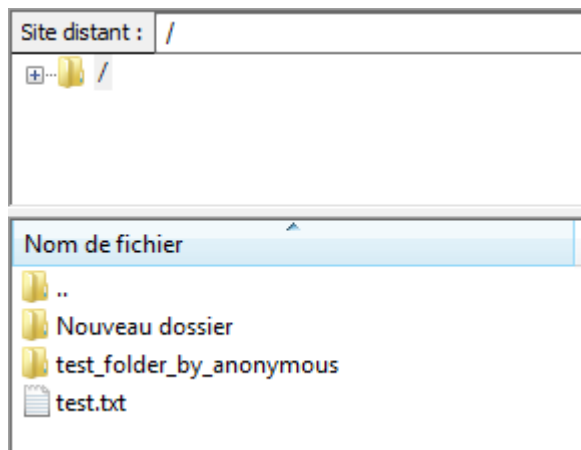
Depuis Linux :

```
root@srvftp:/# ftp 192.168.1.214
Connected to 192.168.1.214.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 2 of 50 allowed.
220-Local time is now 15:49. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (192.168.1.214:root): anonymous
230 Anonymous user logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> mkdir test_folder_by_anonymous
257 "test_folder_by_anonymous" : The directory was successfully created
ftp> ls -l
200 PORT command successful
150 Connecting to port 35039
drwxr-xr-x  2 1002      1001          4096 Apr 16 15:44 Nouveau dossier
-rw-r--r--  1 0        0              0 Apr 16 15:40 test.txt
drwxr-xr-x  2 1002      1001          4096 Apr 16 15:49 test_folder_by_ano
ymous
226-Options: -l
226 3 matches total
ftp> _
```

Ou depuis un client Windows :

Hôte :	<input type="text" value="192.168.1.214"/>
Protocole :	<input type="text" value="FTP - Protocole de Transfert de Fichiers"/>
Chiffrement :	<input type="text" value="Connexion FTP simple (non sécurisée)"/>
Type d'authentification :	<input type="text" value="Anonyme"/>
Identifiant :	<input type="text" value="anonymous"/>
Mot de passe :	<input type="text"/>
Compte :	<input type="text"/>

```
Statut : Connexion à 192.168.1.214:21...
Statut : Connexion établie, attente du message d'accueil...
Réponse : 220----- Welcome to Pure-FTPd [privsep] [TLS] -----
Réponse : 220-You are user number 2 of 50 allowed.
Réponse : 220-Local time is now 15:54. Server port: 21.
Réponse : 220-IPv6 connections are also welcome on this server.
Réponse : 220 You will be disconnected after 15 minutes of inactivity.
Commande : USER anonymous
Réponse : 230 Anonymous user logged in
Commande : OPTS UTF8 ON
Réponse : 200 OK, UTF-8 enabled
Statut : Connecté
Statut : Récupération du contenu du dossier...
Commande : PWD
Réponse : 257 "/" is your current location
Statut : Contenu du dossier affiché avec succès
```



VII– Le logiciel de gestion de parc informatique

A. Les besoins

L'équipe informatique court partout...et se trompe souvent de lieu pour dépanner les utilisateurs. Il n'y a pas d'informations stockées quelque part sur le parc (Nom d'hôtes, type de machines...)

Afin de remédier à ce problème la création d'un logiciel recensant et stockant ces informations est nécessaire.

Ce logiciel permettra de connaître :

- L'ensemble des collaborateurs utilisant un ordinateur
- Les attributs de l'ordinateur (Processeurs, RAM, disque dur)
- Les périphériques associés au poste (imprimantes, écran)
- Sa localisation dans l'entreprise (quel bureau, à quel étage)

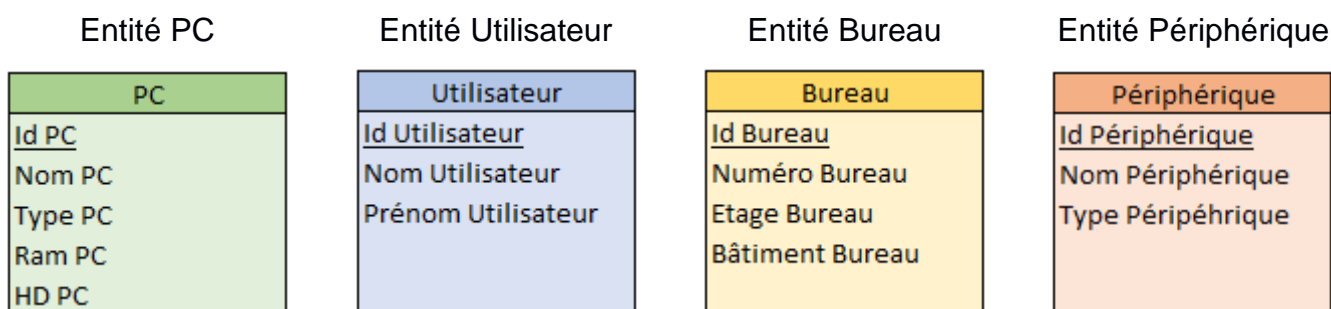
Le logiciel proposera deux modes :

- un mode consultation, qui ne permettra de que lire les informations sur le parc.
- un mode gestion qui permettra d'éditer (ajouter, effacer, modifier) les informations du parc.

B. MCD : Modèle conceptuel de base de donnée

Pour réaliser notre logiciel, nous allons d'abord devoir réaliser un modèle conceptuel de base de donnée dit MCD.

Pour se faire nous allons découper chaque élément qui compose notre parc en entités. Chaque entité comportera plusieurs propriétés, attributs.

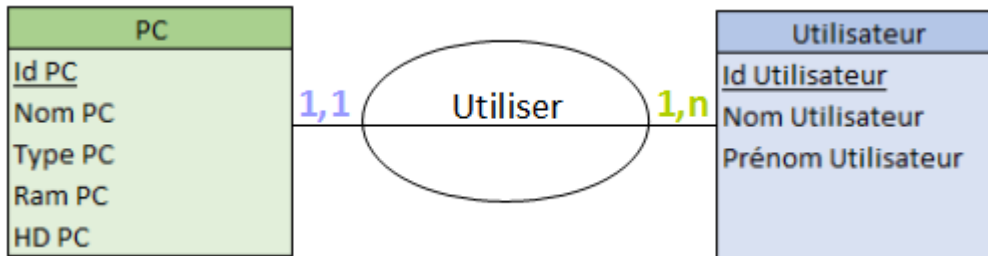


Une fois ces entités et leurs propriétés définies, il faut déterminer les relations qu'elles entretiennent entre elles.

NB : pour des questions pratiques, un utilisateur ne possèdera qu'un ordinateur, et on ne trouvera qu'un seul ordinateur par bureau.

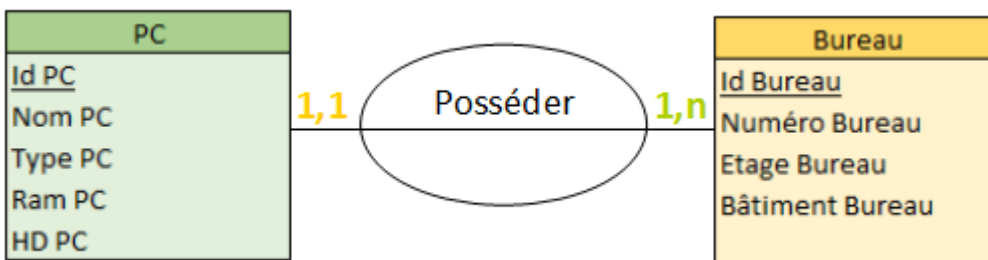
Relation PC – Utilisateur :

- ⇒ Un utilisateur ne peut avoir qu'un seul PC au minimum et au maximum, la cardinalité de la relation sera donc 1,1.
- ⇒ L'entité ordinateur peut être utilisée au minimum par un collaborateur mais peut être aussi utilisée par plusieurs collaborateurs, la cardinalité de la relation sera donc 1,n.



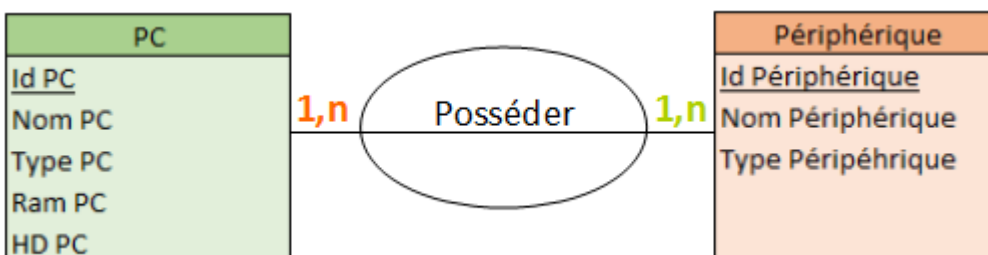
Relation PC – Bureau:

- ⇒ Un bureau ne peut contenir qu'un seul ordinateur au minimum et au maximum, la cardinalité de la relation sera donc 1,1.
- ⇒ L'entité ordinateur peut se trouver dans un bureau au minimum mais aussi dans plusieurs bureaux, la cardinalité de la relation sera donc 1,n.

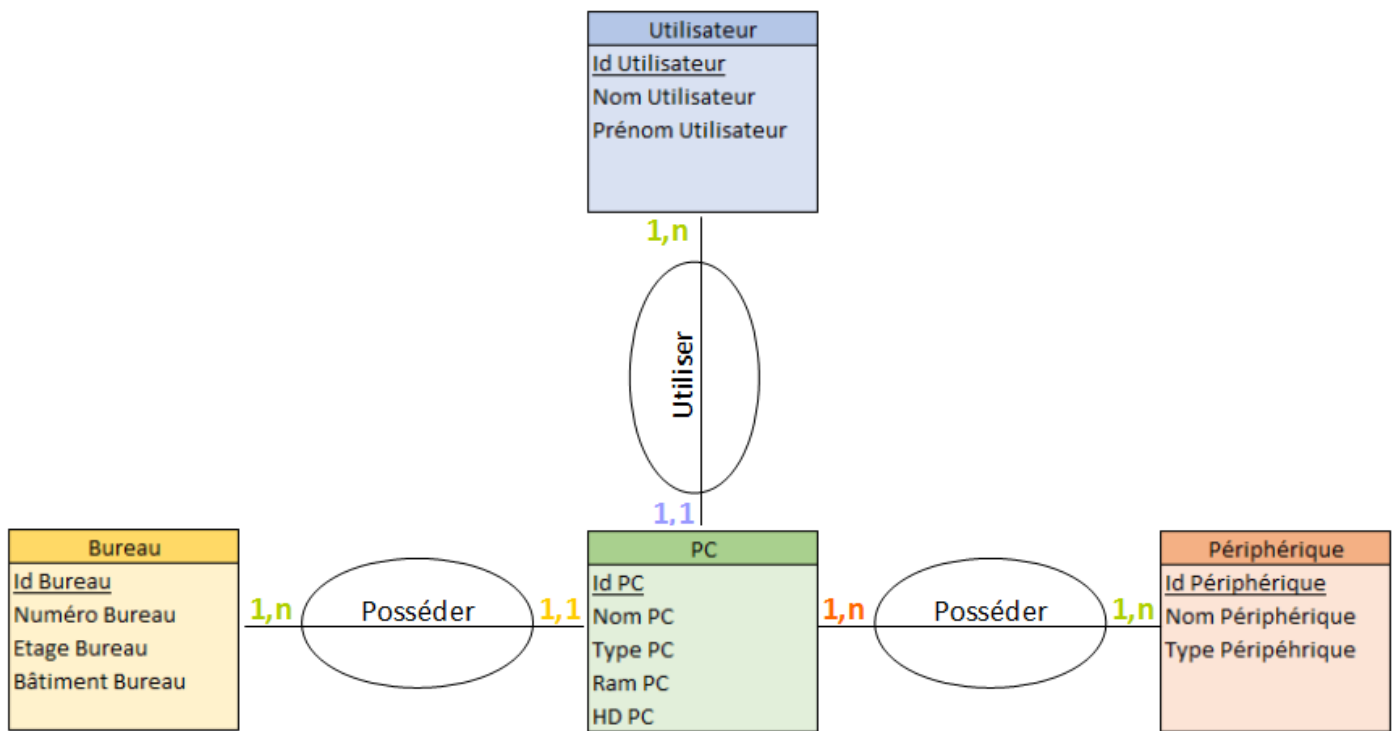


Relation PC – Périphériques

- ⇒ Un PC peut utiliser un périphérique au minimum (1 écran) mais peut aussi utiliser plusieurs périphériques au maximum (plusieurs imprimantes), la cardinalité de la relation sera donc 1,n
- ⇒ Dans la société un périphérique peut être utilisé au minimum par un seul PC mais peut être aussi utilisé par plusieurs PC, la cardinalité de la relation sera donc 1,n



Notre Modèle Conceptuel de Donnée (MCD) final se présente donc comme ci-dessous :



C. MPD : Modèle physique de base de données

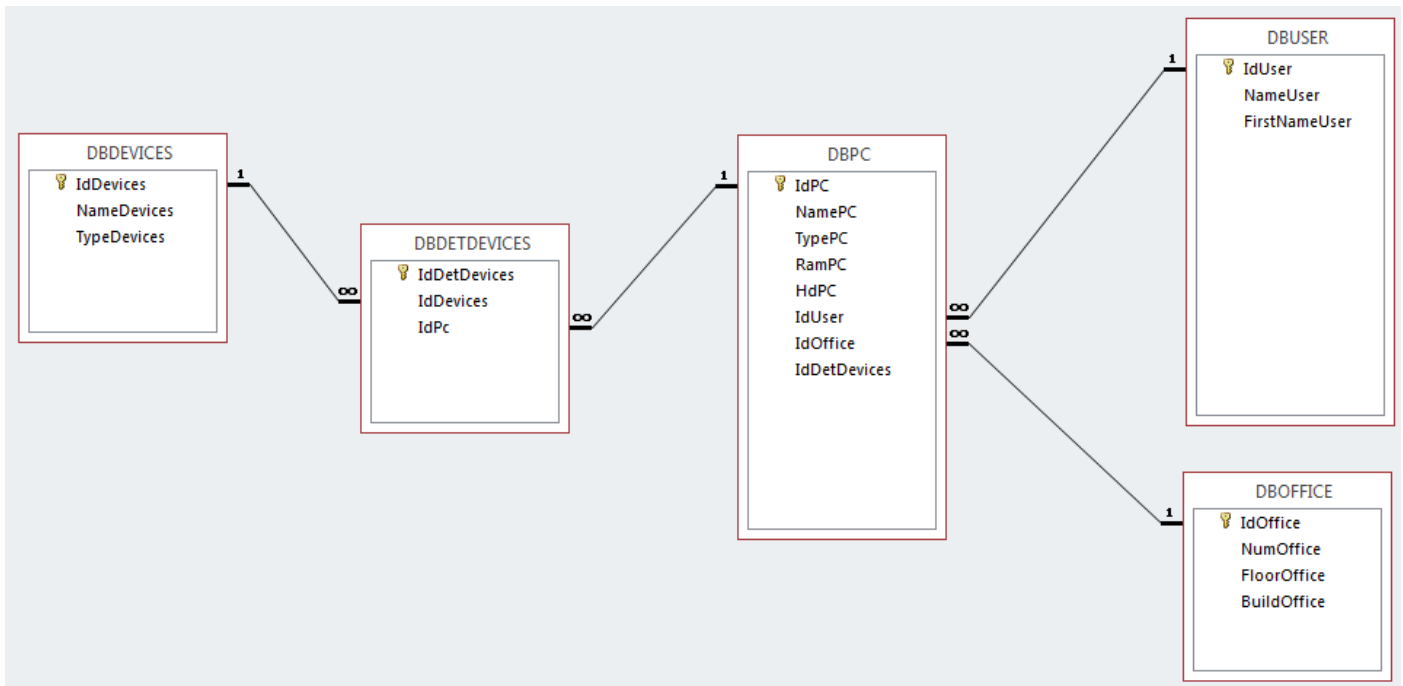
Un modèle physique de base de données est la représentation du MCD sous forme de fichiers. La construction du MPD passe par une transformation de MCD en respectant 3 règles :

- 1) **REGLE 1** : toutes entités doit être représentée par une table.
- 2) **REGLE 2** : dans le cas d'entités reliées par une relation avec au moins une cardinalité maximale à 1, la clé primaire de l'entité de cardinalité (-,n) (ou (-,1) migre dans la table de l'entité (-,1)
- 3) **REGLE 3** : dans le cas d'entités reliées avec les deux cardinalités maximales à n, on ajoute une table représentant la relation, avec migration des clés primaires des deux entités mises en jeu

En suivant ces règles, nous obtenons :






- 5 tables car 4 entités (règle 1) et une table intermédiaire car les 2 cardinalités maximales de la relation entre PC et périphérique est égale à n (règle 3). Les clefs primaires des entités périphériques et PC migreront dans cette table intermédiaire (règle 3)
- Une des 2 cardinalités maximales des autres relations (PC – Utilisateur et PC – Bureau) étant égale à 1, la clef primaire de ces entités (bureau et Utilisateur) vont migrer dans la table PC

Ce qui nous donne le MPD suivant :



Comprenant nos 5 tables :

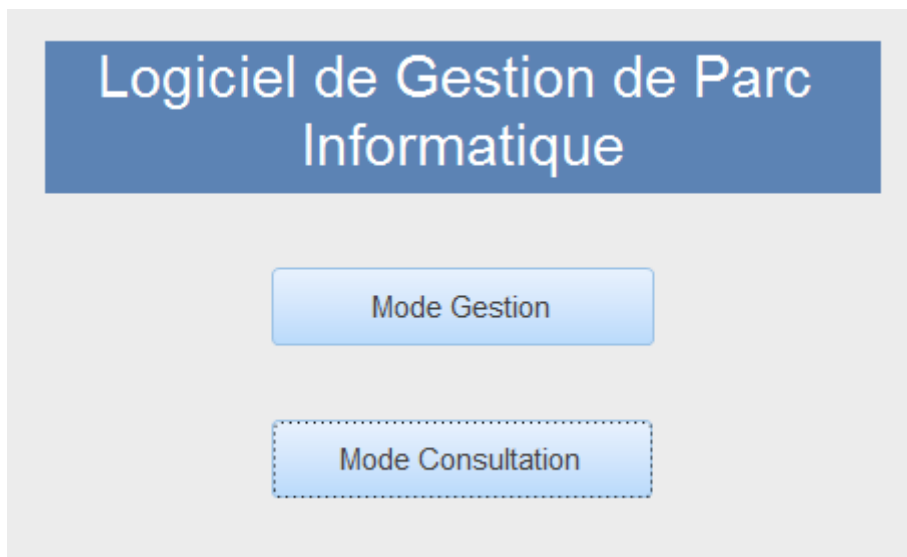
Tables

-  DBDETDEVICES
-  DBDEVICES
-  DBOFFICE
-  DBPC
-  DBUSER

D. Réalisation / Maquette

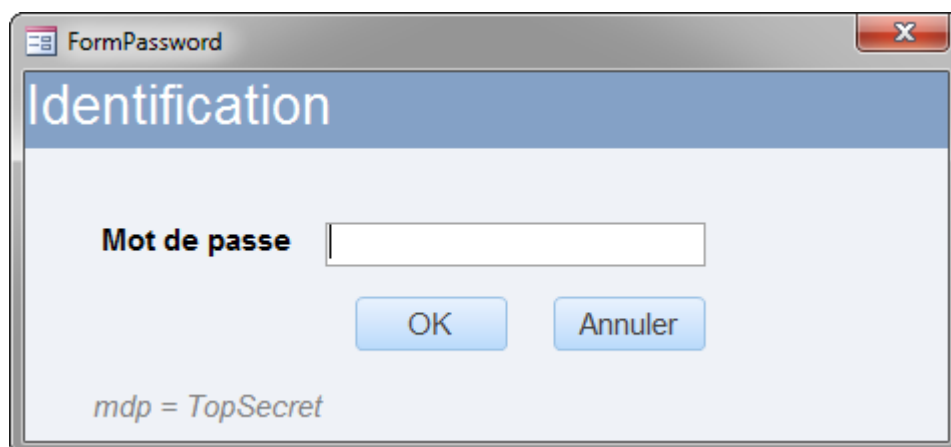
D.1. Page d'accueil

Pour réaliser le logiciel, nous avons d'abord pensé à réaliser une page d'accueil qui redirigera l'utilisateur vers le mode de consultation ou vers le mode de gestion, en fonction de son poste au sein de l'entreprise.



D.2. Mode de Gestion

Par mesure de sécurité le mode de gestion n'est accessible qu'après avoir saisi un mot de passe :



Une fois le mot de passe saisi, nous entrons dans le mode de gestion :

Le mode de gestion est une vue divisée en deux parties :

- Une première partie sous la forme d'un bandeau vertical situé à gauche dans lequel se trouveront plusieurs boutons permettant de modifier, ajouter, enlever des postes, des périphériques, des utilisateurs et des bureaux.
- La partie principale, située au centre, montrera d'un seul coup d'œil l'ensemble des informations relatives à un poste (configuration, périphériques associés, utilisateur et emplacement). Il est notamment possible d'éditer directement les informations des postes dans cette partie sans avoir recours aux boutons de gestion individuelle situés à gauche.

Gestion du Parc Informatique

Gérer les Postes
Gérer les périphériques
Gérer les Utilisateurs
Gérer les Locaux

Partie 1

Fiche Récapitulative

Nom du poste : PC01 Nom : Sion
 Type de poste : Desktop Prénom : John **Partie 2**
 Quantité de RAM : 2 Go Bureau n° : 201
 Capacité disque dur : 1 To Bâtiment : Ouest
 A l'étage ? Oui Non

Fiche Ecrans Fiche Imprimantes

N°Périphérique	Nom du périphériques	Type de périphérique
2	LG2 19" 1900x1600	Ecran
3	Samsung3 22"	Ecran
4	Dell 22"	Ecran

IdPC: 6 IdUser: 4 IdOffice: 1

D.3. Mode de Consultation

La vue du mode consultation reprend la vue du mode de gestion si ce n'est que :

- Le bandeau gauche latéral (partie1) ne contient plus aucun bouton permettant d'éditer des postes, périphériques, utilisateurs ou bureaux.
- La vue principale (partie 2) est quant à elle, en lecture seule uniquement. Là encore il n'est pas possible de modifier quoique ce soit.

VIII – La tolérance de panne

La **tolérance aux pannes** désigne une méthode de conception permettant à un système de continuer à fonctionner, éventuellement de manière réduite (on dit aussi en « **mode dégradé** »), au lieu de tomber complètement en panne, lorsque l'un de ses composants ne fonctionne plus correctement.

L'expression est employée couramment pour les systèmes informatiques étudiés de façon à rester plus ou moins opérationnels en cas de panne partielle, éventuellement avec une réduction du débit ou une augmentation du temps de réponse. En d'autres termes, le système ne s'arrête pas de fonctionner, qu'il y ait défaillance matérielle ou défaillance logicielle.

Il existe deux méthodes qui permettent de mettre place une tolérance de panne :

- **L'utilisation de composants tolérants aux pannes.** Si chaque composant, à son tour, peut continuer à fonctionner quand un de ses sous-composants tombe en panne, le système tout entier pourra continuer à fonctionner.
⇒ C'est le cas par exemple des disques durs montés en RAID 1, 5,10 (voir annexe). En effet, grâce à ces types de RAID, si un disque dur de la grappe vient à tomber en panne ; cela n'affecte pas les données et le système peut continuer à fonctionner.
- **La mise en place de redondance.** Cela signifie avoir une sauvegarde ou une copie des composants qui prendront automatiquement la relève dès qu'un composant tombe en panne.
⇒ C'est le cas par exemple de la réplication mise en place pour les services Active Directory et DNS. En effet si le serveur SRV1 venait à ne plus fonctionner, les services Active Directory et DNS qu'il propose seront toujours assurés par le serveur SRV2.

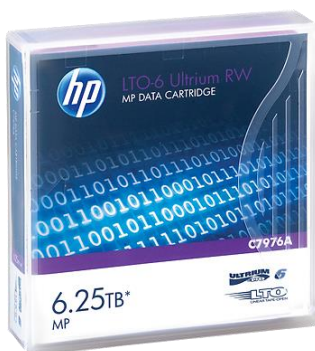
Ainsi voici les différentes méthodes employées pour mettre en place une tolérance de panne au sein de notre infrastructure :

Serveurs et services	Composant tolérant à une panne	Redondance
SRV1 (AD+DNS)	RAID 1	Réplication sur SRV2
SRV2 (AD+DNS)	RAID 1	Réplication sur SRV1
SRVTSEPRINT (TSE+PRINT)	RAID 10	n/a
SRVDATA (Samba + DHCP 1)	RAID 5	DHCP 2 sur SRVFTP
SRVFTP (Ftp + DHCP 2)	RAID 5	DHCP 1 sur SRVDATA

IX – La gestion des sauvegardes

Les sauvegardes de l'entreprise (Contrôleur de Domaine, Profils Itinérants, fichiers de données) seront envoyées vers un lecteur de bande.

Le lecteur de bandes et les bandes que nous allons utiliser ont été achetées lors du déménagement de l'entreprise.







Voici la façon dont nous avons pensé le calendrier de sauvegarde :

Lundi	Mardi	Mercredi	Jeudi	Vendredi
Bande 1	Bande 2	Bande 3	Bande 4	Bande 5
Bande 1	Bande 2	Bande 3	Bande 4	Bande 6
Bande 1	Bande 2	Bande 3	Bande 4	Bande 7
Bande 1	Bande 2	Bande 3	Bande 4	Bande 8

Janvier	Février	Mars	Avril	Mai	Juin
Bande 8	Bande 9	Bande 10	Bande 11	Bande 12	Bande 13

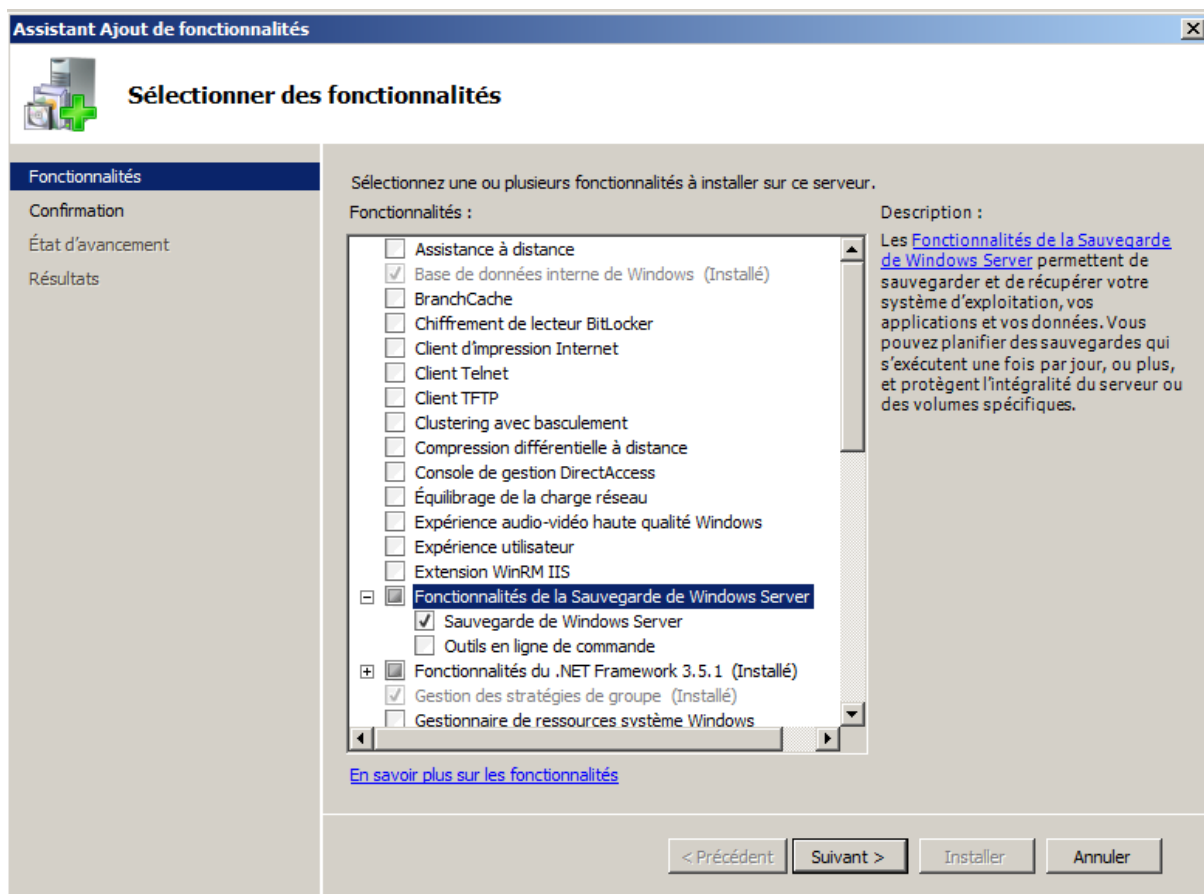
Juillet	Août	Septembre	Octobre	Novembre	Décembre
Bande 14	Bande 15	Bande 16	Bande 17	Bande 18	Bande 19

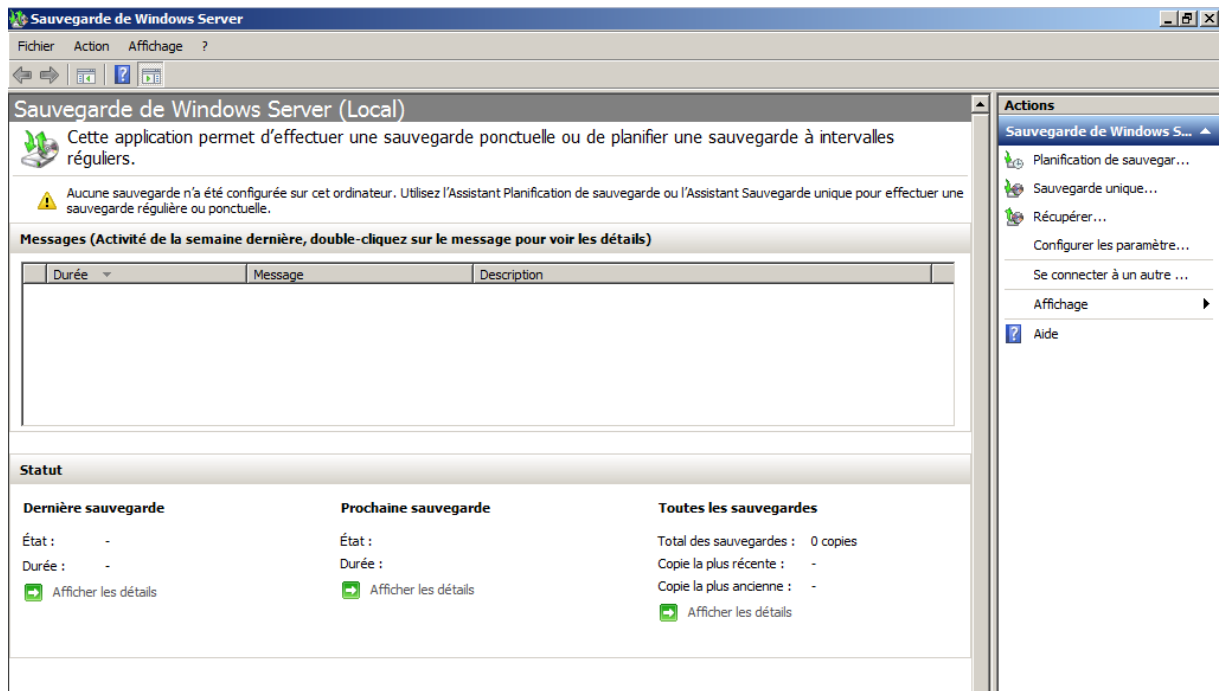
2010	2011	2012	2013	2014
Bande 19	Bande 20	Bande 21	Bande 22	Bande 23

-  Bandes journalières
-  Bandes hebdomadaires
-  Bandes mensuelles
-  Bandes annuelles

A. Sauvegarde du contrôleur de domaine :

Les répertoires NTDS et SYSVOL qui sont installées sur une partition distincte (E:) seront sauvegardées à l'aide de l'outil Windows Server. Ce fichier backup sera ensuite exporté vers le lecteur de bandes.





B. Sauvegarde du serveur de fichiers (profils itinérants, données de l'entreprise)

Les données hébergées sur le serveur de fichiers samba, seront aussi sauvegardées quotidiennement vers le lecteur de bandes mais cette fois à l'aide d'un script.

Ce script fera une copie locale compressée des partitions PROFILS et DATA.

Puis à l'aide d'un client SSH (Secure Shell), ces sauvegardes seront envoyées vers un espace de stockage distant, ici, le lecteur de bandes.

Exemple de script de sauvegarde en ligne de commande sous Linux

```

1 #!/bin/sh
2
3 # Enregistrez ce script sous le nom de backup.sh. Prenez note de son emplacement.
4
5 echo "-----";
6 echo "- Sauvegarde complète du système";
7 echo "-----";
8 echo "";
9
10 echo "Création de l'archive";
11
12 # On crée l'archive .tar en précisant entre guillemets les chemins absolus des dossiers à sauvegarder.
13 tar -cvzf /votre_support/backup.tar.gz "/etc/" "/root" "/home" "/var" "/usr/local"
14 echo "-----";
15 echo "";
16
17 echo "Vérification de l'existence de l'archive";
18 # On teste si l'archive a bien été créée
19 if [ -e /votre_support/backup.tar.gz ]
20 then
21 echo ""
22 echo "Votre archive a bien été créée.";
23 echo ""
24 else
25 echo ""
26 echo "Il y a eu un problème lors de la création de l'archive.";
27 echo ""
28 fi
29
30 echo "### Fin de la sauvegarde. ###";

```

Ce script peut être automatisé et planifié via « [crontab](#) » qui est un programme sous Linux permettant d'éditer les tâches à exécuter et leurs horaires d'exécution avec possibilité d'horaires périodiques.

La ligne, ci-dessous réalise une sauvegarde tous les lundis à 19h30.

```
30 19 * * 1 cd /dossier_où_est_enregistré_backup.sh | ./backup.sh
```

X – Planning prévisionnel

Le Directeur administratif et financier souhaite que la mise en place des serveurs ainsi que de l'ensemble des services associés soit faite en un mois.

Nous envisageons donc le planning prévisionnel suivant :

Tâches	Affectations	Pré-Prod															Post-Prod				
		Semaine 1					Semaine 2					Semaine 3					Semaine 4				
		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Achats & Livraison	Informatique																				
Réception + Installation	Informatique																				
Install. & Config. Win. Server	Karyn																				
Service Active Directory + DNS	Karyn																				
Réplication AD + DNS	Karyn																				
Service Terminal Server	Karyn																				
Serveur Impression	Karyn																				
Install. & Config. Linux Server	Kevin																				
Service DHCP	Kevin																				
Serveur SAMBA	Kevin																				
Seveur FTP	Kevin																				
Application Gestion de Parc	John																				
Déploiement	John																				
Test et correction de bug	Informatique																				
Formation & Documentation	Informatique																				

XI – Bilan Personnel

Bilan personnel Sion John :

Cette étude de cas a été extrêmement enrichissante principalement d'un point de vue technique. En effet les quelques connaissances déjà acquises ont été grandement complétées par la mise en place de ce projet.

Tout d'abord en ce qui concerne l'environnement Windows Serveur, avec le déploiement des services Active Directory et DNS.

Un service d'annuaire d'entreprise, de par sa gestion des utilisateurs, des authentifications, des droits d'accès, se révèle être un outil indispensable dans la mise en place d'une infrastructure informatique.

Grâce au DNS, la compréhension de son rôle et de son fonctionnement, l'identification des ordinateurs d'un parc est facilitée.

Avec les GPO, le TSE (Remote App), et le serveur d'impression, il est possible de configurer des environnements de travail complets pour tout type d'utilisateur.

Ensuite, l'installation de plusieurs environnements Linux fut une véritable découverte.

Outre la mise en place des différents services (samba, ftp, dhcp), c'est l'apprentissage du fonctionnement et du paramétrage d'un système Linux qui furent particulièrement intéressants.

Se passer de toute interface graphique, réaliser des configurations de services ou d'interfaces réseaux en ligne de commande a suscité un grand intérêt et sa maîtrise a renforcé mes compétences.

Le déploiement d'un serveur SAMBA, et la volonté d'intégrer ce serveur au domaine afin que les utilisateurs puissent s'y connecter avec leur compte Microsoft, m'ont permis de connaître l'utilité de services associés tels que Windbind et Kerberos..

Enfin, la maîtrise de l'installation d'un FTP, de la gestion des droits utilisateurs et de la mise en place de quotas sont autant d'atouts supplémentaires qui enrichiront mon parcours.

Il reste néanmoins de nombreuses connaissances à acquérir ou à compléter principalement dans la mise en place d'un serveur web pour l'entreprise, et de connecter celle-ci à internet.

En effet, actuellement l'infrastructure de la société fonctionne en vase clos, elle n'est pas connectée vers l'extérieur. L'entreprise ne dispose pas non plus d'un service intranet ni d'un site web.

Ce sont autant d'axes d'amélioration qui pourraient être mis en place à l'avenir.

Bilan personnel de Kevin Leveque :

Le cas Evolution aura été pour moi un déclencheur dans l'appréhension de la complexité de l'informatique dans le monde de l'entreprise.

La partie Windows Server nous a permis d'apprendre à sécuriser et fiabiliser notre SI, notamment grâce à la réplication, aux deux serveurs DNS. Nous avons pu organiser dans les règles de l'art la partie SI de la société avec le rôle Active Directory.

Toujours dans le but de sécuriser le SI, nous avons appliqué des GPOs en adéquation avec le rôle de chacun de nos collaborateurs. La mise en place du *Bureau à distance* nous permet d'entrevoir d'autres manières de déployer un ERP, ou une application métier. Si celle-ci requiert une version de Windows antérieure à celle actuellement déployée.

La partie Linux quant à elle fût riche en découvertes : nouvel OS, nouvel environnement, nouvelles façons de fonctionner et de penser. Nous avons dû faire preuve de persévérance et d'une rigueur absolue dans la mise en place du SaMBA 3, ainsi que dans celle du NFS et de sa fonction de backup.

Nous avons pu découvrir que sous Linux, toutes les configurations ne sont que fichier, qu'il est possible de modifier, à nos risques et périls...

Les projets futurs nous permettront d'en savoir encore plus, et c'est avec impatience que nous attendons le suivant.

Bilan personnel de Karine Kovacic :

Ce projet a été extrêmement enrichissant d'un point de vue technique. Certains aspects étaient pour moi jusqu'ici non pas inconnus mais assez flous et ce projet m'a permis d'éclaircir toutes ces zones d'ombre.

J'ai beaucoup apprécié la mise en place d'un Active Directory/DNS et des différentes stratégies de groupe.

Mais la partie Linux m'a plus attirée car configurer un système en ligne de commande est certes pas évident mais très enrichissant. J'ai réellement évolué dans le monde Linux.

La configuration des différents rôles de serveurs demande de la rigueur plus particulièrement sous linux.

La réalisation de ce projet m'a permis de comprendre l'importance de l'organisation et de l'anticipation.

XII – Pour aller plus loin

A. Mise en place d'un server OCS et GLPI

A.1. Intérêt d'un server OCS et GLPI



OCS Inventory NG est une application permettant de réaliser un inventaire de la configuration matérielle des machines du réseau et des logiciels qui y sont installés.

Ces informations peuvent être visualisées grâce à une interface web qui permet également de télé-déployer des applications sur un ensemble de machines.

L'interface web OCS Inventory est principalement consultative, elle présente en effet uniquement les informations relatives aux machines qui composent un parc.



Pour rendre la gestion d'un parc plus facile il existe un logiciel dédié, basé lui aussi sur une interface WEB, il s'agit de **GLPI**.

Solution open--source de gestion de parc informatique et de servicedesk, **GLPI** est une application Full Web pour gérer l'ensemble des problématiques de gestion de parc informatique : de la gestion de l'inventaire des composants matérielles ou logicielles d'un parc informatique à la gestion de l'assistance aux utilisateurs.

L'un des atouts principaux de **GLPI** c'est qu'il peut s'interfacer avec **OCS Inventory** afin de récupérer les informations relatives aux machines du parc qu'il contient.



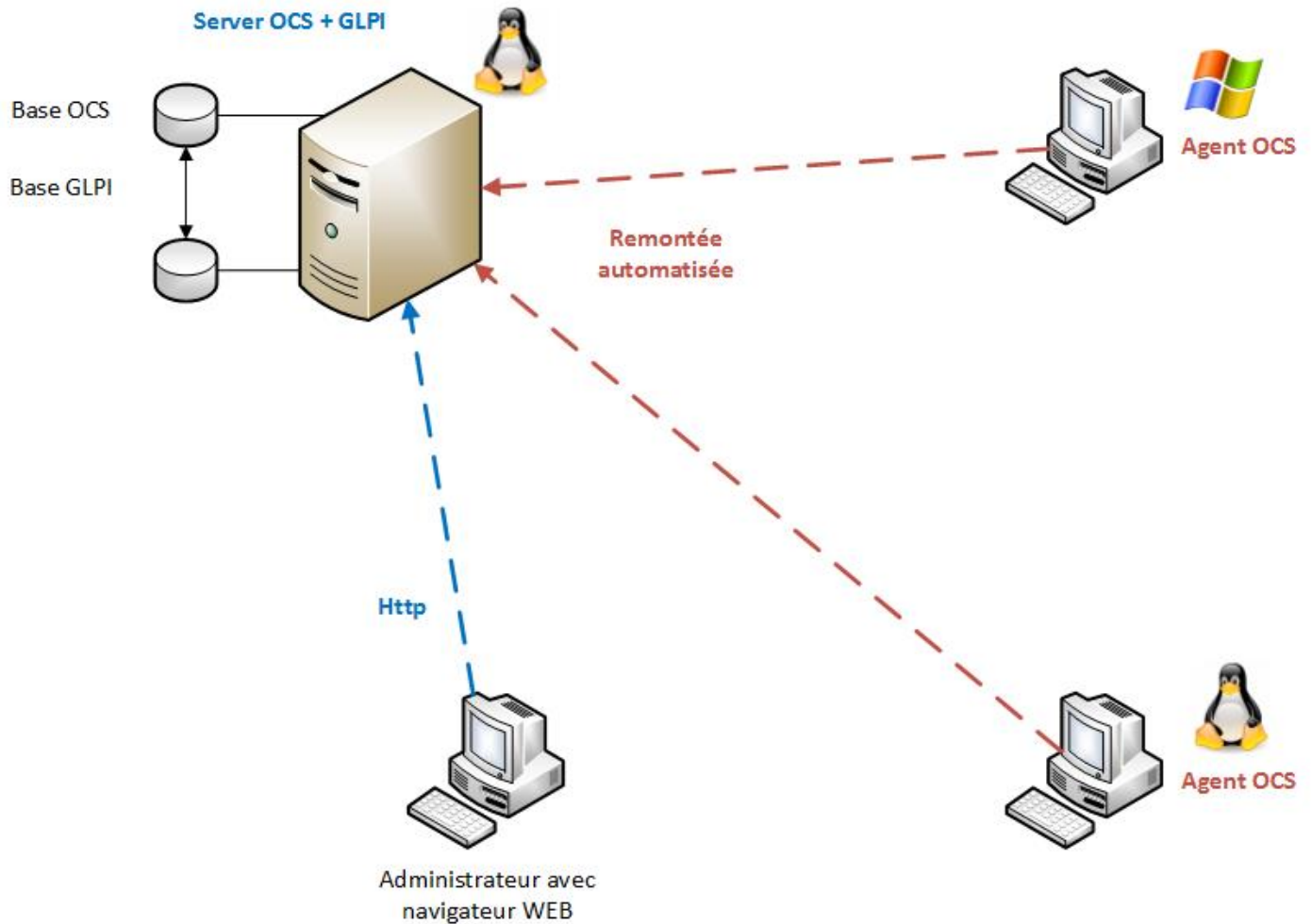
A.2. Principe de fonctionnement

Sur chaque poste du parc informatique sera installé sous forme de service, un logiciel appelé **Agent NG Inventory**.

Cet agent va inventorier la configuration matérielle et logiciel du poste et la sauvegarder sous forme de fichier. Ce fichier sera ensuite envoyé à travers le réseau vers le serveur OCS.

Ce serveur va interpréter ce fichier et créera un enregistrement dans sa base de données correspondant au poste et à toutes ses caractéristiques.

Ces caractéristiques seront ensuite présentées sous la forme d'un tableau visible à travers une interface web générée par le serveur OCS / GLPI.



A.3. Installation et configuration

Sur un serveur fonctionnant sous Linux Debian, nous allons installer un serveur **OCS Inventory** et **GLPI**.

Il suffit de télécharger les paquets et les bibliothèques nécessaires (Apache, Mysql, Perl, OCS_Server, GLPI, etc.)

Une fois ces paquets et bibliothèques installés, la configuration de ces deux serveurs se fait via leurs interfaces web respectives.

A.4. Déploiement de l'agent OCS Inventory sous linux

Il n'existe pas actuellement de méthode pour déployer en masse l'agent OCS sur des distributions Linux.

L'installation doit se faire manuellement sur chaque poste.

Là encore il suffit de télécharger les paquets nécessaires et de les installer.

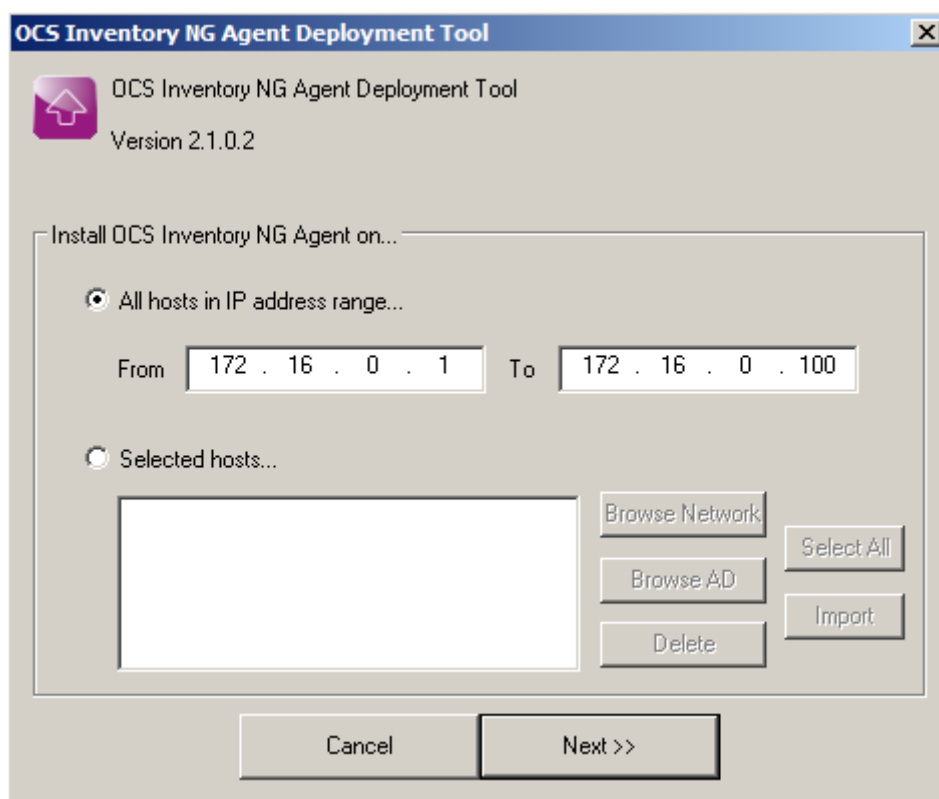
A.5. Déploiement de l'agent OCS Inventory sous Windows

L'agent OCS peut être déployé en masse dans un parc équipé de machines Windows par l'intermédiaire de GPO ou de script logon.

Il existe une 3eme méthode proposée par OCS, en utilisant [l'outil de déploiement OCS](#).

L'[outil de déploiement OCS](#) est un logiciel qui permet l'installation de l'agent OCS sur un parc machine de façon automatique et transparente.

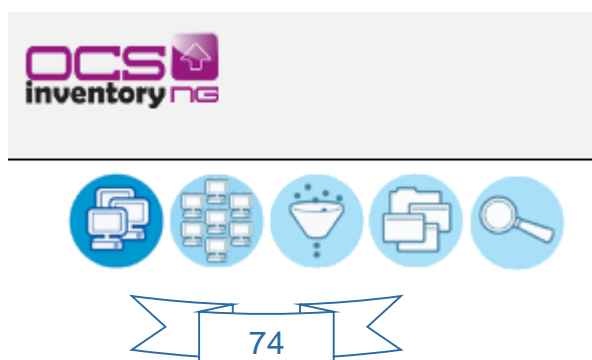
Il suffit pour cela de lui indiquer où se trouve l'exécutable de l'agent et de lui préciser la plage d'adresse IP dans laquelle se situent les machines sous Windows.



A.6. Remontée des informations dans OCS

Une fois l'agent déployé, les machines apparaissent dans l'interface web de gestion d'OCS Inventory.

On peut y voir le nom de la machine, toutes ses caractéristiques matérielles, tous les logiciels qui y sont installés, les périphériques connectés (imprimantes, écran, claviers etc..), ainsi que son adresse IP.



Account info: TAG	Last inventory	Computer	User	Operating system	RAM (MB)	CPU (MHz)	Select	Delete
NA	2014-06-30 09:07:28	COMPTA-002	g.gallez	Microsoft Windows 7 Professionnel	4096	3400	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-30 08:58:45	BE4	L.PINTO	Microsoft Windows XP Professional	3070	2992	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-30 08:34:21	MECA1	JM.CINUS	Microsoft Windows 7 Professionnel	24576	2660	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-30 08:10:57	GIH9	B.CAUDRON	Microsoft Windows 7 Professionnel	4096	1300	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-30 07:59:11	GIH6	s.hennart	Microsoft Windows 7 Professionnel	3072	2262	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-30 07:30:48	GIH10	vdebaveleere	Microsoft Windows 7 Professionnel	2048	2400	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-30 06:52:59	CFA01	TOURCN	Microsoft Windows 2000 Professional	640	1594	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-30 06:30:04	GALLEZ10	g.flament	Microsoft Windows 7 Professionnel	4096	3400	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-30 05:53:12	SRVGALLEZ	Administrateur	Microsoft Windows Server 2003 for Small Business Server	4096	2666	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-30 05:01:46	ADM20	A.Decanter	Microsoft Windows XP Professional	3072	2926	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-30 04:49:24	CADFLOW	S.SIX	Microsoft Windows 7 Professionnel	49152	2793	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-30 04:15:21	ADM1	S.LEROY	Microsoft Windows XP Professional	2048	2605	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-30 03:08:24	CFA06	r.mantone	Microsoft Windows 7 Professionnel	49152	2394	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-30 02:58:41	CTRL-SAS5	gsas	Microsoft Windows XP Professional	512	2793	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-30 01:29:57	GALLEZ08	gsas	Microsoft Windows 7 Professionnel	2048	2600	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-30 01:03:05	BE1	g.carpentier	Microsoft Windows 7 Professionnel	12288	2660	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-30 00:35:27	SAS53	gsas	Microsoft Windows 7 Professionnel	2048	1800	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-30 00:24:34	SAS41	l.pasz	Microsoft Windows 7 Professionnel	2048	3300	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-29 23:42:55	GALLEZ09	d.six	Microsoft Windows 7 Professionnel	4096	3400	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NA	2014-06-29 23:37:17	ADM3	C.DUPISON	Microsoft Windows Vista™ Professionnel	2048	2795	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Name:	COMPTA-002	Domain:	gallezsas.local
Userdomain:	gallezsas	IP address:	192.168.1.180 WOL
User:	g.gallez	Swap:	7994
OS Name:	Microsoft Windows 7 Professionnel	OS Version:	6.1.7601
Service pack:	Service Pack 1	Comments:	Microsoft
Windows user:	Move2IT	Windows licence:	00371-OEM-8992671-00524
Windows key:	32KD2-K9CTF-M3DJT-4J3WC-733WD	User agent:	OCS-NG_WINDOWS_AGENT_v2.1.1.1
Memory:	4096	Last inventory:	06/30/2014 09:07:28
Last contact:	06/30/2014 09:07:28	Uuid:	4C4C4544-0035-4E10-8036-B3C04F4C5931
Architecture:	x86 64 bit	Export:	XML

PROCESSOR(S)

1 Result(s) (Download)

Manufacturer	Type	Serial number	Frequency	Cores number	L2 cache size	Architecture	Data width	Current address width	Logical CPUS	Voltage	Current speed	Socket type
GenuineIntel	Intel(R) Core(TM) i3-3240 CPU @ 3.40GHz	CPU Enabled	3400	2	512	x86_64	64	64	4	2.9 volts	1598	CPU 1

NETWORK(S)

1 Result(s) (Download)

Description	Type	Speed	MAC address	Status	IP address	Netmask	Gateway	Network number	DHCP IP
Realtek PCIe GBE Family Controller	Ethernet	100 Mb/s	A4:1F:72:91:87:FA	Up	192.168.1.180	255.255.255.0	192.168.1.4	192.168.1.0	192.168.1.90

SOFTWARE

Show: 20

Restrict view: Filter

Add column:

383 Result(s) (Download)

Editor	Name	Version	Comments
	7-Zip 9.20		
Adobe Systems Incorporated	Adobe Flash Player 13 ActiveX	13.0.0.214	
	Cobian Backup 10		
Foxit Corporation	Foxit Reader 5.1	5.1.0.1021	
Cieme Informatique	Infoserv	2.7	
Alcatel-Lucent	OHL Driver	2.3.8	
Mozilla	Mozilla Firefox 29.0.1 (x86 fr)	29.0.1	Mozilla Firefox 29.0.1 (x86 fr)
Mozilla	Mozilla Maintenance Service	29.0.1	Mozilla Maintenance Service 29.0.1 (x86 en-US)
OCS Inventory NG Team	OCS Inventory NG Agent 2.1.1.1	2.1.1.1	
Microsoft Corporation	Microsoft Office Professionnel 2010	14.0.7015.1000	
Trend Micro	Trend Micro Client/Server Security Agent	16.0.4177	
Microsoft Corporation	Windows Live	16.4.3505.0912	
Frank Heindörfer, Philip Chinery	PDFCreator	1.2.3	PDFCreator - Opensource
Microsoft Corporation	Windows Live Communications Platform	16.4.3505.0912	
Dell Inc.	Dell Client System Update	1.3.0	Application is used for scanning and deployment of Drivers, Firmware and BIOS Updates for your system.
Microsoft Corporation	Windows Live Mail	16.4.3505.0912	
Sage	Sage 100 pour SQL Server poste Client	17.11	
Microsoft Corporation	Photo Gallery	16.4.3505.0912	
Microsoft Corporation	Junk Mail filter update	16.4.3505.0912	
Microsoft Corporation	Galerie de photos	16.4.3505.0912	

A.7. Interfaçage OCS – GLPI

Comme indiqué, GLPI est un logiciel libre complet facilitant la gestion d'un parc informatique.

Au-delà de pouvoir présenter l'inventaire du parc comme peut le faire OCS, GLPI permet en plus d'y associer différents services comme un service de ticketing de type Helpdesk par exemple.

Ainsi il peut être utile d'interfacer la base de données OCS avec celle de GLPI afin de récupérer automatiquement la liste des ordinateurs composant le parc.

Cette connexion se fait grâce à un plugin pour GLPI qui va synchroniser les données entre la base OCS et celle de GLPI.

Une fois cette synchronisation effectuée, les ordinateurs du parc sont importés et visibles dans GLPI.

Nom	ID	Statut	Fabricant	Numéro de série	Type	Modèle	Système d'exploitation	Lieu	Dernière modification	Usager
MECA1	11		Dell Inc.	7GTH45J	Tower	Precision WorkStation T5500	Microsoft Windows 7 Professionnel		2014-06-06 10:04	jm.cinus
FAO3	12		Dell Inc.	88KQW2J	Tower	Precision WorkStation 390	Microsoft Windows XP Professional		2014-06-13 11:35	b.coquerelle
CFAO10	15		Dell Inc.	7WPZ52J	Tower	Precision WorkStation 380	Microsoft Windows XP Professional		2014-06-13 11:36	erosion
BE1	16		Dell Inc.	4SHJX4J	Tower	Precision WorkStation T5500	Microsoft Windows 7 Professionnel		2014-06-05 08:25	g.carpentier
JOHN-PC	1		Dell Inc.	684LJ3J	Tower	Precision WorkStation T3400	Microsoft Windows 7 Professionnel		2014-06-13 11:36	jsion
BE8	5		Dell Inc.	8594NW1	Tower	Precision T5600	Microsoft Windows 7 Professionnel		2014-06-04 12:14	c.tricat
BE7	35		Dell Inc.	FLTH45J	Tower	Precision WorkStation T5500	Microsoft Windows 7 Professionnel		2014-06-13 11:35	s.six
BE5	6		Dell Inc.	DPZXQ4J	Tower	Precision WorkStation T3500	Microsoft Windows 7 Professionnel		2014-06-13 11:36	H.CHENET
CFAO6	23		Dell Inc.	496S95J	Tower	Precision WorkStation T5500	Microsoft Windows 7 Professionnel		2014-06-04 15:37	r.mantone
BE4	7		Dell Inc.	384LJ3J	Tower	Precision WorkStation T3400	Microsoft Windows XP Professional		2014-06-13 11:36	L.PRINTO
CADFLOW	25		Dell Inc.	8GTH45J	Tower	Precision WorkStation T5500	Microsoft Windows 7 Professionnel		2014-06-05 08:25	S.SIX
GALLEZ10	29		Dell Inc.	474DF02	Space-saving	OptiPlex 3020	Microsoft Windows 7 Professionnel		2014-06-05 08:25	g.flament
GALLEZ09	21		Dell Inc.	354DF02	Space-saving	OptiPlex 3020	Microsoft Windows 7 Professionnel		2014-06-13 11:35	d.six
SRVGALLEZ	50		Dell Inc.	BP8BW4J	Rack Mount Chassis	PowerEdge R510	Microsoft Windows Server 2003 for Small Business Server		2014-06-06 11:46	Administrateur
GALLEZ-GPA03	52		Dell Inc.	3MGSR3J	Rack Mount Chassis	PowerEdge 2950	Microsoft Windows Server 2003 R2 Enterprise Edition		2014-06-06 16:07	administrateur
GIH8	39		Dell Inc.	D0F9GS1	Portable	Vostro 3560	Microsoft Windows 7 Professionnel		2014-06-05 12:21	
GALLEZ07-PC	40		Dell Inc.	B06YQS1	Portable	Dell System Vostro 3450	Microsoft Windows 7 Professionnel		2014-06-05 15:10	Administrateur
SAS40	41		Dell Inc.	F4R4JR1	Portable	Vostro 3550	Microsoft Windows 7 Professionnel		2014-06-13 11:36	M.PLUQUET
ADM7	26		Dell Inc.	C6991M1	Portable	Inspiron 1012	Microsoft Windows XP Professional		2014-06-05 08:25	G.CAPONE
SAS50	42		Dell Inc.	7H4D1N1	Portable	Vostro 3500	Microsoft Windows 7 Professionnel		2014-06-06 11:47	Syst

Dans OCS serveur, chaque caractéristique d'un poste était présentée sur une page web distincte, GLPI permet par contre de visualiser l'ensemble des informations relatives à un poste sur une seule et même page grâce à l'utilisation d'onglets.

Liste : 44/50

Composants(26) Volumes(2) Logiciels(369) Connexions(7) Ports réseaux(1) Gestion Contrats Documents Machines virtuelles

Ordinateur - ID 1

Liste : 44/50

Composants(26) Volumes(2) Logiciels(369) Connexions(7) Ports réseaux(1) Gestion Contrats Documents Machines virtuelles

Ordinateur - ID 1

Nom :	JOHN-PC	Statut :	-----
Lieu :	-----	Type :	Tower
Responsable technique :	-----	Fabricant :	Dell Inc.
Groupe technique :	-----	Modèle :	Precision WorkStation T3400
Usager numéro :		Numéro de série :	684LJ3J
Usager :	ision	Numéro d'inventaire :	
Utilisateur :	ision	Réseau :	-----
Groupe :	-----	GIH-INFO3 Swap : 8058	
Domaine :	gallezas.local		
Système d'exploitation :	Microsoft Windows 7 Professionnel	Commentaires :	
Service pack :	Service Pack 1		
Version du système d'exploitation :	6.1.7601		
Product ID du système d'exploitation :	00371-OEM-8992671-00524		
Numéro de série du système d'exploitation :	32KD2-K9CTF-M3DJT-4J3WC-733WD		
UUID :	4C4C4544-0038-3410-804C-B6C04F4A334A		
Source de mise à jour :	-----		

Dernière modification : 2014-06-13 11:36

Actualiser

Liaison OCSNG

Date dernier inventaire OCSNG :	2014-06-13 00:55
Date d'import dans GLPI :	2014-06-13 11:36
Serveur :	localhost
Agent :	OCS-NG_WINDOWS_AGENT_v2.1.1.1
Mise à jour automatique OCSNG :	Oui

Supprimer

Composants

1	Processeur	Intel(R) Core(TM)2 Duo CPU E6850 @ 3.00GHz [2 core(s) x86_64]	Fréquence :	2992	MHz
1	Mémoire	DDR2 - DIMM_1 (Multi-bit ECC)	Type : DDR2	Fréquence : 800	Taille : 2048 Mio
1	Mémoire	DDR2 - DIMM_2 (Multi-bit ECC)	Type : DDR2	Fréquence : 800	Taille : 2048 Mio
1	Disque dur	WDC WD2500AAJS-75VVA0 ATA Device			Capacité : 238417 Mio
1	Carte réseau	Contr?leur Broadcom NetXtreme 57xx Gigabit	Débit : 100 Mb/s		Adresse Mac : 00:1D:09:2E:D4:EC
1	Lecteur	HL-DT-ST DVD+-RW GSA-H73N ATA Device	Écriture : Oui		
1	Lecteur	ELBY CLONEDRIVE SCSI CdRom Device	Écriture : Oui		
1	Carte graphique	NVIDIA Quadro FX 1700			Mémoire : 512 Mio
1	Carte son	Périphérique High Definition Audio			

B. Mise en place de serveur et client NFS – Sauvegarde du serveur de fichiers

B.1. Intérêt d'un serveur et client NFS

Au sein de notre système informatique, nous avons mis en place du partage de fichier entre machines Linux et machines Windows par l'intermédiaire d'un [serveur Samba](#).

Or si nous voulons mettre en place du partage de fichiers entre machines fonctionnant sous Linux, il nous faut mettre en place un [serveur NFS](#).

Il y a un double intérêt à mettre en place du partage de fichiers entre machines sous Linux.

D'une part cela permettra à d'éventuels postes fonctionnant sous Linux de partager des fichiers entre eux, mais aussi et surtout d'autre part cela va nous permettre de réaliser une sauvegarde de notre serveur de fichier qui lui aussi fonctionne sous Linux.

B.2. Principe de fonctionnement

Nous avons deux serveurs fonctionnant sous Linux.

Serveur NFS
(srvftp)



Le premier serveur, fera office de **serveur NFS** et proposera sur le réseau **un répertoire partagé d'accueil**, qui sera destiné à recevoir l'archive compressée de notre serveur de fichier.

Ici par exemple, il pourra s'agir de notre serveur linux hébergeant le service FTP (srvftp).

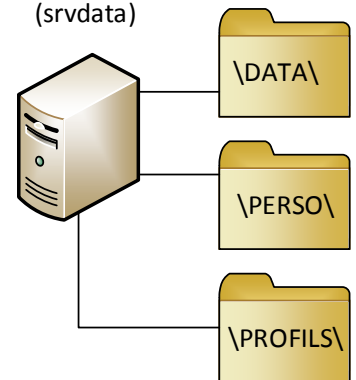
Le second serveur, sera le **client NFS**.

C'est sur ce serveur que se situent les données sensibles que l'on souhaite sauvegarder.

Ici en l'occurrence, il s'agit de l'ensemble des données partagées par notre serveur SAMBA, à savoir les répertoires :

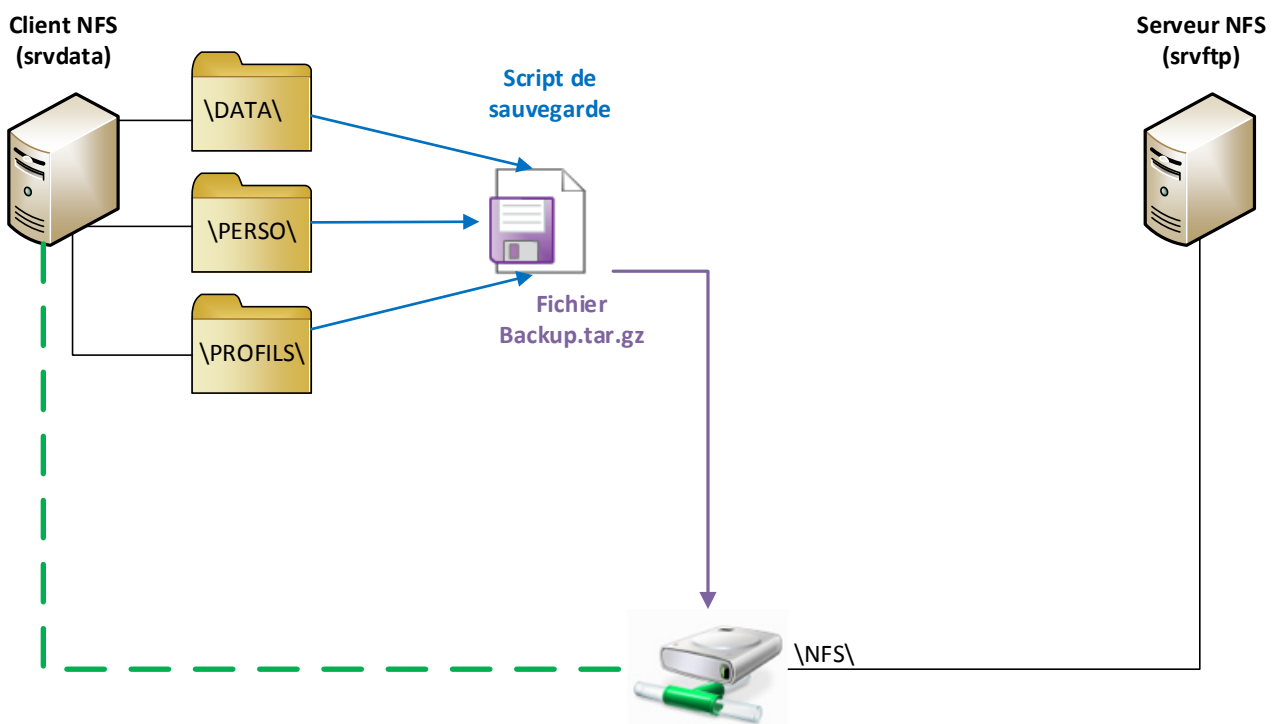
- **DATA** : qui contient l'ensemble des documents et données de chaque service.
- **PERSO** : qui contient l'ensemble des répertoires personnels des collaborateurs.
- **PROFILS** : qui contient l'ensemble des profils itinérants.

Client NFS
(srvdata)



Sur ce serveur sera monté/connecté le **répertoire partagé** proposé par le serveur NFS.

Un script va compresser les 3 répertoires sous **la forme d'un fichier** qui sera sauvegardé sur le **lecteur réseau**.



B.3. Installation et configuration

B.3.1. Coté serveur

Il suffit de télécharger les paquets permettant la mise en place d'un serveur NFS grâce à la ligne de commande suivante.

```
srvnfs:/# apt-get install nfs-kernel-server
```

Une fois l'installation terminée, il faut créer le répertoire partagé destinée à accueillir le fichier de sauvegarde.

```
srvnfs:/# mkdir /srv/NFS/  
srvnfs:/#chmod 777 -R /srv/NFS/
```

Il faut ensuite configurer le fichier « /etc/exports » pour partager ce répertoire sur le réseau.

```
/srv/NFS 172.16.0.3(rw,root_squash,no_subtree_check)
```

Et enfin redémarrer le service NFS

```
/etc/init.d/nfs-kernel-server restart
```

B.3.2. Coté Client

Il faut télécharger les paquets permettant de connecter un répertoire partagé.

```
clientnfs:/# apt-get install nfs-common
```

Puis nous devons créer un répertoire dans lequel viendra se connecté le répertoire partagé.

```
clientnfs:/# mkdir /media/NFS  
clientnfs:/# chmod -R 777 /media/NFS
```


Enfin, nous devons connecter le répertoire partagé, en le montant directement dans la table de partition, en éditant le fichier « /etc/fstab ».

En ajoutant la ligne suivante :

```
172.16.0.5:/srv/NFS/ /media/NFS nfs defaults,user,auto,noatime,intr 0 0
```

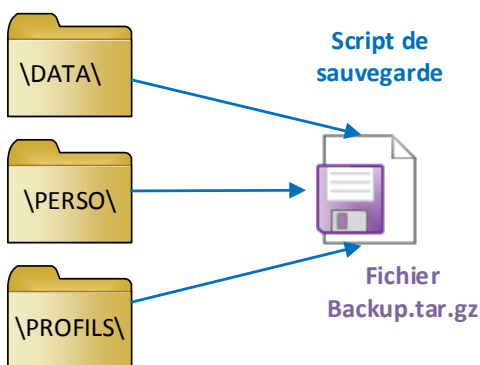
Nous pouvons vérifier la présence d'un répertoire partagé sur le réseau grâce à la ligne de commande suivante :

```
clientnfs:/# showmount -e 172.16.0.5
```

Qui renvoie :

```
Export list for 172.16.0.5  
/srv/NFS/ 172.16.0.3
```

B.4. Sauvegarde du serveur de partage de fichiers



La sauvegarde de notre serveur de fichiers se fera à l'aide d'un script qui va compresser sous la forme d'un fichier nos 3 répertoires (Data, Perso, Profils).

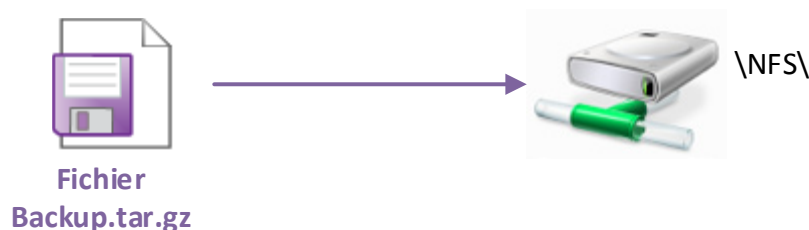
L'intérêt d'un script c'est qu'il va permettre d'une part d'automatiser la sauvegarde.

En effet, il suffira de lancer le script pour générer le fichier, aucune ligne de commande complexe ne devra être saisie à chaque fois.

D'autre part il sera possible de planifier l'exécution de ce script et donc ainsi de planifier la sauvegarde.

A l'intérieur de ce script il sera possible de définir le répertoire dans lequel sera généré/enregistré le fichier compressé.

Ici nous choisisons le répertoire partagé par le serveur NFS.



Voici un exemple de script simple qui crée une sauvegarde à la date du jour.

```
1  !/bin/sh
2
3  echo "-----";
4  echo "- Sauvegarde répertoires DATA/PROFILS/PERSO";
5  echo "-----";
6  echo "";
7
8  echo "Création de l'archive";
9
10 #on crée l'archive en .tar en précisant entre guillemets les chemins
11 # absolus des dossiers à sauvegarder
12 # le nom de l'archive est précédé par la date et l' heure
13 # du jour d'archivage - cela évite un écrasement de l'archive
14
15 tar -cvzf /media/NFS/$(date +%d-%m-%Y-%H:%M).backup.tar.gz "/PERSO/" "/DATA/" "PROFILS"
16 echo "-----";
17 echo "";
18
19 echo "Vérification de l'existence de l'archive";
20 # On test si l'archive à bien été crée
21 if [ -e /media/NFS/$(date +%d-%m-%Y-%H:%M)backup.tar.gz ]
22 then
23 echo "";
24 echo "Votre archive a bien été créée.";
25 echo "";
26 else
27 echo "";
28 echo "il y eu un problème lors de la création de l'archive.";
29 echo "";
30 fi
31
32 echo "----- Fin dela sauvegarde -----";
33
```

Il est ensuite possible de planifier l'exécution de ce script en modifiant le crontab du serveur client

```
clientnfs:/# crontab -e
```

Par exemple, si l'on souhaite effectuer une sauvegarde journalière à 19h00, ajouter la ligne suivante :

```
#m h dom mon dow command
00 19 * * * /script_backup.sh
```

Voici le résultat de l'exécution de ce script planifié toutes les 2 minutes :

```
02-07-2014-09:04.backup.tar.gz  
02-07-2014-09:06.backup.tar.gz  
02-07-2014-09:08.backup.tar.gz  
02-07-2014-09:10.backup.tar.gz  
02-07-2014-09:12.backup.tar.gz  
02-07-2014-09:14.backup.tar.gz  
02-07-2014-09:16.backup.tar.gz
```