
PROJET EVOLUTION

Evolution d'un parc informatique



LOUIS BRET

QUENTIN ROBYNS

FLORIAN GUYOT

WEBER RAPHAEL

TABLE DES MATIERES

Préambule..... 4

Contexte..... 5

 Problématique initiale 5

 L'existant 6

 Choix des locaux techniques 6

 Plan de câblage réseau des bâtiments..... 8

 Matériel 10

 Le réseau 16

Cahier des charges..... 17

Planning de répartition des tâches..... 20

Adressage IP 21

Les serveurs 28

Serveurs Windows 29

 Serveur physique IDM-SRV-DC1 30

 Active Directory (AD) : 30

 DNS..... 31

 Hyperviseur IDM-SRV-HV1 32

 AD-DNS..... 32

 DFS..... 32

 Hyperviseur IDM-SRV-HV2 33

 Serveur d'impression..... 33

 Réplication du DFS..... 34

Sécurité et accès aux données..... 35

 DROIT NTFS 35

 Gestion des imprimantes : 35

 GPO 35

 Scripts PowerShell..... 42

Serveur Linux 43

 Debian 43

 Mise en place 44

 Kerberos 44

 FTP 45

 Samba..... 45

 NFS 46

Service NFS	46
Client NFS	46
DHCP	47
Notre outil de gestion de parc.....	48
Présentation du logiciel développé en interne :	49
Schéma de la base de donnée du logiciel	51
Devis	52
Planning de mise en place globale.....	55
Annexes	56
Installation de Windows Serveur 2016 – CORE	56
Configuration de Windows Serveur 2016 – CORE	61
Installation de Windows 10 Client avec RSAT	66
Configuration IP et nominale de Windows 10.....	71
Liaison entre RSAT et le Serveur	74
Installation du rôle AD-DS/DNS sur le serveur.....	79
Mise en place de la zone inverse du DNS	82
Création et paramétrage du serveur de réplication AD-DNS	87
Installation du rôle DFS	100
Installation du serveur d'impression	106
Scripts PowerShell complets.....	110
Installation Linux Debian	116
FTP	125
Samba.....	128
Configuration du serveur NFS	132
DHCP	134
Tableau des commandes SQL	140
Devis non retenus.....	141
Sources.....	143

PREAMBULE

Dans le cadre du projet Evolution, qui est la suite du projet Start, de notre formation de gestionnaire en maintenance et support informatique, nous devons mettre en place l'administration du parc informatique de l'entreprise.

Ce projet d'administration du parc informatique induit l'implémentation de serveurs, Windows ainsi que Linux.

Voici les objectifs pédagogiques du projet Evolution :

- Mettre en œuvre les outils d'administration de Windows server
- Mettre en œuvre les outils d'administration UNIX/LINUX
- Être capable de sécuriser l'accès aux réseaux et aux données de l'entreprise
- Rédiger des rapports écrits adaptés au contexte professionnel
- Être capable de créer et gérer une base de données relationnelle
- Être capable d'automatiser les tâches à l'aide d'un outil de programmation (PowerShell).

Dans ce projet, nous nous mettons dans la situation où l'entreprise existe réellement donc le rapport est rédigé comme s'il était remis au directeur administratif et financier d'ID'meubles.

CONTEXTE

PROBLEMATIQUE INITIALE

L'entreprise a emménagé il y a maintenant quelques mois dans de nouveaux locaux. L'équipe informatique se heurte cependant à quelques problèmes. Le directeur administratif et financier nous a donc soumis quelques idées afin que nous lui propositions des solutions.

Voici ces idées :

- 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 quelques parts sur le parc (Nom d'hôtes, type de machines...);
- Il n'y a pas de gestion des droits utilisateurs ;
- Le siège social à besoin d'un serveur ftp (ils veulent récupérer des fichiers dessus), c'est le moment de tester la mise en place d'un serveur linux ;
- Vous devez implémenter Active Directory dans l'entreprise (voir « Vos ressources » ci-dessous, vous avez certaines consignes plus précises) ;
- Il veut un planning prévisionnel, un suivi et un planning réel de vos travaux (un tableau d'indicateurs, le qui fait quoi... par exemple) ;
- Il veut un rapport d'activité globale sur la faisabilité et les solutions mises en place suivant le cahier des charges, les procédures d'installation, de déploiement, le prix...tout ça en suivant la charte de l'entreprise.

L'EXISTANT

CHOIX DES LOCAUX TECHNIQUES

BATIMENT PRINCIPAL :

BATIMENT PRINCIPAL

Salle	Ouverture de porte	Porte verrouillable	Type d'éclairage	Interrupteur éclairage	Plafond suspendu	Autres réseaux	Présence d'un local à l'étage	Peinture ignifugée	Nb de prise
A	Interieur	Non	Fluorescent	Oui	Oui	Non	Non	Oui	0
B	Interieur	Oui	Fluorescent	Oui	Oui	Eau	G	Oui	2
C	Exterieur	Oui	Incandescent	Oui	Non	Non	H	Oui	4
D	Exterieur	Oui	Incandescent	Oui	Oui	Electricité	Non	Oui	4
E	Exterieur	Oui	Incandescent	Oui	Oui	Non	Non	Oui	3
F	Exterieur	Oui	Incandescent	Oui	Oui	Non	J	Oui	4
G	Interieur	Non	Incandescent	Oui	Oui	Eau		Oui	4
H	Exterieur	Oui	Fluorescent	Oui	Non	Non		Oui	5
I	Exterieur	Oui	Incandescent	Oui	Oui	Non		Oui	6
J	Interieur	Oui	Fluorescent	Non	Oui	Non		Oui	2
K	Exterieur	Oui	Incandescent	Oui	Oui	Non		Oui	1



Critère éliminatoire

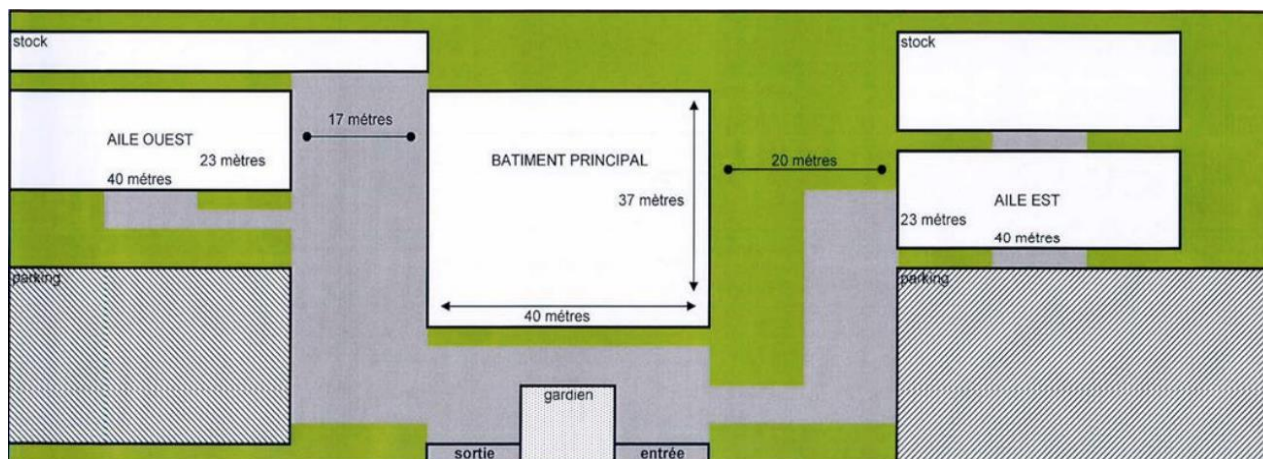


Choix retenu

Pour le rez-de-chaussée du bâtiment principal, nous avons choisi l'emplacement **C** pour l'implantation de notre local technique car il répond aux exigences des normes imposées. Et il contient 4 prises de courant.

Pour le 1er étage du bâtiment principal, nous avons choisi l'emplacement **H** pour l'implantation de notre local technique car il répond aux exigences des normes imposées.

Le seul point négatif était la présence d'un éclairage de type fluorescent dans le local **H** qui a été changé par l'équipe d'électriciens.



BATIMENT AILE EST :

AILE EST

Salle	Ouverture de porte	Porte verrouillable	Type d'éclairage	Interrupteur éclairage	Plafond suspendu	Autres réseaux	Présence d'un local à l'étage	Peinture ignifugée	Nb de prise
L	Exterieur	Oui	Incandescent	Oui	Non	Non	Q	Oui	3
M	Exterieur	Non	Fluorescent	Non	Non	Eau	O	Oui	2
N	Exterieur	Oui	Incandescent	Oui	Non	Electricité	P	Oui	4
O	Exterieur	Oui	Incandescent	Oui	Oui	Eau		Oui	4
P	Exterieur	Oui	Fluorescent	Oui	?	Non		Oui	4
Q	Exterieur	Oui	Incandescent	Oui	Non	Non		Oui	4



Critère éliminatoire



Choix retenu

Pour le rez-de-chaussée de l'aile est, nous avons choisi l'emplacement **L** pour l'implantation de notre local technique car il répond aux exigences des normes imposées. Et il contient 3 prises de courant.

Pour le 1er étage de l'aile est, nous avons choisi l'emplacement **Q** pour l'implantation de notre local technique car il répond aux exigences des normes imposées. Et il contient 4 prises de courant.

BATIMENT AILE OUEST :

AILE OUEST

Salle	Ouverture de porte	Porte verrouillable	Type d'éclairage	Interrupteur éclairage	Plafond sus-pendu	Autres réseaux	Présence d'un local à l'étage	Peinture ignifugée	Nb de prise
R	Exterieur	Oui	Incandescent	Oui	Non	Electricité	U	Oui	4
S	Exterieur	Oui	Incandescent	Non	Oui	Eau	V	Oui	3
T	Exterieur	Oui	Incandescent	Oui	Non	Non	Non	Oui	4
U	Exterieur	Oui	Fluorescent	Oui	Oui	Non		Amiante	4
V	Exterieur	Oui	Incandescent	Oui	Oui	Eau		Amiante	4
W	Exterieur	Oui	Incandescent	Oui	?	Non		Oui	2



Critère éliminatoire







Choix retenu

Pour le rez-de-chaussée de l'aile ouest, nous avons choisi l'emplacement **T** pour l'implantation de notre local technique car il répond aux exigences des normes imposées. Et il contient 4 prises de courant.

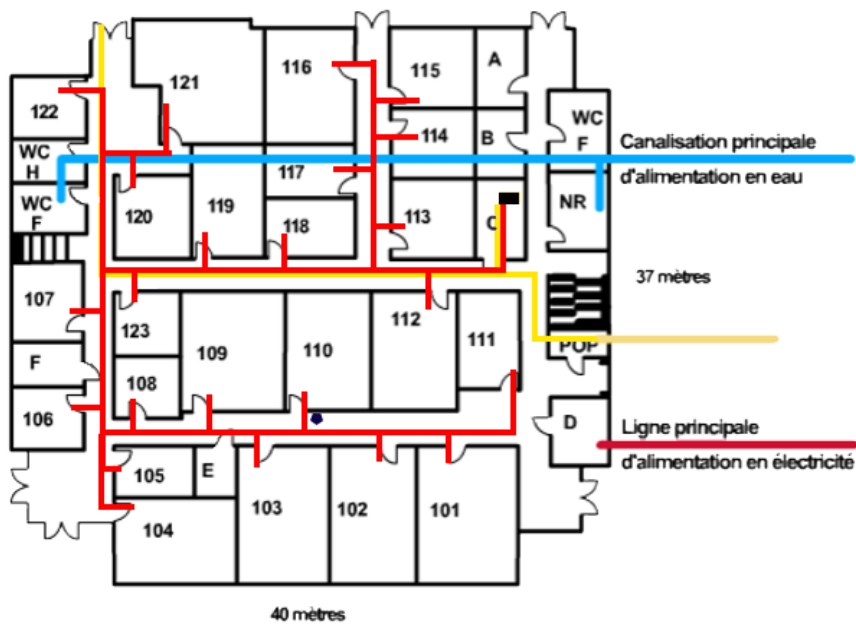
Pour le rez-de-chaussée de l'aile ouest, nous avons choisi l'emplacement **W** pour l'implantation de notre local technique car il répond aux exigences des normes imposées. Et il contient 2 prises de courant.

PLAN DE CABLAGE RESEAU DES BATIMENTS

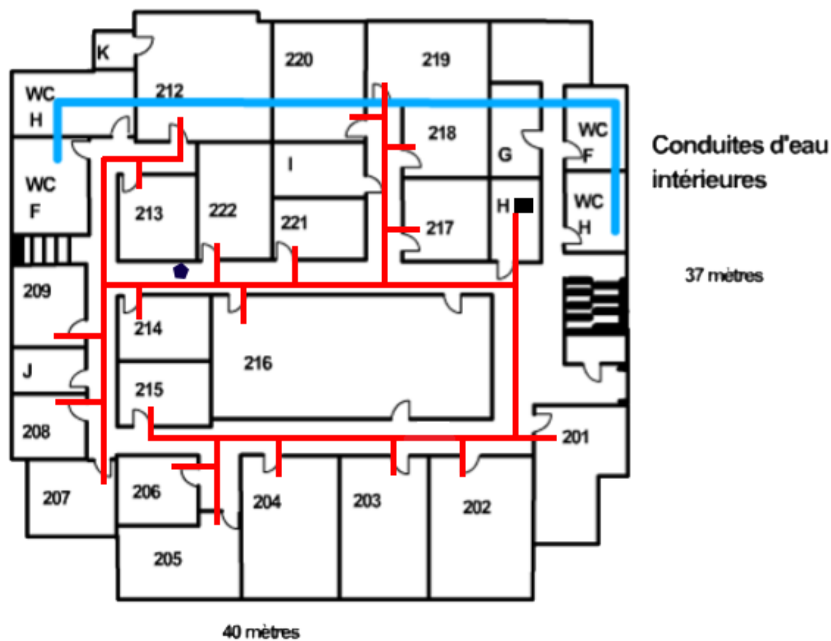
Nous utiliserons les légendes suivantes :

-  Imprimante
-  Câbles RJ45
-  Fibre optique
-  Switch

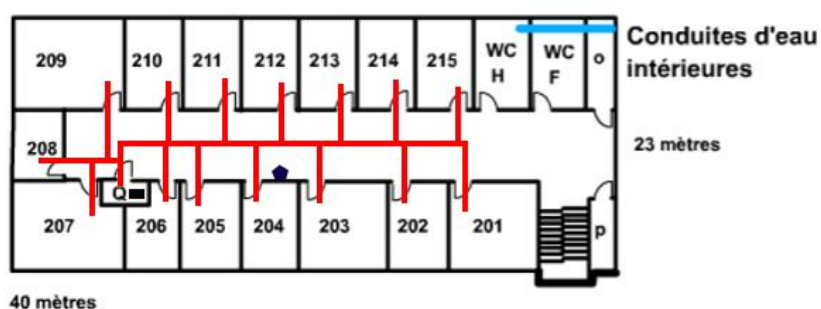
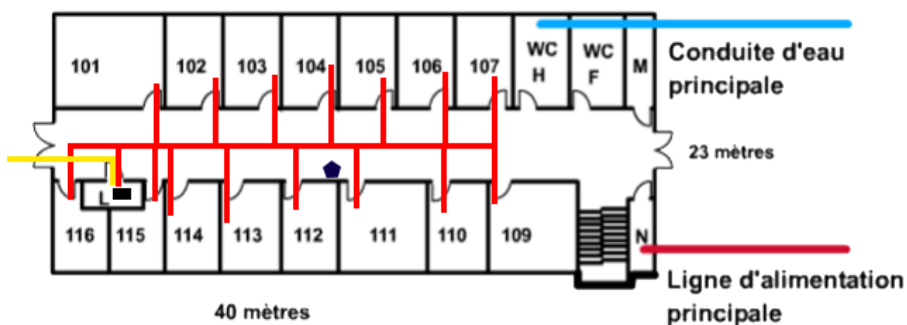
Bâtiment principal :



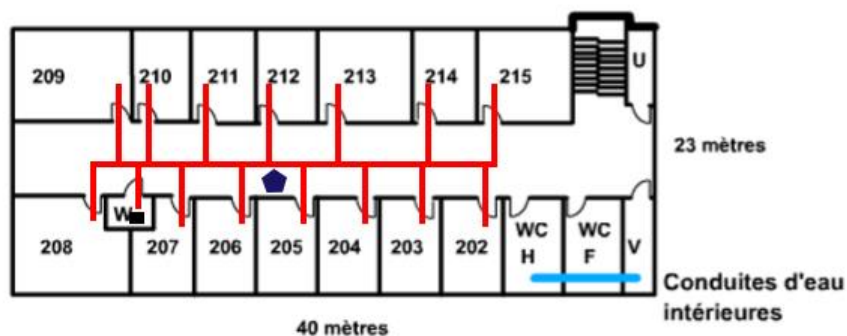
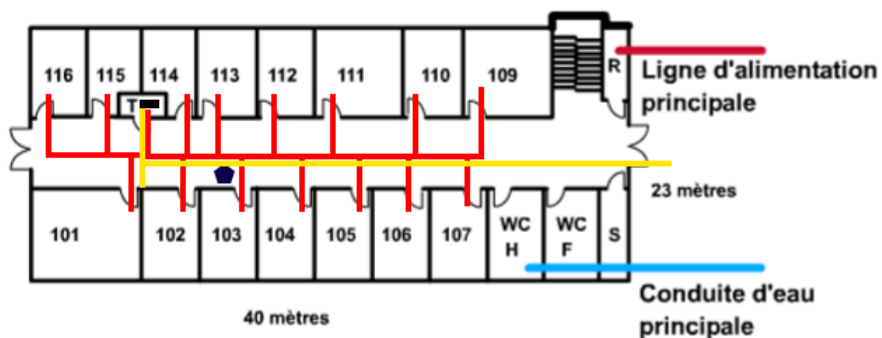
*



Bâtiment Est :



Bâtiment Ouest :



MATERIEL

Cela fait quelques mois que nous avons emménagé dans de nouveaux locaux. Lors de ce changement de locaux, nous avons renouvelé le matériel du parc informatique. Voici, les trois devis du matériel précédemment acheté ainsi que leur description.



DEVIS No.1542174

Date du devis	20/03/2018
Référence du devis	1542174
Numéro de client	51584
Date de validité du devis	19/04/2018
Modalité de paiement	30 jours
Emis par	Jean Michel
Contact client	ID'Meuble

Destinataire :
ID'Meuble
35 rue de sillac
16000
Angoulême

Infos additionnelles

Merci d'avoir choisi Ingram

La livraison sera effectuée dans les 4 semaines après réception de la confirmation de la commande ;

Description	Quantités	Prix unitaires HT	TVA %	TVA	TOTAL TTC
Acer Veriton ES2710G-I3/4Go/128SSD	89	370,00 €	20,00%	74,00 €	39 516,00 €
Acer Veriton M4650G-I7/8Go/256SSD+1HDD/K620	2	950,00 €	20,00%	190,00 €	2 280,00 €
Office 2016 Professional	91	91,00 €	20,00%	18,20 €	9 937,20 €
Eset EndPoint	92	45,00 €	20,00%	9,00 €	4 968,00 €
APC-Onduleur 1000VA	6	350,00 €	20,00%	70,00 €	2 520,00 €

Total HT 58 860,00 €
TVA 361,20 €

Total TTC 59 221,20 €

Signature du client (précédée de la mention « Bon pour accord »)

Acer Veriton ES2710G-I3/4Go/128SSD

Ce sont les PC qui ont remplacés les anciens PC des utilisateurs, qui étaient obsolètes d'un point de vue matériel.

Voici la configuration de ces tours :

- Processeur Intel Core i3-6100 (Dual-Core 3.7 GHz - Cache 3 Mo)
- 4 Go de mémoire vive DDR4 (maximum 32 Go au total)
- Fonctionnement rapide avec un SSD de 256 Go
- Graveur DVD multiformats compatible M-DISC
- 1 slot PCIe x16 pour l'ajout d'une carte graphique
- Connecteurs vidéo : VGA + HDMI
- Connexion réseau Gigabit Ethernet
- Alimentation de 220 Watts certifiée 80PLUS Bronze
- Clavier et souris USB fournis
- Windows 10 Professionnel 64 bits

Acer Veriton M4650G-I7/8Go/256SSD+1HDD/K620

Ce sont les PC qui ont remplacés les anciens présents pour les responsables de service, qui étaient obsolètes et limités d'un point de vue matériel. Nous devons leur donner des PC avec une puissance supérieure aux PC des autres utilisateurs en vue de l'utilisation de logiciels plus lourds.

Office 2016 Professionnel

Office est une suite bureautique qui comprend notamment :

- Excel
- Word
- PowerPoint

Office offre une pleine compatibilité avec les fichiers reçus et envoyés par d'autres sociétés, là où une suite bureautique autre pourrait causer un problème de compatibilité, ou d'affichage de certains caractères.

Eset EndPoint

Eset EndPoint est l'antivirus que nous avons choisi. D'après une étude du meilleur anti-virus, Eset EndPoint semble faire partie des meilleurs anti-virus en ce moment, d'après des benchmarks ainsi qu'un Gartner.

APC-Onduleur 1000VA

L'onduleur protège efficacement l'alimentation des équipements réseau. Cet onduleur protège les données critiques en fournissant une alimentation réseau fiable.

REXEL

DEVIS No.1542184

Date du devis 20/03/2018
Référence du devis 1542184
Numéro de client 51818
Date de validité du devis 19/04/2018
Modalité de paiement 30 jours
Emis par Michel Brutini
Contact client ID'Meuble

Destinataire :
ID'Meuble
35 rue de sillac
16000
Angoulême

Infos additionnelles

Merci d'avoir choisi Rexel

La livraison sera effectuée dans les 4 semaines après réception de la confirmation de la commande ;

Description	Quantités	Prix unitaires HT	TVA %	TVA	TOTAL TTC
Bandeaux de Brassage 24 Ports avec noyaux	12	130,00 €	20,00%	26,00 €	1 872,00 €
Prise RJ45 Mural Cat 7	218	11,00 €	20,00%	2,20 €	2 877,60 €
Baie 26U	1	350,00 €	20,00%	70,00 €	420,00 €
Baie 12U	5	170,00 €	20,00%	34,00 €	1 020,00 €
Cable Reseau Cat 7(Bobine de 300M)	19	265,00 €	20,00%	53,00 €	6 042,00 €
Fibre Optique OM3	200	2,33 €	20,00%	0,47 €	559,20 €
Materiel de Brassage(Cable ,Panneau Balais,...	1	200,00 €	20,00%	40,00 €	240,00 €

Total HT 12 805,13 €
TVA 225,67 €

Total TTC 13 030,80 €

Signature du client (précédée de la mention « Bon pour accord »)

Bandeaux de Brassage 24 Ports avec noyaux

Le bandeau de brassage sert, dans la baie de brassage, à repérer les câbles réseau. Cela facilite le raccordement entre les équipements réseau et les points d'accès.

Prise RJ45 Murale Cat 7

Suite à notre emménagement dans ces nouveaux locaux, nous avons dû installer des prises réseau dans les bâtiments.

Baie 26U et Baie 12U

La baie est l'endroit où sera installé tous les équipement réseaux, entre autres, les switchs, les serveurs, le bandeau de brassage... « 26U » est la place disponible dans la baie, cela signifie que l'on peut stocker 26 unités, soit 26 équipement qui prennent la place d'une unité.

Câble informatique Cat 7 (Bobine de 300M)

Suite à notre emménagement dans ces nouveaux locaux, nous devons installer les câbles réseaux dans ceux-ci. L'installation de câbles informatique Catégorie 7 est important à ce jour car il propose un débit de 40Gb/s, ce qui est largement suffisant à l'heure actuelle, et pour les années à venir.

Fibre Optique OM3

Suite à notre emménagement dans ces nouveaux locaux, nous devons installer les câbles fibre dans ceux-ci, ainsi qu'à l'extérieur, afin de relier les bâtiments. Le débit de ce type de fibre est de 10 Gbits/s jusqu'à 300 mètres.

Matériel de brassage (Câble, Panneau Balais...)

Matériel qui est nécessaire dans la baie de brassage.



DEVIS No.1972174

Date du devis 20/03/2018
Référence du devis 1972174
Numéro de client 5189
Date de validité du devis 19/04/2018
Modalité de paiement 30 jours
Emis par Frederique Pipiche
Contact client ID'Meuble

Destinataire :
ID'Meuble
35 rue de sillac
16000
Angouleme

Infos additionnelles

Merci d'avoir choisi InMac

La livraison sera effectuée dans les 4 semaines après réception de la confirmation de la commande ;

Description	Quantités	Prix unitaires HT	TVA %	TVA	TOTAL TTC
Imprimante Xerox 6551V	6	340,00 €	20,00%	68,00 €	2 448,00 €
Switch Cisco SG500	6	700,00 €	20,00%	140,00 €	5 040,00 €
Module MiniGbic	15	100,00 €	20,00%	20,00 €	1 800,00 €

Total HT 9 060,00 €
TVA 228,00 €

Total TTC 9 288,00 €

Signature du client (précédée de la mention « Bon pour accord »)

Imprimante Xerox 6551V

Nous avons choisi de prendre ces imprimantes car elles ont de multiples fonctionnalités. Elles peuvent imprimer, copier, numériser, télécopier et envoyer par e-mail les fichiers scannés. Elles disposent, de plus, d'un port Ethernet afin de rajouter l'imprimante sur le réseau.

Switch Cisco SG500

Ces switch Cisco nous garantissent une performance et un management à la hauteur de nos espérances. Les 4 ports mini-GBIC qui sont présent sur le switch nous permettent de brancher la fibre arrivant au point de branchement. Le côté management nous donnent la possibilité de gérer en temps réel certains paramètres essentiels au bon fonctionnement du réseau.

Module MiniGbic

Ce module permet de convertir un signal électrique en signal optique. Autrement dit, il nous sert d'adaptateur pour câble Ethernet fibre optique/câble Ethernet cuivre.

LE RESEAU

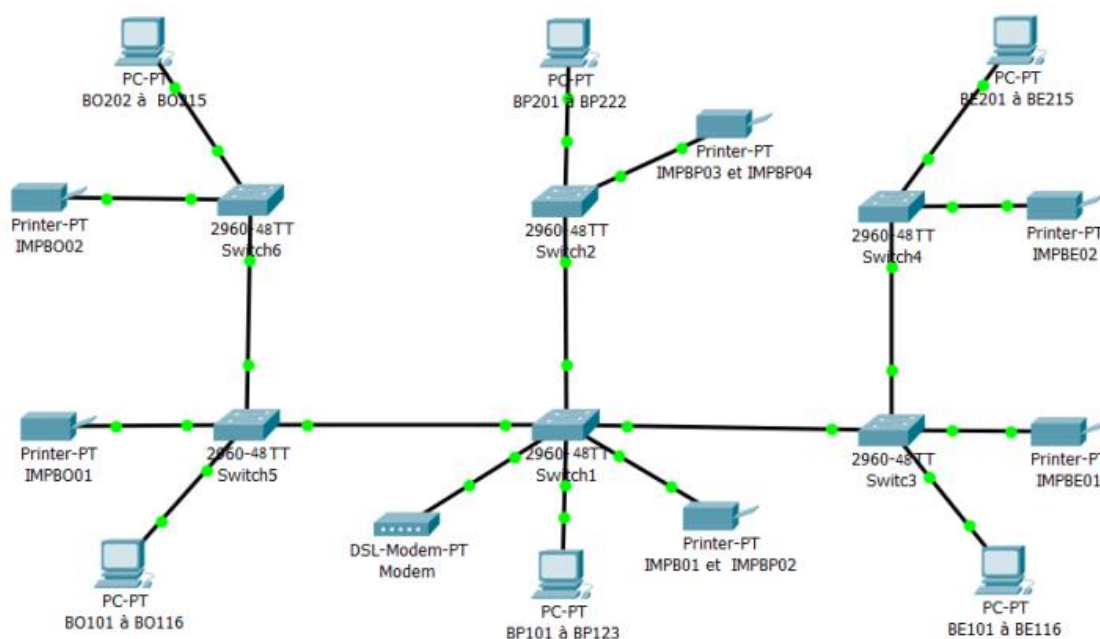
Notre choix topologique :

Après une étude des différents modèles de réseaux, nous avons arrêté notre choix sur l'utilisation d'un système en étoile.

Ce type de réseau est avantageux en termes de simplicité de mise en place, ainsi que de sa flexibilité concernant l'ajout ou la suppression de périphérique. Ce sont les arguments majeurs qui ont induit à ce choix.

En cas d'éventuelle panne et pour éviter à tout secteur d'être coupé du reste, nous possédons une Box de rechange.

Afin de rendre la visualisation de notre réseau actuel plus simple, voici une représentation graphique de celui-ci :



CAHIER DES CHARGES

Dans ce projet, nous devons mettre en place deux serveurs : un serveur Windows serveur, ainsi qu'un serveur sous Linux. Nous devons également implémenter certains applicatifs afin de faciliter l'administration du parc informatique.

Concernant le serveur Microsoft, voici ce qui est requis :

DNS :

- Configurer les zones.
- Prévoir une solution de tolérance de panne et la justifier.

Sécurité :

- Le mot de passe doit répondre aux exigences de complexité.
- Il doit être de dix caractères minimums.

Les impressions :

- Il faut 1 imprimante pour chaque service.
- Une imprimante réseau pour tout le monde (les services Produit 1 et 2 ne peuvent imprimer qu'entre 8 heures du matin et 17 heures).
- La direction est prioritaire sur toutes les impressions et les utilisent 24/24.
- Le service informatique a contrôle total sur toutes les impressions.
- Mme. LAPORTE et Mlle ADA (les assistantes des services SAV et direction peuvent imprimer chez les Services Informatique, Service Produit A et B.

Les connexions réseaux :

- Mme BEZIAT, ELLA, AYO et ACIEN ne peuvent se connecter qu'entre 08 heures et 18 heures et à 19 heures elles doivent être déconnectées (elles sont du service Produit A).
- Aucun salarié sauf la direction, le SAV et l'informatique ne peut se connecter entre 20 heures et 07 heures du matin.

Stratégie locale :

- En dehors de la direction, des services informatiques, personne ne peut installer de logiciels sur sa machine ni modifier l'heure.
- Les lecteurs CD et USB sont désactivés sur les postes des services Produit A et B.
- Les services Produit A et B, SAV ne peuvent parcourir ou ouvrir les dossiers ou fichiers à partir d'un CD ou d'une Clé USB.

Gestion de l'espace disque :

- Chaque utilisateur a droit à 5 Go sur le disque.
- Mettre les alertes en cas dépassement.

Connexion aux lecteurs réseau :

- Chaque service doit avoir un répertoire nommé « Communservice » qui sera attribué à chacun des salariés lors de sa connexion réseau.
- A l'intérieur de chaque répertoire, vous créez un dossier pour chaque salarié (contrôle total sur celui-ci et aucun accès sur ceux des collègues).
- Seuls la direction et l'informatique peuvent y accéder en plus (juste lire pour la direction).
- Attribuer un dossier de base à 2 users locaux au choix.
- Attribuer un dossier de base à 2 users du domaine au choix.
- Planifier 2 audits au hasard.
- Configurer au moins 3 journaux à 3 jours.
- Désactiver le moniteur d'évènements.

Accès à distance :

- Tous les postes doivent être accessibles à distance.

Tolérance de panne (au niveau de chaque machine et de tout le domaine) :

- Prévoir une solution de tolérance de panne, la justifier et l'expliquer.
- Donner une liste de matériels prévus et les coûts associés.

Créer des scripts facilitant l'administration des serveurs.

Créer des scripts de connexion définissant l'environnement propre à chaque utilisateur.

Concernant le serveur Linux, voici ce qui est requis :

- Partage de ressources Windows via samba serveur.
- Serveur NFS.
- Service FTP (sécurisé et anonyme).
- Client NFS avec sauvegarde automatique des ressources de l'autre serveur.

Concernant le côté applicatif, voici ce qui est requis :

En mode consultation :

- Consulter la liste des postes décrit par : les noms/prénoms d'utilisateur, le nom du local, les caractéristiques de l'UC.
- Pour chaque poste, offrir la possibilité de consulter : la fiche liste des écrans associés au poste, la liste des imprimantes associées au poste.
- Permettre la recherche multicritère de poste : utilisateur, local, mémoire vive, disque dur.

En mode gestion :

- Enregistrer/modifier/supprimer des utilisateurs.
- Enregistrer/modifier/supprimer des locaux.
- Enregistrer/modifier/supprimer des écrans.
- Enregistrer/modifier/supprimer des imprimantes.
- Enregistrer un poste en sélectionnant un utilisateur existant, un local existant, un ou plusieurs écrans existants, une ou plusieurs imprimantes existantes, et en saisissant les caractéristiques de l'UC ainsi que la date de début d'utilisation.
- Modifier un poste.
- Supprimer un poste.

Remarques :

Le mode consultation est accessible à tous les utilisateurs.

Le mode gestion est interdit aux utilisateurs non membres du service informatique.

PLANNING DE REPARTITION DES TACHES

TACHES	AFFECTATION
Rappel cahier des charges/problématique	Raphaël WEBER
Rédaction	
Mise en page	
Charte graphique	
Réalisation du MS PROJECT	Louis BRET
Base de données	Florian GUYOT
Devis matériels / comparatifs	Louis BRET
Server windows / AD / DNS / DHCP / IMP	Florian GUYOT - Raphaël WEBER Louis BRET
Serveur LINUX / SMB / sFTP	Quentin ROBYNS
Script Power Shell	Quentin ROBYNS - Florian GUYOT
Procédures	Tout le monde

ADRESSAGE IP

Il existe différents adressages IP possible, dans notre cas, nous avons choisis une IP de classe C, ce qui signifie que nous pouvons accueillir 254 matériels sur notre réseau. Les différentes IP attribuées sont donc toutes en /24. Le /24 renvoie à la classe du réseau, et donc au nombre de machines maximales que ce réseau peut accueillir.

Concrètement, l'adresse IP de chaque machine ressemble donc à ceci :

192.168.1.X/24

Le « X » est la valeur modifiable de l'IP, cette valeur peut aller de « 1 » à « 254 ».

Nous disposons donc d'une plage de 254 adresses IP disponibles, que nous avons réparti de la façon suivante :

Périphérique	Plage IP	Adresses utilisées
Ordinateur (DHCP)	192.168.10.100 à 200	100
Imprimantes	192.168.10.51 à 99	48
Serveur Linux	192.168.10.10 à 18	8
Serveur Windows	192.168.10.1 à 9	8
Management Serveur Windows	192.168.10.19 et 20	2
Switch	192.168.10.21 à 50	21
Firewall	192.168.10.254	1
Restant	66	188

Plus précisément :

Voici le tableau d'attribution de chaque adresse IP :

ADRESSE IP	GENERAL	NOM DU POSTE
192.168.10.0	ADDRESSE RESEAU	
192.168.10.1	SERVEUR	IDM-SRV-DC1
192.168.10.2	HyperViseur_1	IDM-SRV-HV1
192.168.10.3	HyperViseur_2	IDM-SRV-HV2
192.168.10.4	VM	IDM-SRV-DC2
192.168.10.5	VM	IDM-SRV-SF1
192.168.10.6	VM	IDM-SRV-SF2
192.168.10.7	VM	IDM-SRV-IMP
192.168.10.8	SERVEUR	
192.168.10.9	SERVEUR	

192.168.10.10	SERVEUR	IDM-SRV-LIN1
192.168.10.11	SERVEUR	IDM-SRV-LIN2
192.168.10.12	SERVEUR	IDM-SRV-NAS1
192.168.10.13	SERVEUR	IDM-SRV-NAS2
192.168.10.14	SERVEUR	
192.168.10.15	SERVEUR	
192.168.10.16	SERVEUR	
192.168.10.17	SERVEUR	
192.168.10.18	SERVEUR	
192.168.10.19	RESERVE-SERVEUR\ADMINISTRATION	
192.168.10.20	SERVEUR\ADMINISTRATION	IDM-RSAT-01
192.168.10.21	MAT-RESEAU	IDM-SW-BP-01
192.168.10.22	MAT-RESEAU	IDM-SW-BP-02
192.168.10.23	MAT-RESEAU	IDM-SW-BP-03
192.168.10.24	MAT-RESEAU	IDM-SW-BP-04
192.168.10.25	MAT-RESEAU	IDM-SW-AE-01
192.168.10.26	MAT-RESEAU	IDM-SW-AE-02
192.168.10.27	MAT-RESEAU	IDM-SW-AE-03
192.168.10.28	MAT-RESEAU	IDM-SW-AE-04
192.168.10.29	MAT-RESEAU	IDM-SW-AO-01
192.168.10.30	MAT-RESEAU	IDM-SW-AO-02
192.168.10.31	MAT-RESEAU	IDM-SW-AO-03
192.168.10.32	MAT-RESEAU	IDM-SW-AO-04
192.168.10.33	MAT-RESEAU	
192.168.10.34	MAT-RESEAU	
192.168.10.35	MAT-RESEAU	
192.168.10.36	MAT-RESEAU	
192.168.10.37	MAT-RESEAU	
192.168.10.38	MAT-RESEAU	
192.168.10.39	MAT-RESEAU	
192.168.10.40	MAT-RESEAU	
192.168.10.41	MAT-RESEAU	
192.168.10.42	MAT-RESEAU	
192.168.10.43	MAT-RESEAU	
192.168.10.44	MAT-RESEAU	
192.168.10.45	MAT-RESEAU	
192.168.10.46	MAT-RESEAU	
192.168.10.47	MAT-RESEAU	
192.168.10.48	MAT-RESEAU	
192.168.10.49	MAT-RESEAU	
192.168.10.50	MAT-RESEAU	
192.168.10.51	IMPRIMANTE	IDM-IMP-GEN
192.168.10.52	IMPRIMANTE	IDM-IMP-PR1
192.168.10.53	IMPRIMANTE	IDM-IMP-PR2
192.168.10.54	IMPRIMANTE	IDM-IMP-SAV

192.168.10.55	IMPRIMANTE	IDM-IMP-DAF
192.168.10.56	IMPRIMANTE	IDM-IMP-DGE
192.168.10.57	IMPRIMANTE	
192.168.10.58	IMPRIMANTE	
192.168.10.59	IMPRIMANTE	
192.168.10.60	IMPRIMANTE	
192.168.10.61	IMPRIMANTE	
192.168.10.62	IMPRIMANTE	
192.168.10.63	IMPRIMANTE	
192.168.10.64	IMPRIMANTE	
192.168.10.65	IMPRIMANTE	
192.168.10.66	IMPRIMANTE	
192.168.10.67	IMPRIMANTE	
192.168.10.68	IMPRIMANTE	
192.168.10.69	IMPRIMANTE	
192.168.10.70	IMPRIMANTE	
192.168.10.71	IMPRIMANTE	
192.168.10.72	IMPRIMANTE	
192.168.10.73	IMPRIMANTE	
192.168.10.74	IMPRIMANTE	
192.168.10.75	IMPRIMANTE	
192.168.10.76	IMPRIMANTE	
192.168.10.77	IMPRIMANTE	
192.168.10.78	IMPRIMANTE	
192.168.10.79	IMPRIMANTE	
192.168.10.80	IMPRIMANTE	
192.168.10.81	IMPRIMANTE	
192.168.10.82	IMPRIMANTE	
192.168.10.83	IMPRIMANTE	
192.168.10.84	IMPRIMANTE	
192.168.10.85	IMPRIMANTE	
192.168.10.86	IMPRIMANTE	
192.168.10.87	IMPRIMANTE	
192.168.10.88	IMPRIMANTE	
192.168.10.89	IMPRIMANTE	
192.168.10.90	IMPRIMANTE	
192.168.10.91	IMPRIMANTE	
192.168.10.92	IMPRIMANTE	
192.168.10.93	IMPRIMANTE	
192.168.10.94	IMPRIMANTE	
192.168.10.95	IMPRIMANTE	
192.168.10.96	IMPRIMANTE	
192.168.10.97	IMPRIMANTE	
192.168.10.98	IMPRIMANTE	
192.168.10.99	IMPRIMANTE	

192.168.10.100	DHCP	POSTE CLIENT
192.168.10.101	DHCP	POSTE CLIENT
192.168.10.102	DHCP	POSTE CLIENT
192.168.10.103	DHCP	POSTE CLIENT
192.168.10.104	DHCP	POSTE CLIENT
192.168.10.105	DHCP	POSTE CLIENT
192.168.10.106	DHCP	POSTE CLIENT
192.168.10.107	DHCP	POSTE CLIENT
192.168.10.108	DHCP	POSTE CLIENT
192.168.10.109	DHCP	POSTE CLIENT
192.168.10.110	DHCP	POSTE CLIENT
192.168.10.111	DHCP	POSTE CLIENT
192.168.10.112	DHCP	POSTE CLIENT
192.168.10.113	DHCP	POSTE CLIENT
192.168.10.114	DHCP	POSTE CLIENT
192.168.10.115	DHCP	POSTE CLIENT
192.168.10.116	DHCP	POSTE CLIENT
192.168.10.117	DHCP	POSTE CLIENT
192.168.10.118	DHCP	POSTE CLIENT
192.168.10.119	DHCP	POSTE CLIENT
192.168.10.120	DHCP	POSTE CLIENT
192.168.10.121	DHCP	POSTE CLIENT
192.168.10.122	DHCP	POSTE CLIENT
192.168.10.123	DHCP	POSTE CLIENT
192.168.10.124	DHCP	POSTE CLIENT
192.168.10.125	DHCP	POSTE CLIENT
192.168.10.126	DHCP	POSTE CLIENT
192.168.10.127	DHCP	POSTE CLIENT
192.168.10.128	DHCP	POSTE CLIENT
192.168.10.129	DHCP	POSTE CLIENT
192.168.10.130	DHCP	POSTE CLIENT
192.168.10.131	DHCP	POSTE CLIENT
192.168.10.132	DHCP	POSTE CLIENT
192.168.10.133	DHCP	POSTE CLIENT
192.168.10.134	DHCP	POSTE CLIENT
192.168.10.135	DHCP	POSTE CLIENT
192.168.10.136	DHCP	POSTE CLIENT
192.168.10.137	DHCP	POSTE CLIENT
192.168.10.138	DHCP	POSTE CLIENT
192.168.10.139	DHCP	POSTE CLIENT
192.168.10.140	DHCP	POSTE CLIENT
192.168.10.141	DHCP	POSTE CLIENT
192.168.10.142	DHCP	POSTE CLIENT
192.168.10.143	DHCP	POSTE CLIENT
192.168.10.144	DHCP	POSTE CLIENT

192.168.10.145	DHCP	POSTE CLIENT
192.168.10.146	DHCP	POSTE CLIENT
192.168.10.147	DHCP	POSTE CLIENT
192.168.10.148	DHCP	POSTE CLIENT
192.168.10.149	DHCP	POSTE CLIENT
192.168.10.150	DHCP	POSTE CLIENT
192.168.10.151	DHCP	POSTE CLIENT
192.168.10.152	DHCP	POSTE CLIENT
192.168.10.153	DHCP	POSTE CLIENT
192.168.10.154	DHCP	POSTE CLIENT
192.168.10.155	DHCP	POSTE CLIENT
192.168.10.156	DHCP	POSTE CLIENT
192.168.10.157	DHCP	POSTE CLIENT
192.168.10.158	DHCP	POSTE CLIENT
192.168.10.159	DHCP	POSTE CLIENT
192.168.10.160	DHCP	POSTE CLIENT
192.168.10.161	DHCP	POSTE CLIENT
192.168.10.162	DHCP	POSTE CLIENT
192.168.10.163	DHCP	POSTE CLIENT
192.168.10.164	DHCP	POSTE CLIENT
192.168.10.165	DHCP	POSTE CLIENT
192.168.10.166	DHCP	POSTE CLIENT
192.168.10.167	DHCP	POSTE CLIENT
192.168.10.168	DHCP	POSTE CLIENT
192.168.10.169	DHCP	POSTE CLIENT
192.168.10.170	DHCP	POSTE CLIENT
192.168.10.171	DHCP	POSTE CLIENT
192.168.10.172	DHCP	POSTE CLIENT
192.168.10.173	DHCP	POSTE CLIENT
192.168.10.174	DHCP	POSTE CLIENT
192.168.10.175	DHCP	POSTE CLIENT
192.168.10.176	DHCP	POSTE CLIENT
192.168.10.177	DHCP	POSTE CLIENT
192.168.10.178	DHCP	POSTE CLIENT
192.168.10.179	DHCP	POSTE CLIENT
192.168.10.180	DHCP	POSTE CLIENT
192.168.10.181	DHCP	POSTE CLIENT
192.168.10.182	DHCP	POSTE CLIENT
192.168.10.183	DHCP	POSTE CLIENT
192.168.10.184	DHCP	POSTE CLIENT
192.168.10.185	DHCP	POSTE CLIENT
192.168.10.186	DHCP	POSTE CLIENT
192.168.10.187	DHCP	POSTE CLIENT
192.168.10.188	DHCP	POSTE CLIENT
192.168.10.189	DHCP	POSTE CLIENT

192.168.10.190	DHCP	POSTE CLIENT
192.168.10.191	DHCP	POSTE CLIENT
192.168.10.192	DHCP	POSTE CLIENT
192.168.10.193	DHCP	POSTE CLIENT
192.168.10.194	DHCP	POSTE CLIENT
192.168.10.195	DHCP	POSTE CLIENT
192.168.10.196	DHCP	POSTE CLIENT
192.168.10.197	DHCP	POSTE CLIENT
192.168.10.198	DHCP	POSTE CLIENT
192.168.10.199	DHCP	POSTE CLIENT
192.168.10.200	DHCP	POSTE CLIENT
192.168.10.201	Libre	
192.168.10.202	Libre	
192.168.10.203	Libre	
192.168.10.204	Libre	
192.168.10.205	Libre	
192.168.10.206	Libre	
192.168.10.207	Libre	
192.168.10.208	Libre	
192.168.10.209	Libre	
192.168.10.210	Libre	
192.168.10.211	Libre	
192.168.10.212	Libre	
192.168.10.213	Libre	
192.168.10.214	Libre	
192.168.10.215	Libre	
192.168.10.216	Libre	
192.168.10.217	Libre	
192.168.10.218	Libre	
192.168.10.219	Libre	
192.168.10.220	Libre	
192.168.10.221	Libre	
192.168.10.222	Libre	
192.168.10.223	Libre	
192.168.10.224	Libre	
192.168.10.225	Libre	
192.168.10.226	Libre	
192.168.10.227	Libre	
192.168.10.228	Libre	
192.168.10.229	Libre	
192.168.10.230	Libre	
192.168.10.231	Libre	
192.168.10.232	Libre	
192.168.10.233	Libre	
192.168.10.234	Libre	

192.168.10.235	Libre	
192.168.10.236	Libre	
192.168.10.237	Libre	
192.168.10.238	Libre	
192.168.10.239	Libre	
192.168.10.240	Libre	
192.168.10.241	Libre	
192.168.10.242	Libre	
192.168.10.243	Libre	
192.168.10.244	Libre	
192.168.10.245	Libre	
192.168.10.246	Libre	
192.168.10.247	Libre	
192.168.10.248	Libre	
192.168.10.249	Libre	
192.168.10.250	Libre	
192.168.10.251	Libre	
192.168.10.252	Libre	
192.168.10.253	Libre	
192.168.10.254	MAT-RESEAU	FIREWALL
192.168.10.255	BROADCAST	

LES SERVEURS

L'entreprise dispose de trois serveurs physiques, ces trois serveurs sont répartis de la façon suivante :

- IDM-SRV-DC1, ce serveur est notre contrôleur de domaine principal. Par convention, il occupe seulement cette fonction.
- IDM-SRV-HV1, ce serveur est notre premier hyperviseur (serveur de virtualisation), il comprend trois serveurs virtualisés :
 - o Le IDM-SRV-DC2, qui est notre second contrôleur de domaine ;
 - o Le IDM-SRV-SF1, qui est notre serveur DFS ;
 - o Le IDM-SRV-Linux2, qui est la réplication du serveur Linux principal.
- IDM-SRV-HV2, ce serveur est notre second hyperviseur, il comprend également trois serveurs virtualisés :
 - Le IDM-SRV-SF2, qui est la réplication du serveur de fichier principal ;
 - Le IDM-SRV-IMP, qui est notre serveur d'impression ;
 - Le IDM-SRV-Linux1, qui comprend partage de fichier SAMBA ainsi que notre DHCP.



IDM-SRV-DC1

AD-DNS



IDM-SRV-HV1

IDM-SRV-DC2

AD-DNS(Repliat)

IDM-SRV-SF1

DFS

IDM-SRV-Linux2



IDM-SRV-HV2

IDM-SRV-SF2

DFS(Repliat)

IDM-SRV-IMP

Impression

IDM-SRV-Linux1

Le choix de virtualiser les serveurs cités ci-dessus sont pour les avantages suivants :

- Moins de serveurs physiques, c'est-à-dire un cout à l'achat des serveurs moins important ;
- Pouvoir disposer d'un plan de reprise d'activité fiable est une condition essentielle pour assurer la continuité d'activité. La Virtualisation permet d'être indépendant du matériel et d'accélérer la reprise en cas de sinistre ou de basculement ;
- Optimiser les ressources d'un parc de machines (répartition des machines virtuelles sur les machines physiques en fonction des charges respectives) ;
- Installation, déploiement et migration facile des machines virtuelles d'une machine physique à une autre ;
- Gagner du temps car il est considérablement plus rapide d'administrer des serveurs virtuels plutôt que physiques, grâce à la centralisation de l'administration et de la surveillance.

SERVEURS WINDOWS

A la suite d'un audit réalisé par une ESN, et après une discussion avec notre directeur administratif et financier, nous avons décidé qu'il est nécessaire d'implémenter une solution de serveur sous Windows Server 2016.

Notre choix est d'implémenter à notre réseau des serveurs Windows Server 2016, qui sont les serveurs suivants : IDM-SRV-DC1, qui est sur une machine physique, puis et IDM-SRV-DC2 ainsi qu'IDM-SRV-SF1 qui sont virtualisés sur une machine nommée IDM-SRV-HV1. Egalement IDM-SRV-SF2 et IDM-SRV-IMP qui sont virtualisés sur un autre serveur, le IDM-SRV-HV2. Ce choix se justifie, de fait, par la présence d'une tolérance à la panne. Le second serveur, le IDM-SRV-DC2, servira de serveur de réplication. Cette réplication peut être utile si nous rencontrons un problème avec le serveur numéro un, le IDM-SRV-DC1. Le serveur secondaire prendra alors le relais, sans affecter le fonctionnement du réseau. Les configurations de ces deux serveurs au niveau des rôles sont donc identiques.

Nous avons fait le choix d'installer des serveurs Windows Server 2016 sans interface graphique (Core). Ce choix possède des avantages intéressants :

- Système plus léger : Aucune interface graphique, aucun logiciel préinstallé sur l'OS (Internet Explorer, explorateur Windows...). Ce système requiert moins d'espace disque par rapport à une installation complète ;
- Économie de ressources : Moins de services signifient moins de processus et donc moins de ressources consommées. La mémoire vive sera moins sollicitée et le disque dur se remplira moins vite.

Le gain de ressources avec Windows Server Core est réellement intéressant et permet d'optimiser au mieux l'utilisation des ressources pour des services plus importants.

La procédure concernant l'installation ainsi que le paramétrage de base d'un serveur sous Windows Serveur 2016 Core se trouve en annexe page 56.

Le serveur Windows Core peut être géré via plusieurs moyens :

- SCONFIG : Un utilitaire intégré à Windows Server Core et qui permet d'effectuer des actions de configuration basiques ;
- Invite de commande : Permet d'effectuer des actions de configuration ;
- PowerShell ;
- RSAT : Un outil d'administration de serveur distant, pour les systèmes d'exploitation Windows. Nous utiliserons principalement ce moyen. La procédure concernant l'installation de cet outil se trouve en annexe page 66. Cela revient à installer et paramétrer un Windows 10 Client classique, et rajouter l'outil RSAT.

SERVEUR PHYSIQUE IDM-SRV-DC1

Sur ce serveur, nous avons fait le choix de dédier entièrement un serveur physique pour notre contrôleur de domaine principal. Cela fait partie des bonnes pratiques recommandé par Microsoft. Cela garantie son indépendance aux yeux d'un hyperviseur. Virtualiser ce serveur pourrait poser des problèmes, notamment le fait d'intégrer l'hyperviseur dans le domaine qui est virtualisé sur lui-même.

ACTIVE DIRECTORY (AD) :

Active Directory est un service d'annuaire développé par Microsoft pour les systèmes d'exploitation Windows.

L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, l'installation de mises à jour par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées.

Nous avons fait le choix d'installer ce service pour plusieurs raisons. Pour une gestion centralisée des ressources et de la sécurité. En effet, il est possible d'appliquer des stratégies de sécurité renforcées et sur mesure pour protéger l'infrastructure et les données de l'entreprise. Il facilite également la mise en place de nouvelles ressources en simplifiant la mise en place de l'environnement de travail souhaité (poste de travail, logiciels, documents collaboratifs...).

La mise en place de l'Active Directory est également lié à un contrôleur de domaine dans laquelle les utilisateurs et les ordinateurs sont organisés en groupes et sous-groupes afin de faciliter l'administration des droits et restrictions utilisateur. Notre choix de nom de domaine local pour notre entreprise est le suivant : **IDM.lan**

Vous trouverez la procédure de la mise en place de notre Active Directory en annexe page 79.

DNS

Précédemment, nous avons procédé à l'implémentation d'un contrôleur de domaine ainsi que d'un Active Directory dans notre réseau. Le serveur DNS est lié lors de l'implémentation du contrôleur de domaine.

Un DNS, Domain Name System, ou système de nom de domaine, en français, est un service qui permet de traduire un nom d'hôte en une adresse IP.

Par exemple, pour un ordinateur, le DNS nous permet de traduire son nom d'hôte, par exemple "Ordinateur_1" en une adresse IP, par exemple : 192.168.10.100, qui lui est associée. Cela nous aide à identifier plus facilement le matériel associé à cette adresse IP, en l'occurrence dans l'exemple, un ordinateur.

Dans un premier temps, nous avons créé une nouvelle zone, une zone primaire, dans la zone de recherche directe. Nous avons ajouté une zone de recherche directe "IDM.lan". La zone directe permet de faire correspondre les noms d'hôte en adresse IP.

Dans un second temps, nous avons installé une zone de recherche inverse. A l'inverse du DNS, le reverse DNS permet de convertir une adresse IP en nom d'hôte. Ce service permet d'identifier plus facilement une machine. Au lieu de voir apparaître une adresse IP, ce mécanisme permet de voir apparaître un nom d'hôte et dans la plupart des cas un nom de machine. Cela permet d'appeler une ressource par son nom d'hôte au lieu de son adresse IP. Vous trouverez la procédure de mise en place du DNS en annexe page 79.

HYPERVISEUR IDM-SRV-HV1

AD-DNS

La redondance, autrement dit, la duplication d'un élément essentiel au fonctionnement normal du système informatique, en vue de pallier la défaillance éventuelle de cet élément et d'assurer ainsi la continuité d'une fonction informatique vitale, est nécessaire dans une entreprise. Nous souhaitons que la continuité de service dans notre entreprise soit un point essentiel. C'est pourquoi nous avons mis en place des solutions pour palier à tout éventuel événement qui pourrait venir perturber le bon fonctionnement de l'entreprise.

Cet hyperviseur possède un serveur virtualisé, le IDM-SRV-DC2, qui est la réplique du contrôleur de domaine principal.

La procédure concernant la mise en place du serveur de réplique se trouve en annexe page 87.

DFS

L'acronyme DFS signifie Distributed File System, il s'agit d'un système de fichiers distribués. Il va donc permettre de regrouper un ensemble de partages qu'il faudra rendre accessibles de manière uniforme et de centraliser l'ensemble des espaces disponibles. Du point de vue utilisateur, celui-ci ne verra pas le nom du serveur sur lequel il accède pour lire les données. Très pratique en cas de panne ou bien d'évolution, le chemin restera toujours le même.

L'utilisation d'un système de fichier DFS apporte certains avantages :

- Simplifier l'administration : Si une des cibles DFS tombe, la liaison DFS peut être déplacée sur un autre serveur contenant une copie des données.

- DFS intégré à Windows ;
- Un nom unique pour accéder aux ressources ;
- Mise en cache pour un gain de performance ;
- Gestion des ACL au niveau du système de fichiers ;
- Equilibrage de charge (si plusieurs cibles).

La procédure afin d'installer le rôle DFS se trouve en annexe page 100.

HYPERVISEUR IDM-SRV-HV2

SERVEUR D'IMPRESSION

Un serveur d'impression est une application logicielle, un périphérique réseau ou un ordinateur qui gère les demandes d'impression et rend les informations d'état de la file d'attente d'imprimantes accessibles aux utilisateurs finaux et aux administrateurs réseau. Dans notre cas, il s'agit d'un rôle que l'on ajoute à notre serveur Windows. Ce rôle se nomme « Services d'impression », et c'est lui qui nous permet de créer un serveur d'impression.

Notre serveur d'impression est le serveur virtualisé nommé : IDM-SRV-IMP.

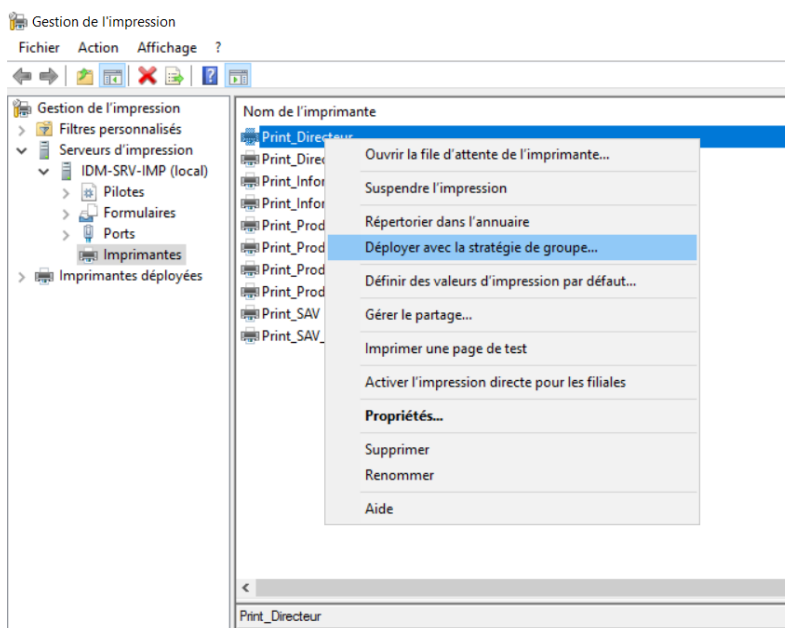
Un serveur d'impression possède les avantages qui sont les suivants :

- Economies de matériels et de maintenance. En effet, il n'est plus nécessaire d'avoir une imprimante dédiée à un utilisateur. Chaque imprimante peut desservir une multitude d'utilisateurs.
- Facilité d'administration. Les paramétrages des différentes imprimantes peuvent être gérées et accessibles à distance.
- Sécurité accrue. Il est possible de contrôler l'accès aux imprimantes à travers les groupes et autorisations.
- Les imprimantes sont accessibles pour tous les utilisateurs connectés sur le réseau. Il n'est pas nécessaire de paramétrer ou d'ajouter chaque imprimante sur chaque ordinateur d'un utilisateur.
- Gestion des impressions. Si une imprimante est utilisée avec un gros travail d'impression, un utilisateur peut éviter la file d'attente en utilisant une autre imprimante. Le serveur offre une gestion des travaux d'impressions et des files d'attente.

Nos imprimantes seront visibles sur le réseau sous le nom type suivant : **IDM-IMP-<Nom_imprimante>**.

Vous trouverez la mise en place du service d'impression en annexe page 106.

Concrètement, le déploiement des imprimantes se fera via une GPO, en sélectionnant l'imprimante et en liant cette même imprimante à un groupe d'ordinateurs.



Seul ce serveur n'est pas répliqué. En effet, le service qu'il propose n'est pas jugé vital à l'entreprise. En cas de défaillance, l'intervention d'un technicien reste nécessaire afin de remettre en marche le serveur préalablement sauvegardé. Nous assurons une reprise du service dans un délai de quarante-cinq minutes.

REPLICATION DU DFS

Sur ce serveur virtualisé, nommé IDM-SRV-SF2, est le second serveur DSF, c'est une réplication du premier présent sur le serveur IDM-SRV-HV1.

Il est important d'avoir une copie des données car l'entreprise peut faire face à plusieurs types de risques qui mettent en danger ses données :

- Risques humains : la perte ou le vol d'un appareil dont les données sont liées à celles de l'entreprise, une mauvaise manipulation entraînant l'effacement de données sensibles, piratage des données... ;
- Risques liés à l'environnement : perte de données suite à un incendie dans les locaux de l'entreprise, catastrophes (incendies, inondations...) ;
- Risques liés aux dysfonctionnements matériels : perte d'un serveur par exemple.

En cas de pertes de données, l'impact financier peut être notable pour l'entreprise en raison de la disparition de fichiers sensibles ou de la perte de temps engendrée par la remise en ligne de ces données.

SECURITE ET ACCES AUX DONNEES

En ce qui concerne la sécurité et l'accès aux données, Microsoft dispose d'outils performants et simples d'utilisation pour un administrateur réseau, qui nous permettent de mettre en place les points de sécurité suivants :

DROIT NTFS

Windows utilise un système de fichier nommé NTFS. Celui-ci permet de gérer l'accès aux données en fonction des utilisateurs et groupes. Dans notre cas, ces droits seront attribués aux utilisateurs et groupe du domaine.

GESTION DES IMPRIMANTES :

Comme vu précédemment notre serveur d'impressions nous permettra de gérer l'accès aux imprimantes ainsi que de gérer des priorités, il permet également de distribuer aux utilisateurs les drivers nécessaires au bon fonctionnement de l'imprimante.

GPO

Afin de répondre aux exigences de notre entreprise, nous allons mettre en place une administration qui va nous permettre de gérer au mieux l'utilisation du réseau ainsi que les utilisateurs comme convenus dans notre cahier des charges.

« LE MOT DE PASSE DOIT REpondre AUX EXIGENCES DE COMPLEXITE »

Nous mettons en place une GPO qui s'appliquera à tous les utilisateurs. Pour cela nous allons dans gestion de stratégie de groupe, notre domaine IDM et créer un objet GPO dans ce domaine, et y ajouter une nouvelle entrée que nous appelons « Mot de Passe ».

Default Domain Policy	
Données recueillies le : 13/06/2018 14:51:20	
Configuration ordinateur (activée)	
Stratégies	
Paramètres Windows	
Paramètres de sécurité	
Stratégies de comptes/Stratégie de mot de passe	
Stratégie	Paramètre
Le mot de passe doit respecter des exigences de complexité	Activé
Longueur minimale du mot de passe	10 caractères

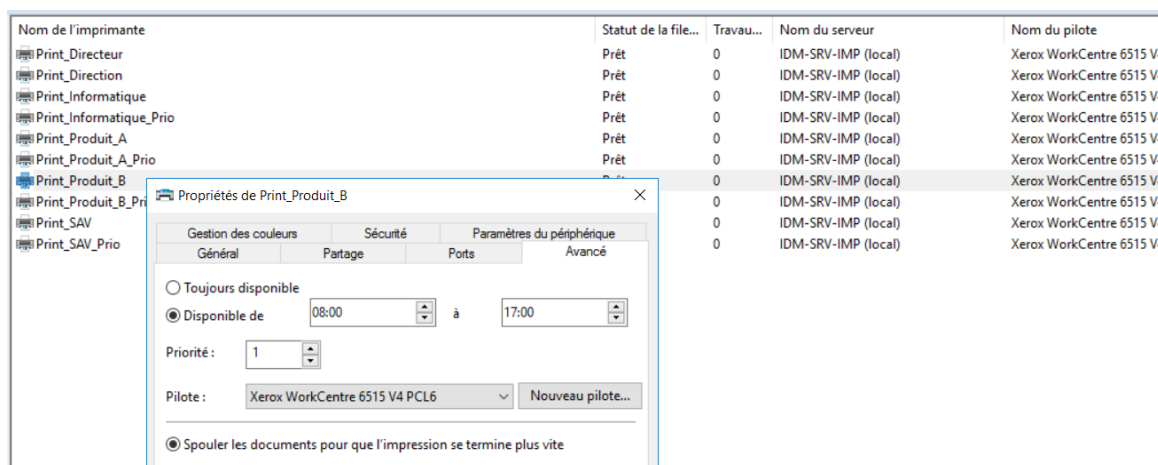
Le mot de passe des utilisateurs doit donc respecter les points suivants :

- Ils ne peuvent pas contenir la valeur du nom de compte de l'utilisateur ;
- Le mot de passe contient des caractères des trois catégories suivantes :
 - o Lettres majuscules de langues européennes (A à Z, avec caractères diacritiques, grecs et cyrilliques) ;
 - o Lettres minuscules de langues européennes (a à z, sharp-s avec marques diacritiques, grecques et cyrilliques) ;
 - o 10 chiffres de base (0 à 9) ;
 - o Caractères non alphanumériques (caractères spéciaux) (par exemple, !, \$, #, %) ;
 - o Tout caractère Unicode classé comme caractère alphabétique mais non en majuscule ou minuscule. Cela inclut les caractères Unicode de langues asiatiques.
- La longueur minimale du mot de passe est de dix caractères.

Ces exigences de complexité sont appliquées lorsque des mots de passe sont modifiés ou créés.

« UNE IMPRIMANTE RESEAU POUR TOUT LE MONDE (LES SERVICES PRODUIT 1 ET 2 NE PEUVENT IMPRIMER QU'ENTRE 8 HEURES DU MATIN ET 17 HEURES) »

Nous avons fait en sorte que l'impression ne soit pas possible en dehors de la plage horaire 8h00 – 17h00 pour les services « Produit 1 » et le service « Produit 2 ». Ce paramétrage se fait directement dans les propriétés de l'imprimante définie pour le service.



« LA DIRECTION EST PRIORITAIRE SUR TOUTES LES IMPRESSIONS ET LES UTILISENT 24/24 »

Etant donné que la direction est prioritaire sur les impressions nous avons créé spécialement des imprimantes pour la direction avec la priorité maximale « 99 », la priorité « 1 » étant pour un utilisateur normal. Plus la valeur attribuée est élevée (entre 1 et 99), plus la priorité sera haute.

Nom de l'imprimante	Statut de la file...	Travaux...	Nom du serveur	Nom du pilote
Print_Directeur	Prêt	0	IDM-SRV-IMP (local)	Xerox WorkCentre 6515 V4
Print_Direction	Prêt	0	IDM-SRV-IMP (local)	Xerox WorkCentre 6515 V4
Print_Informatique	Prêt	0	IDM-SRV-IMP (local)	Xerox WorkCentre 6515 V4
Print_Informatique_Prio	Prêt	0	IDM-SRV-IMP (local)	Xerox WorkCentre 6515 V4
Print_Produit_A	Prêt	0	IDM-SRV-IMP (local)	Xerox WorkCentre 6515 V4
Print_Produit_A_Prio	Prêt	0	IDM-SRV-IMP (local)	Xerox WorkCentre 6515 V4
Print_Produit_B	Prêt	0	IDM-SRV-IMP (local)	Xerox WorkCentre 6515 V4
Print_Produit_B_Prio	Prêt	0	IDM-SRV-IMP (local)	Xerox WorkCentre 6515 V4
Print_SAV	Prêt	0	IDM-SRV-IMP (local)	Xerox WorkCentre 6515 V4
Print_SAV_Prio	Prêt	0	IDM-SRV-IMP (local)	Xerox WorkCentre 6515 V4

Propriétés de Print_Produit_A_Prio

Général

Toujours disponible

Disponible de 00:00 à 00:00

Priorité : 99

Pilote : Xerox WorkCentre 6515 V4 PCL6

Spouler les documents pour que l'impression se termine plus vite

Lancer l'impression après la mise en spouler de la dernière page

« LE SERVICE INFORMATIQUE A LE CONTROLE TOTAL SUR TOUTES LES IMPRESSIONS »

Nous nous sommes attribué les droits sur le contrôle total des impressions. Ce paramétrage se fait également dans les propriétés de l'imprimante. Le groupe informatique a été ajouté et possède tous les droits.

Propriétés de Print_Directeur

Général

Noms de groupes ou d'utilisateurs :

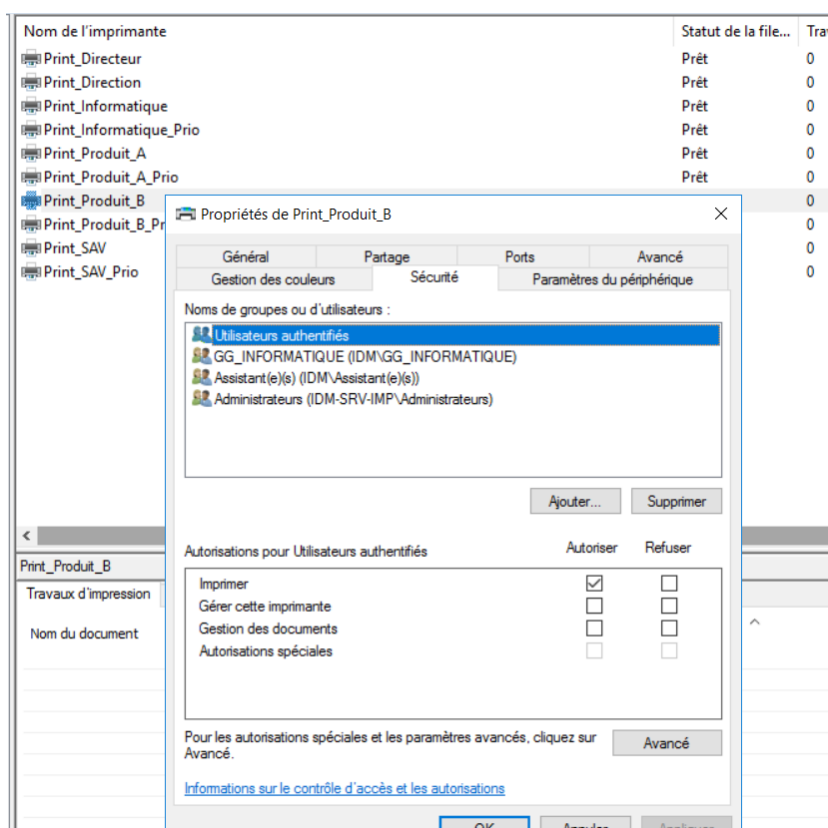
- Utilisateurs authentifiés
- GG_INFORMATIQUE (IDM\GG_INFORMATIQUE)**
- Administrateurs (IDM-SRV-IMP\Administrateurs)

Autorisations pour GG_INFORMATIQUE

	Autoriser	Refuser
Imprimer	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Gérer cette imprimante	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Gestion des documents	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autorisations spéciales	<input type="checkbox"/>	<input type="checkbox"/>

« MME. LAPORTE ET MLLE ADA (LES ASSISTANTES DES SERVICES SAV ET DIRECTION) PEUVENT IMPRIMER CHEZ LES SERVICES INFORMATIQUE, SERVICE PRODUIT A ET B »

Nous avons créé un groupe d'utilisateur « Assistant(e)s » avec les utilisateurs adéquats et nous les avons placées dans la sécurité d'imprimantes afin de satisfaire leur besoin d'impression à de multiples endroits.



« MME BEZIAT, ELLA, AYO ET ACIEN NE PEUVENT SE CONNECTER QU'ENTRE 08 HEURES ET 18 HEURES ET A 19 HEURES ELLES DOIVENT ETRE DECONNECTEES »

Dans notre Active Directory, dans l'onglet Compte et Horaire d'accès, nous avons instauré sur chaque profil utilisateur du service produit A, les horaires d'accès entre 8h et 18h, puis nous avons créé une GPO avec un script qui force l'extinction du poste après avoir averti d'utilisateur.

« AUCUN SALARIE SAUF LA DIRECTION, LE SAV ET L'INFORMATIQUE NE PEUT SE CONNECTER ENTRE 20 HEURES ET 07 HEURES DU MATIN »

Pour appliquer cette règle, nous avons défini sur les profils des utilisateurs des services Produit A, Produit B et Administratif des horaires de connexion de 7h à 20 h.

The image shows two overlapping windows from the 'Utilisateur' application. The top window is titled 'Propriétés d'éléments multiples' and has tabs for 'Général', 'Compte', 'Adresse', 'Profil', and 'Organisation'. The 'Compte' tab is active, showing a 'Suffixe UPN' field with the value '@idm.lan' and a checked 'Horaires d'accès' checkbox. The bottom window is titled 'Horaires d'accès' and displays a grid for configuring access hours. The grid has columns for hours from 0 to 22 and rows for days of the week. A blue shaded area covers the hours from 06:00 to 20:00 for all days from Monday to Sunday. To the right of the grid are 'OK' and 'Annuler' buttons, and radio buttons for 'Ouverture de session autorisée' (selected) and 'Ouverture de session refusée'. At the bottom of the window, it says 'Du lundi au dimanche, de 06:00 à 20:00'.

« EN DEHORS DE LA DIRECTION ET DU SERVICE INFORMATIQUE, PERSONNE NE PEUT INSTALLER DE LOGICIELS SUR SA MACHINE NI MODIFIER L'HEURE »

Ces fonctionnalités ont été désactivées afin de garder un contrôle sur les postes utilisateurs, d'en maîtriser la sécurité et l'usage.

Logiciel
Données recueillies le : 13/06/2018 14:49:22

Configuration ordinateur (activée)
Aucun paramètre n'est défini.

Configuration utilisateur (activée)

Stratégies

Modèles d'administration
Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Composants Windows/Windows Installer

Stratégie	Paramètre	Commentaire
Toujours installer avec des droits élevés	Activé	

Pour être appliqué, ce paramètre de stratégie doit être activé pour l'ordinateur et l'utilisateur.

Horloge
Données recueillies le : 13/06/2018 14:47:42

Configuration ordinateur (activée)

Stratégies

Paramètres Windows

Paramètres de sécurité

Stratégies locales/Attribution des droits utilisateur

Stratégie	Paramètre
Modifier l'heure système	

Configuration utilisateur (activée)
Aucun paramètre n'est défini.

« LES LECTEURS USB ET CD SONT DESACTIVES SUR LES POSTES DES SERVICES PRODUIT A ET B »

&

« LES SERVICES PRODUIT A ET B, SAV NE PEUVENT PARCOURIR OU OUVRIR LES DOSSIERS OU FICHIERS A PARTIR D'UN SUPPORT EXTERNE »

Dans la même optique que la GPO précédente, nous désactivons ces options pour des raisons de sécurité.

CD+USB Données recueillies le : 13/06/2018 14:45:58		
Configuration ordinateur (activée)		
Aucun paramètre n'est défini.		
Configuration utilisateur (activée)		
Stratégies		
Modèles d'administration		
Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.		
Système/Accès au stockage amovible		
Stratégie	Paramètre	Commentaire
Toutes les classes de stockage amovible : refuser tous les accès	Activé	

SCRIPTS POWERSHELL

Nous avons procédé à la création de deux scripts. Ces deux scripts concernent :

- La création des objets AD ;
- La création des lecteurs réseau.

Le script PowerShell concernant la création des objets AD nous permet de faire les choses suivantes :

- Création d'unités d'organisation ;
- Création de groupes ;
- Créations d'utilisateurs ;
- Création de dossiers ;
- Création de permissions.

Le script se présente sous la forme d'un menu proposant les paramètres ci-dessus. Il nous suffit de choisir le paramètre désiré pour ensuite passer à la configuration de celui-ci.

Notez que pour le bon fonctionnement de celui-ci, il est nécessaire d'incrémenter un fichier au format .csv contenant les informations nécessaires à la création de ces objets.

Le script complet se trouve en annexe page 110.

Le script PowerShell concernant la connexion aux lecteurs réseau est simple. Il connecte automatiquement :

- Un répertoire nommé « Service <Nom du service> » qui sera attribué à chacun des salariés lors de sa connexion réseau. C'est un dossier commun au service.
- Un dossier personnel, nommé « Perso », pour chaque salarié.
- Un dossier commun à toute l'entreprise.

Le script complet se trouve en annexe page 115.

SERVEUR LINUX

Notre réseau est composé de deux serveurs Linux. Un serveur principal, et un serveur secondaire.

Sur ces deux serveurs, nous pouvons trouver :

- Un serveur samba ;
- Un serveur NFS ;
- Un client NFS avec sauvegarde automatique des ressources de l'autre serveur ;
- Un service FTP ;
- Un serveur DHCP.

Nous avons besoin d'une distribution Linux, appelée aussi distribution GNU/Linux pour faire référence aux logiciels du projet GNU, est un ensemble cohérent de logiciels, la plupart étant libres, assemblés autour du noyau Linux.

Il existe une très grande variété de distributions, ayant chacune des objectifs et une philosophie particulière.

Les éléments différenciant principalement les distributions sont :

- La convivialité (facilité de mise en œuvre) ;
- L'intégration (taille du parc de logiciels validés distribués) ;
- La notoriété (communauté informative pour résoudre les problèmes) ;
- L'environnement de bureau (GNOME, KDE...),
- Le type de paquet utilisé pour distribuer un logiciel (principalement deb et RPM) ;
- Le mainteneur de la distribution (généralement une entreprise ou une communauté).

Le point commun est le noyau (kernel) et un certain nombre de commandes.

DEBIAN

Pour permettre de communiquer entre une machine Windows et linux, il est essentiel d'une part que le serveur Windows soit correctement configuré (DNS, ACTIVE DIRECTORY) et que tous les paquets et fichiers de configuration soient renseignés sur la machine linux. Tous ces paramètres sont essentiels pour la bonne cohésion des deux environnements. En effet, si l'un ou l'autre des serveurs est mal paramétré, le partage de ressources ne fonctionnera pas.

La configuration de ce partage se situe sur la machine linux : il n'y a aucune action à mener sur le serveur Windows si les paramètres de ce dernier ont été convenablement préétablis.

La procédure concernant l'installation de Debian se trouve en annexe page 116.

MISE EN PLACE

Tout d'abord, il faut que la machine Debian rejoigne le domaine à l'aide de la commande « realm join » : cette opération est essentielle pour que le linux soit renseigné auprès de notre contrôleur de domaine et que l'ordinateur soit visible dans l'active directory. Sans cette première configuration nous ne pourrions pas communiquer avec le reste du parc correctement.

Une fois notre machine ajoutée au domaine, le fichier de configuration « sssd » va être automatiquement généré et renseigné. Le paquet « sssd » a pour fonctionnalité de faire remonter tous les utilisateurs présents dans l'active directory sur le Debian, mais à ce stade les utilisateurs ne peuvent toujours pas s'identifier ou se connecter sur le linux.

Pour pouvoir autoriser nos utilisateurs de l'AD à s'authentifier au Debian il faut éditer le fichier configuration Kerberos.

KERBEROS

Kerberos est un protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes et l'utilisation de tickets, et non de mots de passe en clair, évitant ainsi le risque d'interception frauduleuse des mots de passe des utilisateurs.

Afin d'obtenir l'autorisation d'accès à un service, un utilisateur distant doit envoyer son identifiant au serveur d'authentification. Le serveur d'authentification vérifie que l'identifiant existe et envoie un ticket initial au client distant, chiffré avec la clé associée au client.

Le ticket initial contient :

Une clé de session, faisant office de mot de passe temporaire pour chiffrer les communications suivantes.

Un ticket d'accès au service de distribution de ticket.

Le client distant déchiffre le ticket initial avec sa clé et obtient ainsi un ticket et une clé de session. Grâce à son ticket et sa clé de session, le client distant peut envoyer une requête chiffrée au service de distribution de ticket, afin de demander l'accès à un service.

A présent, si la configuration est réussie, les utilisateurs de notre domaine peuvent se connecter sur la machine.

FTP

Qu'est-ce qu'un FTP et à quoi sert-il ?

FTP est l'abréviation de File Transfer Protocol.

Grâce au FTP, des données comme par exemple des pages internet, des images ou des animations sont déposées dans une case d'une mémoire externe. Le FTP sera donc un langage qui va permettre l'échange de fichiers entre 2 ordinateurs, et plus exactement dans notre cas entre un serveur et un client.

On va donc parler de Serveur FTP et de Client FTP. Lorsque le premier reçoit une demande, il vérifie les droits et si le client a les droits suffisants, il répond à cette demande, sinon elle est rejetée. Le Client sera celui qui va être à l'initiative de toutes les transactions.

Nous avons fait un comparatif de quelques serveurs FTP :

- ProFTPd est l'un des serveurs FTP le plus connu et le plus ancien. Il a donc évolué au fil du temps ce qui en fait aujourd'hui le serveur ftp le plus fourni en plugin.
- PureFTPd se veut être sécurisé avant tout. Malgré le fait qu'il soit moins connu, on peut trouver pas mal de ressources le concernant sur Internet.
- VsFTPd signifie : Very Security FTP Daemon. Comme son nom l'indique, c'est un serveur très sécurisé mais également très léger. Toutefois, cela n'en fait pas un serveur de moindre envergure car il est tout de même utilisé par de gros sites tel que ftp.debian.org.

Pour répondre à la requête nous avons donc choisis d'installer VsFTPd sur linux et avons opté pour Filezilla, un très bon client FTP.

La procédure concernant l'installation du FTP se trouve en annexe page 125.

SAMBA

Samba est un logiciel qui permet à des ordinateurs Unix de mettre à disposition des imprimantes et des fichiers dans des réseaux Windows, en mettant en œuvre le protocole SMB/CIFS de Microsoft Windows. Samba donne la possibilité aux ordinateurs Windows d'accéder aux imprimantes et aux fichiers des ordinateurs Unix en permettant aux serveurs Unix de se substituer à des serveurs Windows.

La procédure de l'installation du serveur Samba se trouve en annexe page 128.

Le protocole SMB (Server Message Block) est un protocole permettant le partage des ressources (fichiers et imprimantes) sur des réseaux locaux avec des PC sous Windows. Dans l'ancien Windows NT 4, il était appelé CIFS (Common Internet File System). Il faut ensuite créer les dossiers des différents services de l'entreprise sur le Debian, si le fichier de configuration de samba a bien été renseigné les différents dossiers « commun service » doivent être visibles sur l'environnement Windows.

NFS

SERVICE NFS

Le Network File System (NFS) est à l'origine un protocole développé par Sun Microsystems en 1984 permettant à un ordinateur d'accéder aux fichiers présents sur des machines distantes via un réseau.

Pour notre part nous en aurons besoins afin de sauvegarder les fichiers présents sur Debian dans un autre Debian. Nous avons donc mis en place un deuxième linux pour pouvoir installer le client NFS, qui pourra sauvegarder automatiquement les ressources du serveur NFS.

CLIENT NFS

Nous avons mis en place un deuxième linux pour pouvoir installer le client NFS, qui pourra sauvegarder automatiquement les ressources du serveur NFS.

La procédure concernant la configuration du NFS se trouve en annexe page 132.

DHCP

Ce serveur permet de délivrer des adresses IP aux ordinateurs qui se connectent au réseau, de façon automatique.

Par rapport à un adressage IP manuel, les avantages d'utiliser un serveur DHCP sont :

- Pas besoin d'attribuer une adresse IP à un ordinateur. Cela se fait tout seul. Il suffit d'attribuer une plage d'adresses au serveur. Lorsqu'un ordinateur client DHCP demande l'accès au réseau, son adresse est allouée dynamiquement à l'intérieur d'une plage d'adresses définie sur le serveur.
- Évite les conflits d'adresse IP.
- Permet de contrôler l'utilisation des adresses IP de façon centralisée. Ainsi, si un paramètre change au niveau du réseau, comme, par exemple l'adresse de la passerelle par défaut, il suffit de changer la valeur du paramètre au niveau du serveur DHCP, pour que tous les ordinateurs aient une prise en compte du nouveau paramètre dès que le bail sera renouvelé.
- Le changement de plan d'adressage se trouve facilité par le dynamisme d'attribution.

Vous trouverez la mise en place de ce serveur DHCP en annexe page 134.

NOTRE OUTIL DE GESTION DE PARC

Pour notre solution de gestion de parc, il était convenu avec la direction de ne pas utiliser de logiciel existant déjà sur le marché. Il est important de vous informer que des logiciels en open source, très complets et fonctionnels se trouvent sur le marché (GLPI pour ne citer que celui-ci) pourraient vous éviter un coup financier et un gain de temps certain.

Nous vous proposons donc, grâce à un de nos technicien en interne, de développer un logiciel propre à notre entreprise.

Le logiciel en question sera développé avec le logiciel WinDev, métrisé en partie par ce même technicien.

Nous vous présentons donc une première ébauche de ce logiciel qu'il faudra rendre totalement opérationnel si la proposition est retenue.

Mais tout d'abord, qu'est-ce que WinDev ?

WinDev est un atelier de génie logiciel (AGL) édité par la société française PC SOFT et conçu pour développer des applications, principalement orientées données pour Windows 10, 8, 7, Vista, XP, 2008, 2003, 2000, et également pour Linux, .NET et Java. Il propose son propre langage : le WLangage. La première version de l'AGL est sortie en 1993.

WinDev inclut en standard un ensemble d'éditeurs qui composent l'Atelier de Génie Logiciel : éditeur d'analyse (description des données), éditeur de fenêtres, éditeur de requêtes SQL, éditeur d'états, éditeur de tests automatisés, éditeur d'aide, éditeur d'images, éditeur UML, éditeur de code, éditeur de télémétrie, robot de surveillance, audit d'application, éditeur de dossier RGPD...

WinDev utilise son propre langage de programmation, le WLangage, ressemblant beaucoup à du pseudo-code par son côté langage naturel qui peut faciliter la lecture du code par un débutant.

L'éditeur d'interface graphique permet de créer des IHM par glisser-déplacer. Il permet également de choisir un modèle de charte graphique parmi un ensemble proposé et d'en créer de nouveaux.

Le logiciel développé sera relié à une base de données. La base de données est au centre des dispositifs informatiques de collecte, mise en forme, stockage et utilisation d'informations.

Une base de données (database en anglais), permet de stocker et de retrouver l'intégralité de données brutes ou d'informations en rapport avec un thème ou une activité ; celles-ci peuvent être de natures différentes et plus ou moins reliées entre elles. Dans la très grande majorité des cas, ces informations sont très structurées, et la base est localisée dans un même lieu et sur un même support. Ce dernier est généralement informatisé.

Nous nous permettons de vous fournir en annexe page 140, un tableau récapitulatif des principales commandes SQL d'administration et de fonctionnement de la base de données.

PRESENTATION DU LOGICIEL DEVELOPPE EN INTERNE :

Nous proposons de faire une gestion en fonction des emplacements en suivant les plans des bâtiment fournis par vos soins.

En effet, cela permettra de connaître précisément l'emplacement de chaque matériel directement sur ces derniers.

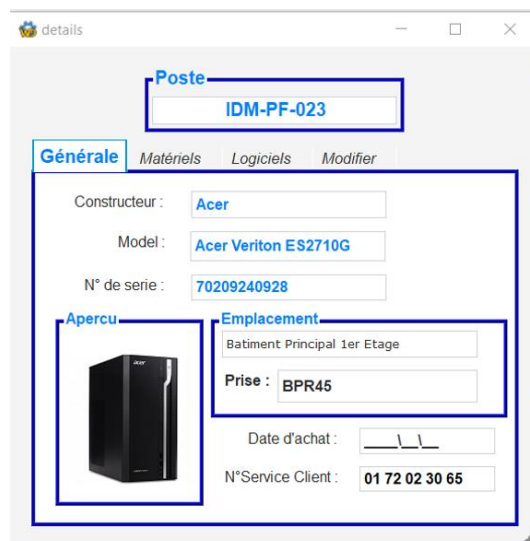
Chaque prise murale y étant représentée, les techniciens n'aurons donc plus de problème lors de leurs interventions sur site, ainsi que dans leur prise de décision concernant la disponibilité des prises dans les locaux.

Fenêtre principale de l'application :



La liste de la fenêtre principale permet de voir tous les postes de l'entreprise ainsi que leur emplacement.

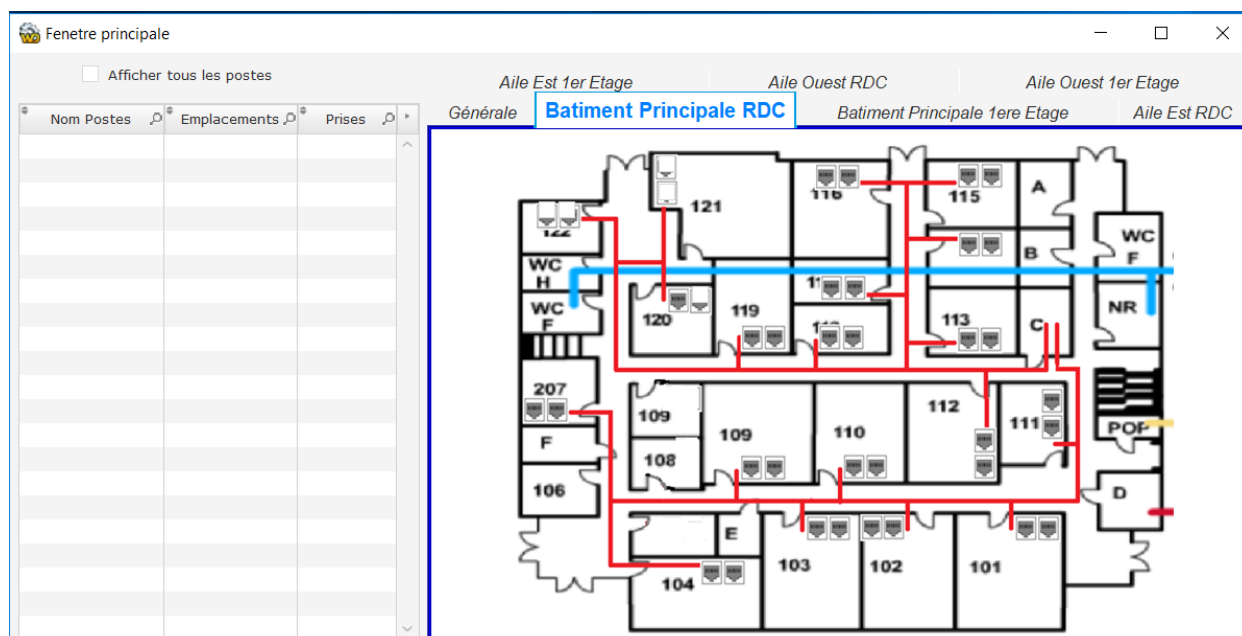
Une simple double clique dessus vous amènera vers la fiche technique de celui-ci.



Depuis cette fiche, il sera possible de modifier le contenu de ce même matériel ainsi que son emplacement, etc...

Il y a également un bouton permettant l'ajout de matériel au parc (il sera néanmoins nécessaire de renseigner les informations techniques de base de la machine).

Onglet pour les bâtiments :



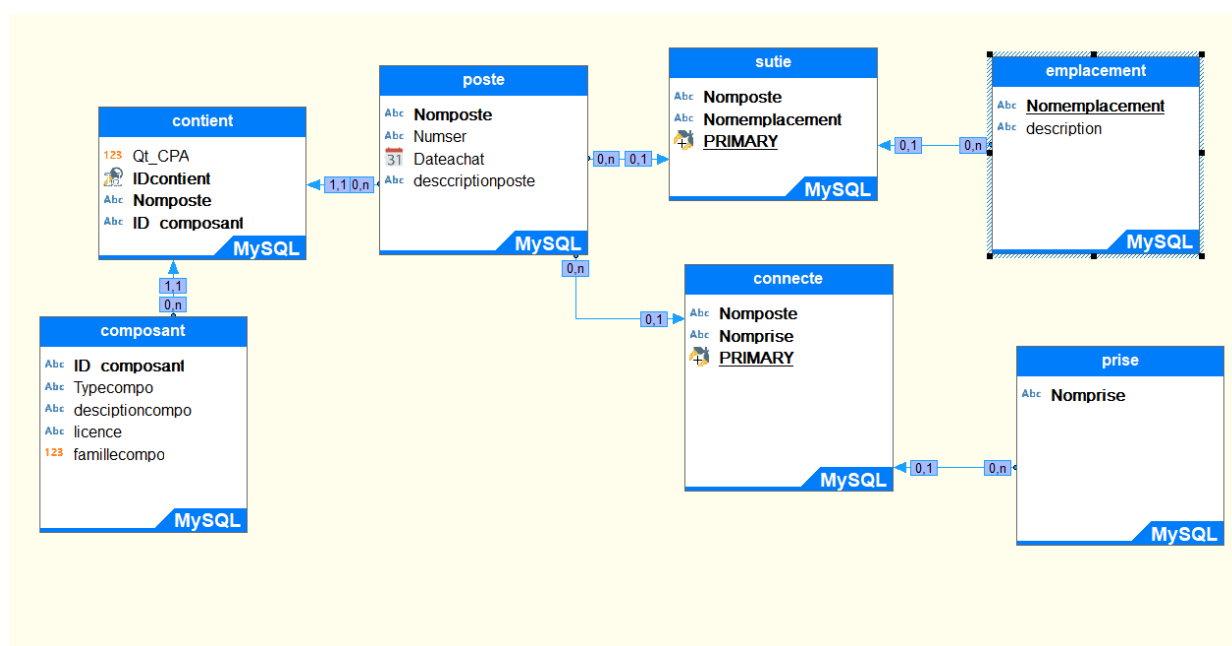
Les onglets présentant le plan des différentes ailes montreront l'emplacement de chaque prise, et effectuera un filtre sur la liste de gauche, répertoriant uniquement les postes présents sur l'aile en question.

Un simple double clic sur une prise murale du plan permettra soit d'y assigner un poste si celle-ci est libre, soit de voir le matériel câblé à cet endroit.

Nous prévoyons de rajouter des onglets et fenêtres permettant de répertorier les serveurs, ainsi que les imprimantes.

Nous sommes également prêts à écouter vos demandes concernant les fonctionnalités disponible, ou que vous souhaiteriez ajouter dans le programme.

SCHEMA DE LA BASE DE DONNEE DU LOGICIEL



DEVIS

Afin de mettre en place notre solution présentée dans ce dossier, des acquisitions matérielles, détaillées dans le devis suivant, sont nécessaires.

Vous trouverez en annexe page 142, les différents devis, tous équivalents niveau équipement, qui n'ont pas été retenus pour cause de prix trop élevés.



DEVIS No.1542965

Date du devis 15/06/2018
Référence du devis 1542174
Numéro de client 51584
Date de validité du devis 15/07/2018
Modalité de paiement 30 jours
Emis par Jean Michel
Contact client ID'Meuble

Destinataire :
ID'Meuble
35 rue de sillac
16000
Angoulême

Infos additionnelles

Merci d'avoir choisi Ingram
La livraison sera effectuée dans les 4 semaines après réception de la confirmation de la commande ;

Description	Quantités	Priz unitaires HT	TVA %	TVA	TOTAL TTC
Serveur HPE ProLiant DL380 G10	3	2 200,00	20,00%	440,00	7 920,00
3 ans Care Pack Pour Serveur(Intervention H+4)	4	865,00	20,00%	173,00	4 152,00
Windows Serveur 2016	3	800,00	20,00%	160,00	2 880,00
Disque Dur Seagate Enterprise 1To SAS	9	75,00	20,00%	15,00	810,00
Licence Utilisateur Windows Serveur	95	29,00	20,00%	5,80	3 306,00
Licence WinDev 23	1	1 320,00	20,00%	264,00	1 584,00
Buffalo TeraStation 3410RN 12To	2	930,00	20,00%	186,00	2 232,00
Veeam Backup et Replication a vie	2	1 365,00	20,00%	273,00	3 276,00
OU					
eam Backup et Replication Annuel Sur 3 A	6	69,65	20,00%	13,93	501,48
REMISE FOURNISSEUR					-10%
Total Abonnement VEEAM			Total Licence Definitive VEEAM		
Total HT	19 927,51			Total HT	22 424,58
TVA	1 530,73			TVA	1 530,73
Total TTC	21 458,24 		Total TTC		23 955,31

Signature du client (précédée de la mention « Bon pour accord »)

Serveur HPE ProLiant DL380 G10

Le serveur HPE ProLiant DL380 G10 est un serveur d'une taille de deux unités. Il est équipé des éléments suivants :

- Intel Xeon Silver 4114 de dix cœurs à 2,2 GHz ;
- 32 Go de SDRAM en DDR4 ;
- Contrôleur SAS à 12Gb/s ;
- Deux emplacements de processeur.

Ce serveur est en Gigabit Ethernet et a une consommation de 500 W.

3 ans Care Pack pour serveur (Intervention H+4)

Ce service HPE nous offre 3 ans de garantie, avec une intervention en H+4 en cas de problème. Cela signifie que l'intervention du constructeur se fera en moins de 4 heures après la demande. Le service est acheté en même temps que les serveurs.

Windows Serveur 2016

Windows Server 2016 est le système d'exploitation que nous souhaitons installer sur deux de nos serveurs. Nous avons fait le choix de prendre trois licences, du fait que nous avons trois serveurs avec Windows Serveur d'installé sur ceux-ci. Mais en sachant néanmoins que le nombre de licences est en adéquation avec le nombre de cœurs des machines. Il est nécessaire d'acheter une extension de licence lorsque le cap de 16 cœurs est dépassé sur une machine. Comme nous possédons des machines à 10 cœurs, une seule licence par machine est suffisante.

Disque Dur Seagate Enterprise 1To SAS

Afin d'avoir de la capacité de stockage dans nos serveurs, il est nécessaire d'ajouter des disques durs dans ceux-ci. Nous avons fait le choix d'ajouter deux disques sur d'1To dans chacun de nos serveurs. Un disque dur a également été acheté en plus, en cas de panne.

Licence Utilisateur Windows Serveur

Chaque utilisateur ou appareil accédant à Windows Server sous licence nécessite une licence d'accès client (CAL) Windows Server. Concrètement, ce type de licence est pour permettre à aux clients de se connecter et d'utiliser un logiciel serveur.

Licence WinDev 23

Certaines applications sont développées en interne avec ce logiciel. Notamment notre application de gestion de parc.

Buffalo TeraStation 3410RN 12To

L'acronyme NAS, pour Network Attached Storage, désigne un périphérique de stockage utilisé pour le stockage et le partage de fichiers via un réseau. Ces NAS nous serviront pour les sauvegardes. Les sauvegardes seront effectuées grâce au logiciel Veeam Backup.

Veeam Backup

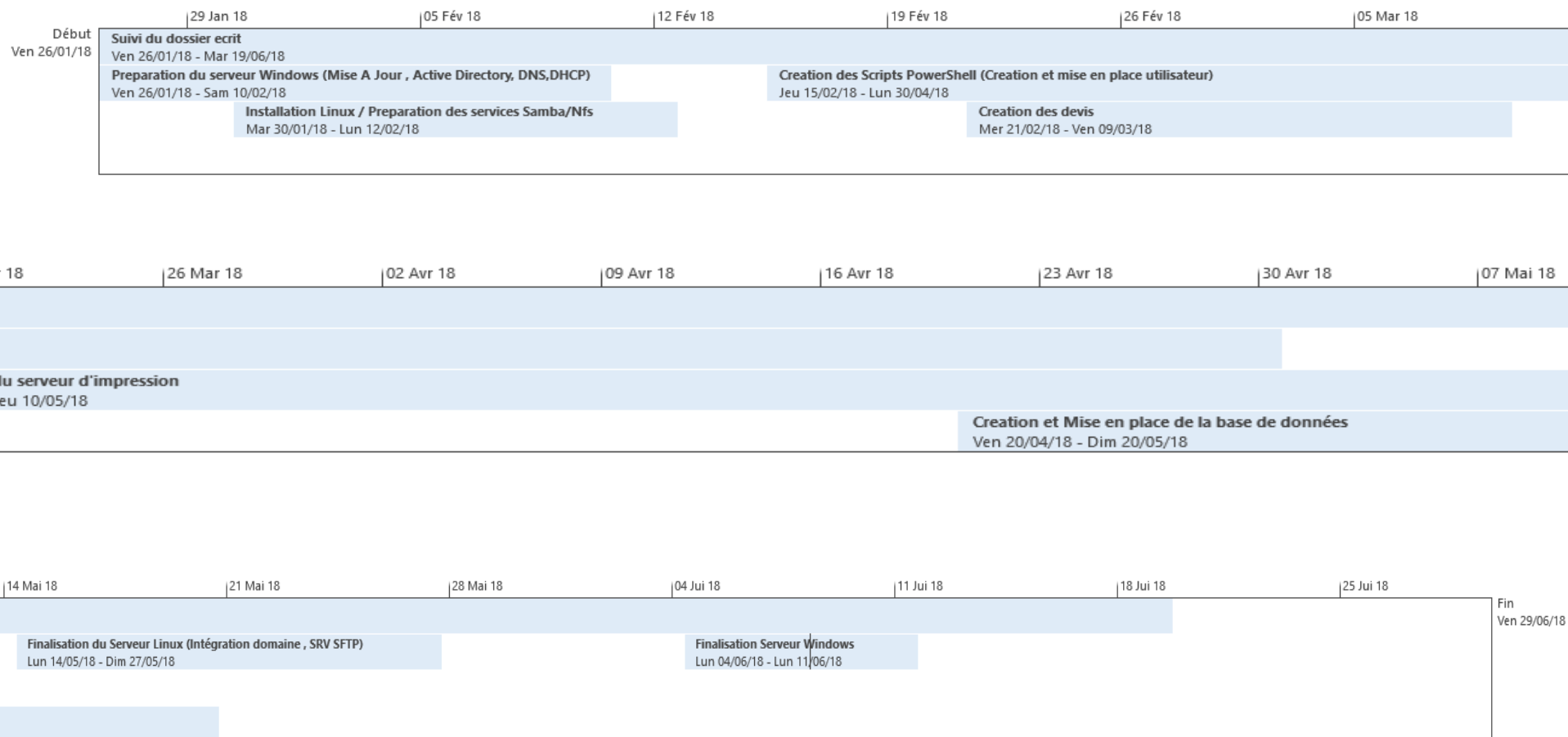
Veeam Backup est un logiciel de sauvegarde des données et de reprise d'activité pour les machines virtuelles VMware vSphere et Microsoft Hyper-V. Ce logiciel va nous servir à sauvegarder le contrôleur de domaine principal, les fichiers utilisateurs, la base de données ainsi que le FTP.

Concernant le budget, il est de 100 000 €. Dans le projet précédent, nous avons fait des dépenses pour un montant total de 72 252 €.

Le budget a été respecté, puisque pour ce projet actuel, nous avons un devis d'un montant de 23 955,31 €.

Nos dépenses totales s'élèvent donc à un montant de 96 207,31 €.

PLANNING DE MISE EN PLACE GLOBALE



ANNEXES

INSTALLATION DE WINDOWS SERVEUR 2016 – CORE

Prérequis :

Une fois que vous avez téléchargé Windows Server 2016, vous pouvez lancer l'installation. Si vous êtes sur une machine physique, vous pouvez graver l'image ISO sur un DVD ou sur une clé USB Bootable avec Rufus par exemple et il suffit de « Booter » dessus afin de démarrer l'installation.

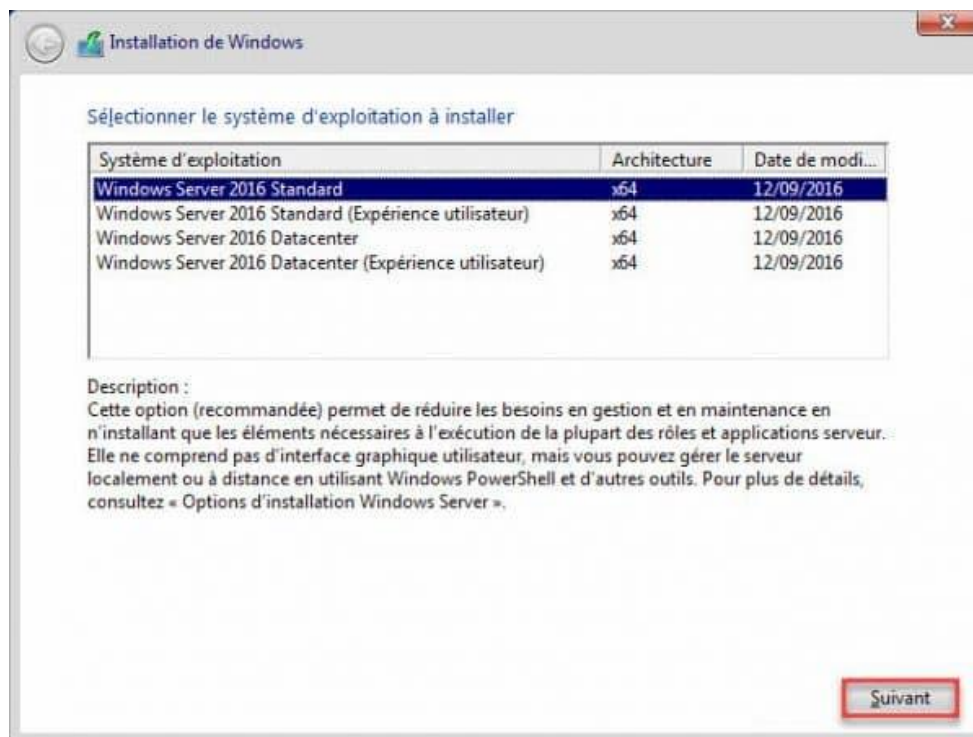
Le premier écran concerne le choix de la langue, Il nous suffit de sélectionner la langue désirée dans la liste.



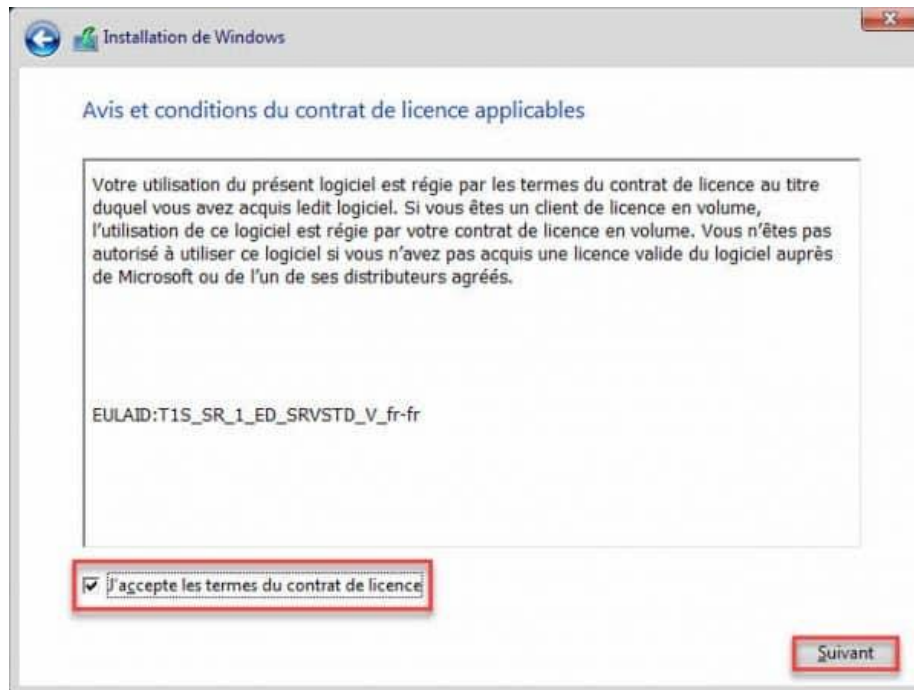
Vous pouvez maintenant passer à l'installation en cliquant simplement sur « Installer maintenant ». En cliquant sur « Réparer l'ordinateur » vous aurez la possibilité d'utiliser les utilitaires de dépannage.



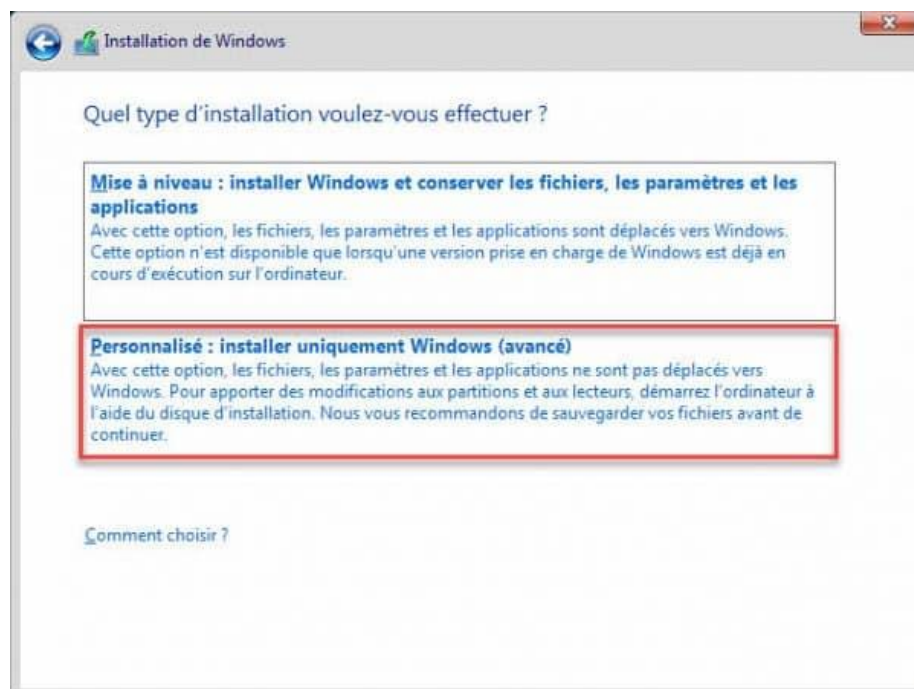
En fonction de la version de Windows Server 2016 que vous utiliserez, vous aurez accès à plusieurs versions. Sélectionnez ici la version qui nous concerne « Windows Server 2016 Standard » puis cliquez sur « Suivant ».



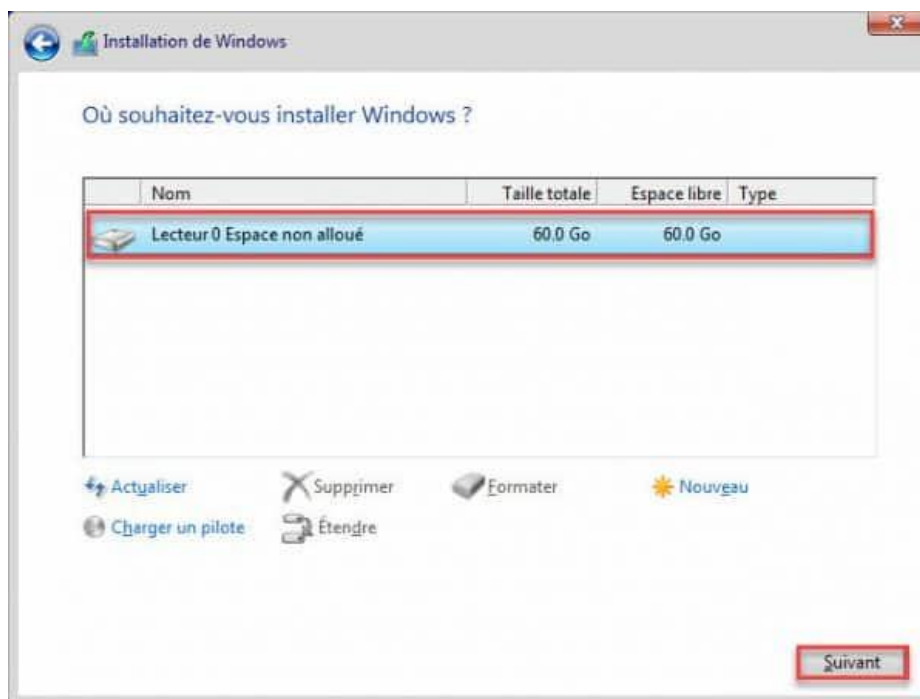
Acceptez les termes du contrat de licence après en avoir pris connaissance puis cliquez sur « Suivant ».



Sélectionner le type d'installation : Dans le cas présent, nous ferons une installation sur un disque vierge du coup, nous sélectionnerons « Personnalisé : installer uniquement Windows (avancé) ».



Sélectionnez le lecteur où vous souhaitez effectuer l'installation. Si besoin vous pouvez créer une ou des partitions directement depuis cette interface. Cliquez sur « Suivant » pour lancer l'installation.

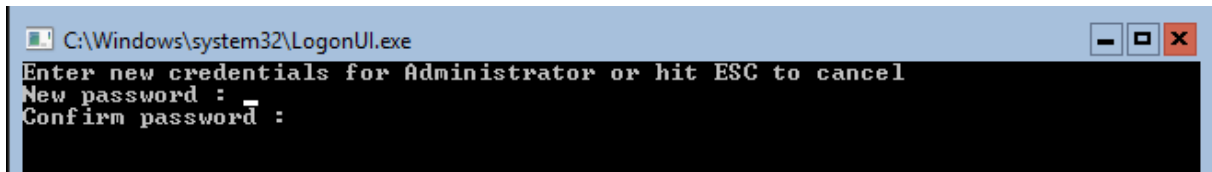


L'installation prendra quelques minutes, en fonction de la puissance de votre serveur.



Le processus redémarrera automatiquement le serveur, il faut changer le mot de passe du compte administrateur avec les critères de sécurités :

Minimum 8 Caractères dont : Majuscule(s)-Minuscule(s)-Chiffre(s)-Caractère(s) Spécial(aux)



Si les critères sont réunis cela vous affichera :



L'installation est maintenant terminée.

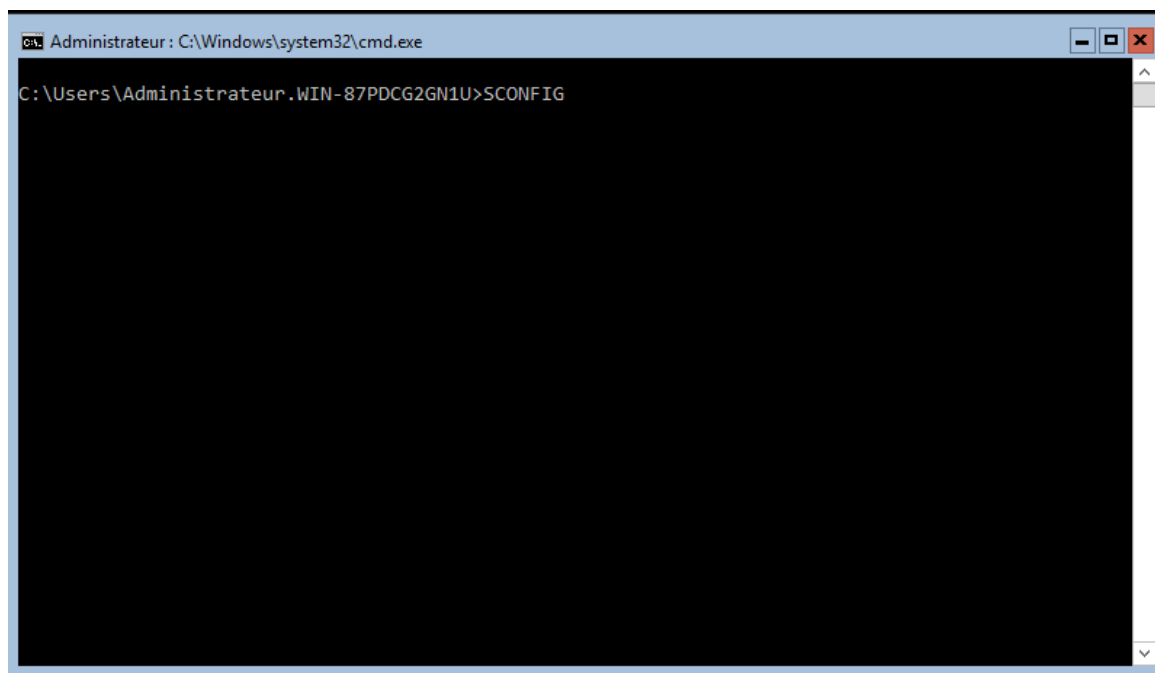
CONFIGURATION DE WINDOWS SERVEUR 2016 – CORE

Une fois que vous avez installé Windows Server 2016, nous allons voir la configuration « de base ».

Dans un premier temps nous allons modifier le nom du serveur puis nous modifierons l'adresse IP.

Pour cela nous allons faire appel à l'utilitaire « SCONFIG »

Une fois identifié en Administrateur il nous suffit de taper « SCONFIG » et de valider



The image shows a screenshot of a Windows command prompt window. The title bar reads "Administrateur : C:\Windows\system32\cmd.exe". The command prompt shows the current directory as "C:\Users\Administrateur.WIN-87PDCG2GN1U" and the command "SCONFIG" has been entered. The rest of the window is black, indicating that the command has been executed and the output is not visible.

Vous devriez arriver sur un écran similaire au suivant, afin de modifier le nom d'ordinateur nous allons sélectionner l'option « 2 ».

```

C:\Administrateur: C:\Windows\system32\cmd.exe - SCONFIG
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. Tous droits réservés.

Inspection en cours du système...

=====
Configuration du serveur
=====

1) Domaine ou groupe de travail :      Groupe de travail: WORKGROUP
2) Nom d'ordinateur :                  UN-NOM-BIZARD
3) Ajouter l'administrateur local
4) Configurer l'administration à distance  Activé
5) Paramètres de Windows Update :      DownloadOnly
6) Télécharger et installer les mises à jour
7) Bureau à distance :                  Désactivé

8) Paramètres réseau
9) Date et Heure
10) Paramètres de télémétrie            Renforcée
11) Activation de Windows

12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter pour revenir à la ligne de commande

Entrez un nombre pour sélectionner une option : 2
    
```

Il nous suffit de renseigner un nom approprié dans notre cas « IDM-SRV-DC1 ».

```

C:\Administrateur: C:\Windows\system32\cmd.exe - SCONFIG

=====
Configuration du serveur
=====

1) Domaine ou groupe de travail :      Groupe de travail: WORKGROUP
2) Nom d'ordinateur :                  UN-NOM-BIZARD
3) Ajouter l'administrateur local
4) Configurer l'administration à distance  Activé
5) Paramètres de Windows Update :      DownloadOnly
6) Télécharger et installer les mises à jour
7) Bureau à distance :                  Désactivé

8) Paramètres réseau
9) Date et Heure
10) Paramètres de télémétrie            Renforcée
11) Activation de Windows

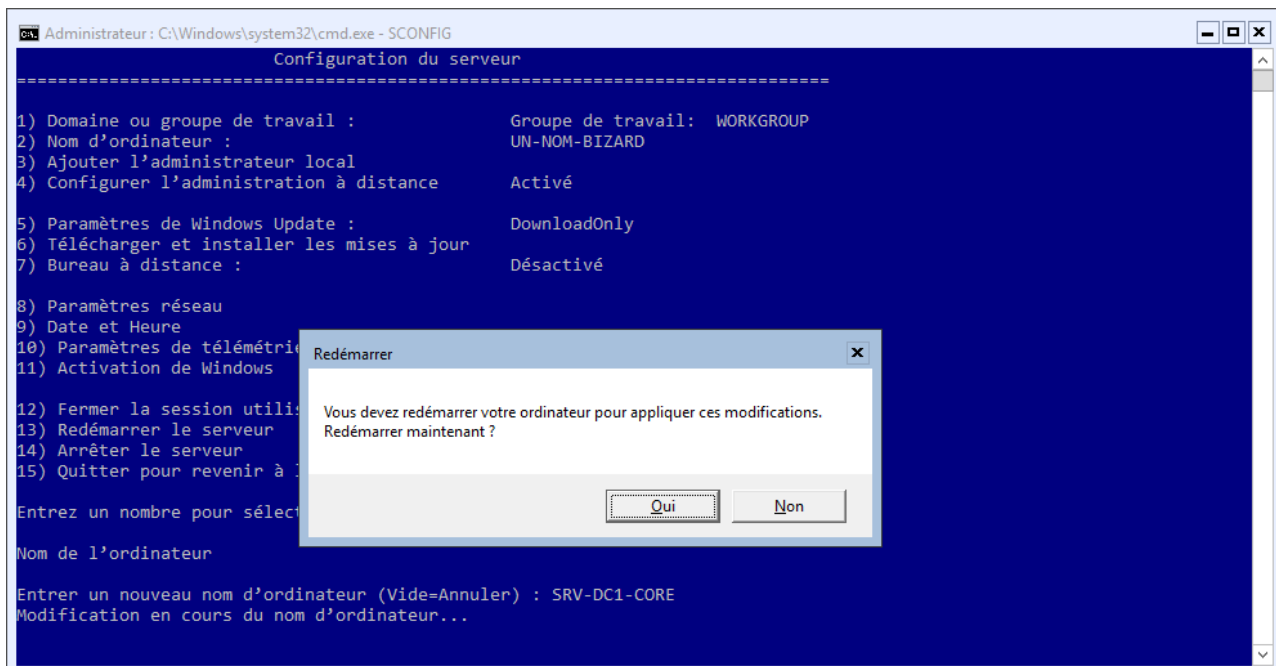
12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter pour revenir à la ligne de commande

Entrez un nombre pour sélectionner une option : 2

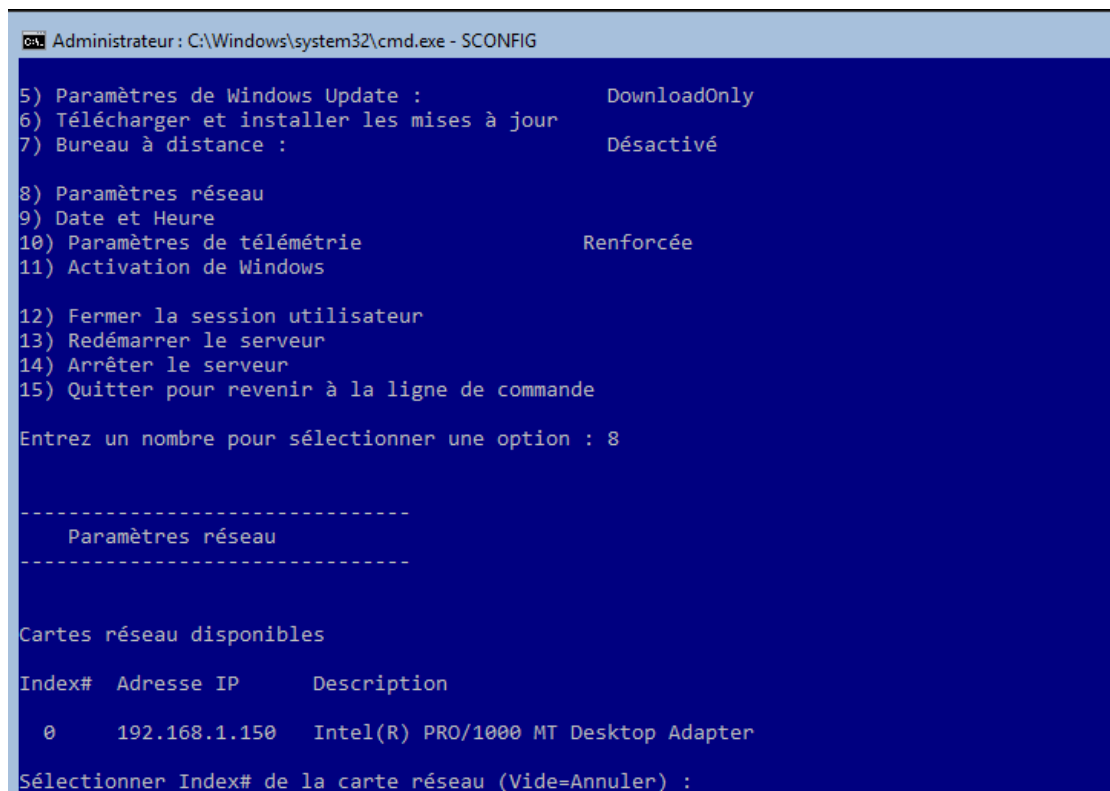
Nom de l'ordinateur
Entrez un nouveau nom d'ordinateur (Vide=Annuler) : SRV-DC1-CORE
    
```

Après avoir validé le serveur demandera à redémarrer.

Pour les besoins des paramètres qui suivent, nous le ferons redémarrer après la modification de l'adresse IP. Nous sélectionnons donc « NON ».



Pour modifier l'adresse IP il faut sélectionner l'option 8. Nous arrivons donc sur le choix de la carte réseau à modifier. Nous en disposons que d'une seule donc nous sélectionnons le choix « 0 ».



Sur cet écran nous sélectionnons « 1 » afin de modifier l'adresse IP

```

C:\> Administrateur : C:\Windows\system32\cmd.exe - SCONFIG

Cartes réseau disponibles

Index#  Adresse IP      Description
-----  -
      0      192.168.1.150    Intel(R) PRO/1000 MT Desktop Adapter

Sélectionner Index# de la carte réseau (Vide=Annuler) : 0

-----
Paramètres de carte réseau
-----

Index NIC                0
Description               Intel(R) PRO/1000 MT Desktop Adapter
Adresse IP                192.168.1.150    fe80::ccc3:99d2:4644:c1e6
Masque de sous-réseau    255.255.255.0
DHCP activé              Faux
Passerelle par défaut
Serveur DNS préféré
Serveur DNS auxiliaire

1) Définir l'adresse de la carte réseau
2) Définir les serveurs DNS
3) Effacer les paramètres du serveur DNS
4) Retourner au menu principal

Sélectionner une option : 1
  
```

Le choix concerne le type d'attribution de l'adresse IP DHCP(Automatique) ou statique (Manuelle).

Nous allons choisir statique en saisissant un « S »

```

C:\> Administrateur : C:\Windows\system32\cmd.exe - SCONFIG

Index#  Adresse IP      Description
-----  -
      0      192.168.1.150    Intel(R) PRO/1000 MT Desktop Adapter

Sélectionner Index# de la carte réseau (Vide=Annuler) : 0

-----
Paramètres de carte réseau
-----

Index NIC                0
Description               Intel(R) PRO/1000 MT Desktop Adapter
Adresse IP                192.168.1.150    fe80::ccc3:99d2:4644:c1e6
Masque de sous-réseau    255.255.255.0
DHCP activé              Faux
Passerelle par défaut
Serveur DNS préféré
Serveur DNS auxiliaire

1) Définir l'adresse de la carte réseau
2) Définir les serveurs DNS
3) Effacer les paramètres du serveur DNS
4) Retourner au menu principal

Sélectionner une option : 1

Sélectionner (D)HCP, IP (s)tatique (Vide=Annuler) : S
  
```


Une suite d'information va vous être demandé. En premier, l'adresse IP : renseignez l'adresse voulu. Le masque comme la passerelle, laissez les champs vide et validez. (Cf Plan IP).

```

Administrateur : C:\Windows\system32\cmd.exe - SCONFIG
Passerelle par défaut
Serveur DNS préféré
Serveur DNS auxiliaire

1) Définir l'adresse de la carte réseau
2) Définir les serveurs DNS
3) Effacer les paramètres du serveur DNS
4) Retourner au menu principal

Sélectionner une option : 1

Sélectionner (D)HCP, IP (s)tatique (Vide=Annuler) : s

Définir IP statique
Entrer une adresse IP statique : 192.168.1.150
Entrer un masque de sous-réseau (Vide = par défaut 255.255.255.0) :
Entrez la passerelle par défaut :
Affectation d'une adresse IP statique à la carte réseau...

-----
Paramètres de carte réseau
-----

Index NIC                0
Description              Intel(R) PRO/1000 MT Desktop Adapter
Adresse IP               192.168.1.150   fe80::ccc3:99d2:4644:c1e6
Masque de sous-réseau    255.255.255.0
  
```

Nous allons retourner sur les menus précédent en utilisant le choix « 4 » puis le choix « 13 » pour redémarrer.

Le paramétrage de base est ensuite terminé.

INSTALLATION DE WINDOWS 10 CLIENT AVEC RSAT

Prérequis :

-Avoir téléchargé le paquet « RSAT 1803 » et le copier sur une clé USB pour pouvoir l'installer ultérieurement.

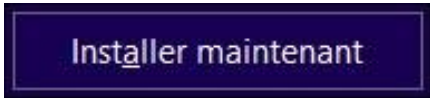
-Une fois que vous avez téléchargé Windows 10 (1803), vous pouvez lancer l'installation. Si vous êtes sur une machine physique, vous pouvez graver l'image ISO sur un DVD ou sur une clé USB Bootable avec Rufus par exemple et il suffit de « Booter » dessus afin de démarrer l'installation

Insérer le DVD ou la clé USB d'installation de Windows 10 et démarrer l'ordinateur à partir de ce support.

Confirmer la langue du système, le fuseau horaire et le type de clavier utilisé.



Cliquer sur « Installer maintenant » au milieu de l'écran.



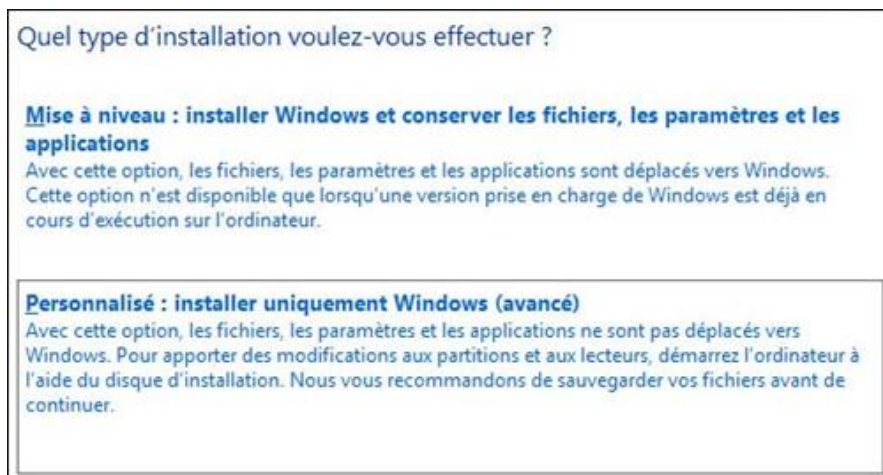
Indiquer la clé de produit : le numéro de série qui correspond à la licence Windows 10.



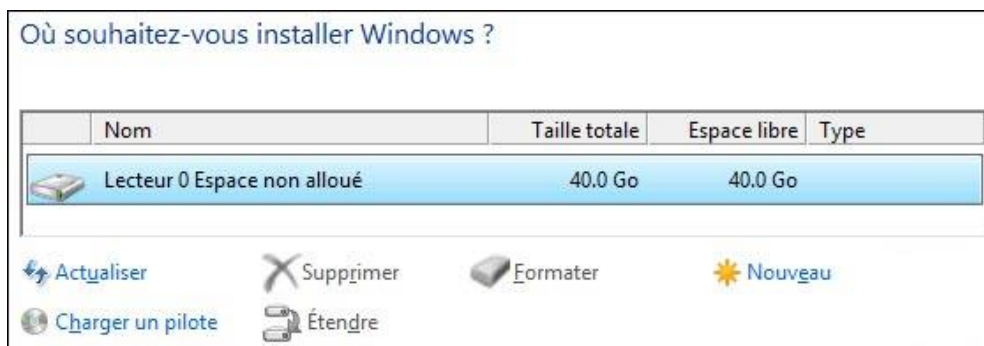
Accepter le contrat de licence.



Choisir l'installation « Personnalisé ».

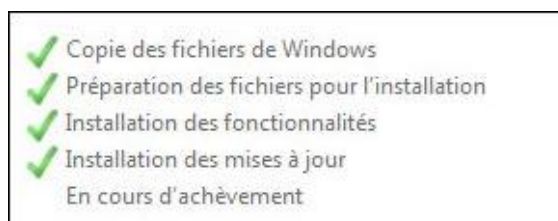


Sélectionner le disque dur de l'ordinateur. Il n'y a qu'un seul choix dans le cas d'un seul disque ou une seule partition, sinon indiquer le lecteur système où sera installé Windows 10.



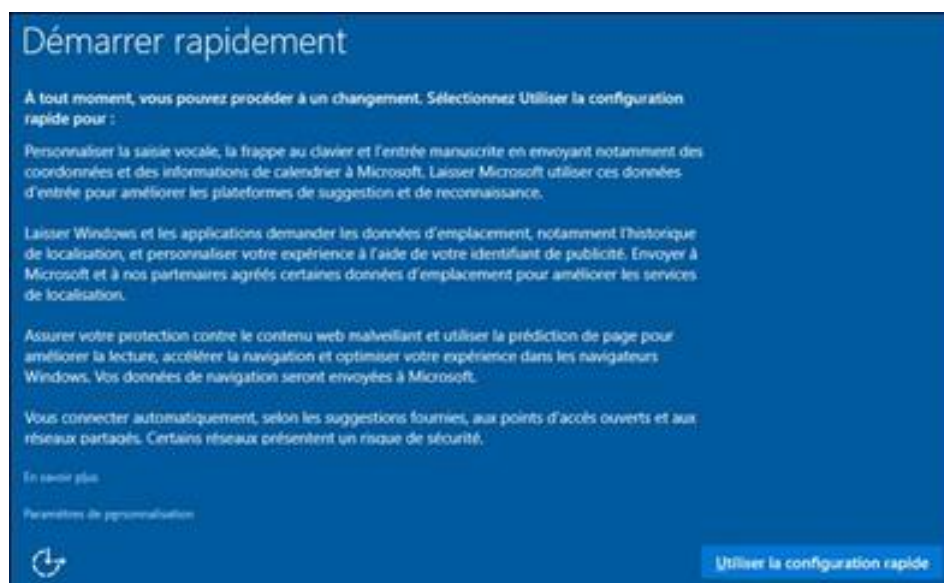
Le partitionnement peut également se faire par la suite par la configuration des disques et partitions du PC.

La copie de fichiers commence et l'installation se fait automatiquement.



Après un premier redémarrage de l'ordinateur, quelques écrans demandent à configurer et personnaliser l'ordinateur Windows 10.

Cliquer sur « Utiliser la configuration rapide » ou aller sur « Paramètres de personnalisation » pour spécifier les paramètres de confidentialité : aider à améliorer certaines fonctions, envoyer l'historique de localisation, utiliser un identifiant de publicité.



Paramètres de personnalisation

Personnalisation

Personnaliser la saisie vocale, la frappe au clavier et l'entrée manuscrite en envoyant des coordonnées, des informations de calendrier et d'autres données d'entrée connexes à Microsoft.

Désactivé

Envoyer des données de saisie clavier et manuscrite à Microsoft pour améliorer la plateforme de reconnaissance et de suggestion.

Désactivé

Laisser les applications utiliser votre identifiant de publicité pour l'exploitation des applications.

Désactivé

Localisation

Laisser Windows et les applications demander les données d'emplacement, notamment l'historique de localisation. Envoyez à Microsoft et à nos partenaires agréés certaines données d'emplacement pour améliorer les services de localisation.

Désactivé

Navigateur et protection

Utiliser les services en ligne SmartScreen pour favoriser la protection contre le contenu et les téléchargements malveillants présents sur des sites chargés par les navigateurs Windows et les applications issues du Windows Store.

Activé

Utiliser la prédiction de page pour améliorer la lecture, accélérer la navigation et optimiser votre expérience dans les navigateurs Windows. Vos données de navigation seront envoyées à Microsoft.

Désactivé

Connectivité et rapports d'erreurs

Se connecter automatiquement, selon les suggestions fournies, aux points d'accès ouverts. Certains réseaux présentent un risque de sécurité.

Désactivé

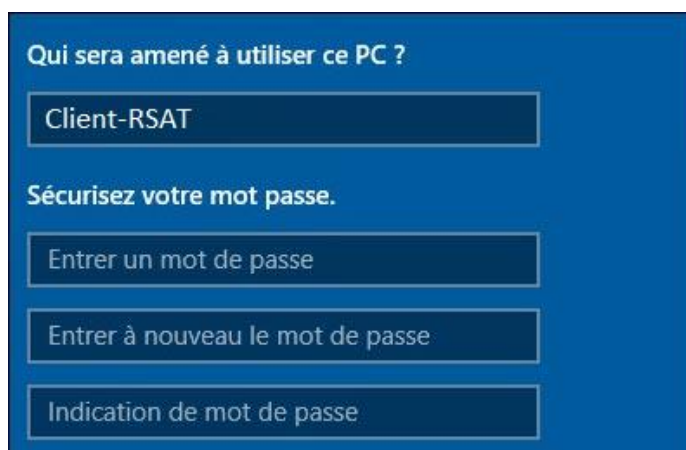
Se connecter automatiquement aux réseaux partagés par vos contacts.

Désactivé

Envoyer des rapports d'erreurs et de diagnostics à Microsoft.

Désactivé

Indiquer les informations pour créer un compte utilisateur et le protéger par un mot de passe.



Qui sera amené à utiliser ce PC ?

Client-RSAT

Sécurisez votre mot passe.

Entrer un mot de passe

Entrer à nouveau le mot de passe

Indication de mot de passe

Quelques minutes peuvent être nécessaires pour préparer la session. On arrive enfin sur le Bureau de Windows 10 avec son menu Démarrer de nouvelle génération.



Nous allons procéder à présent à l'installation du package RSAT. Pour cela il suffit tout simplement de télécharger et de l'installer. L'installation est simple il suffit de faire suivant lorsque vous y êtes invité. A la fin de l'installation vous serez invité à redémarrer pour finir l'installation. L'intégralité des fonctionnalités aura été ajouté au menu démarrage dans un dossier « Outils d'administration Windows ».

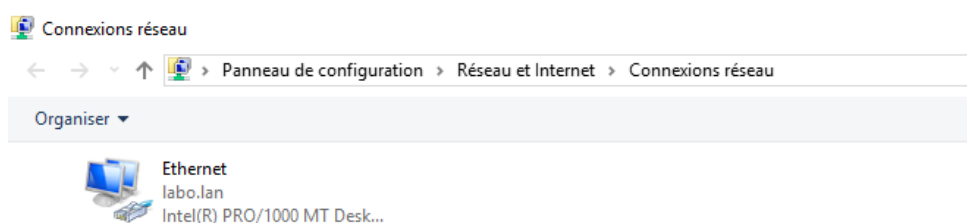
CONFIGURATION IP ET NOMINALE DE WINDOWS 10

A présent nous allons modifier l'adresse IP ainsi que le Nom du PC.

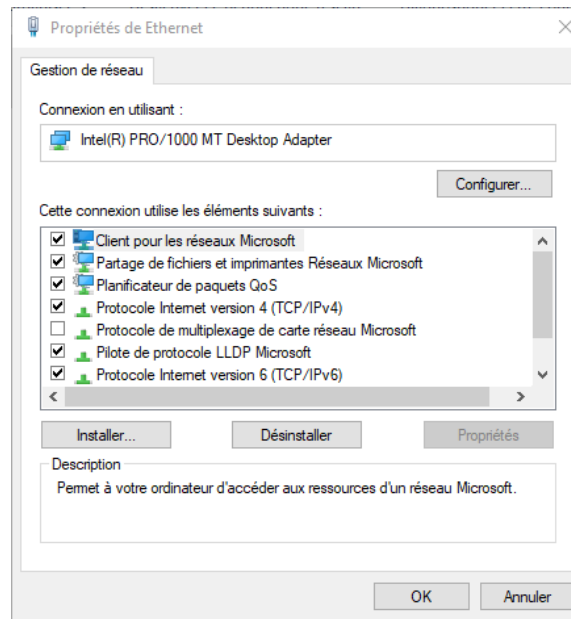


Pour modifier l'adresse IP il suffit de faire : la combinaison de touche « Windows » + R. Une fenêtre apparaît. Saisir « ncpa.cpl » est valider.

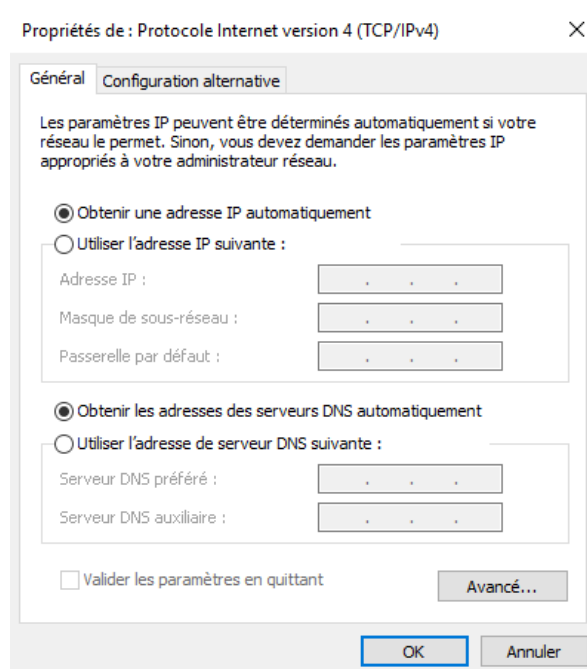
Vous arriverez dans le gestionnaire de carte réseau. Sélectionnez la carte concernée et cliquez sur « Propriétés ».



Double cliquez sur « Protocole Internet V4 »

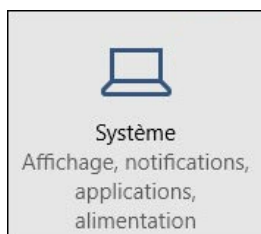


Sur cette fenêtre désélectionnez l'IP Automatique et passez en manuel, « Utiliser l'adresse IP suivante ». Il suffit d'y renseigner les IP qui sont présent sur le Plan Réseau et de valider en cliquant sur « OK ».

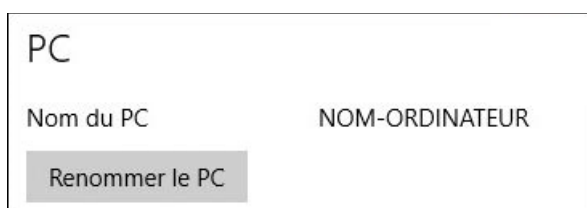


A présent nous allons modifier la Dénomination du poste

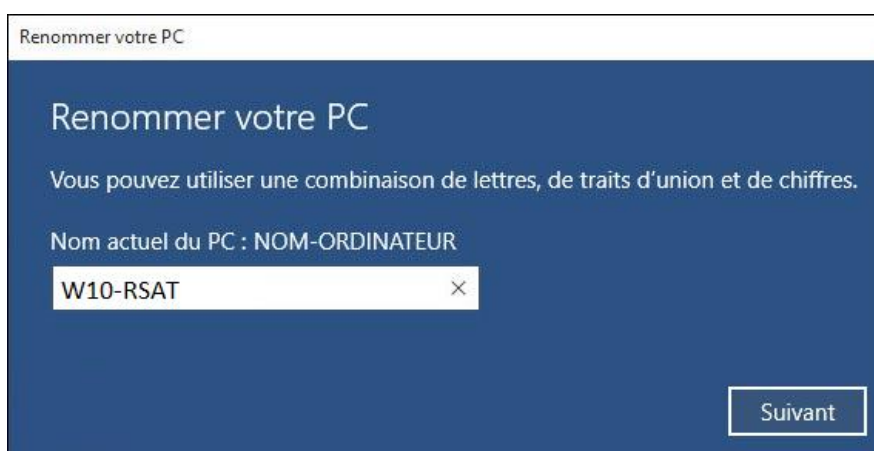
Tout d'abord ouvrez le **menu Démarrer, Paramètres**.
Cliquer sur l'icône **Système**.



A l'onglet « **Informations système** », cliquer sur « **Renommer le PC** » de la partie de droite.



Indiquer le **nouveau nom de l'ordinateur**.



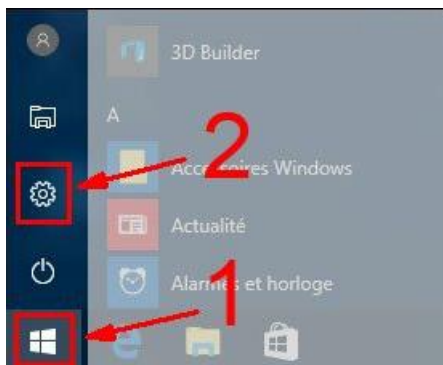
Redémarrez l'ordinateur maintenant ou plus tard pour valider les modifications.



LIAISON ENTRE RSAT ET LE SERVEUR

Pour pouvoir faire la liaison entre RSAT et le serveur nous devons intégrer le poste au domaine.

Ouvrir le menu Démarrer et les Paramètres



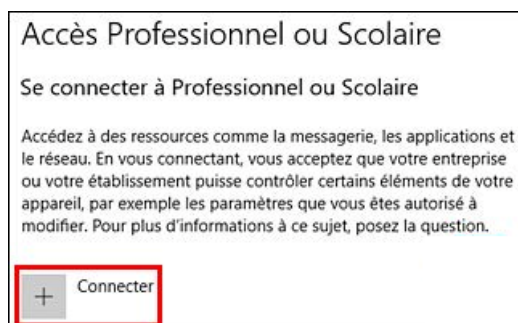
Ouvrir les Comptes.



Dans le menu de gauche, cliquer sur « Accès professionnel ou scolaire » :



Cliquer sur le bouton « + » de « Connecter » :



Joindre cet appareil à un Domaine Active Directory local Dans le cas d'un domaine local traditionnel, choisir la seconde option.

Configurer un compte professionnel ou scolaire

Vous aurez accès à des ressources comme les e-mails, les applications et le réseau. Si vous vous connectez, votre entreprise ou votre école pourront contrôler certaines choses sur cet appareil, par exemple les paramètres que vous pouvez modifier. Adressez-vous à elles pour obtenir des informations spécifiques.

xyz@example.com

Actions alternatives :

Ces actions configureront l'appareil comme appartenant à votre organisation, qui en aura le contrôle total.

Joindre cet appareil à Azure Active Directory

Joindre cet appareil à un domaine Active Directory local

Suivant

Saisir le nom du domaine sous sa forme DNS (par exemple « domaine.local ») et continuer par Suivant.

Joindre un domaine

Joindre un domaine

Nom du domaine

domaine.local

Suivant Annuler

S'authentifier avec un compte Administrateur AD ou un utilisateur autorisé à ajouter des postes dans le réseau.

Sécurité Windows

Joindre un domaine

Entrez les informations de votre compte de domaine afin de vérifier que vous avez les autorisations pour vous connecter au domaine.

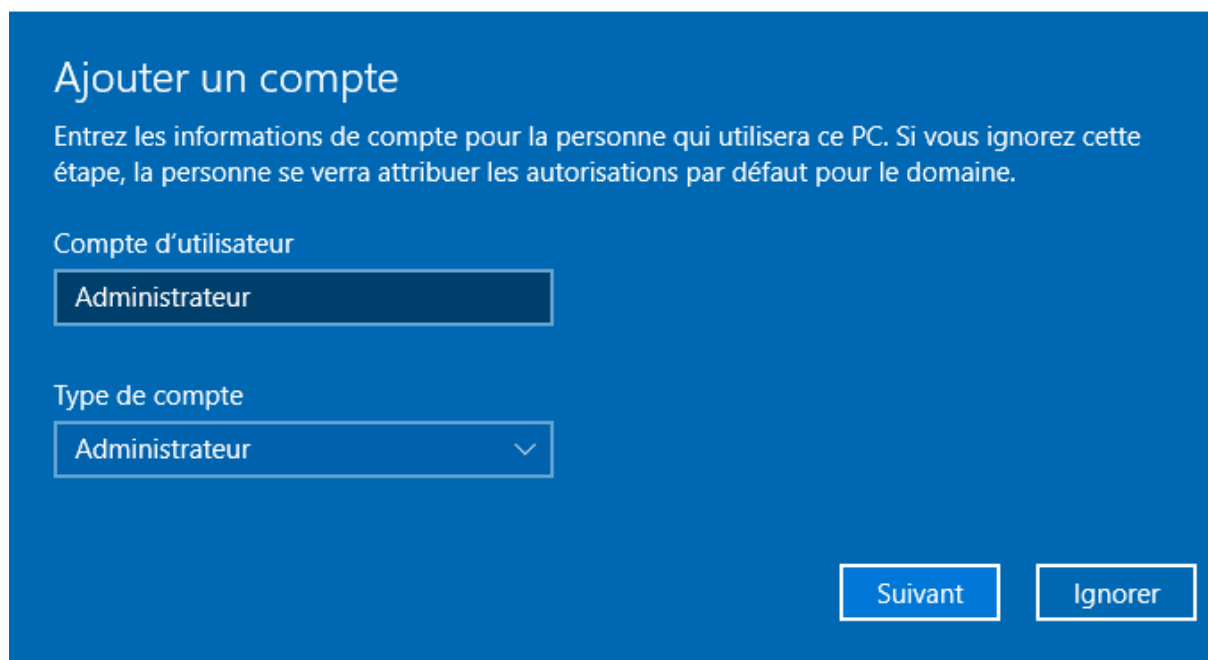
DOMAINE\Administrateur

.....

OK Annuler

A présent il faut bien sélectionner le type de compte « Administrateur » pour pouvoir gérer nos serveurs

Ajouter un compte



Ajouter un compte

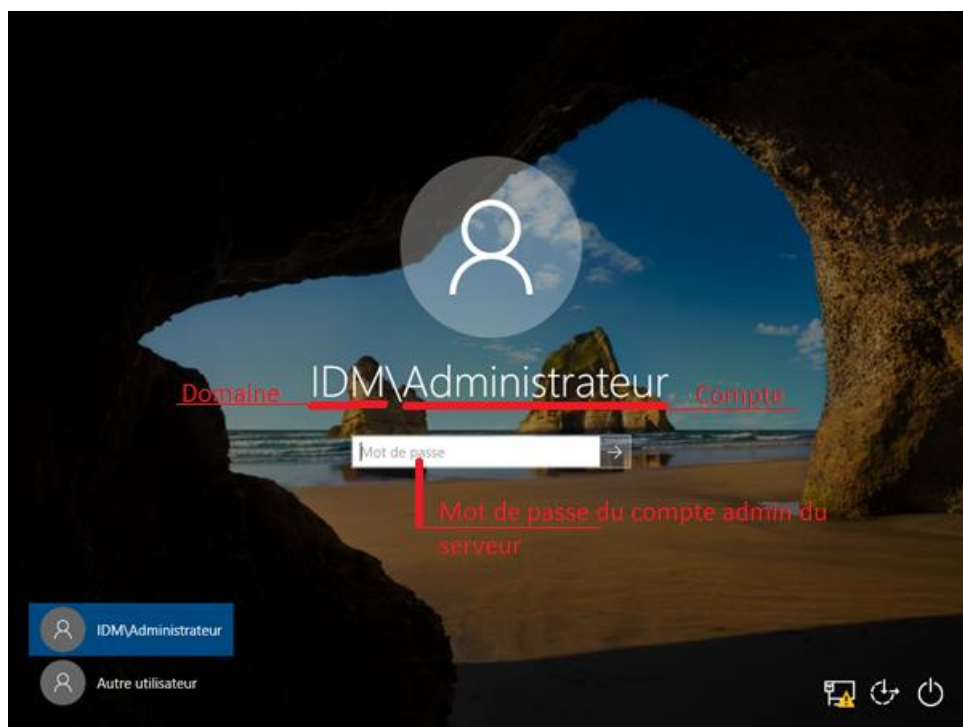
Entrez les informations de compte pour la personne qui utilisera ce PC. Si vous ignorez cette étape, la personne se verra attribuer les autorisations par défaut pour le domaine.

Compte d'utilisateur
Administrateur

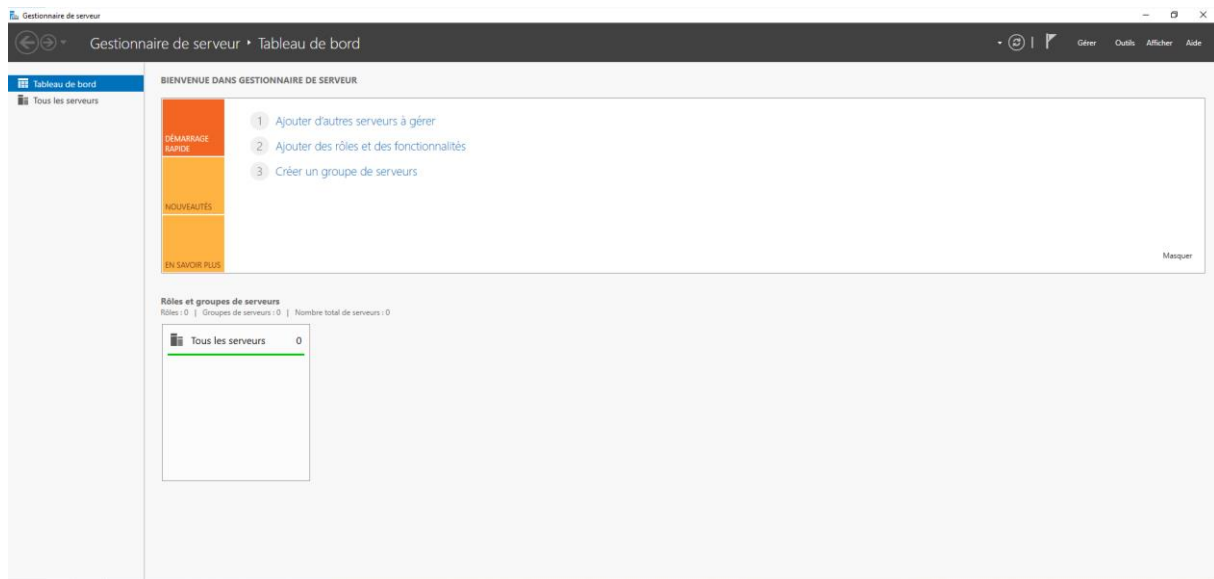
Type de compte
Administrateur

Suivant Ignorer

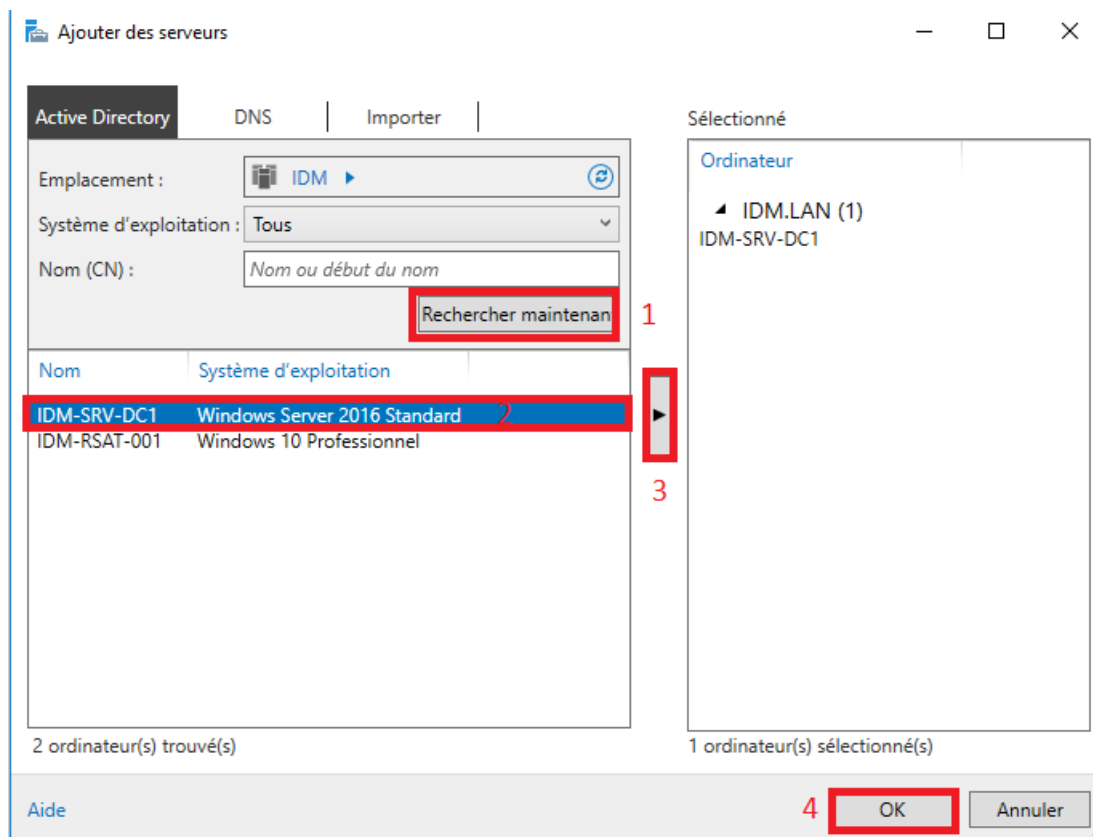
Il nous suffit juste de redémarrer le poste après avoir validé. Ensuite, nous connecter avec le mot de passe administrateur du serveur



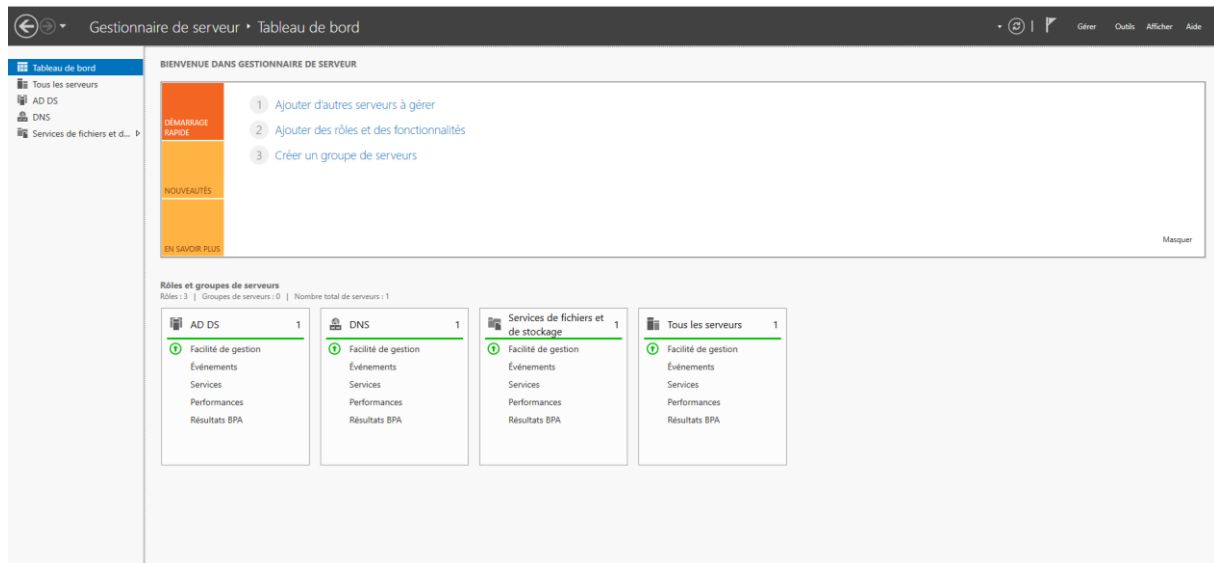
Puis, exécuter le « Serveur manager » (installé grâce aux RSAT).



Cliqué sur « Gérer » puis sur « Ajouter des serveurs ».



Une fois validé, les deux serveurs communiqueront et vous devriez avoir un affichage similaire.



INSTALLATION DU ROLE AD-DS/DNS SUR LE SERVEUR

Prérequis :

- Avoir ajouté 3 Disques durs de 4Go chacun et les avoirs initialisés.

Exécuté Notepad et copier le programme si dessous :

```
select disk 1 Nous selectionnons le disque concerné  
attribute disk clear readonly Autorisation de l'écriture sur le disque  
convert gpt Convertir le disque en GPT  
convert dynamic Convertir le disque en Dynamic  
create volume simple Creation du volume  
format quick fs=ntfs label=Base Formatage en NTFS et Nommage  
assign letter=B Assignment de la lettre  
select disk 2  
attribute disk clear readonly  
convert gpt  
convert dynamic  
create volume simple  
format quick fs=ntfs label=Logs  
assign letter=L  
select disk 3  
attribute disk clear readonly  
convert gpt  
convert dynamic  
create volume simple  
format quick fs=ntfs label=sysVol  
assign letter=S
```

Enregistré le script dans un dossier « Scripts » à la racine du C : sous le nom (par exemple : « Disque »)

Pour l'exécuter il nous suffit de taper dans l'invite de commande :

```
C:\Users\Administrateur.WIN-TGCQ1MGVIER>diskpart -s C:\Scripts\Disque.txt
```

Pour vérifier le bon déroulement du script il faut entrer :

Nous voyons bien que 3 partitions ont été créées :

-Sysvol avec la lettre « S » d'une capacité de 4Go

-Logs avec la lettre « L » d'une capacité de 4Go

-Base avec la lettre « B » d'une capacité de 4Go

```
C:\Users\Administrateur.WIN-TGCQ1MGVIER>diskpart 1
Microsoft DiskPart version 10.0.14393.0
Copyright (C) 1999-2013 Microsoft Corporation.
Sur l'ordinateur : SRV-DC1

DISKPART> list volume 2
```

N° volume	Ltr	Nom	Fs	Type	Taille	Statut	Info
Volume 0	S	SysVol	NTFS	Simple	4062 M	Sain	
Volume 1	L	Logs	NTFS	Simple	4062 M	Sain	
Volume 2	B	Base	NTFS	Simple	4062 M	Sain	
Volume 3	D	VBox_GAs_5	CDFS	CD-ROM	55 M	Sain	
Volume 4		Réservé au	NTFS	Partition	500 M	Sain	Système
Volume 5	C		NTFS	Partition	29 G	Sain	Démarrag

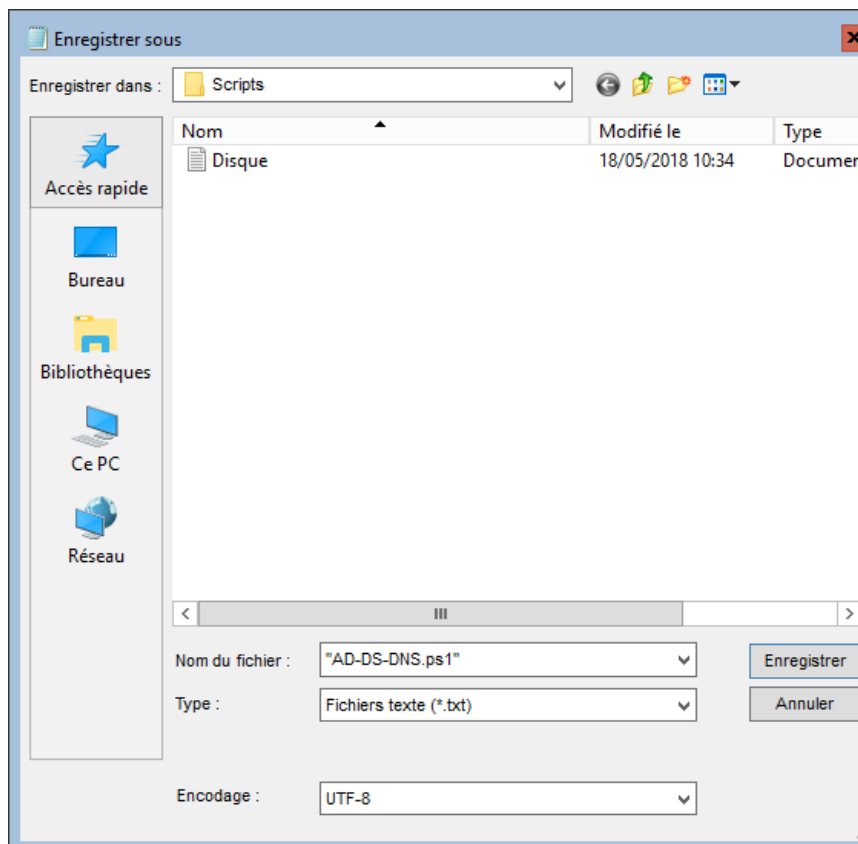
```
DISKPART>
```

A présent nous allons créer le script pour mettre en place L'active Directory et le service DNS

Le Script PowerShell est le suivant :

```
install-windowsfeature AD-Domain-Services Installation du service AD-DS
install-ADDSTForest Installation de la Forêt
-DomainName "IDM.lan" Déterminatoin du nom de domaine
-DomainNetbios "IDM" Netbios du Domaine
-DomainMode "7" Mode de compatibilité du domaine
-ForestMode "7"
-InstallDns:$true Installation du service DNS
-CreateDnsDelegation:$false
-DatabasePath "B:\NTDS" Chemin d'accès au dossier Data
-Logpath "L:\NTDS" Chemin d'accès au dossier Logs
-SysvolPath "S:\SYSVOL" Chemin d'accès au dossier Sysvol
-NorebootOnCompletion:$false Redemarrage a la fin de la creation
-Force:$true
```


Enregistrez le script dans un dossier « Scripts » à la racine du C : sous le nom (par exemple : « AD-DS-DNS ») avec la configuration suivante :



Pour l'exécuter il faut taper :

```
C:\Users\Administrateur.WIN-TGCQ1MGVIER> cd c:\Scripts 1
c:\Scripts> powershell 2
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Tous droits réservés.

PS C:\Scripts> .\AD-DS-DNS.ps1 3
```

A présent il nous faut rentrer un mot de passe qui nous servira à restaurer l'AD en cas de crash.

```
PS C:\Scripts> .\AD-DS-DNS.ps1

Success Restart Needed Exit Code      Feature Result
-----
True      No           Success      {Services AD DS, Outils d'administration d...
SafeModeAdministratorPassword: _
```

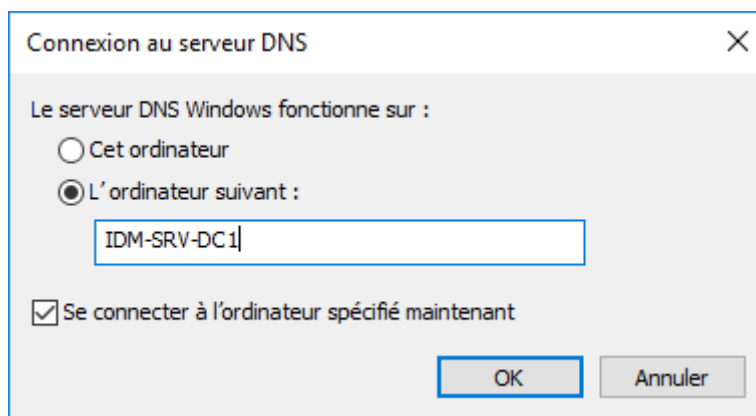
Après avoir validé le serveur installera le rôle et redémarrera.

MISE EN PLACE DE LA ZONE INVERSE DU DNS

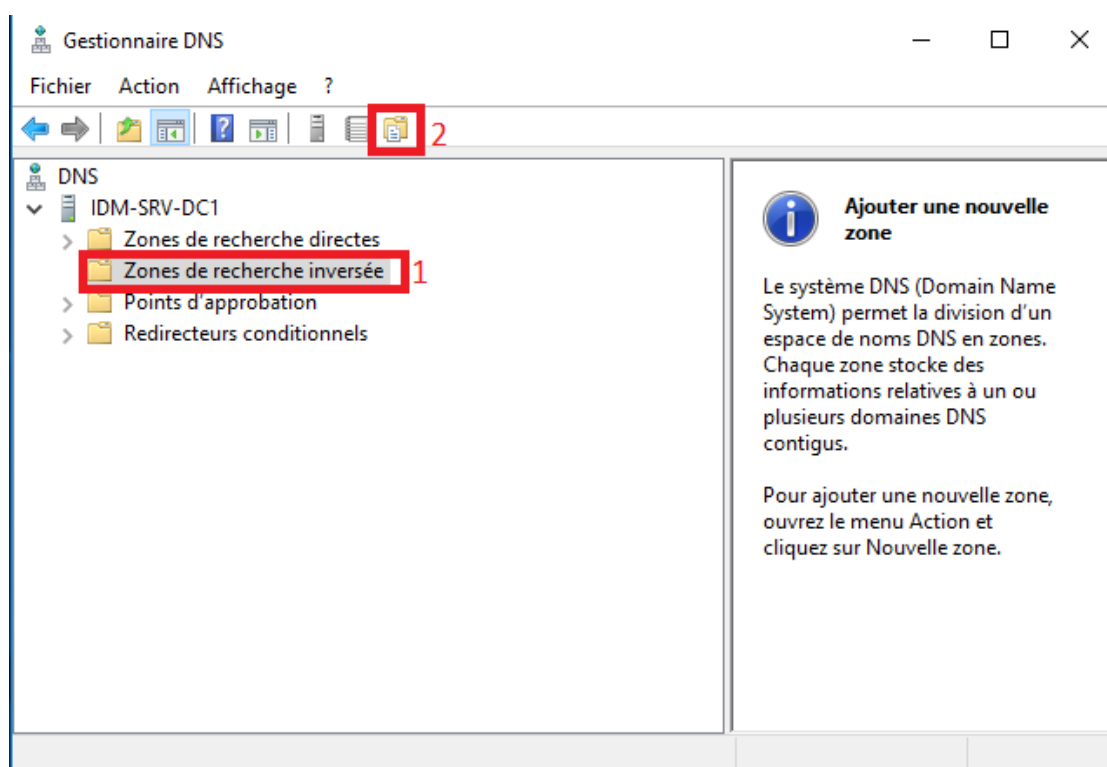
Exécutez le « DNS » (installé grâce aux RSAT). Remplissez la fenêtre de la façon suivante :

-L'ordinateur suivant : car nous travaillons sur le serveur à distance.

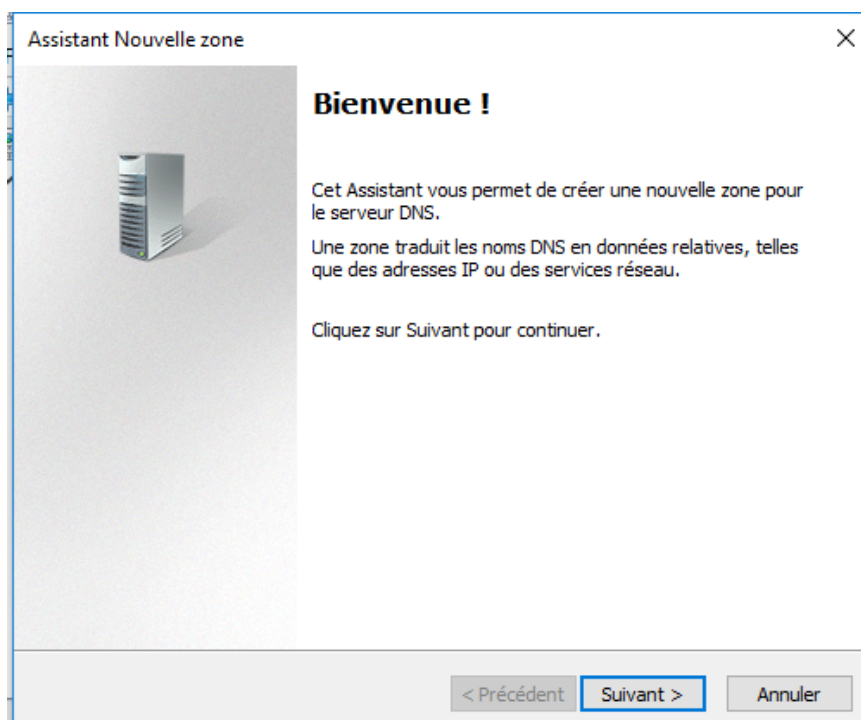
-IDM-SRV-DC1 : Il s'agit du nom du serveur à paramétrer.



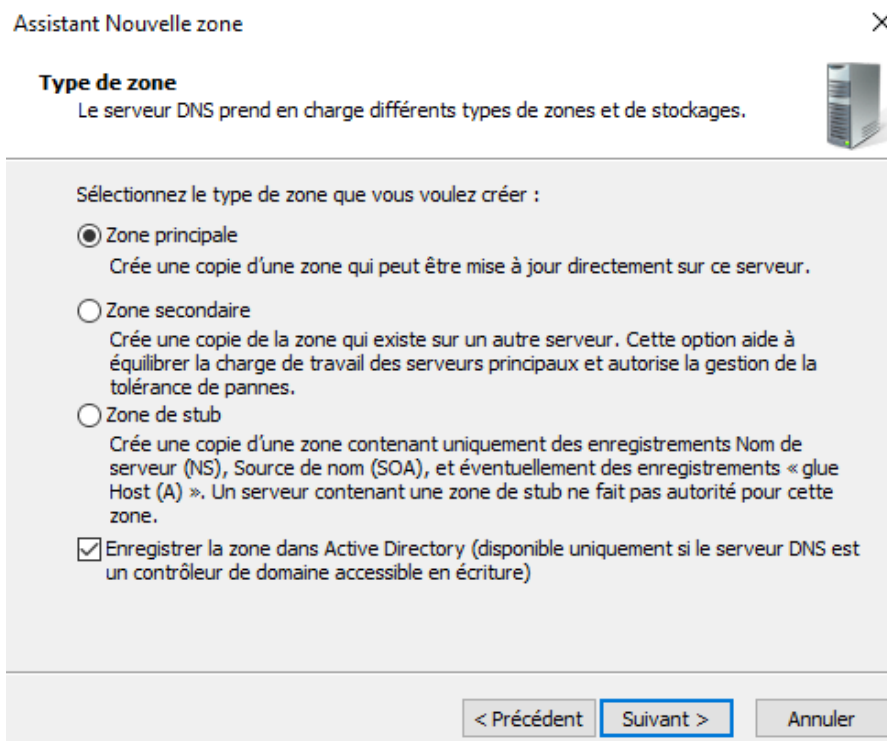
Après avoir validé suivez les manipulations suivantes :



Ensuite suivez les étapes suivantes : « Suivant ».



« Suivant ».



« Suivant ».

Étendue de la zone de réplication de Active Directory

Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau.



Choisissez la façon dont les données de la zone doivent être répliquées :

- Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt : IDM.lan
- Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : IDM.lan
- Vers tous les contrôleurs de ce domaine (compatibilité avec Windows 2000) : IDM.lan
- Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition d'annuaire :

< Précédent

Suivant >

Annuler

« Suivant ».

Assistant Nouvelle zone



Nom de la zone de recherche inversée

Une zone de recherche inversée traduit les adresses IP en noms DNS.



Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4 ou les adresses IPv6.

- Zone de recherche inversée IPv4
- Zone de recherche inversée IPv6


< Précédent

Suivant >

Annuler

Entrez y le début de vos adresses IP (ex : si votre réseau est en 192.168.10.X – renseignez 192.168.10) puis « Suivant ».

Assistant Nouvelle zone ×

Nom de la zone de recherche inversée 

Une zone de recherche inversée traduit les adresses IP en noms DNS.

Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.

ID réseau :


L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

Nom de la zone de recherche inversée :

Mettez sur le second choix puis « Suivant »

Assistant Nouvelle zone ×


Mise à niveau dynamique 

Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.

Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.
Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)
Cette option n'est disponible que pour les zones intégrées à Active Directory.

Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées
Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.

 Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.

Ne pas autoriser les mises à jour dynamiques
Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

Et il suffit de mettre « Terminer »

Pour finaliser la création de la zone inverse utilisez la combinaison de touches :

« Windows » + R et écrivez « ipconfig /registerdns » puis validez. Cela va créer automatiquement les pointeurs PTR.

CREATION ET PARAMETRAGE DU SERVEUR DE REPLICATION AD-DNS

Prérequis :

- Avoir un second Windows Serveur 2016, adressé et nommé correctement (cf. : début de la procédure).

Une fois votre second serveur « DC2 » initialisé et opérationnel nous allons l'intégrer au domaine pour cela il suffit d'exécuter « sconfig ».

Pour intégrer un poste dans un domaine il faut sélectionner le choix 1

```

=====
Configuration du serveur
=====
1) Domaine ou groupe de travail :      Groupe de travail: WORKGROUP
2) Nom d'ordinateur :                  IDM-SRV-DC2
3) Ajouter l'administrateur local
4) Configurer l'administration à distance      Activé
5) Paramètres de Windows Update :      DownloadOnly
6) Télécharger et installer les mises à jour
7) Bureau à distance :                  Désactivé

8) Paramètres réseau
9) Date et Heure
10) Paramètres de télémétrie            Renforcée
11) Activation de Windows

12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter pour revenir à la ligne de commande

Entrez un nombre pour sélectionner une option :

```

Pour un domaine il faut choisir « D » pour Domaine.

```

Administrateur : C:\Windows\system32\cmd.exe - sconfig
=====
Configuration du serveur
=====
1) Domaine ou groupe de travail :      Groupe de travail: WORKGROUP
2) Nom d'ordinateur :                  IDM-SRV-DC2
3) Ajouter l'administrateur local
4) Configurer l'administration à distance      Activé
5) Paramètres de Windows Update :        DownloadOnly
6) Télécharger et installer les mises à jour
7) Bureau à distance :                  Désactivé
8) Paramètres réseau
9) Date et Heure
10) Paramètres de télémétrie             Renforcée
11) Activation de Windows
12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter pour revenir à la ligne de commande

Entrez un nombre pour sélectionner une option : 1

Changer l'appartenance du domaine ou groupe de travail
Joindre le (D)omaine ou (G)roupe de travail ? (Vide=Annuler)
  
```

Sur cet écran il nous suffit de renseigner le nom du domaine (IDM.lan) puis le nom d'utilisateur (Administrateur) et le mot de passe associé.

```

4) Configurer l'administration à distance      Active
5) Paramètres de Windows Update :        DownloadOnly
6) Télécharger et installer les mises à jour
7) Bureau à distance :                  Désactivé
8) Paramètres réseau
9) Date et Heure
10) Paramètres de télémétrie             Renforcée
11) Activation de Windows
12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter pour revenir à la ligne de commande

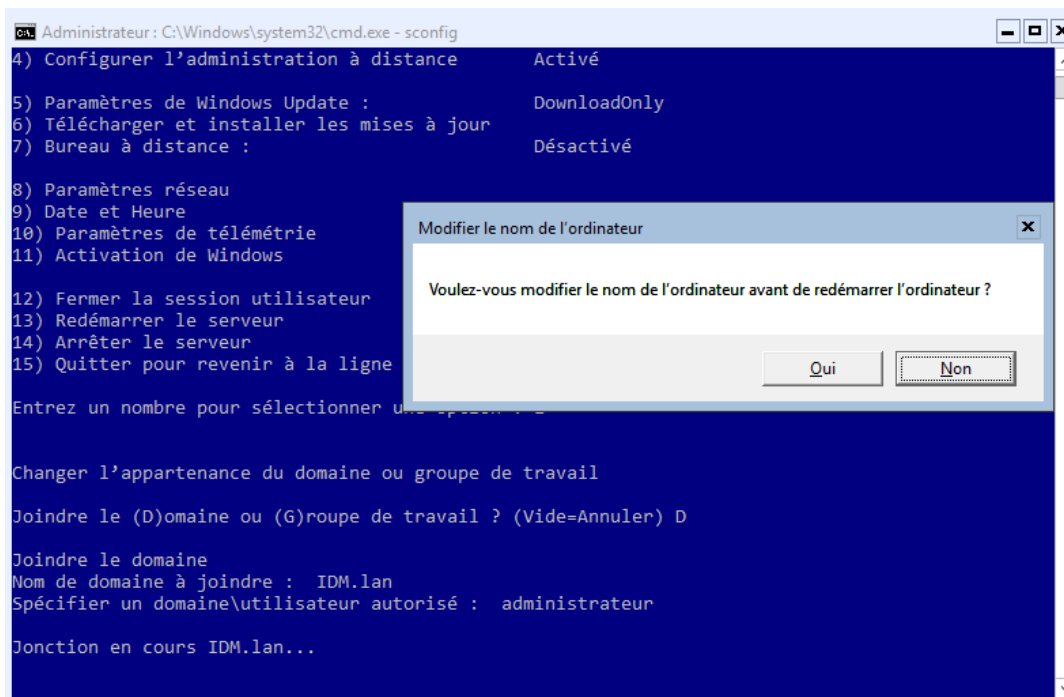
Entrez un nombre pour sélectionner une option : 1

Changer l'appartenance du domaine ou groupe de travail
Joindre le (D)omaine ou (G)roupe de travail ? (Vide=Annuler) D

Joindre le domaine
Nom de domaine à joindre : IDM.lan
Spécifier un domaine\utilisateur autorisé : administrateur

Jonction en cours IDM.lan...
  
```


Une fois que le serveur est dans le domaine. L'ordinateur va nous demander de changer le nom du poste avant de redémarrer. Il nous suffit de mettre « non » et de valider le redémarrage par « Oui ».

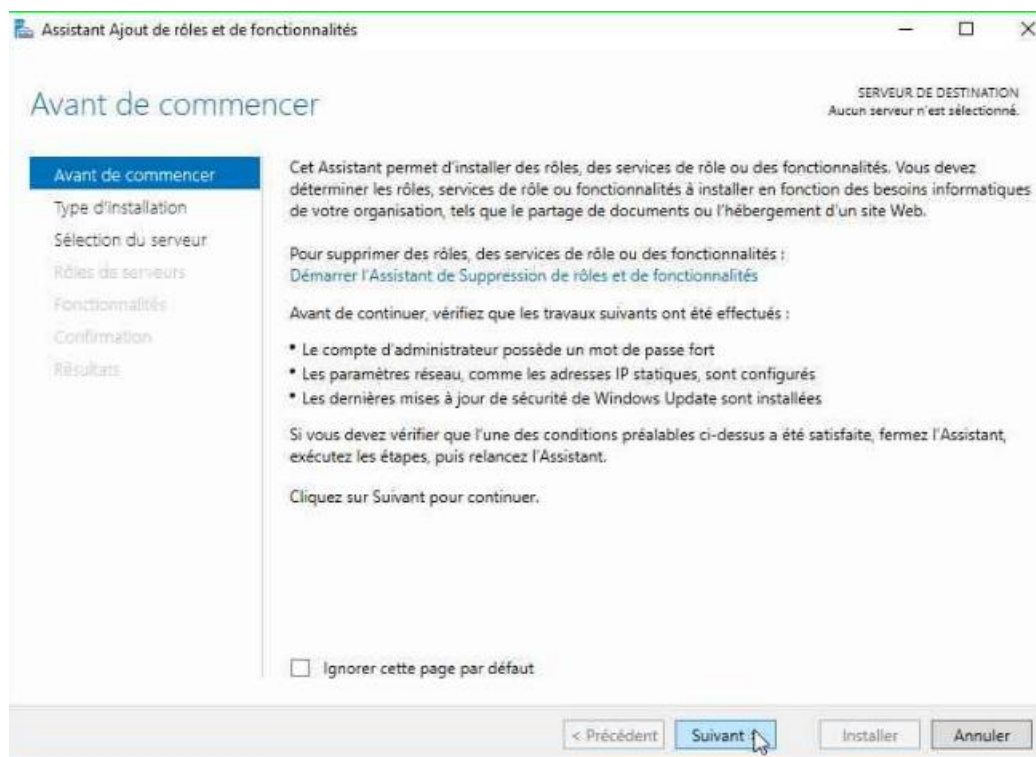
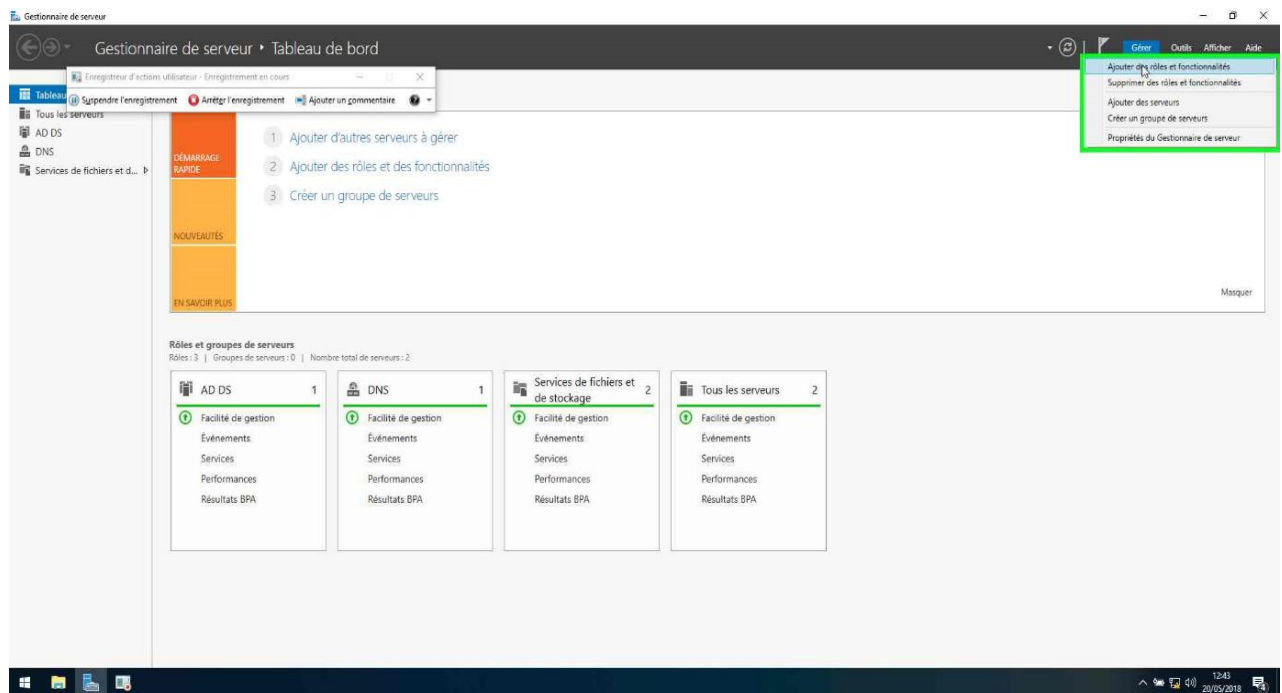


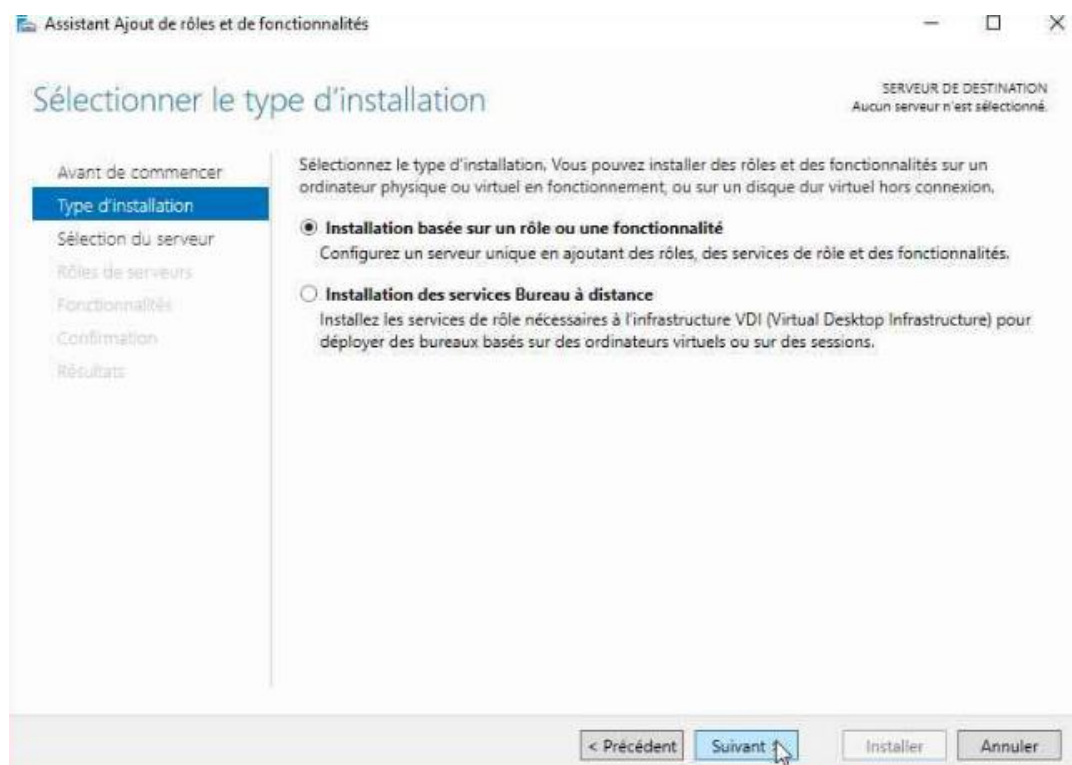
Maintenant nous allons créer le rôle AD-DS et DNS en mode réplication, pour pouvoir procéder à cela il faut :

- Avoir ajouté 3 Disques durs de 4Go chacun et les avoirs initialisé (même procédure que pour le DC1).

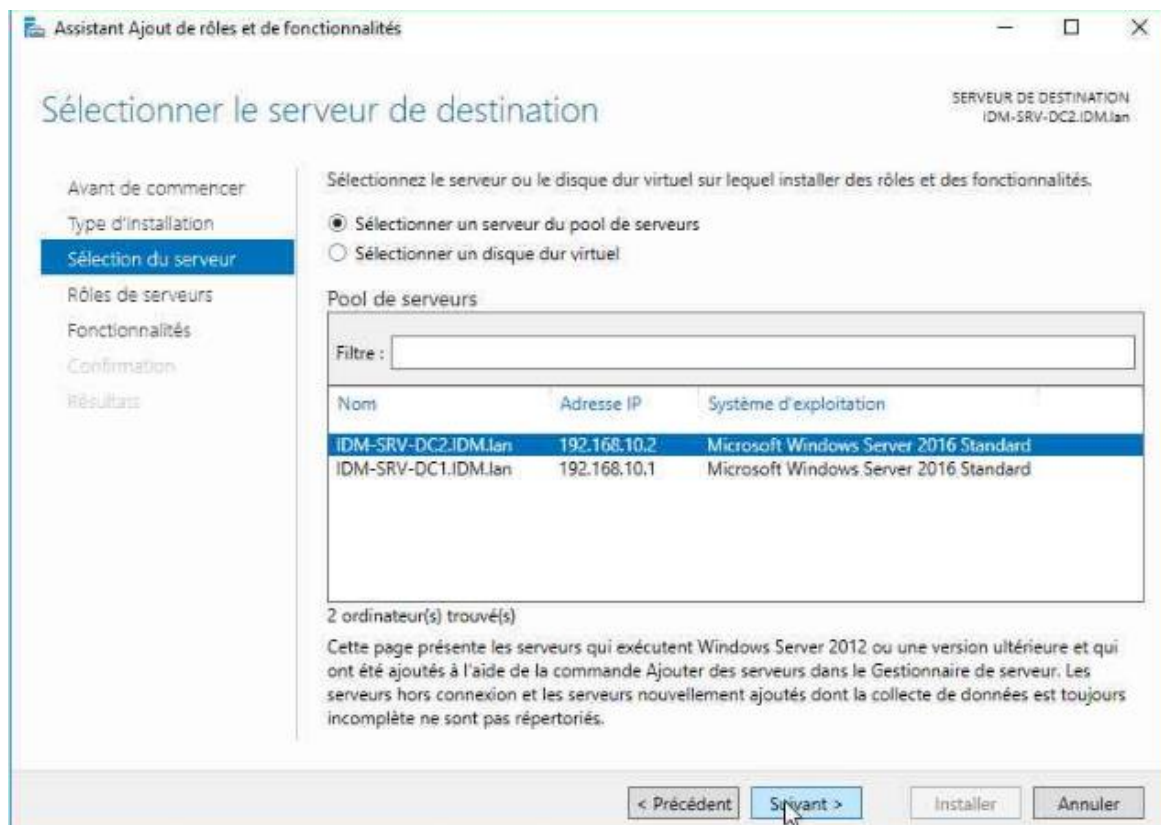
Pour pouvoir créer un serveur de réplication nous allons le faire de façon graphique en utilisant l'outil RSAT. Il faut juste ajouter le DC2 sur le « Server Manager » du client RSAT.

A présent nous allons installer les rôles en suivant les captures suivantes :

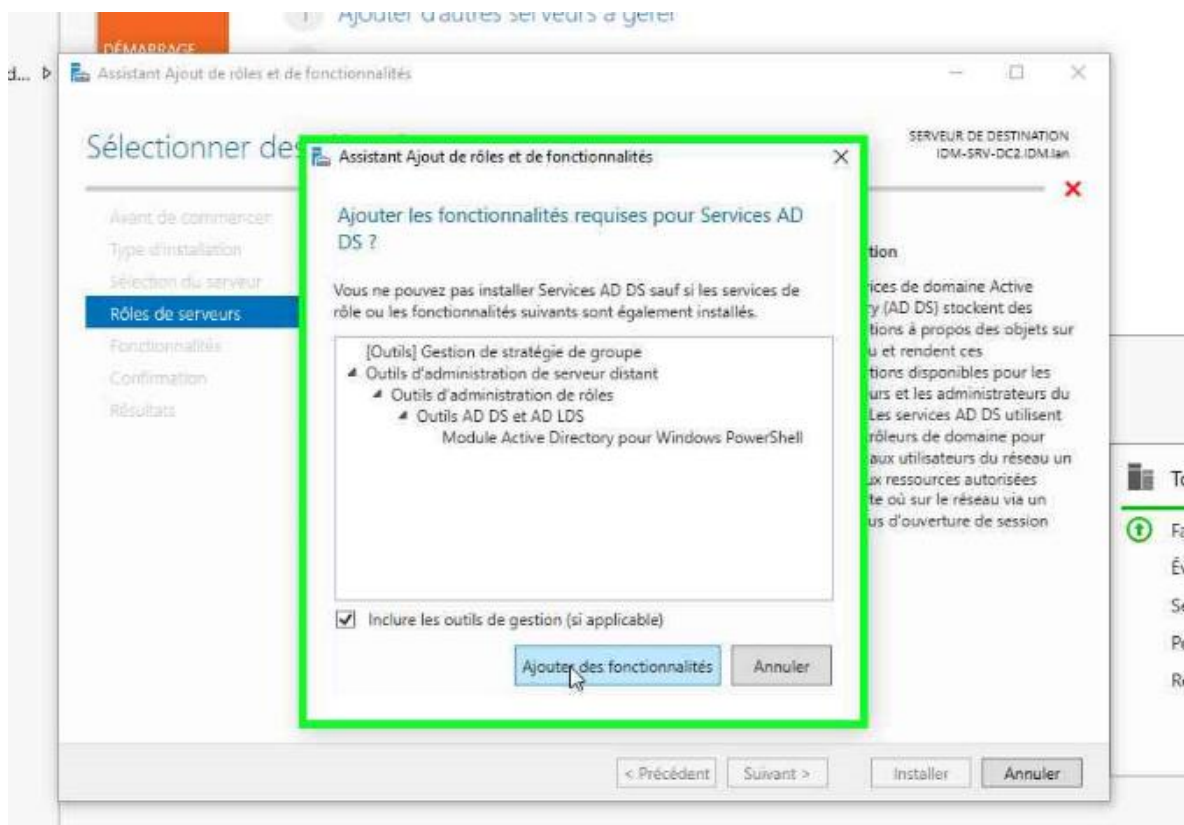
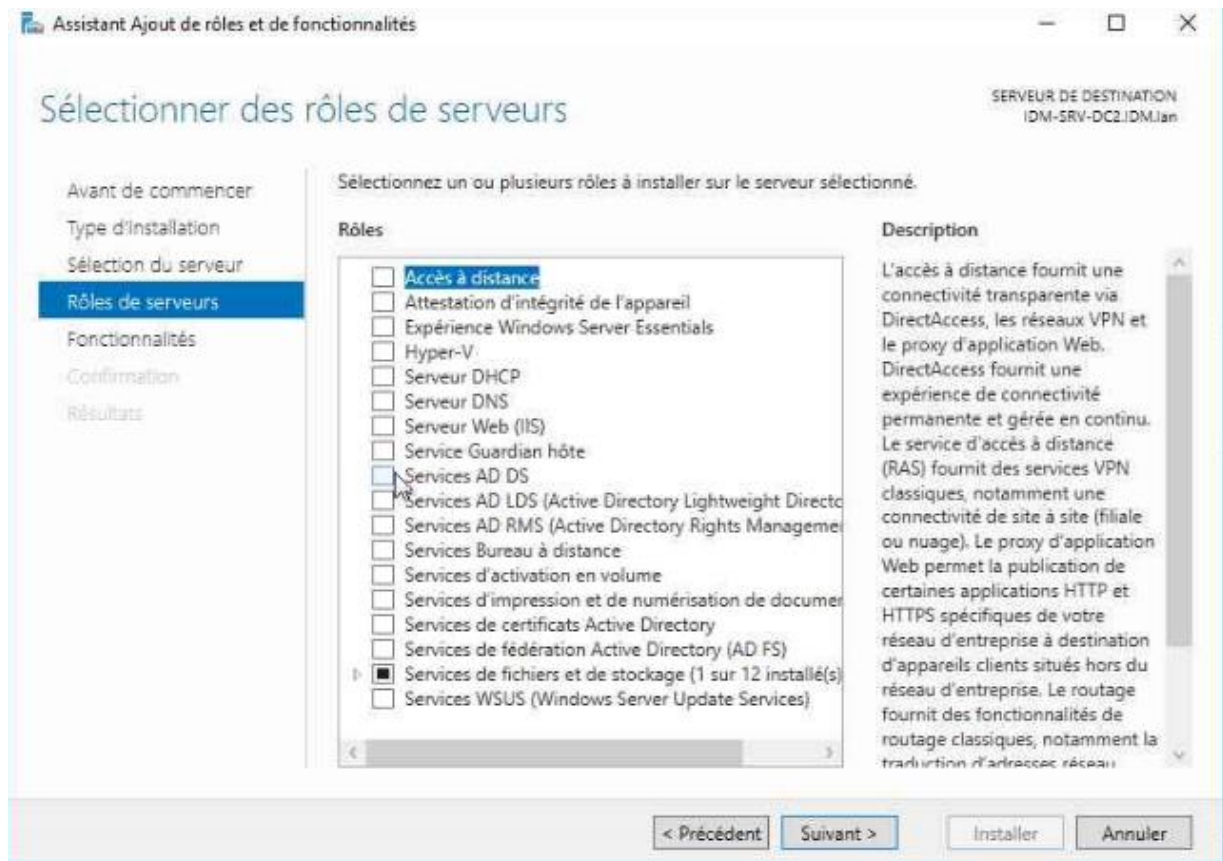




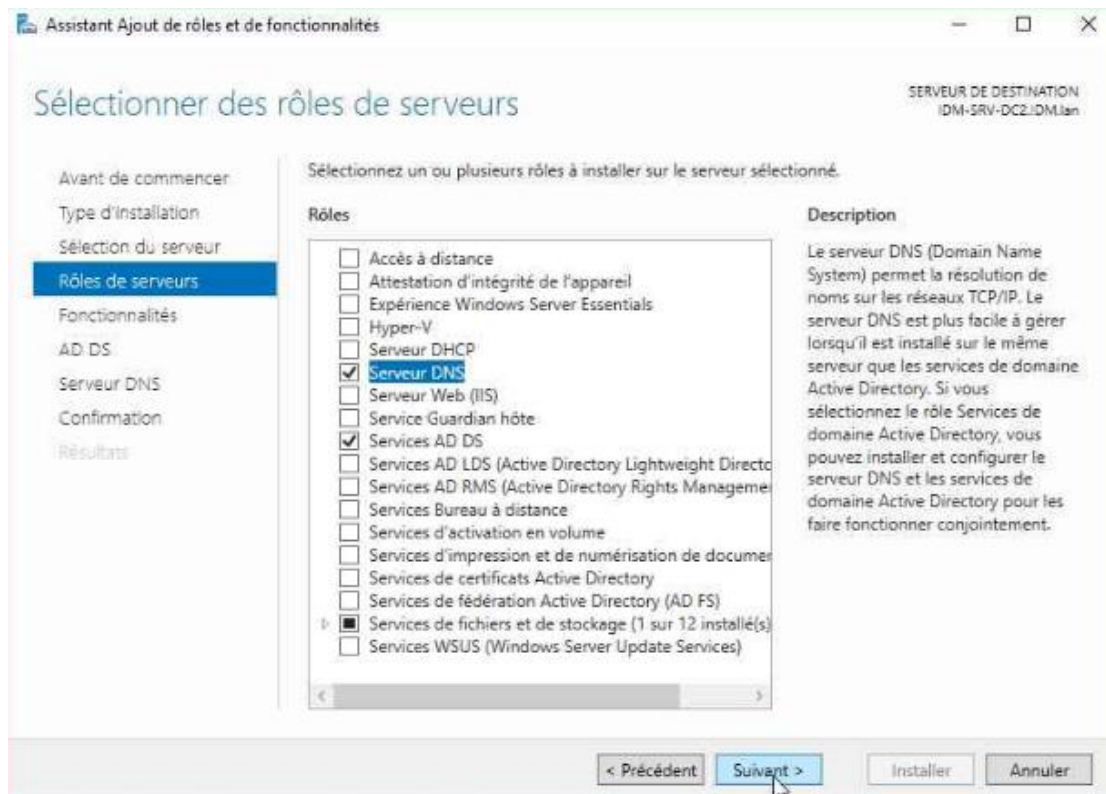
A cette étape l'assistant nous demande sur quel serveur installer les rôles. Nous sélectionnons le DC2.



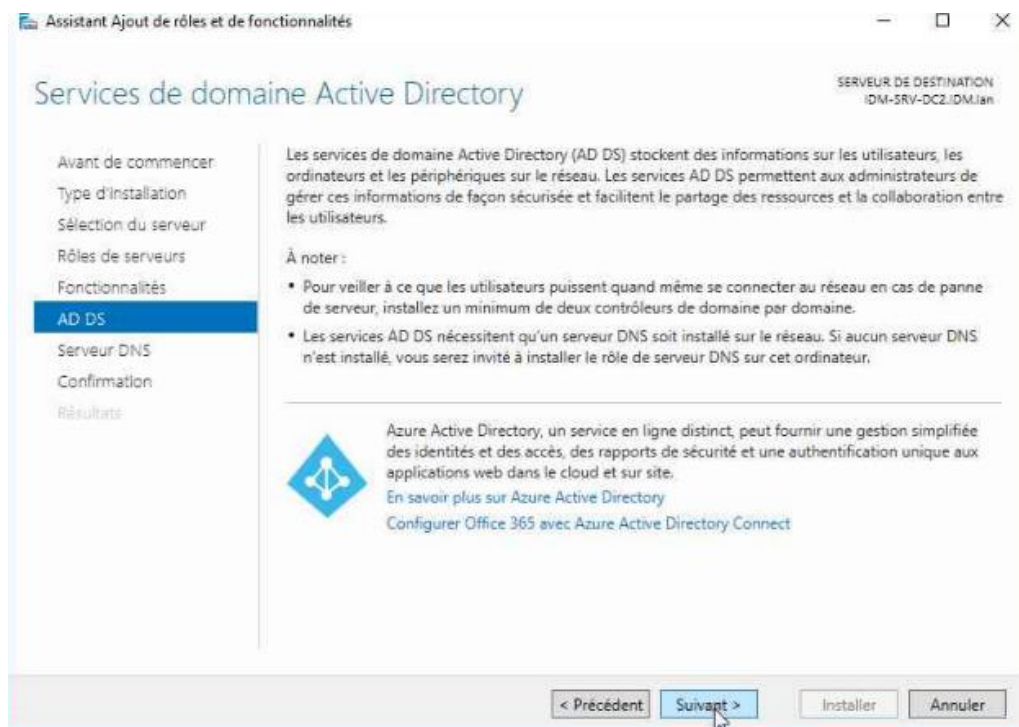
Maintenant nous allons sélectionner les rôles à ajouter nous sélectionnons donc AD-DS.



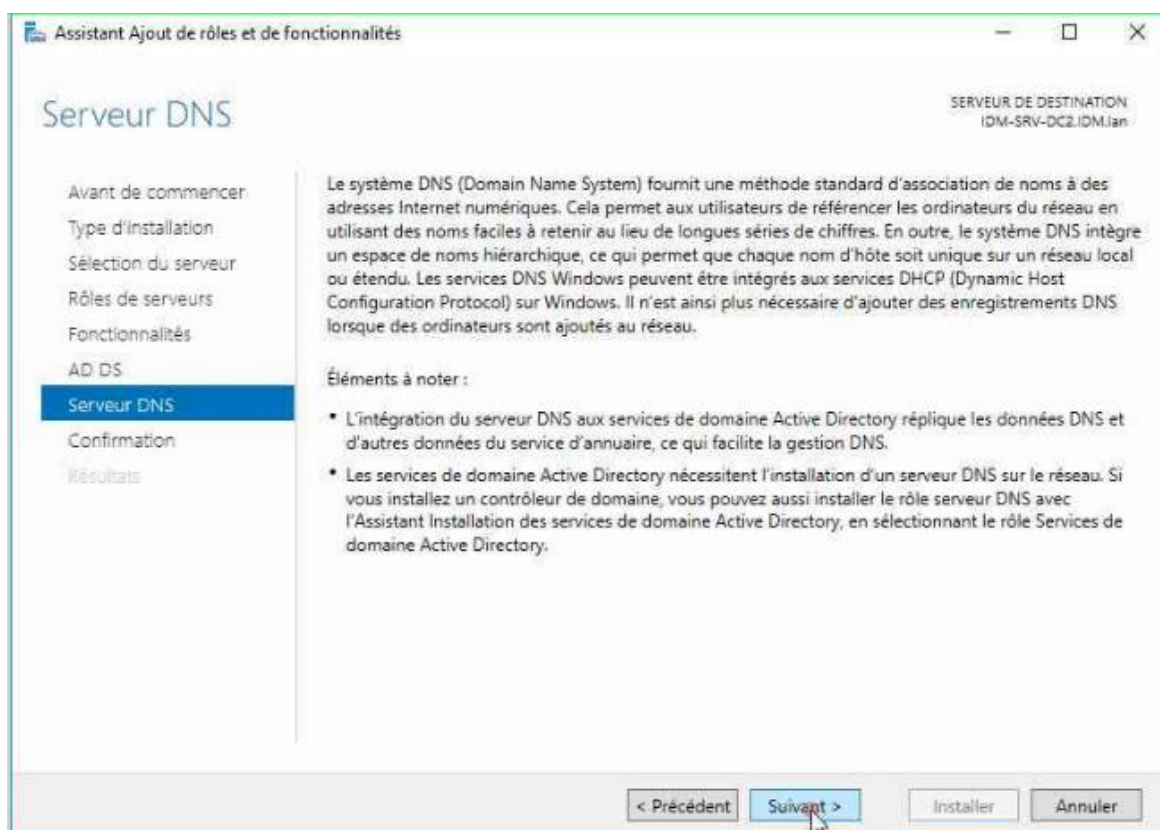
Et le rôle DNS et validons avec « Suivant ».



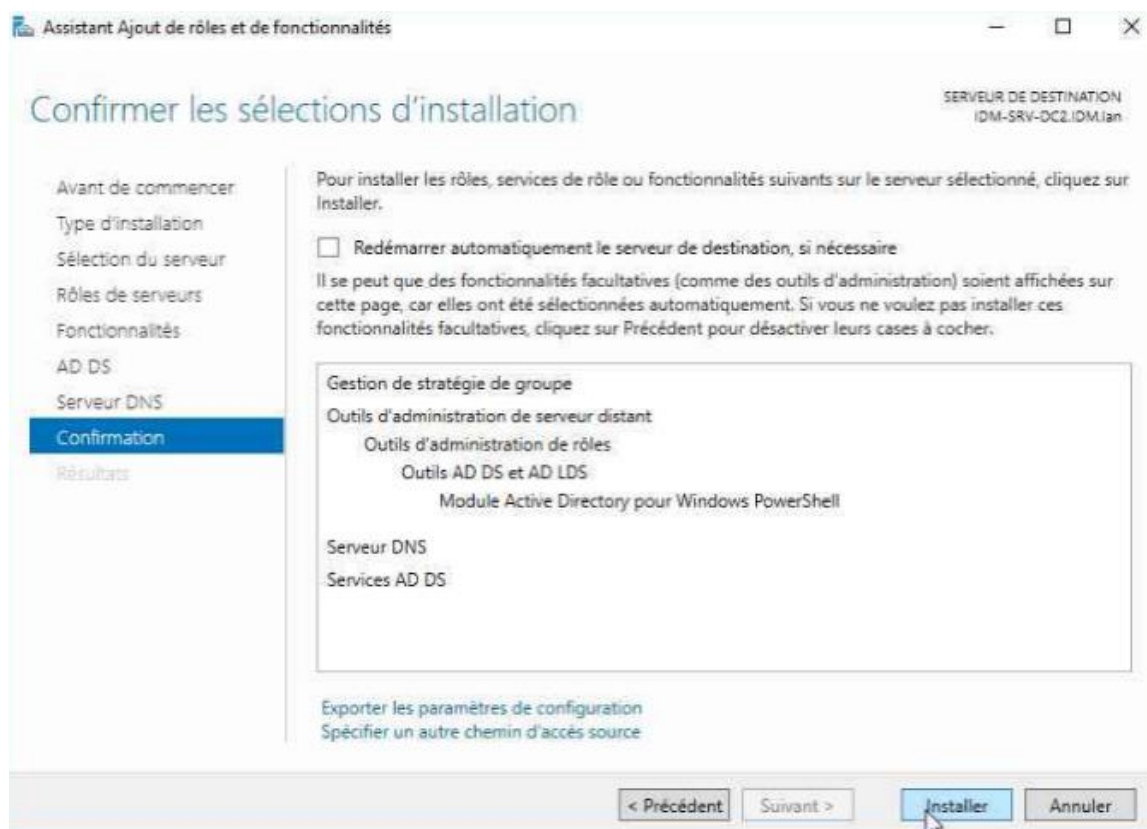
Cet écran nous explique le rôle et les fonctions d'un Active Directory



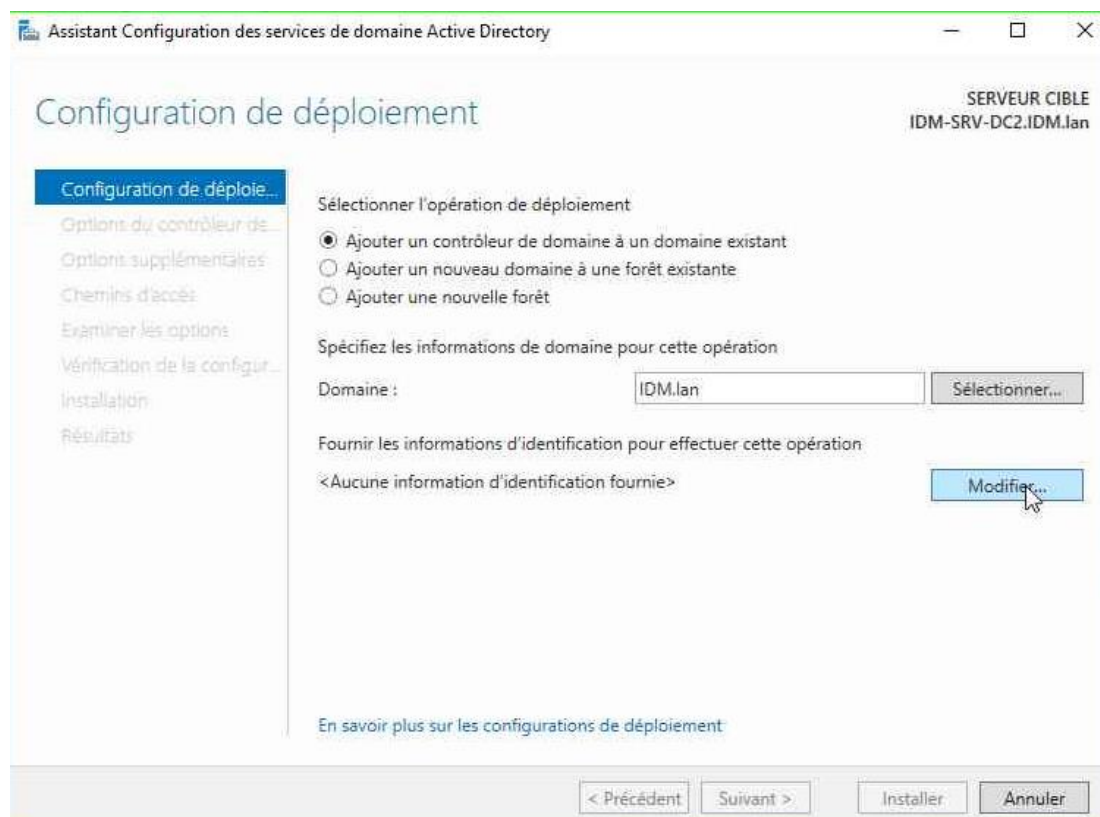
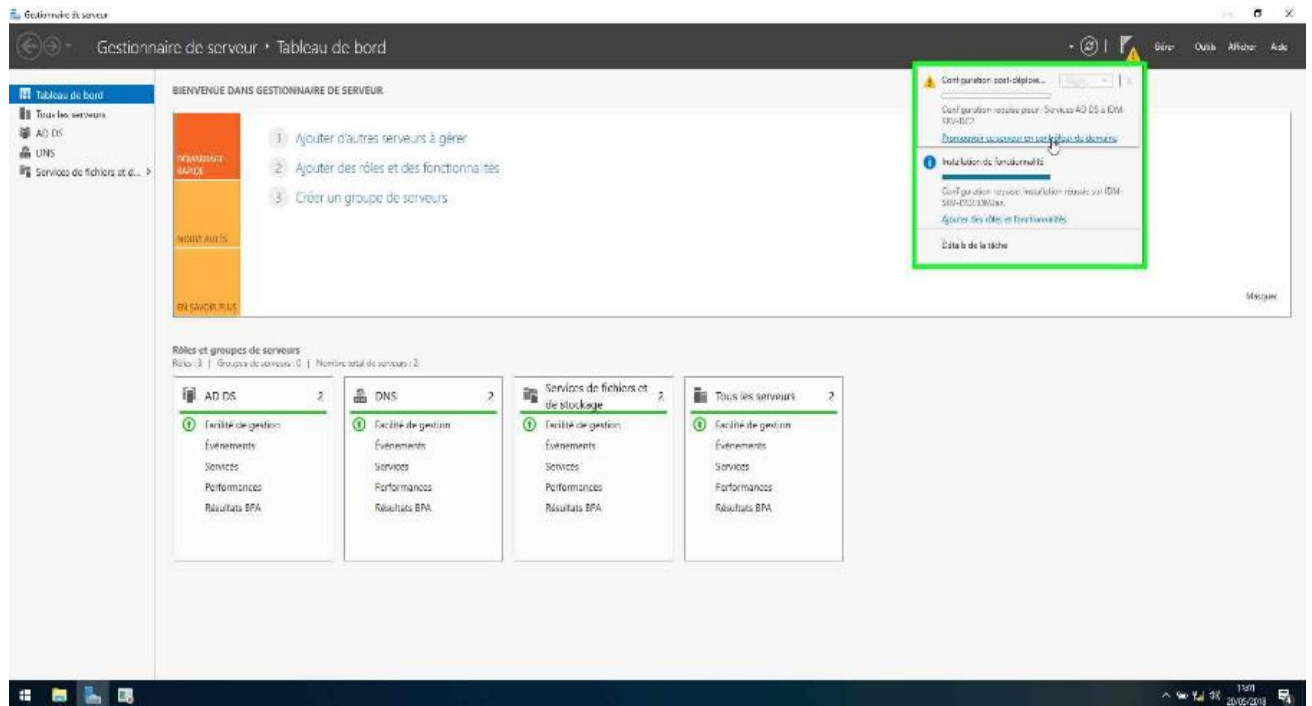
Cet écran nous explique le rôle et les fonctions d'un DNS.



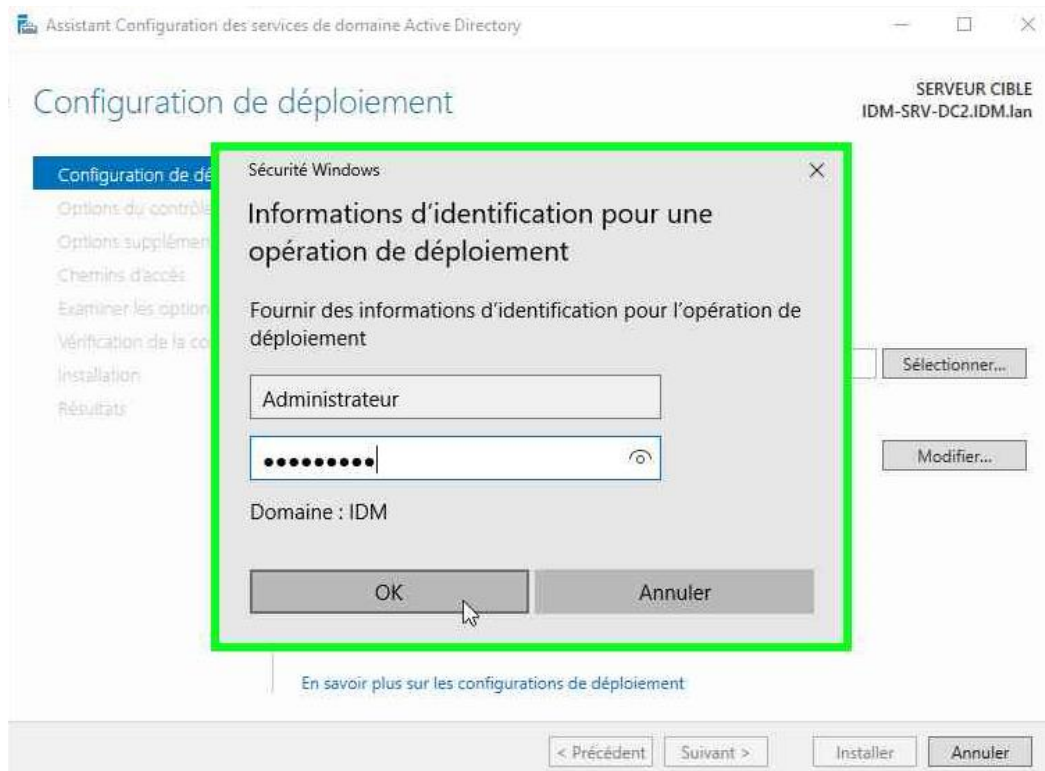
Et nous pouvons valider l'installation.



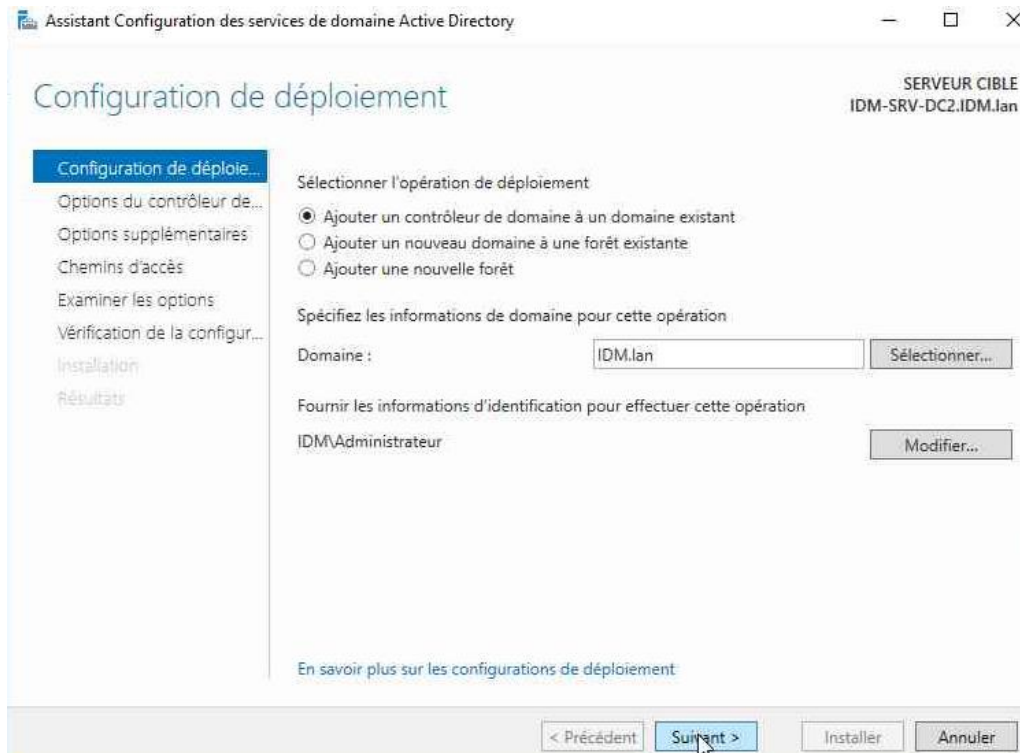
A présent nous allons paramétrer la réplication. Pour cela il suffit de suivre les étapes suivantes :



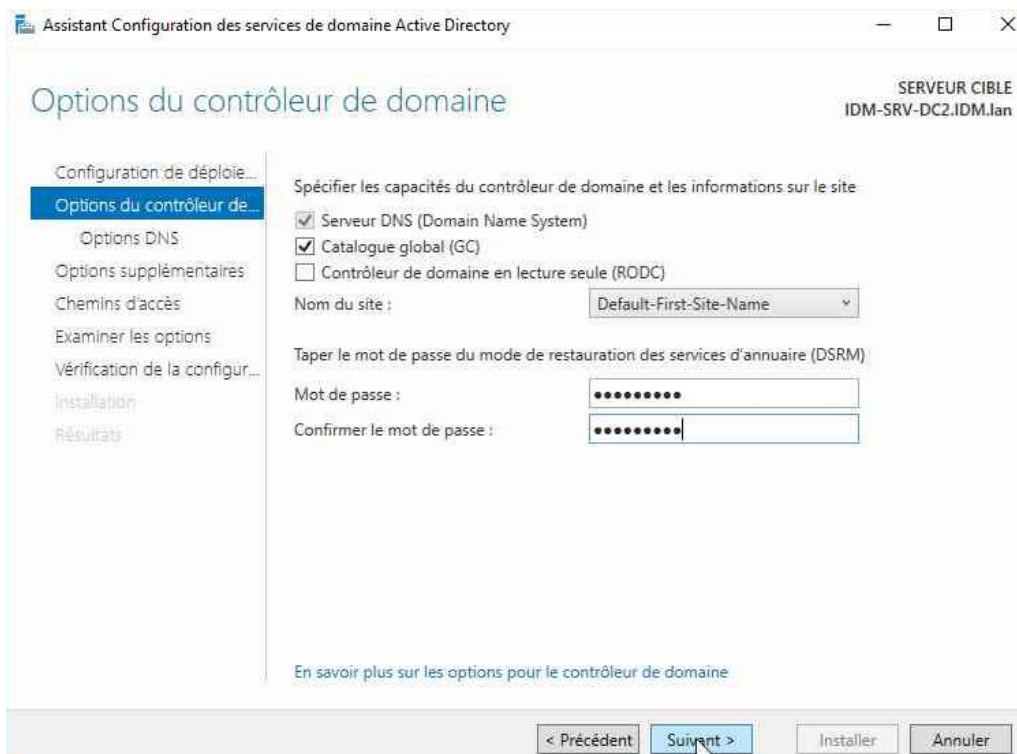
A ce moment il faut renseigner le mot passe Administrateur de l'AD à répliquer.



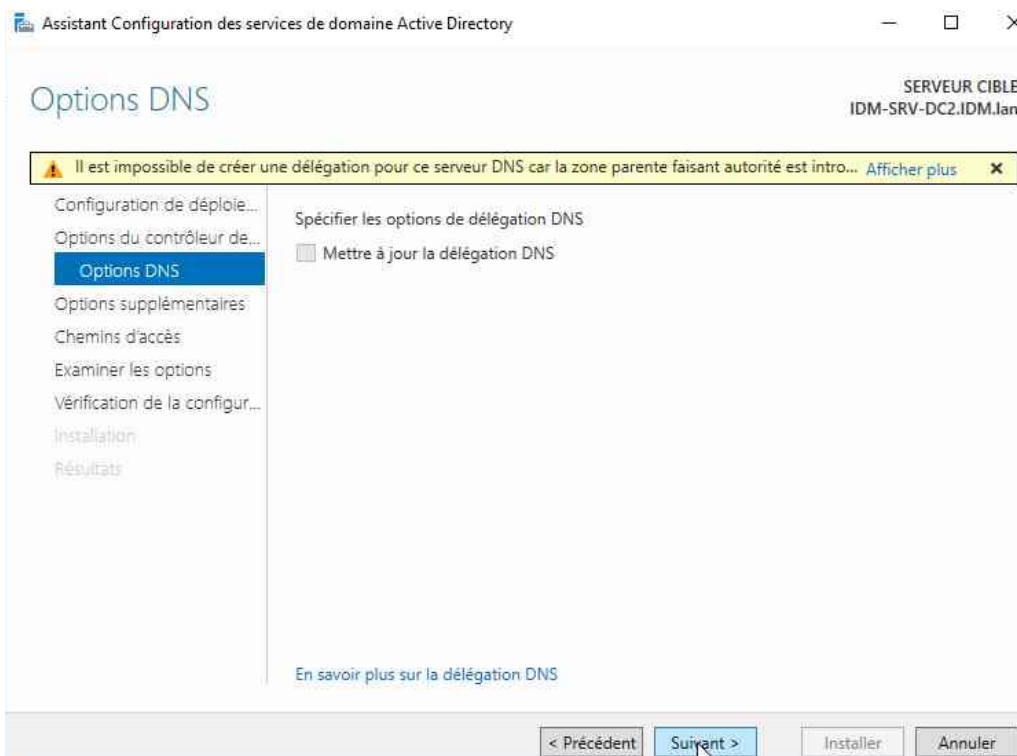
Puis de cliquer sur « Suivant »



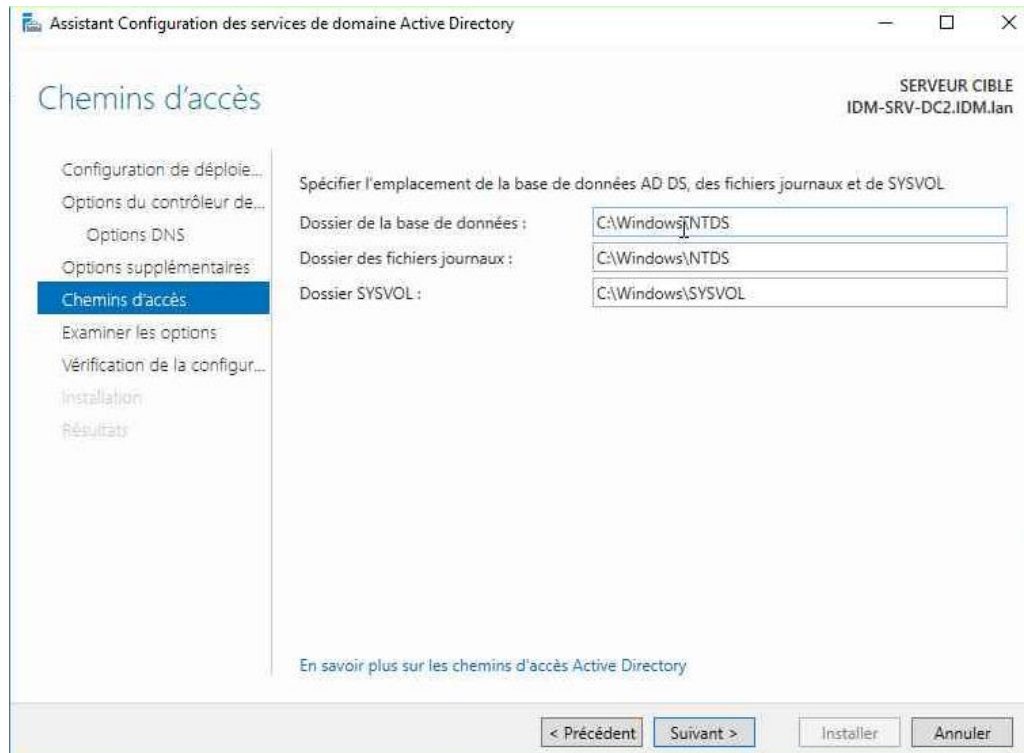
A présent renseignez le mot de passe de restauration de L'AD créée lors de la mise en service sur le DC1.



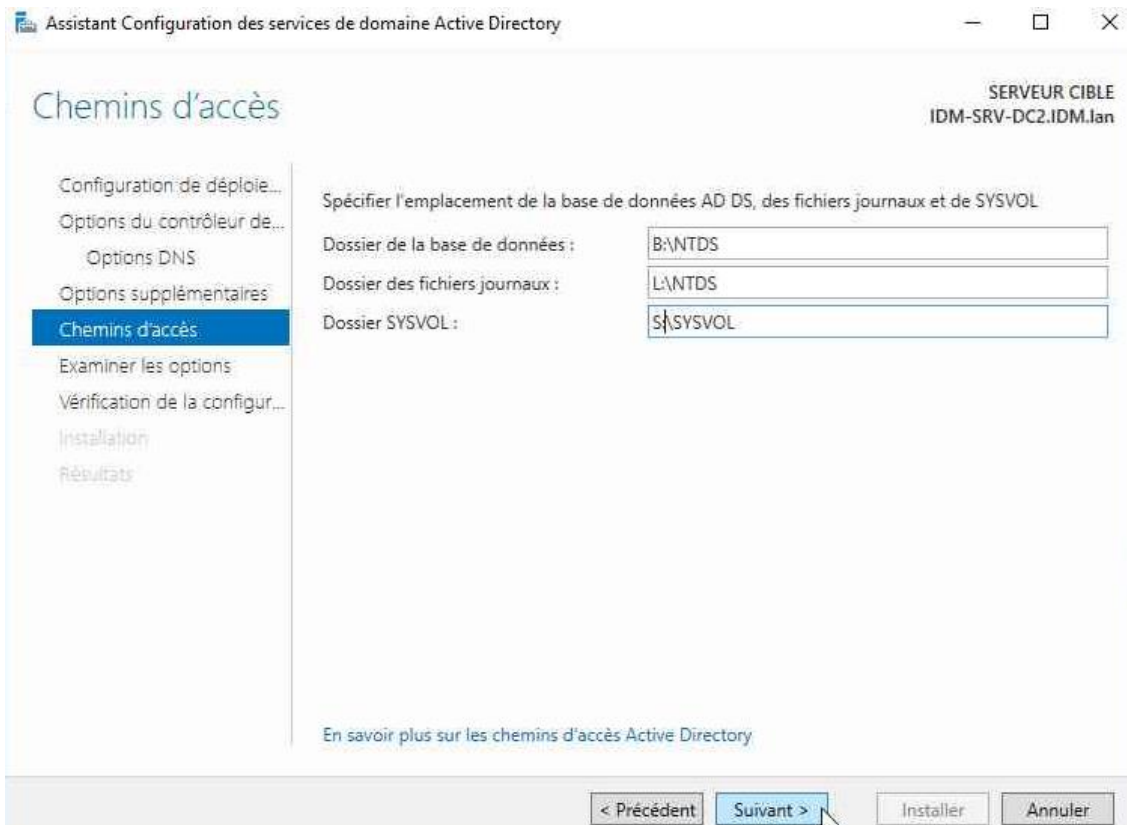
L'assistant nous informe que déjà un DNS est en service et qu'il n'est pas possible de créer un second.



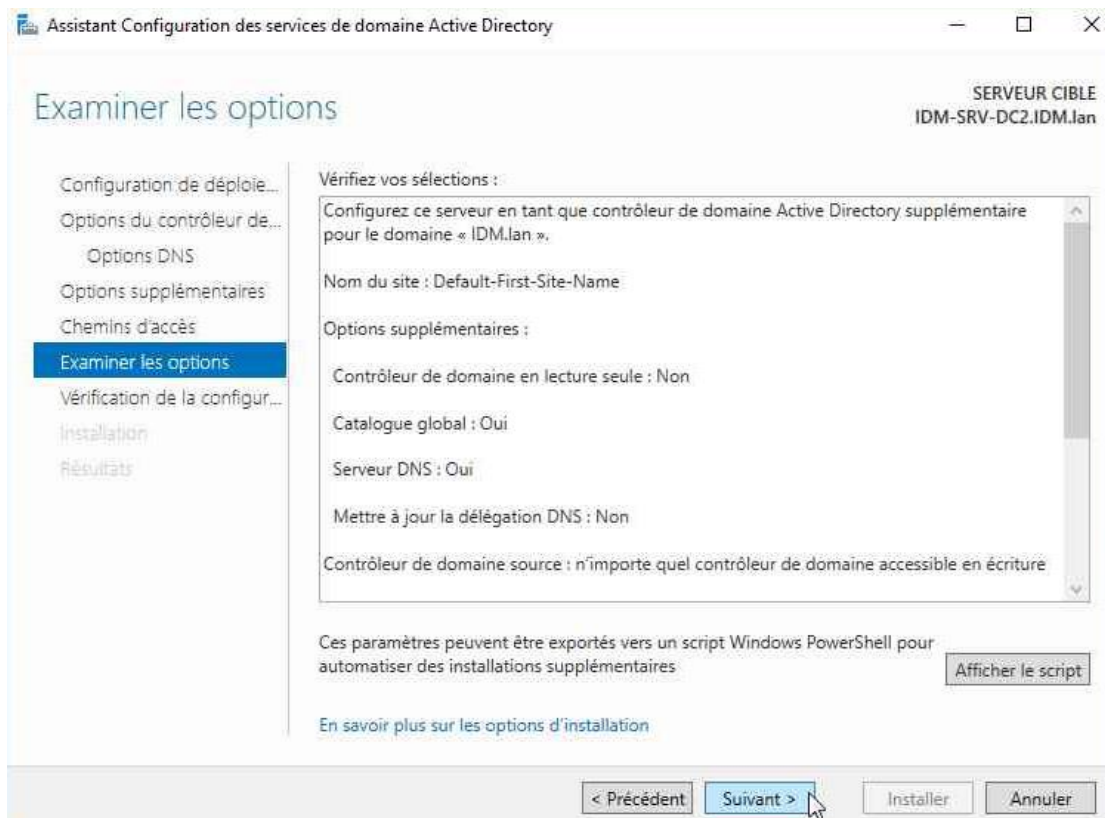
L'étape des chemins et très important il faut remplacer les chemins par les disques créés précédemment :



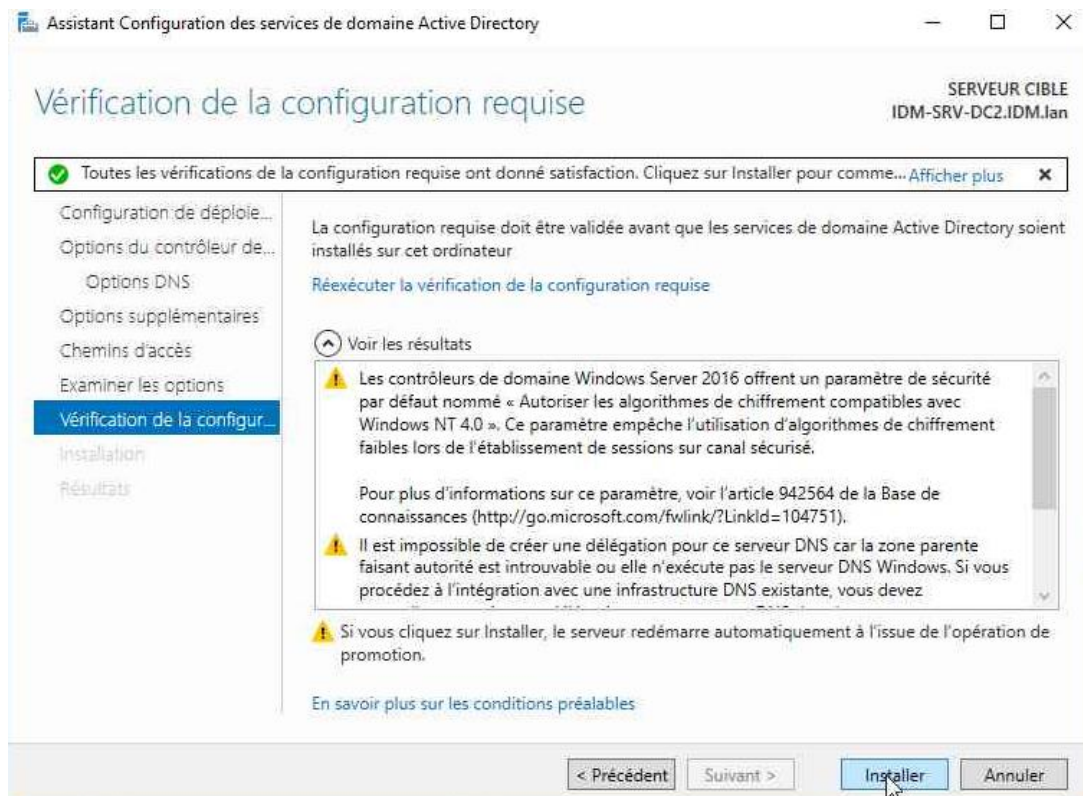
Cela doit donner :



Ceci est un résumé du paramétrage si tout semble correct, validez.



Puis lancez l'installation

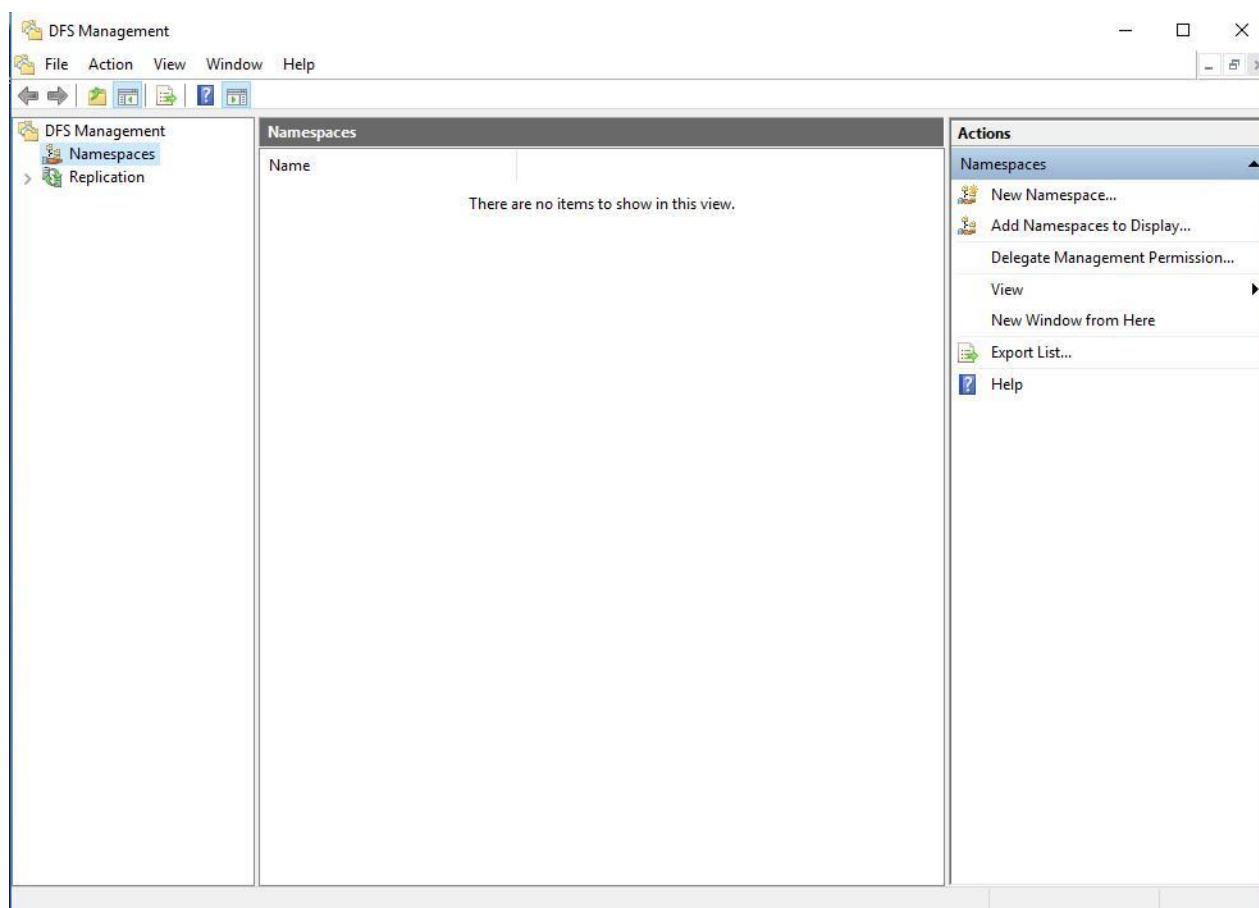


INSTALLATION DU ROLE DFS

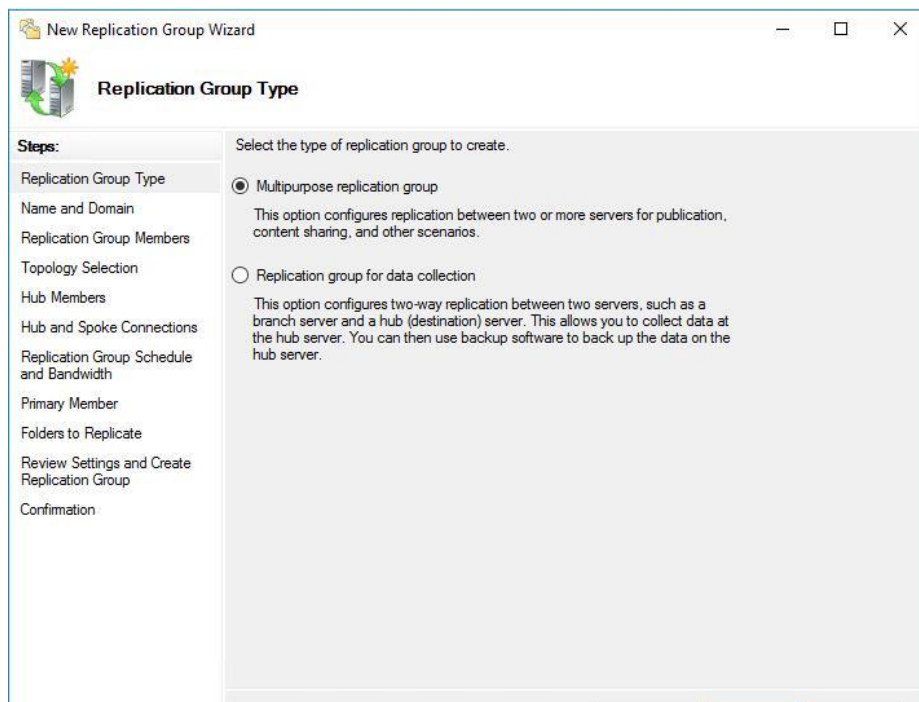
Pour cela lorsque votre serveur manager est lancé, cliquez sur « Manage » puis « Add roles and features ». Lorsque que vous arriverez dans la partie « server role », dérouler l'onglet « file and Storage » puis « File and ISCI services », puis cochez les cases suivantes : « DFS réplication », « DFS namespaces » puis « data deduplication ». Une fois cela fait, continuez de cliquer sur « next » jusqu'à l'installation du rôle.

Configuration de DFS

Sur un des serveurs où vous avez installé le rôle. Revenez sur le server manager, puis cliquez sur Tools et DFS management. Vous devriez tomber sur une interface comme ceci :

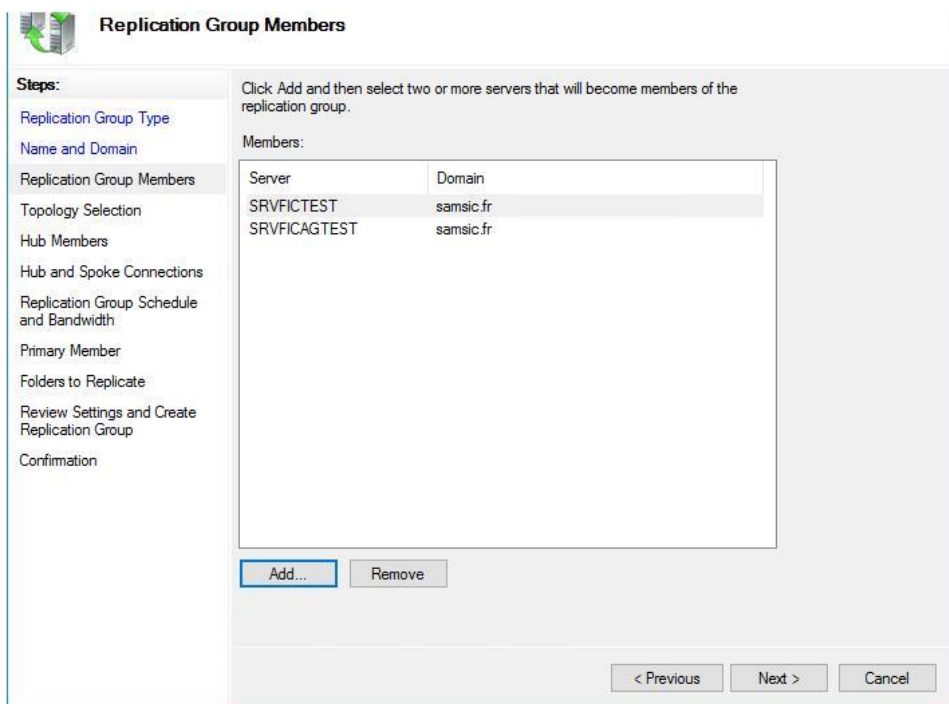


Ensuite, allez dans la partie réplication, faites un clic droit sur réplication puis sur new replication group. Cette interface va apparaître :



Laissez le choix par défaut puis cliquez sur next. Ensuite, renseignez un nom pour le groupe de réplication puis cliquez sur Next.

Ajoutez les différents serveurs qui vont devenir membre du groupe de réplication.



Pour la topologie du type de connections pour les membres du groupe de réplication laissez par défaut en full mesh.

Ensuite, il s'agit de déterminer si vous voulez une réplication en temps réel de vos données ou bien appliqué un intervalle de réplication en spécifiant des jours spécifiques pour effectuer la réplication où bien un horaire précis. Dans mon cas j'ai laissé la réplication en temps réel.

Dans cette partie, il s'agira de renseigner votre serveur qui contient les données que vous souhaitez répliquer.

Primary Member

Steps:

- Replication Group Type
- Name and Domain
- Replication Group Members
- Topology Selection
- Replication Group Schedule and Bandwidth
- Primary Member**
- Folders to Replicate
- Review Settings and Create Replication Group
- Confirmation

Select the server that contains the content you want to replicate to other members. This server is known as the primary member.

Primary member:
SRVFICAGTEST

i If the folders to be replicated already exist on multiple servers, the folders and files on the primary member will be authoritative during initial replication.

< Previous **Next >** Cancel

Vous devrez également renseigner le path du dossier qui va être répliqué.

Member:
SRVFICAGTEST

Local path of folder to replicate:
C:\commun\RENNES **Browse...**

Example: C:\Documents

Select or type a name to represent this folder on all members of the replication group. This name is known as the replicated folder name.

Use name based on path:
RENNES

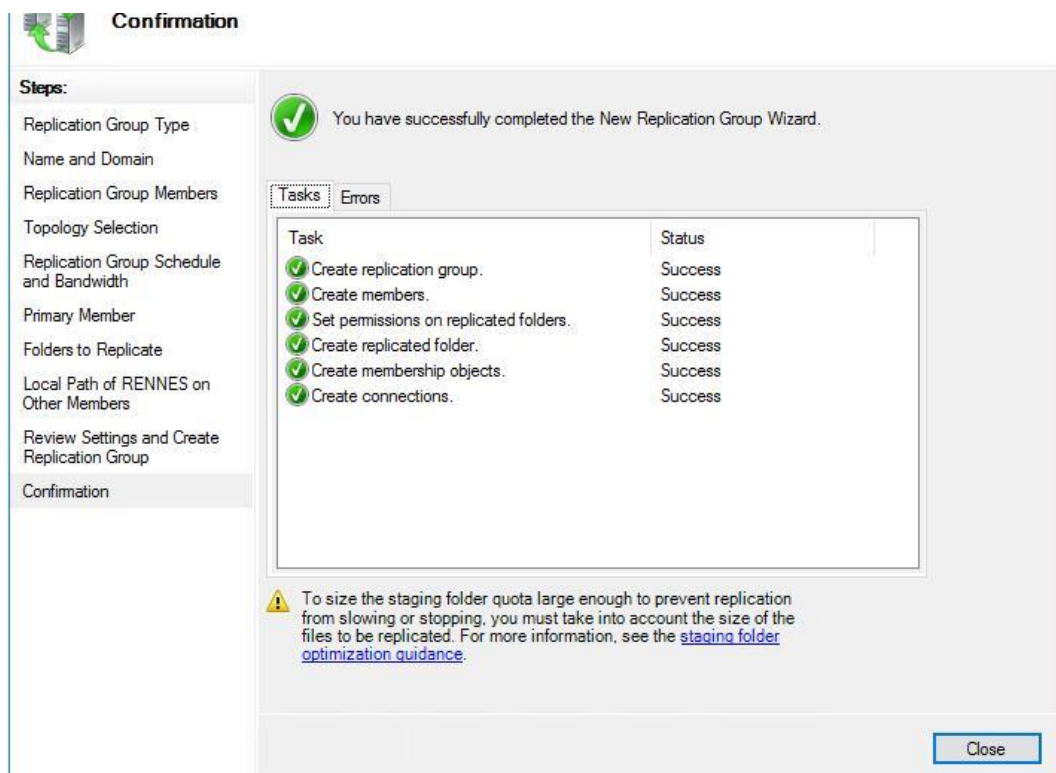
Use custom name:
Example: Documents

Permissions >> OK Cancel

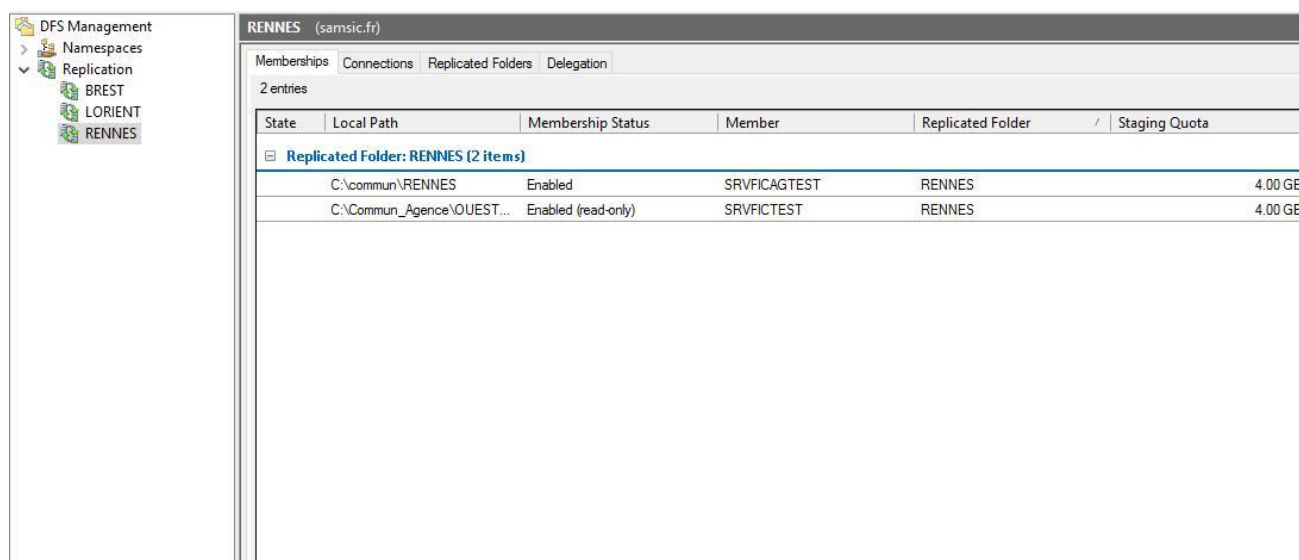
Après avoir cliqué sur next, vous verrez directement l'autre serveur. Faites un double-clic dessus afin d'ouvrir une nouvelle console afin d'éditer les paramètres de celui-ci. Cliquez sur enabled puis renseignez le path du dossier qui sera synchronisé avec l'autre serveur. Cochez la case Make the selected replicated folder on this member read-only, cela empêchera les utilisateurs de supprimer des dossiers, d'ajouter de nouveaux dossiers etc...

Une fois tout ceci fait vous allez donc avoir un review de ce qui va être créé pour votre réplication puis cliquez sur create afin de la mettre en place.

Une fois la création terminée vous devriez obtenir ceci :

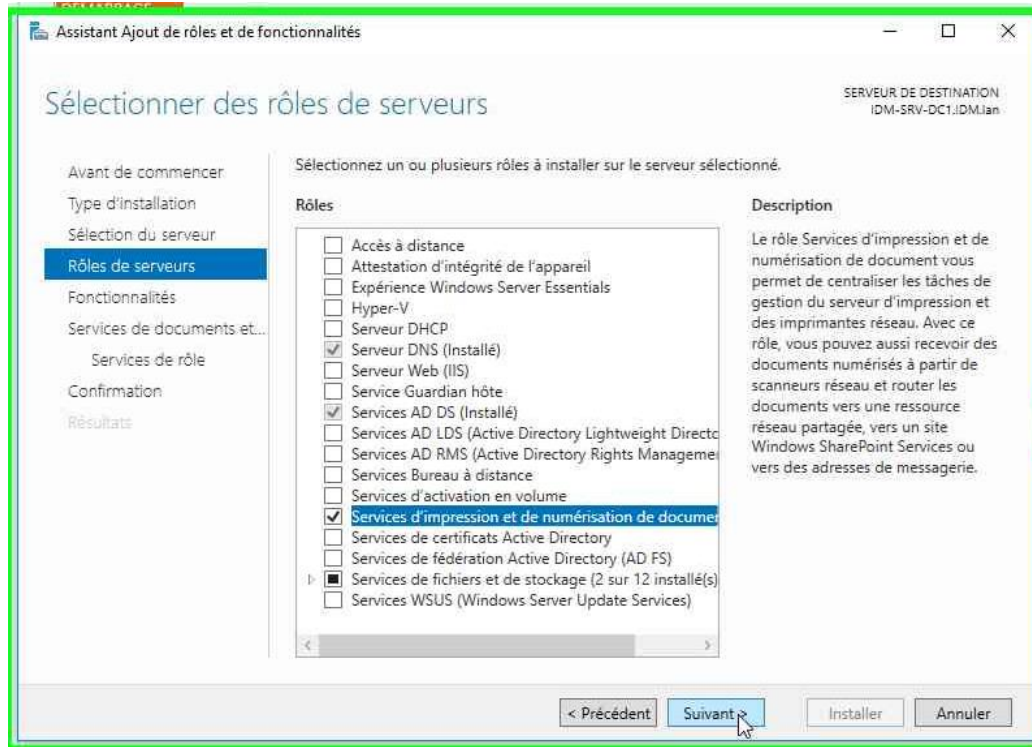


Une fois la création de la réplication terminée vous allez être de retour sur la console DFS avec cette fois-ci dans la partie réplication vous verrez afficher le nom de votre groupe de réplication. Cliquez ensuite sur le nom de votre groupe de réplication dans mon cas il s'agira de Rennes. Dans la partie membership vous retrouvez vos serveurs qui sont membres du groupe de réplication.

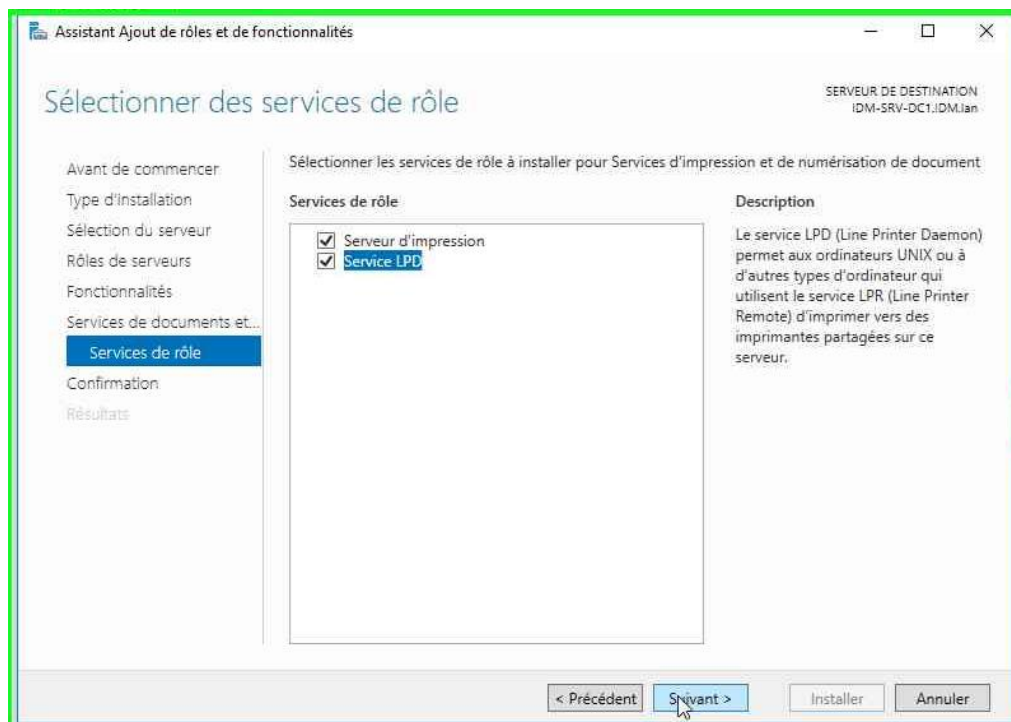


INSTALLATION DU SERVEUR D'IMPRESSION

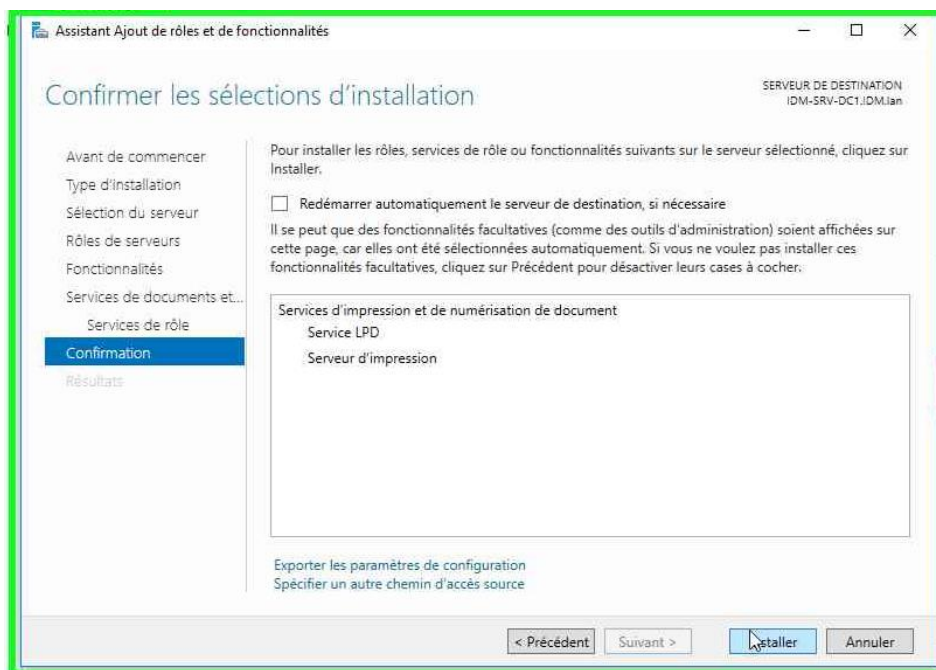
Nous allons à présent installer le rôle « Serveur d'impression ».



Nous allons installer le Service LPD qui permettra aux personnes utilisant Linux d'imprimer.



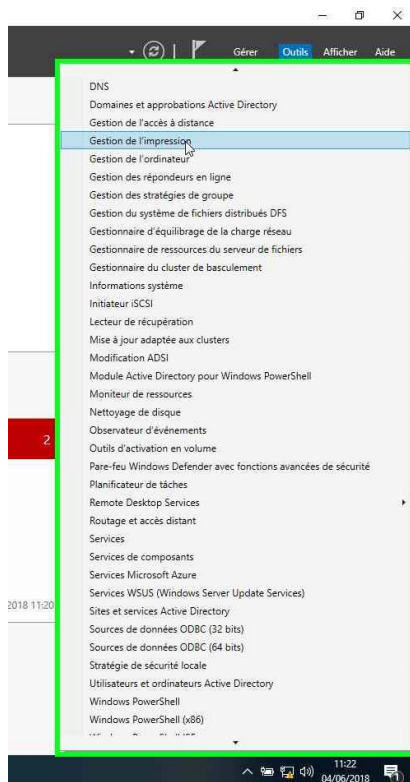
Il nous suffit juste de lancer l'installation



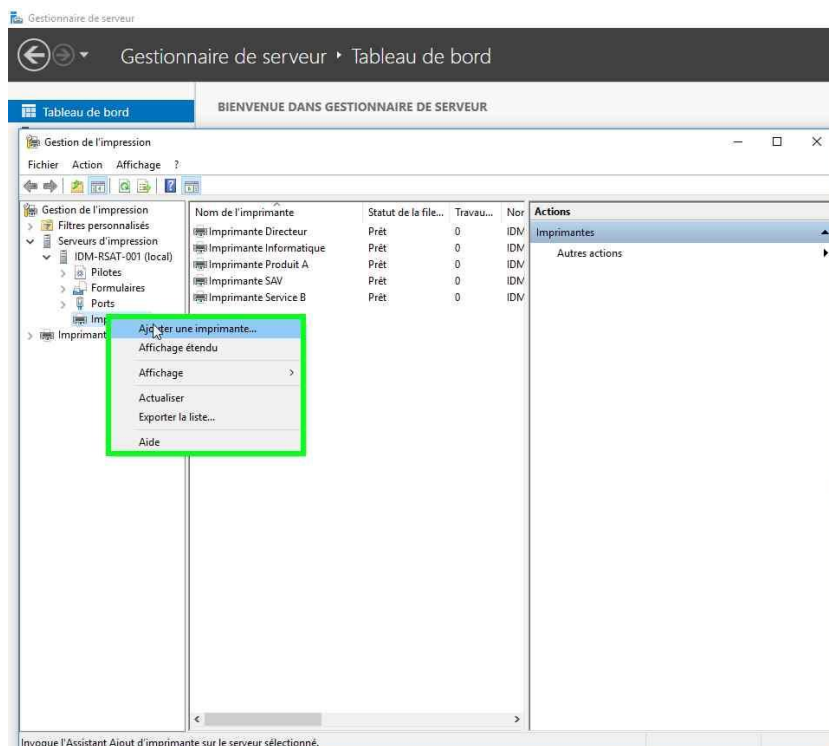
Configuration du serveur d'impression

Nous allons ajouter les imprimantes dans notre serveur

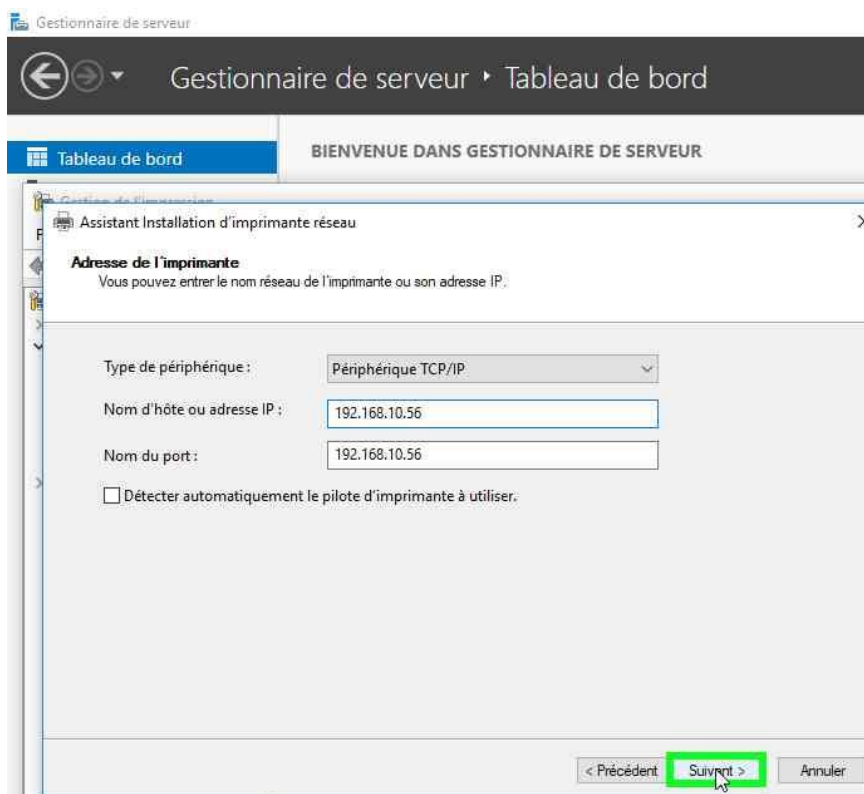
Nous allons dans « Outils » puis Gestion de l'impression



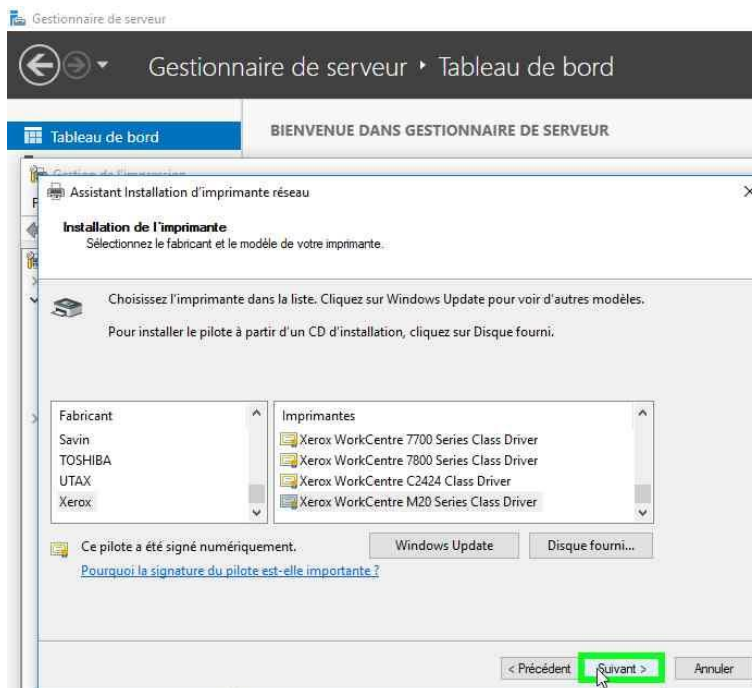
Puis dans notre serveur, sélectionnez imprimante, faites clique droit, puis ajouter une imprimante.



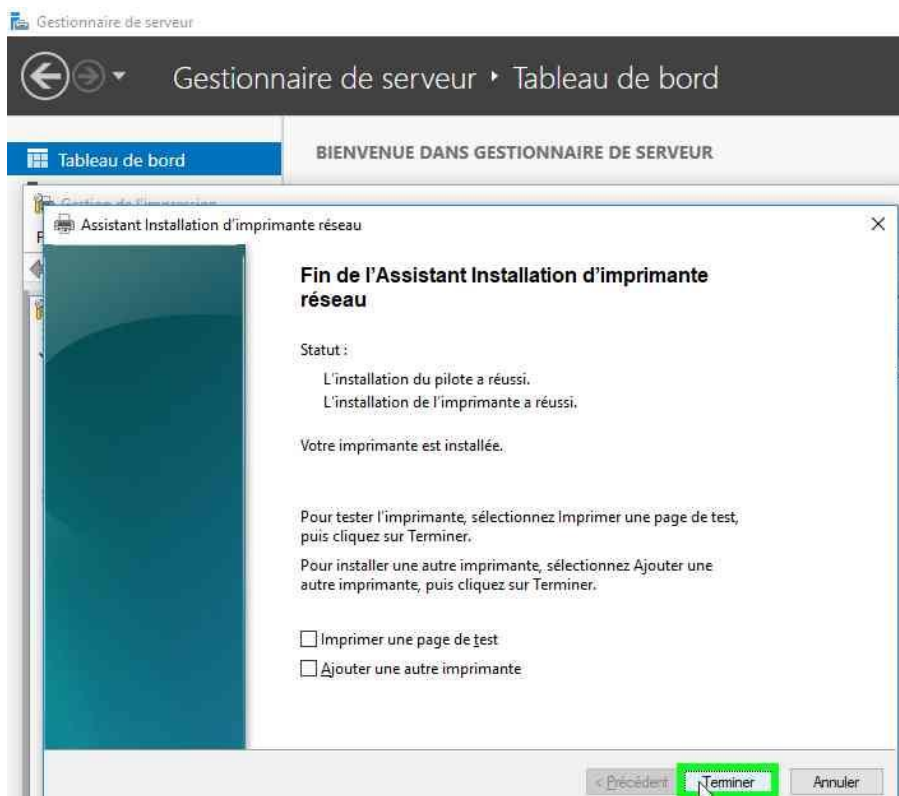
Nous allons sélectionner TCP/IP puis y renseigner l'adresse IP de notre imprimante



L'imprimante a donc été détectée par le serveur, et il suffit de sélectionner le pilote d'impression adapté et valider.



Nommer est validé puis cliquer sur terminer.



SCRIPTS POWERSHELL COMPLETS

Script de la création des objets AD :

```

1  ####
2  Set-ExecutionPolicy unrestricted
3  Import-module ActiveDirectory
4  Import-module GroupPolicy
5
6  ##### CREATION DES VARIABLES GLOBALES #####
7
8
9  $oubase=Read-host " Votre OU de base ? "
10 $NomDomaine=Get-ADDomain |select -ExpandProperty distinguishedname
11 $Schemingroupes="OU=GROUPE,"+$cheminbase
12 $Scheminimps="OU=IMPRIMANTES,"+$cheminbase
13 $Scheminusers="OU=UTILISATEURS,"+$cheminbase
14 $Scheminordis="OU=ORDINATEURS,"+$cheminbase
15 $dfspath=(get-dfsroot).path
16 $Dossierperso=$dfspath+"\Perso\"
17 $Dossiersevice=$dfspath+"\Service\"
18
19
20 try {
21     New-ADOrganizationalUnit -name $oubase `
22         -path $NomDomaine `
23         -ProtectedFromAccidentalDeletion $false `
24         -Verbose `
25     } catch {}
26
27     $csv=Import-csv ".\liste.csv" -delimiter ";" -Encoding UTF8
28     $cheminbase= "OU="+$oubase+","+$NomDomaine
29     $Schemingroupes="OU=GROUPES,"+$cheminbase
30     $Scheminimps="OU=IMPRIMANTES,"+$cheminbase
31     $Scheminusers="OU=UTILISATEURS,"+$cheminbase
32     $Scheminordis="OU=ORDINATEURS,"+$cheminbase
33     write-host "C'est ca : "$cheminbase
34
35
36
37

```

```

37
38 #####
39 ##### Menu GENERAL #####
40 #####
41
42 function menu ()
43 {
44     write-host "      Script pour la creation des objets AD      "
45     write-host "*-----*"
46     write-host "      Menu General      "
47     write-host "*-----*"
48     write-host " Choix 1 : Creation d'Unités d'Organisation"
49     write-host " Choix 2 : Creation des Groupes"
50     write-host " Choix 3 : Creation des Users"
51     write-host " Choix 4 : Creation des dossiers"
52     write-host " choix 5 : Creation permissions"
53
54     $choix=Read-Host "Saisissez votre choix"
55     switch ($choix)
56     {
57     1{Creation_OUs;menu}
58     2{Creation_Groupes;menu}
59     3{Creation_Users;menu}
60     4{Creation_dossiers;menu}
61     5{Creation_permissions;menu}
62     0{exit}
63     default {menu}
64
65     }
66 }
67
68 ##### CREATION UNITE ORGANISATION #####
69
70 function Creation_OUs()
71 {
72     New-ADOrganizationalUnit -name "GROUPES" -path $Chemindebase -ProtectedFromAccidentalDeletion $false -verbose `
73
74     New-ADOrganizationalUnit -name "IMPRIMANTES" -path $Chemindebase -ProtectedFromAccidentalDeletion $false -verbose `
75     New-ADOrganizationalUnit -name "ORDINATEURS" -path $Chemindebase -ProtectedFromAccidentalDeletion $false -verbose `
76
77     New-ADOrganizationalUnit -name "UTILISATEURS" -path $Chemindebase -ProtectedFromAccidentalDeletion $false -verbose `
78
79     foreach ($i in $csv)
80     {
81         $ou=$i.service.toupper()
82         New-ADOrganizationalUnit -name $ou -path $chemingroupes -ProtectedFromAccidentalDeletion $false -verbose `
83         New-ADOrganizationalUnit -name $ou -path $cheminimps -ProtectedFromAccidentalDeletion $false -verbose `
84
85         New-ADOrganizationalUnit -name $ou -path $cheminusers -ProtectedFromAccidentalDeletion $false -verbose `
86         New-ADOrganizationalUnit -name $ou -path $cheminordis -ProtectedFromAccidentalDeletion $false -verbose `
87     }
88 }
89

```

```

91 ##### CREATION GROUPES #####
92
93 function Creation_Groupes ()
94 {
95     foreach ($i in $csv)
96     {
97         $service=$i.service.toupper()
98         $GG="GG_"+$service
99         $GU="GU_"+$service
100        $GDL_R="GDL_R_"+$service
101        $GDL_RW="GDL_RW_"+$service
102        $GDL_F="GDL_F_"+$service
103        $chemingroup="OU="+$service+", "+$chemingroupes
104
105        New-ADGroup -Name $GG `
106        -path $chemingroup `
107        -GroupCategory Security `
108        -GroupScop Global -verbose
109
110        New-ADGroup -Name $GU `
111        -path $chemingroup `
112        -GroupCategory Security `
113        -GroupScop universal -verbose
114
115        New-ADGroup -Name $GDL_R `
116        -path $chemingroup `
117        -GroupCategory Security `
118        -GroupScop DomainLocal -verbose
119
120        New-ADGroup -Name $GDL_RW `
121        -path $chemingroup `
122        -GroupCategory Security `
123        -GroupScop DomainLocal -verbose
124
125        New-ADGroup -Name $GDL_F `
126        -path $chemingroup `
127        -GroupCategory Security `
128        -GroupScop DomainLocal -verbose
129
130        Add-ADGroupMember $GU -Members $GG
131        Add-ADGroupMember $GDL_R -Members $GU
132        Add-ADGroupMember $GDL_RW -Members $GU
133        Add-ADGroupMember $GDL_F -Members $GU
134    }
135 }
136
---
```



```

137
138 ##### CREATION UTILISATEURS #####
139
140 function Creation_Users ()
141 {
142     foreach ($i in $csv)
143     {
144         $Nom=$i.nom.Toupper()
145         $Prenom=$i.prenom.substring(0,1).Toupper()+$i.prenom.substring(1).tolower()
146         $NomCompleat=$Nom+" "+$Prenom
147         $Login=$Prenom.toLowerCase()+"."+$Nom.toLowerCase()
148         $Upn=($login+"@"+$env:userdnsdomain).Tolower()
149         $Description=$s.description
150         $Fonction=$i.fonction
151         $Service=$i.service
152         $Chemin="OU="+$Service+", "$cheminusers
153         $Groupe="GG_"+$Service
154         $Pass=convertTo-SecureString("Angouleme1") -AsPlainText -Force
155
156
157         New-ADUser -name $NomCompleat -GivenName $Prenom -Surname $Nom `
158         -DisplayName $NomCompleat `
159         -SamAccountName $Login `
160         -UserPrincipalName $Upn `
161         -Path $Chemin `
162         -Department $Service `
163         -Description $Description `
164         -AccountPassword $Pass `
165         -Title $Fonction `
166         -ChangePasswordAtLogon $true `
167         -Enabled $true `
168         -EmailAddress $Upn
169
170         Add-ADGroupMember $Groupe -Members $Login
171     }
172 }
173
174 }
175
-----

```

```

175 -
176 ##### CREATION DOSSIERS #####
177
178 function Creation_dossiers()
179 {
180
181
182     foreach ($i in $csv)
183     {
184         $Nom=$i.nom.Toupper()
185         $Prenom=$i.prenom.substring(0,1).Toupper()+$i.prenom.substring(1).tolower()
186         $Login=$Prenom.toLowerCase()+"."+$Nom.toLowerCase()
187         $Service=$i.service
188
189         New-item -name $Login -itemtype Directory -path $dossierperso
190
191         try {
192             new-item -name $service -itemtype Directory -path $dossierservice
193         }
194         catch {
195             write-host "Les dossier" + $dossierservice + "existe deja"
196         }
197     }
198 }
199
200 -
201 ##### CREATION PERMISSIONS #####
202
203 function creation_permissions
204 {
205     $listedossierperso=get-childitem -Directory -Path $Dossierperso
206     $listedossierservice=get-childitem -directory -path $Dossierservice
207
208
209     foreach ($dossier in $listedossierperso)
210     {
211         $chemindossier=$dossier.fullname
212         $acl=(get-item $chemindossier).GetAccessControl('Access')
213         $username=$dossier.name
214         $ar=New-Object security.accesscontrol.filesystemaccessrule($username,'modify','containerinherit,objectinherit','none','allow')
215         $acl.SetAccessRule($ar)
216         set-acl -path $chemindossier -aclobject $acl
217     }
218
219
220     foreach ($dossier in $listedossierservice)
221     {
222         $chemindossier=$dossier.fullname
223         $acl=(get-item $chemindossier).GetAccessControl('Access')
224         $username="GDL_RW_"+$dossier.name
225         $ar=New-Object security.accesscontrol.filesystemaccessrule($username,'modify','containerinherit,objectinherit','none','allow')
226         $acl.SetAccessRule($ar)
227         set-acl -path $chemindossier -aclobject $acl
228     }
229 }
230
231 menu

```

Script concernant la connexion aux lecteurs réseau :

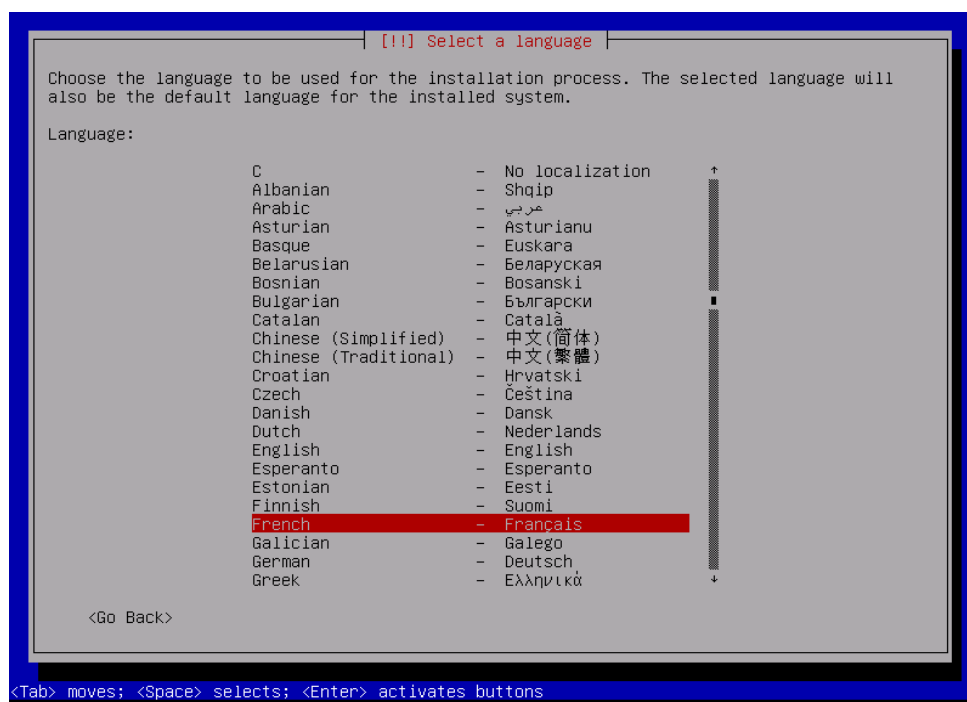
```
1
2
3 $servicepath=(get-dfsroot).path +"\service"
4 New-PSDrive -Name "S" -PSProvider "FileSystem" -Root $servicepath -persist
5
6
7 $persopath=(get-dfsroot).path +"\PERSO\"+$env:USERNAME
8 New-PSDrive -Name "P" -PSProvider "FileSystem" -Root $persopath -persist
9
10
11 $communpath=(get-dfsroot).path +"\commun"
12 New-PSDrive -Name "T" -PSProvider "FileSystem" -Root $communpath -persist
```

INSTALLATION LINUX DEBIAN

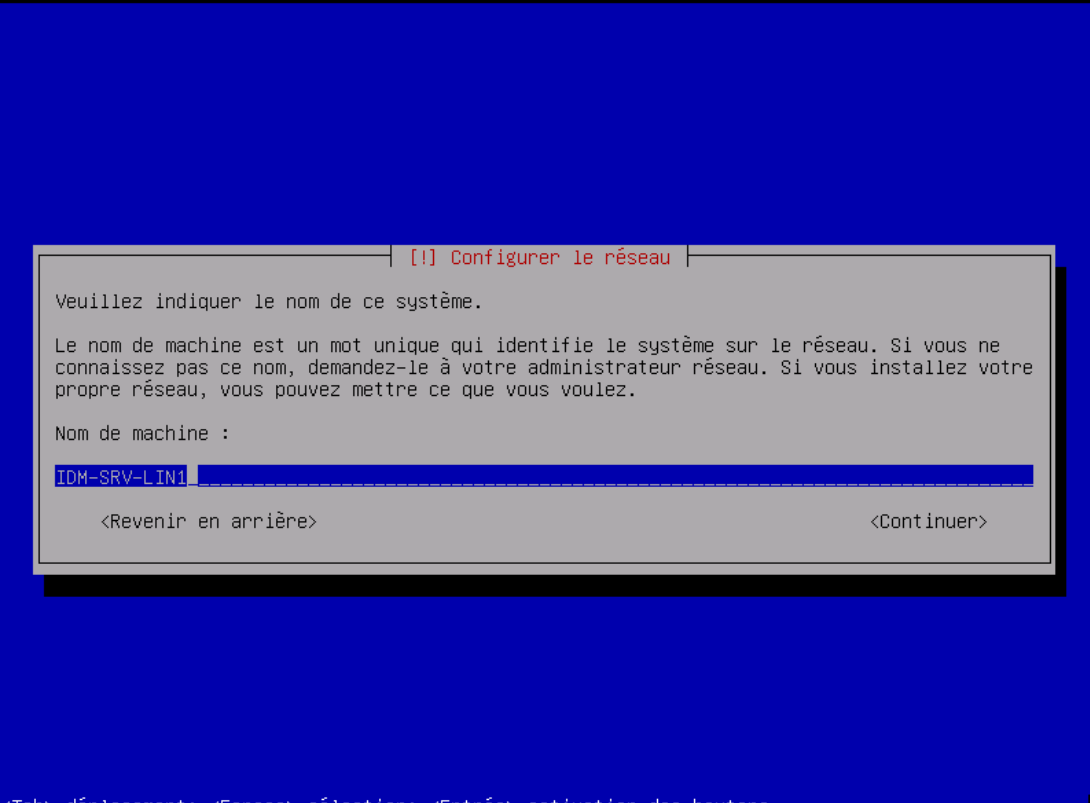
Pour une question de stabilité, de robustesse et de sécurité nous avons fait le choix de la distribution Debian Stretch.
Nous choisissons l'installation minimale pour économiser les ressources du serveur.



Nous choisissons la langue par défaut du système



Nous configurons ensuite le domaine.



[!] Configurer le réseau

Veillez indiquer le nom de ce système.

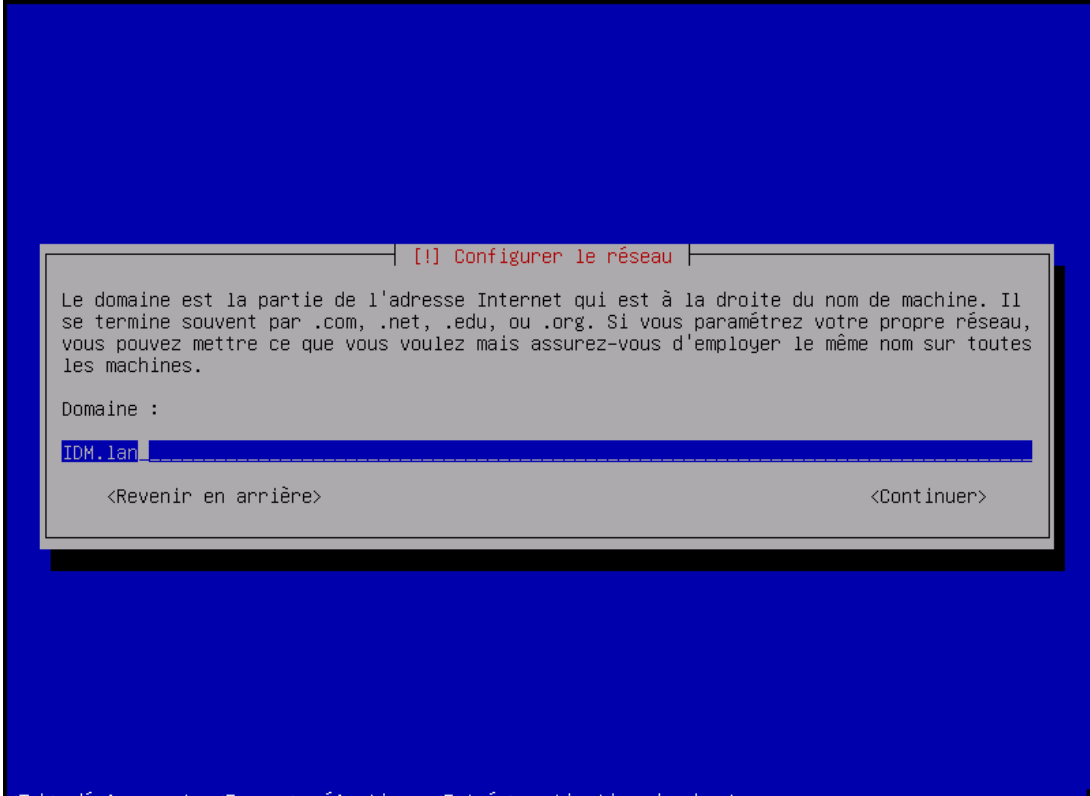
Le nom de machine est un mot unique qui identifie le système sur le réseau. Si vous ne connaissez pas ce nom, demandez-le à votre administrateur réseau. Si vous installez votre propre réseau, vous pouvez mettre ce que vous voulez.

Nom de machine :

IDM-SRV-LIN1

<Revenir en arrière> <Continuer>

<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons



[!] Configurer le réseau

Le domaine est la partie de l'adresse Internet qui est à la droite du nom de machine. Il se termine souvent par .com, .net, .edu, ou .org. Si vous paramétrez votre propre réseau, vous pouvez mettre ce que vous voulez mais assurez-vous d'employer le même nom sur toutes les machines.

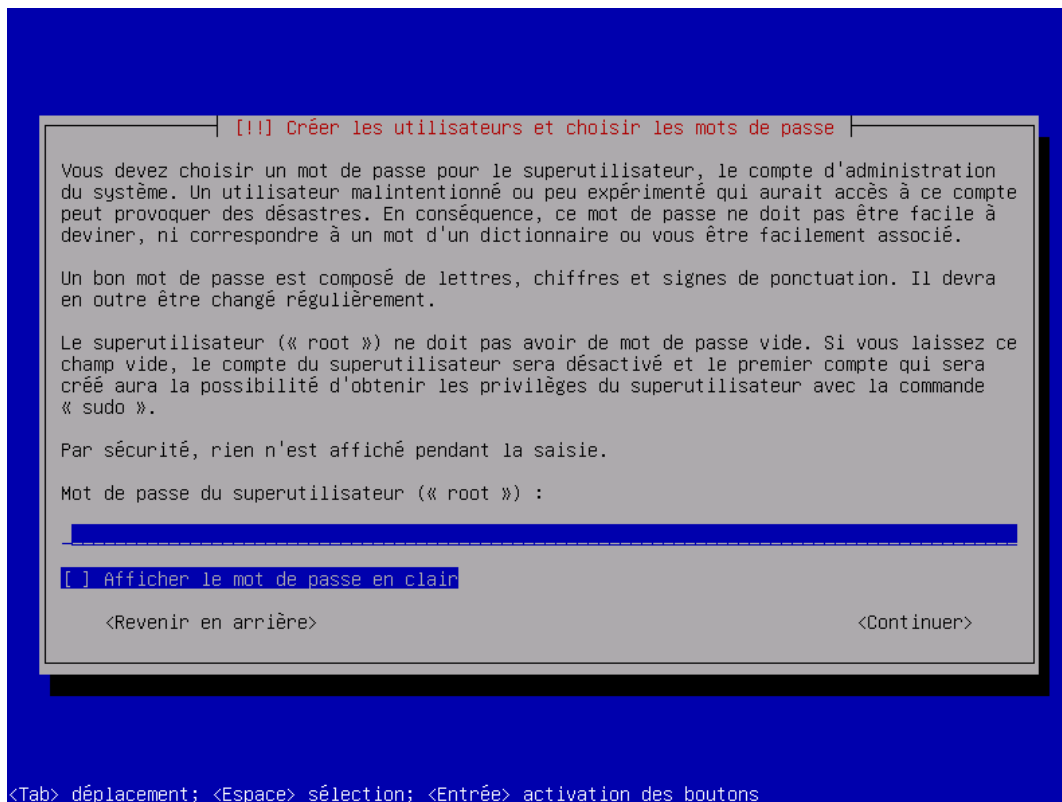
Domaine :

IDM.lan

<Revenir en arrière> <Continuer>

<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons

Il faut maintenant créer le mot de passe pour le super user.



[[!]] Créer les utilisateurs et choisir les mots de passe

Vous devez choisir un mot de passe pour le superutilisateur, le compte d'administration du système. Un utilisateur malintentionné ou peu expérimenté qui aurait accès à ce compte peut provoquer des désastres. En conséquence, ce mot de passe ne doit pas être facile à deviner, ni correspondre à un mot d'un dictionnaire ou vous être facilement associé.

Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement.

Le superutilisateur (« root ») ne doit pas avoir de mot de passe vide. Si vous laissez ce champ vide, le compte du superutilisateur sera désactivé et le premier compte qui sera créé aura la possibilité d'obtenir les privilèges du superutilisateur avec la commande « sudo ».

Par sécurité, rien n'est affiché pendant la saisie.

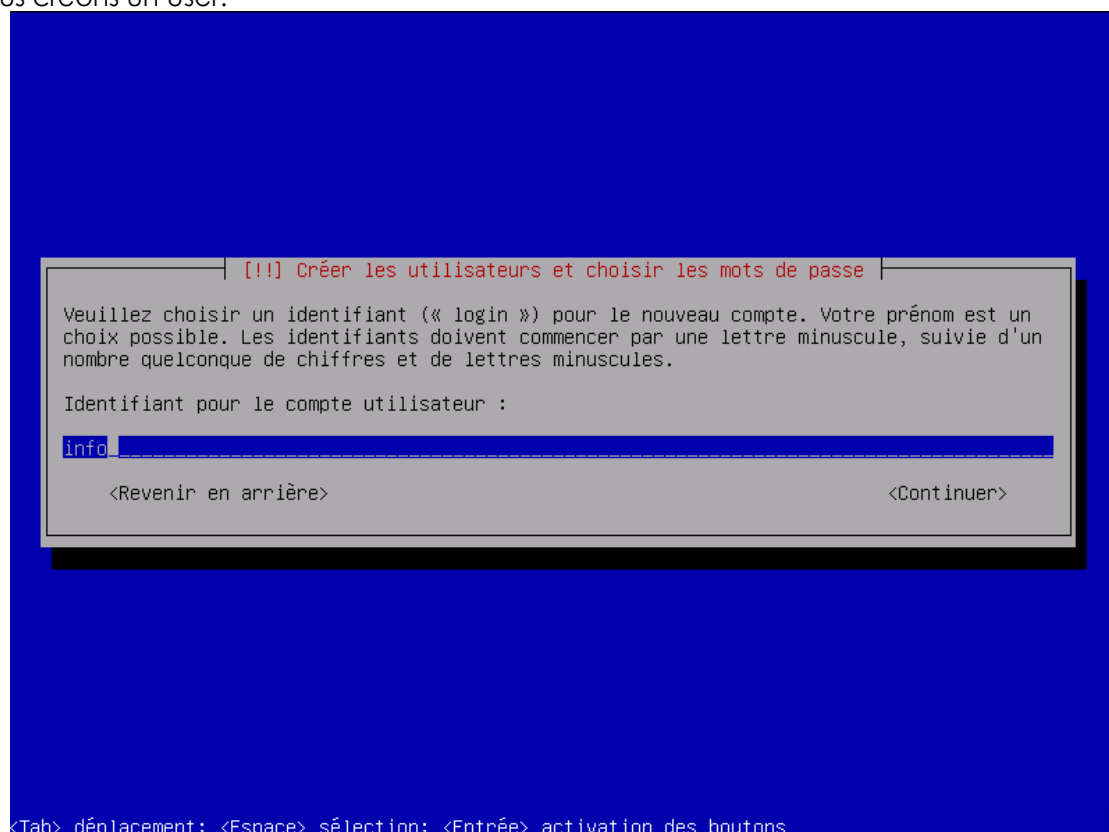
Mot de passe du superutilisateur (« root ») :

[] Afficher le mot de passe en clair

<Revenir en arrière> <Continuer>

<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons

Nous créons un User.



[[!]] Créer les utilisateurs et choisir les mots de passe

Veillez choisir un identifiant (« login ») pour le nouveau compte. Votre prénom est un choix possible. Les identifiants doivent commencer par une lettre minuscule, suivie d'un nombre quelconque de chiffres et de lettres minuscules.

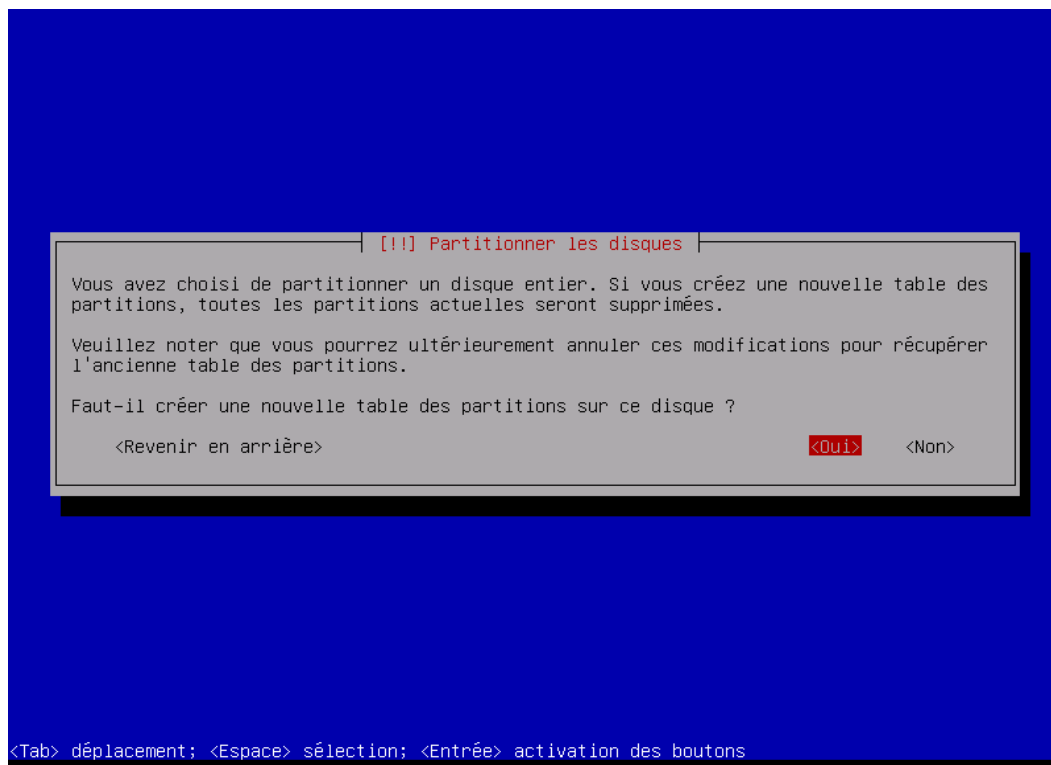
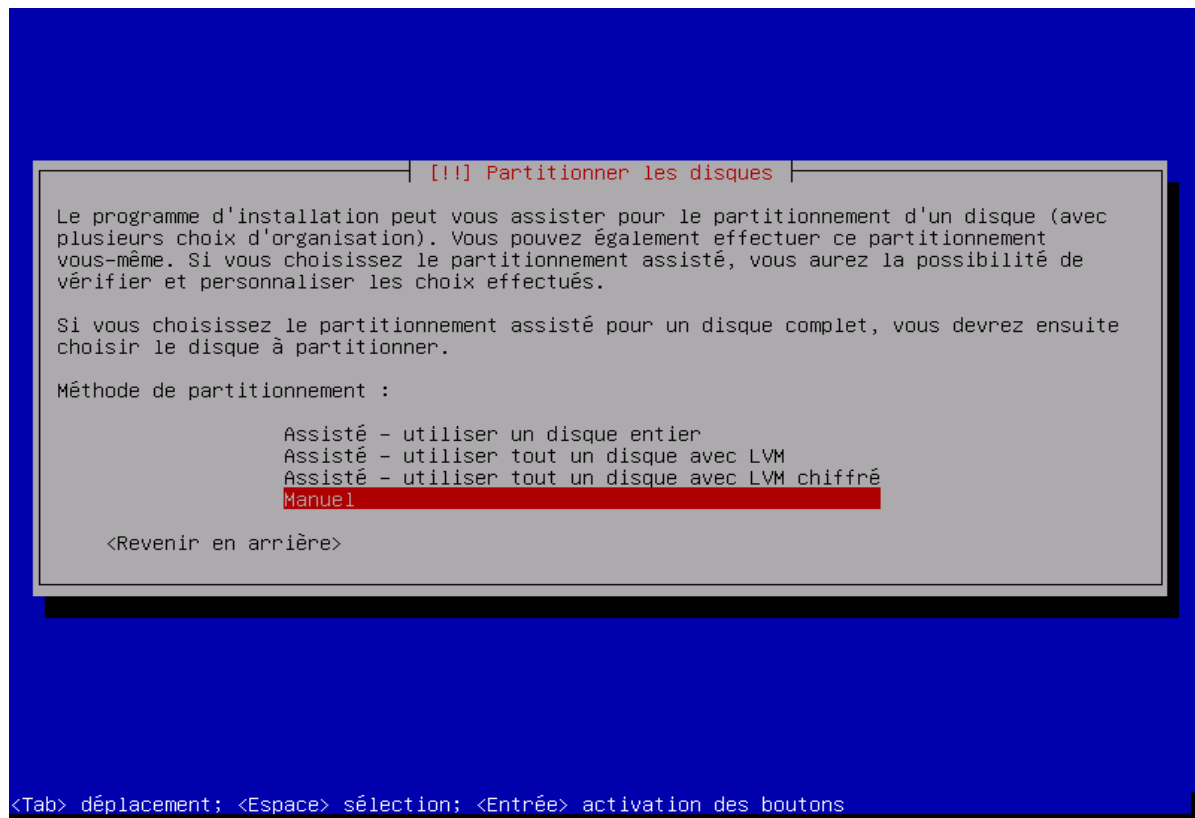
Identifiant pour le compte utilisateur :

info

<Revenir en arrière> <Continuer>

<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons

Nous partitionnons maintenant nos disques :



[!!] Partitionner les disques

Action sur cet espace disponible :

Créer une nouvelle partition
 Partitionner automatiquement l'espace disponible
 Afficher les informations sur les cylindres, têtes et secteurs

<Revenir en arrière>

<F1> aide; <Tab> déplacement; <Espace> sélection; <Entrée> activation boutons

[!!] Partitionner les disques

Voici la table des partitions et les points de montage actuellement configurés. Vous pouvez choisir une partition et modifier ses caractéristiques (système de fichiers, point de montage, etc.), un espace libre pour créer une nouvelle partition ou un périphérique pour créer sa table des partitions.

Partitionnement assisté
 Configurer le RAID avec gestion logicielle
 Configurer le gestionnaire de volumes logiques (LVM)
 Configurer les volumes chiffrés
 Configurer les volumes iSCSI

SCSI3 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S

n° 1	primaire	8.0 GB	f	ext4	/
n° 5	logique	3.0 GB	f	ext4	/var
n° 6	logique	1.1 GB	f	swap	swap
n° 7	logique	398.5 MB	f	ext4	/tmp
n° 8	logique	9.0 GB	f	ext4	/home

Annuler les modifications des partitions
Terminer le partitionnement et appliquer les changements

<Revenir en arrière>

<F1> aide; <Tab> déplacement; <Espace> sélection; <Entrée> activation boutons

[!] Partitionner les disques

Si vous continuez, les modifications affichées seront écrites sur les disques. Dans le cas contraire, vous pourrez faire d'autres modifications.

Les tables de partitions des périphériques suivants seront modifiées :
SCSI3 (0,0,0) (sda)

Les partitions suivantes seront formatées :

- partition n° 1 sur SCSI3 (0,0,0) (sda) de type ext4
- partition n° 5 sur SCSI3 (0,0,0) (sda) de type ext4
- partition n° 6 sur SCSI3 (0,0,0) (sda) de type swap
- partition n° 7 sur SCSI3 (0,0,0) (sda) de type ext4
- partition n° 8 sur SCSI3 (0,0,0) (sda) de type ext4

Faut-il appliquer les changements sur les disques ?

<Oui> <Non>

<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons

[!] Installer le programme de démarrage GRUB sur un disque dur

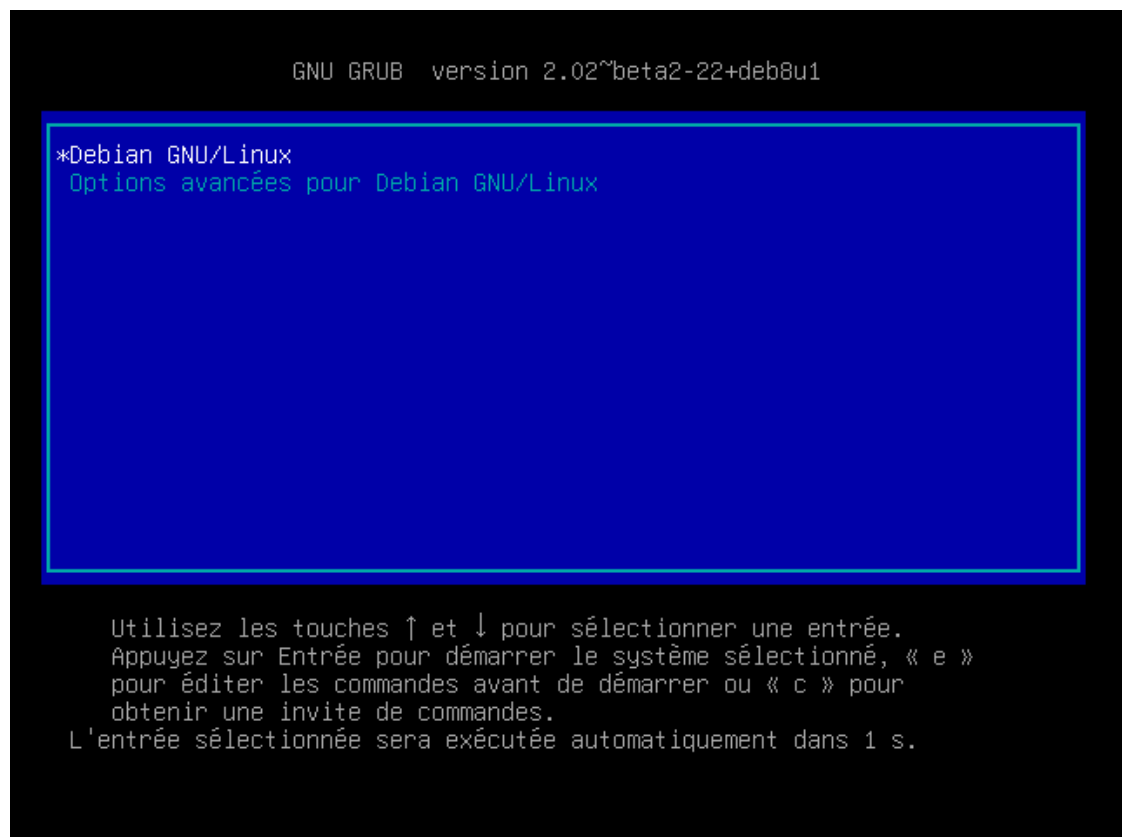
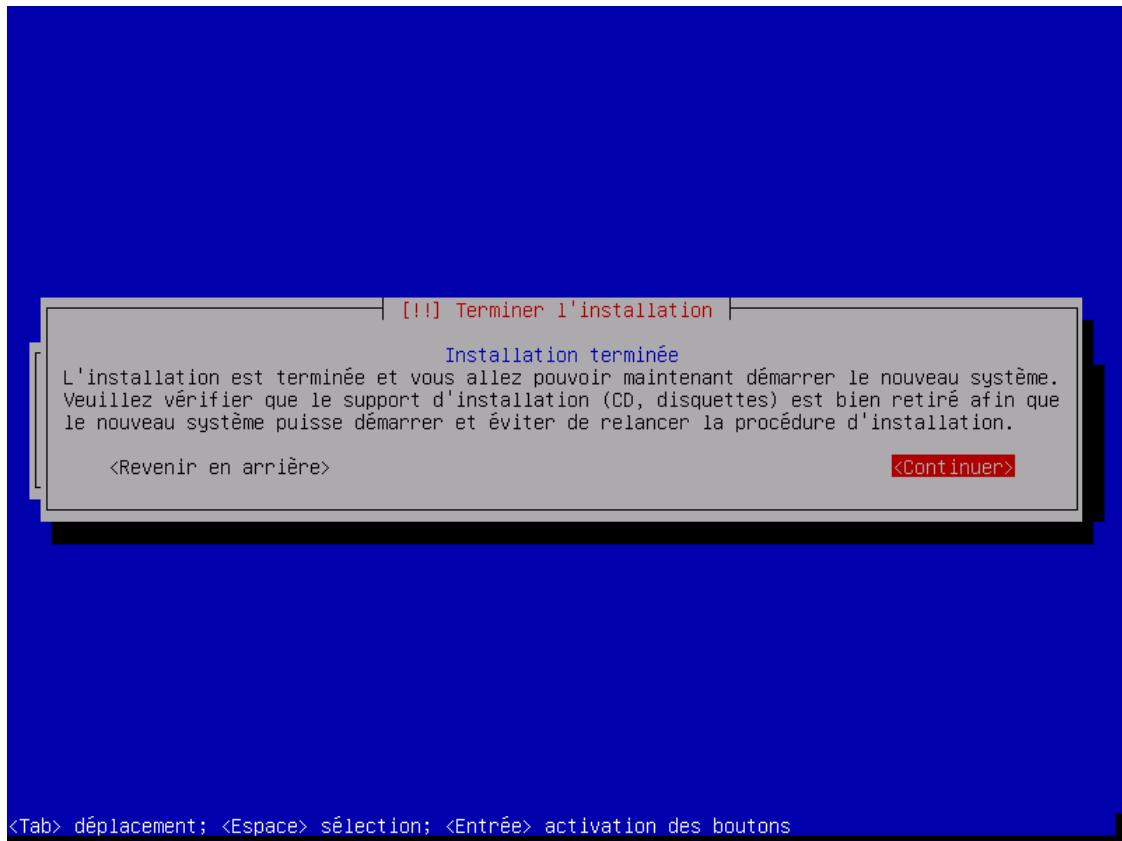
Le système nouvellement installé doit pouvoir être démarré. Cette opération consiste à installer le programme de démarrage GRUB sur un périphérique de démarrage. La méthode habituelle pour cela est de l'installer sur le secteur d'amorçage principal du premier disque dur. Vous pouvez, si vous le souhaitez, l'installer ailleurs sur le disque, sur un autre disque ou même sur une disquette.

Périphérique où sera installé le programme de démarrage :

Choix manuel du périphérique
/dev/sda

<Revenir en arrière>

<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons



Paramétrage réseau :

Maintenant que notre serveur linux est prêt à être utilisé, nous commençons par paramétrer notre carte réseau en tapant la commande suivante :

```
root@IDM-SRV-LIN1:~# nano /etc/network/interfaces
```

Cela va nous ouvrir la page de configuration et il nous restera plus qu'à la remplir de la manière suivante :

```
GNU nano 2.7.4      Fichier : /etc/network/interfaces      Modifié
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet static
address 192.168.10.10
netmask 255.255.255.255
gateway 192.168.10.1
dns-nameservers 192.168.10.1 192.168.10.4_

^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^J Justifier  ^C Pos. cur.  ^Y Page préc.
^X Quitter   ^R Lire fich.^N Remplacer  ^U Coller    ^T Orthograp.^D Aller lig. ^V Page suiv.
```

Nous enregistrons notre fichier modifié et pour finir nous effectuons la commande suivante pour que nos modifications soient prises en compte :

```
root@IDM-SRV-LIN1:~# service networking restart
```

Mise en place des différents disques et partitionnement :

Chaque service disposera d'un disque dur qui lui sera propre pour éviter que celui-ci n'empiète sur le système.

Nous créons tout d'abord les fichiers /FTP /samba /nfs, puis nous créons nos partitions en tapant la commande suivante :

```
root@IDM-SRV-LIN1:~# fdisk /dev/sd(lettre du disque)
```

Ensuite choisir « n » et laisser les paramètres par défaut pour créer la partition primaire Notre partition étant maintenant créée nous allons la formater au format ext4.

```
root@IDM-SRV-LIN1:~# mkfs.ext4 /dev/sd(lettre du disque)1
```

Maintenant nous attachons la partition à notre dossier crée précédemment.

```
root@IDM-SRV-LIN1:~# mount /dev/sd(lettre du disque)1 /samba
```

Pour que ce disque reste actif au redémarrage du serveur il nous faut modifier le fichier « fstab » comme ci-dessous :

```
GNU nano 2.2.6          Fichier : /etc/fstab          Modifié
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options>          <dump> <pass>
# / was on /dev/sda1 during installation
UUID=95596a7a-9e2b-4902-9c7c-7cb27fffef27 /          ext4    errors=remount-ro 0    1
# swap was on /dev/sda5 during installation
UUID=7acc4917-aa83-4a82-8a21-6cf18ade5220 none        swap    sw        0    0
/dev/sr0          /media/cdrom0   udf,iso9660 user,noauto 0    0
/dev/sdb1        /samba ext4    defaults    0    2
/dev/sdc1        /FTP  ext4    defaults    0    2
/dev/sde1        /nfs  ext4    defaults    0    2

^G Aide           ^O Écrire       ^R Lire fich.   ^Y Page préc.  ^K Couper
^X Quitter       ^J Justifier   ^W Chercher    ^V Page suiv.  ^U Coller
^C Pos. cur.     ^T Orthograp.
```

FTP

Installer VsFTPd :

L'installation est l'étape la plus rapide.

```
aptitude install vsftpd
```

Notez que par défaut le serveur est immédiatement lancé. Comme nous allons le configurer, on peut l'arrêter le temps de tout préparer.

```
service vsftpd stop
```

Configurer VsFTPd :

Tout se passe dans un seul fichier : /etc/vsftpd.conf. Première chose à faire, toujours, faire une copie du fichier d'origine pour garder une configuration saine en cas de problème de paramétrage.

```
cp /etc/vsftpd.conf /etc/vsftpd.conf.ori
```

Et maintenant on peut éditer notre fichier.

```
nano /etc/vsftpd.conf
```

Le fichier de configuration de VsFTPd est bien commenté. Je vais donc me contenter de présenter les options à modifier.

```
listen_ipv6=YES
```

Si vous avez désactivé ipv6 vous pouvez laisser cette option commentée. Sinon décommentez là.

```
anonymous_enable=NO
```

On ne veut pas accepter les connexions sans identification ou d'utilisateurs inconnus pour le moment. Donc on passe l'option à « NO ».

```
local_enable=YES
```

Activez cette option à « YES » pour que les utilisateurs ayant un compte sur la machine puissent se connecter en FTP

```
write_enable=YES
```

Cette option permet aux utilisateurs connectés de pouvoir écrire des fichiers. Si l'option est à « NO » ils pourront uniquement télécharger des fichiers mais pas en envoyer.

```
local_umask=022
```

Nous passons par le UMASK à 022 au lieu de 077 par défaut. De cette façon les fichiers seront créés avec des permissions 644 au lieu de 600. Cela reste tout à fait sécurisé et permet plus de flexibilité en cas de déplacement de fichiers ailleurs dans l'arborescence.

```
xferlog_file=/var/log/vsftpd.log
```

Activer les logs est recommandé pour savoir ce qu'il se passe. Choisissez le chemin de destination que vous souhaitez mais l'emplacement par défaut est satisfaisant.

```
idle_session_timeout=600
```

On définit ici le timeout en cas d'inactivité.

Le chroot des utilisateurs sur VsFTPd :

« Chrooter » un utilisateur signifie « l'enfermer » dans son dossier racine. Dossier que nous pouvons définir. Cela veut dire que l'utilisateur ne pourra jamais sortir, ou remonter plus haut que son dossier initial.

Sans chroot, l'utilisateur pourra remonter l'arborescence pour accéder à /home puis à /. Et de là se balader dans n'importe quel dossier du serveur.

Avec le chroot, l'utilisateur aura cette fois pour racine « virtuelle » non pas /home/admin mais / qui symbolise /home/admin.

Donc il se trouve déjà à la racine et ne plus se déplacer au-dessus ou en dehors de ce point. Il est en quelque sorte emprisonné.

Configurer le chroot de VsFTPd

Pour configurer le chroot il faut activer les options suivantes

```
chroot_local_user=YES
```

```
chroot_list_enable=YES
```

```
chroot_list_file=/etc/vsftpd.chroot_list
```

Ces trois options signifient que 1/ nous chrootons tous les utilisateurs, 2/ que nous allons faire une liste d'utilisateurs pour la gestion du chroot, et 3/ que cette liste est disponible à tel endroit dans tel fichier.

VsFTPd a une gestion particulière de sa « chrootlist ». Si on active globalement le chroot avec notre première option, la chrootlist listera des utilisateurs qui ne DEVRONT PAS être chrootés. Tous nos utilisateurs seront chrootés.

A l'inverse si je n'active pas globalement le chroot pour mes 50 utilisateurs mais que « admin » doit être, lui, chrooté, j'irai mettre son nom dans la liste. Cette fois-ci, si `chroot_localuser=NO`, le comportement de la `chrootlist` s'inverse et on indiquera alors à l'intérieur les utilisateurs qui DEVRONT être chrootés.

Pour résumer, la `chrootlist` gère les exceptions du paramétrage global. Si globalement OUI -> `chrootlist = NON` Si globalement NON -> `chrootlist = OUI`.

Démarrer le serveur VsFTPd :

Notre configuration est maintenant terminée, il n'y a plus qu'à démarrer le serveur.

```
service vsftpd start
```

S'il y a un problème de configuration VsFTPd ne démarrera pas.

Testez votre FTP les permissions que vous avez ou pas et ajustez les paramètres en conséquence.

Le client FTP :

Pour se connecter au FTP, l'utilisateur va avoir besoin d'un logiciel appelé « client FTP ». Un des plus connus et usité est Filezilla. Qui plus est, il est open source.

SAMBA

Dans un premier temps nous devons l'installer :

```
root@IDM-SRV-LIN1:~# apt-get install smbclient samba-common
```

Puis, nous téléchargeons le nécessaire pour intégrer notre serveur au domaine.

```
root@IDM-SRV-LIN1:~# apt-get install winbind libnss-winbind libpam-winbind
```

Nous installons ensuite « ntp » pour synchroniser la date et l'heure du serveur AD.

```
root@IDM-SRV-LIN1:~# apt-get install ntp
```

Nous installons Kerberos pour l'authentification à l'AD.

```
root@IDM-SRV-LIN1:~# apt-get install libpam-krb5 krb5-user
```

Après avoir installés tous les paquets nécessaires au bon fonctionnement de Samba nous nous attaquons maintenant à la configuration de celui-ci, dans un premier temps nous synchronisons la date et l'heure de notre serveur Linux à l'AD. Pour cela nous modifions le fichier comme ci-dessous :

```
GNU nano 2.7.4      Fichier : /etc/ntp.conf      Modifié
# /etc/ntp.conf, configuration for ntpd; see ntp.conf(5) for help
driftfile /var/lib/ntp/ntp.drift

# Enable this if you want statistics to be logged.
#statsdir /var/log/ntpstats/

statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable

# You do need to talk to an NTP server or two (or three).
#server ntp.your-provider.example

# pool.ntp.org maps to about 1000 low-stratum NTP servers. Your server will
# pick a different set every time it starts up. Please consider joining the
# pool: <http://www.pool.ntp.org/join.html>
server IDM-SRV-DC1.lan_

# Access control configuration; see /usr/share/doc/ntp-doc/html/acopt.html for
# details. The web page <http://support.ntp.org/bin/view/Support/AccessRestrictions>
# might also be helpful.
#
# Note that "restrict" applies to both servers and clients, so a configuration
# that might be intended to block requests from certain clients could also end
# up blocking replies from your own upstream servers.

# By default, exchange time with everybody, but don't allow configuration.
restrict -4 default kod notrap nomodify nopeer noquery limited

^G Aide      ^O Écrire   ^W Chercher ^K Couper   ^J Justifier ^C Pos. cur. ^Y Page préc.
^X Quitter   ^R Lire fich. ^_ Remplacer ^U Coller   ^T Orthograp. ^G Aller lig. ^V Page suiv.
```


Une fois notre serveur de temps configuré nous passons à configuration de Kerberos en ajoutant les lignes suivantes :

```
GNU nano 2.7.4 Fichier : /etc/krb5.conf Modifié
[libdefaults]
    default_realm = IDM.LAN
    dns_lookup_realm = false
    dns_lookup_kdc = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true

# The following krb5.conf variables are only for MIT Kerberos.
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true

# The following encryption type specification will be used by MIT Kerberos
# if uncommented. In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
#
# The only time when you might need to uncomment these lines and change
# the enctypees is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).

#     default_tgs_enctypes = des3-hmac-sha1
#     default_tkt_enctypes = des3-hmac-sha1
#     permitted_enctypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
    fcc-mit-ticketflags = true

[realms]
^G Aide      ^O Écrire   ^W Chercher  ^K Couper    ^J Justifier  ^C Pos. cur.  ^Y Page préc.
^X Quitter   ^R Lire fich. ^N Remplacer ^U Coller    ^T Orthograp. ^L Aller lig. ^V Page suiv.
```

```
GNU nano 2.7.4 Fichier : /etc/krb5.conf Modifié
# encryption types as they are added, creating interoperability problems.
#
# The only time when you might need to uncomment these lines and change
# the enctypees is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).

#     default_tgs_enctypes = des3-hmac-sha1
#     default_tkt_enctypes = des3-hmac-sha1
#     permitted_enctypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
    v4_instance_resolve = false
    v4_name_convert = {
        host = {
            rcmd = host
            ftp = ftp
        }
        plain = {
            something = something-else
        }
    }
    fcc-mit-ticketflags = true

[realms]
    IDM.LAN = {
        kdc = kerberos.mit.edu
        admin_server = IDM-SRV-DC1.idm.lan
        default_domain = IDM.lan
    }

[domain_realm]
^G Aide      ^O Écrire   ^W Chercher  ^K Couper    ^J Justifier  ^C Pos. cur.  ^Y Page préc.
^X Quitter   ^R Lire fich. ^N Remplacer ^U Coller    ^T Orthograp. ^L Aller lig. ^V Page suiv.
```

```
GNU nano 2.7.4          Fichier : /etc/krb5.conf          Modifié
}
plain = {
    something = something-else
}
fcc-mit-ticketflags = true

[realms]
IDM.LAN = {
    kdc = kerberos.mit.edu
    admin_server = IDM-SRV-DC1.idm.lan
    default_domain = IDM.lan
}

[domain_realm]
.idm.lan = IDM.LAN
idm.lan = IDM.LAN

[login]
krb4_convert = true
krb4_get_tickets = false

^G Aide          ^O Écrire
^X Quitter      ^R Lire fich.   ^W Chercher
^_ Orthograp.   ^K Couper      ^C Pos. cur.
^T Coller      ^J Justifier   ^C Pos. cur.
^Y Page préc.  ^V Page suiv.
```

Nous configurons maintenant Samba :

```
GNU nano 2.7.4          Fichier : /etc/samba/smb.conf          Modifié
# NOTE: Whenever you modify this file you should run the command
# "testparm" to check that you have not made any basic syntactic
# errors.

#===== Global Settings =====

[global]

workgroup = IDM
realm = idm.lan
security = ADS
password server = P@ssw0rd
ps_level = 0
local master = No
domain master = No
template shell = /bin/bash
winbind enum users = yes
winbind enum groups = yes
winbind use default domain = yes
idmap config IDM:range = 10000000-19000000
idmap config IDM:backend = rid
idmap config * : range = 11000-20000
idmap config * : backend = tdb

## Browsing/Identification ##

# Change this to the workgroup/NT-domain name your Samba server will part of
workgroup = WORKGROUP

# Windows Internet Name Serving Support Section:
# WINS Support - Tells the NMBD component of Samba to enable its WINS Server
# wins support = no

root@IDM-SRV-LIN1:~#
```

Notre Samba étant terminé d'être configuré nous vérifions que notre « resolv.conf » est lui aussi bien configuré :

```
GNU nano 2.7.4          Fichier : /etc/resolv.conf          Modifié
domain idm.lan_
search idm.lan
nameserver 192.168.10.1 192.168.10.4

^G Aide          ^O Écrire        ^W Chercher      ^K Couper        ^J Justifier     ^C Pos. cur.      ^V Page préc.
^X Quitter      ^R Lire fich.   ^M Remplacer    ^U Coller       ^T Orthograp.   ^L Aller lig.   ^N Page suiv.
```

Nous pouvons maintenant rejoindre le domaine :

```
root@IDM-SRV-DC1:~# net join IDM-SRV-DC1.idm.lan -U administrateur
```

Pour vérifier que l'intégration s'est bien effectuée nous faisons un :

```
root@IDM-SRV-DC1:~# wbinfo -u
```

Afin de lister tous les users de l'AD.

CONFIGURATION DU SERVEUR NFS

Suivez les instructions ci-dessous pour le configurer.

Mettez à jour vos références de package :

```
apt update
```

Installez le paquet du serveur NFS nfs-kernel-server :

```
apt install nfs-kernel-server
```

Installez le portmap package Portmapper:

```
apt-get install portmap
```

Créez un répertoire dans votre système de fichiers local à utiliser comme emplacement racine du partage NFS :

```
mkdir /var/nfsroot
```

Affectez la propriété appropriée à la racine du partage NFS:

```
chown nobody:nogroup /var/nfsroot/
```

Ajoutez la ligne suivante au fichier `/etc/exports` , en remplaçant `exemple_IP` par l'adresse IPv4 privée du client Linux. Assurez-vous qu'il n'y a pas d'espace entre la parenthèse ouvrante / 17 et la ligne vide à la fin du fichier.

```
/ etc / exports
```

```
1 /var/nfsroot exemple_IP/17 ( rw,root_squash,subtree_check )
```

Mettez à jour la table des systèmes de fichiers exportés avec la commande suivante:

```
sudo exportfs -ra
```

Redémarrez le service NFS sur le serveur pour que vos modifications prennent effet:

```
sudo systemctl restart nfs-kernel-server
```

Vous avez maintenant un serveur NFS de base sur votre serveur, configuré pour servir le répertoire /var/nfsroot à votre deuxième serveur.

Options du serveur NFS

Ces options peuvent être spécifiées dans l'entrée /etc/exports :

rw : Système de fichiers en lecture / écriture.

ro : Force les clients à se connecter uniquement en mode de système de fichiers en lecture seule.

no_root_squash : Le compte root sur la machine client aura le même niveau de privilège que la racine sur la machine serveur. Cette option a des implications de sécurité ; N'utilisez pas, sauf si vous êtes sûr que vous en avez besoin. D'un autre côté, root_squash fait que le client racine a le même type d'accès que personne sur le serveur - empêchant ainsi les clients root de diffuser des fichiers indésirables aux autres.

no_subtree_check : Désactive l'emplacement des fichiers vérifie les exportations de volume partiel. Cette option accélérera les transferts sur les exportations en volume.

sync : Force tous les transferts à fonctionner en mode synchrone, de sorte que tous les clients attendent que leurs opérations soient terminées. Cela peut éviter la corruption de données en cas de panne du serveur.

DHCP

Il faut installer les paquets nécessaires sur les serveurs Unix. Faisons une mise à jour des paquets puis on installe « isc-dhcp-server » via le paquet « dhcp3-server ».

```
apt-get update
```

```
apt-getinstall dhcp3-server
```

Le fichier de configuration du service DHCP est le suivant :

```
/etc/dhcp/dhcpd.conf
```

Renommez le fichier de configuration afin de le garder par sécurité. Nous partirons d'un fichier de configuration vierge :

```
mv /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.old
```

```
touch /etc/dhcp/dhcpd.conf
```

La base de données de gestion des adresses IP et des baux est située dans le fichier suivant :

```
/var/lib/dhcp/dhclient.leases
```

En ce qui concerne la gestion du service, pour le démarrer, le redémarrer et l'arrêter on procède comme ceci :

```
service isc-dhcp-serverstart | restart | stop
```

La directive MCLT

Cette directive qui signifie « Max Client Lead Time » et qui est présente lors de la configuration du service DHCP en mode « failover » correspond au temps maximum, pendant lequel le serveur peer peut renouveler des requêtes après avoir perdu contact avec son partenaire.

La directive SPLIT

La directive « SPLIT » est également présente dans la configuration du service DHCP en mode « failover » tout comme la directive MCLT. Elle permet de « splitter » c'est-à-dire de diviser la plage d'adresses IP disponible en deux parties, afin de répartir la charge sur les deux serveurs.

Lorsque cette directive a la valeur « 128 », on part sur une répartition 50%/50%, c'est-à-dire que chaque serveur gère 50% de la plage d'adresses disponible.

Configuration du serveur DHCP Master

Commençons par configurer le serveur DHCP Master, c'est-à-dire le serveur actif et maître. Stoppez le service DHCP le temps de la configuration puis éditez le fichier de configuration vierge « dhcpd.conf » que nous avons créé.

Commencez par ajouter ceci à votre fichier de configuration :

```
# Paramétrage du failover du DHCP Master

failoverpeer "idm" {

primary      ;           # Déclare ce serveur comme master.

address 192.168.10.10 ;   # Adresse du serveur master.

port 520     ;           # Port d'écoute du serveur master.

peeraddress 192.168.10.11 ; # Adresse du serveur slave.

peer port 520 ;          # Port d'écoute du serveur slave.

max-response-delay 60 ;  # Temps de non réponse du slave.

max-unacked-updates 10 ;

mclt 3600 ;

split 128 ;             # Répartition des plages d'adresses.

load balance max seconds 3;

}
```

Le bloc de configuration ci-dessus, permet de configurer la paire de failover appelée « idm ».

Le port d'écoute peut être changé comme vous le souhaitez mais vous devez être cohérent dans la façon dont vous allez configurer le second serveur selon le numéro de port indiqué dans la configuration du premier serveur.

La seule directive qui permet d'indiquer que ce serveur est le master/primaire est la présence de la ligne « primary » qui sera remplacée par « secondary » sur le serveur slave/secondaire. De plus, les directives « split » et « mclt » sont présentes uniquement sur le serveur maître.

Nos postes clients se verront attribuer une adresse sur la plage d'adresses IP allant de 192.168.10.100 à 192.168.10.199 soit 100 adresses disponibles. La passerelle par défaut sera 192.168.10.1, le serveur DNS 192.168.10.1 et le bail quant à lui sera 6 heures pouvant être prolongé jusqu'à 10 heures si besoin.

```
subnet 192.168.10.0 netmask 255.255.255.0 {  
  
    pool{  
  
        failoverpeer "idm";          # Indique la configuration du failover  
  
        optionrouters 192.168.10.1;          # Passerelle par défaut  
  
        optiondomain-name-servers 192.168.10.1; # Serveur DNS  
  
        range 192.168.10.100 192.168.10.199; # Plage d'adresses IP  
  
        default-lease-time 21600 ;      # Bail de 6 heures par défaut  
  
        max-lease-time 36000 ;          # Bail pouvant aller jusqu'à 10 heures  
  
    }  
  
}
```

Pour finir, on ajoute la directive « authoritative » en début de fichier pour indiquer que ce serveur DHCP fait autorité sur ce subnet.

En résumé on obtient ceci sur le serveur Master :

```
authoritative;  
  
# Paramétrage du failover du DHCP Master  
  
failoverpeer "idm" {  
  
    primary          ;      # Déclare ce serveur comme master.  
  
    address 192.168.10.10    ; # Adresse du serveur master.  
  
    port 520          ;      # Port d'écoute du serveur master.  
  
    peeraddress 192.168.10.11 ; # Adresse du serveur slave.  
  
    peer port 520          ; # Port d'écoute du serveur slave.  
  
    max-response-delay 60    ; # Temps de non réponse en secondes.  
  
    max-unacked-updates 10   ;
```



```
mclt 3600 ;  
split 255 ; # Répartition des plages d'adresses.  
load balance max seconds 3;  
}  
  
# Paramétrage de la configuration à distribuer aux postes clients  
subnet 192.168.10.0 netmask 255.255.255.0 {  
pool{  
failoverpeer "idm"; # Indique la configuration du failover  
optionrouters 192.168.10.1; # Passerelle par défaut  
optiondomain-name-servers 192.168.10.1 ; # Serveur DNS  
range 192.168.10.100 192.168.10.199; # Plage d'adresses IP  
default-lease-time 21600 ; # Bail de 6 heures par défaut  
max-lease-time 36000 ; # Bail pouvant aller jusqu'à 10 heures  
}  
}
```

Configuration du serveur DHCP Slave

Passons maintenant à la configuration du serveur DHCP Slave, on se base sur la configuration du serveur DHCP Master. En effet, la configuration est quasiment identique sur les deux serveurs. Pensez à inverser les adresses IP indiquant l'adresse du serveur master et celle du slave, remplacer « primary » par « secondary » et supprimer les directives « mclt » et « split ». Pour le reste, rien ne change.

Paramétrage du failover du DHCP Slave

```
failoverpeer "idm" {  
  
    secondary      ;           # Déclare ce serveur comme slave.  
  
    address 192.168.10.11    ;   # Adresse du serveur slave.  
  
    port 520           ;           # Port d'écoute du serveur slave.  
  
    peeraddress 192.168.10.10 ; # Adresse du serveur master.  
  
    peer port 520        ;   # Port d'écoute du serveur master.  
  
    max-response-delay 60    ;   # Temps de non réponse en secondes.  
  
    max-unacked-updates 10   ;   # Nombre de mises à jour avant de déclarer le pair en échec  
  
    load balance max seconds 3; # Durée max avant de décharger la requête vers le pair  
}
```

Paramétrage de la configuration à distribuer aux postes clients

```
subnet 192.168.10.0 netmask 255.255.255.0 {  
  
    pool{  
  
        failoverpeer "idm";      # Indique la configuration du failover  
  
        optionrouters 192.168.10.1; # Passerelle par défaut  
  
        optiondomain-name-servers 192.168.10.1; # Serveur DNS  
  
        range 192.168.10.100 192.168.10.199; # Plage d'adresses IP  
  
        default-lease-time 21600 ; # Bail de 6 heures par défaut  
  
        max-lease-time 36000 ; # Bail pouvant aller jusqu'à 10 heures  
  
    }  
  
}
```

Démarrez le service

Nous pouvons désormais passer le service en phase de test, démarrez-le sur chacun de vos serveurs en commençant par le démarrer sur le serveur master puis sur le slave.

```
service isc-dhcp-server start
```

TABLEAU DES COMMANDES SQL

Résumé de quelques commandes MySQL importantes

Connexion et exécution de script	Connexion à MySQL (via la console unix)	<code>mysql -u nomUsager -p</code>
	Quitter MySQL	<code>QUIT;</code>
	Exécuter un script .sql (le chemin, lorsque nécessaire, peut être en mode absolu ou relatif. En mode relatif, le point de référence est le répertoire actif lors de la connexion à MySQL)	<code>SOURCE chemin/nomDuFichier.sql;</code>
	Annuler une commande en cours de frappe	<code>\c</code>

Gestion des bases de données	Créer une BD (sur Cogito <i>nomDeLaDB = tixxx</i>)	<code>CREATE DATABASE nomDeLaDB;</code>
	Afficher les bases de données existantes	<code>SHOW DATABASES;</code>
	Utiliser une base de données	<code>USE nomBD;</code>
	Effacer une base de données	<code>DROP DATABASE nomDeLaDB;</code>
Gestion des tables	Créer une table	<code>CREATE TABLE nomDeLaTable (nomDeLaColonne TypeDeValeurs AttributDesValeurs, nomDeLaColonne TypeDeValeurs AttributDesValeurs, ...);</code>
	Afficher les tables existantes	<code>SHOW TABLES;</code>
	Afficher la structure d'une table	<code>DESCRIBE nomDeLaTable;</code>
	Modifier une table	<code>ALTER TABLE nomDeLaTable RENAME AS nouveauNomDeLaTable;</code>
		<code>ALTER TABLE nomDeLaTable ADD nomDeLaColonne TypeDeValeurs;</code>
		<code>ALTER TABLE nomDeLaTable CHANGE nomDeLaColonne nouveauNomDeLaColonne TypeDeValeurs;</code>
<code>ALTER TABLE nomDeLaTable DROP COLUMN nomDeLaColonne;</code>		
Effacer une table	<code>DROP TABLE nomDeLaTable;</code>	
Gestions des données	Ajouter des données	<code>INSERT INTO nomDeLaTable VALUES (valeur1, valeur2, ...);</code>
		<code>INSERT INTO nomDeLaTable (nomDeLaColonne1, nomDeLaColonne2, ...) VALUES (valeur1, valeur2, ...);</code>
	Afficher des données	<code>SELECT nomDeLaColonne1, nomDeLaColonne2, ... FROM nomDeLaTable WHERE certainesColonnes=CertainesValeurs GROUP BY nomDeLaColonne ORDER BY nomDeLaColonne AttributD'ordre;</code>
	Mises à jour de données	<code>UPDATE nomDeLaTable SET nomDeLaColonne1=valeur1, nomDeLaColonne2=valeur2, ... WHERE certainesColonnes=CertainesValeurs;</code>
	Modifier l'affichage du nom de colonne	<code>SELECT ... FROM ... AS nomAlias;</code>
	Recherche d'un pattern. (Retourne ici ce qui commence par 'a')	<code>SELECT ... FROM ... WHERE ... LIKE 'a%';</code>
	Effacer des données	<code>DELETE FROM nomDeLaTable WHERE certainnesColonnes=CertainesValeurs;</code>

Types de valeurs	Entiers, Flottant, Double	<code>INT, FLOAT, DOUBLE</code>
	Chaîne de caractères à longueur variable	<code>VARCHAR(nombreDeCaractère)</code>
	Liste	<code>ENUM('élément1', 'élément2', ...)</code>
	Date (format aaaa-mm-jj)	<code>DATE</code>
	Heure (format hh:mm:ss)	<code>TIME</code>
	Date et Heure (mis à jours lorsque l'enregistrement est modifié)	<code>TIMESTAMP</code>
Attribut des valeurs	Le champ ne peut pas être laissé vide	<code>NOT NULL</code>
	Le champ peut être laissé vide	<code>NULL</code>
	Valeurs positives	<code>UNSIGNED</code>
	Assignation automatique d'une valeur	<code>AUTO_INCREMENT</code>
	Clé primaire	<code>PRIMARY KEY</code>
Valeurs par défaut	<code>DEFAULT 'Texte'</code>	
Attribut d'ordre	Ascendant	<code>ASC</code>
	Descendant	<code>DESC</code>
Opérateurs	Opérateurs	<code>AND, OR, NOT, =, !=, <, >, +, -, *, /</code>
Fonctions	Fonctions mathématiques	<code>SUM(nomDeLaColonne), MIN(nomDeLaColonne), MAX(nomDeLaColonne), AVG(nomDeLaColonne), COUNT(nomDeLaColonne), COUNT(*)</code>
	Fonction génératrices de dates	<code>NOW(), CURDATE(), CURRENT_DATE(), CURTIME()</code>
	Fonctions pour extraire de l'information à partir des dates	<code>YEAR(uneDate), MONTH(uneDate), DAYOFMONTH(uneDate), TO_DAYS(uneDate)</code>
	Fonctions de concaténation	<code>CONCAT(nomDeLaColonne1, nomDeLaColonne2, ...)</code>

Source : MySQL - Commands, par Stefan Bracher, 2008 <http://www.w3schools.com/sql/> Mise en page, correction et traduction par Sébastien Riendeau 2012

DEVIS NON RETENUS

Voici les deux devis qui n'ont pas été retenus :



DEVIS No.196865

Date du devis 15/06/2018
Référence du devis 196865
Numéro de client 51584
Date de validité du devis 15/07/2018
Modalité de paiement 30 jours
Emis par Marie creuse
Contact client ID'Meuble

Destinataire :
ID'Meuble
35 rue de sillac
16000
Angoulême

Infos additionnelles

Merci d'avoir choisi Ingram
La livraison sera effectuée dans les 4 semaines après réception de la confirmation de la commande ;

Description	Quantités	Prix unitaires HT	TVA %	TVA	TOTAL TTC
Serveur HPE ProLiant DL380 G10	3	2 600,00	20,00%	520,00	9 360,00
3 ans Care Pack Pour Serveur(Intervention H+4)	4	970,00	20,00%	194,00	4 656,00
Windows Serveur 2016	3	825,00	20,00%	165,00	2 970,00
Disque Dur Seagate Enterprise 1To SAS	9	95,00	20,00%	19,00	1 026,00
Licence Utilisateur Windows Serveur	95	32,00	20,00%	6,40	3 648,00
Licence WinDev 23	1	1 400,00	20,00%	280,00	1 680,00
Buffalo TeraStation 3410RN 12To	2	860,00	20,00%	172,00	2 064,00
Veeam Backup et Replication a vie	2	1 300,00	20,00%	260,00	3 120,00
OU					
am Backup et Replication Annuel Sur 3 A	6	73,95	20,00%	14,79	532,44
REMISE FOURNISSEUR					-10%
Total Abonnement VEEAM			Total Licence Definitive VEEAM		
Total HT	22 122,04			Total HT	24 450,84
TVA	1 631,19			TVA	1 631,19
Total TTC	23 753,23 		Total TTC		26 082,03

Signature du client (précédée de la mention « Bon pour accord »)



DEVIS No.1569865

Date du devis 15/06/2018
Référence du devis 1569865
Numéro de client 51584
Date de validité du devis 15/07/2018
Modalité de paiement 30 jours
Emis par Jeanne Lamesse
Contact client ID'Meuble

Destinataire :
ID'Meuble
35 rue de sillac
16000
Angoulême

Infos additionnelles

Merci d'avoir choisi Ingram

La livraison sera effectuée dans les 4 semaines après réception de la confirmation de la commande ;

Description	Quantités	Prix unitaires HT	TYA %	TYA	TOTAL TTC
Serveur HPE ProLiant DL380 G10	3	2 700,00	20,00%	540,00	9 720,00
3 ans Care Pack Pour Serveur(Intervention H+4)	4	1 050,00	20,00%	210,00	5 040,00
Windows Serveur 2016	3	860,00	20,00%	172,00	3 096,00
Disque Dur Seagate Enterprise 1To SAS	9	110,00	20,00%	22,00	1 188,00
Licence Utilisateur Windows Serveur	95	30,00	20,00%	6,00	3 420,00
Licence WinDev 23	1	1 600,00	20,00%	320,00	1 920,00
Buffalo TeraStation 3410RN 12To	2	940,00	20,00%	188,00	2 256,00
Veeam Backup et Replication a vie	2	1 416,00	20,00%	283,20	3 398,40
OU					
am Backup et Replication Annuel Sur 3	6	82,00	20,00%	16,40	590,40
REMISE FOURNISSEUR					-10%
Total Abonnement VEEAM					Total Licence Definitive VEEAM
Total HT		23 195,16	Total HT		25 722,36
TYA		1 757,60	TYA		1 757,60
Total TTC		24 952,76 	Total TTC		27 479,96

Signature du client (précédée de la mention « Bon pour accord »)

SOURCES

<https://www.supinfo.com>

<https://fr.wikipedia.org>

<https://support.microsoft.com>

<http://speedweb1.free.fr>

<https://wikiclic.com>

<http://www.clemanet.com>

<http://speedweb1.free.fr>

<https://fr-new.ingrammicro.com>

<https://www.inmac-wstore.com>

<https://www.picata.fr>

debian.org

rootusers.com