



Pixy

Projet ÉVOLUTION

Présenté par :

- Sacha OCHMIANSKY (chef de projet)
- Fabien GUILHEMJOUAN
- Simon GUITTON

Introduction	4
Rappel du contexte	4
Présentation de l'entreprise	4
Présentation du contexte	5
Cahier des charges	6
Rappel des besoins	6
DNS	6
Sécurité	6
Les impressions	6
Les connexions réseaux	6
Stratégie locale	7
Gestion de l'espace disque	7
Connexion aux lecteurs réseau	7
Accès à distance	7
Application	8
Remarques	9
Contraintes	9
Planning	10
Plan de nos bâtiments	11
Bâtiment Principal	11
RDC	11
1er étage	12
Aile EST	12
RDC	12
1er étage	13
Aile OUEST	13
RDC	13
1er étage	14
Topologie en étoile	15
Solution retenue	16
Présentation des serveurs	16
Les points forts de ce serveur :	16
Caractéristiques techniques :	16
Switch (existant)	17
Baie de Brassage (existant)	18
Présentation du Serveur de fichier (évolution de stockage)	19
Firewall	20
Onduleur	21
Les points fort de cet onduleur :	21
Choix des salles serveurs	21
Topologie du réseau	22
Réseau	22
Plan d'adressage	22
Wi-Fi	23

Récapitulatif	23
Windows Server 2012 R2	23
Configuration des rôles :	24
Rôle AD DS	26
Rôle DNS	33
Configuration du DNS	33
Vérification du DNS par NSLOOKUP	40
Réplication du serveur 2 (Site et service AD)	43
Installation et réplication du second contrôleur de domaine	44
Rôle DHCP	48
Rôles Hyper-V	56
Installation des Vm sur Hyper-V	60
Serveur d'impression	68
Sauvegarde et Récupération Windows Server 2012 R2	75
Installation de la fonctionnalité	75
Configuration de la sauvegarde	76
Planification de la sauvegarde	76
Sauvegarde unique	78
Sauvegarde sur le serveur de fichier	78
Rapport de Sauvegarde	80
Récupération de sauvegarde	81
Créations des utilisateurs et des OU	82
Stratégie de groupes	86
GPO mappage lecteurs	87
GPO supplémentaires	88
Serveur de fichiers DFS (Distributed File System)	92
Linux	93
Samba	95
DHCP	98
NTP	101
Host	102
Krb5	102
Apache2	103
PAM	104
FTP	105
MySQL	109
Sauvegardes	112
Base de données	112
Archives Linux	112
NFS	113
Charte informatique	114
Introduction	114
Champ d'application	114
Moyens informatiques concernés	114

Utilisateurs concernés	114
Règles d'utilisation et de sécurité	114
Conditions d'accès	114
Conditions d'utilisation	115
Principes d'utilisation	116
Respect de la confidentialité	116
Accès à notre répertoire	116
Préservation de l'intégrité	116
Textes Applicables	117
Textes législatifs	117
Textes réglementaires	117
Sanctions	118
Conclusion	118
Résumé de notre projet	118
Evolutivité	118
Remerciements	119
Sources	119
Infrastructure Linux	119
Annexe	122
Installation de Windows Server 2012 R2	122
Installation serveur Linux	129
Installation DFS	138
Configuration réseau	138
Installation de SRV-FICHIERS1	138
Installation de SRV-FICHIERS2	142
SCRIPT Création des OU, Groupes et Users	167
Glossaire	171
Devis	172
Serveur hyperviseur	172
Serveur NAS	172
Disques durs de spare	173
Total Security 2017	173
Inventaire logiciel et matériel du parc	173
Extincteur	174
Onduleur	174
Climatisation	176
Windows serveur	177
Tableau récapitulatif des devis	178
Charte graphique	179
Diagramme de Gantt	180

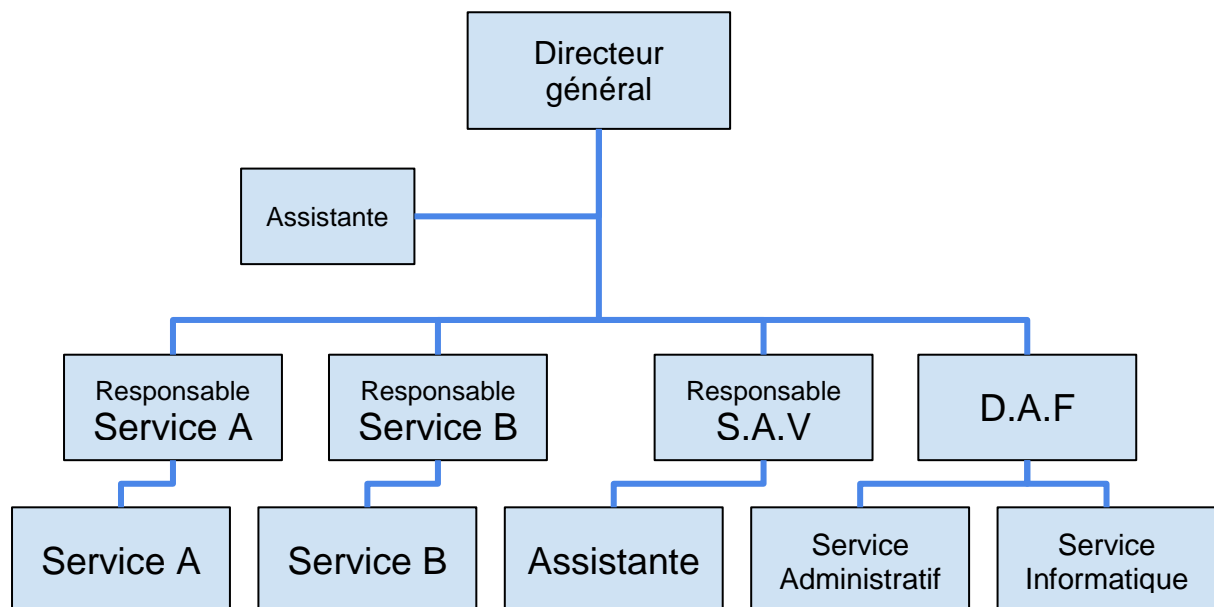
Introduction

Rappel du contexte

Nous avons été chargé de nous occuper de la continuité de notre entreprise, ce qui fait directement suite au projet START, qui a permis de réaliser certaines tâches. En effet, nous avons maintenant depuis 6 mois de nouveaux locaux, le câblage informatique a été mise en place, nos utilisateurs ont de nouveaux postes à jour. Deux nouveaux utilisateurs ont également rejoint nos locaux. Aujourd'hui, nous allons proposer plusieurs solutions pour l'évolution de notre entreprise.

Présentation de l'entreprise

Notre entreprise, PIXY, centrale d'achats pour un regroupement de franchisés, est composée de 90 employés dont voici l'organigramme :



Le service A se compose de 40 personnes, le service B se compose lui de 30 personnes, le service S.A.V se compose de 2 personnes.

Le service administratif se compose de 10 personnes.

Le service informatique, chargé d'améliorer les outils informatique, se compose de Sacha OCHMIANSKY, Fabien GUILHEMJOUAN et Simon GUITTON.

Voici le listing de nos utilisateurs selon leurs services :

Direction Générale	Produit A	Produit B	S.A.V	Direction Administratif et Financier	Service Informatique
Vincent Edmond	Pierre Michon	Michel Lasole	Gerard Gabriel	Nicolas Peltier	Fabien GUILHEMIQUAN
Mlle. Ada	Abra Berry	Howard Fowler	Mme. Laporte	Steven Mcmillan	Simon Guitton
	Acton Cantu	Isabelle Bolton		Stuart Kent	Sacha Ochmiansky
	Adele Owen	Jenette Ramos		Timon Davis	
	Ainsley Pacheco	Jillian Benjamin		Timon Noel	
	Alexandra Randall	Josephine Glenn		Urrah Rodgers	
	Amela Cohen	Julie Ballard		Wade Kirk	
	Autumn Landry	Karen McMahon		Xenos Perkins	
	Avram Hudson	Klara Jefferson		Yvette Reynolds	
	Ayye O'Brien	Kitra Parsons		Harcen Uber	
	Beck Humphrey	Lacey Dudley		Sonia Lahscourn	
	Benedict Bryant	Leila Jensen			
	Berk Burns	Levi Buchanan			
	Bernard Hinton	Madaline Carlson			
	Brandon Kennedy	Madaline Richardson			
	Cally James	Mannix Webster			
	Cally Walsh	Mara Trevino			
	Calvin Hudson	Mari Salazar			
	Chaim Jarvis	Martha Morrow			
	Chastity Aguirre	Mary Hendricks			
	Christine McCarty	Melodie Foster			
	Clare Pale	Mollie Jimenez			
	Colt Hurley	Murphy Calderon			
	Cooper Benson	Natalie Sears			
	Damian Flores	Quail Fitzpatrick			
	Dara Landry	Rachel Contreras			
	Derek Macdonald	Rina Suarez			
	Destiny Cummings	Roary Mooney			
	Destiny Mendoza	Shana Beard			
	Doris Bonner	Sophia Trevino			
	Emerson Sweet	Stacy Macias			
	Emory Dotson				
	Emi Sanford				
	Gabriel Henson				
	Gannon Hughes				
	Geoffrey Jimenez				
	Gray Lewis				
	Mme. Beziat				
	Mme. Ella				
	Mme. Ayo				
	Mme. Acien				

Présentation du contexte

Notre D.A.F nous a fait part de la situation, pour que l'on puisse lui faire des propositions. Voici ses idées et ses remarques :

- L'équipe informatique 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 de droits utilisateurs.
- Le siège social a besoin d'un serveur ftp (ils veulent récupérer des fichiers dessus).
- Nous devons implémenter Active Directory dans l'entreprise.
- Nous avons 7 sessions pour faire aboutir les projets.
- Il veut un compte rendu mensuel sur votre avancé (un tableau d'indicateurs, un planning, le qui fait quoi...)
- 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.

Cahier des charges

Afin de mener à bien ce projet et répondre au mieux aux problématiques, voici les axes qui ont été retenues et auxquels nous devons nous contraindre pour respecter le cahier des charges :

- Tolérance aux pannes
- Serveur DHCP
- Serveur DNS
- Serveur d'impression
- Active Directory
- Service de fichiers
- Gestion des GPO
- Intranet
- Base de donnée

Rappel des besoins

Serveur Windows 2012, nous devons avoir :



DNS

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

Sécurité

- Mot de passe doit répondre aux exigences de complexité
- 8 caractères minimum

Les impressions

- Il faut 1 imprimante pour chaque service nommée Printnom_du_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 sont prioritaires sur toutes les impressions et les utilisent 24/24.
- Le service informatique a le 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 informatique, personne ne peut installer de logiciels sur sa machine ni modifier l'heure.
- Les lecteurs CD 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'une disquette ou d'un disque compact.

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.
- À l'intérieur de chaque répertoire, vous créerez 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'événements.

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.

Serveur Linux, nous devons avoir :

- Partage de ressources Windows via samba serveur.
- Serveur NFS.
- Option : serveur DHCP.
- Service FTP (sécurisé et anonyme).
- Option : service HTTP (intranet PHP MySQL) avec visualisation des caractéristiques techniques et logiciel des autres machines du parc informatiques.
- Client NFS avec sauvegarde automatique des ressources de l'autre serveur.

Application

Le modèle de données sera réalisé en sortie du module base de données relationnelle.

Utilisateurs de l'application développée :

- Les membres du service informatique (en mode gestion).
- Les utilisateurs du parc informatique (en mode consultation).

*Fonctionnalités souhaitées****En mode consultation :***

- Consulter la liste des postes décrits 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 multicritères 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 existant, 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.

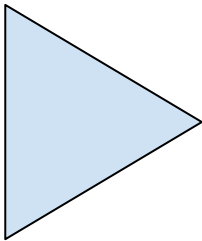
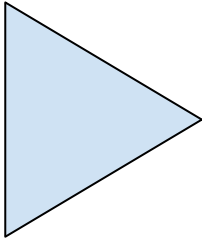
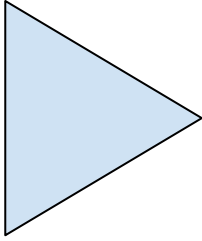
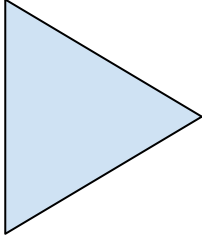
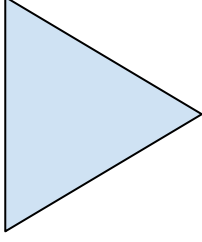
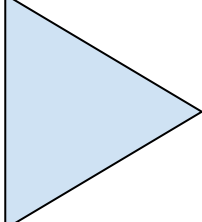
Remarques

- Le mode consultation est accessible à tous les utilisateurs.
- Le mode gestion est interdit aux utilisateurs non membre du service informatique.

Contraintes

- Budget inconnu.
- Délai limité.

Planning

Décembre		Découverte du projet. Analyse de l'existant. Affectation des rôles de chacun. Rédaction du cahier des charges.
Janvier		Découverte univers Windows Server Installation serveur Windows AD et DNS
Février		Installation serveur Windows DHCP Installation serveur Windows DFS Installation serveur Linux Création de la base de données
Mars		Mise en place de la redondance des serveurs Mise en place de la maquette Création du site Web
Avril		Mise en place de la redondance de la base de données Création des utilisateurs
Mai		Mise en place des GPO Rédaction du projet. Mise en place imprimantes

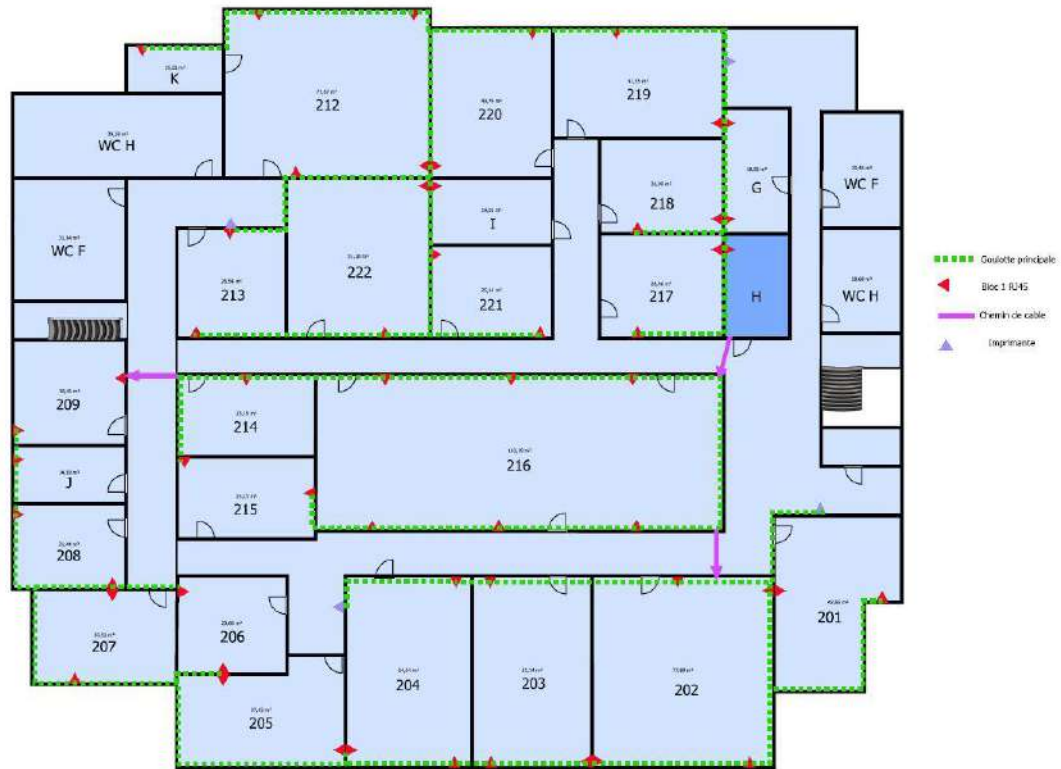
Plan de nos bâtiments

Bâtiment Principal

RDC



1er étage

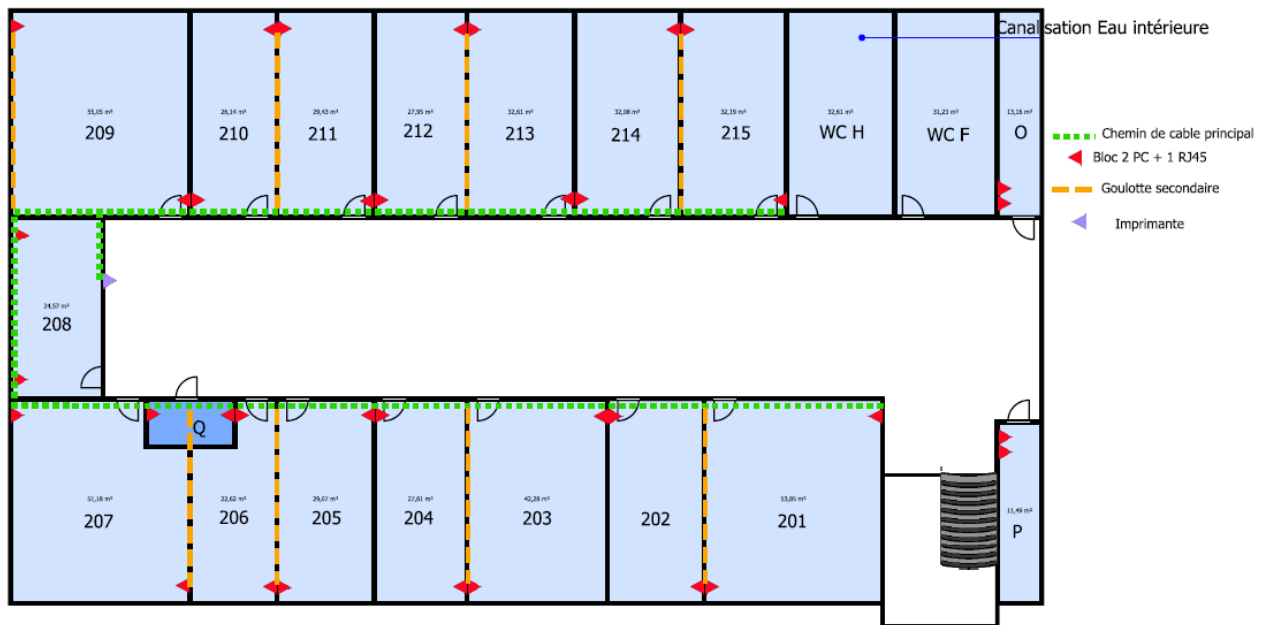


Aile EST

RDC



1er étage



Aile OUEST

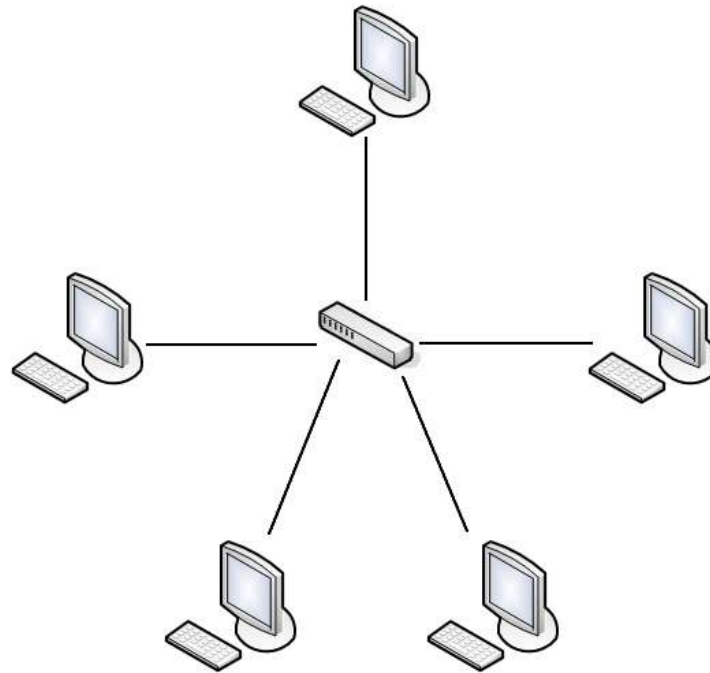
RDC



1er étage



Topologie en étoile



Dans cette topologie les ordinateurs sont reliés à un système matériel central (commutateur, concentrateur, routeur) qu'on appelle le « **nœud** ».

Cette topologie est la plus utilisée car elle est beaucoup moins vulnérable aux déconnexions des éléments composant le réseau. Le seul élément capable de provoquer une interruption du réseau est le switch où sont reliées toutes les connexions.

Avantages : Ajout facile des postes, le débranchement d'une connexion ne paralyse pas le reste du réseau.

Inconvénients : Si le concentrateur est défectueux tout le réseau est en panne.

Nous choisirons donc cette topologie qui répondra aux besoins de notre entreprise afin de raccorder les différents bâtiments et les équipements réseau qui leur sont associés. Pour assurer la continuité de service, nous aurons en spare un deuxième switch préconfiguré, prêt à être mis en place.

Solution retenue

Déménager dans de nouveaux locaux demande également de créer une infrastructure réseau répondant aux besoins de la société.

Nous cherchons à un prix correct une bonne infrastructure et à limiter les problèmes dus aux connexions et perte de liens.

Voici ci-dessous les éléments qui composeront notre réseau.

Présentation des serveurs

Nous avons un serveur maître (Windows Server : AD / DHCP / DNS avec virtualisation du serveur d'impression et du serveur linux (serveur web + ftp)) et un serveur pour la réplication. Nous nous sommes tournés vers DELL car les disques dur sont vendus avec les machines et il y a possibilité de personnaliser le serveur. Nous sommes donc parti sur deux PowerEdge R620 de chez DELL.



Les points forts de ce serveur :

- Optimisez l'efficacité du datacenter avec un moteur de base de données ou de virtualisation ultra dense qui prend en charge jusqu'à 24 disques SSD Flash dans un boîtier 1U.

Caractéristiques techniques :

OS : Windows Server 2012 R2

Processeur : Intel Xeon

RAM : 4 x 8Go

Disque dur : 2 x 900 Go

Pour plus de détails, voir le devis en annexe.

Switch (existant)

HP 2920 48G POE+ SWITCH



Ce switch répondra à nos attentes, c'est un switch « **manageable** » de niveau 3 qui possède 48 ports.

Nous choisirons de placer 1 switch par niveau.

Il permet de se racker sur une baie de brassage 19 pouces.

Il supporte le débit jusqu'à 1GB/s et comprend 4 ports SFP pour une liaison entre les différents bâtiments via une fibre optique grâce aux module GBIC qui leurs seront associés.

Nous anticipons l'arrivée de la To/IP grâce au fait qu'il soit POE, c'est le switch qui donnera l'alimentation électrique via le câble RJ45 au téléphone.

Sa garantie sans limite à vie nous a aussi fortement intéressé.

Baie de Brassage (existant)



Nous avons choisi de mettre en place pour notre cœur de réseau une baie de brassage 19 pouces de 27U.

Cette baie est destinée à recevoir les différents équipements qui serviront à notre cœur de réseau. (Switch, panneaux de brassage, firewall...)

Elle comporte des portes avant et arrière qui sont sécurisées par une serrure dont seuls les membres de l'équipe informatique auront les clés.

Pour les autres bâtiments, nous avons choisi de mettre en place de plus petites baies de brassage mais qui seront amplement suffisantes pour subvenir à nos besoins. Ces baies comportent 12U et seront aussi sécurisées par une serrure.

Chaque baie sera munie d'un panneau de brassage de 48 ports pour relier les switches aux câbles arrivant du mur.

Présentation du Serveur de fichier (évolution de stockage)

Nous prenons un serveur de fichier pour la sécurité des données utilisateurs. Nous nous sommes tourné vers le Dell PowerVault NX3200.



Dell PowerVault NX3200
Processeur : Xeon E5-2609 2.40GHz 4 coeurs.
Mémoire : 2x 8Go 1600MHz.
RAID1 PERC H710 de 2 disques durs 300Go en SAS 10k 3.5" pour le système.
RAID6 PERC H710 de 9 disques durs 600Go en SAS 15k 3.5" pour les données
(4.2To utile).
Alimentation redondée de 750W.
Cartes réseaux : double cartes de 2 port Ethernet chacune.
Garantie 5 ans sur site.

Firewall

Sophos UTM 9



Pour sécuriser notre réseau nous avons décidé de mettre en place un firewall.

Ce dernier servira de bouclier entre le réseau extérieur (WAN) et notre réseau local (LAN).

Il permettra également de servir de proxy pour un filtrage web, mais aussi nous permettra de créer un tunnel VPN.

Le VPN servira à nos commerciaux qui lors de leurs déplacements pourront aisément se connecter sur notre réseau de manière sécurisée via l'application « **Sophos VPN SSL** » qui sera installée sur leurs postes. Ils pourront accéder à leur fichiers dès qu'ils ont une connexion internet.

Toutes les connexions arrivant de l'extérieur passeront obligatoirement par le firewall avant d'entrer sur notre réseau.

Sophos propose également un « **Mail manager** » : tous les mails arrivant de l'extérieur seront scannés et bloqués si le pare-feu détecte quoi que ce soit lui paraissant suspect (comme des virus, logiciels espions ou publicitaires, vers et chevaux de Troie par exemple).

Onduleur



Nous avons choisis l'*Eaton 5PX Rack line-interactive* pour assurer la protection des serveurs, des systèmes de stockage et des équipements réseaux.

Les points fort de cet onduleur :

- Une garantie de 3 ans pour l'électronique et les batteries.
- Mesure de la consommation d'énergie au niveau des groupes de prises.
- Facilité d'utilisation : écran LCD multilingue moderne.
- Onduleur haut rendement: jusqu'à 99%.
- Un facteur de puissance de 0,9 en sortie : plus de watts pour le même nombre de VA.
- Livré avec kit de montage en rack (19").

Nous vous invitons à voir en annexe les caractéristiques de nos équipements.

Choix des salles serveurs

Serveur Windows 1 : Bâtiment principal RDC salle C

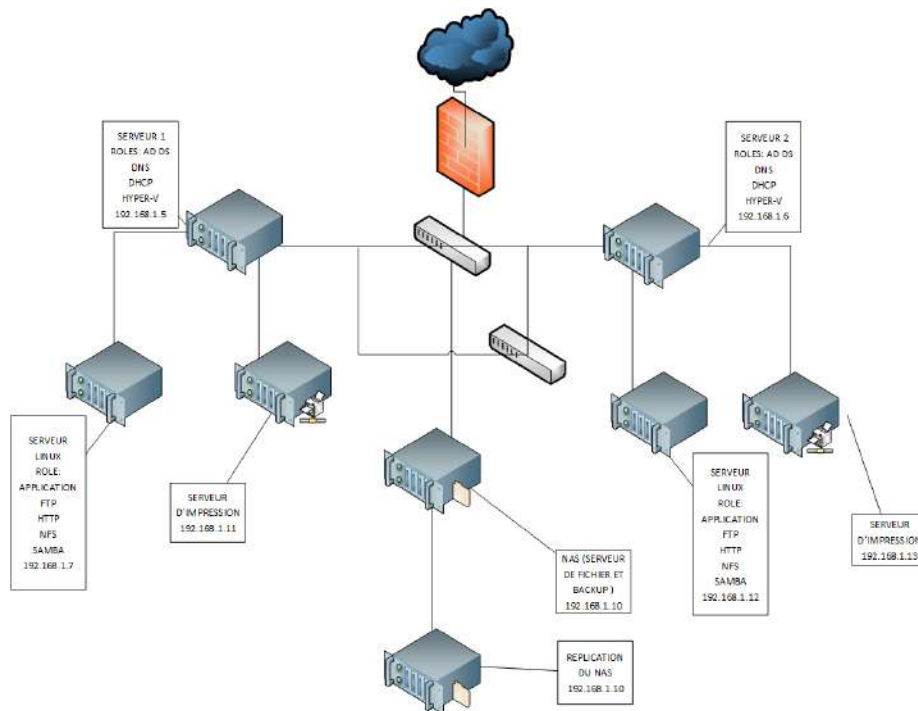
Serveur Windows 2 : Bâtiment EST RDC salle L

Serveur de fichier 1 : Bâtiment principal RDC salle C

Serveur de fichier 2 : Bâtiment Ouest RDC salle T

Ces salles informatique sont dans les normes de sécurité (elles ont été définis dans le projet précédent, par conséquent nous y avons récupéré le matériel présent)

Topologie du réseau



Réseau

Plan d'adressage

- Adresse du réseau : 192.168.1.0/24 192.168.1.2 – 192.168.1.5 = Serveurs
192.168.1.15 – 192.168.1.21 = Imprimantes
- Adresse de Broadcast : 192.168.1.255

Réseau Wi-Fi : 192.168.2.0/24

Adresses IP statiques :

- Routeur = 192.168.1.2
- Serveur 1 (AD + DNS + DHCP) = 192.168.1.5
- Serveur 2 = 192.168.1.6
- Base de données + FTP = 192.168.1.7
- Serveur de fichiers (NAS) = 192.168.1.9
- Serveur d'impression = 192.168.1.11

Wi-Fi



Nous mettons en place un réseau sans-fil afin de permettre à nos collaborateurs et à nos visiteurs autorisés à se connecter à l'Internet. Le Wi-Fi permettra notamment d'obtenir une mobilité accrue pour les utilisateurs d'un ordinateur portable, sera disponible dans les trois bâtiments et principalement utilisé dans les salles de réunion.

Pour cette installation, nous avons besoin de plusieurs points d'accès sans fil qui autoriseront la connexion au réseau local ainsi qu'à l'Internet pour les utilisateurs. Tous les points d'accès seront positionnés au niveau du plafond, d'une part pour éviter les maladresse et malveillances humaines (débranchements, antennes déplacées...) et d'autre part pour simplifier et améliorer le câblage. Nous privilégions les murs côté couloirs et bureaux afin d'étendre la couverture vers l'intérieur plutôt que vers l'extérieur du bâtiment.

Pour des raisons de sécurité, ils seront également éloignés le plus possible des éclairages, des systèmes d'alarme infrarouges, des alimentations électriques,, et des autres éléments perturbateurs éventuels.

Notre choix de points d'accès Wi-Fi s'est porté sur la série 2600 Cisco, modèle idéal pour les petites et moyennes entreprises avec un prix accessible pour une entreprise et une configuration simple.

Récapitulatif

Nous avons retenue cette solution, car elle respecte l'intégrité du cahier des charges;

De plus celle-ci nous permet d'envisager une solution d'évolution dans l'avenir.

Windows Server 2012 R2

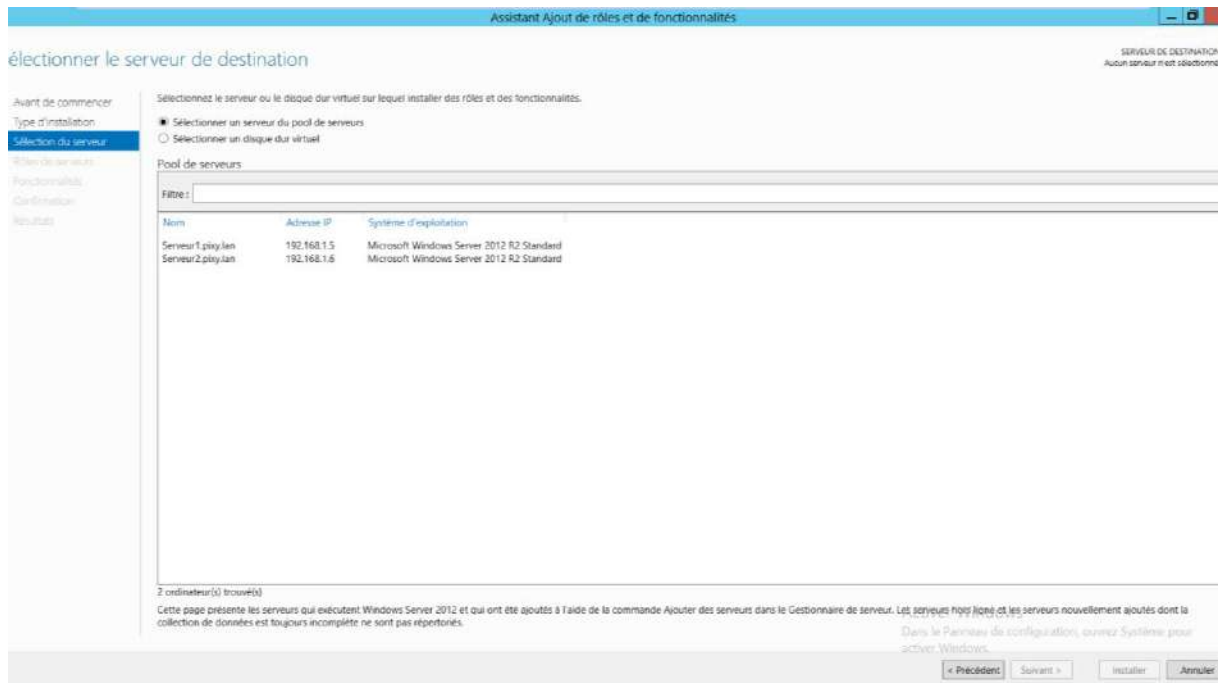
Nous avons choisi d'installer Windows 2012 R2 qui a déjà fait ses preuves tant par sa fiabilité que par son ergonomie. Afin d'assurer l'évolutivité des serveurs, nous nous sommes tournés vers des versions datacenter notamment
L'installation de notre serveur Windows est pleinement détaillé en annexe.

Configuration des rôles :

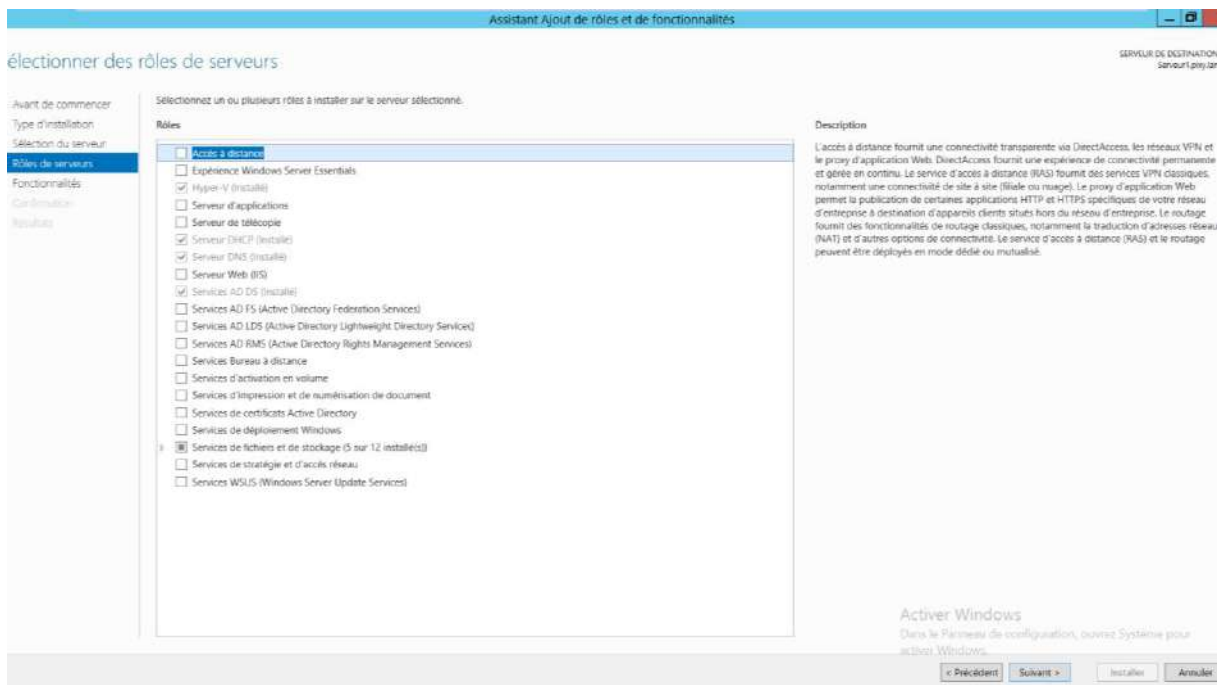
Tout d'abord nous commençons par ajouter les rôles qui nous sont nécessaires.

Voici les étapes pour ajouter des rôles :

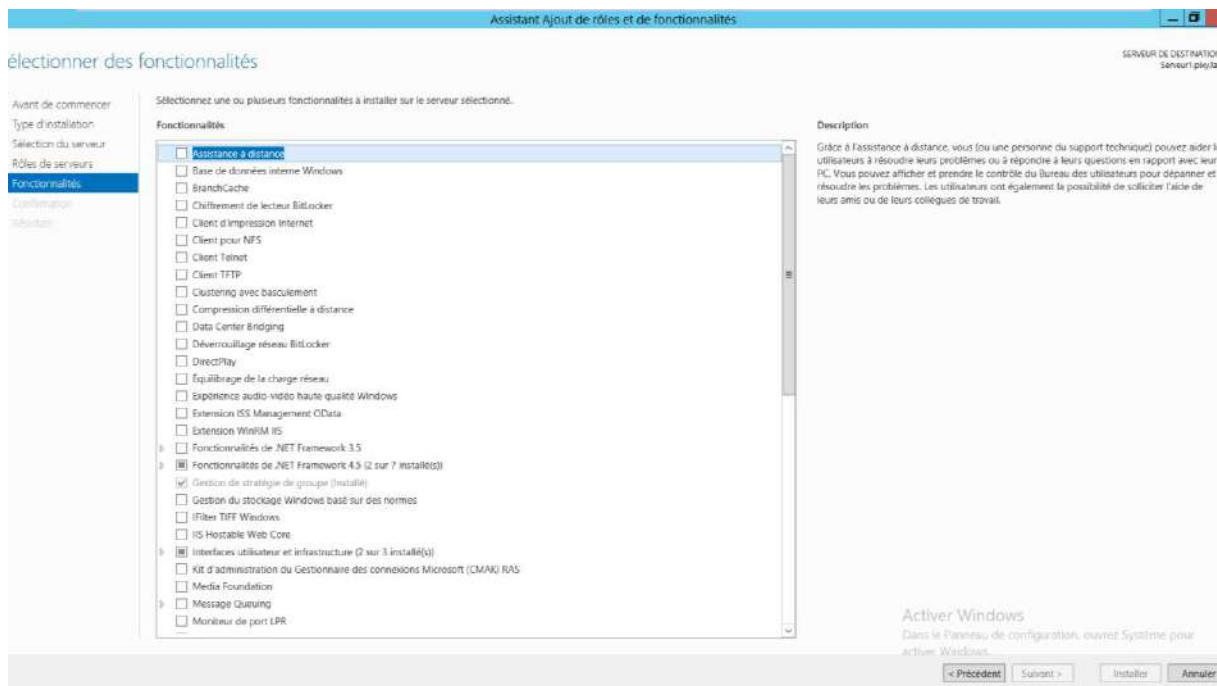




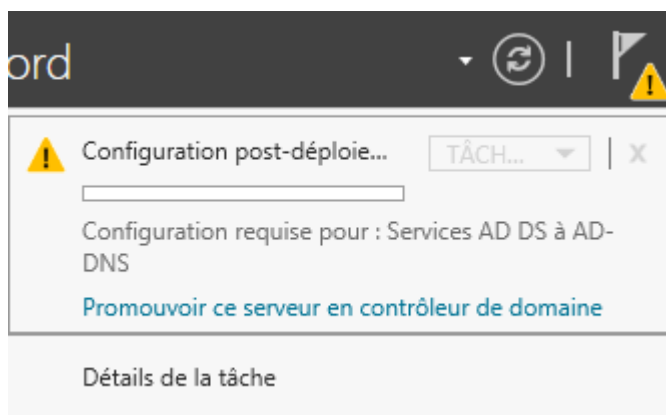
Nous sélectionnons des rôles à installer



Nous sélectionnons des fonctionnalités à installer.



Rôle AD DS



Assistant Configuration des services de domaine Active Directory

Configuration de déploiement

SERVEUR CIBLE
srvdc1

Configuration de déploie...

Options du contrôleur de...

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configur...

Installation

Résultats

Sélectionner l'opération de déploiement

☐ Ajouter un contrôleur de domaine à un domaine existant

☐ Ajouter un nouveau domaine à une forêt existante

☒ Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Nom de domaine racine :

[En savoir plus configurations de déploiement](#)

Neoflow.fr

< Précédent

Suivant >

Installer

Annuler

Assistant Configuration des services de domaine Active Directory

Options du contrôleur de domaine

SERVEUR CIBLE
srvdc1

Configuration de déploie...

Options du contrôleur de...

Options DNS

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configur...

Installation

Résultats

Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine

Niveau fonctionnel de la forêt :

Niveau fonctionnel du domaine :

Spécifier les fonctionnalités de contrôleur de domaine

☒ Serveur DNS (Domain Name System)

☒ Catalogue global (GC)

☐ Contrôleur de domaine en lecture seule (RODC)

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe :

Confirmer le mot de passe :

[En savoir plus options du contrôleur de domaine](#)

Neoflow.fr

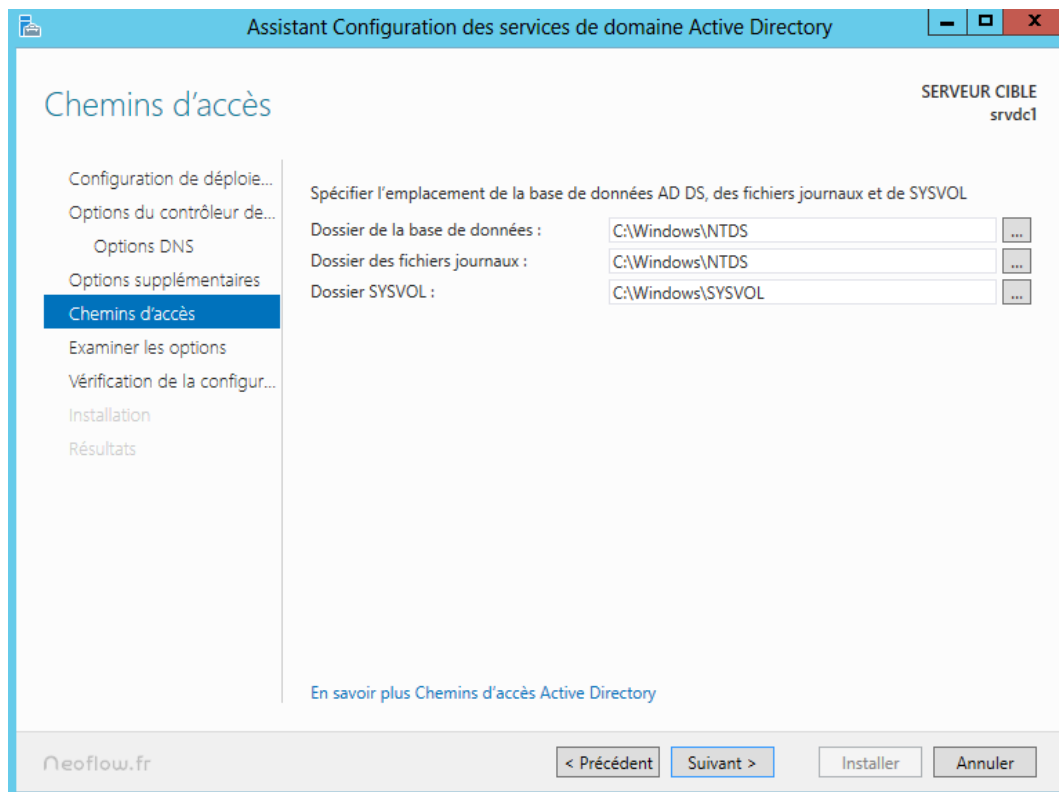
< Précédent

Suivant >

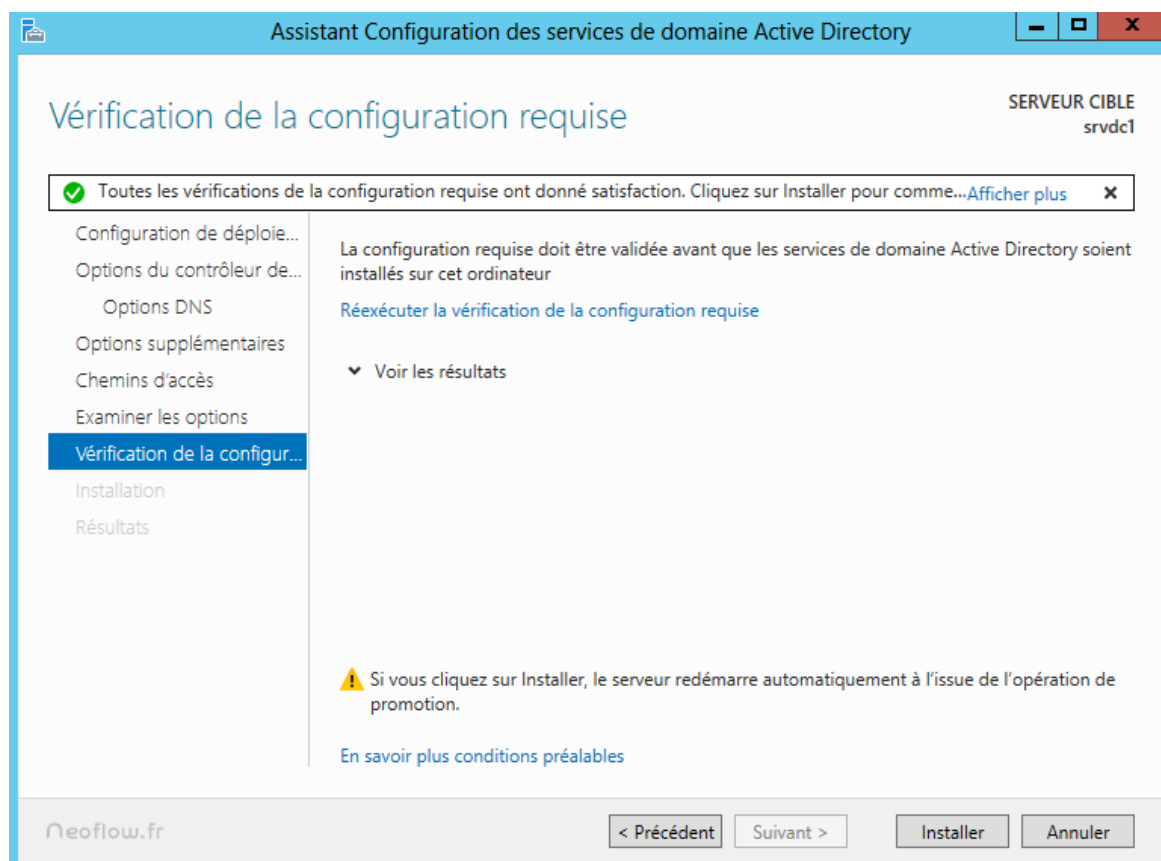
Installer

Annuler

En ce qui concerne les options DNS, 'il n'y a aucune modification à effectuer.



Enfin, 'il n'y a pas d'erreur(s) critique(s) et on clique sur « **Installer** ». Le serveur redémarrera automatiquement une fois le déploiement terminé.



Vous allez être déconnecté

L'ordinateur est redémarré car les services de domaine Active Directory ont été installés ou supprimés.

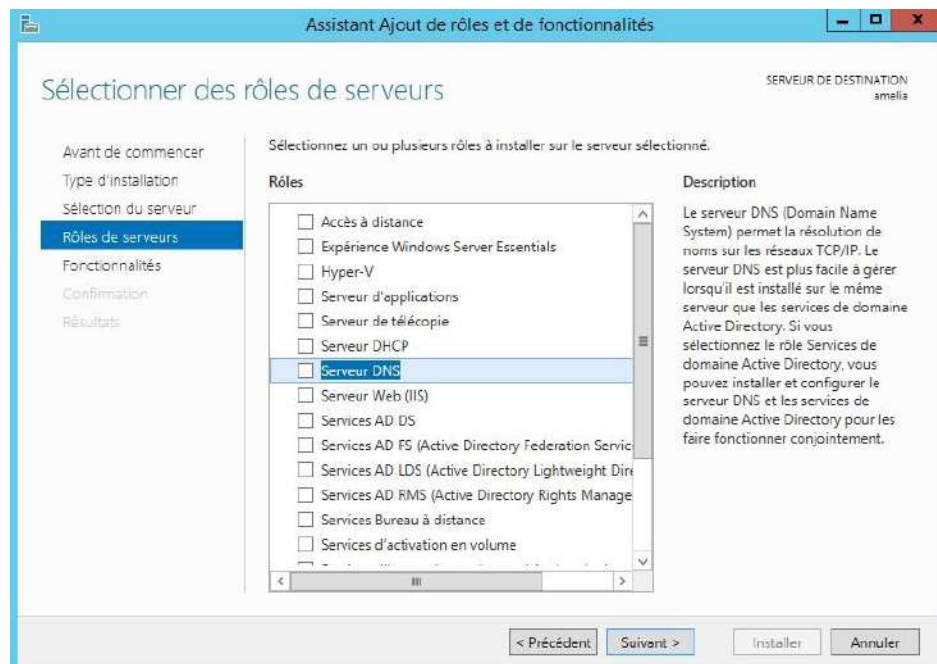
[Fermer](#)

Neoflow.fr

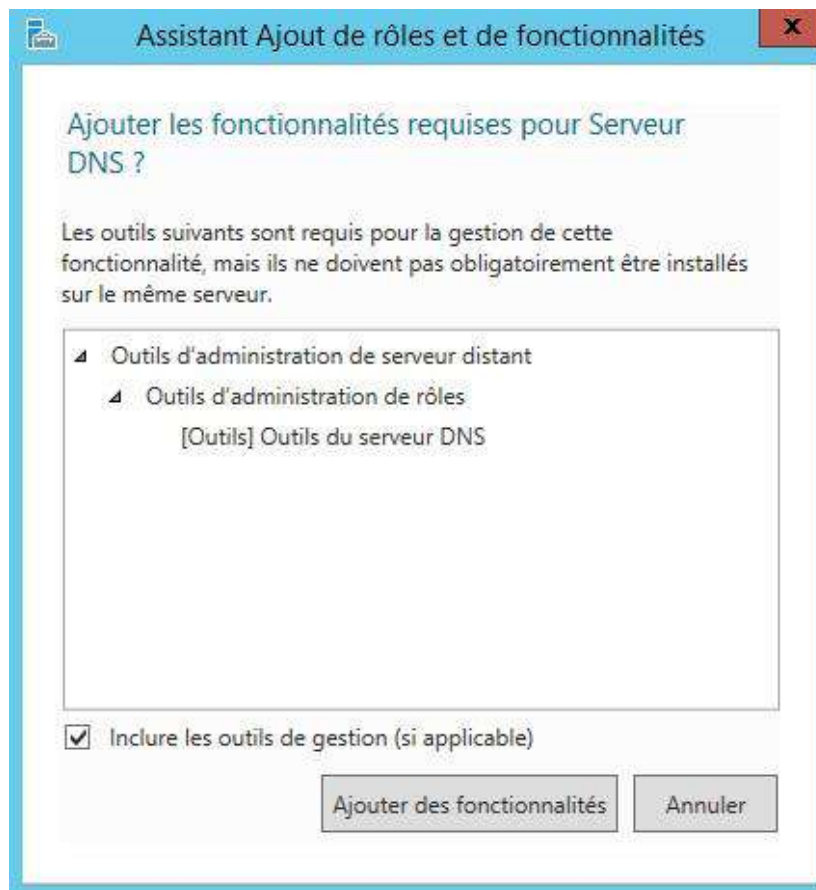
Une fois le serveur redémarré, on se connecte avec le compte Administrateur présent désormais dans l'Active Directory et commencez à administrer votre domaine.

Le Domain Name System (ou DNS, système de noms de domaine) est un service permettant de traduire un nom de domaine en information de plusieurs types qui y sont associés, notamment en adresses IP de la machine portant ce nom.

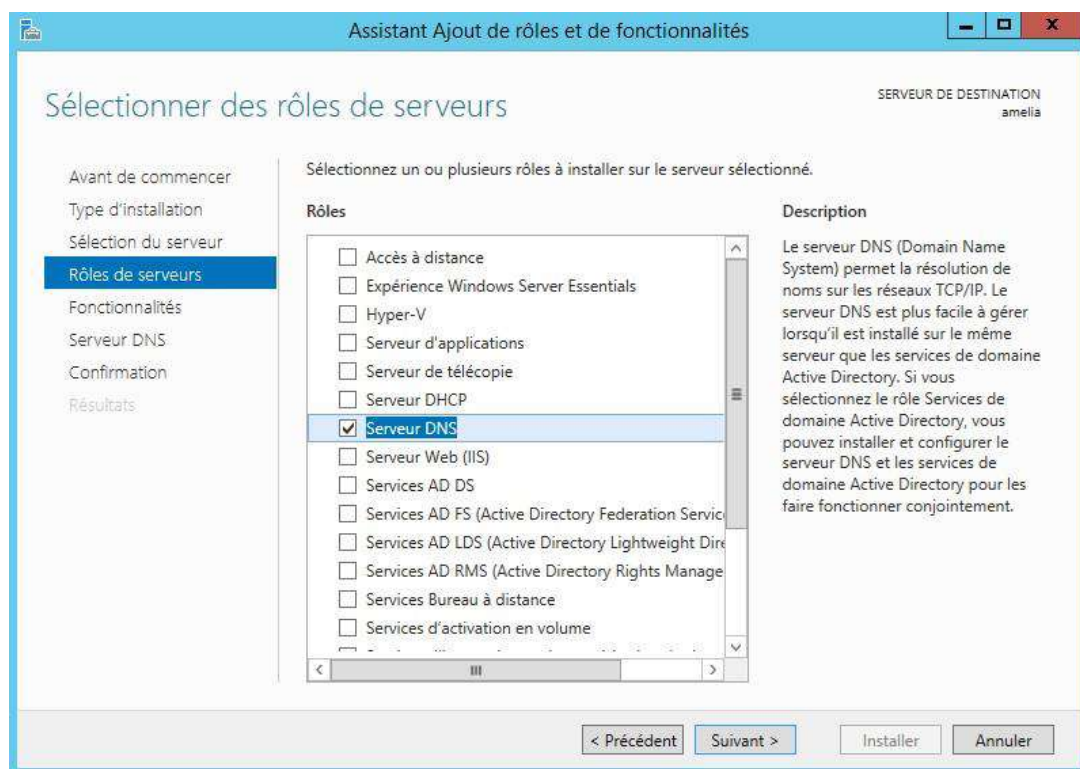
Le prérequis pour l'installation du rôle DNS, est de posséder une adresse IP fixe.



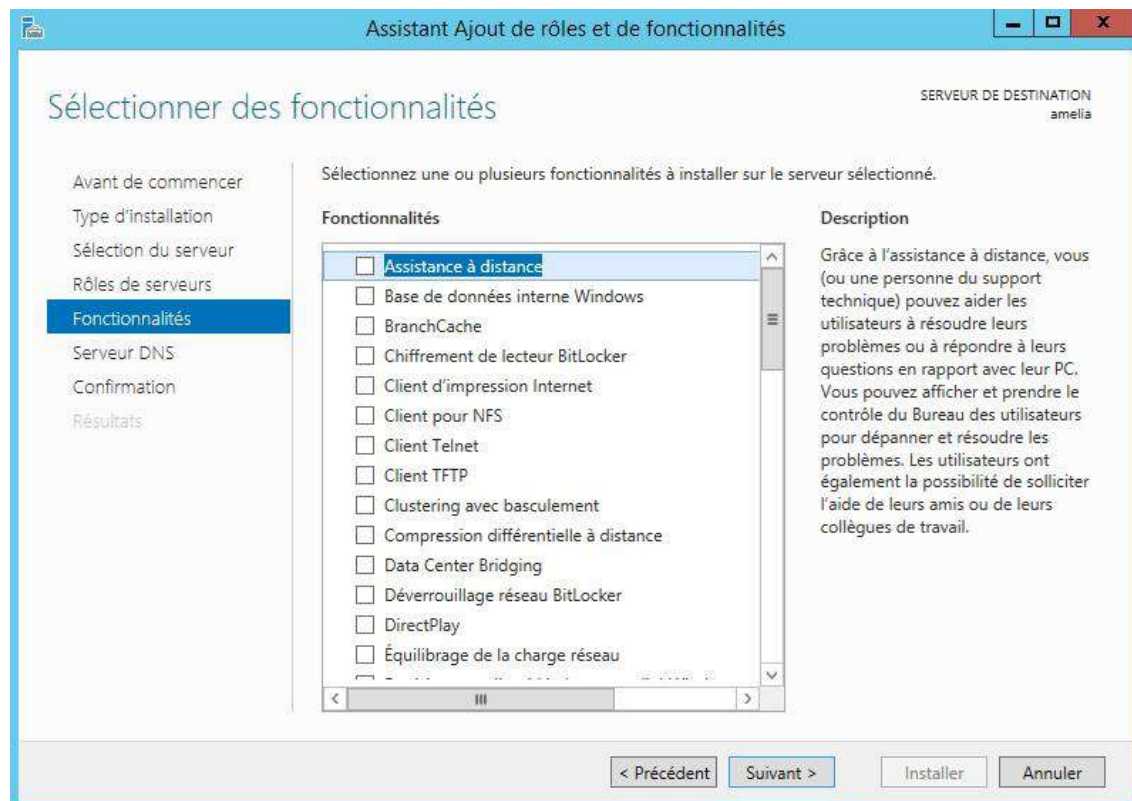
Nous cochons la case « **Serveur DNS** ».



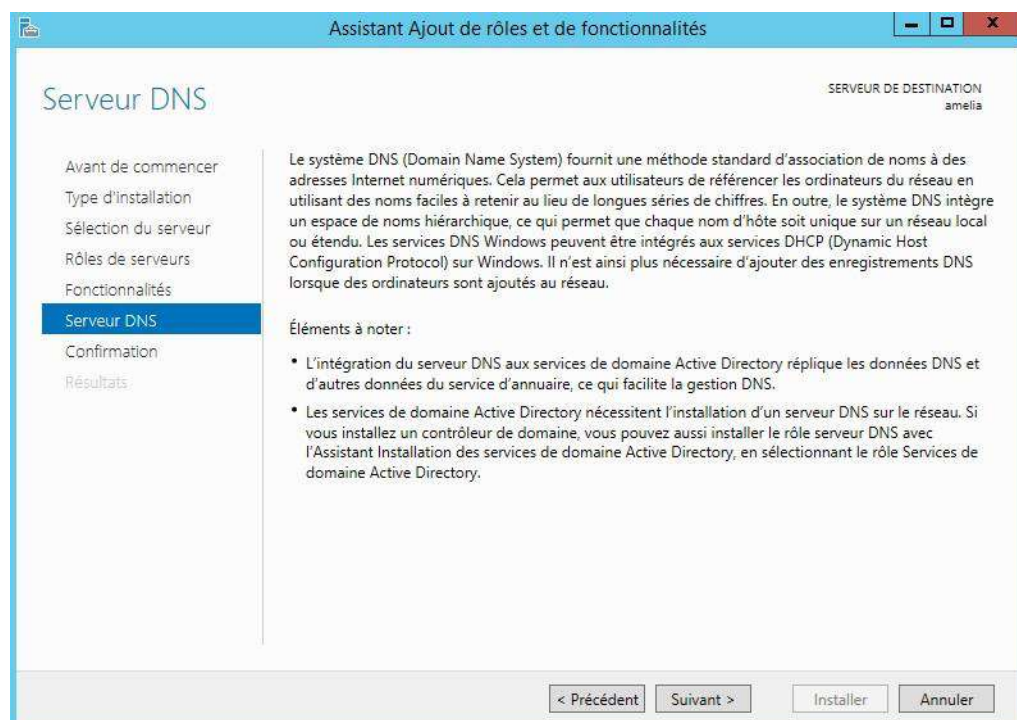
Nous cliquons sur « **Ajouter des fonctionnalités** ».



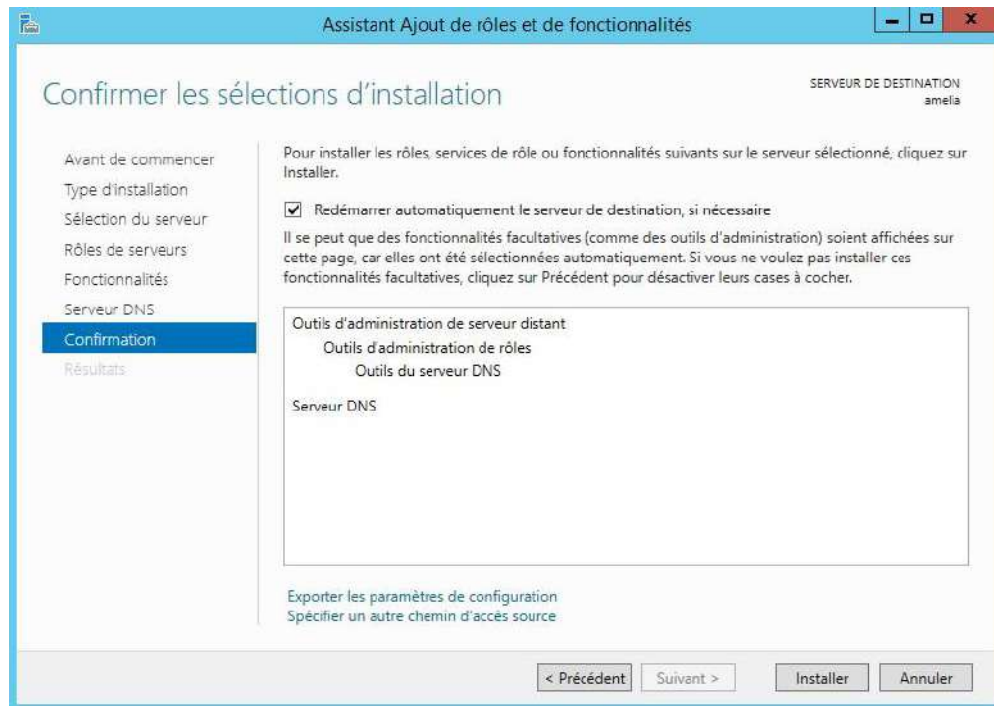
Nous cliquons sur « **Suivant** ».



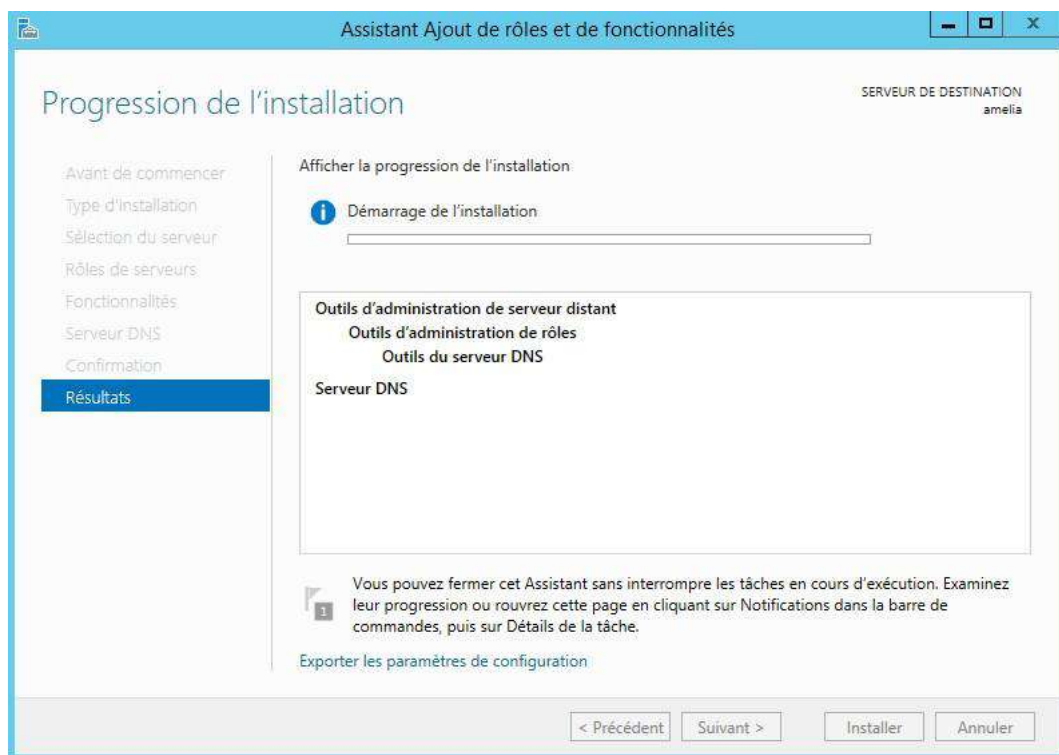
De nouveau cliquez sur « **Suivant** ».



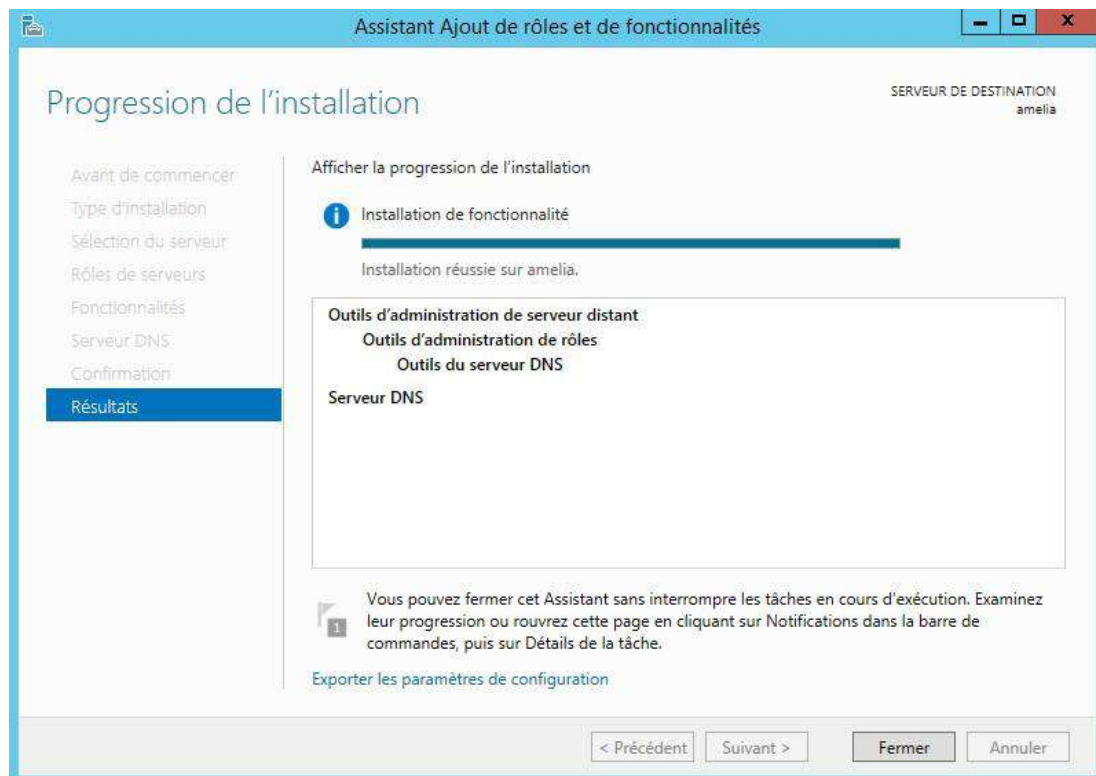
Cliquez sur « **Suivant** ».



Est on clique sur « **Installer** ».



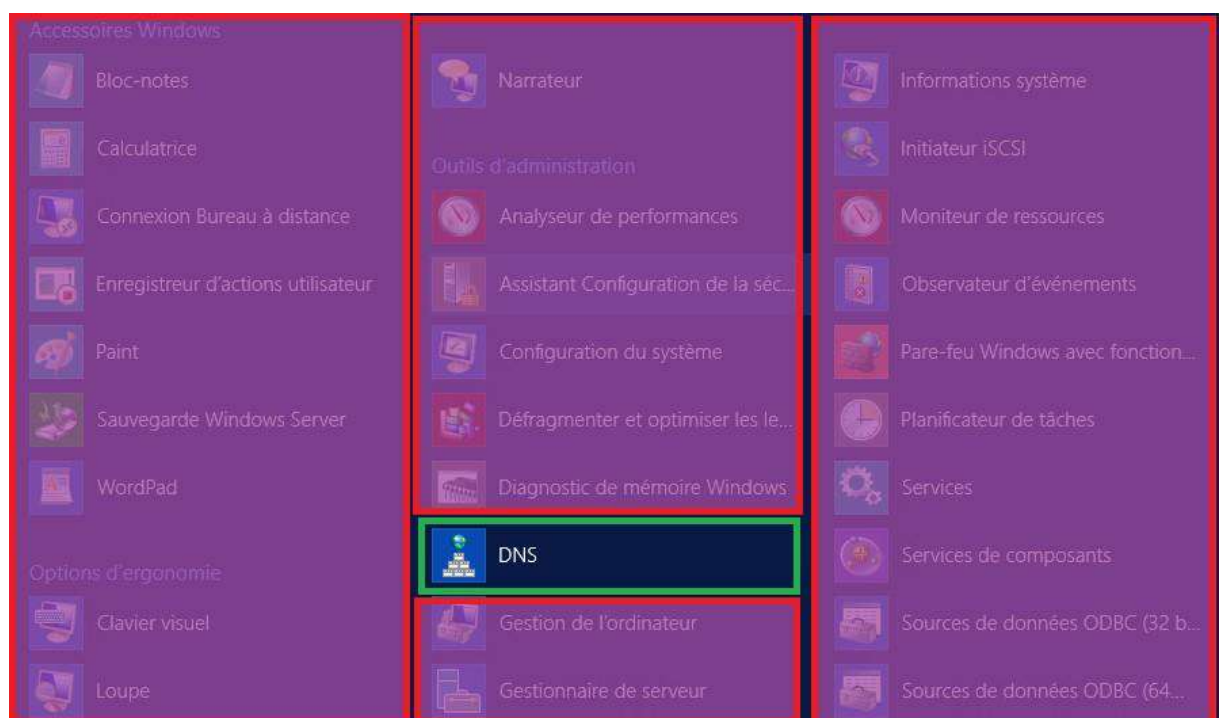
L'installation se lance.



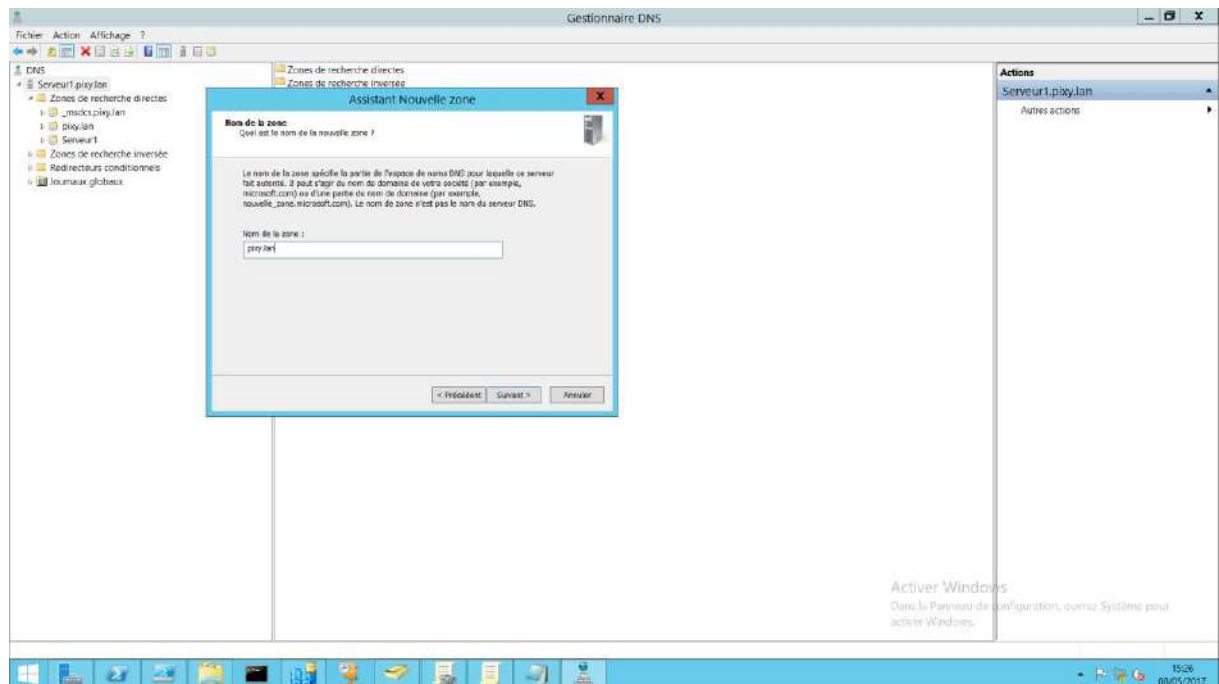
L'installation est terminée. Il faut maintenant configurer le service DNS du serveur.

Rôle DNS

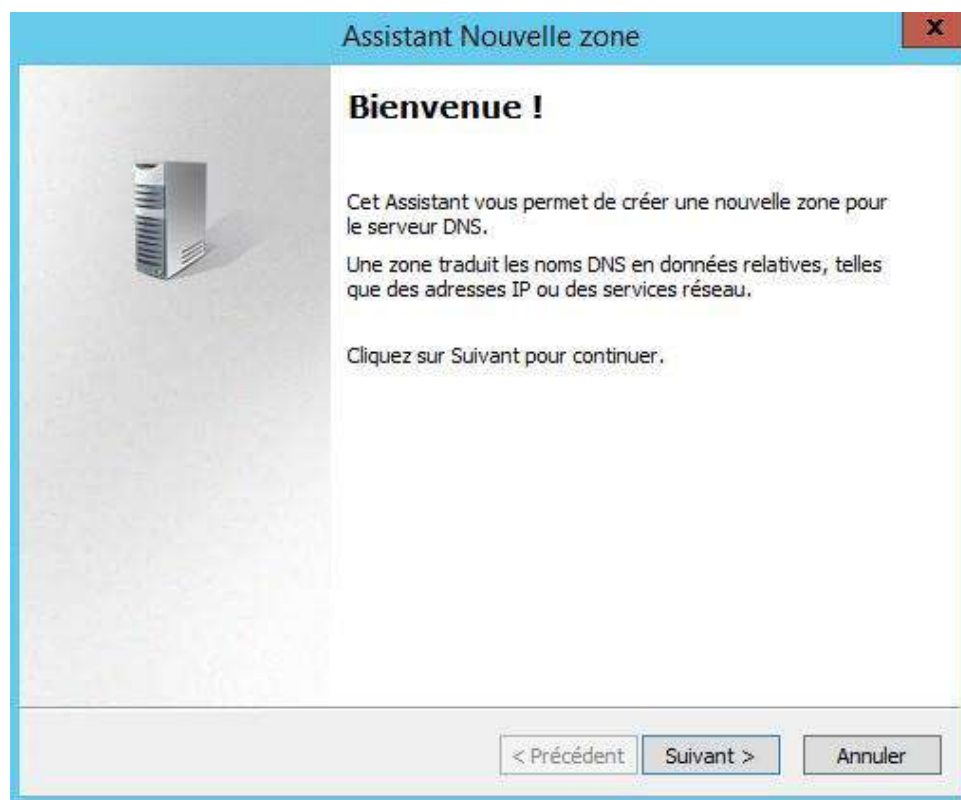
Configuration du DNS



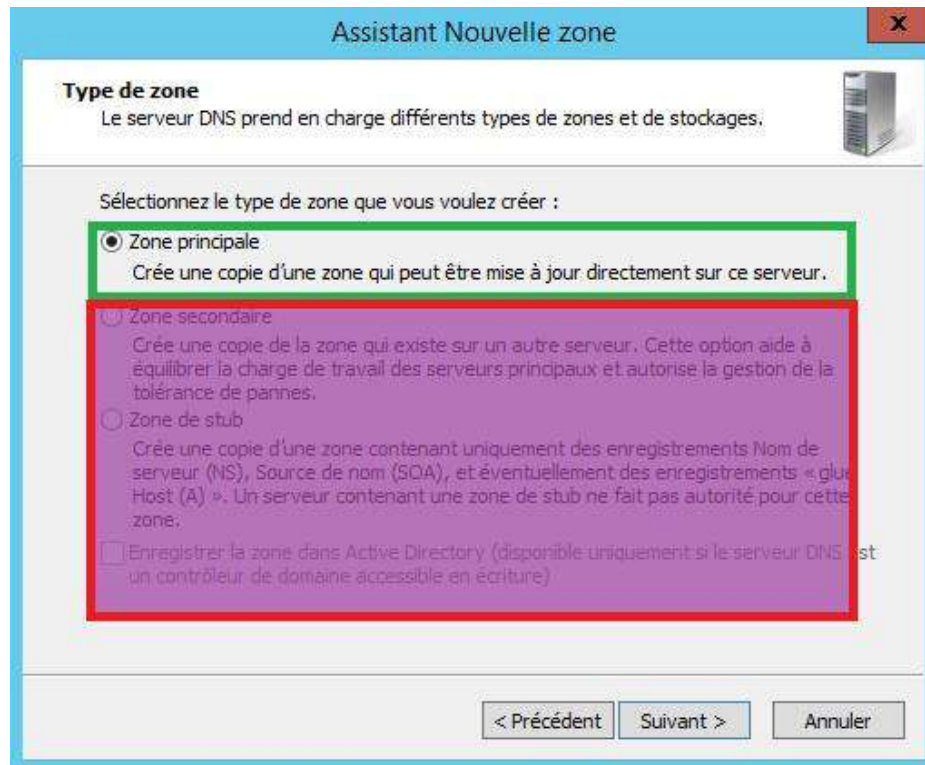
Dans le menu démarrer de Windows Server 2012 R2, on clique sur l'outil d'administration « **DNS** ».



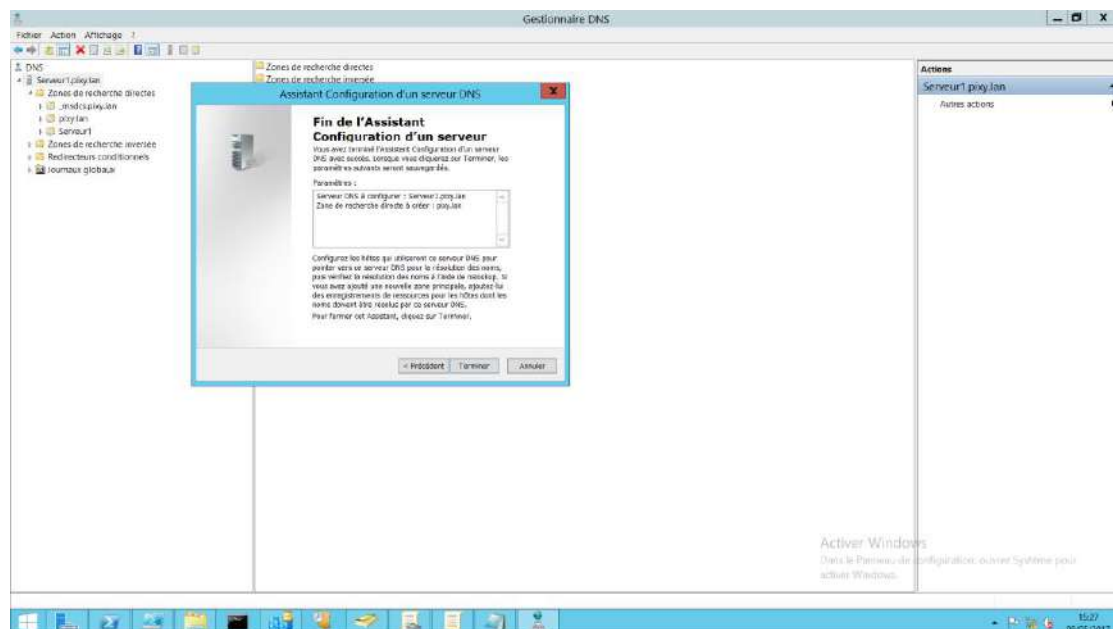
Dans la fenêtre MMC, un clic droit sur « **Zones de recherche directe** » et cliquez sur « **Nouvelle zone...** »



On clique sur « **Suivant** ».

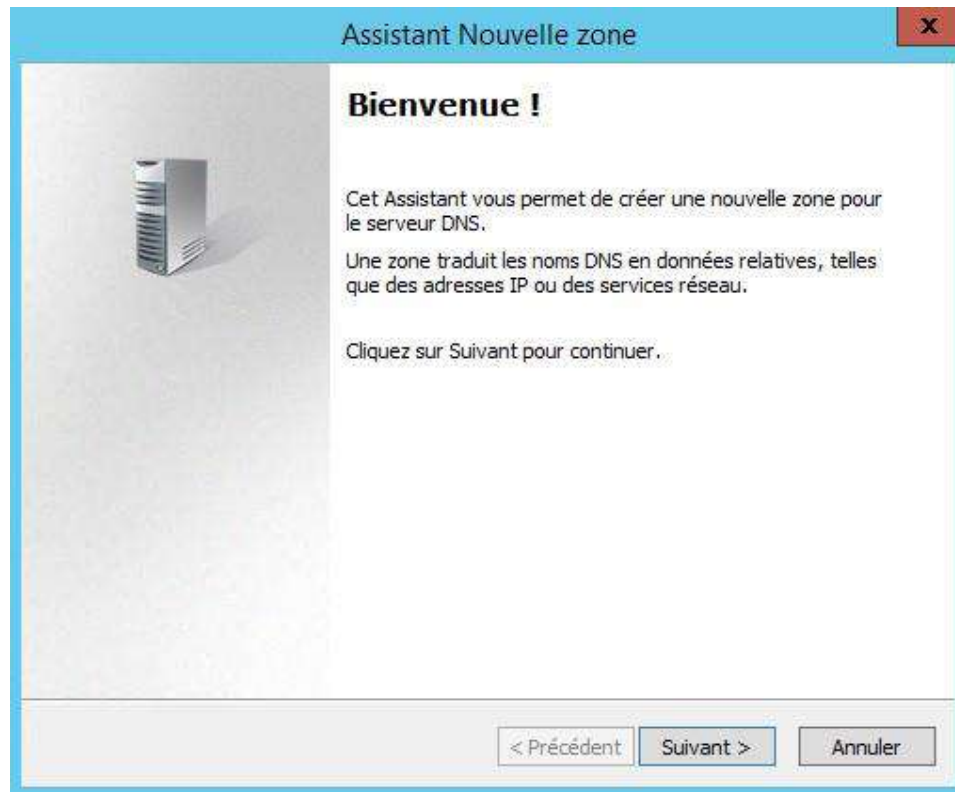


On choisisse la première option « **Zone principale** » et « **Suivant** ».

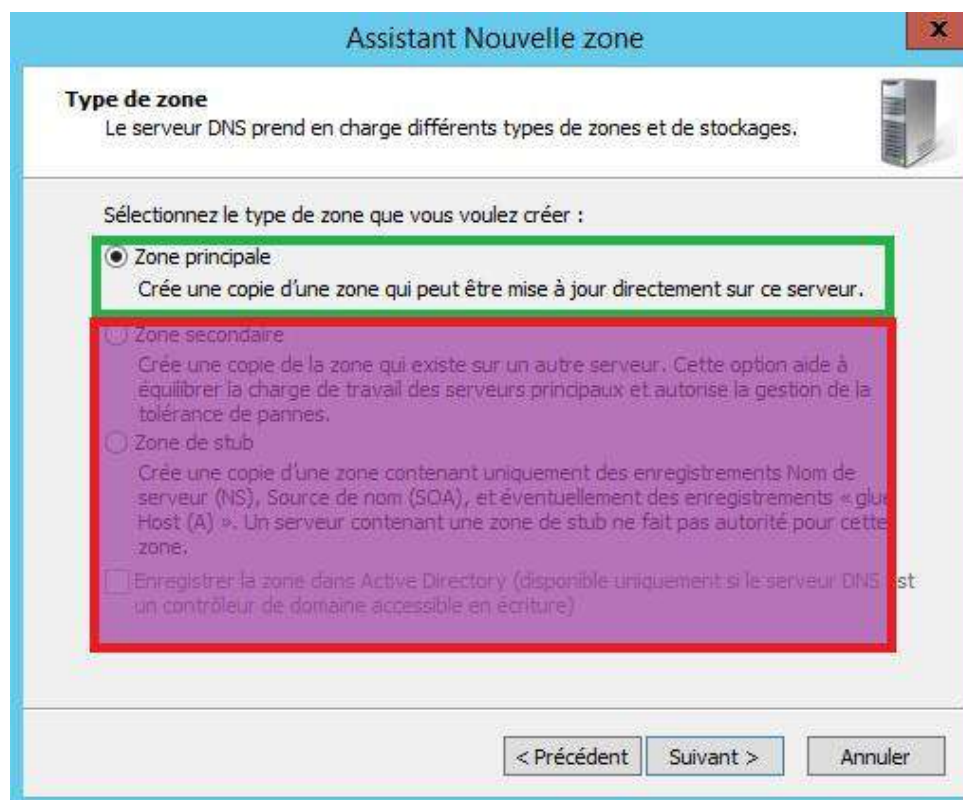


Ensuite « **Terminer** ». Il reste à créer la zone de recherche inversée et son pointeur.

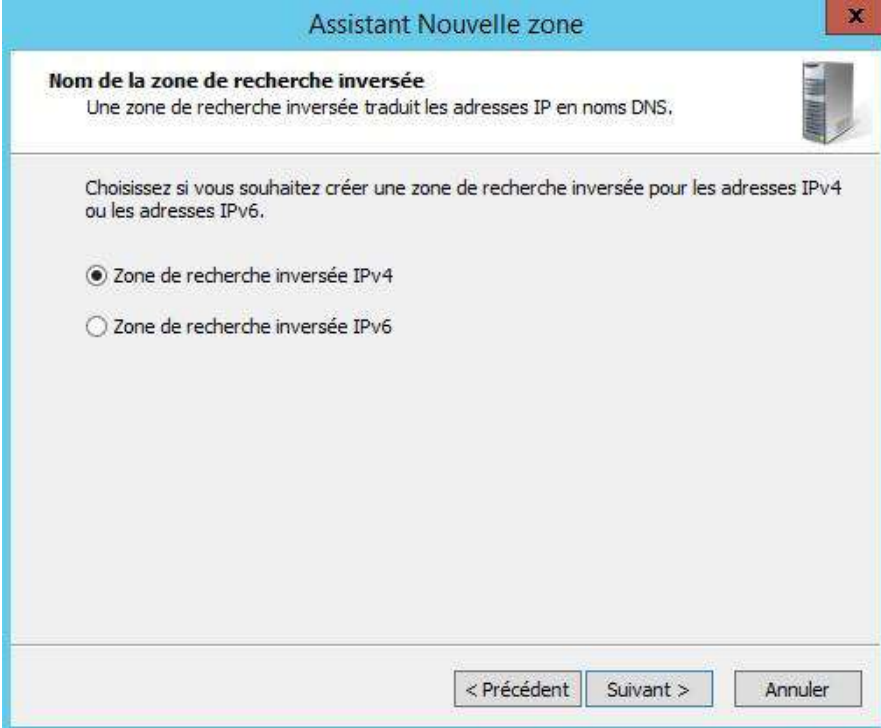
un clic droit sur « **Zones de recherche inversée** » et « **Nouvelle zone...** »



On clique sur « **Suivant** ».



On choisisse la première option « **Zone principale** » et « **Suivant** ».



Assistant Nouvelle zone

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

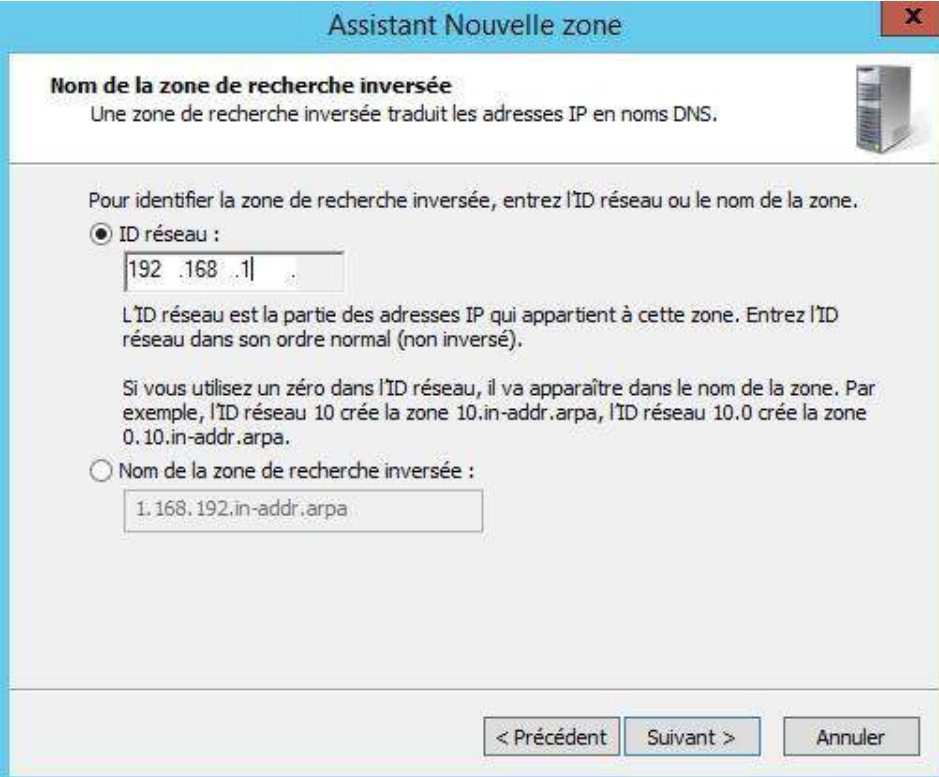
Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4 ou les adresses IPv6.

☒ Zone de recherche inversée IPv4

☐ Zone de recherche inversée IPv6

< Précédent Suivant > Annuler

On prendra la première option « **Zone de recherche inversée IPv4** ». et « **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 :

192.168.1

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

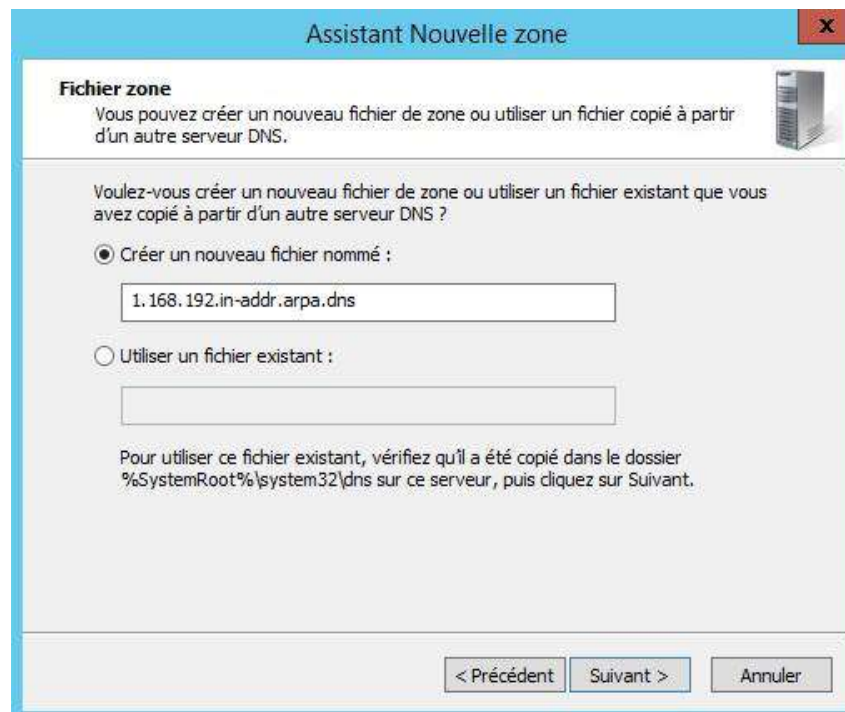
Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

☐ Nom de la zone de recherche inversée :

1.168.192.in-addr.arpa

< Précédent Suivant > Annuler

On entre l'identifiant réseau qui est « **192.168.1** » et « **Suivant** ».



Assistant Nouvelle zone

Fichier zone
Vous pouvez créer un nouveau fichier de zone ou utiliser un fichier copié à partir d'un autre serveur DNS.

Voulez-vous créer un nouveau fichier de zone ou utiliser un fichier existant que vous avez copié à partir d'un autre serveur DNS ?

☒ Créer un nouveau fichier nommé :

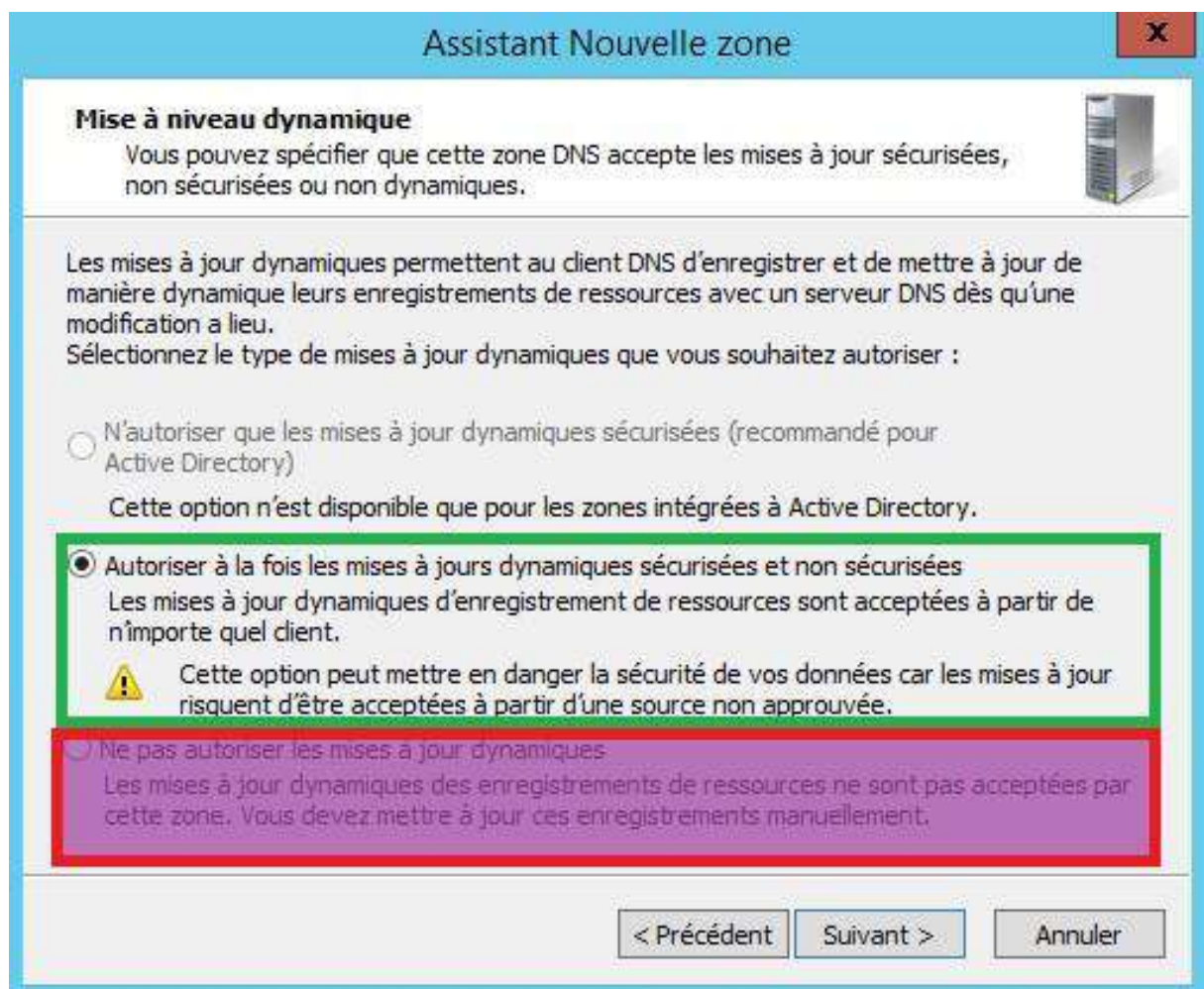
1.168.192.in-addr.arpa.dns

☐ Utiliser un fichier existant :

Pour utiliser ce fichier existant, vérifiez qu'il a été copié dans le dossier %SystemRoot%\system32\dns sur ce serveur, puis cliquez sur Suivant.

< Précédent Suivant > Annuler

On laisse le nom enregistré et « **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 :

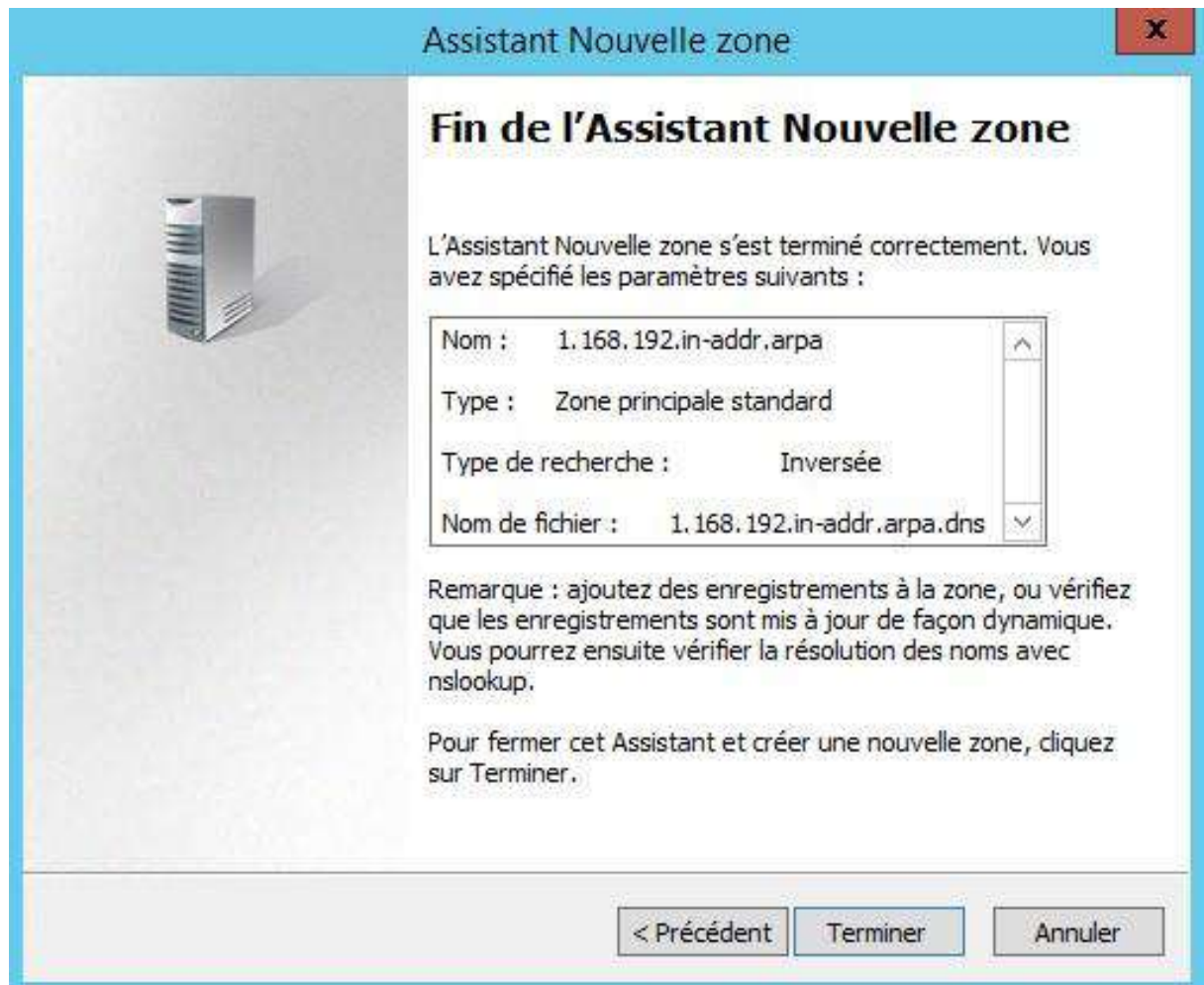
☐ N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)
Cette option n'est disponible que pour les zones intégrées à Active Directory.

☒ 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.

< Précédent Suivant > Annuler

On choisisse la première option non grisée « **Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées** ».



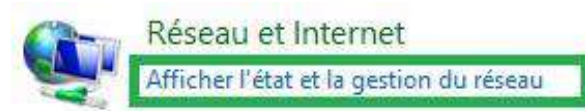
On clique sur « **Terminer** ». La zone de recherche inversée est créée, il ne reste que le pointeur à mettre.

Dans l'arborescence du DNS, clic droit sur notre zone de recherche inversée, ici « **1.168.192.in-addr.arpa** » et « **Nouveau pointeur** ».

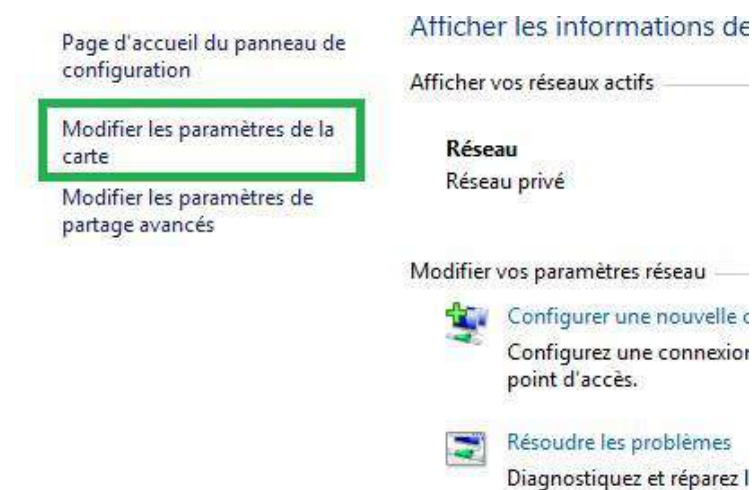
On y renseigne l'adresse IP de notre serveur et le nom d'hôte complet (nomdelamachine.nomdudomaine). Et ensuite sur « **OK** ».

Vérification du DNS par NSLOOKUP

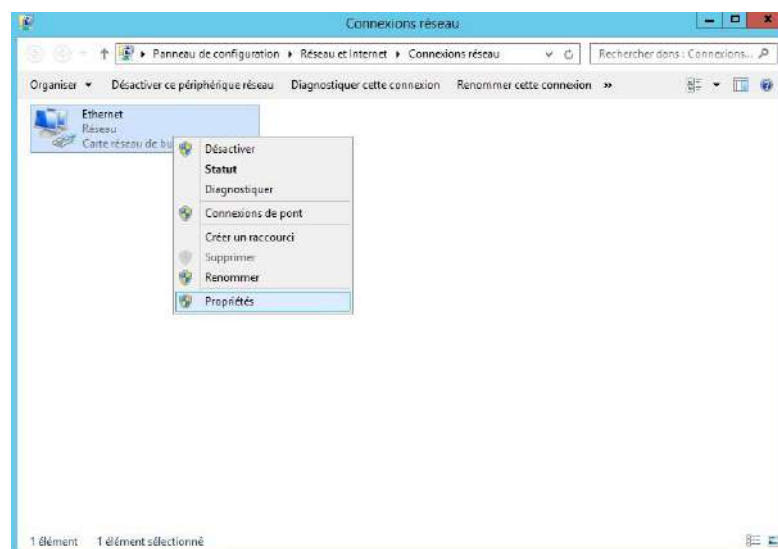
Pour vérifier que notre DNS fonctionne, on définit notre serveur comme DNS principal dans les paramètres de sa carte réseau. Pour cela, dans les paramètres TCP/IP de notre carte. Pour ce faire, « **Panneau de configuration** ».



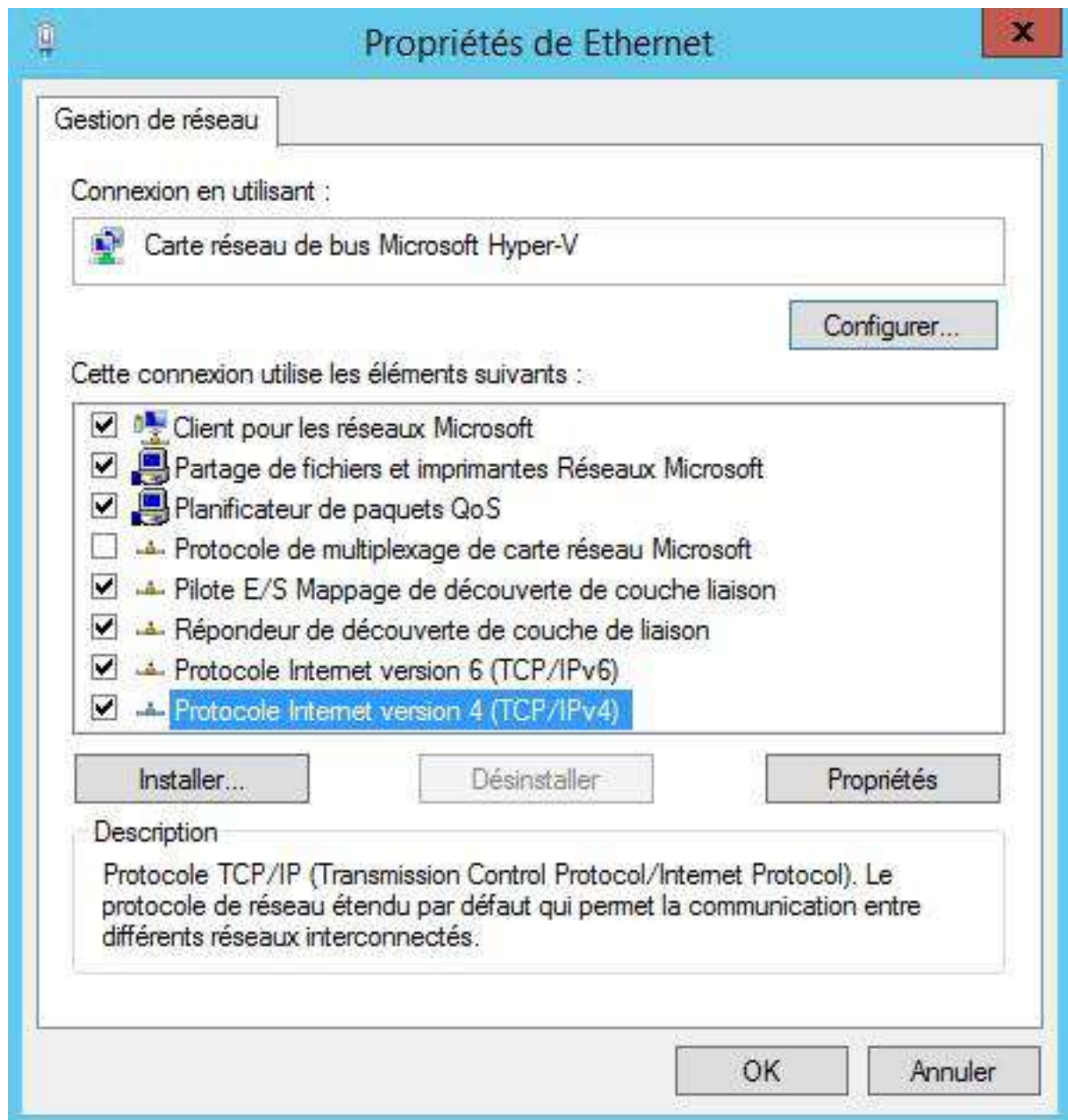
On clique sur « **Afficher l'état et la gestion du réseau** » en dessous de « **Réseau et Internet** ».



En haut à gauche, sur « **Modifier les paramètres de la carte** ».



un clic droit sur notre carte réseau et sur « **Propriétés** ».



Dans les propriétés du protocole, on renseigne le serveur DNS préféré avec l'adresse IP de notre serveur. Ensuite faite « **OK** »

On lance « **nslookup** » avec le CMD.

Le résultat de la commande nous indique que nous avons correctement configuré le DNS.

```
> serveur1
Serveur :   serveur2.pixy.lan
Address:   192.168.1.6

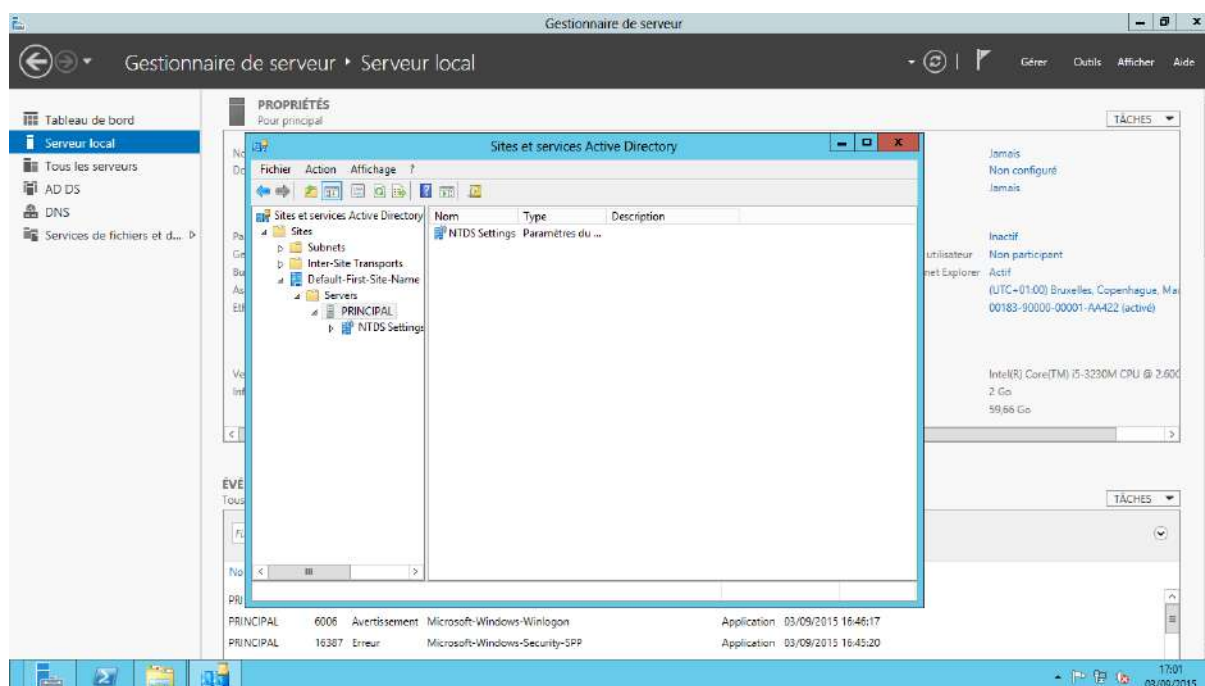
Nom :      serveur1.pixy.lan
Address:   192.168.1.5

> serveur2
Serveur :   serveur2.pixy.lan
Address:   192.168.1.6
```

Réplication du serveur 2 (Site et service AD)

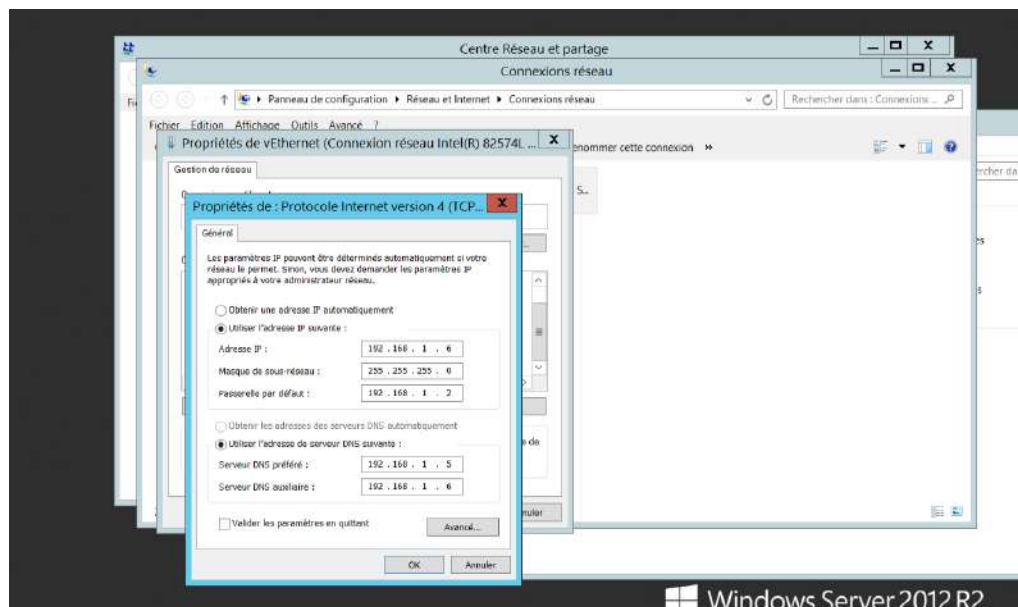
Après avoir redémarré une seconde fois, l'Active Directory est maintenant installé ainsi que le serveur DNS. Il est alors impératif de passer en IP fixe. Pour se faire, un simple « **ipconfig** » tapé dans l'invite de commande vous donne les renseignements voulus. La suite se passe dans les paramètres de la carte réseau, où il faut renseigner les champs vides. **Centre réseau et partage** > **connexion réseau** > **ethernet0** > **propriété IPv4**.

Dernière étape avant de passer sur le serveur secondaire. Rendez-vous dans « **site et services Active Directory** » afin de vérifier que notre contrôleur de domaine apparaît bien.

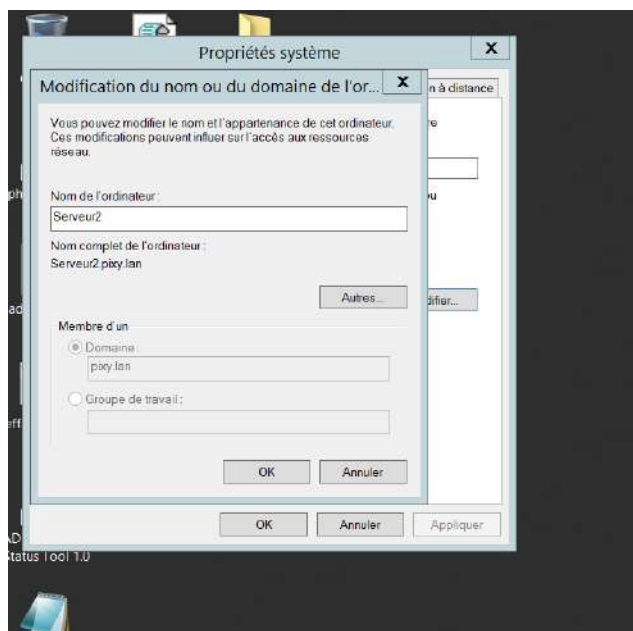


Installation et réplication du second contrôleur de domaine

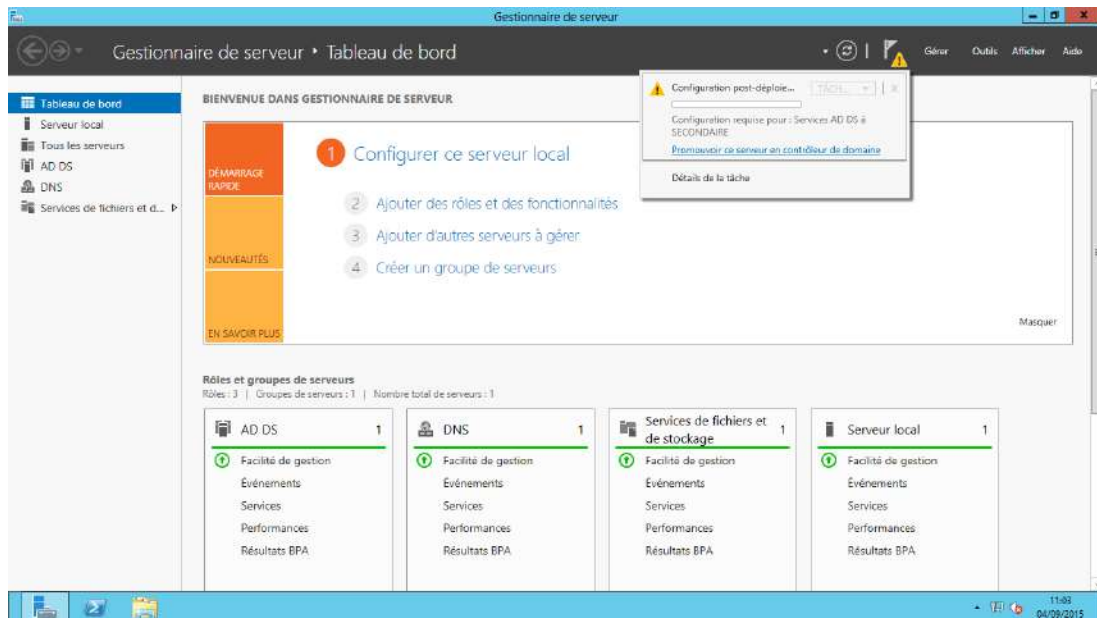
Nous sommes maintenant sur le serveur secondaire où il faut également fonctionner en IP fixe. On indique l'IP du serveur DNS (notre serveur principal) !



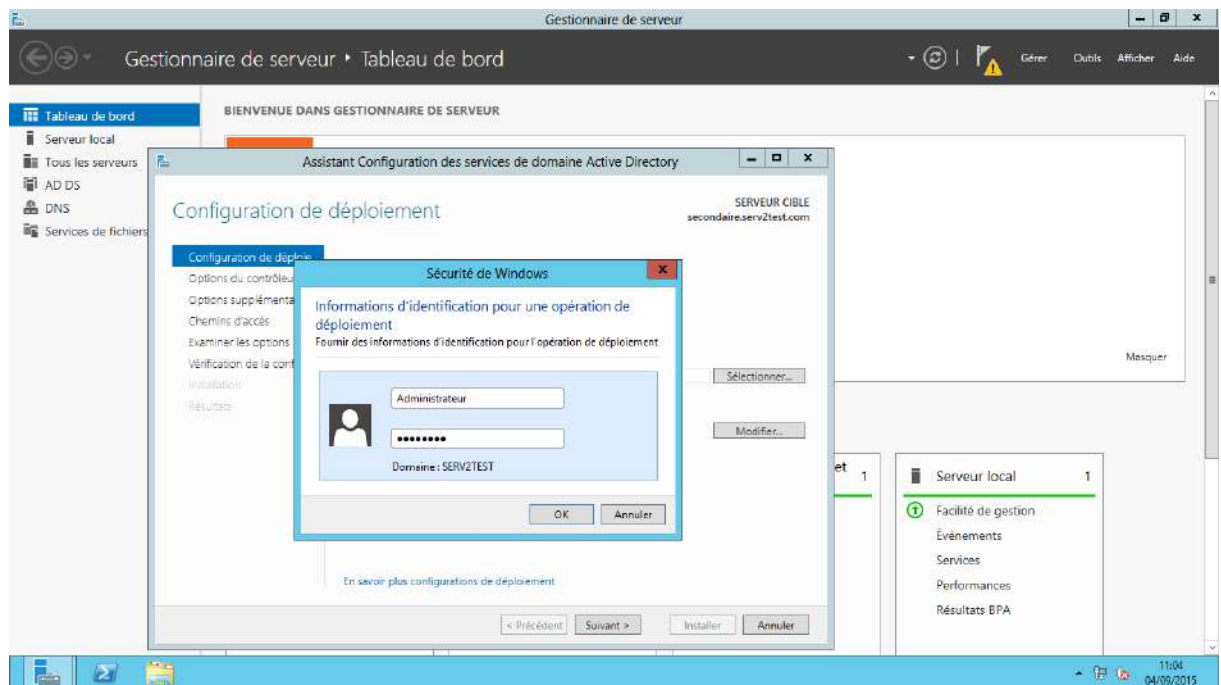
Après avoir fini, on peut dès à présent rejoindre le domaine. Pour cela, il faut donc spécifier que l'on est bien membre du domaine « **pixy.lan** » et se connecter avec le compte administrateur de la session.



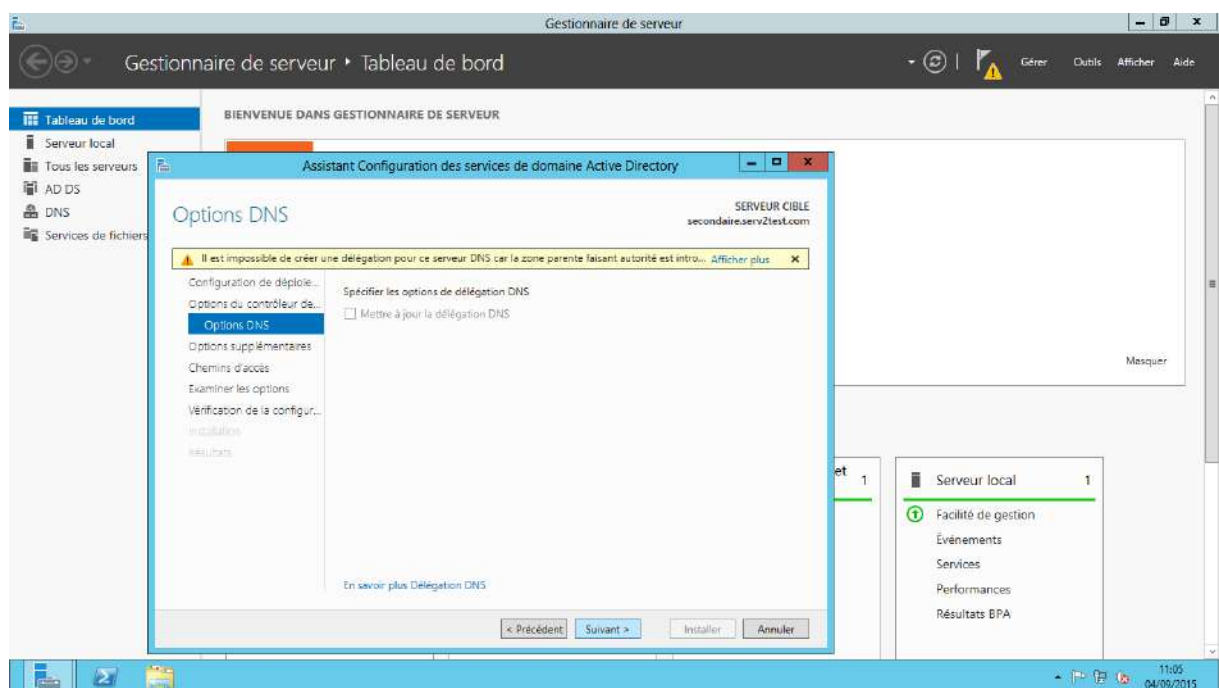
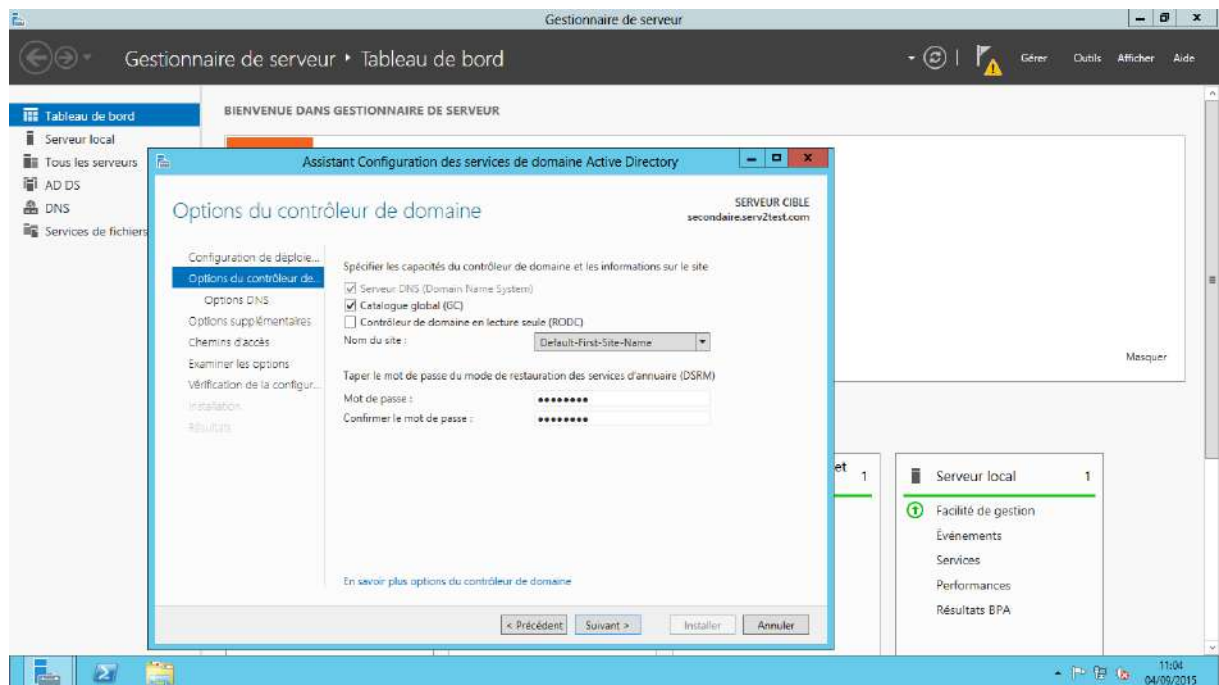
Ici, nous nous retrouvons au même point que tout à l'heure, après avoir installé les services « **ADDS** ». Une fois encore, il faut se rendre dans le centre de notifications où il nous est proposé de passer le serveur en contrôleur de domaine.



On arrive alors dans un environnement sensiblement similaire à celui que nous avons avec le premier serveur, toutefois, avec quelques différences. Après avoir cliqué sur « **modifier** » on renseigne à nouveau l'utilisateur et le mot de passe.

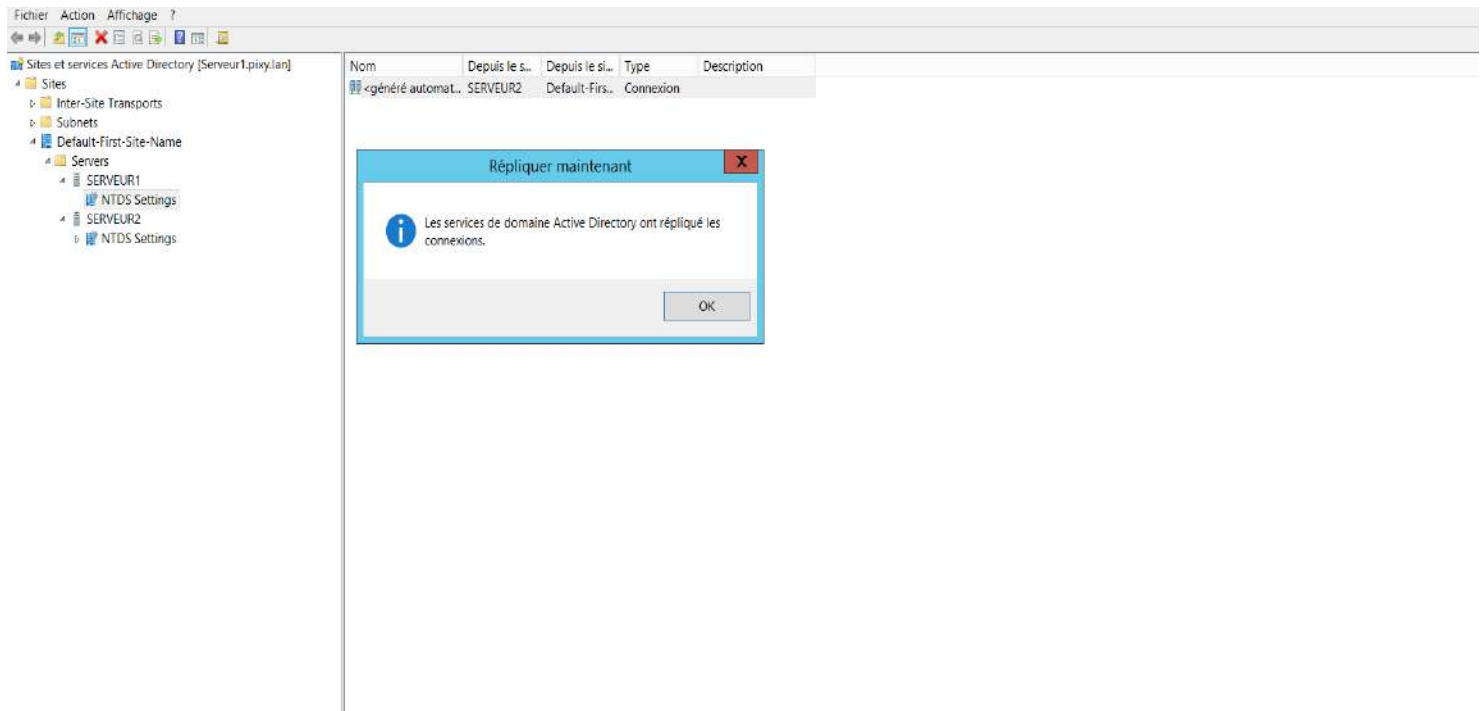


Dans les options du contrôleur de domaine il y a juste besoin de créer un mot de passe pour la restauration des services d'annuaire.

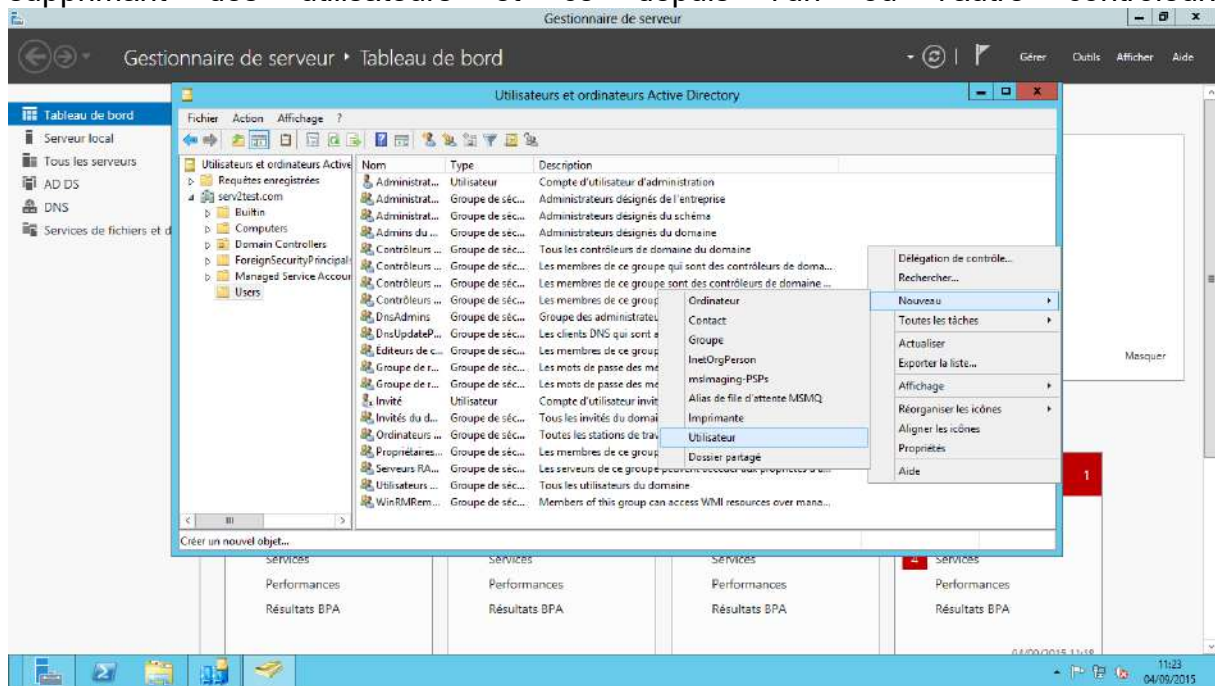


Dans les « **options supplémentaires** » On sélectionne le premier contrôleur de domaine afin d'indiquer au second contrôleur, d'où il devra répliquer l'active directory.

Une fois notre serveur redémarré, On va dans « **site et services Active Directory** » afin de vérifier si les deux serveurs sont présents. Dès lors, on peut sélectionner les paramètres des deux contrôleurs, puis **clic droit** et « **Répliquer** ».



Une fois cette étape terminée, on peut vérifier si l'opération fonctionne en créant / supprimant des utilisateurs et ce depuis l'un ou l'autre contrôleur.

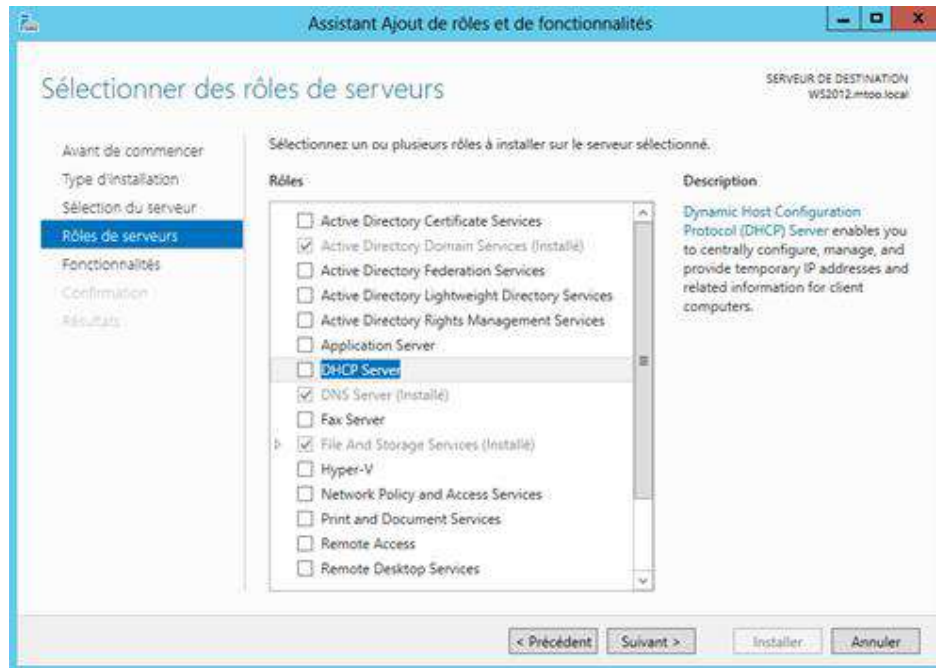


Les deux Active Directory fonctionnant en miroir.

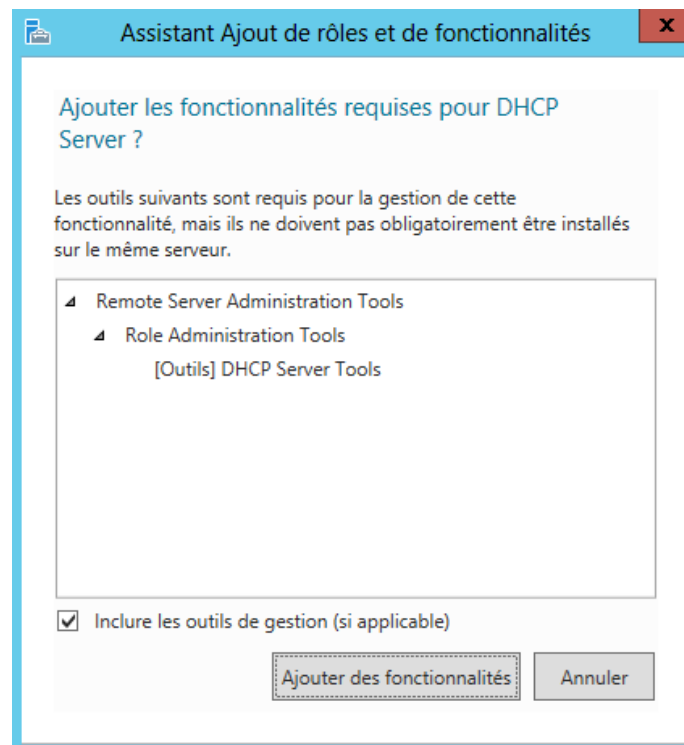
Rôle DHCP

Pour ajouter le rôle DHCP , On passe par l'assistant de gestion des Rôles.

« DHCP Server » :



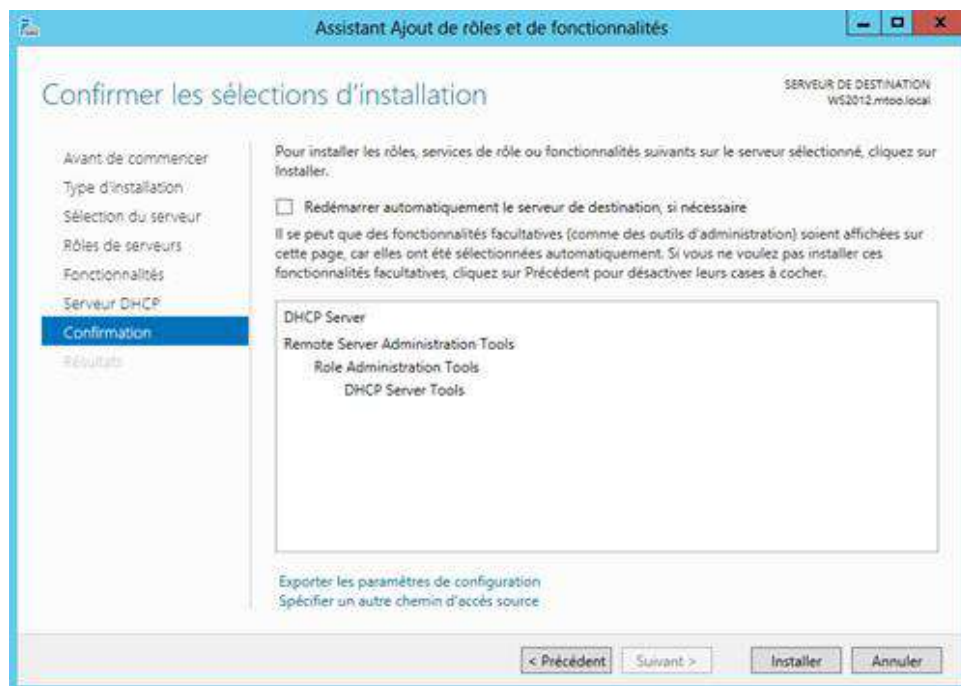
Cela provoque l'ajout des fonctionnalités suivantes.



Il s'agit de la console d'administration, on clique sur « **Ajouter des fonctionnalités** ».

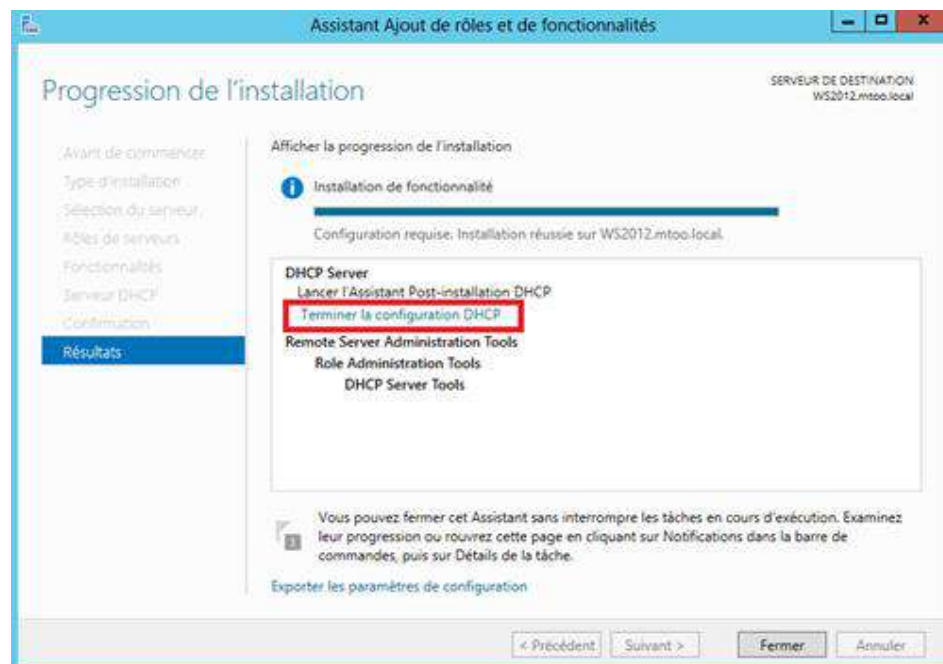
Comme pour Active Directory, il est important que notre serveur possède une adresse IP fixe.

Un écran vous rappelle les opérations effectuées.

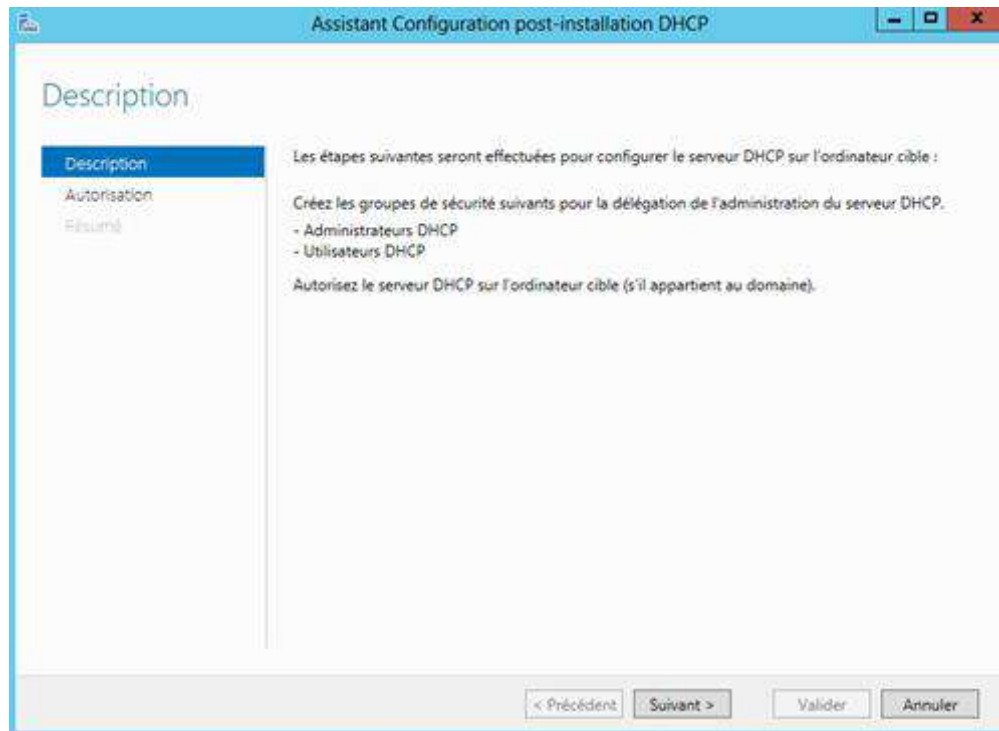


On clique sur « **Installer** ».

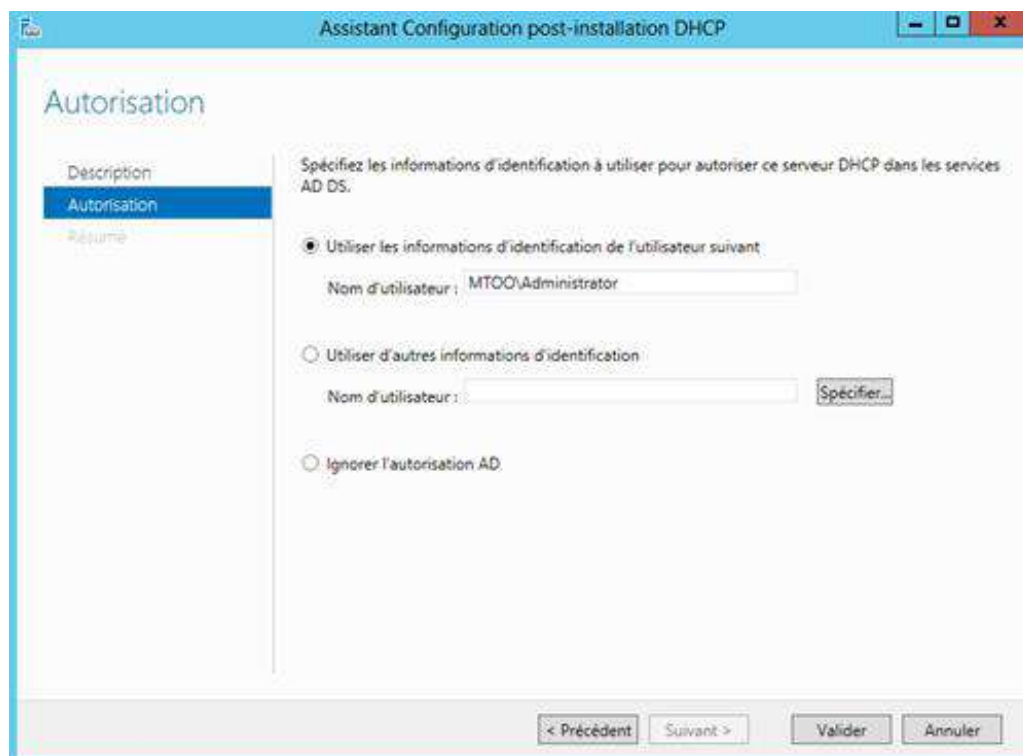
Après quelques minutes le rôle est installé, l'écran final nous invite à commencer la configuration de DHCP.



Un clic sur le lien provoque le lancement de l'assistant de configuration DHCP.



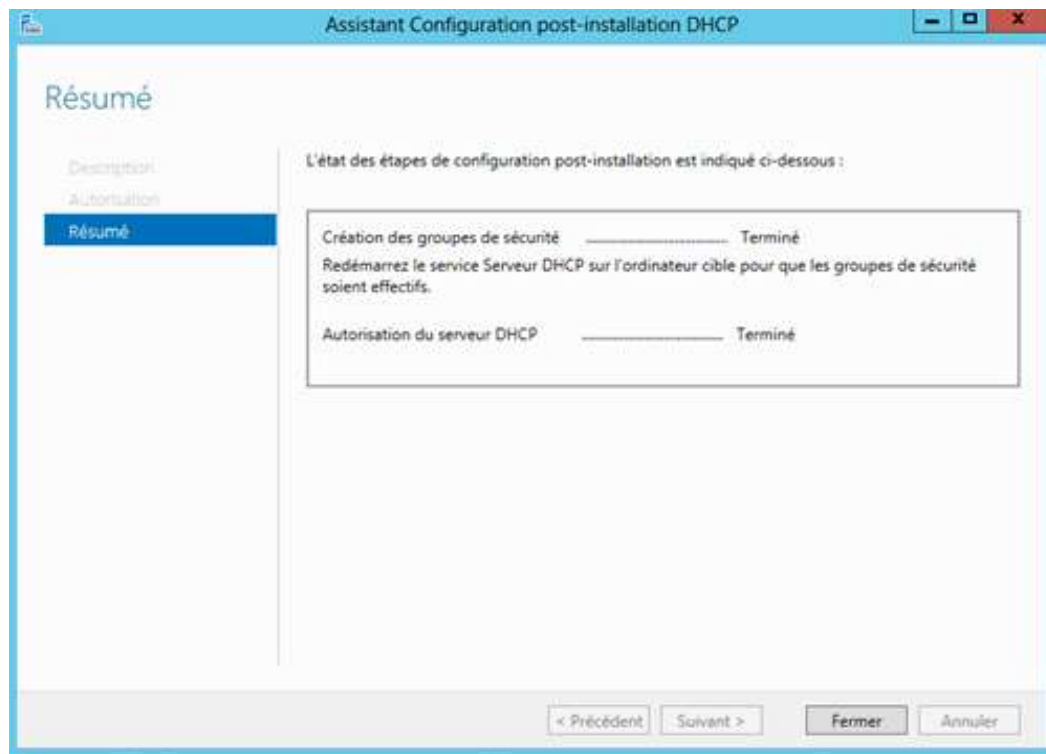
Pour monter un serveur DHCP dans un domaine, celui-ci doit être autorisé par un administrateur du domaine, l'assistant vous propose de le faire directement, après authentification.



Entrez si nécessaire les informations de connexion, puis on clique sur « **Valider** ».

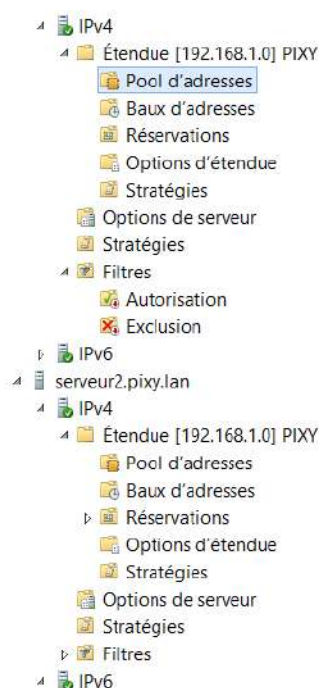
Le résumé des opérations est affiché.

Les groupes de sécurité des administrateurs et utilisateurs de DHCP est créé. Le serveur sur lequel on installe le DHCP est autorisé dans Active Directory.



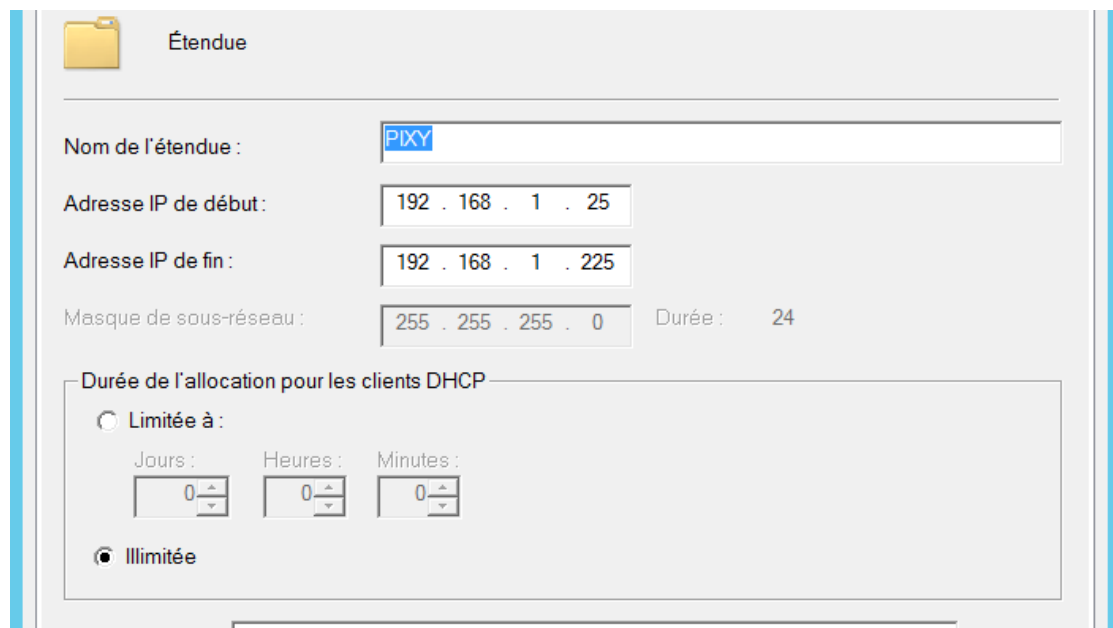
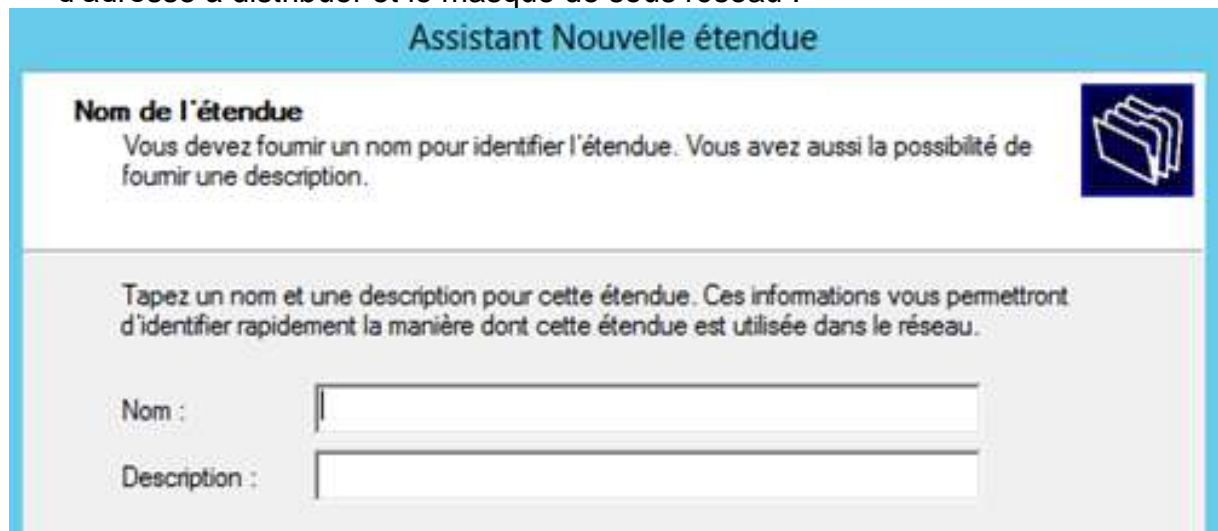
Maintenant on crée nos étendues DHCP à l'aide de la console d'administration DHCP qu'on lance depuis le menu «**Outils**» du gestionnaire de serveur.

Pour créer une étendue IPv4, on clique avec le bouton droit sur IPv4, puis en choisissant «**Nouvelle étendue**».



L'assistant de création de nouvelle étendue permet ensuite:

- De donner un nom et une description à votre étendue, de définir la plage d'adresse à distribuer et le masque de sous réseau :



- D'y ajouter d'éventuelles exclusions afin de ne pas provoquer de conflit avec un périphérique qui serait configuré sur ces adresses (imprimante, webcam IP, PC en adresse fixe, serveur...) :

Assistant Nouvelle étendue

Ajout d'exclusions et de retard

Les exclusions sont des adresses ou une plage d'adresses qui ne sont pas distribuées par le serveur. Un retard est la durée pendant laquelle le serveur retardera la transmission d'un message DHCP OFFER.

Entrez la plage d'adresses IP que vous voulez exclure. Si vous voulez exclure une adresse unique, entrez uniquement une adresse IP de début.

Adresse IP de début : Adresse IP de fin :

Plage d'adresses exclue :

Retard du sous-réseau en millisecondes :

Puis la durée du bail, c'est à dire le temps pendant lequel le PC est autorisé à utiliser cette adresse sans la renouveler.

Assistant Nouvelle étendue

Durée du bail

La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.

La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.

De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.

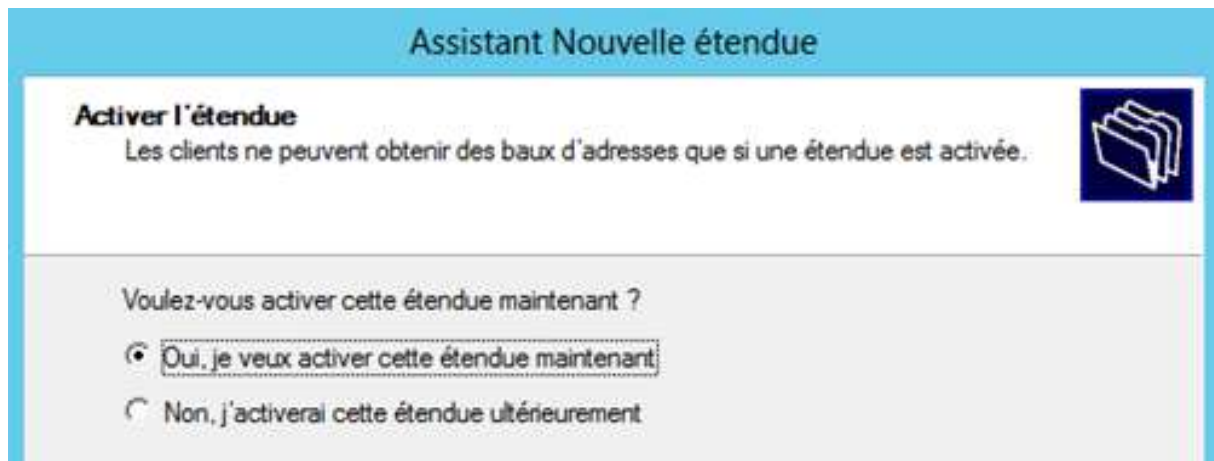
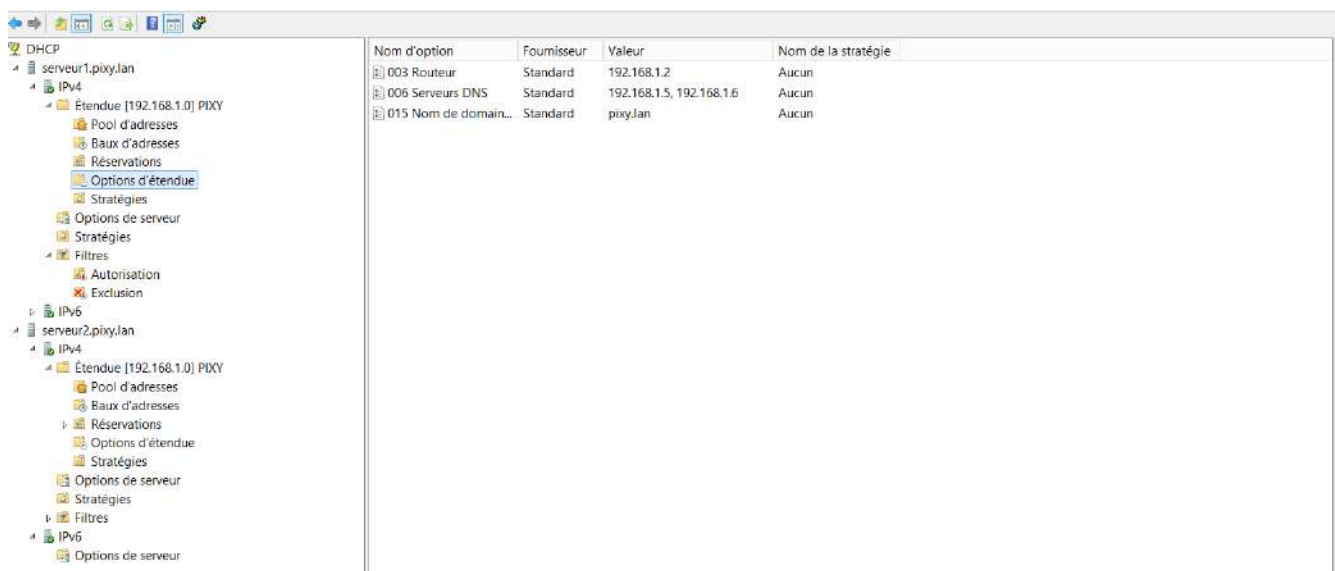
Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.

Limitée à :

Jours : Heures : Minutes :

On peut ensuite configurer des options : les options sont des paramètres supplémentaires que vous pouvez configurer : comme l'adresse de la passerelle, des serveurs DNS et WINS.

Ensuite on active l'étendue.

Nom d'option	Fournisseur	Valeur	Nom de la stratégie
003 Routeur	Standard	192.168.1.2	Aucun
006 Serveurs DNS	Standard	192.168.1.5, 192.168.1.6	Aucun
015 Nom de domain...	Standard	pixy.lan	Aucun

Voici les résultats de l'étendue.

Nos PC peuvent maintenant disposer des paramètres IP corrects automatiquement.

Nom de la relation :	serveur1.pixy.lan-serveur2.pixy.lan
Serveur partenaire :	serveur2.pixy.lan
Mode :	Équilibrage de charge
Délai de transition maximal du client :	1 h 0 min
Intervalle de basculement d'état :	Désactivé
État de ce serveur :	Normale
État du serveur partenaire :	Normale
Pourcentage d'équilibrage de charge	
Serveur local :	50 %
Serveur partenaire :	50 %

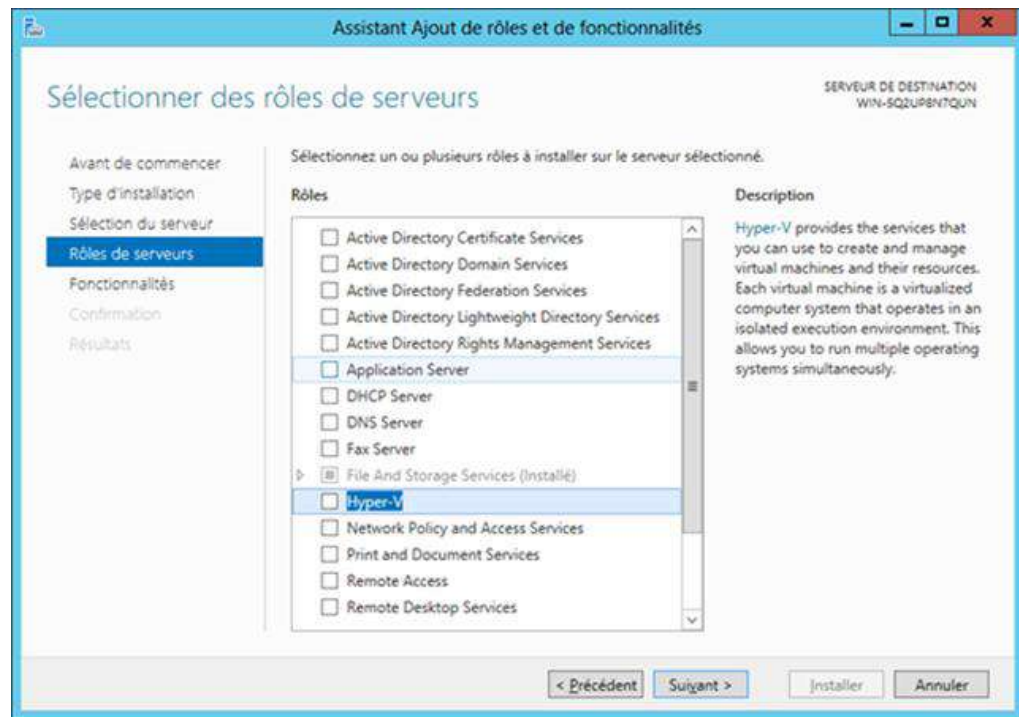
On voit ici que le basculement du DHCP est fonctionnelle.

DHCP								
Adresse IP du cli...	Nom	Expiration du bail	Type	ID unique	Description	Protection d'accès réseau	Expiration de la période d'essai	Actions
192.168.1.25	TEST.pixy.lan	Infini	DHCP	000c29be...	Accès complet	N/D		Baux d
192.168.1.91	iPhone-6-Sacha...	01/06/2017 23:10:57	DHCP	bc6c2165...	Accès complet	N/D		Autr

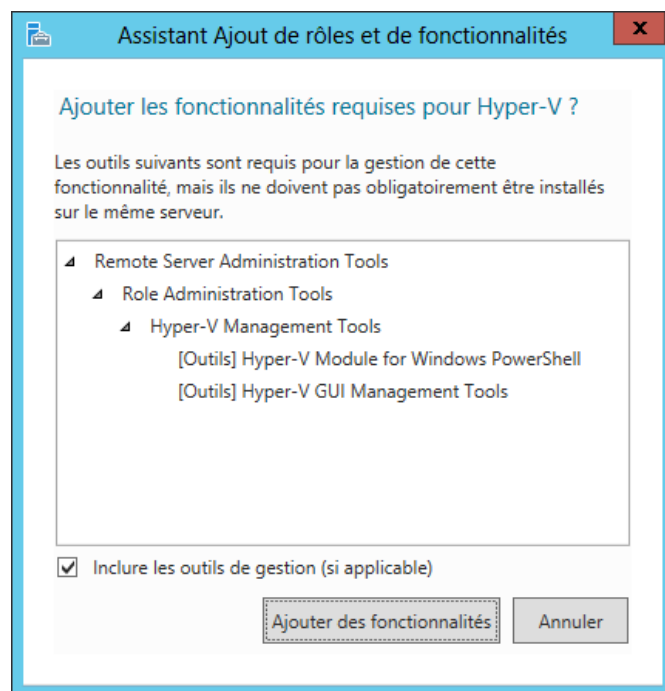
Le DHCP distribue bien des adresses, puisque que l'on a des appareils auxquelles ont été distribués une adresse IP.

Rôles Hyper-V

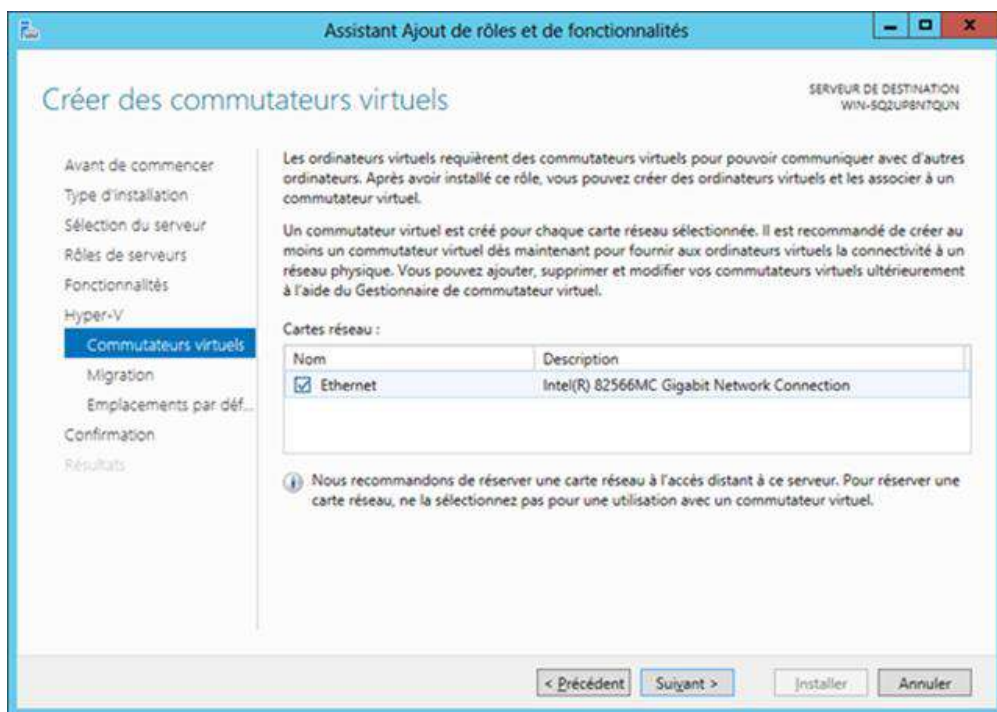
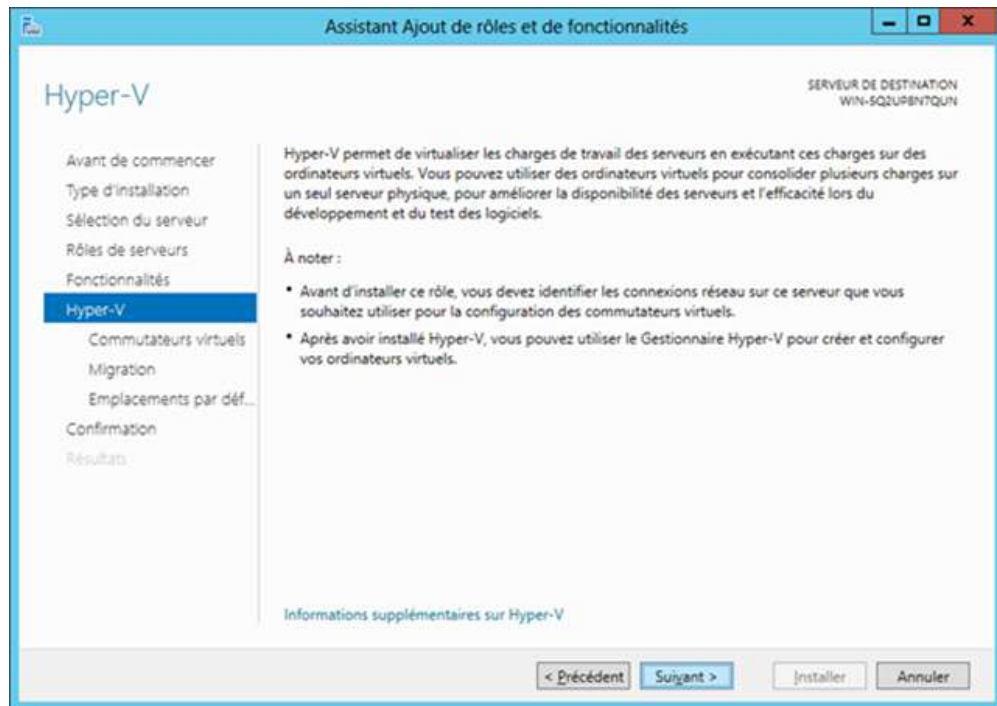
On peut maintenant lancer l'assistant d'ajout de rôles, après avoir sélectionné le serveur sur lequel on installe Hyper-V.



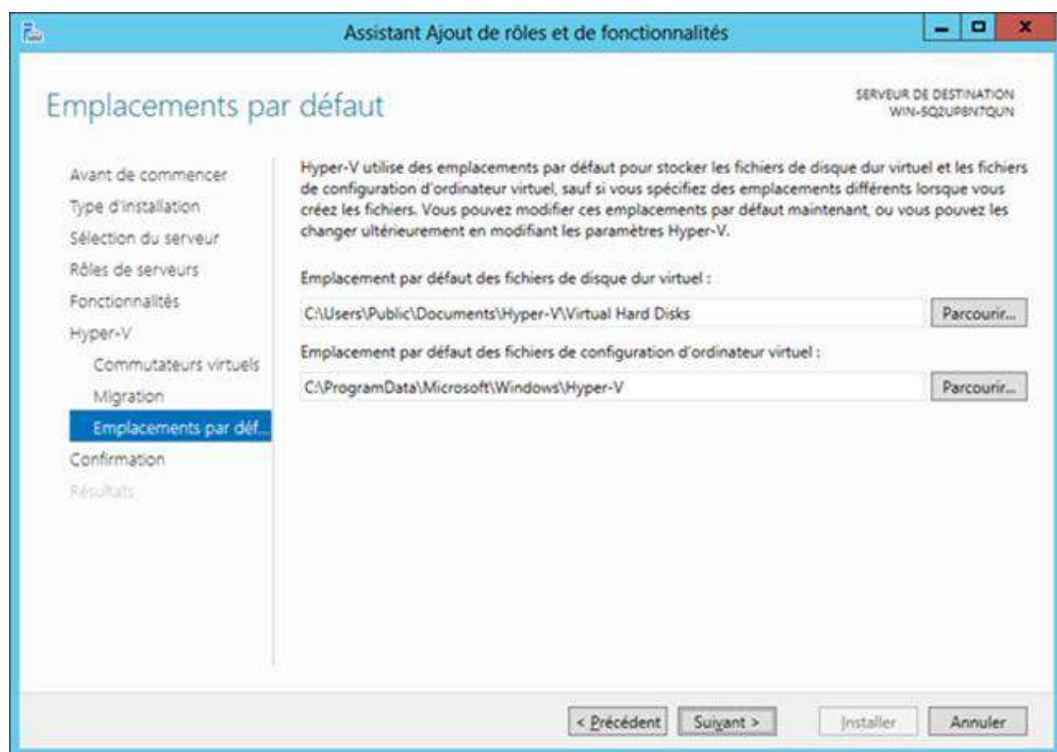
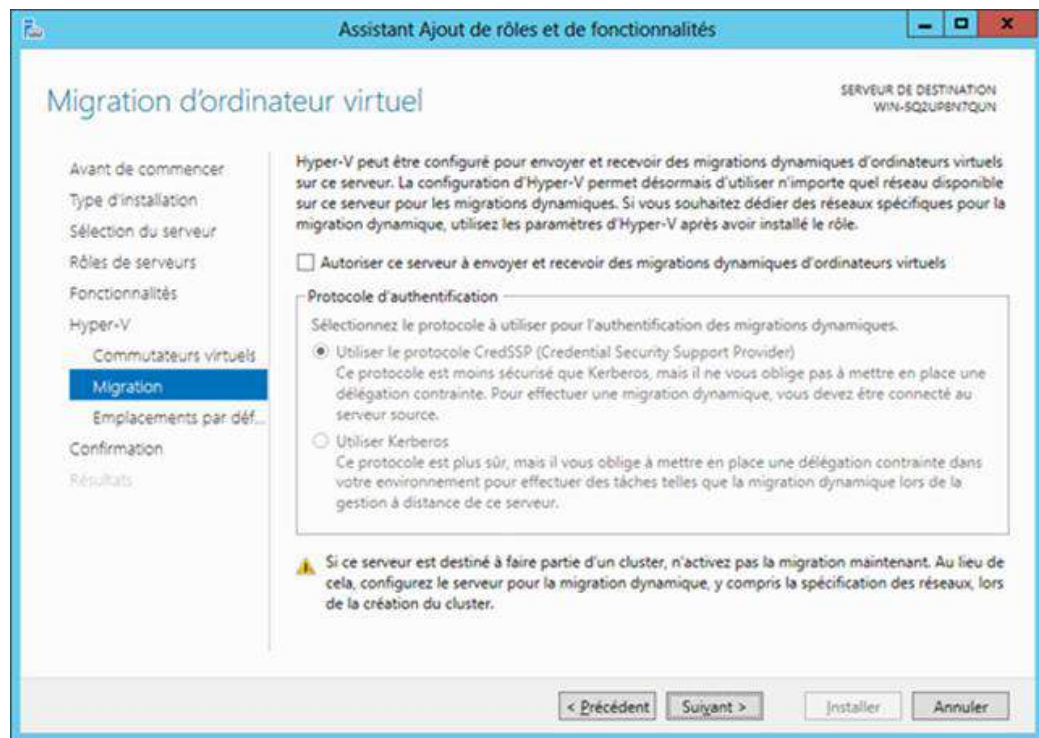
Lorsqu'on sélectionne l'ajout de rôle Hyper-V, les fonctionnalités suivantes sont proposées : RSAT, avec les outils de gestion de Hyper-V en powershell et la console.



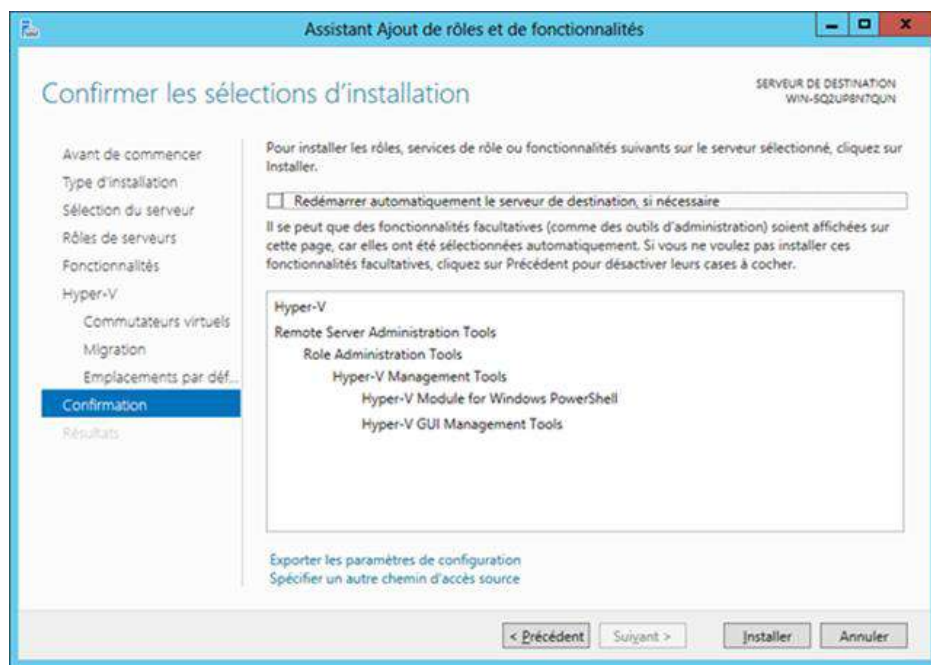
L'installation de Hyper-V débute, en rappelant quelques principes.



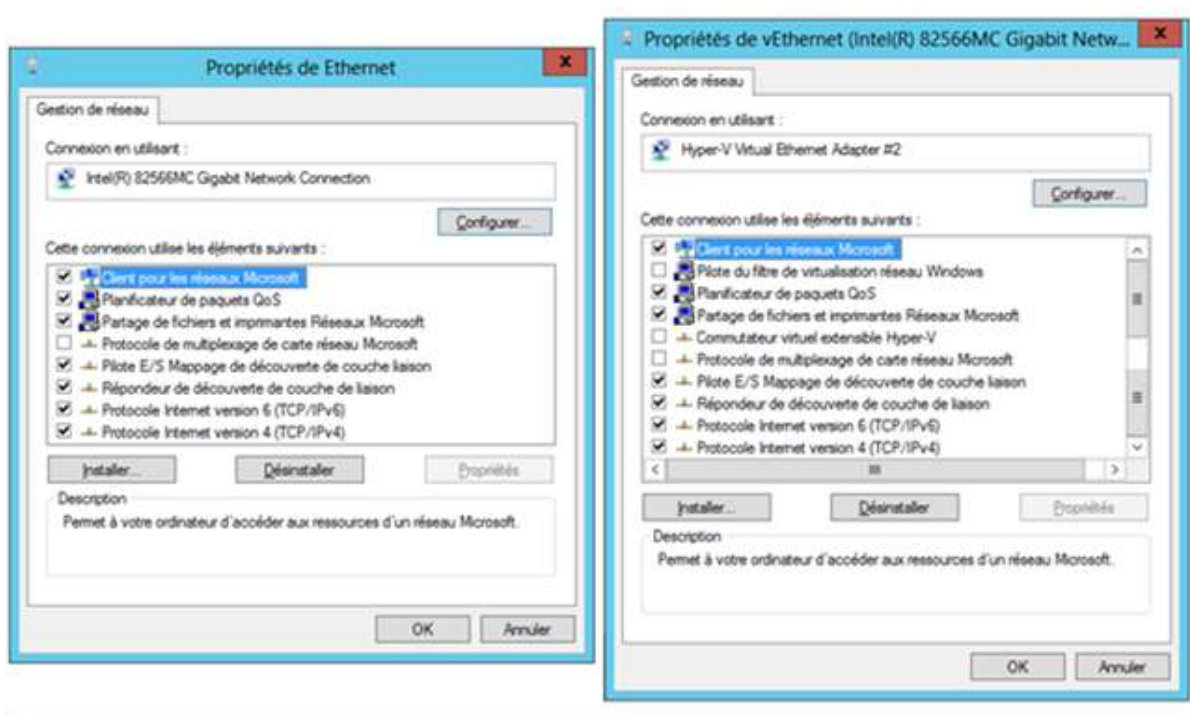
On peut aussi autoriser notre futur serveur pour la migration de machines virtuelles.



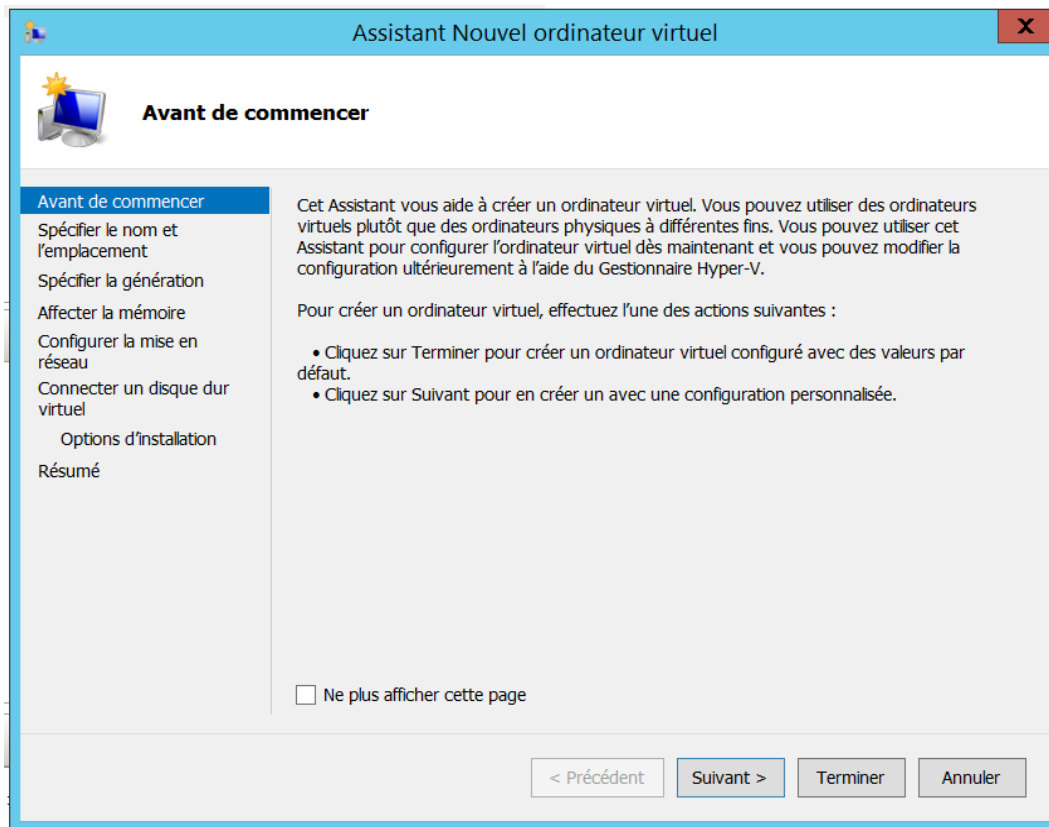
Le dernier écran propose un récapitulatif de l'installation qui sera lancé dès l'appui sur « **Installer** » :



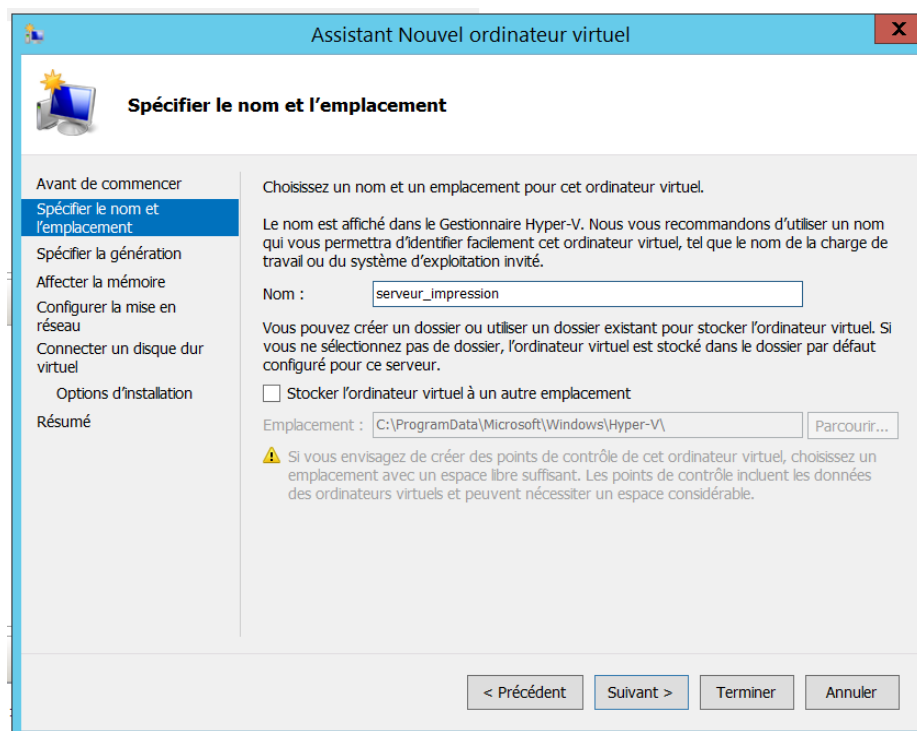
Avant, les protocoles TCP-IP sont attachés à la carte réseau matérielle, après ceux-ci sont attachés à la carte réseau Hyper-V, car le matériel est contrôlé par l'Hyperviseur.



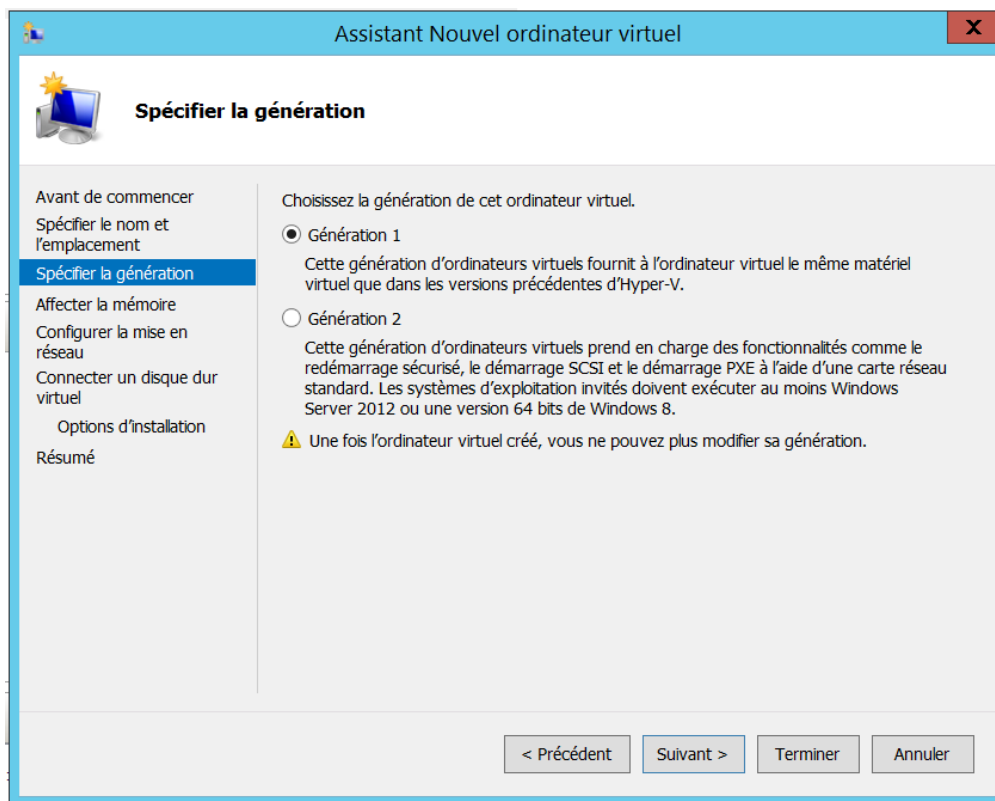
Installation des Vm sur Hyper-V



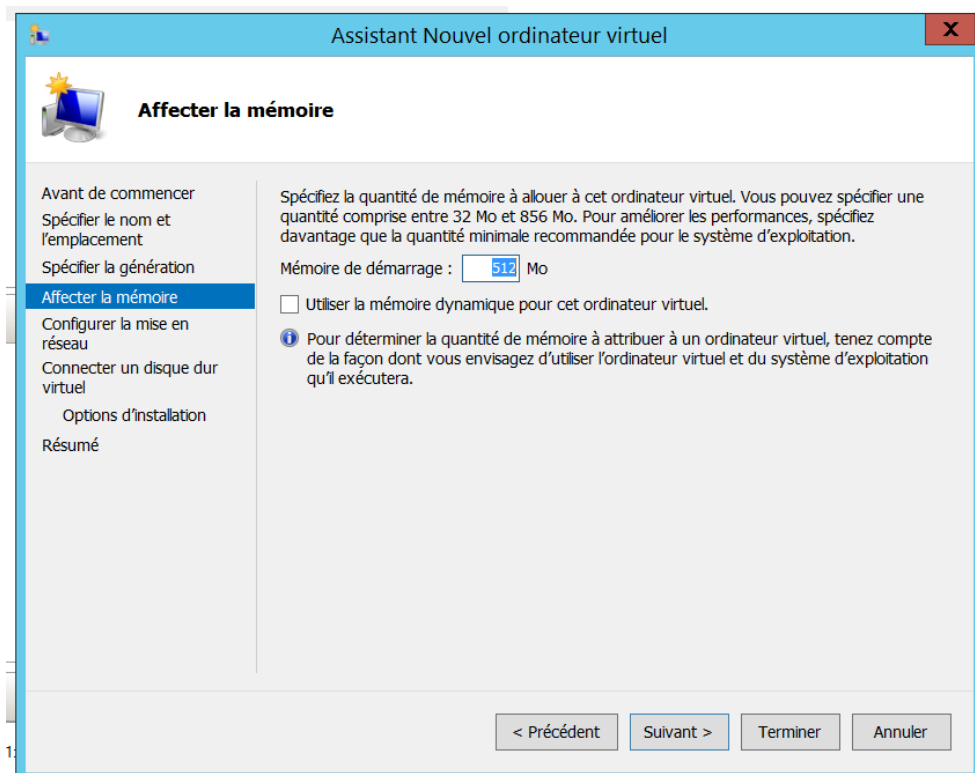
L'assistant démarre on clique sur “ **Suivant** ”



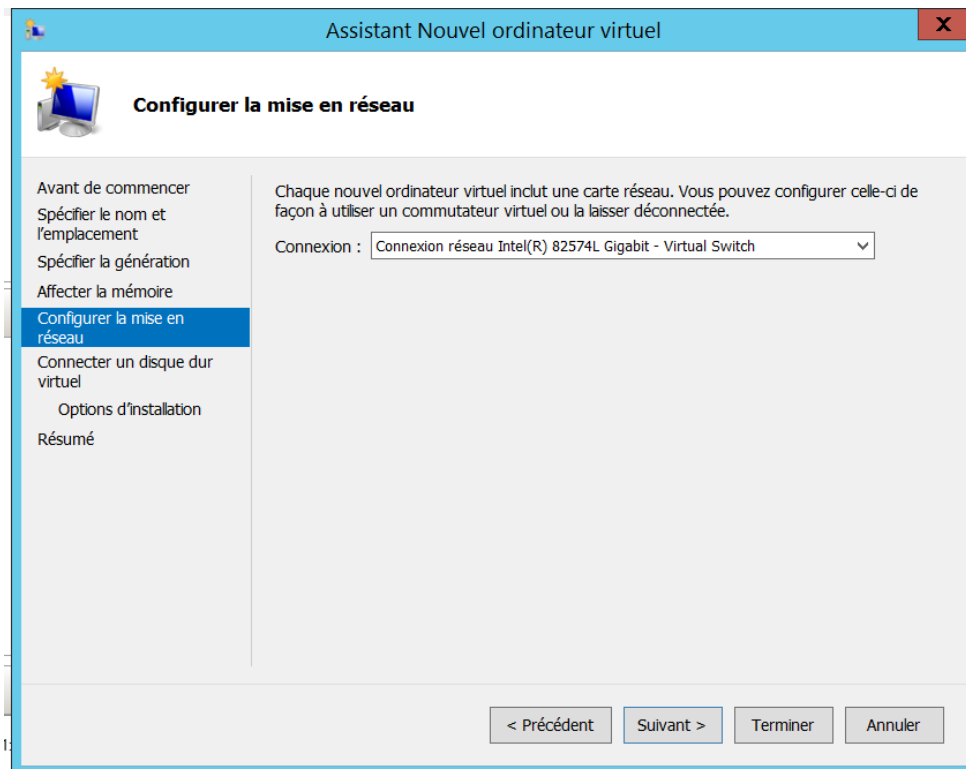
On nomme notre VM Hyper-v “serveur_impression” puis on clique sur “suivant”



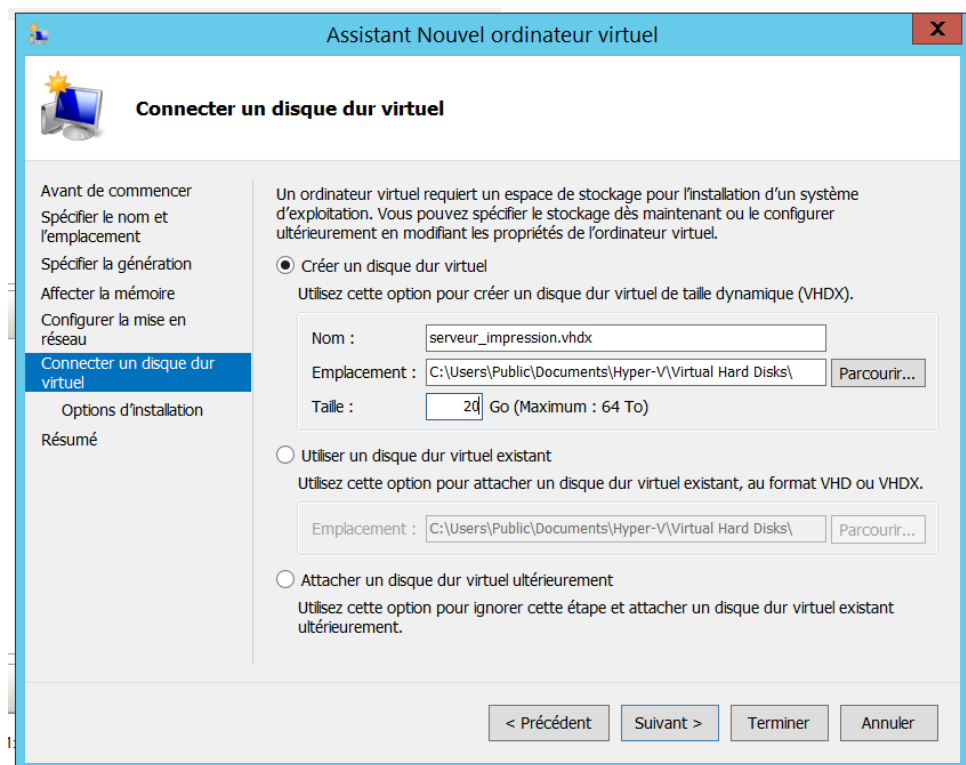
Nous prenons la 1ère génération pour cet ordinateur virtuel.



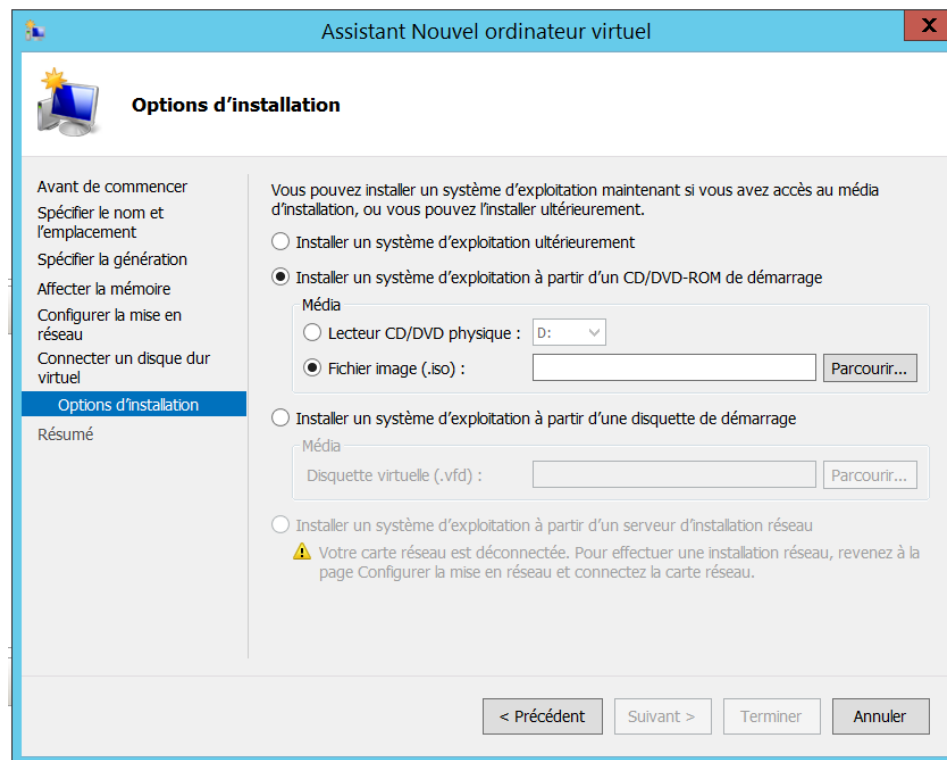
Nous affectons la memoire virtuel soit 512 Mo



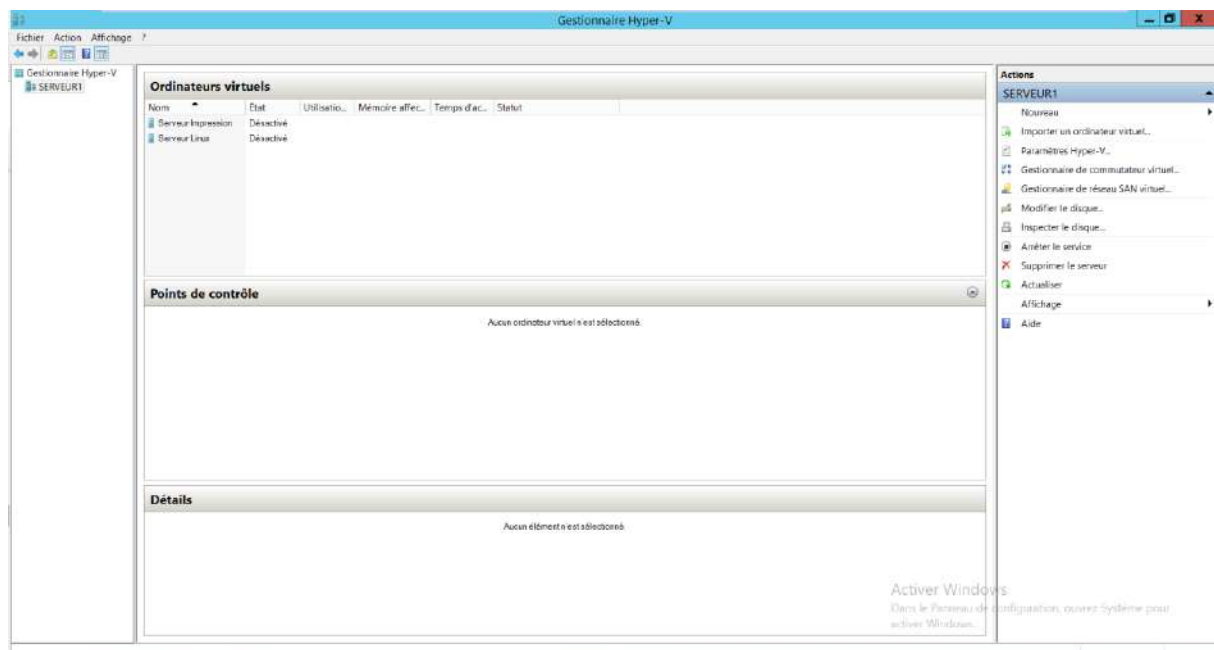
On affecte une carte réseau.



On applique un disque dur virtuel.



On précise l'ISO sur lequel démarre l'ordinateur virtuel.



Notre ordinateur virtuel est créé.

Une fois nos VM Hyper-V on les fais répliquer avec le serveur 2.

Avant de commencer

Spécifier le serveur de réplication

Spécifier les paramètres de connexion

Choisir les disques durs virtuels de réplication

Configurer la fréquence de la réplication

Configurer les points de récupération supplémentaires

Choisir la méthode de réplication initiale

Résumé

Spécifiez le nom du serveur de réplication à utiliser pour la réplication de cet ordinateur virtuel. Si le serveur de réplication se trouve sur un cluster de basculement, spécifiez le nom du service Broker de réplication Hyper-V en tant que serveur de réplication. Utilisez le Gestionnaire du cluster de basculement sur le serveur de réplication pour trouver le nom du serveur du service Broker de réplication.

Serveur de réplication :

Avant de commencer

Spécifier le serveur de réplication

Spécifier les paramètres de connexion

Choisir les disques durs virtuels de réplication

Configurer la fréquence de la réplication

Configurer les points de récupération supplémentaires

Choisir la méthode de réplication initiale

Résumé

Serveur de réplication :

Port du serveur de réplication :

Type d'authentification

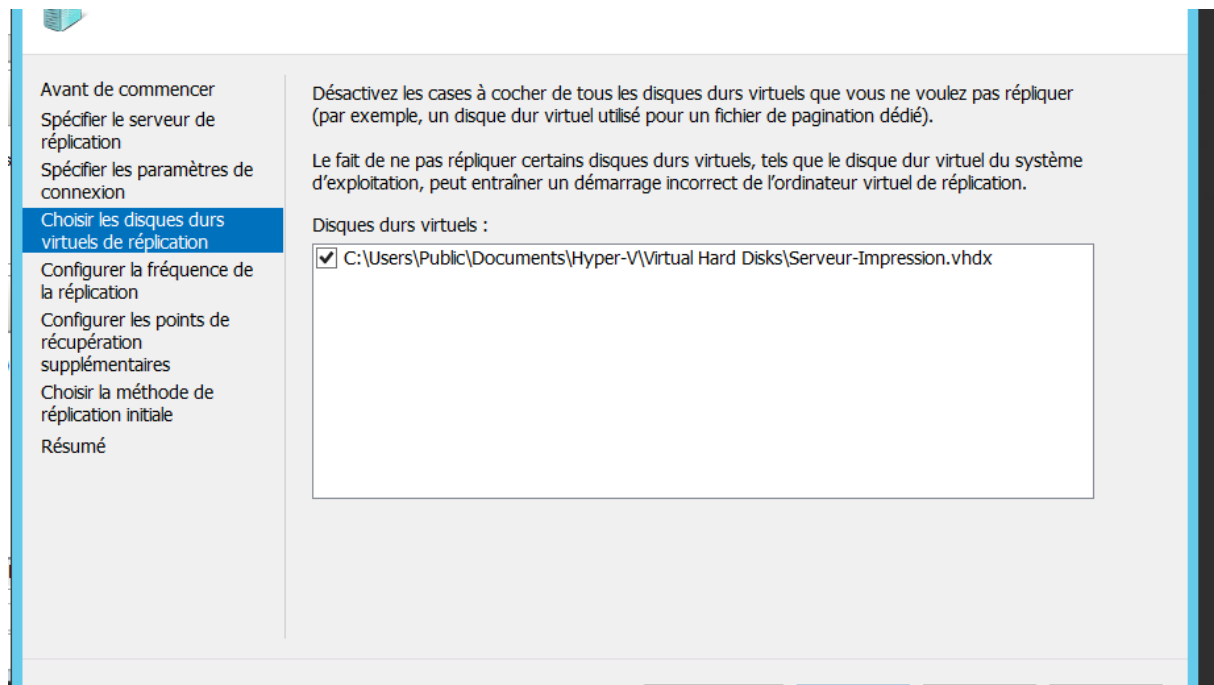
☒ Utiliser l'authentification Kerberos (HTTP)
Les données ne seront pas chiffrées lors de leur transmission sur le réseau.

☐ Utiliser l'authentification basée sur les certificats (HTTPS)
Les données seront chiffrées lors de leur transmission sur le réseau.

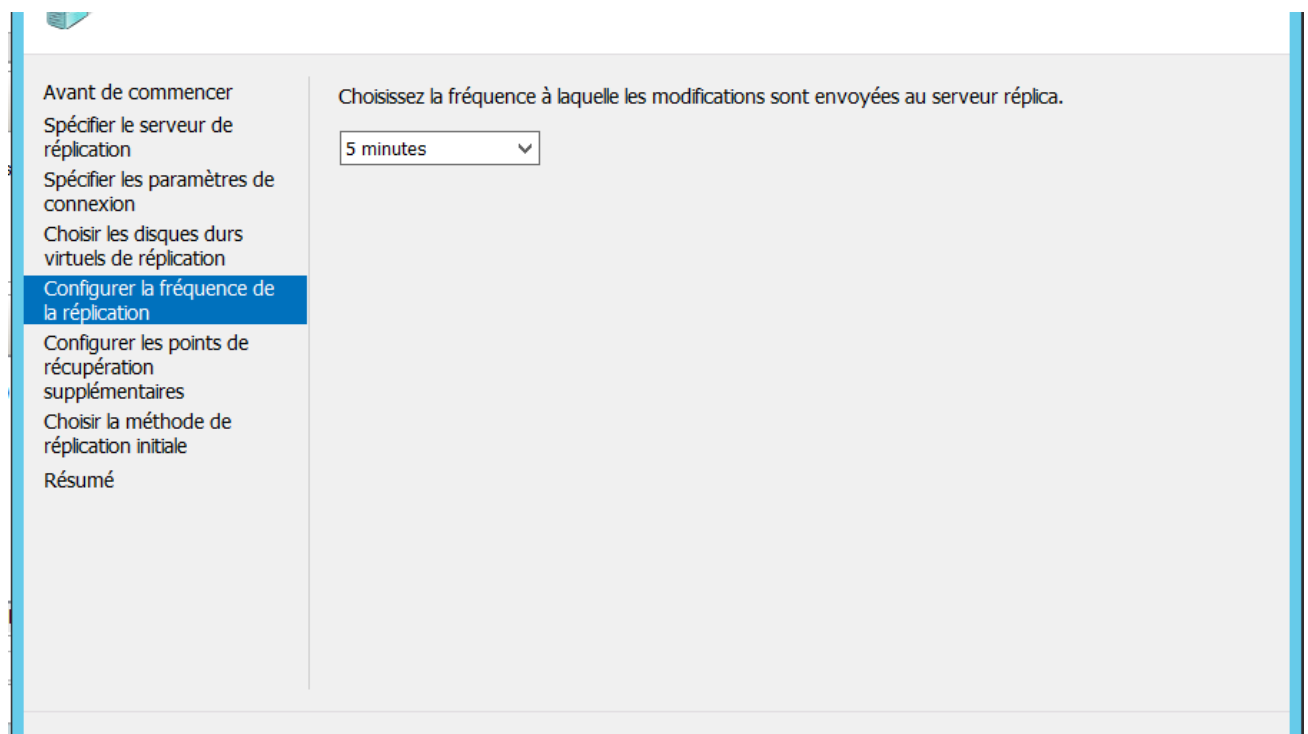
Délivré à :
Délivré par :
Date d'expiration :
Rôle prévu :

☒ Compresser les données transmises sur le réseau.

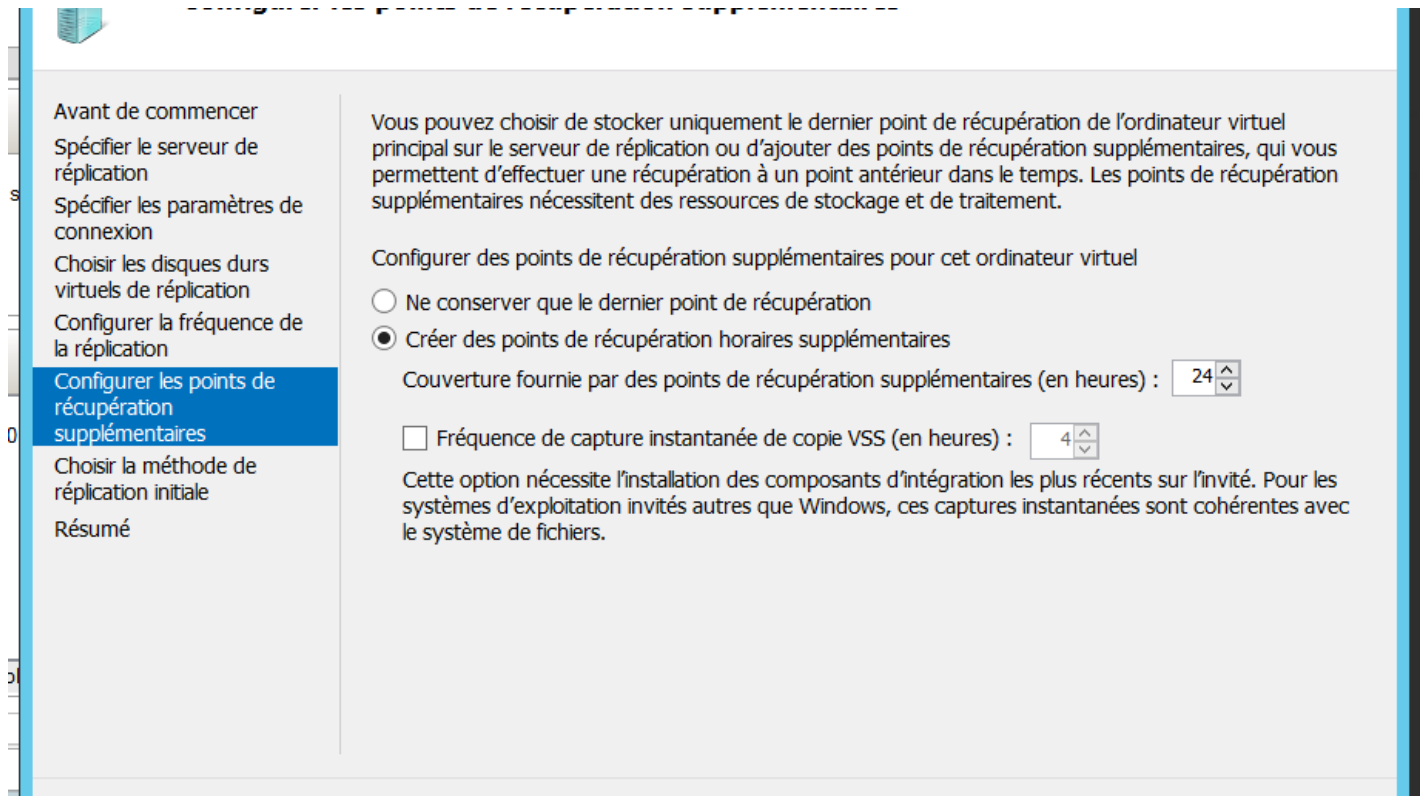
On regarde que les paramètres de connexion sont corrects.



on sélectionne le disque virtuel .



Puis la fréquence des modifications envoyé au serveur de réplication qui est mis sur 5 minutes.



Avant de commencer

Spécifier le serveur de réplication

Spécifier les paramètres de connexion

Choisir les disques durs virtuels de réplication

Configurer la fréquence de la réplication

Configurer les points de récupération supplémentaires

Choisir la méthode de réplication initiale

Résumé

Vous pouvez choisir de stocker uniquement le dernier point de récupération de l'ordinateur virtuel principal sur le serveur de réplication ou d'ajouter des points de récupération supplémentaires, qui vous permettent d'effectuer une récupération à un point antérieur dans le temps. Les points de récupération supplémentaires nécessitent des ressources de stockage et de traitement.

Configurer des points de récupération supplémentaires pour cet ordinateur virtuel

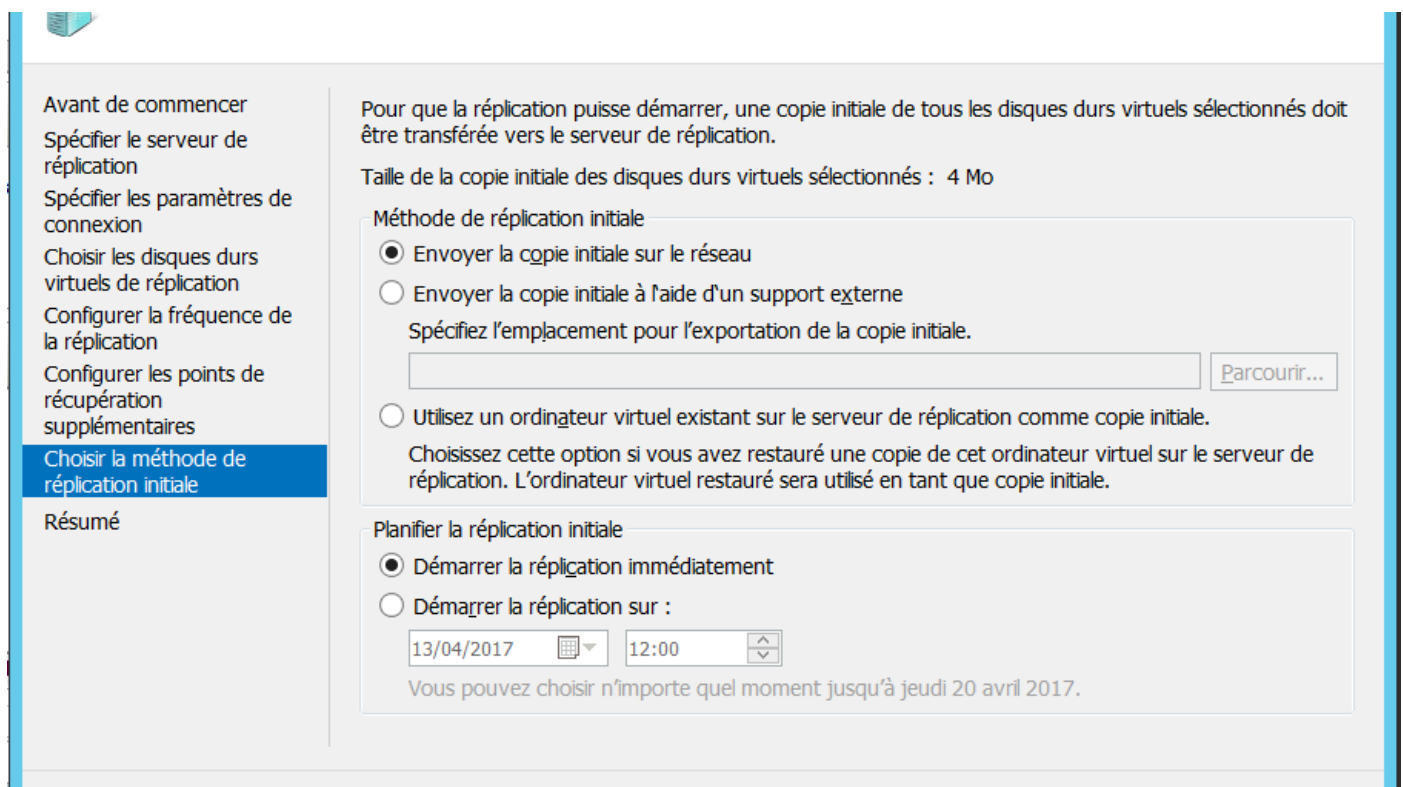
☐ Ne conserver que le dernier point de récupération

☒ Créer des points de récupération horaires supplémentaires

Couverture fournie par des points de récupération supplémentaires (en heures) : 24

☐ Fréquence de capture instantanée de copie VSS (en heures) : 4

Cette option nécessite l'installation des composants d'intégration les plus récents sur l'invité. Pour les systèmes d'exploitation invités autres que Windows, ces captures instantanées sont cohérentes avec le système de fichiers.



Avant de commencer

Spécifier le serveur de réplication

Spécifier les paramètres de connexion

Choisir les disques durs virtuels de réplication

Configurer la fréquence de la réplication

Configurer les points de récupération supplémentaires

Choisir la méthode de réplication initiale

Résumé

Pour que la réplication puisse démarrer, une copie initiale de tous les disques durs virtuels sélectionnés doit être transférée vers le serveur de réplication.

Taille de la copie initiale des disques durs virtuels sélectionnés : 4 Mo

Méthode de réplication initiale

☒ Envoyer la copie initiale sur le réseau

☐ Envoyer la copie initiale à l'aide d'un support externe

Spécifiez l'emplacement pour l'exportation de la copie initiale.

Parcourir...

☐ Utilisez un ordinateur virtuel existant sur le serveur de réplication comme copie initiale.

Choisissez cette option si vous avez restauré une copie de cet ordinateur virtuel sur le serveur de réplication. L'ordinateur virtuel restauré sera utilisé en tant que copie initiale.

Planifier la réplication initiale

☒ Démarrer la réplication immédiatement

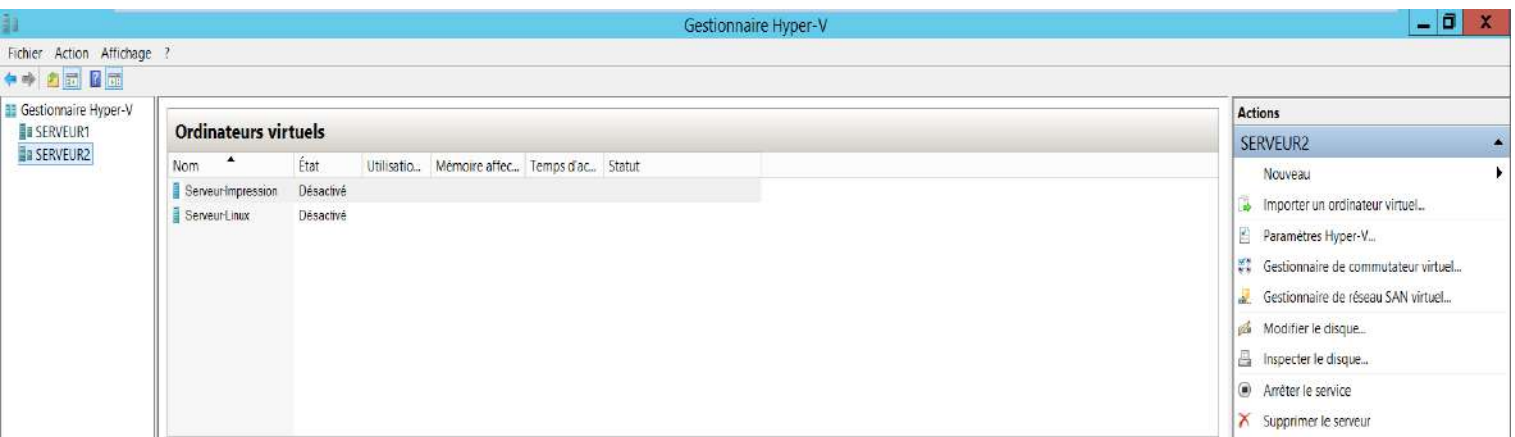
☐ Démarrer la réplication sur :

13/04/2017 12:00

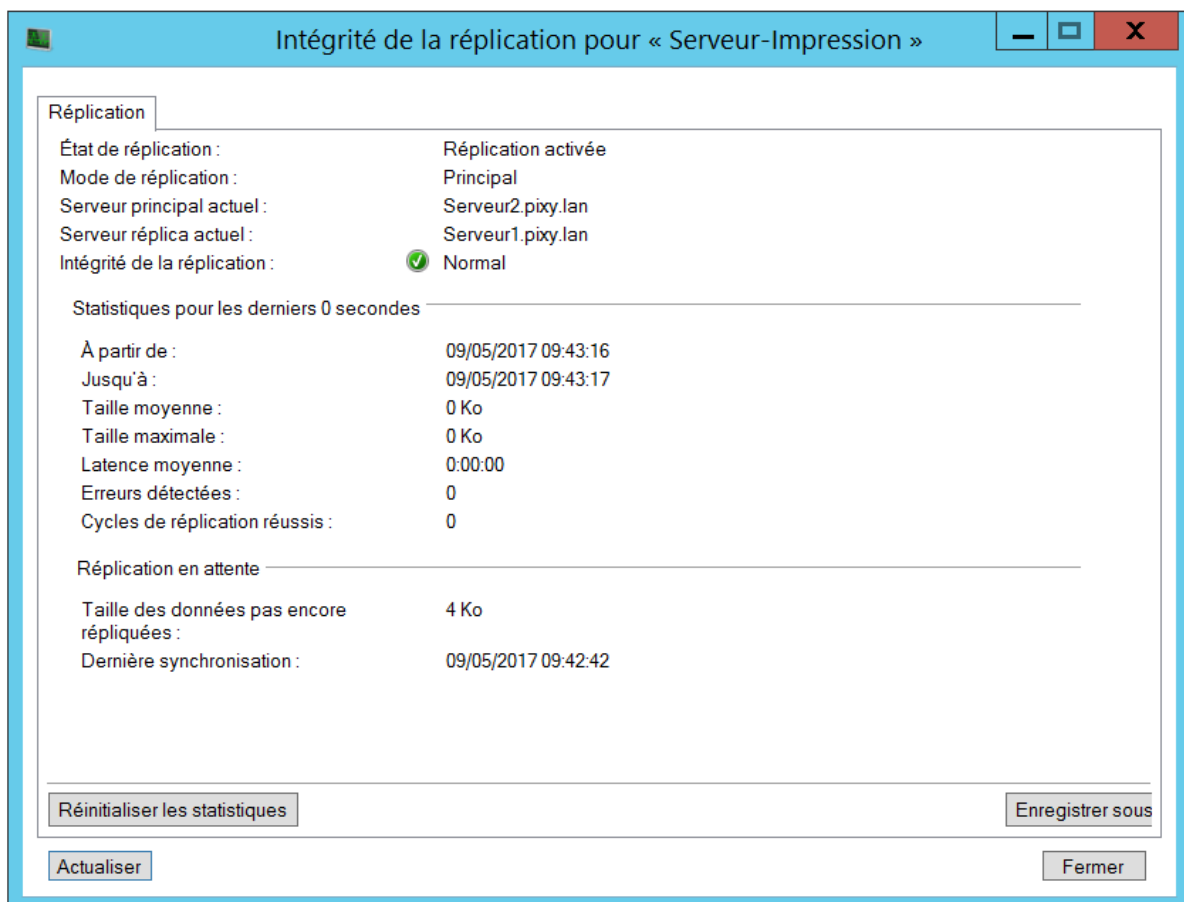
Vous pouvez choisir n'importe quel moment jusqu'à jeudi 20 avril 2017.

On sélectionne : créer des points de récupérations

Puis on choisit les méthodes de réplications



On peut voir ci dessous que la réplication a bien fonctionnée sur le serveur 2.



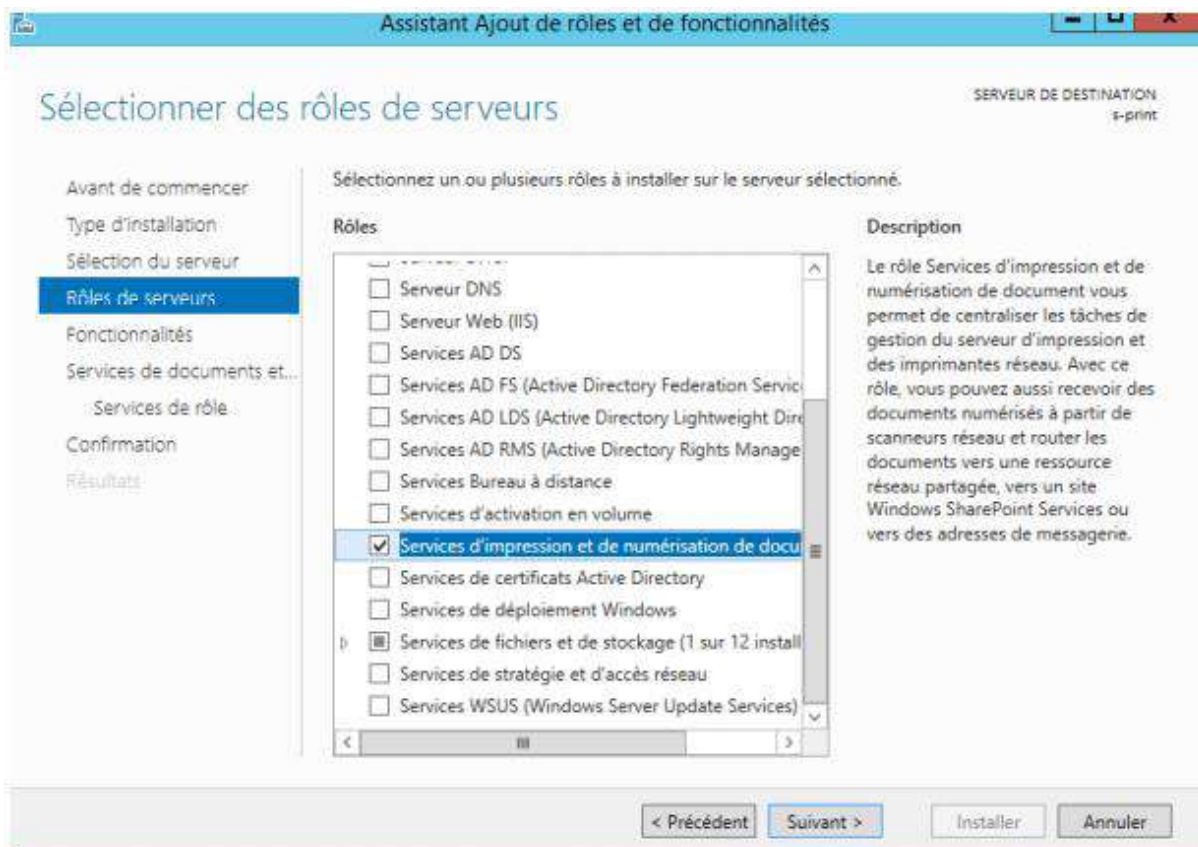
Ci-dessus on voit l'intégrité de la réplication qui est normal.

Serveur d'impression

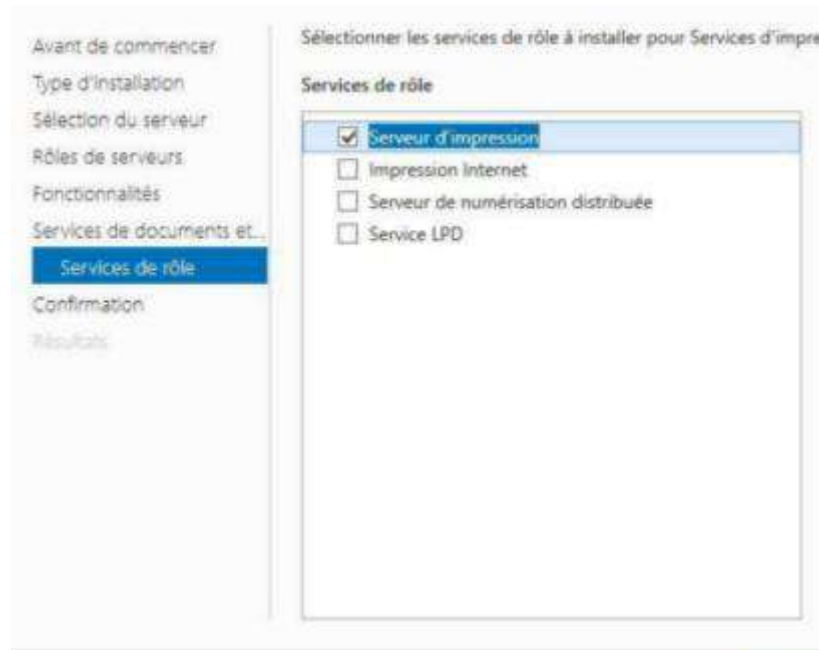
Nous allons procéder à l'installation de notre serveur d'impression.

Sur notre serveur d'impression ainsi que notre contrôleur de domaine, il faut ajouter le rôle adéquat.

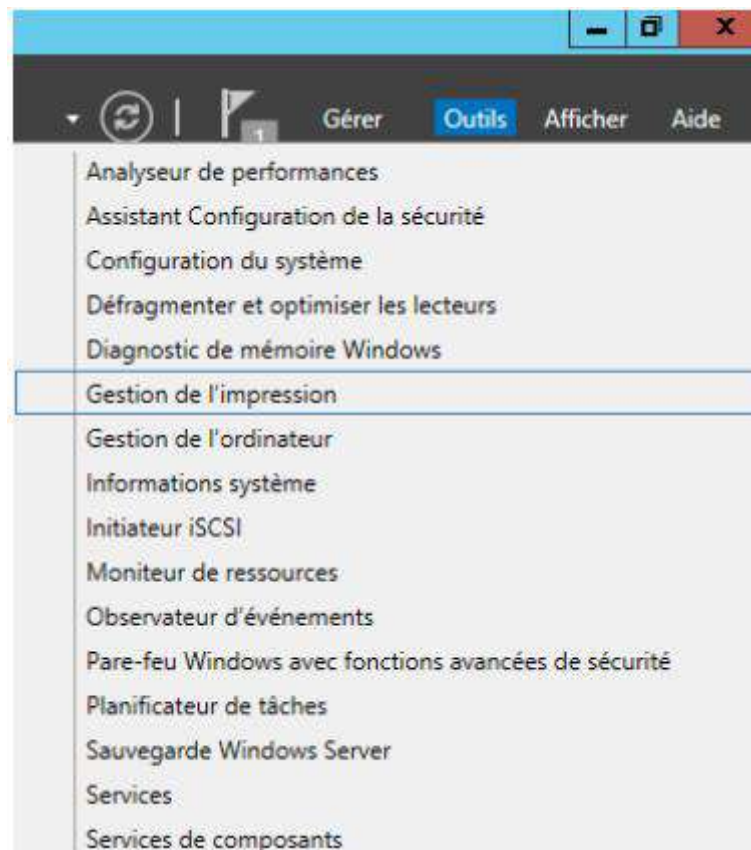
Cochez uniquement « **Services d'impression et de numérisation de documents** » pour installer le rôle.



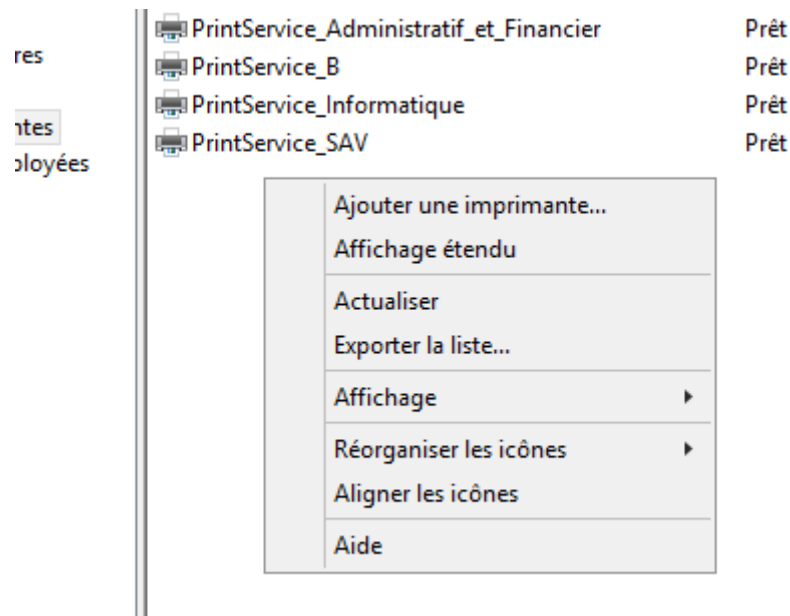
Dans les « **Services de rôle** », nous choisissons « **Serveur d'impression** ».



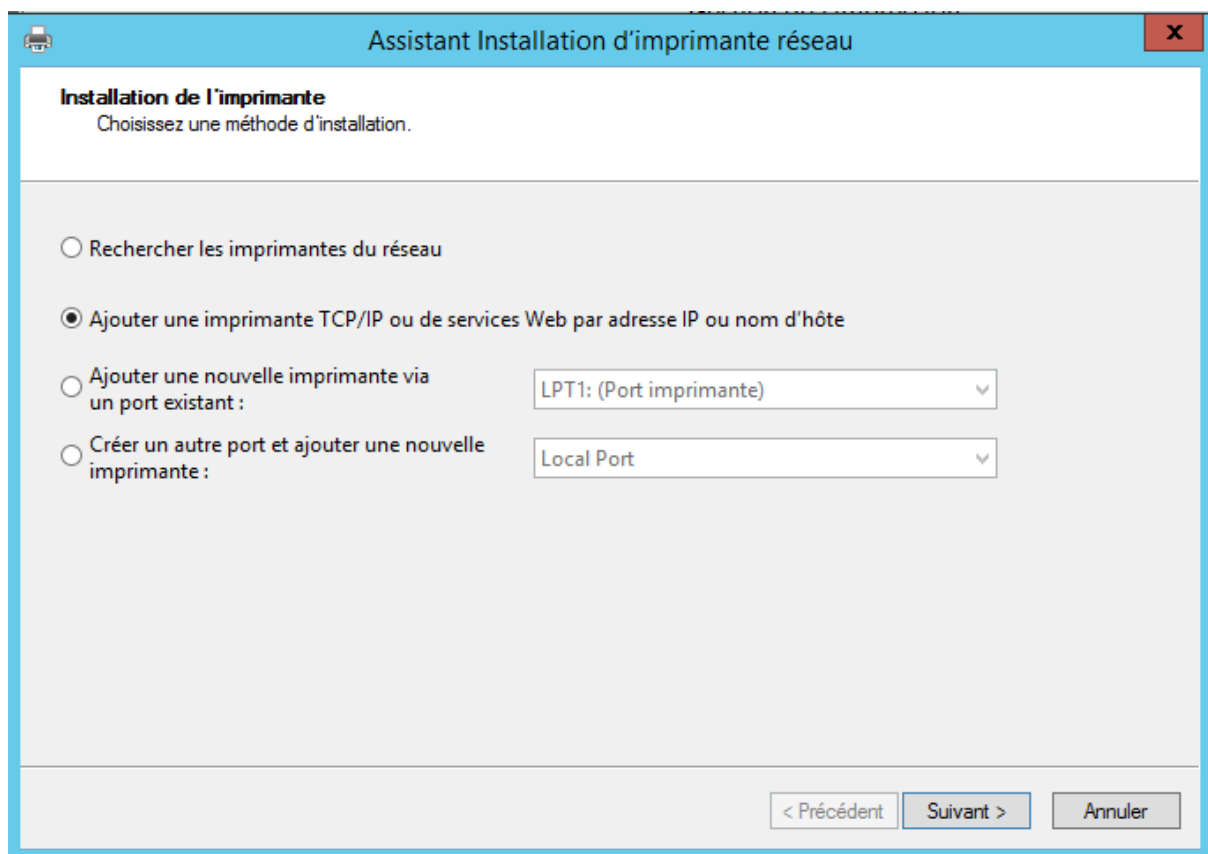
Nous avons donc maintenant l'outil « **Gestion de l'impression** ».



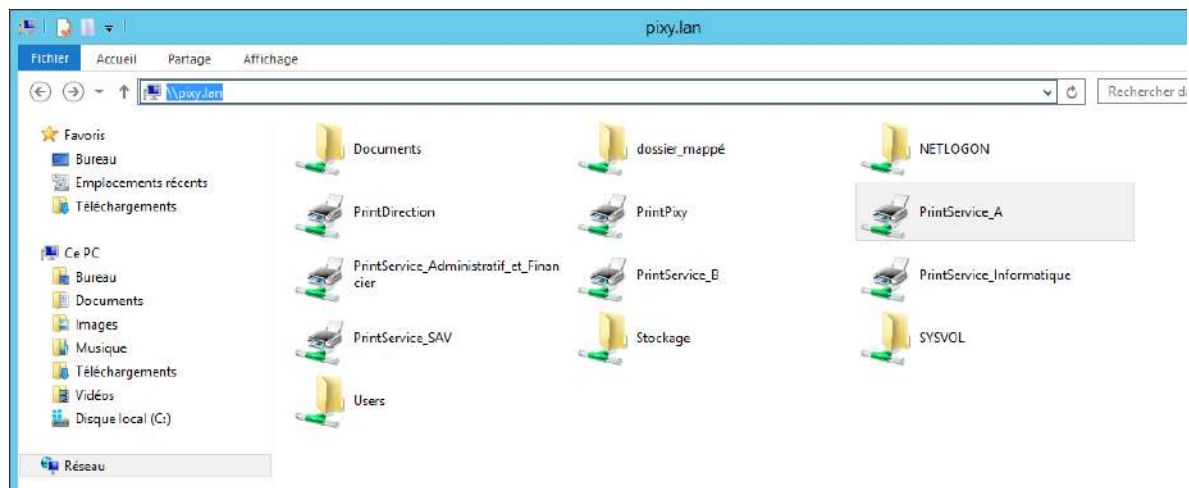
Sur notre serveur d'impression, depuis « **Gestion de l'impression** » nous ajoutons nos imprimantes.



Nous les ajoutons en renseignant leurs adresses IP.



Une fois nos imprimantes installées et partagées, nous pouvons les retrouver ci-dessous.



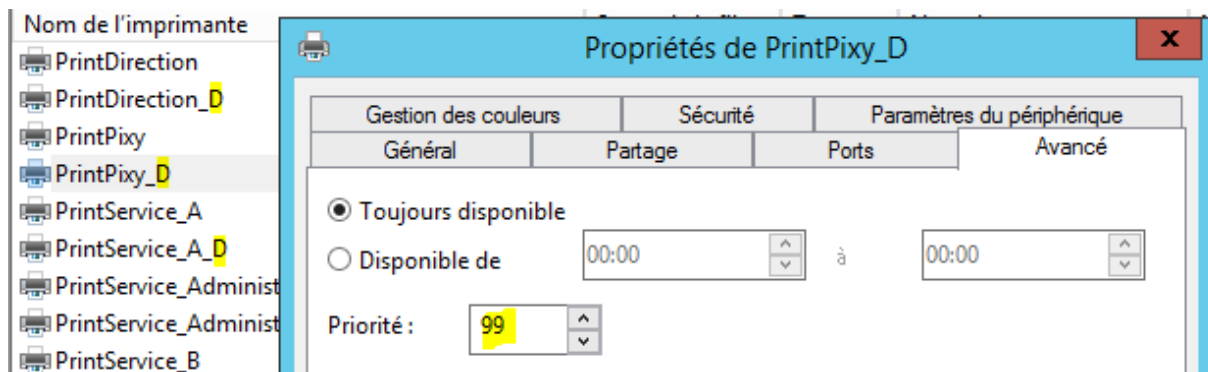
Nous les listons dans l'Active Directory.

Nom	Type
PrintDirection	Imprimante
PrintSAV	Imprimante
PrintService_A	Imprimante
PrintService_Administratif_et_Financier	Imprimante
PrintService_B	Imprimante
PrintService_Informatique	Imprimante
PrintPixy	Imprimante

Etant donné que certaines imprimantes ont des spécificités au niveau des utilisateurs et de leurs droits d'impression, nous les dupliquons de manière à avoir 2 imprimantes similaires pour chaque services.

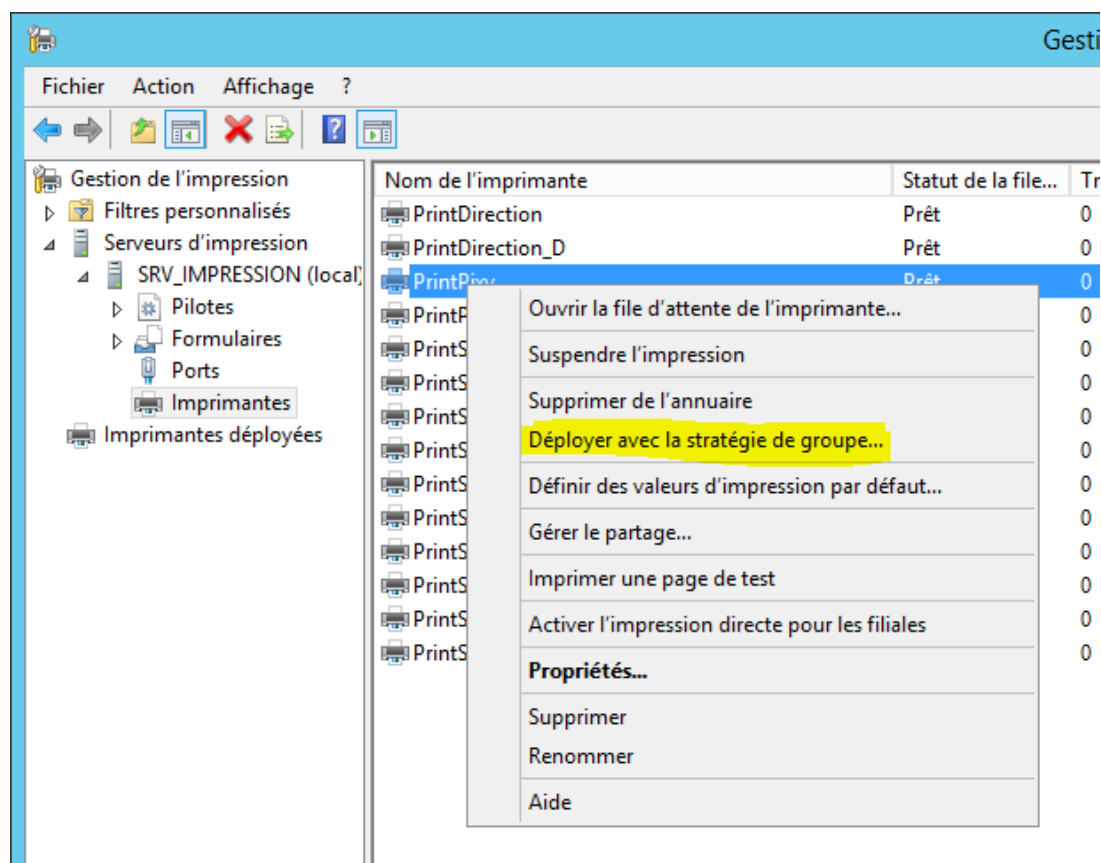
Nom de l'imprimante	Statut de la file...	Travau...	Nom du serveur
PrintDirection	Prêt	0	SRV_IMPRESSION (local)
PrintDirection_D	Prêt	0	SRV_IMPRESSION (local)
PrintPixy	Prêt	0	SRV_IMPRESSION (local)
PrintPixy_D	Prêt	0	SRV_IMPRESSION (local)
PrintService_A	Prêt	0	SRV_IMPRESSION (local)
PrintService_A_D	Prêt	0	SRV_IMPRESSION (local)
PrintService_Administratif_et_Financier	Prêt	0	SRV_IMPRESSION (local)
PrintService_Administratif_et_financier_D	Prêt	0	SRV_IMPRESSION (local)
PrintService_B	Prêt	0	SRV_IMPRESSION (local)
PrintService_B_D	Prêt	0	SRV_IMPRESSION (local)
PrintService_Informatique	Prêt	0	SRV_IMPRESSION (local)
PrintService_Informatique_D	Prêt	0	SRV_IMPRESSION (local)
PrintService_SAV	Prêt	0	SRV_IMPRESSION (local)
PrintService_SAV_D	Prêt	0	SRV_IMPRESSION (local)

Pour les imprimantes dupliquées, nous appliquons une priorité à 99 pour le service de la direction qui doit être prioritaire sur toutes les imprimantes.

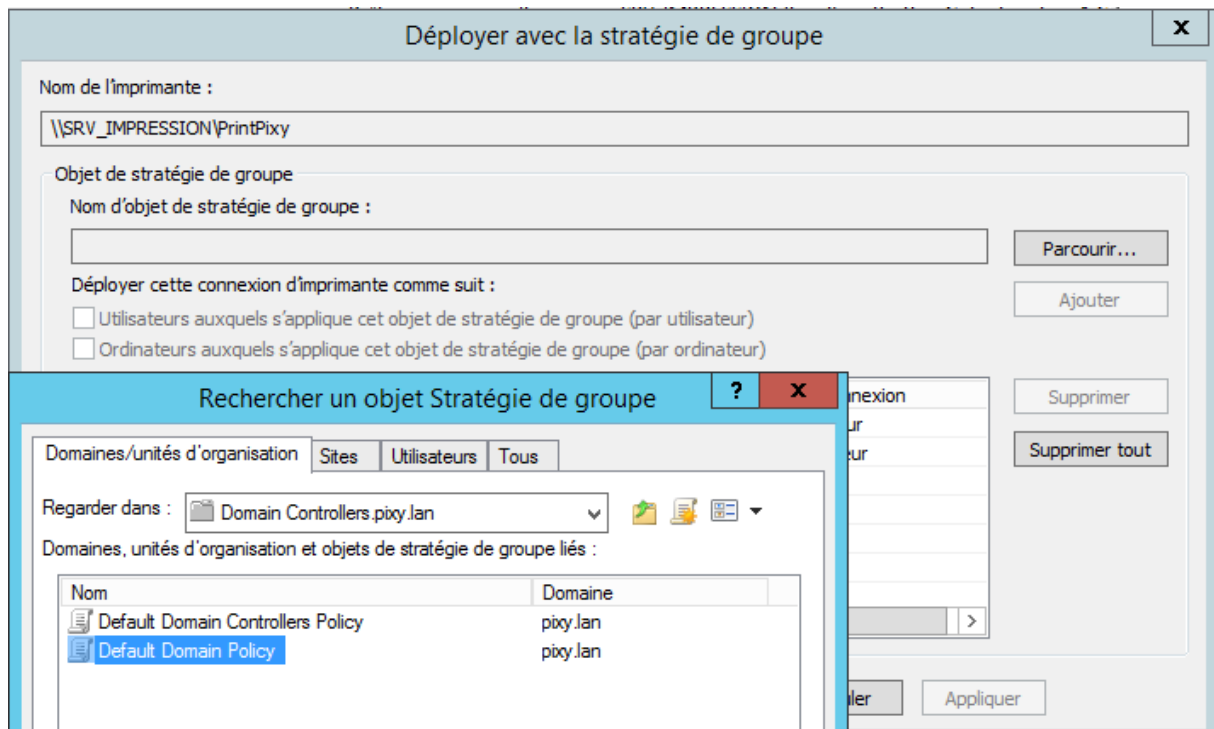


Nous devons également mettre en place quelques GPO, notamment pour Mme. LAPORTE ou Mlle. ADA qui doivent pouvoir imprimer sur plusieurs imprimantes. Nous les avons donc mises en place sur le Contrôleur de domaine.

Ensuite, sur notre serveur d'impression, nous déployons nos imprimantes par stratégie de groupe.

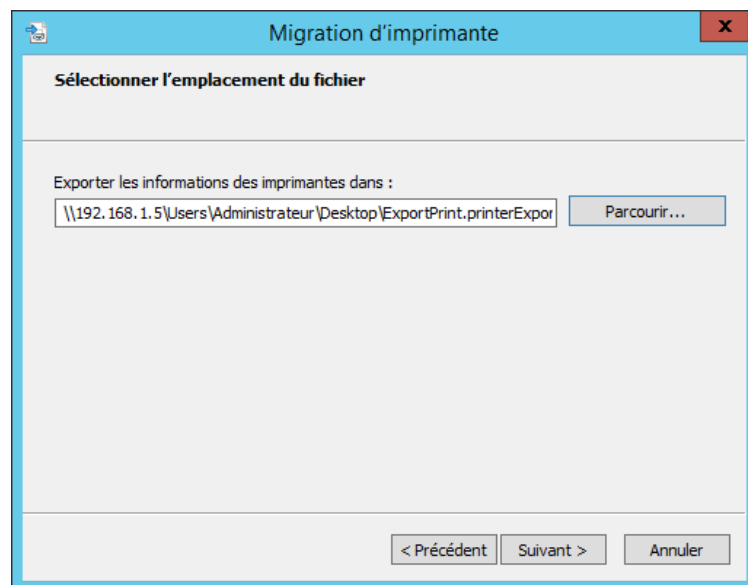


Nous appliquons la GPO.

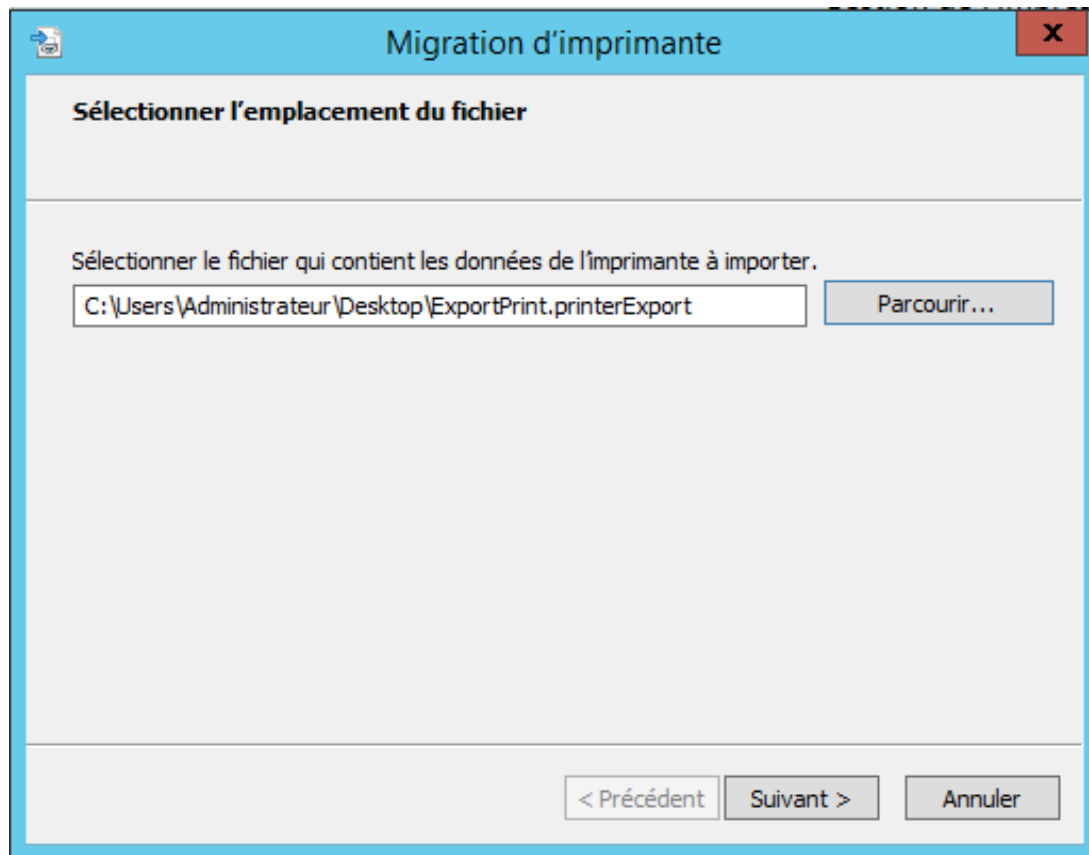


Après vérification, sur un client Windows du service A, l'imprimante remonte bien à l'ouverture de session.

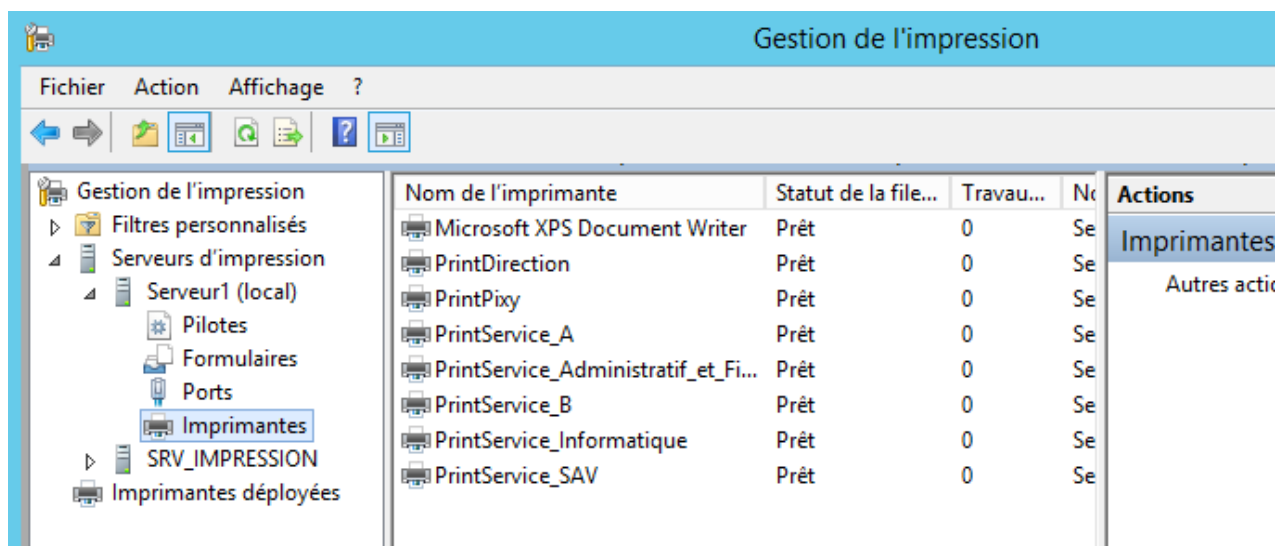
Sur notre serveur d'impression, nous exportons nos imprimantes en un fichier pour le rediriger vers notre contrôleur de domaine.



Ensuite, nous importons sur le contrôleur de domaine.



Les imprimantes se sont bien importées.



Sauvegarde et Récupération Windows Server 2012 R2

On a choisi l'outil de windows pour effectuer nos sauvegarde du serveur 1

Linux sera aussi sauvegardé sur le serveur de fichier 1 .

Le serveur de fichier 1 est sauvegardé sur le disque prévue pour la sauvegarde qui est répliqué sur le serveur de fichier 2.

Il est possible de **sauvegarder les éléments qui se trouvent sur un serveur**.

Cette fonctionnalité est très utile pour les entreprises en possédant un (voir plusieurs) et qui abritent dessus des applications métiers, des machines virtuelles Hyper-V, des dossiers partagés, etc...

En effet, **en cas de problèmes, il est possible de récupérer les données** grâce aux sauvegardes qui auront été effectuées.

Nous allons commencer par installer la fonctionnalité sur le serveur.

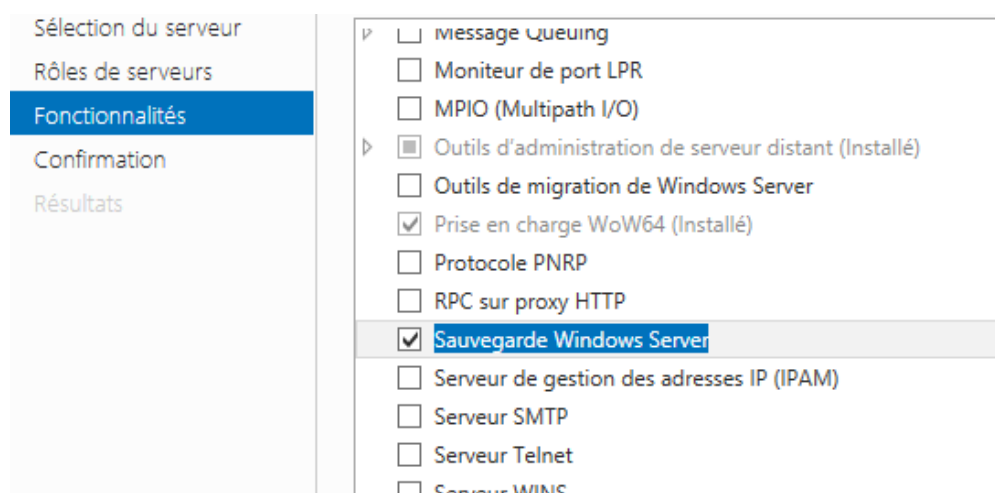
Installation de la fonctionnalité

Sur votre serveur, « **Gestionnaire de serveur** » puis dans la partie supérieure droite de la fenêtre, on clique sur « **Gérer** » > « **Ajouter des rôles et des fonctionnalités** ».

Dans « **l'Assistant Ajout de rôles et fonctionnalités** »,

« Avant de commencer » : il n'y a aucune action à effectuer sur cette page si ce n'est de cliquer sur « **Suivant** ».

- « Type d'installation » : On sélectionne « **Installation basée sur un rôle ou une fonctionnalité** ».
- « Sélection du serveur » : On choisit sur quel serveur on installe l'utilitaire de sauvegarde.
- « Rôles de serveurs » : on clique « **Suivant** »
- « Fonctionnalités » : On coche « **Sauvegarde Windows Server** ». et « **Suivant** ».



- « Confirmation » : On clique « **Installer** ».
- « Résultats »: On clique « **Fermer** ».

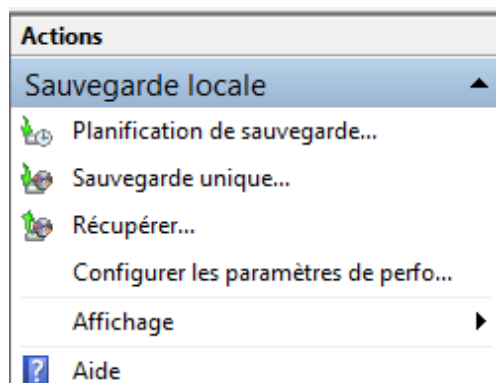
La Fonctionnalité étant à présent installée, nous allons sur Outils dans le Gestionnaire de serveur (à droite de « **Gérer** ») puis « **Sauvegarde Windows Serveur** » dans la liste.

Une nouvelle fenêtre s'ouvrira, nous amenant à la partie suivante.

Configuration de la sauvegarde

Nous voilà dans l'assistant permettant de configurer les sauvegardes ou de récupérer des données.

Dans le bandeau de gauche, on clique sur « **Sauvegarde locale** ».



Dans celui-ci il y'a plusieurs options:

- « Planification de sauvegarde... » : Comme son nom l'indique, cette option de permettra de programmer les sauvegardes. Nous y reviendrons rapidement.
- « Sauvegarde Unique... » : Encore une fois, comme son l'indique, celle-ci nous permet de faire une sauvegarde à l'instant T.
- « Récupérer... » : Permettant de récupérer des données, cette option sera détaillée dans la partie suivante.

Planification de la sauvegarde

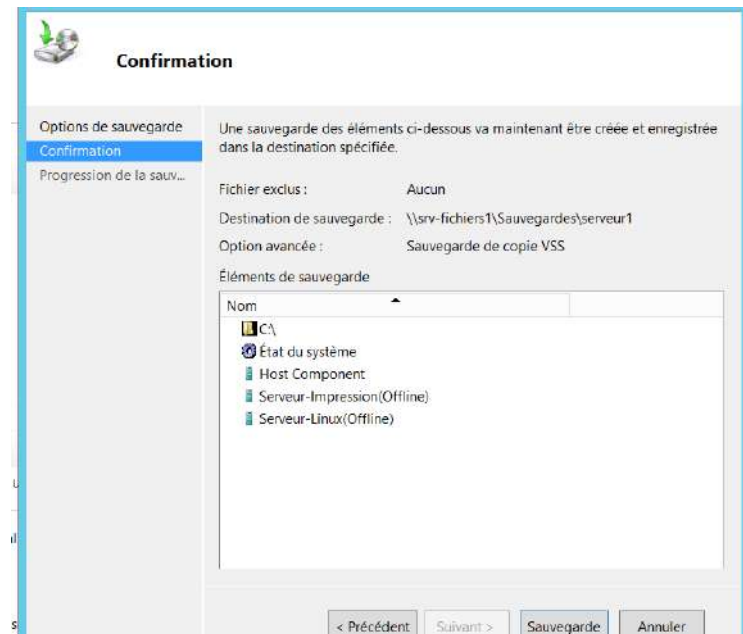
On clique sur son nom pour lancer l'assistant. Après un temps de chargement, « **L'Assistant Planification de sauvegarde** » se lance avec plusieurs étapes :

- « On sélectionne la configuration de sauvegarde » : 2 choix s'offrent à nous:
 - « **Serveur complet** » : Sauvegarde toutes les données et applications présentes sur le serveur ainsi que l'état du système. Faires « **Suivant** » et alors on a accès à « **Spécifier l'heure de la sauvegarde** ».
 - « **Personnalisée** » : On choisit ce que nous allons sauvegarder.
 - « **Suivant** » et vous aura accès à une étape supplémentaire « **Sélectionner les éléments à sauvegarder** » avant « **Spécifier l'heure de la sauvegarde** ».
- « Spécifier l'heure de la sauvegarde » : C'est ici que l'on choisit l'heure de sauvegarde. On a choisi d'effectuer une sauvegarde par jour. **Le mieux est**

de choisir un horaire dans la soirée car la sauvegarde pourra se faire tranquillement dans la nuit.

- « **Spécifier le type de destination** » : ici le on a le choix entre 3 options. Une description se trouve sous chacune d'entres elles.
- « Sélectionner le disque de destination » : On choisit ici le disque sur lequel la sauvegarde devra être stockée. On choisit le disque distant qui est sur le serveur de fichier (\\srv-fichiers1\sauvegarde\serveur1)

- Une fois que le disque est choisi, alors on clique sur « **Suivant** » puis « **Oui** ».
- « Confirmation » : Enfin, on clique sur « **Terminer** ».

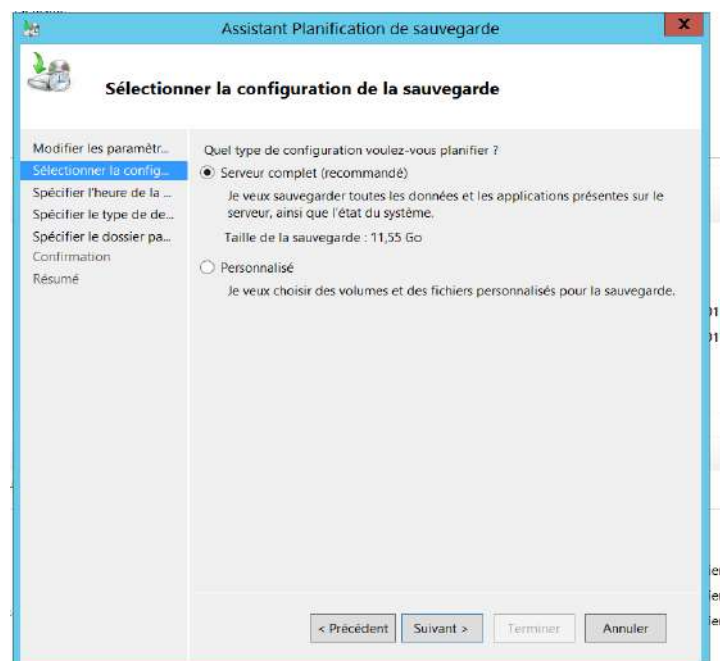


Sauvegarde unique

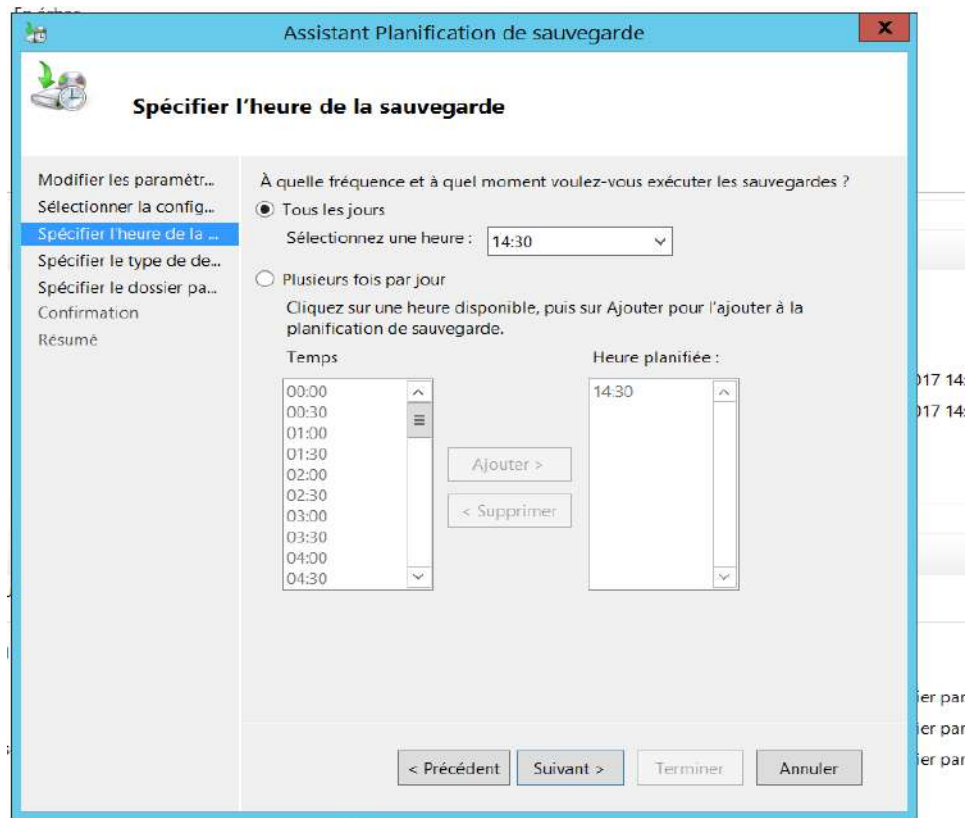
Cette option permet de faire une sauvegarde à l'instant T. Elle s'effectue donc dès que vous l'avez paramétrée.

Sauvegarde sur le serveur de fichier

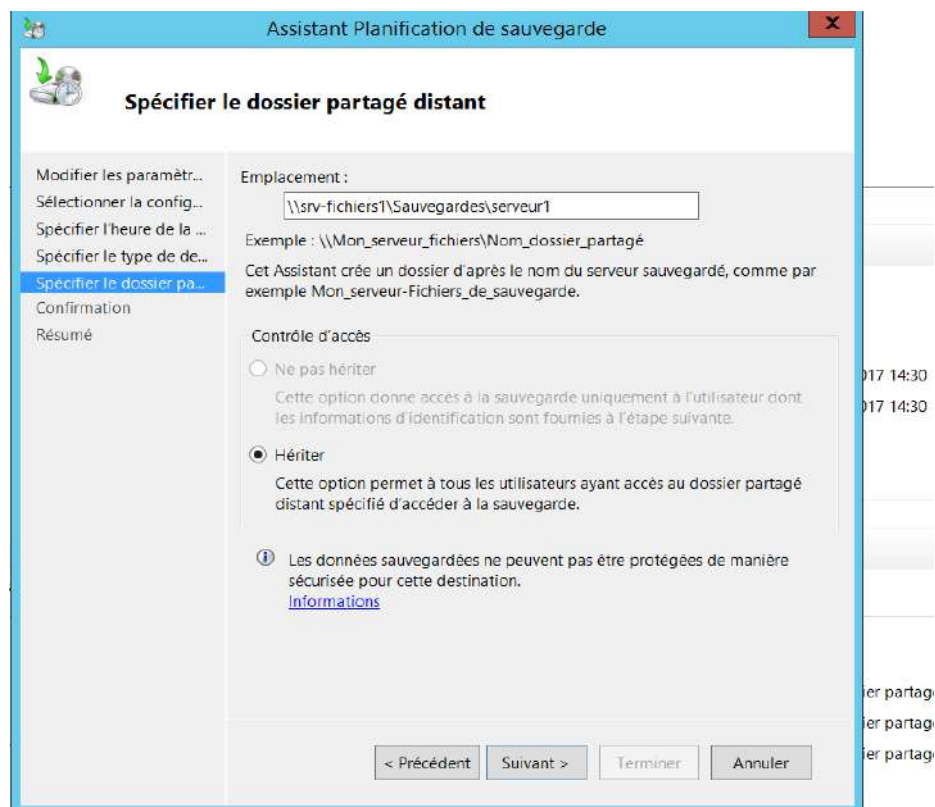
On a donc choisi une sauvegarde complète

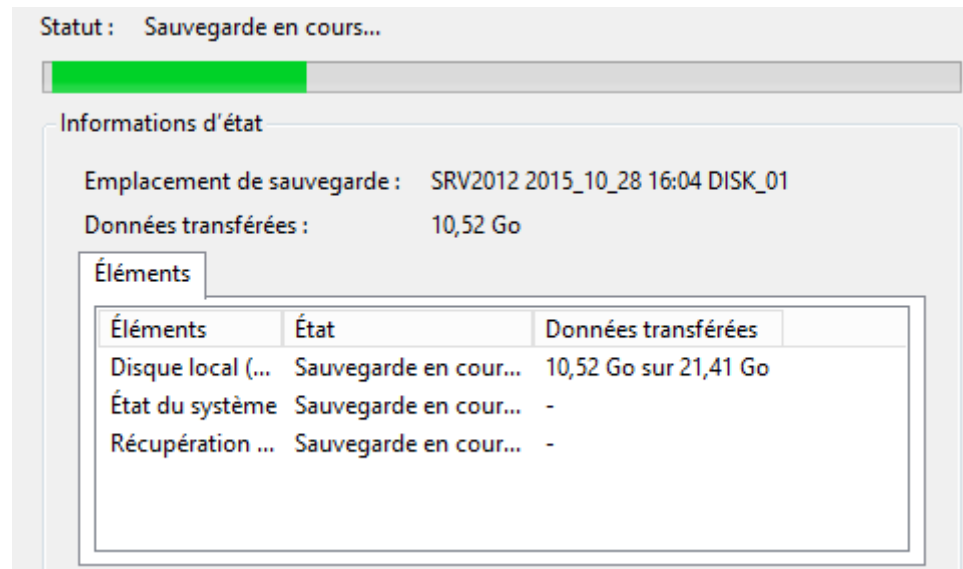


Puis on sélectionne l'heure de la sauvegarde.



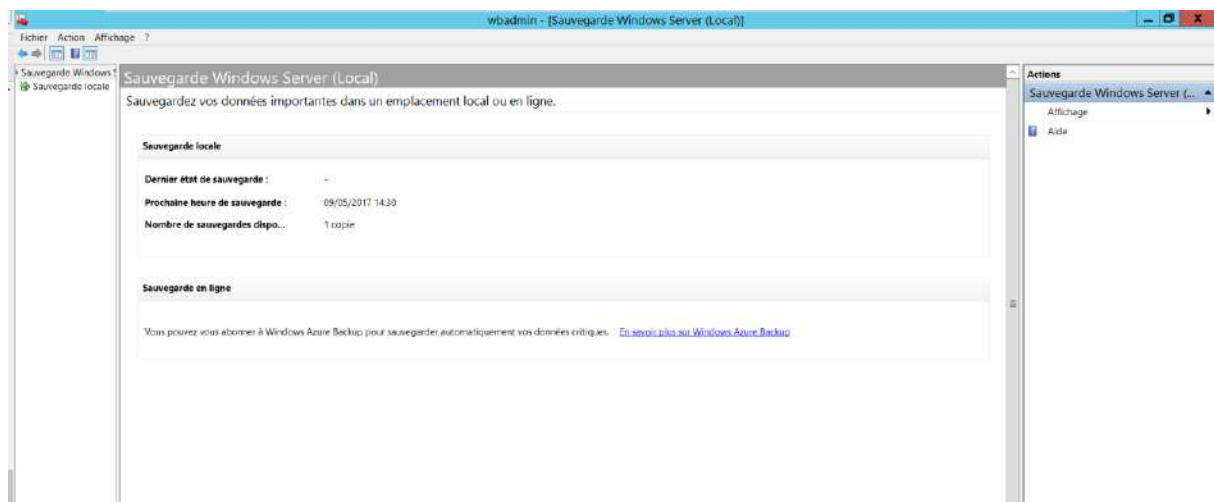
Et ensuite l'emplacement de la sauvegarde.



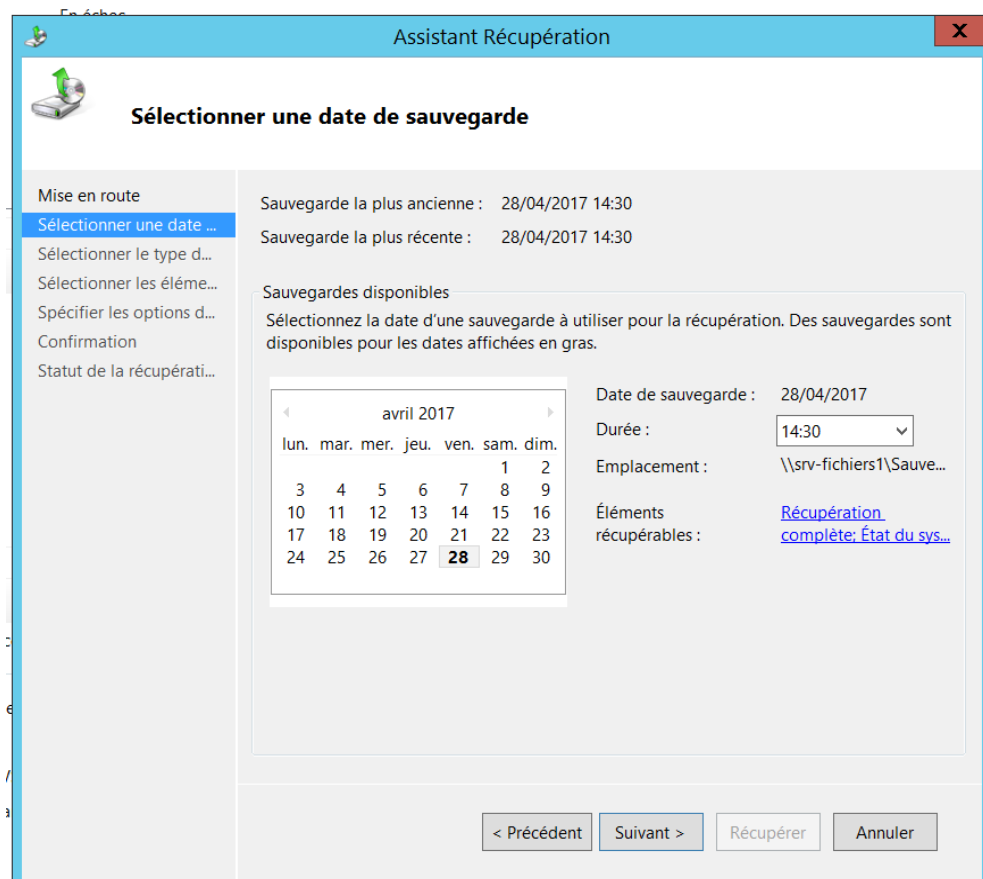
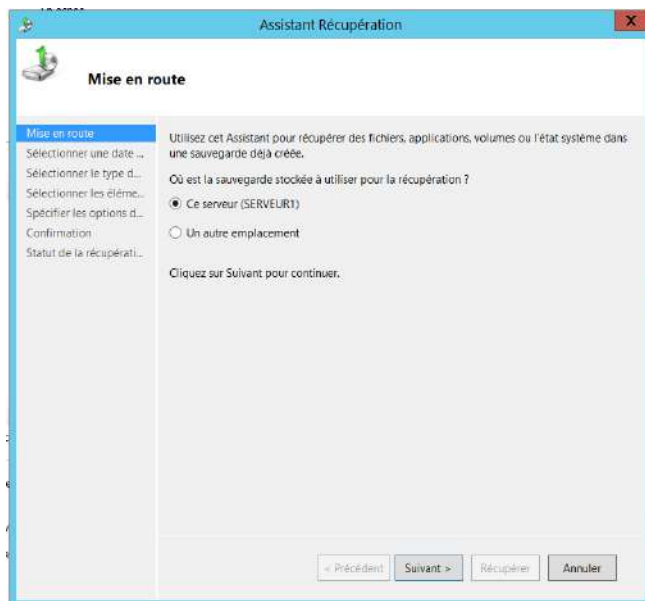


Rapport de Sauvegarde

Nous avons un historique des sauvegardes dans la partie centrale de l'application. On sais alors si la sauvegarde s'est correctement déroulée ou non.



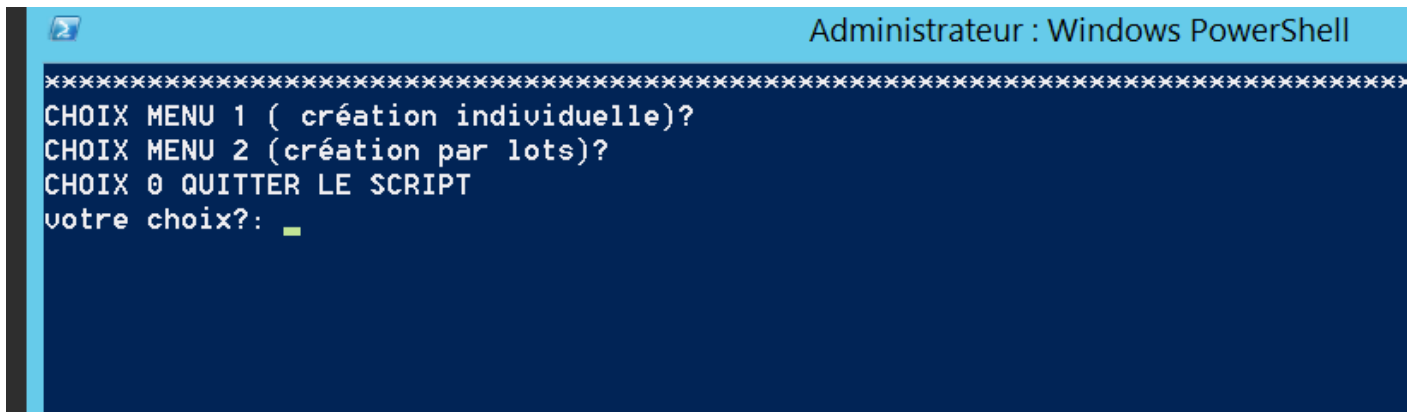
Récupération de sauvegarde



- « Sélectionner le type de récupération » : Différentes options s'offrent à nous selon le type de données que l'on veut récupérer. Encore une fois, une description claire se trouve sous chaque option. Selon certaines options,
- « **Sélectionner les éléments à récupérer** » et « **Spécifier les options de récupérations** », cette dernière nous permet de choisir où est-ce que nous voulons stocker les éléments récupérés.
- « Confirmation » : Cette étape récapitule les réglages
- « **Récupérer** ».
- « Staut » : Nous informe de l'avancement de la récupération. Une fois celle ci terminée, nos données ont été récupérées.

Créations des utilisateurs et des OU

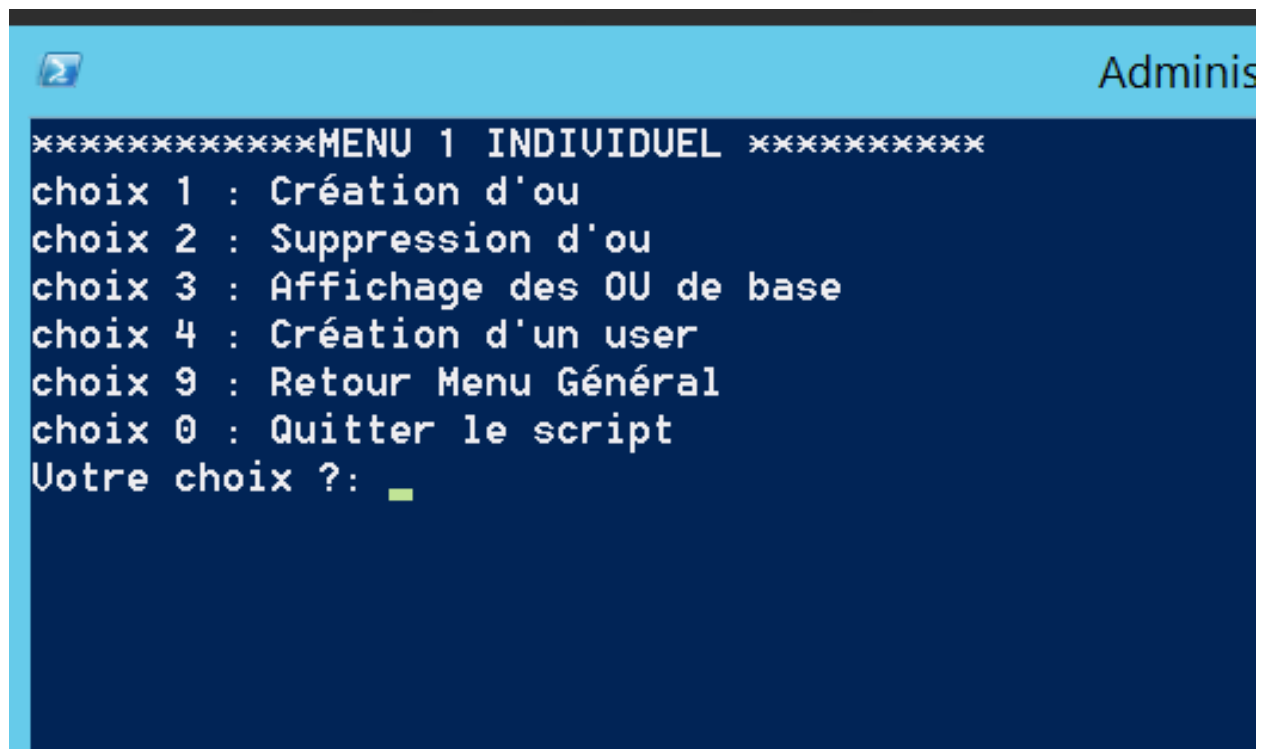
Nous avons mis en place un script pour mettre en place des OU et les Utilisateurs qui y sont liées.
Voici le résultat du script :



```
Administrateur : Windows PowerShell
*****
CHOIX MENU 1 ( création individuelle)?
CHOIX MENU 2 (création par lots)?
CHOIX 0 QUITTER LE SCRIPT
votre choix?:
```

Ci-dessous le menu général.

Ensuite le menu 1 qui permet la création à l'unité.



```
2 Adminis
*****MENU 1 INDIVIDUEL *****
choix 1 : Création d'ou
choix 2 : Suppression d'ou
choix 3 : Affichage des OU de base
choix 4 : Création d'un user
choix 9 : Retour Menu Général
choix 0 : Quitter le script
Votre choix ?:
```

Ensuite le menu 2 avec la création par lots.

```
*****MENU 2 PAR LOTS *****
choix 1 : Création d'ou et des Groupes
choix 2 : Création des Users
choix 3 : permission NTFS sur dossier
choix 4 : Suppression totale
choix 9 : Retour Menu Général
choix 0 : Quitter le script
Votre choix ?:
```

Pour la création d'OU et des groupes le script nous demande L'OU qui nous servira de base et ensuite il prend un cvs comme base de donnée pour la création des OU.

```

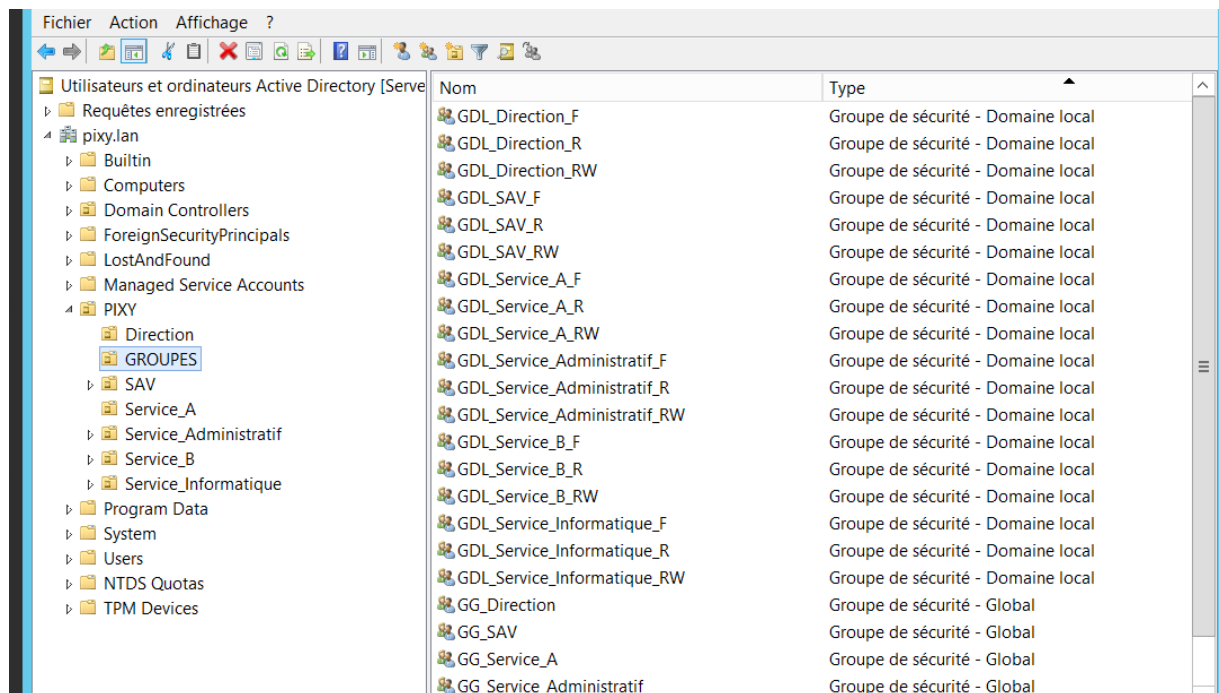
*****MENU 2 PAR LOTS *****
choix 1 : Création d'ou et des Groupes
choix 2 : Création des Users
choix 3 : permission NTFS sur dossier
choix 4 : Suppression totale
choix 9 : Retour Menu Général
choix 0 : Quitter le script
Votre choix ? : 1
Créez votre OU de base ? : PIXY_

```

Voici le résultat de la création des OU et des groupes.

Utilisateurs et ordinateurs Active Directory [Serveur]		Nom	Type
Requêtes enregistrées		Direction	Unité d'organisation
pixy.lan		GROUPE	Unité d'organisation
Builtin		SAV	Unité d'organisation
Computers		Service_A	Unité d'organisation
Domain Controllers		Service_Administratif	Unité d'organisation
ForeignSecurityPrincipals		Service_B	Unité d'organisation
LostAndFound		Service_Informatique	Unité d'organisation
Managed Service Accounts			
PIXY			
Direction			
GROUPE			
SAV			
Service_A			
Service_Administratif			
Service_B			
Service_Informatique			
Program Data			
System			
Users			
NTDS Quotas			
TPM Devices			

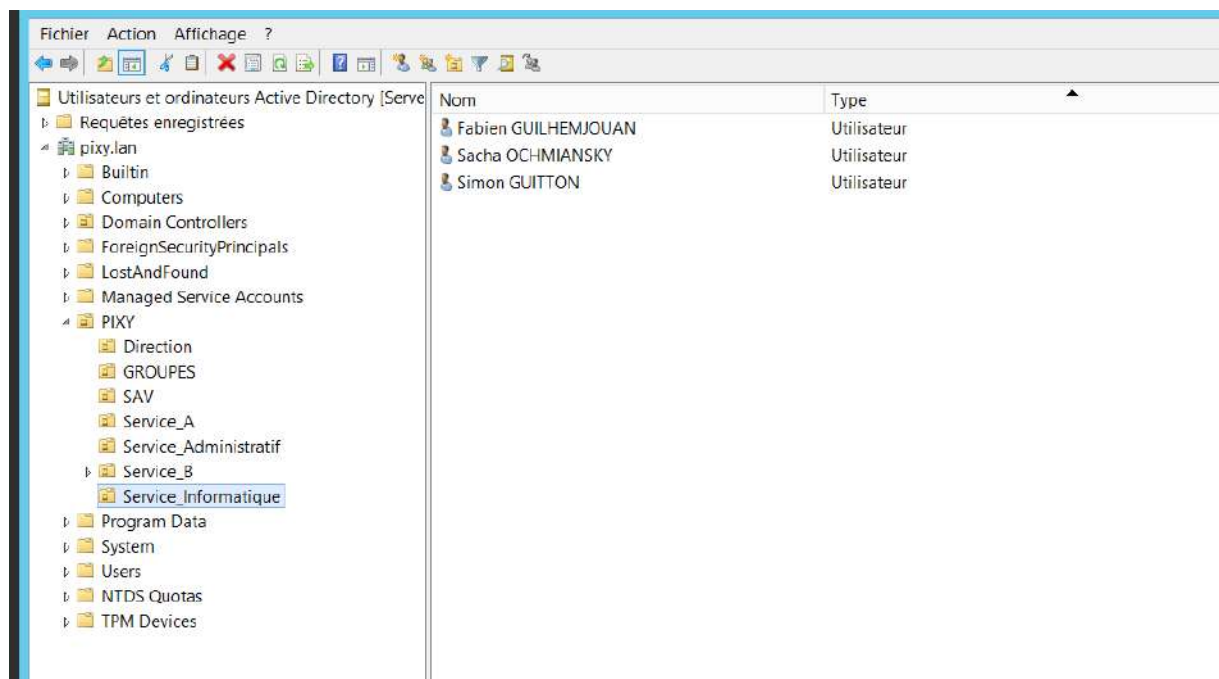
Les groupes ont bien été ajoutés :



The screenshot shows the 'Utilisateurs et ordinateurs Active Directory [Serveur]' window. The left pane shows the tree structure with 'GROUPES' selected under the 'PIXY' container. The right pane displays a list of groups with their names and types.

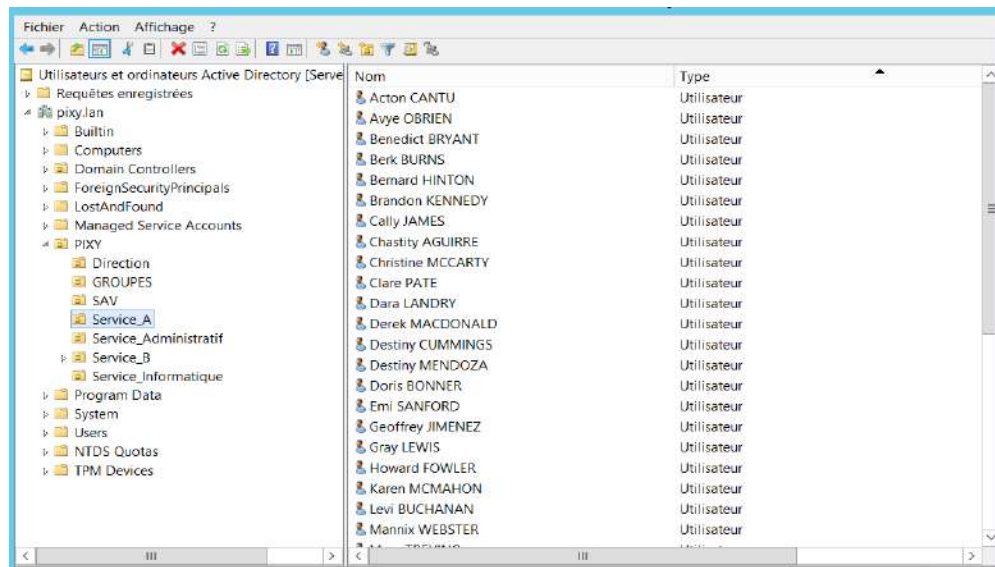
Nom	Type
GDL_Direction_F	Groupe de sécurité - Domaine local
GDL_Direction_R	Groupe de sécurité - Domaine local
GDL_Direction_RW	Groupe de sécurité - Domaine local
GDL_SAV_F	Groupe de sécurité - Domaine local
GDL_SAV_R	Groupe de sécurité - Domaine local
GDL_SAV_RW	Groupe de sécurité - Domaine local
GDL_Service_A_F	Groupe de sécurité - Domaine local
GDL_Service_A_R	Groupe de sécurité - Domaine local
GDL_Service_A_RW	Groupe de sécurité - Domaine local
GDL_Service_Administratif_F	Groupe de sécurité - Domaine local
GDL_Service_Administratif_R	Groupe de sécurité - Domaine local
GDL_Service_Administratif_RW	Groupe de sécurité - Domaine local
GDL_Service_B_F	Groupe de sécurité - Domaine local
GDL_Service_B_R	Groupe de sécurité - Domaine local
GDL_Service_B_RW	Groupe de sécurité - Domaine local
GDL_Service_Informatique_F	Groupe de sécurité - Domaine local
GDL_Service_Informatique_R	Groupe de sécurité - Domaine local
GDL_Service_Informatique_RW	Groupe de sécurité - Domaine local
GG_Direction	Groupe de sécurité - Global
GG_SAV	Groupe de sécurité - Global
GG_Service_A	Groupe de sécurité - Global
GG_Service_Administratif	Groupe de sécurité - Global

De même pour les Utilisateurs provenant du CSV.



The screenshot shows the 'Utilisateurs et ordinateurs Active Directory [Serveur]' window. The left pane shows the tree structure with 'Service_Informatique' selected under the 'PIXY' container. The right pane displays a list of users with their names and types.

Nom	Type
Fabien GUILHEMJOUAN	Utilisateur
Sacha OCHMIANSKY	Utilisateur
Simon GUITTON	Utilisateur

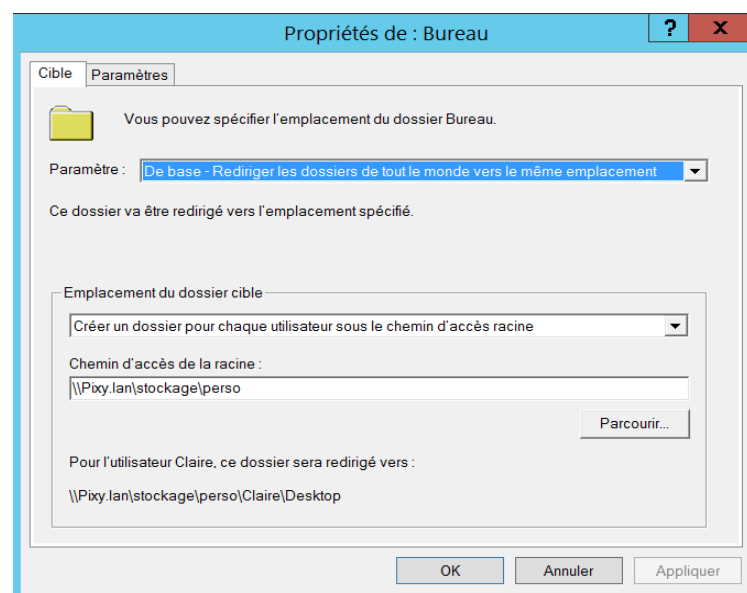


Le Script est en annexe.

Stratégie de groupes

Les stratégies de groupe nous permettent une gestion centralisée dans un environnement Active Directory, notamment la redirection de dossier, le mappage de lecteur réseau, l'autorisation d'utiliser des périphériques ou non, etc...

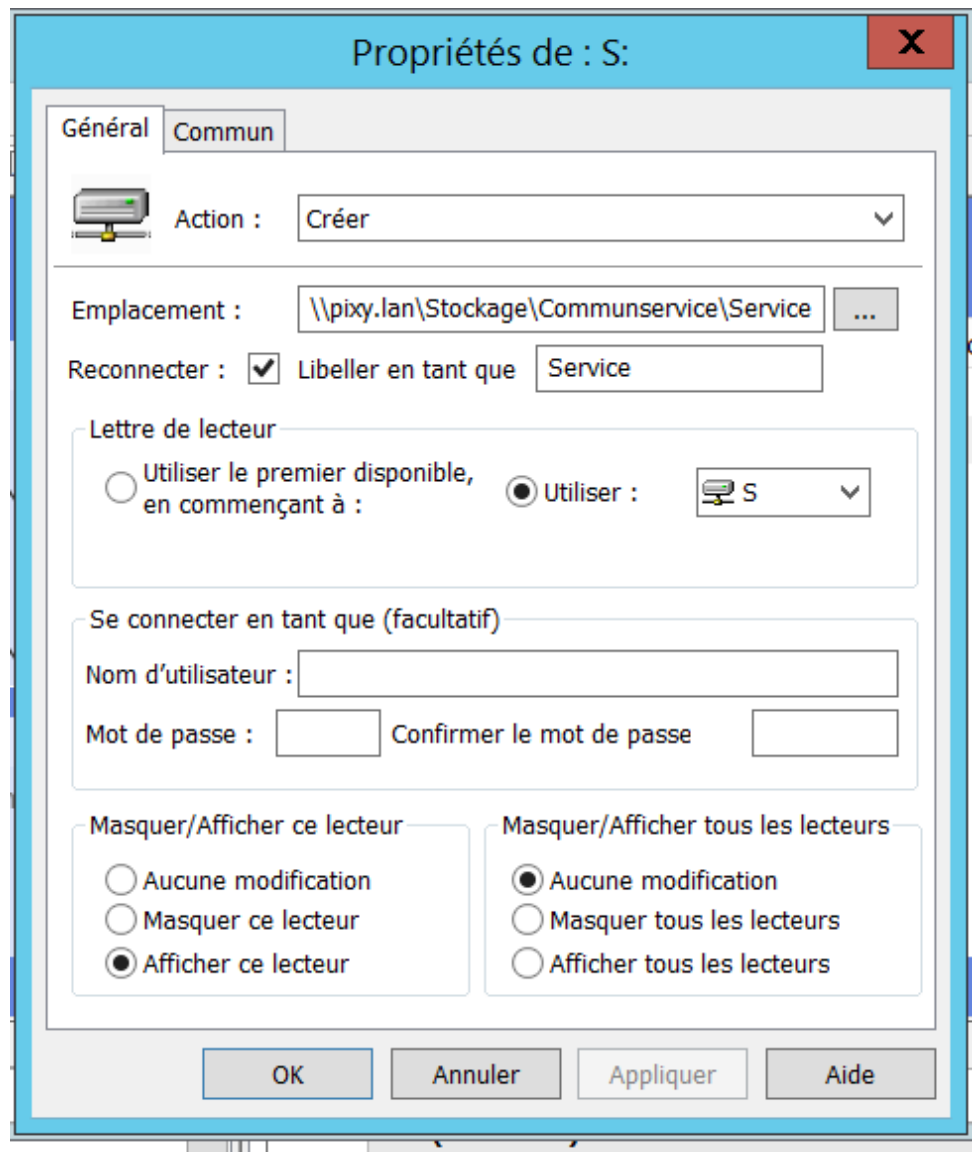
Tous les dossiers présent sur le « **Bureau** » de l'utilisateur concerné seront maintenant redirigé sur le dossier partagé « **Perso** », celui en sera également CRÉATEUR PROPRIÉTAIRE, et aura donc un « **Droit Total** » sur son dossier. La même chose est effectué sur le dossier « **Mes documents** ».



GPO mappage lecteurs

Pour automatiser la montée des lecteurs réseaux sur les sessions Utilisateurs et leur permettre d'accéder à leur dossiers « **Perso** » et « **Service** », nous mettons en place deux mappages de lecteurs réseaux.

Un premier concernant le dossier « **service** » permettant à chacun d'accéder à son dossier de service.



Enfin, le lecteur « **Perso** » qui lui est directement créé en lançant le script de création des Users.

```
function creation_users()
{
    $oubase=Read-Host "OU BASE?"
    $cheminbase="OU="+$oubase+",DC=PIXY,DC=LAN"
    $pass=ConvertTo-SecureString("Blanquefort1") -AsPlainText -Force

    foreach ($i in $utils)
    {
        $nom=($i.nom).ToUpper()
        $prenom=$i.prenom.substring(0,1).ToUpper()+$i.prenom.substring(1).ToLower()
        $nomcomplet=$prenom+" "+$nom
        $login=$prenom.ToLower()+"."+ $nom.ToLower()
        $supn=($login+"@"+$env:USERDNSDOMAIN).ToLower()
        $titre=$i.fonction
        $service=$i.service
        $cheminuser="OU="+$service+", "+$cheminbase
        $groupe="GG_"+$service
        $description=$i.description
        $cheminlecteur="//Pixy.lan\stockage\perso\"+$login
    }
}
```

GPO supplémentaires

Dans le cahier des charges il nous est demandé de paramétrer :

- 3 journaux sur 3 jours :

Journaux

Données recueillies le : 09/05/2017 10:45:34

Configuration ordinateur (activée) [masquer](#)

Stratégies [masquer](#)

Paramètres Windows [masquer](#)

Paramètres de sécurité [masquer](#)

Journal des événements [masquer](#)

Stratégie	Paramètre
Conserver le journal de sécurité	3 jours
Conserver le journal des applications	3 jours
Conserver le journal système	3 jours
Méthode de conservation du journal de sécurité	Par jour
Méthode de conservation du journal des applications	Par jour
Méthode de conservation du journal système	Par jour

Configuration utilisateur (activée) [masquer](#)

Aucun paramètre n'est défini.

- 2 audits au hasard :

audit 1 - evement système

Données recueillies le : 09/05/2017 10:45:16

Configuration ordinateur (activée) [masquer](#)

Stratégies [masquer](#)

Paramètres Windows [masquer](#)

Paramètres de sécurité [masquer](#)

Stratégie locale/Stratégie d'audit [masquer](#)

Stratégie	Paramètre
Auditer les événements système	Échec

Configuration utilisateur (activée) [masquer](#)

Aucun paramètre n'est défini.

audit - 2 connexion au compte		
Étendue	Détails	Paramètres
audit - 2 connexion au compte		
Données recueillies le : 09/05/2017 10:44:35		
Configuration ordinateur (activée)		afficher tout
Stratégies		masquer
Paramètres Windows		masquer
Paramètres de sécurité		masquer
Stratégie locale/Stratégie d'audit		masquer
Stratégie	Paramètre	
Auditer les événements de connexion aux comptes	Opération réussie	
Configuration utilisateur (activée)		masquer
Aucun paramètre n'est défini.		

- La désactivation du moniteur d'événement.

desactiver moniteur d'evenements		
Étendue	Détails	Paramètres
desactiver moniteur d'evenements		
Données recueillies le : 09/05/2017 10:45:32		
Configuration ordinateur (activée)		afficher tout
Stratégies		masquer
Modèles d'administration		masquer
Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.		
Système		masquer
Stratégie	Paramètre	Commentaire
Afficher le moniteur d'événements de mise hors tension	Désactivé	
Configuration utilisateur (activée)		masquer
Aucun paramètre n'est défini.		

Installation logiciel

De la même manière que pour la redirection des dossiers nous allons créer une GPO interdisant les utilisateurs d'installer des logiciels.

Interdire l'installations de logiciel

Étendue | Détails | Paramètres | Délégation

Données recueillies le : 09/05/2017 11:02:29 [afficher tout](#)

Configuration ordinateur (activée) [masquer](#)

Stratégies [masquer](#)

Paramètres Windows [masquer](#)

Paramètres de sécurité [masquer](#)

Stratégies de restriction logicielle [afficher](#)

Stratégies de restriction logicielle/Niveaux de sécurité [afficher](#)

Stratégies de restriction logicielle/Règles additionnelles [masquer](#)

Règles de chemins d'accès [afficher](#)

Modèles d'administration [masquer](#)

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

Composants Windows/Windows Installer [masquer](#)

Stratégie	Paramètre	Commentaire
Désactiver Windows Installer	Activé	Toujours
Interdire les installations par les utilisateurs	Activé	Masquer l'installation par l'utilisateur

Configuration utilisateur (activée) [masquer](#)

Aucun paramètre n'est défini.

Désactivation du lecteur CD

Lecteur CD désactiver

Étendue | Détails | Paramètres | Délégation

Données recueillies le : 13/05/2017 17:38:15 [afficher tout](#)

Configuration ordinateur (activée) [masquer](#)

Aucun paramètre n'est défini.

Configuration utilisateur (activée) [masquer](#)

Stratégies [masquer](#)

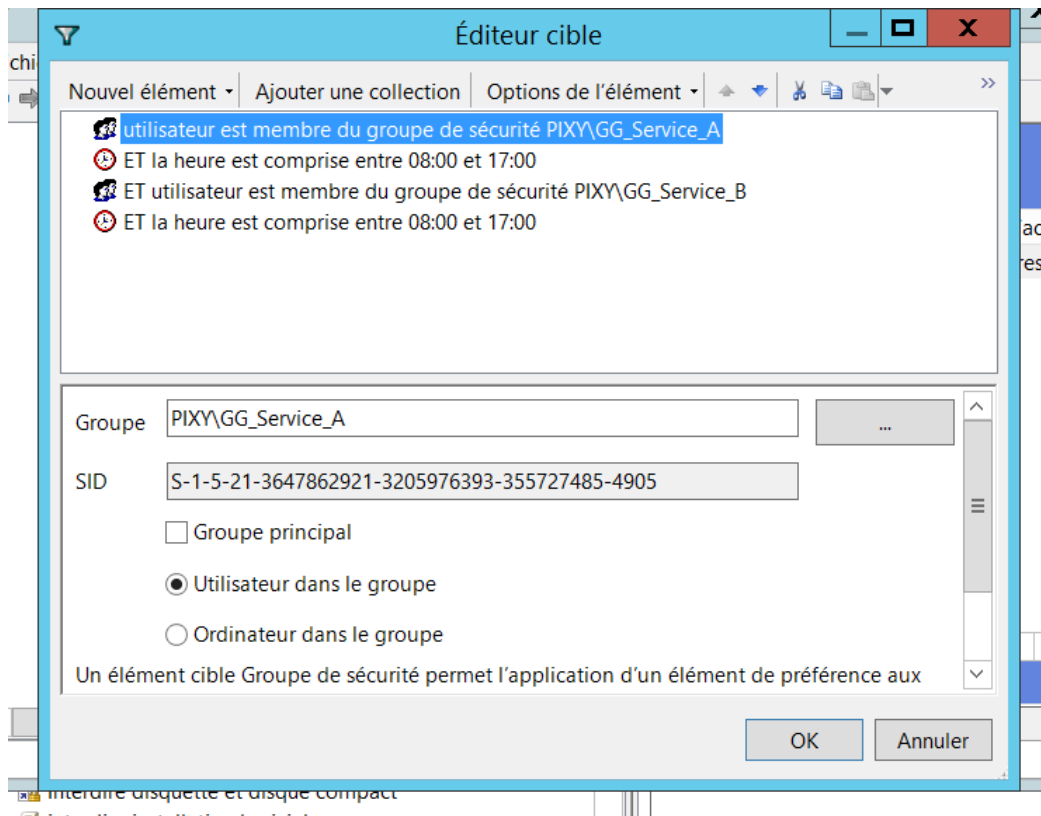
Modèles d'administration [masquer](#)

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

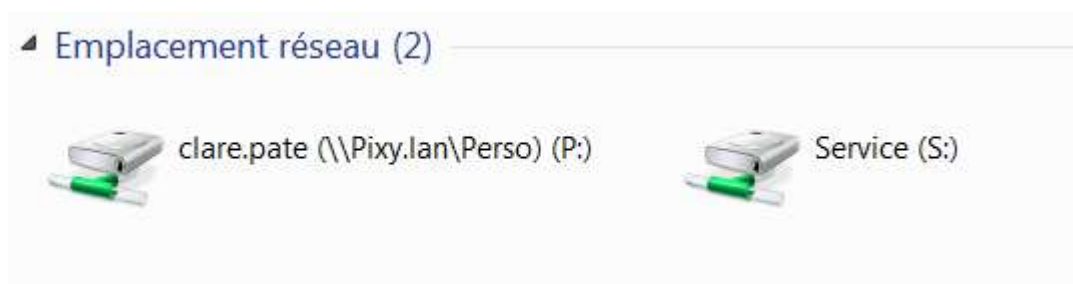
Système/Accès au stockage amovible [masquer](#)

Stratégie	Paramètre	Commentaire
CD et DVD : refuser l'accès en écriture	Activé	
CD et DVD : refuser l'accès en lecture	Activé	

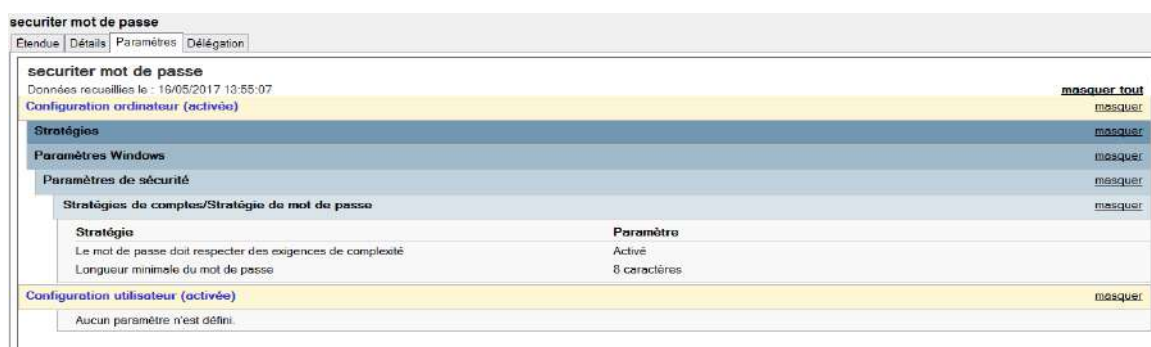
Horaire d'impression



Partage des lecteurs réseau



Complexité du mot de passe



Serveur de fichiers DFS (Distributed File System)

Un serveur de fichiers permet de stocker les documents des différents services des utilisateurs de l'entreprise. Il assure le partage des dossiers au sein du réseau et les rend accessibles depuis les clients en respectant les stratégies de groupe mises en place au niveau de l'Active Directory.

Il est primordial que dans une entreprise de la taille de PIXY, l'ensemble du personnel puisse échanger des fichiers sans avoir recours à des protocoles de partage peu sécurisés, tel que les mails ou les supports amovibles. Grâce au DFS, le serveur auquel accède l'utilisateur pour lire un fichier n'est pas visible par ce dernier. Nous avons configuré deux serveurs derrière le même espace de nom. Ils contiennent les mêmes données grâce à la réplication DFSR. Cette dernière assure notamment la réplication SYSVOL. Cette solution nous permet de maintenir une haute disponibilité de données, car si l'un des serveurs n'est plus disponible, les données seront toujours accessibles depuis l'autre serveur.

Lorsque l'on parle de DFS, les trois termes importants à retenir sont :

- **Racine DFS** : Point d'entrée principal d'un système DFS, la racine DFS contient le chemin d'accès aux différentes liaisons DFS qui lui sont associées.
- **Dossier** : Le dossier sera le nom du partage affiché côté client et dans la configuration du serveur, une liaison sera effectuée entre ce dossier DFS et la cible DFS afin de faire un lien entre les deux éléments. Les dossiers sont également appelés « Liaison DFS ».
- **Cible** : Serveur sur lequel sont situées les données, la cible représente le chemin d'accès vers le dossier partagé situé sur ce serveur.

Ces 3 éléments sont essentiels à la mise en place d'une infrastructure DFS.

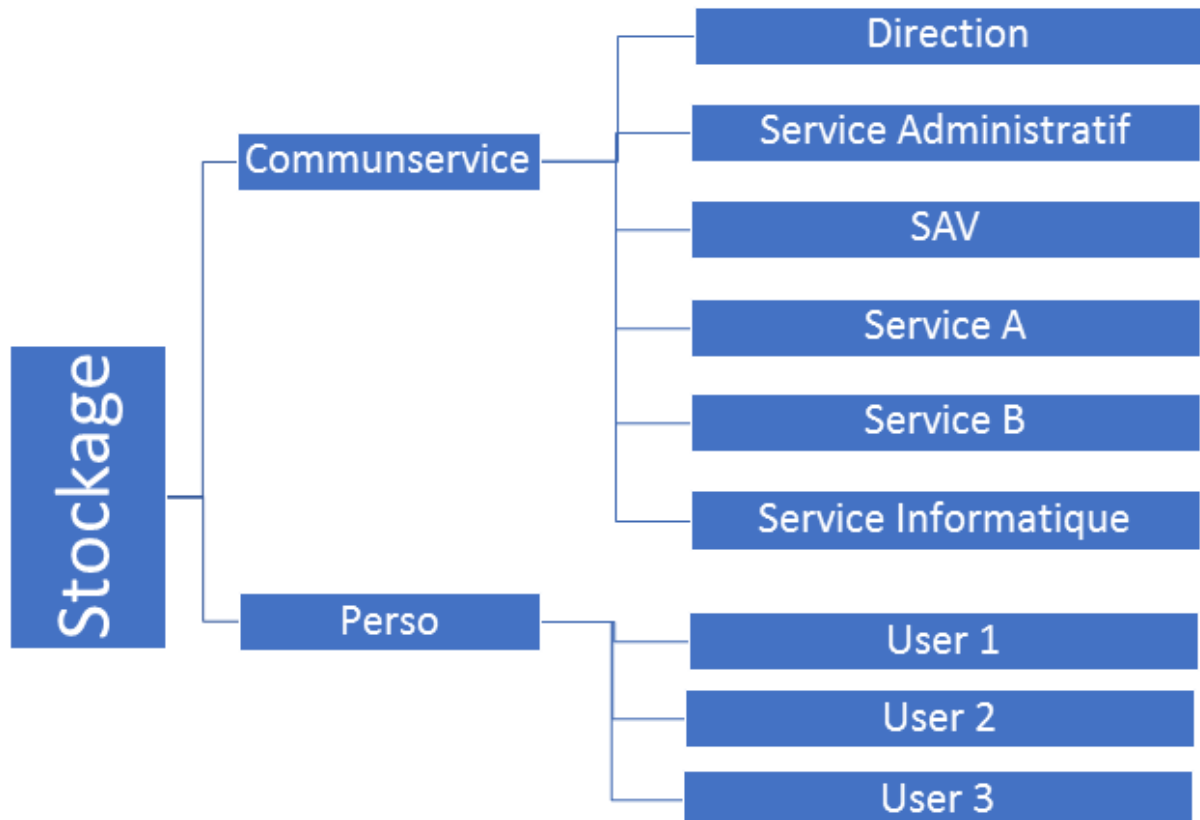
Les rôles de serveur de fichier seront attribués à nos deux NAS qui sont compatibles avec l'authentification windows. Il seront configurés en respectant les différents critères du cahier des charges :

- Chaque service doit avoir un répertoire qui sera attribué à chacun des salariés lors de sa connexion réseau.
- À l'intérieur de chaque répertoire, les utilisateurs du service devront avoir leur dossier personnel.
- L'utilisateur devra avoir un contrôle total sur son dossier personnel et aucun accès sur le dossier de ses collègues.

- Les membres de la direction pourront avoir un droit de lecture sur les répertoires et les membres du service informatique auront un contrôle total sur les dossiers de partage.

Nous créerons deux partages. Un premier, nommé « Communservice », qui contiendra les dossiers communs des différents services, et un second nommé « Perso », regroupant les répertoires personnels des utilisateurs.

Voici à quoi ressemblera l'arborescence :



Linux

Vous pourrez trouver la procédure d'installation du serveur Debian en annexe.

Une fois le serveur démarré, nous nous identifions en root.

```
Debian GNU/Linux 8 SRVLINUX tty1

SRVLINUX login: root
Password:
Last login: Fri Apr 28 16:03:52 CEST 2017 on tty1
Linux SRVLINUX 3.16.0-4-amd64 #1 SMP Debian 3.16.39-1+deb8u2 (2017-03-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@SRVLINUX:~#
```

En tapant « **nano /etc/network/interfaces** », nous pouvons modifier certaines informations. Nous avons donc configuré notre adresse IP, notre netmask, gateway et dns-nameserver. Il faut également ajouter « **iface lo inet loopback** ».

```
GNU nano 2.2.6          Fichier : /etc/network/interfaces

# 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
#auto eth0
allow-hotplug eth0
iface eth0 inet static
address 192.168.1.7
netmask 255.255.255.0
gateway 192.168.1.2
dns-nameserver 192.168.1.5
```

Ensuite, il faut redémarrer le service networking.

```
root@SRVLINUX:~# service networking restart
```

Dans le fichier « **/etc/resolv.conf** »,il faut bien sélectionner le nom de domaine et le nameserver.

```
GNU nano 2.2.6          Fichier : /etc/resolv.conf

domain pixy.lan
search pixy.lan
nameserver 192.168.1.5
```

Pour pouvoir attribuer des droits aux autres utilisateurs que root, il faut installer « **sudo** ».

```
root@SRV LINUX:~# apt-get install sudo
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
```

Samba

Il nous faut Samba pour le partage de ressources vers notre serveur de fichier Windows..

Il faut maintenant créer une table de partition en sélectionnant « **partition primaire** », puis en choisissant les valeurs par défaut par la suite. Ne pas oublier de sauvegarder les modifications en appuyant sur « **W** » et en le validant.

```
root@SRV LINUX:~# fdisk /dev/sdb

Bienvenue dans fdisk (util-linux 2.25.2).
Les modifications resteront en mémoire jusqu'à écriture.
Soyez prudent avant d'utiliser la commande d'écriture.

Le périphérique ne contient pas de table de partitions reconnue.
Created a new DOS disklabel with disk identifier 0xd68fb363.

Commande (m pour l'aide) : n
Type de partition
  p primaire (0 primaire, 0 étendue, 4 libre)
  e étendue (conteneur pour partitions logiques)
Sélectionnez (p par défaut) : p
Numéro de partition (1-4, 1 par défaut) :
Premier secteur (2048-2097151999, 2048 par défaut) :
Dernier secteur, +secteurs ou +taille{K,M,G,T,P} (2048-2097151999, 2097151999 par défaut) :

Une nouvelle partition 1 de type « Linux » et de taille 1000 GiB a été créée.
```

Il faut maintenant formater la table de partition créée précédemment.

```
root@SRV LINUX:~# mkfs.ext4 /dev/sdb1
mke2fs 1.42.12 (29-Aug-2014)
En train de créer un système de fichiers avec 262143744 4k blocs et 65536000 i-noeuds.
UUID de système de fichiers=3da1793e-8404-4064-995e-cf34b8d939a0
Superblocs de secours stockés sur les blocs :
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000, 23887872, 71663616, 78675968,
    102400000, 214990848

Allocation des tables de groupe : complété
Écriture des tables d'i-noeuds : complété
Création du journal (32768 blocs) : complété
Écriture des superblocs et de l'information de comptabilité du système de
fichiers : complété
```

Ne pas oublier de modifier ce fichier en ajoutant la dernière ligne avant de redémarrer.

```

GNU nano 2.2.6          Fichier : /etc/fstab

# /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>
/dev/mapper/SRV--FICHIER22--vg-root /          ext4      errors=remount-ro 0      1
# /boot was on /dev/sda1 during installation
UUID=f3797c04-dc55-498d-af07-b92f4900ec61 /boot      ext2      defaults          0      0
/dev/mapper/SRV--FICHIER22--vg-home /home      ext4      defaults          0      2
/dev/mapper/SRV--FICHIER22--vg-tmp /tmp       ext4      defaults          0      2
/dev/mapper/SRV--FICHIER22--vg-var /var       ext4      defaults          0      2
/dev/mapper/SRV--FICHIER22--vg-swap_1 none      swap      sw                0      0
/dev/sr0      /media/cdrom0  udf,iso9660 user,noauto      0      0
/dev/sdb1     /samba ext4      defaults          0      2_

```

Il va falloir créer le dossier samba dans lequel nous créons un fichier, puis il faut attacher la partition à l'arborescence.

```

root@SRV LINUX:~# mkdir /samba
root@SRV LINUX:~# touch /samba/fichier1
root@SRV LINUX:~# mount /dev/sdb1 /samba/

```

Il va falloir répéter les mêmes opérations 2 fois pour les données FTP et les données NFS.

Il faut maintenant installer le client ci-dessous.

```
apt-get install samba smbclient samba-common winbind_
```

Puis modifier le fichier.

```

GNU nano 2.2.6          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]

## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will part of
Workgroup = PIXY_
realm = pixy.lan
security = ADS
password server = SERVEUR1.pixy.lan
os level = 0
local master = No
domain master = No
template shell = /bin/bash
winbind enum users = yes
winbind enum groups = yes
winbind use default domain = true
idmap config PIXY : schema_mode = rfc2307
idmap config PIXY : range = 10000000-19000000
idmap config PIXY : default = yes
idmap config PIXY : backend = rid
idmap config * : range = 20000-29999
idmap config * : backend = tdb

```

```
GNU nano 2.2.6          Fichier : /etc/samba/smb.conf

# Windows clients look for this share name as a source of downloadable
# printer drivers
[print$]
    comment = Printer Drivers
    path = /var/lib/samba/printers
    browseable = yes
    read only = yes
    guest ok = no
# Uncomment to allow remote administration of Windows print drivers.
# You may need to replace 'lpadmin' with the name of the group your
# admin users are members of.
# Please note that you also need to set appropriate Unix permissions
# to the drivers directory for these users to have write rights in it
;   write list = root, @lpadmin

[fichier]
    comment = Fichier de la societe
    path = /samba
    read only = no
    guest ok = yes
    public = yes
```

Il faut redémarrer le service.

```
root@SRV LINUX:~# service winbind stop
root@SRV LINUX:~# service smbd restart
root@SRV LINUX:~# service winbind start
```

On tente de joindre l'Active Directory.

```
root@SRV LINUX:~# net join -S SERVEUR1.pixy.lan -U administrateur
```

Pour en être sûr, on affiche la liste des utilisateurs.

```
madaline.richardson  
ainsley.pacheco  
emerson.sweet  
rina.suarez  
martha.morrow  
jenette.ramos  
kitra.parsons  
calvin.hudson  
colt.hurley  
gannon.hughes  
xenos.perkins  
yvette.reynolds  
stuart.kent  
gabriel.henson  
murphy.calderon  
roary.mooney  
gerard.gabriel  
mme.laporte  
nicolas.peltier  
cooper.benson  
avram.hudson  
julie.ballard  
adele.owen  
mary.hendricks  
damian.flores  
chaim.jarvis  
leila.jensen  
lacey.dudley  
beck.humphrey  
sonia.lahecoun  
harcen.uber  
simon.guitton  
sacha.ochmiansky  
fabien.guilhemjouan  
vincent.edmond
```

DHCP

Le rôle DHCP est mis en place sur notre contrôleur de domaine, mais nous décidons d'installer le rôle sur notre Debian aussi, sans pour autant l'activer.

On installe DHCP.

```
root@SRV-FICHER22:~# apt-get install isc-dhcp-server
```

Dans le fichier « **/etc/default/isc-dhcp-server** », il faut modifier le fichier DHCP en ajoutant « **eth0** » en bas.


```
GNU nano 2.2.6          Fichier : /etc/default/isc-dhcp-server

# Defaults for isc-dhcp-server initscript
# sourced by /etc/init.d/isc-dhcp-server
# installed at /etc/default/isc-dhcp-server by the maintainer scripts
#
# This is a POSIX shell fragment
#
# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPD_CONF=/etc/dhcp/dhcpd.conf
#
# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPD_PID=/var/run/dhcpd.pid
#
# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""
#
# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACES="eth0"
```

Dans le fichier « **/etc/dhcp/dhcpd.conf** », il faut renseigner le nom de domaine et l'adresse IP du contrôleur de domaine comme ci-dessous.

```
GNU nano 2.2.6          Fichier : /etc/dhcp/dhcpd.conf          Modifié

#
# Sample configuration file for ISC dhcpd for Debian
#
#
# The ddns-update-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# option definitions common to all supported networks...
option domain-name "pixy.lan";
option domain-name-servers 192.168.1.5;

default-lease-time 600;
max-lease-time 7200;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
#authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

#subnet 10.152.187.0 netmask 255.255.255.0 {
#}
```

Dans le même fichier, il faut également renseigner les bons subnet et netmask ainsi que le range et l'option routers comme ci-dessous.

```

GNU nano 2.2.6 Fichier : /etc/dhcp/dhcpd.conf Modifié

default-lease-time 600;
max-lease-time 7200;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
#authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

#subnet 10.152.187.0 netmask 255.255.255.0 {
#}

# This is a very basic subnet declaration.

subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.15 192.168.1.135;
    option routers 192.168.1.2;
}

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

#subnet 10.254.239.32 netmask 255.255.255.224 {
#    range dynamic-bootp 10.254.239.40 10.254.239.60;
#    option broadcast-address 10.254.239.31;
#    option routers rtr-239-32-1.example.org;
#}

G Aide      O Écrire  R Lire fich.  Y Page préc.  K Couper      C Pos. cur.
X Quitter  J Justifier  K Chercher  V Page suiv.  U Collier    I Orthograp.

```

On stop le service, puis on regarde son statut. Il est bien désactivé.

```

root@SRV1LINUX:~# service isc-dhcp-server stop
root@SRV1LINUX:~# service isc-dhcp-server status
• isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server)
   Active: inactive (dead) since dim. 2017-04-30 21:30:28 CEST; 2s ago
   Process: 1679 ExecStop=/etc/init.d/isc-dhcp-server stop (code=exited, status=0/SUCCESS)
   Process: 652 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)

avril 30 20:38:51 SRV1LINUX dhcpd[708]: Copyright 2004-2014 Internet Systems Consortium.
avril 30 20:38:51 SRV1LINUX dhcpd[708]: All rights reserved.
avril 30 20:38:51 SRV1LINUX dhcpd[708]: For info, please visit https://www.isc.org/software/dhcp/
avril 30 20:38:51 SRV1LINUX dhcpd[708]: Wrote 6 leases to leases file.
avril 30 20:38:51 SRV1LINUX dhcpd[715]: Server starting service.
avril 30 20:38:53 SRV1LINUX isc-dhcp-server[652]: Starting ISC DHCP server: dhcpd.
avril 30 20:38:53 SRV1LINUX systemd[1]: Started LSB: DHCP server.
avril 30 21:30:28 SRV1LINUX systemd[1]: Stopping LSB: DHCP server...
avril 30 21:30:28 SRV1LINUX isc-dhcp-server[1679]: Stopping ISC DHCP server: dhcpd.
avril 30 21:30:28 SRV1LINUX systemd[1]: Stopped LSB: DHCP server.

```

NTP

On installe ntp.

```
apt-get install ntp
```

Il faut modifier le fichier « **/etc/ntp.conf** » en renseigner le nom du contrôleur de domaine en bas.

```
GNU nano 2.2.6          Fichier : /etc/ntp.conf

# /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 SERVEUR1.pixy.lan
```

On démarre le service ntp.

```
root@SRV LINUX:~# /etc/init.d/ntp start
[ ok ] Starting ntp (via systemctl): ntp.service.
root@SRV LINUX:~#
```

Host

Dans le fichier « **/etc/hosts** », il faut renseigner son adresse IP, son nom de serveur, puis son nom de machine.

```
GNU nano 2.2.6      Fichier : /etc/hosts      Modifié
127.0.0.1      localhost
192.168.1.7    SRV LINUX.pixy.lan      SRV LINUX_

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

Krb5

Il faut installer « **krb5** », avec la commande « **apt-get install krb5** », puis il faut modifier le fichier « **/etc/krb5.conf** » comme ci-dessous.

```
GNU nano 2.2.6      Fichier : /etc/krb5.conf

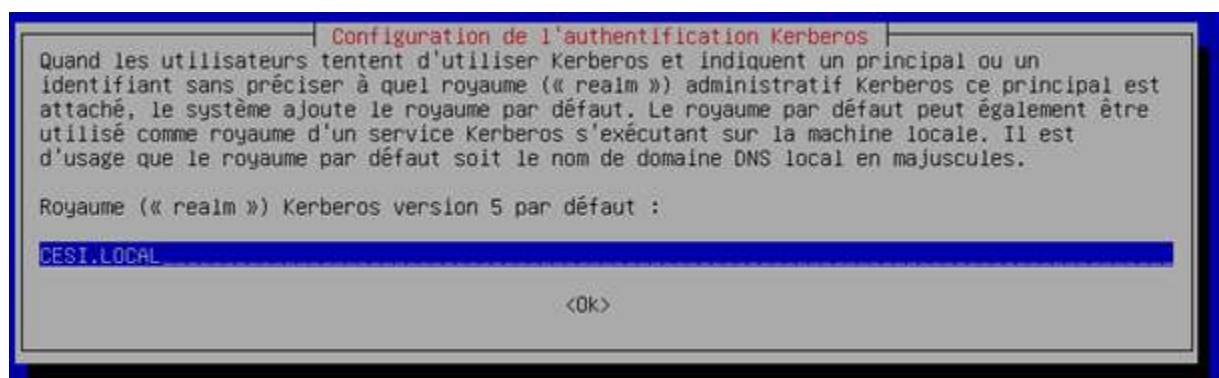
        rcmd = host
        ftp = ftp
    }
    plain = {
        something = something-else
    }
    fcc-mit-ticketflags = true

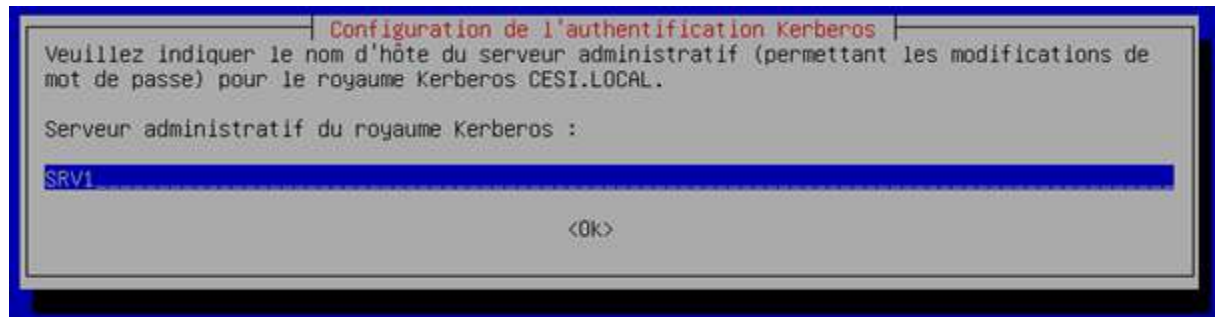
[realms]
    PIXY.LAN = {
        kdc = SERVEUR1.pixy.lan
        admin_server = SERVEUR1.pixy.lan
        default_domain = pixy.lan
    }

[domain_realm]
    .pixy.lan = PIXY.LAN
    pixy.lan = PIXY.LAN

[login]
    krb4_convert = true
    krb4_get_tickets = false
```

Il faut configurer l'authentification Kerberos.





Apache2

On installe Apache2.

```
apt-get install apache2
```

On fait une copie du fichier « **000-default.conf** ».

```
root@SRVLINUX:~# cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/parc.conf
```

Il faut modifier le fichier « **/etc/apache2/sites-available/parc.conf** » comme ci-dessous.

```
GNU nano 2.2.6      Fichier : /etc/apache2/sites-available/parc.conf

<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.

    ServerName SERVEUR1.pixy.lan
```

On crée un fichier inventaire.

```
root@SRVLINUX:~# mkdir /var/www/parc
```

Grep.

```
root@debian:~# grep www-data /etc/passwd
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
root@debian:~#
```

Il faut modifier le fichier ci-dessous.

```
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/bin/bash
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
```

Nous choisissons un mot de passe UNIX.

```
root@SRV LINUX:~# passwd www-data
Enter new password:
Retype new password:
passwd : le mot de passe a été mis à jour avec succès
root@SRV LINUX:~# _
```

Il faut activer le site « **parc** ».

```
root@SRV LINUX:~# a2ensite parc
```

Il faut redémarrer le service apache2.

```
root@SRV LINUX:~# service apache2 restart
```

PAM

On installe libpam.

```
apt-get install libnss-winbind libpam-winbind
```

```
root@SRV-FICHER22:~# getent passwd | grep simon
simon:x:1000:1000:simon guiton,,,:/home/simon:/bin/bash
root@SRV-FICHER22:~# getent passwd | grep administrateur
root@SRV-FICHER22:~# _
```

On modifie le fichier.


```

GNU nano 2.2.6      Fichier : /etc/pam.d/common-session
#
# /etc/pam.d/common-session - session-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be performed
# at the start and end of sessions of *any* kind (both interactive and
# non-interactive).
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
session [default=1]                pam_permit.so
# here's the fallback if no module succeeds
session requisite                  pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
session required                  pam_permit.so
# and here are more per-package modules (the "Additional" block)
session optional                  pam_krb5.so minimum_vid=1000
session required                  pam_unix.so
session required                  pam_nkhomedir.so umask=0022 skel=/etc/skel
session optional                  pam_winbind.so _
# end of pam-auth-update config

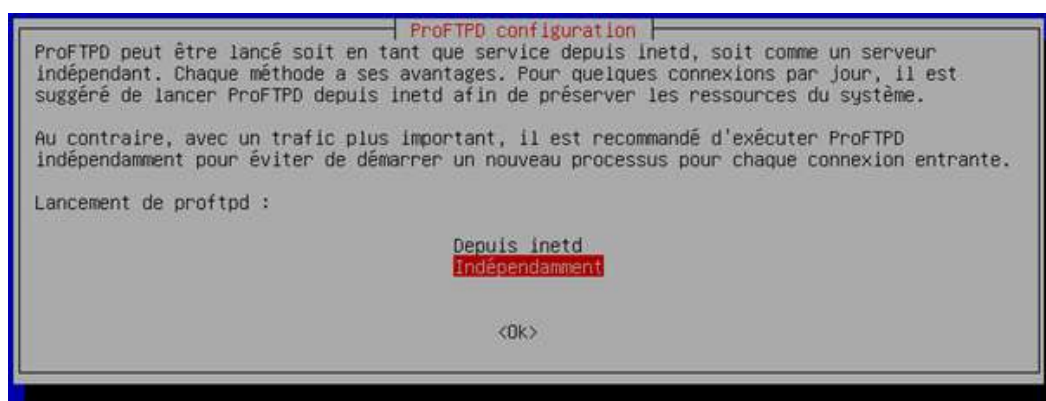
```

FTP

Il faut installer ftp pour pouvoir mettre à jour notre application hébergée sur notre Linux. Cela va nous permettre également de pouvoir s'y connecter de façon anonyme et sécurisé.

```
apt-get install proftpd-basic
```

Il faut choisir « **Indépendamment** ».



Il faut modifier les fichiers ci-dessous.


```
GNU nano 2.2.6 Fichier : /etc/proftpd/virtuals.conf

#
# Proftpd sample configuration for Virtual Hosts and Virtual Roots.
#
# Note that FTP protocol requires IP based virtual host, not name based.
#
#
# A generic sample virtual host.
#
<VirtualHost ftp.server.com>
ServerAdmin      ftpmaster@server.com
ServerName       "Big FTP Archive"
TransferLog      /var/log/proftpd/xfer/ftp.server.com
MaxLoginAttempts 3
RequireValidShell no
DefaultRoot      /ftp
AllowOverwrite   yes
</VirtualHost>
```

```
GNU nano 2.2.6 Fichier : /etc/proftpd/proftpd.conf

Group                                nogroup

# Umask 022 is a good standard umask to prevent new files and dirs
# (second parm) from being group and world writable.
Umask                                022 022
# Normally, we want files to be overwriteable.
AllowOverwrite                       on

# Uncomment this if you are using NIS or LDAP via NSS to retrieve passwords:
# PersistentPasswd                    off

# This is required to use both PAM-based authentication and local passwords
AuthOrder                            mod_auth_pam.c* mod_auth_unix.c
-
# Be warned: use of this directive impacts CPU average load!
# Uncomment this if you like to see progress and transfer rate with ftpwho
# in downloads. That is not needed for uploads rates.
#
# UseSendFile                        off
```

On modifie « **MaxInstances** » à 90 pour que tout le monde puisse être connecté en simultané au serveur FTP.

```
GNU nano 2.2.6 Fichier : /etc/proftpd/proftpd.conf

# This is useful for masquerading address with dynamic IPs:
# refresh any configured MasqueradeAddress directives every 8 hours
<IfModule mod_dynmasq.c>
# DynMasqRefresh 28800
</IfModule>

# To prevent DoS attacks, set the maximum number of child processes
# to 30. If you need to allow more than 30 concurrent connections
# at once, simply increase this value. Note that this ONLY works
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd)
MaxInstances 90
```

Il faut modifier le fichier ci-dessous.

```
GNU nano 2.2.6 Fichier : /etc/proftpd/tls.conf

#
# Proftpd sample configuration for FTPS connections.
#
# Note that FTPS impose some limitations in NAT traversing.
# See http://www.castaglia.org/proftpd/doc/contrib/ProFTPD-mini-HOWTO-TLS.html
# for more information.
#

<IfModule mod_tls.c>
TLSEngine on
TLSLog /var/log/proftpd/tls.log
TLSProtocol SSLv23

# Server SSL certificate. You can generate a self-signed certificate using
# a command like:
#
# openssl req -x509 -newkey rsa:1024 \
#             -keyout /etc/ssl/private/proftpd.key -out /etc/ssl/certs/proftpd.crt \
#             -nodes -days 365
#
# The proftpd.key file must be readable by root only. The other file can be
# readable by anyone.
#
# chmod 0600 /etc/ssl/private/proftpd.key
# chmod 0640 /etc/ssl/private/proftpd.key
#
TLRSACertificateFile /etc/ssl/certs/proftpd.crt
TLRSACertificateKeyFile /etc/ssl/private/proftpd.key
```

Il faut démarrer le service ftp.

```
service proftpd start
```

On vérifie son statut.

```

root@SRVLINUX:~# service proftpd status
• proftpd.service - LSB: Starts ProFTPd daemon
  Loaded: loaded (/etc/init.d/proftpd)
  Active: active (running) since jeu. 2017-04-27 11:46:28 CEST; 1h 8min ago
  Process: 527 ExecStart=/etc/init.d/proftpd start (code=exited, status=0/SUCCESS)
  CGroup: /system.slice/proftpd.service
          └─615 proftpd: (accepting connections)

avril 27 11:46:28 SRVLINUX proftpd[527]: Starting ftp server: proftpd.
avril 27 11:46:28 SRVLINUX systemd[1]: Started LSB: Starts ProFTPd daemon.
avril 27 12:54:34 SRVLINUX systemd[1]: Started LSB: Starts ProFTPd daemon.

```

Pour une connexion anonyme, il faut d'abord faire les manipulations ci-dessous.

```

root@SRVLINUX:~# mkdir /etc/proftpd/ssl
root@SRVLINUX:~# cd /etc/proftpd/ssl
root@SRVLINUX:/etc/proftpd/ssl# openssl genrsa -out proftpd.key 1024
Generating RSA private key, 1024 bit long modulus
.....+++++
...+++++
e is 65537 (0x10001)
root@SRVLINUX:/etc/proftpd/ssl# openssl req -new -x509 -days 3650 -key proftpd.key -out proftpd.crt

```

On rentre la clé.

```

root@SRVLINUX:~# openssl req -new -x509 -days 3650 -key /etc/ssl/private/proftpd.key -out /etc/ssl/certs/proftpd.crt

```

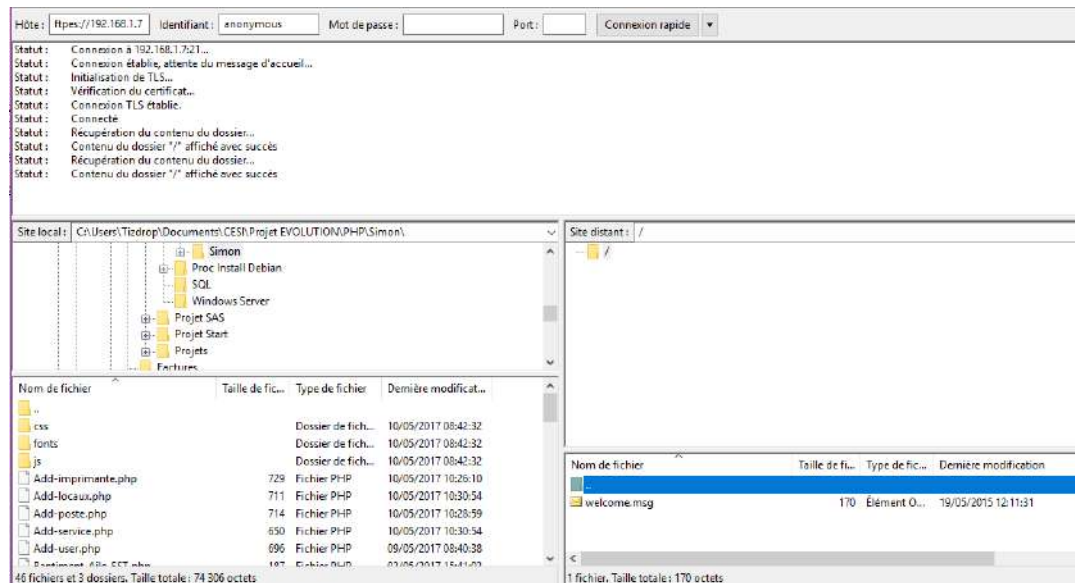
On répond au questionnaire.

```

-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Aquitaine
Locality Name (eg, city) []:Bordeaux
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Pixy
Organizational Unit Name (eg, section) []:Pixy
Common Name (e.g. server FQDN or YOUR name) []:Administrateur
Email Address []:admin@pixy.com
root@SRVLINUX:~# service proftpd restart

```

On tente de se connecter avec FileZilla en anonyme.



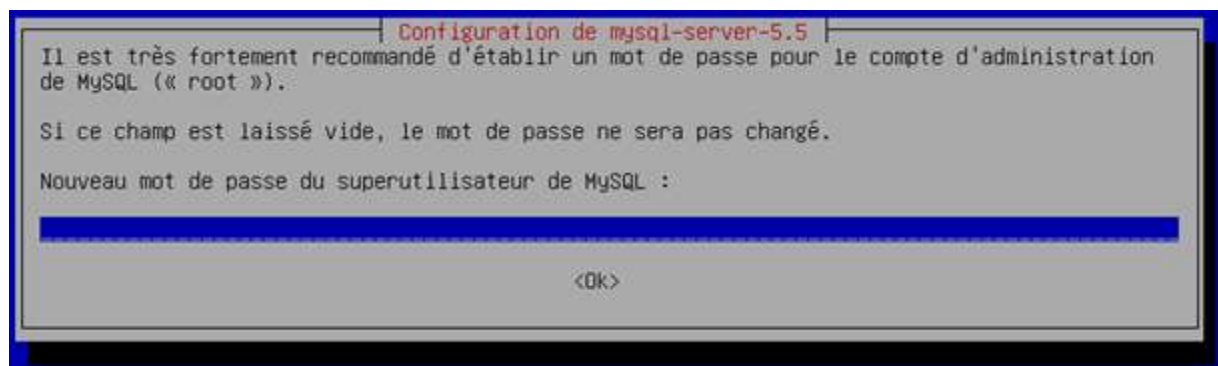
Nous arrivons maintenant à nous connecter depuis FileZilla en anonyme. Nous pouvons donc nous connecter en anonyme et avec un compte sécurisé.

MySQL

Il faut installer mysql-server pour la gestion de notre base de données.

```
apt-get install mysql-server phpmyadmin
```

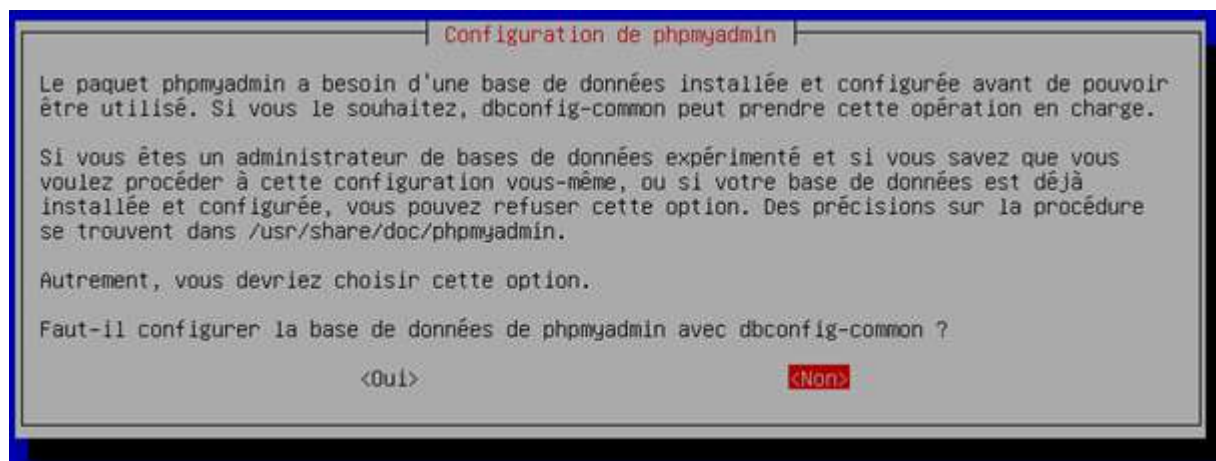
Choisir un mot de passe et le confirmer.



Sélectionner apache2.

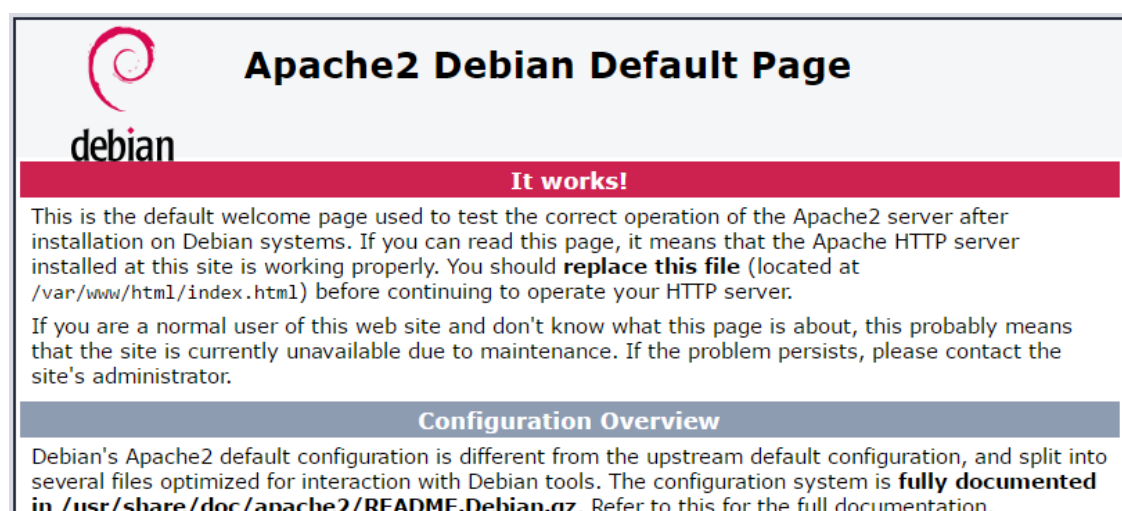


Il faut configurer la base de données.



Il faut ensuite choisir un mot de passe, puis le confirmer.

Dans un navigateur internet, on entre notre adresse IP pour vérifier.



En ajoutant « /phpmyadmin » à la suite de notre IP, nous accédons à une authentification de notre base de donnée.



Bienvenue dans phpMyAdmin

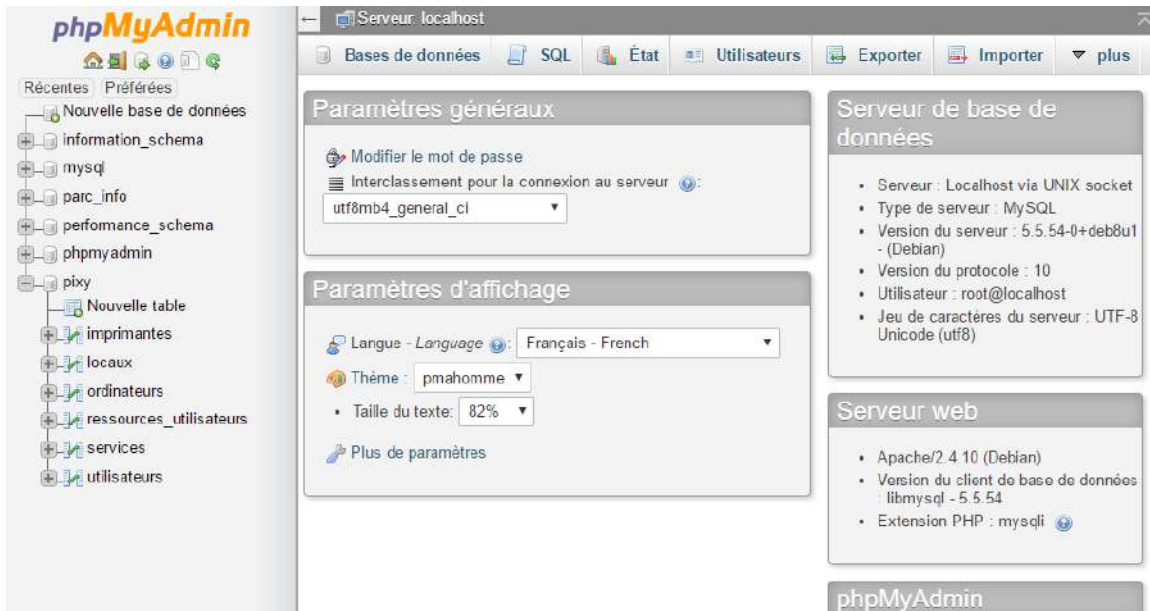
Langue - Language
Français - French ▼

Connexion ⓘ

Utilisateur :
Mot de passe :

Exécuter

On peut maintenant accéder à notre base de données.



phpMyAdmin

Sauvegardes

Base de données

Pour la sauvegarde de notre base de données, nous avons mis en place un script permettant d'effectuer cette sauvegarde. Il génère un fichier au format « **tar** » qui sera donc stocké dans un dossier partagé « **linux** » sur notre serveur de fichier.

```
GNU nano 2.2.6 Fichier : /sauve.sh

#!/bin/bash

#On réalise une variable pour la date
date du jour=$(date +%F)

#On récupère notre base de données avec mysqldump
mysqldump -u root -proot pixy > /var/www/save/sauvegarde${datedu jour}.sql

#On se rend dans le dossier /var/www/save
cd /var/www/save

#On compresse au format tar le dossier
tar cvzf Savebase${datedu jour}.tar.gz *

#On se connecte au serveur de fichiers
mount -t cifs -o username=administrateur,password=Admin@01 //192.168.1.9/linux /media/linux

#cp -r /etc/samba/smb.conf /media/linux

#On déplace la base de données dans le serveur de fichiers
mv Savebase${datedu jour}.tar.gz /media/linux

#Nous attendons la fin du transfert
sleep 10

#Nous démontons le point de montage
umount /media/linux
```

Archives Linux

Voici le script pour la sauvegarde de nos archives Linux.

```
GNU nano 2.2.6 Fichier : backup.sh Modifié

#!/bin/bash

# Date du jour
backupdate=$(date +%Y'-'%m'-'%d')

# Repertoire de backup
# Dirbackup=/backup/backup-$backupdate

# Création du répertoire de backup
# /bin/mkdir

mount -t cifs -o username=administrateur,password=Admin@01 //192.168.1.9/linux /media/linux

/bin/mkdir /media/linux/backup-$backupdate

# tar -cjs /destination/fichier.tar.gz /source1 /source2 /sourceN
# Créé une archive gz
# Sauvegarde de /home
/bin/tar cvzf /media/linux/backup-$backupdate/backuplinux.tar.gz /home /etc /ftp /samba
```

Sur le serveur de fichier, nous retrouvons bien le fichier de sauvegarde.

NFS

Nous avons établie une procédure NFS, mais nous ne comptons pas nous en servir car nous n'avons qu'un seul serveur Linux.

On crée un espace partitionné dans /nfs

```
root@SRVLINUX:~# fdisk /dev/sdd

Bienvenue dans fdisk (util-linux 2.25.2).
Les modifications resteront en mémoire jusqu'à écriture.
Soyez prudent avant d'utiliser la commande d'écriture.

Le périphérique ne contient pas de table de partitions reconnue.
Created a new DOS disklabel with disk identifier 0x79deddcc.

Commande (m pour l'aide) : n
Type de partition
  p primaire (0 primaire, 0 étendue, 4 libre)
  e étendue (conteneur pour partitions logiques)
Sélectionnez (p par défaut) : p
Numéro de partition (1-4, 1 par défaut) :
Premier secteur (2048-2097151999, 2048 par défaut) :
Dernier secteur, +secteurs ou +taille{K,M,G,T,P} (2048-2097151999, 2097151999 par défaut) :

Une nouvelle partition 1 de type « Linux » et de taille 1000 GiB a été créée.

Commande (m pour l'aide) : w
La table de partitions a été altérée.
Appel d'ioctl() pour relire la table de partitions.
Synchronisation des disques.
```

On installe les sources.

```
root@SRVLINUX:~# apt-get install nfs-kernel-server_
```

On modifie les fichiers ci-dessous.

```
GNU nano 2.2.6 Fichier : /etc/exports

# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
/home/simon 192.168.1.7/24(rw,root_squash)
```

Charte informatique

Introduction

Notre charte informatique a pour but de définir les règles d'utilisation des moyens informatiques de notre entreprise PIXY et de préciser les responsabilités des utilisateurs.

Cette charte est associée au règlement intérieur de notre société. Elle permet aux utilisateurs de connaître leur responsabilités envers la législation afin de faire un usage correct des moyens informatiques et réseau internet.

Champ d'application

Moyens informatiques concernés

Il s'agit de l'ensemble des moyens informatiques, matériels et logiciels, faisant partie de la société PIXY (postes de travail et ressources pour se connecter au réseau, la messagerie électronique, la téléphonie fixe et internet).

Utilisateurs concernés

Ce sont les personnes ayant accès aux moyens informatiques et internet.

Règles d'utilisation et de sécurité

Conditions d'accès

La mise à disposition de moyens et ressources informatiques à un utilisateur s'effectue sous la responsabilité de son manager, l'utilisation de ces moyens n'est autorisée que dans le cadre de l'activité professionnelle de l'utilisateur.

Conditions d'utilisation

L'utilisation des moyens informatiques est subordonnée à des droits d'accès, qui sont délivrés par le service informatique. Ces droits d'accès sont strictement personnels et non transmissibles.

L'utilisateur est pleinement responsable de l'usage des moyens informatiques qui lui sont confiés et il doit respecter les règles de sécurité et les recommandations prescrites (et notamment le présent document).

L'utilisateur n'est pas autorisé à modifier la configuration système qui lui a été fournie avec son poste de travail ; à ce titre l'usage de comptes avec privilèges administrateurs est, en règle générale, interdit. Si par incident la configuration du poste devait être altérée, l'utilisateur devra en informer le service informatique sans tarder.

L'utilisateur doit assurer la protection matérielle et logicielle des moyens informatiques qui lui sont confiés, en particulier :

- Choisir ses mots de passe en respectant les recommandations de fiabilité diffusées par le service informatique. Ces mots de passe ne doivent jamais être communiqués à quiconque.
- En cas d'activité nécessitant une utilisation partagée, faire limiter les droits d'accès aux seuls tiers concernés.
- Verrouiller son compte lorsqu'il quitte son poste de travail et de se déconnecter ou éteindre son ordinateur lorsqu'il s'absente des locaux.
- Signaler toute intrusion frauduleuse, vol, ou tentative de ces infractions, et de façon générale, toute anomalie constatée telle que suspicion de virus par exemple. Dans ces circonstances, le service informatique peut être amené à intervenir sur l'ordinateur de l'utilisateur, ce dernier étant tenu informé au préalable, sauf impossibilité, des opérations effectuées.

Principes d'utilisation

Respect de la confidentialité

On entend par confidentialité le caractère réservé d'une information dont l'accès est limité aux seules personnes admises à la connaître pour les besoins du service.

Les informations, fichiers et documents présents sur les postes des utilisateurs sont réservés à leur usage propre.

Voici une liste d'interdiction :

- Prendre connaissance d'informations détenues par des tiers.
- Captation de mot de passe.
- Usurpation d'identité.
- Accéder aux données d'autrui sans son accord, même non protégées.
- Utiliser un poste sans autorisation.
- Utiliser d'autres comptes que ceux fournis légitimement.

Cette interdiction est également valable pour les informations échangées par messagerie électronique ou par les services réseaux (Internet, Intranet, Réseau Social Entreprise, outils collaboratifs,...).

Accès à notre répertoire

Nos utilisateurs auront accès à notre base de données uniquement en mode lecture. Ils devront utiliser l'identifiant « **guest01** » ainsi que le mot de passe « **12345** » pour visualiser le contenu de notre répertoire.

Préservation de l'intégrité

On entend par intégrité la garantie que le système et l'information ne sont modifiés que par une action volontaire et légitime. L'utilisateur est pleinement responsable de la conservation et de la protection des données qu'il utilise sur son poste de travail.

Il est rappelé que sont pénalement sanctionnés :

- De porter atteinte à l'intégrité, à l'image de quiconque sous n'importe quelles formes (racisme, antisémitisme, sexisme, etc.)
- De profaner des injures ou diffamation.
- Le fait d'entraver ou de fausser le fonctionnement d'un système informatique.
- La propagation volontaire de virus.
- L'utilisation de logiciels permettant de contourner les dispositifs de sécurité.

- Le détournement des outils d'exploitation des systèmes à des fins de piratage.
- La détention de logiciels pour lesquels il n'a pas été acquis de licence.
- Le fait d'introduire frauduleusement des données dans un système informatique ou de modifier frauduleusement les données qu'il contient.
- De mettre à disposition d'autrui des informations sans y être préalablement autorisé.
- De répondre aux sollicitations externes visant à l'obtention de renseignements (démarchage téléphonique, courrier électronique, formulaires, enquêtes, etc.)
- D'effectuer ou d'utiliser, même à titre provisoire, des copies de logiciels, même si l'acquisition d'une licence n'est pas nécessaire.

Textes Applicables

(Pour information, liste non exhaustive.)

Textes législatifs

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (dispositions pénales reprises dans le Code pénal – art. 226-16 à 266-64).
- Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique (art. 323-1 à 323-7 du Code Pénal).
- Loi n° 92-597 du 1er juillet 1992 portant Code de la propriété intellectuelle.

Textes réglementaires

- Recommandation n° 600/SGDSN/DISSI/SCSSI de mars 1993 pour la protection des informations sensibles ne relevant pas du secret de défense – postes de travail informatiques.
- Recommandation n° 901/DISSI/SCSSI du 2 mars 1994 pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense.
- Document n° 650/DISSI/SCSSI du 28 mars 1994 relatif à la menace et aux attaques informatiques.

Sanctions

Les utilisateurs ne respectant pas les règles et obligations définies dans la présente charte et ceux qui ne signalent pas les tentatives de violation de leur compte sont passibles de sanctions :

- Ils peuvent être sommairement déconnectés par les administrateurs systèmes qui peuvent surveiller en détail des sessions de travail d'un utilisateur s'il existe un soupçon de non-respect de la présente charte.
- Leur compte peut être fermé, sur décision du responsable pédagogique.
- Ils peuvent être convoqués devant le conseil de discipline.
- Ils peuvent faire l'objet de poursuites judiciaires.

Conclusion

Résumé de notre projet

Durant notre projet, nous avons donc répondu au cahier des charges qui nous a été imposé.

Evolutivité

En termes d'évolutivité de l'infrastructure :

- Installation de client léger,
- Installation d'un serveur d'application redondé RDS

Arrivé d'une ligne Internet :

- Mise d'un service WSUS
- Sauvegarde sur Cloud
- Sortie du site Web sur Internet

o Mise en place d'un proxy inverse

o Achat d'un nom de domaine

- Mise en place d'un système de VPN pour le télétravail

En termes d'évolutivité du site Web :

- Création de nouveaux modules via l'interface web
- Messagerie instantanée
- Installation d'une GED

Nous vous proposons avec ce dossier d'envisager une infrastructure informatique aux normes, avec :

- une protection contre les coupures électriques,
- une haute disponibilité avec un taux de 99.99% (52 minute par an),
- une multiplication des méthodes de sauvegarde,
- une supervision pour avertir rapidement en cas de dysfonctionnement,
- une excellente réactivité et rapidité des services.

Le tout afin d'éviter le plus possible la perte de données, et la continuité d'activité en cas de panne.

Remerciements

Nous tenons à remercier l'ensemble du personnel du CESI de Blanquefort.

Remerciements particulier à :

Monsieur Laurent BUREAU, Windows serveur et virtualisation,

Monsieur Arnaud De VILLEDON, Linux et Base de données,

Monsieur Thierry AMET, maintenance logicielle

Monsieur Benjamin TOUCHARD, Algorithmique

Sources

Infrastructure Linux

<https://pve.proxmox.com/>

<http://binbash.fr/>

<http://technet.microsoft.com/>

<http://community.spiceworks.com/>

<http://doc.ubuntu-fr.org/>

<http://denisrosenkranz.com/>

<https://wiki.debian.org/>

<http://www.guillaume-leduc.fr/>

<http://vpourchet.com/>

<http://www.tuto-it.fr/>

<http://www.severalnines.com/>

<http://xymon.sourceforge.net/>

<http://herve-labenere.developpez.com/>

<http://www.ovh.com/>

<http://www.vmware.com/>

<http://documentation.online.net/>

<http://openvz.org/>

<http://www.howtoforge.com/>

Infrastructure Windows :

<http://mizitechinfo.wordpress.com/>

<http://fr.wikipedia.org/>

<http://support.microsoft.com/>

<http://social.technet.microsoft.com/>

<http://sysadminblogger.wordpress.com/>

<http://it-connect.fr/>

Site Web

<http://getbootstrap.com/>

<http://sqldesigner.fr>

<http://gestsup.fr/>

Divers

<http://fr.wikipedia.org/>

<http://www.sanstorageworks.com/>

<http://www.ylea.eu/>

<http://www.coffrefortplus.com/>

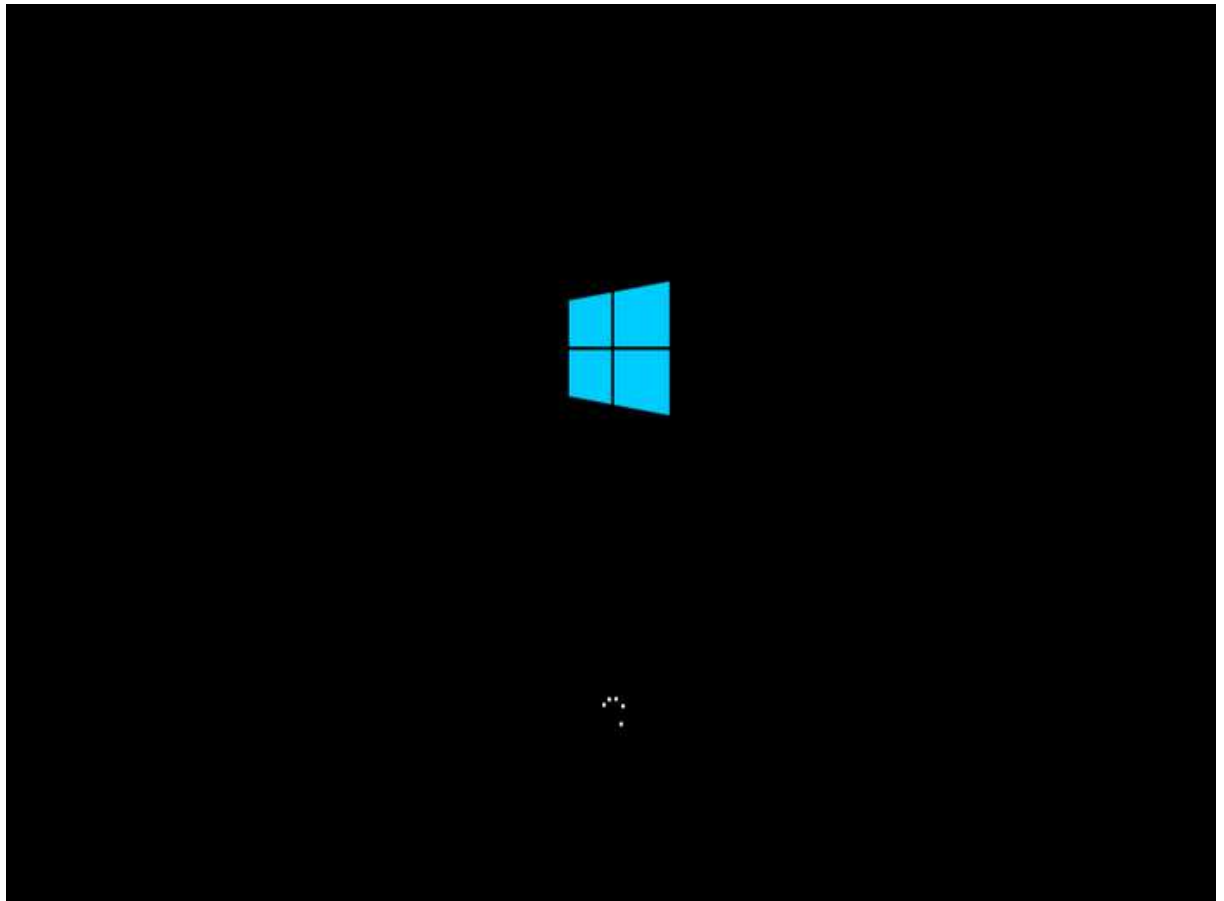
<http://www.misco.fr/>

<http://www.darty.com/>

Annexe

Installation de Windows Server 2012 R2

Booter sur le DVD d'installation de Windows Server 2012, où sur l'image ISO.



On selectionne « **Français (France)** » dans les trois champs, qui correspondent respectivement à la langue d'installation pour l'interface, au format horaire, et au type de clavier.

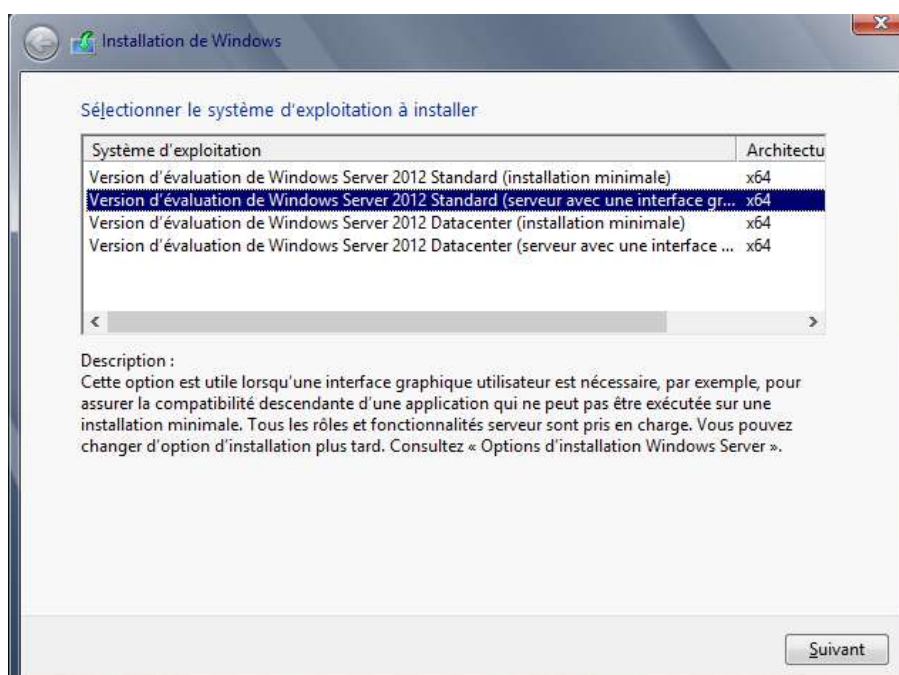


Comme lorsqu'on installe Windows 7 ou Windows Server 2008 R2, il faut cliquer sur « **Installer maintenant** ».

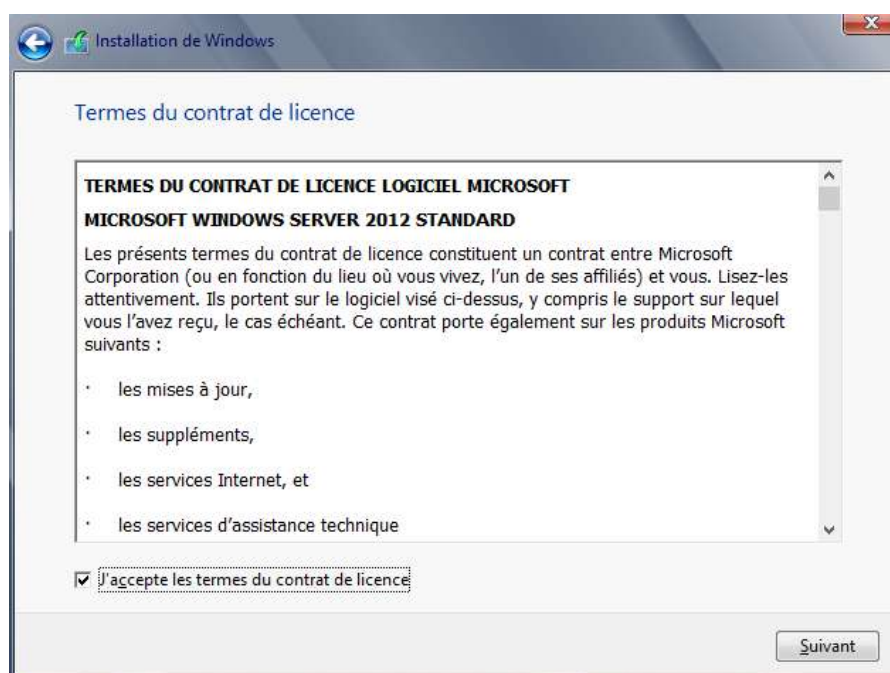


Il faut sélectionner le type d'installation, « **Windows Server 2012 Standard** » étant donné que la version Datacenter est réservée aux serveurs ayant des configurations matérielles importantes. Pour la version Standard, vous avez le choix entre l'installation minimale et l'installation standard c'est à dire avec une interface

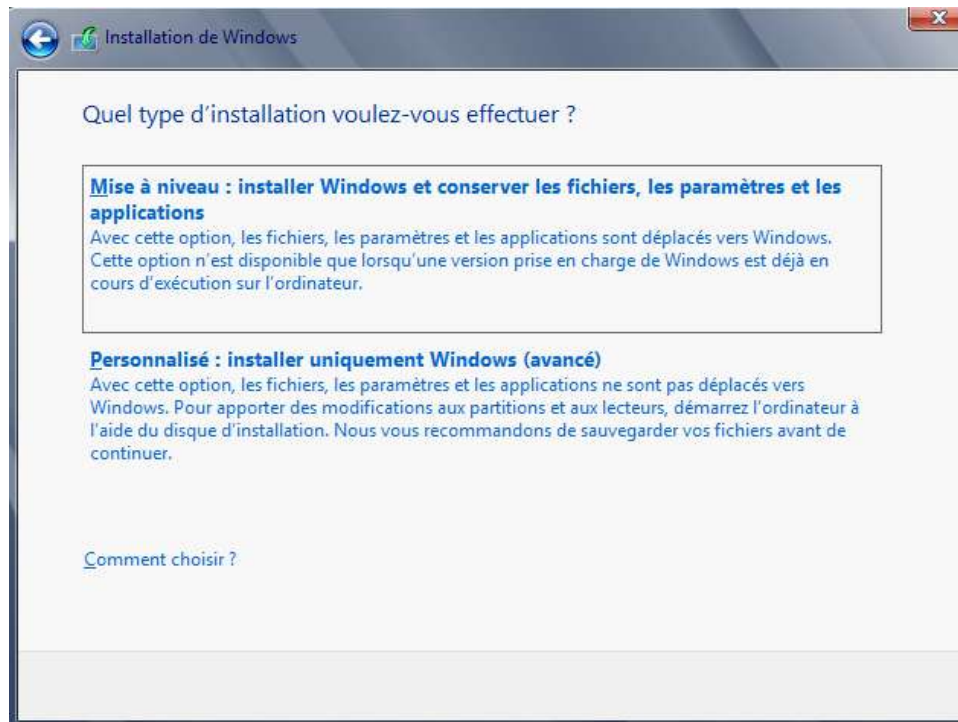
graphique. Effectivement, l'installation minimale correspond à l'installation « **Server Core** » de Windows Server 2008 et 2008 R2 c'est à dire sans interface graphique. On choisit « **Windows Server 2012 Standard (serveur avec une interface graphique)** ».



On accepte les termes du contrat de licence et cliquez sur « **Suivant** ».



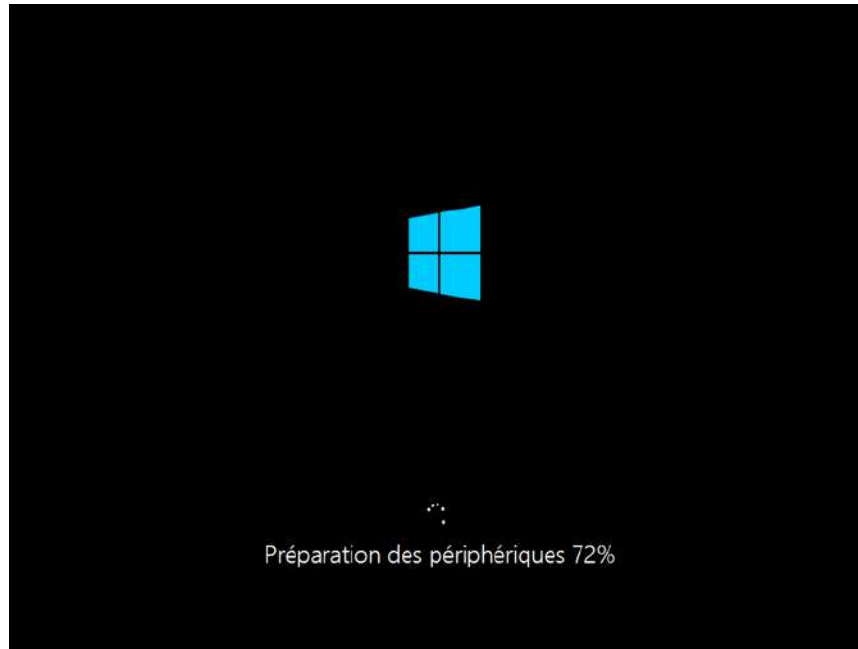
Là encore on retrouve un écran similaire à l'installation de Windows 7 et Windows Server 2008 R2. « **Personnalisé : installer uniquement Windows (avancé)** » étant donné que nous partons d'un disque dur vierge.



On sélectionne votre disque dur et cliquez sur « **Suivant** ». Ce disque dur sera formaté, partitionné, et utilisé par Windows Server 2012.



Une fois que l'installation est terminée, la machine redémarre automatiquement et Windows la prépare.



On définit un mot de passe pour le compte Administrateur. On clique sur « **Terminer** » pour confirmer et continuer.

A screenshot of the 'Paramètres' (Settings) screen in Windows 10. The background is dark blue. At the top, the word 'Paramètres' is written in white. Below it, there is a line of text: 'Tapez un mot de passe pour le compte Administrateur intégré que vous pouvez utiliser pour vous connecter automatiquement à cet ordinateur.' Below this text, there are three input fields: 'Nom d'utilisateur' (Username) with the text 'Administrateur', 'Mot de passe' (Password), and 'Entrer de nouveau le mot de passe' (Re-enter password). At the bottom right, there is a blue button labeled 'Terminer' (Finish). At the bottom left, there is a small white icon of a computer monitor.



⋮ Finalisation de vos paramètres

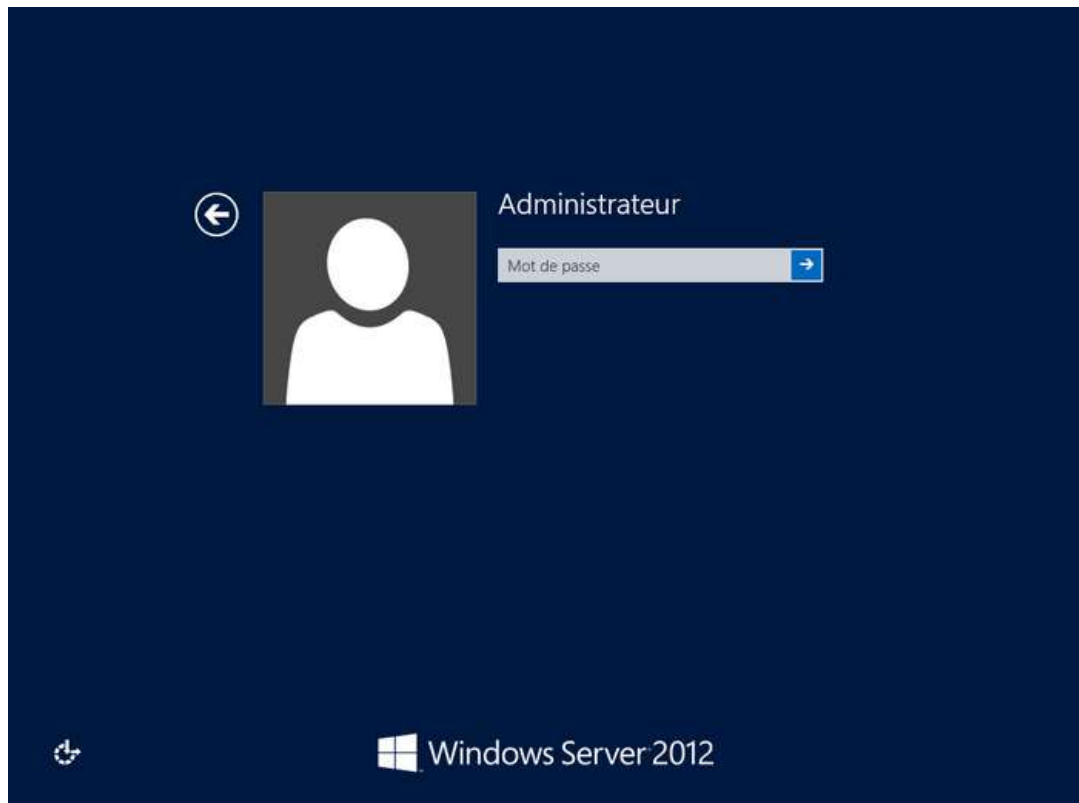
On ouvre la session Administrateur en appuyant sur « **CTRL+ALT+SUPPR** » comme toujours sous Windows.



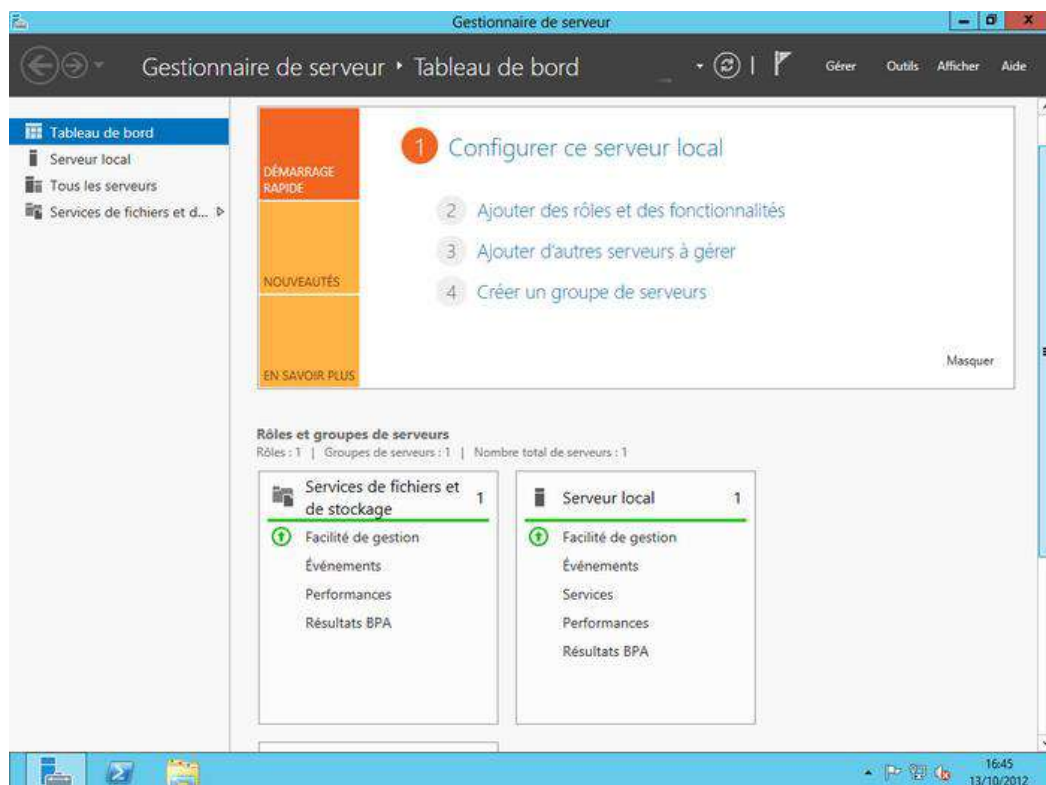
Appuyez sur Ctrl+Alt+Suppr pour vous connecter.

16:30
samedi 13 octobre





Installation terminée et finalisée ! On arrive sur le Bureau de Windows Server 2012 est le Gestionnaire de serveur s'ouvre.



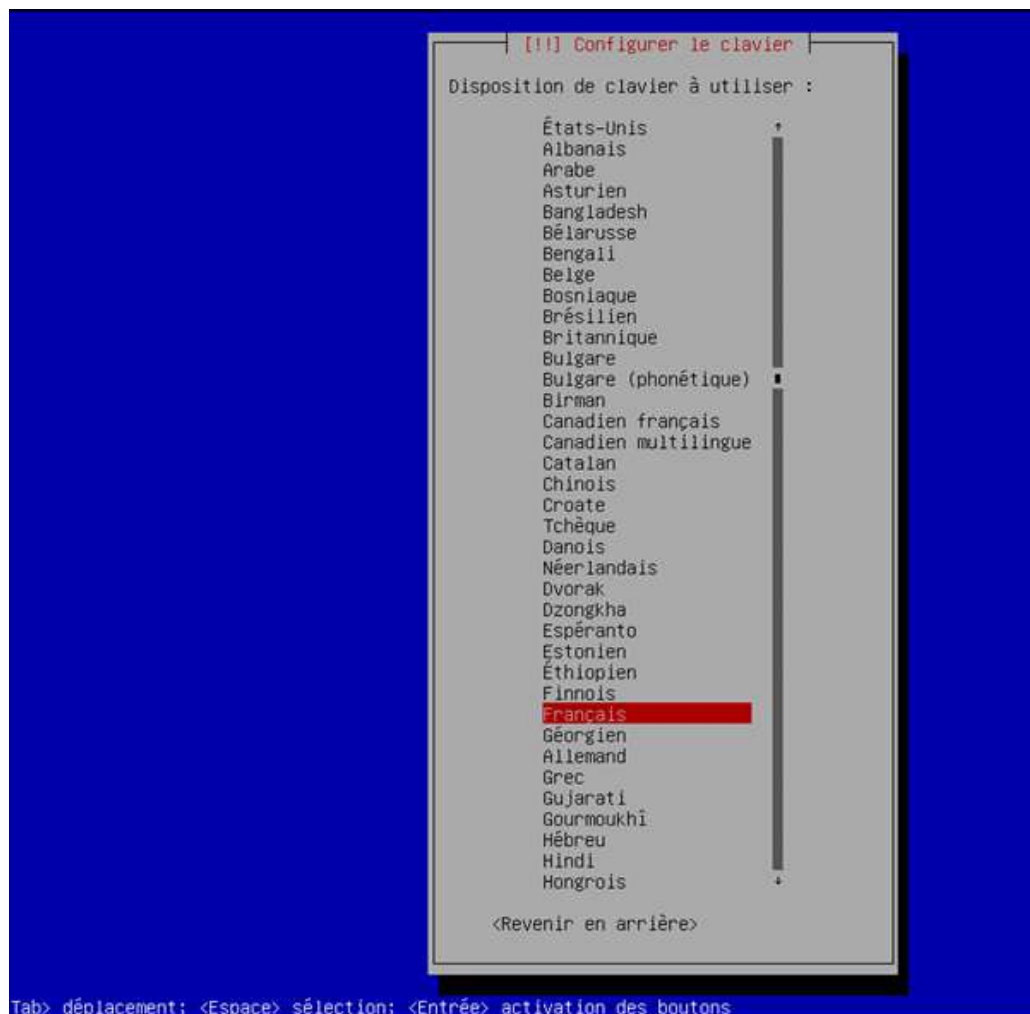
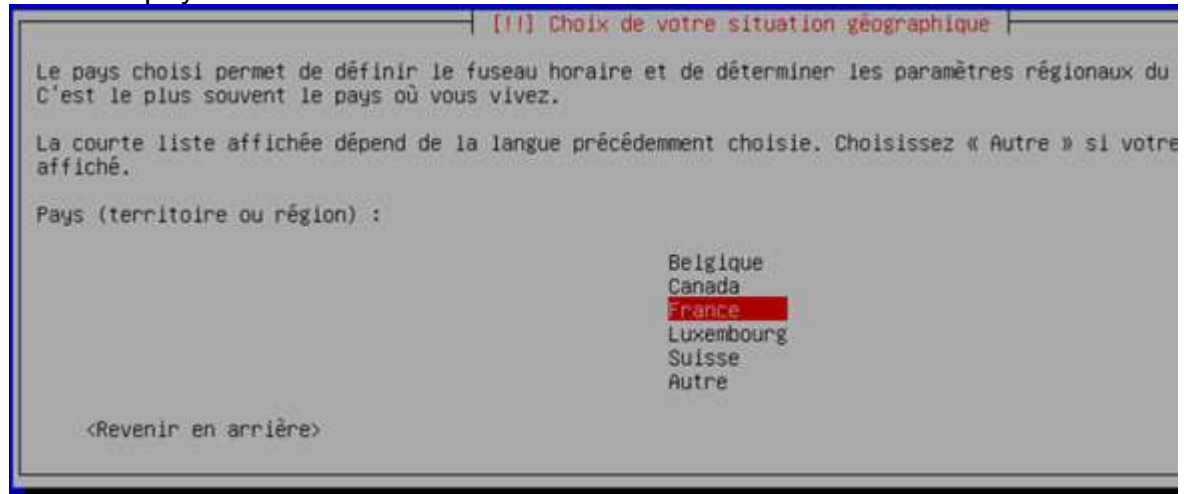
Installation serveur Linux

Au démarrage du serveur, il faut sélectionner « install » pour une installation non-graphique. Puis nous sélectionnons :

- Notre langue

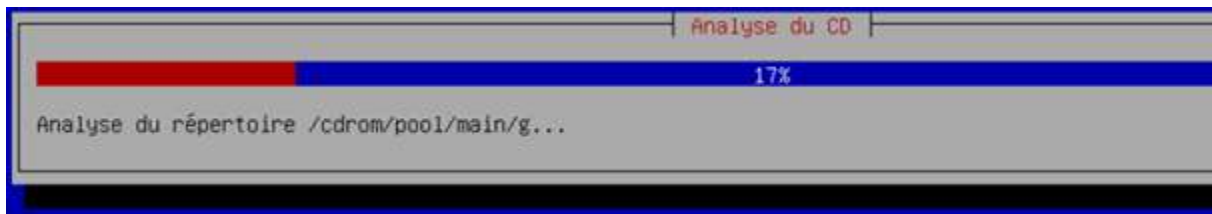


- Notre pays

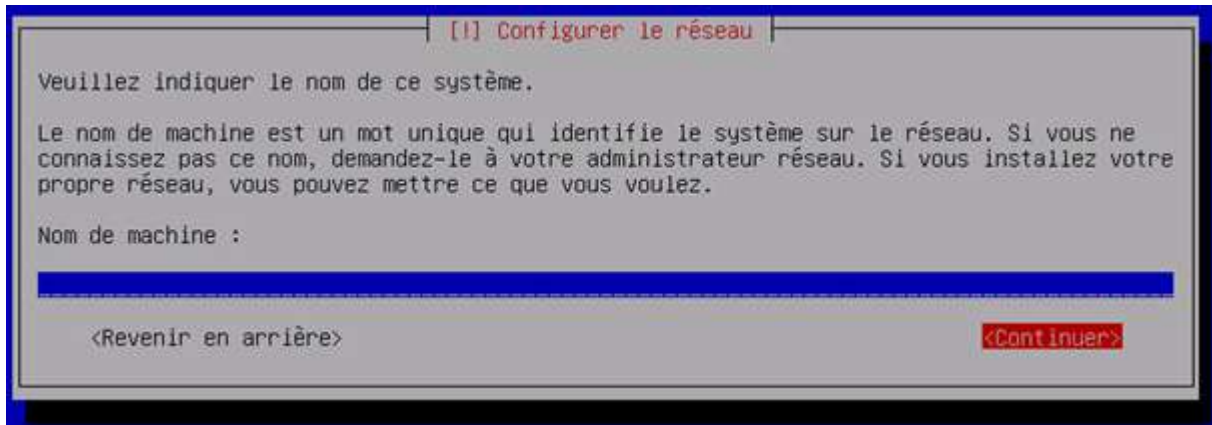


- La configuration du clavier

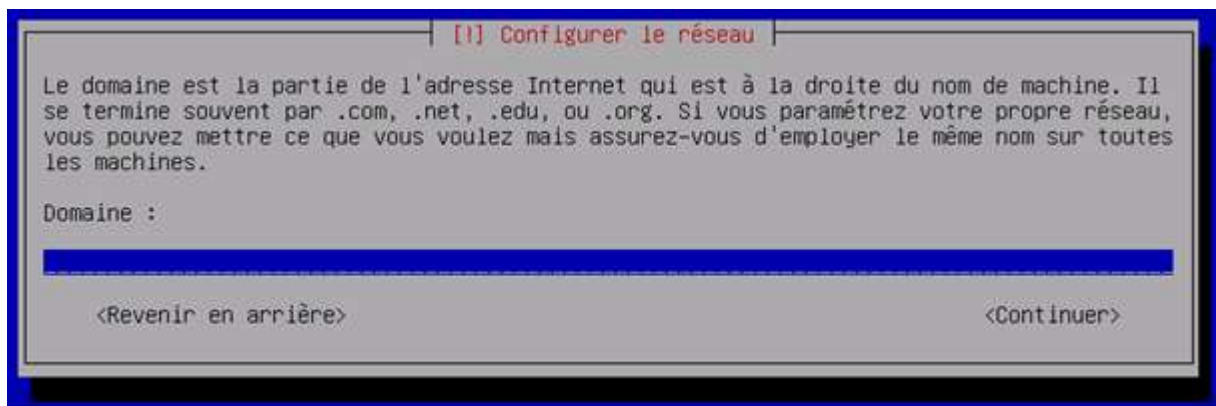
Suite à quoi une analyse du CD s'exécute.



Il faut maintenant choisir le nom de machine. Dans notre cas, nous choisissons «**SRVLINUX**».



Il faut renseigner son nom de domaine. Dans notre cas : « **pixy.lan** ».



Il faut choisir un mot de passe pour le superutilisateur « **root** ».

[[!]] 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 ») :

<Revenir en arrière> <Continuer>

Une confirmation du mot de passe est demandée juste après.

Nous créons un utilisateur (ici : simon guitton)

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

Un compte d'utilisateur va être créé afin que vous puissiez disposer d'un compte différent de celui du superutilisateur (« root »), pour l'utilisation courante du système.

Veuillez indiquer le nom complet du nouvel utilisateur. Cette information servira par exemple dans l'adresse origine des courriels émis ainsi que dans tout programme qui affiche ou se sert du nom complet. Votre propre nom est un bon choix.

Nom complet du nouvel utilisateur :

<Revenir en arrière> <Continuer>

Puis, il faut choisir son identifiant.

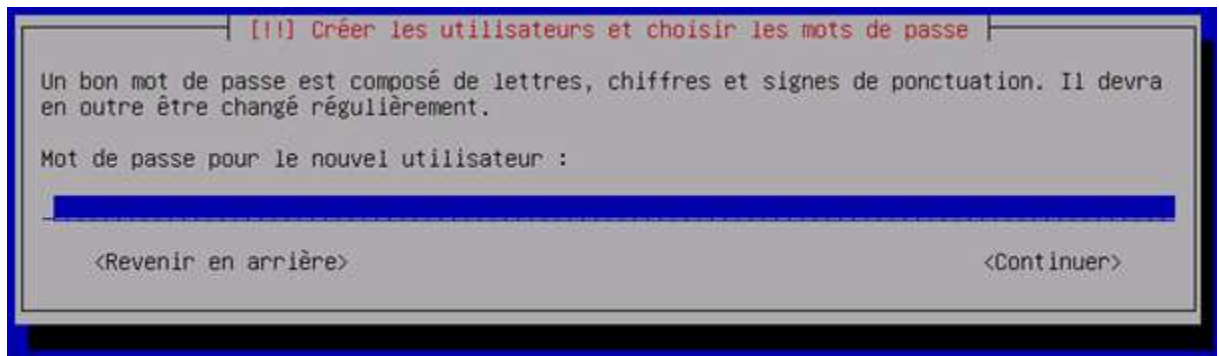
[[!]] Créer les utilisateurs et choisir les mots de passe

Veuillez 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.

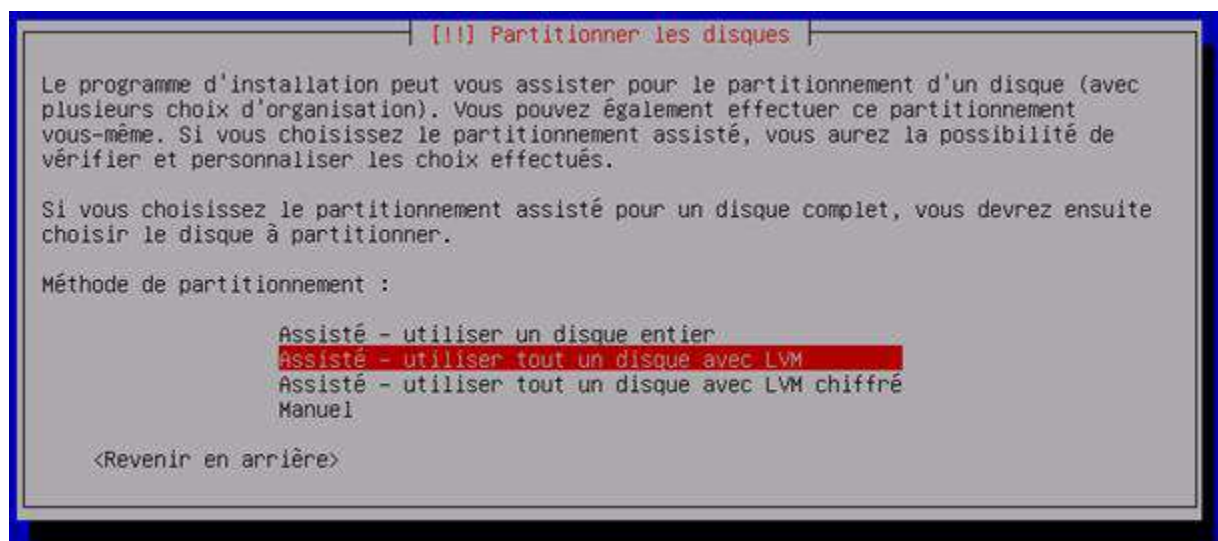
Identifiant pour le compte utilisateur :

<Revenir en arrière> <Continuer>

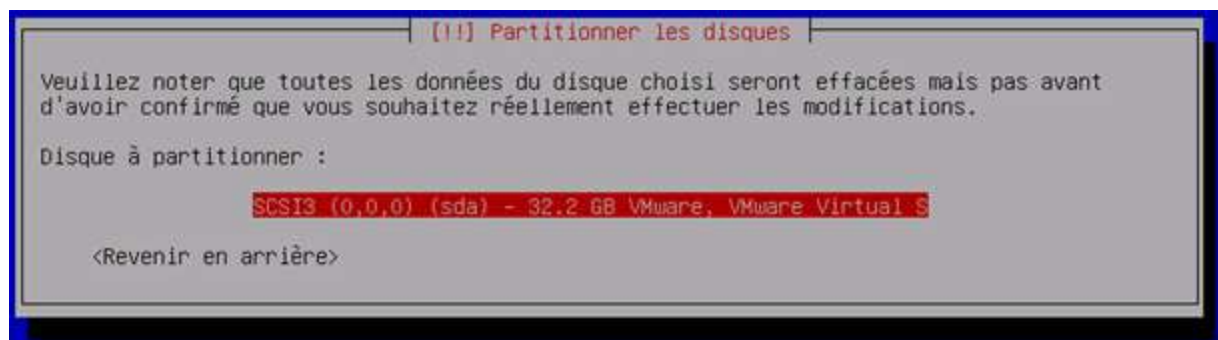
Il faut aussi lui attribuer un mot de passe, puis le confirmer.



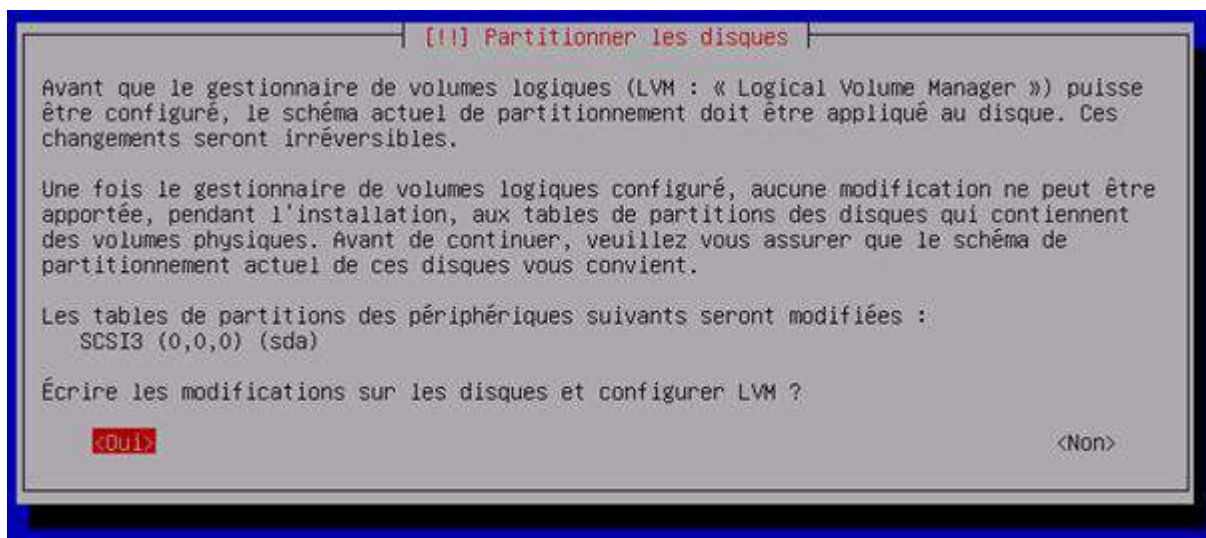
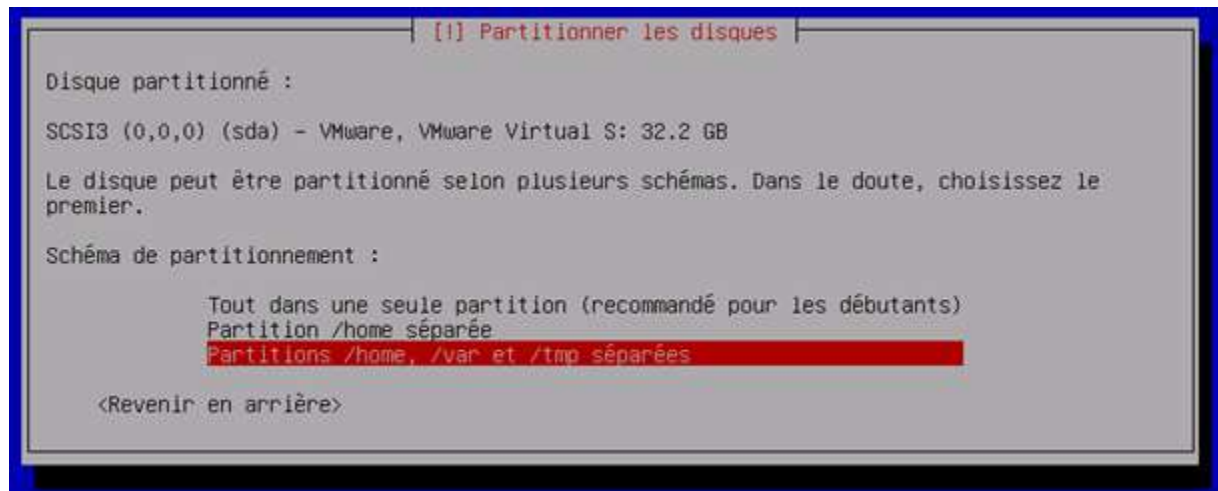
Après avoir terminé l'installation, il faut maintenant partitionner les disques. Nous optons pour un partitionnage assisté en utilisant tout un disque avec LVM.



On sélectionne notre disque.

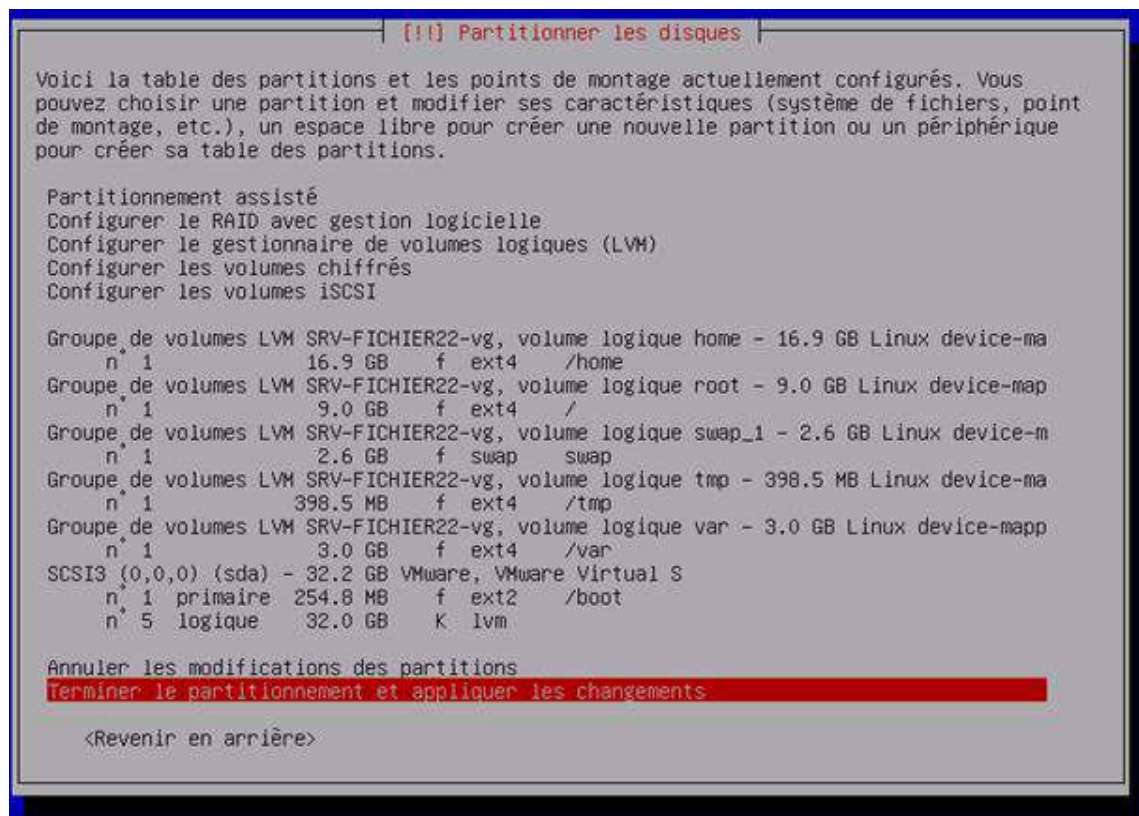


Pour le schéma de partitionnement, il faut sélectionner « **Partitions /home, /var** » (qui héberge les sites) et « **/tmp séparées** ».

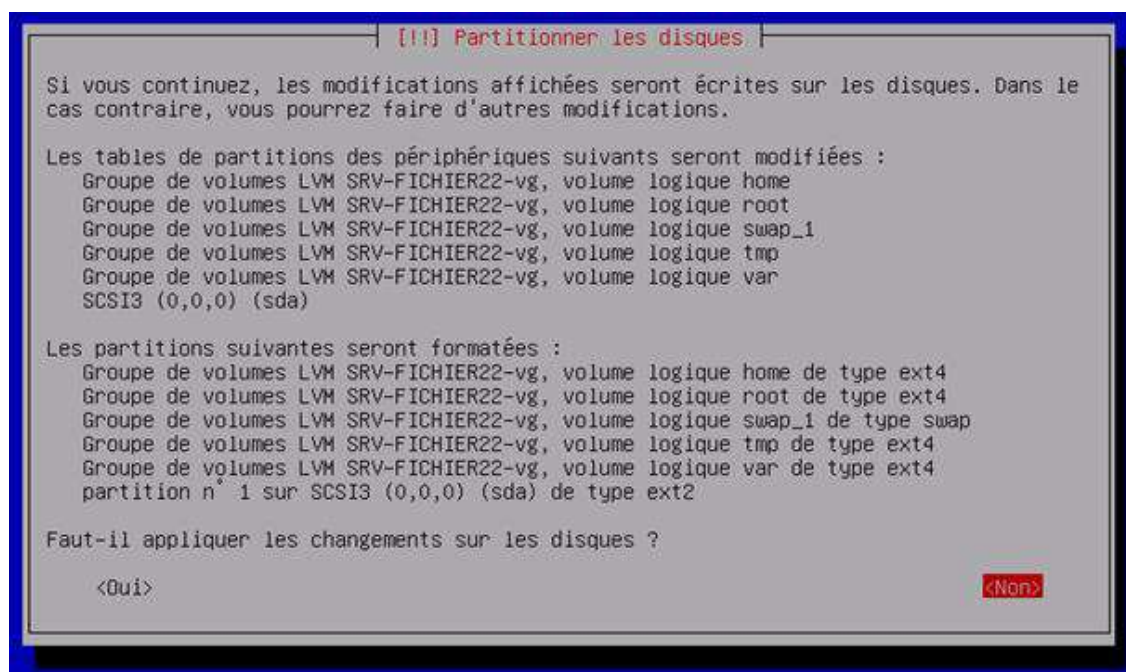


Il faut valider les modifications.

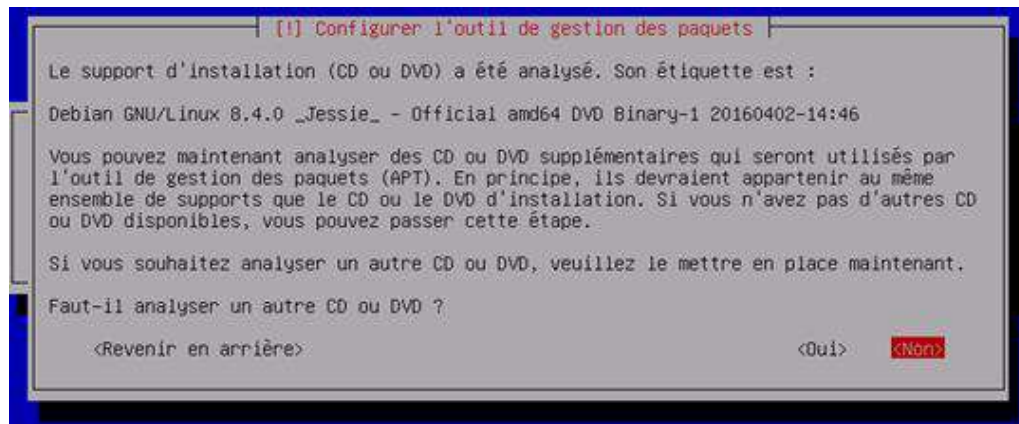
Il faut à nouveau valider en choisissant « **Terminer** ».



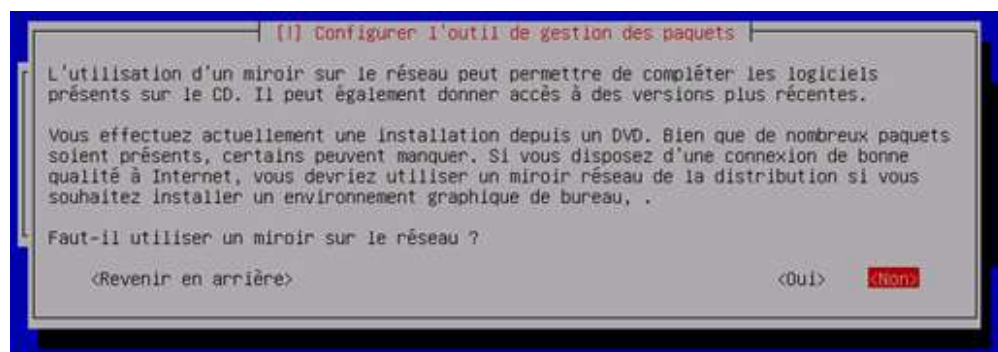
Il faut appliquer les changements.



Il ne faut pas analyser un autre CD ou DVD.



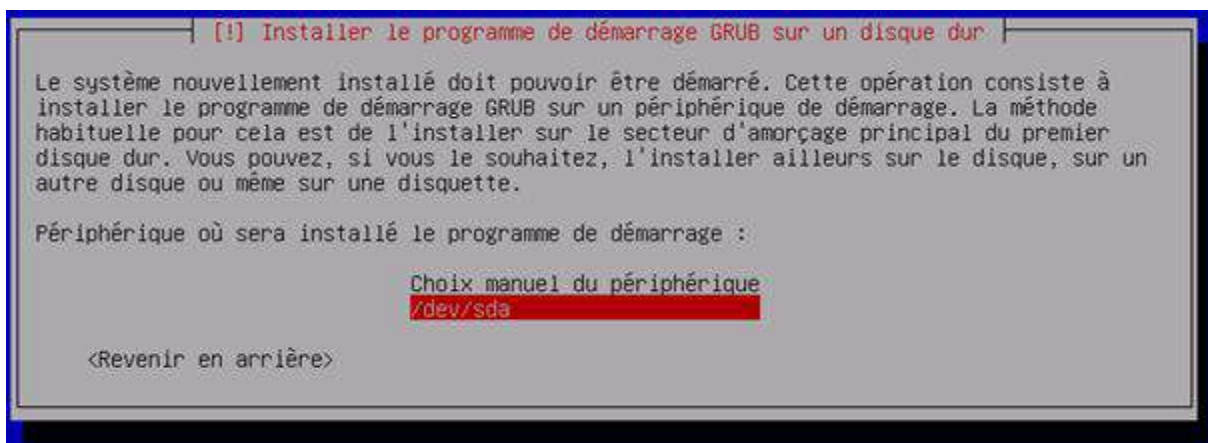
Il ne faut pas non-plus utiliser un miroir sur le réseau.



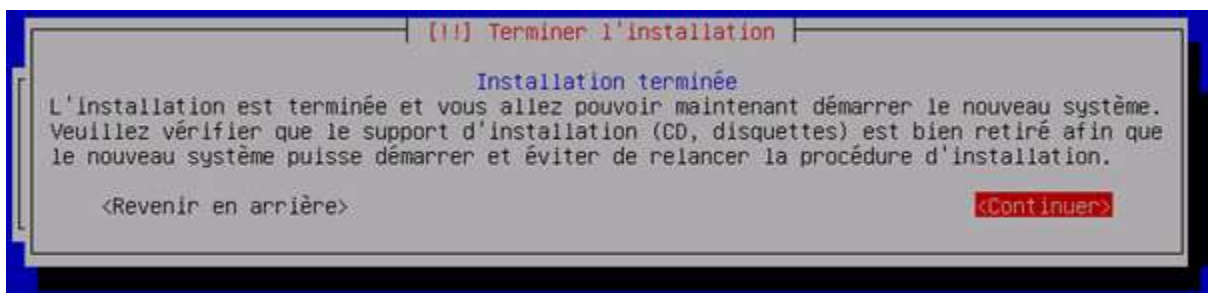
Il faut désélectionner tous les logiciels présélectionnés et ne sélectionner que « **serveur SSH** » et « **utilitaires usuels du système** ».



Il faut installer le programme GRUB.



Il faut choisir le périphérique « **/dev/sda** » pour que le programme y soit installé.



L'installation est maintenant terminée.

Installation DFS

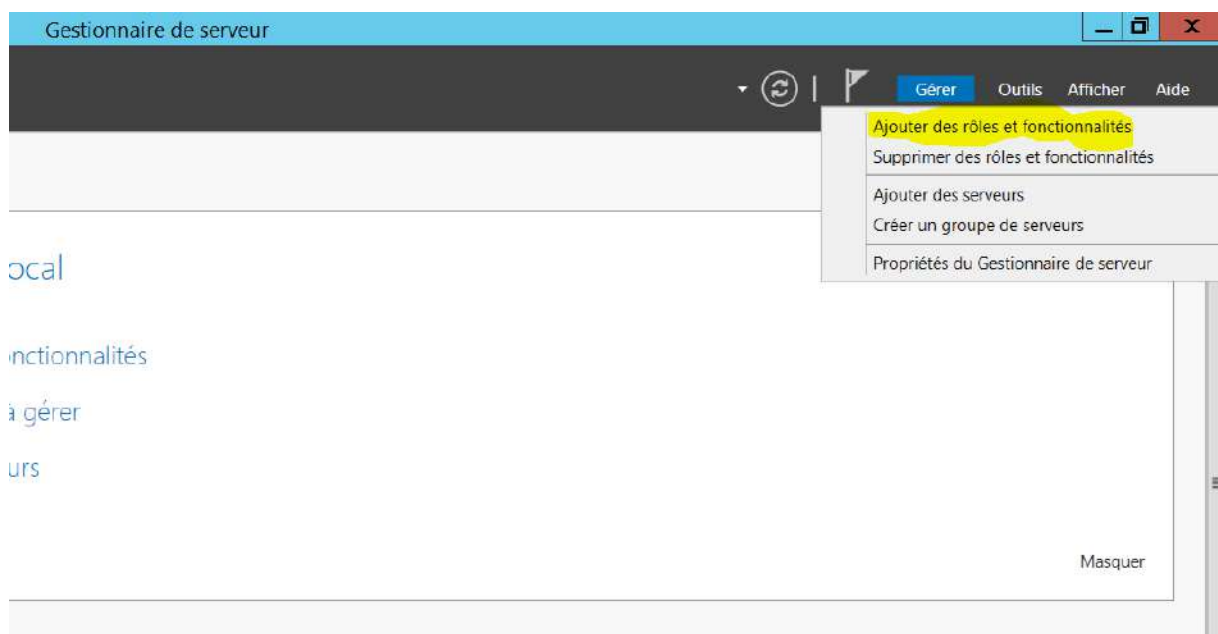
À présent, nous allons aborder l'installation des serveurs de fichier SRV-FICHIERS1, SRV-FICHIERS2 et la configuration DFS. Nous installerons Windows server 2012 R2 x64 en mode « **graphique** » sur le premier serveur et nous installerons Windows server 2012 R2 x64 en mode « **core** » sur le second.

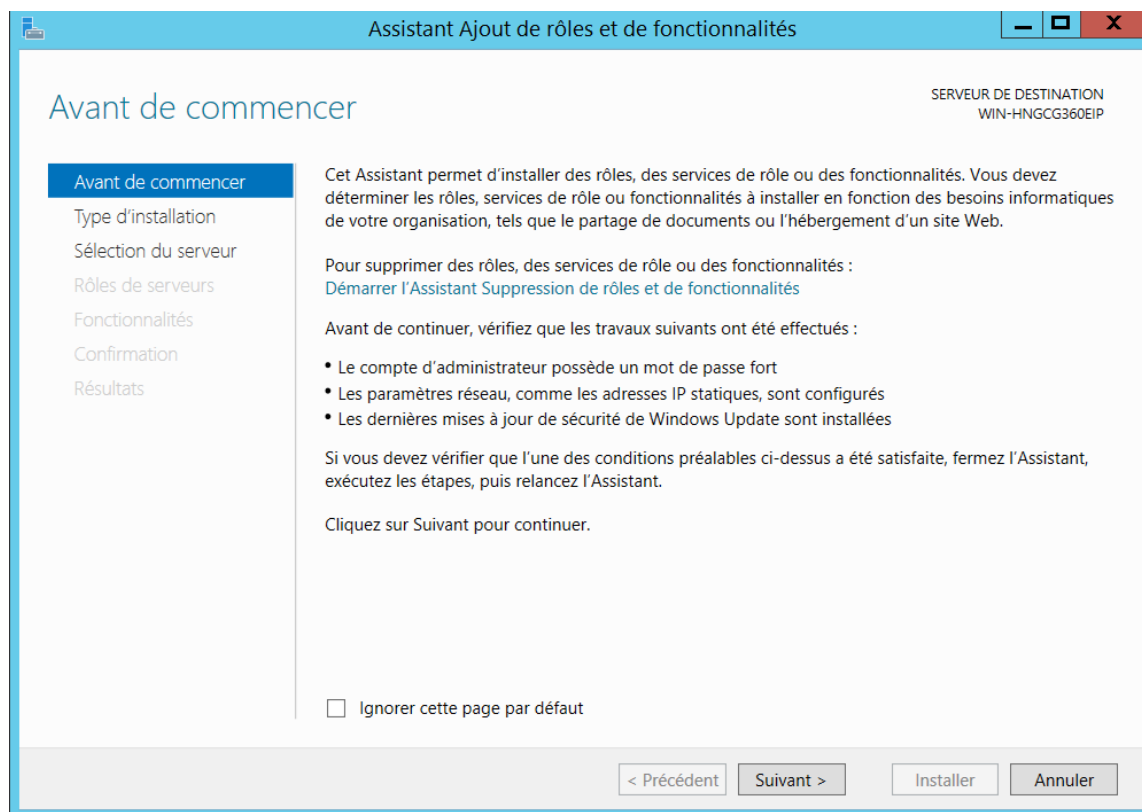
Configuration réseau

La configuration réseau des serveurs sera mise en place en suivant le même protocole que pour le SERVEUR1 ou le SERVEUR2. L'IP du serveur SRV-FICHIERS1 sera 192.168.1.9 et l'IP correspondant au serveur SRV-FICHIERS2 sera 192.168.1.10. Pour les serveurs DNS, nous renseignerons l'IP des serveurs SERVEUR1 et SERVEUR2 qui sont respectivement 192.168.1.5 et 192.168.1.6.

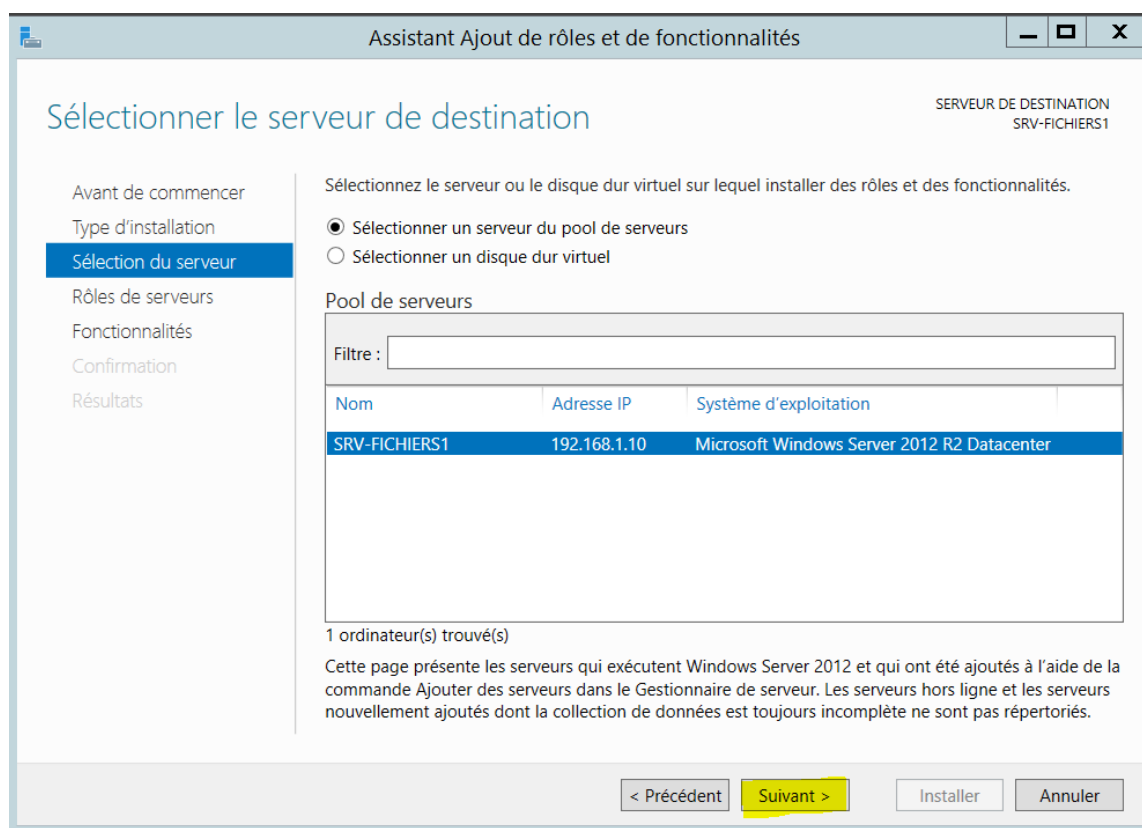
Installation de SRV-FICHIERS1

De la même façon que nous avons installé les rôles DHCP ou DNS sur SERVEUR1, nous installons le rôle serveur de fichiers depuis le gestionnaire de serveur en cliquant sur « **Gérer** », puis sur « **Ajouter des rôles et fonctionnalités** ».

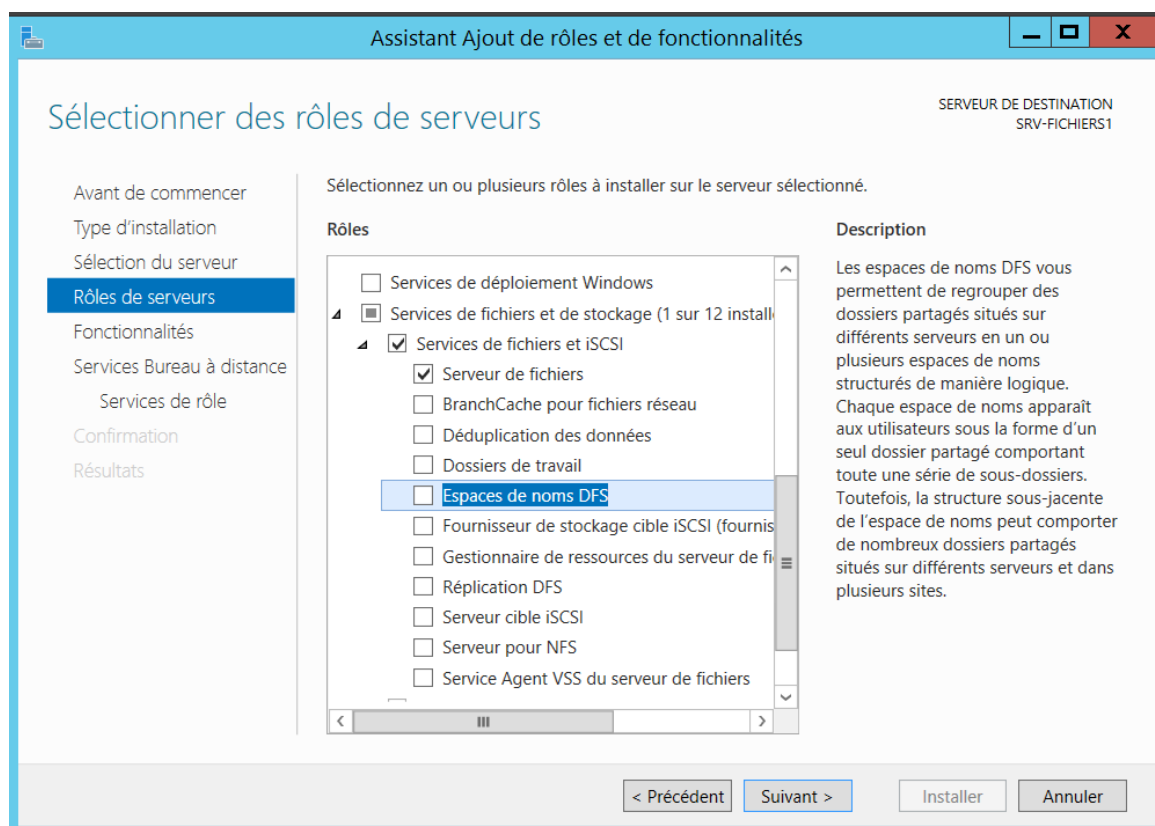




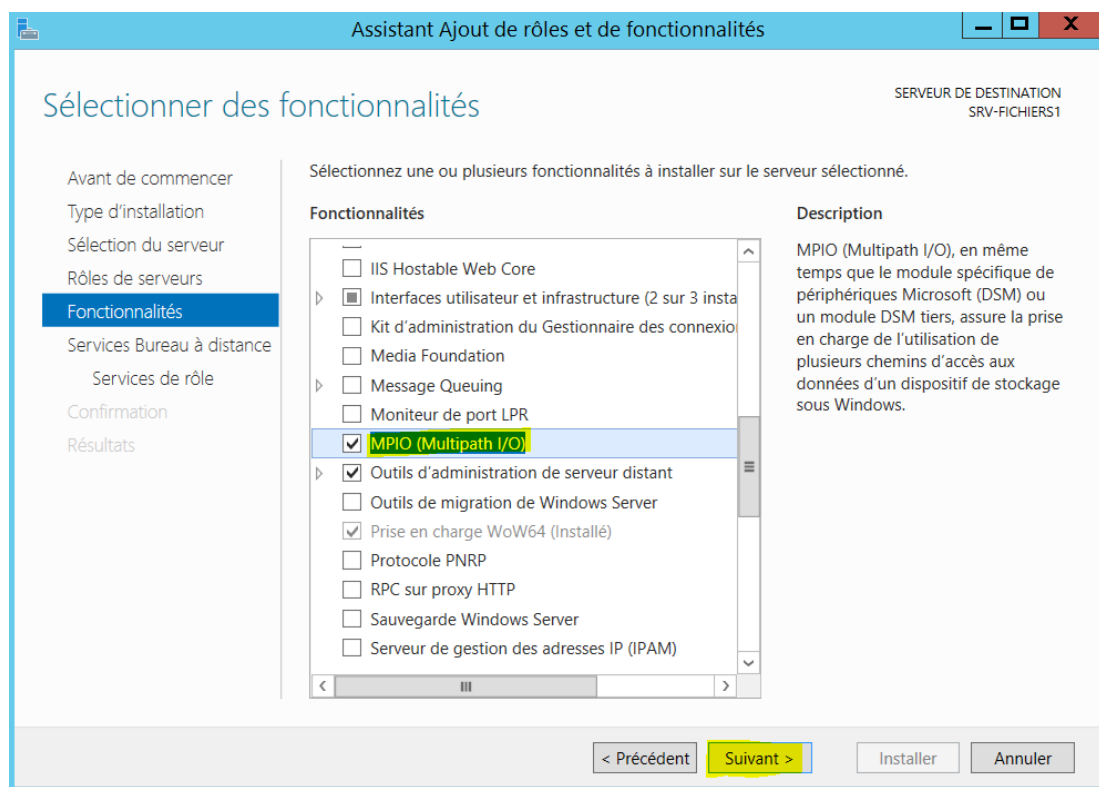
Cliquez sur « **suivant** » après avoir sélectionné votre serveur .



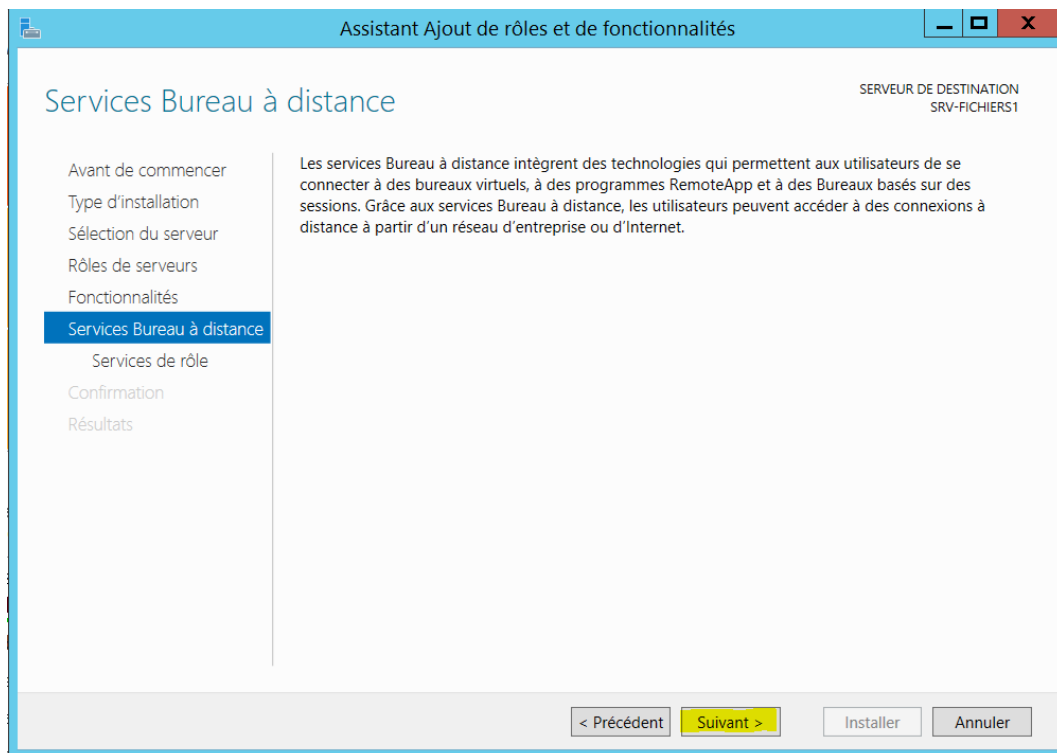
Sélectionnez « **Serveur de Fichiers** », « **Espace de noms DFS** » et « **Réplication DFS** ».



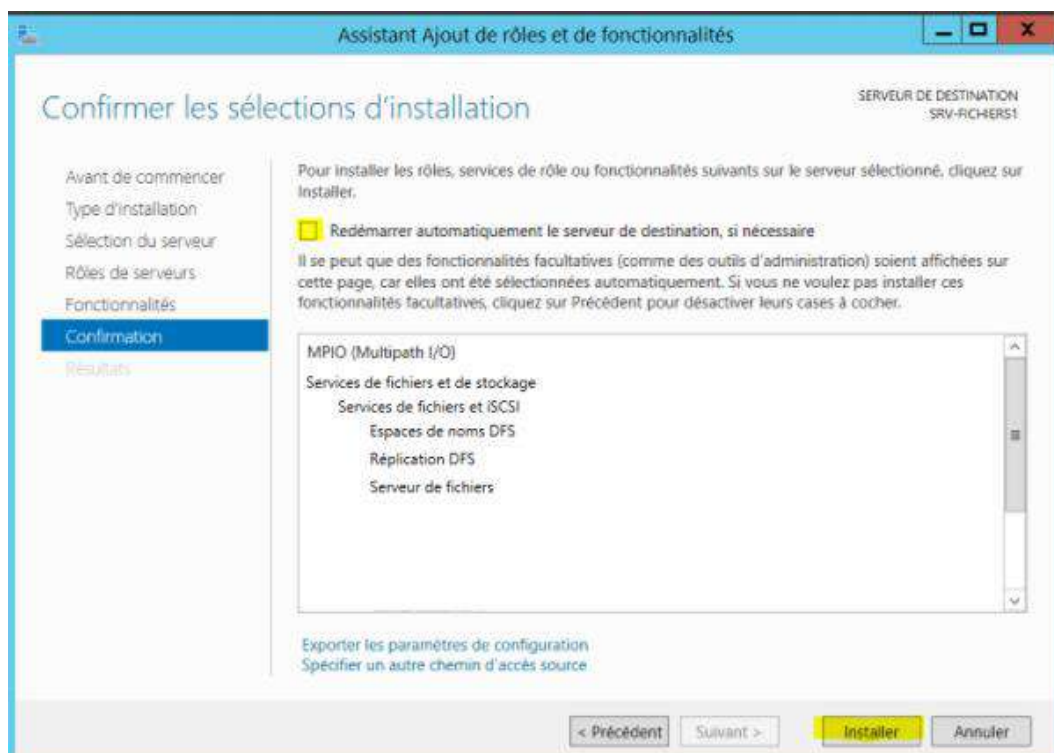
Ensuite dans « **Fonctionnalités** », sélectionnez « **MPIO** ».



Cliquez sur « **Suivant** ».



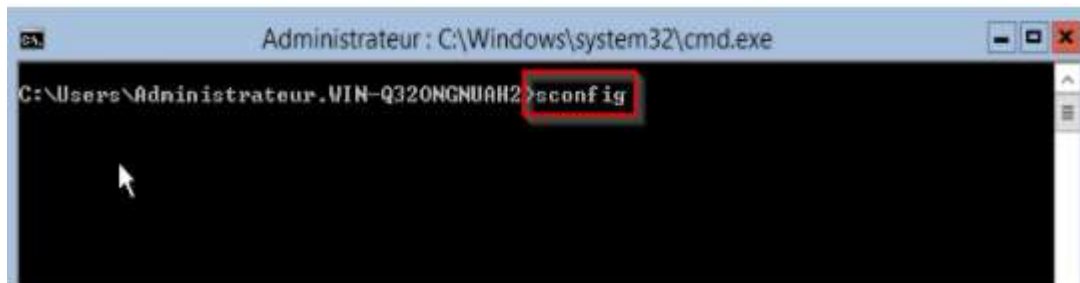
Cliquez sur « **Installer** ».



SRV-FICHIERS1 est installé, passons à l'installation en « **core** », du SRV-FICHIERS2.

Installation de SRV-FICHIERS2

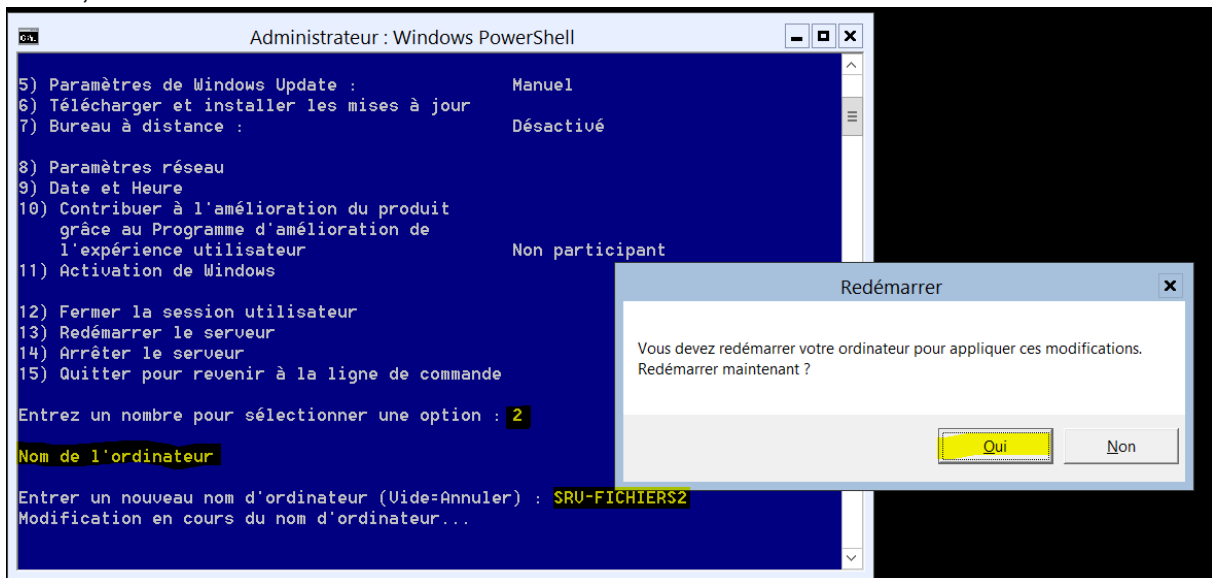
Lors de l'installation de Windows, nous choisirons le mode « **Installation minimale** ». Une fois l'installation terminée, Windows démarre et une invite de commande se lance. Afin de configurer le serveur, tapez « **sconfig** ».



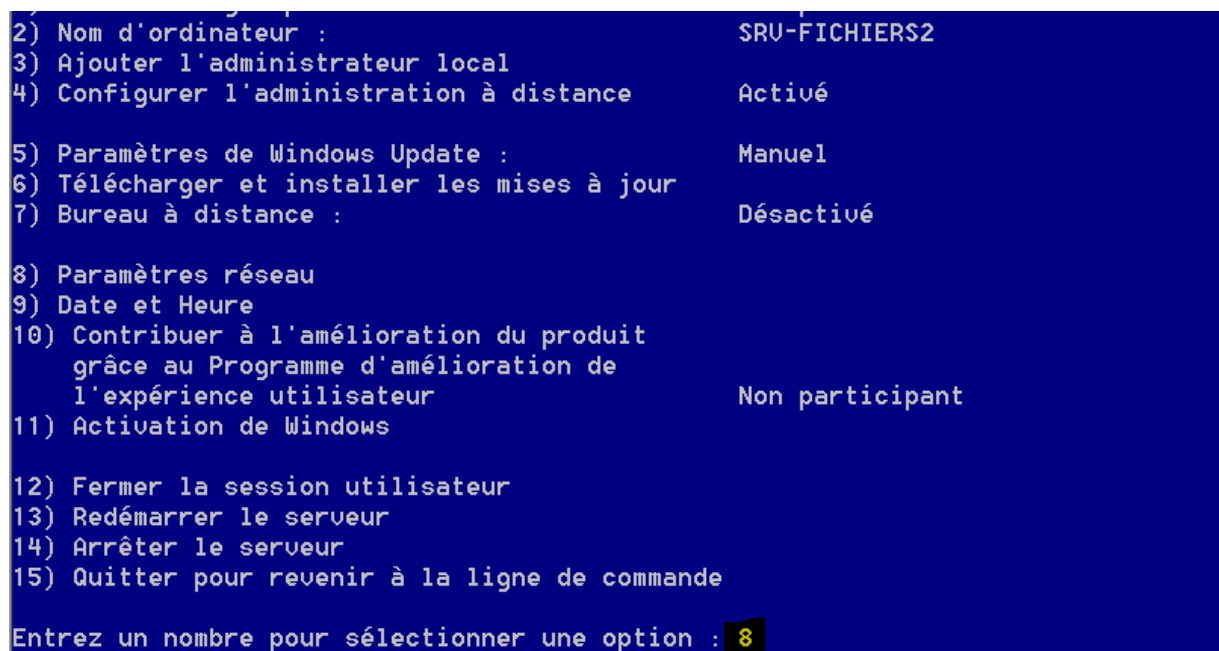
Par ce menu, nous allons pouvoir configurer le nom de la machine, joindre le domaine ou configurer le réseau.



Pour modifier le nom, tapez « 2 », puis renseignez SRV-FICHIERS2 et cliquez sur « OK »,



Pour les paramètres réseau, tapez « 8 ».



Tapez « 10 » pour sélectionner la carte réseau.



```

Administrateur : Windows PowerShell

10) Contribuer à l'amélioration du produit
    grâce au Programme d'amélioration de
    l'expérience utilisateur                Non participant
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 : 8

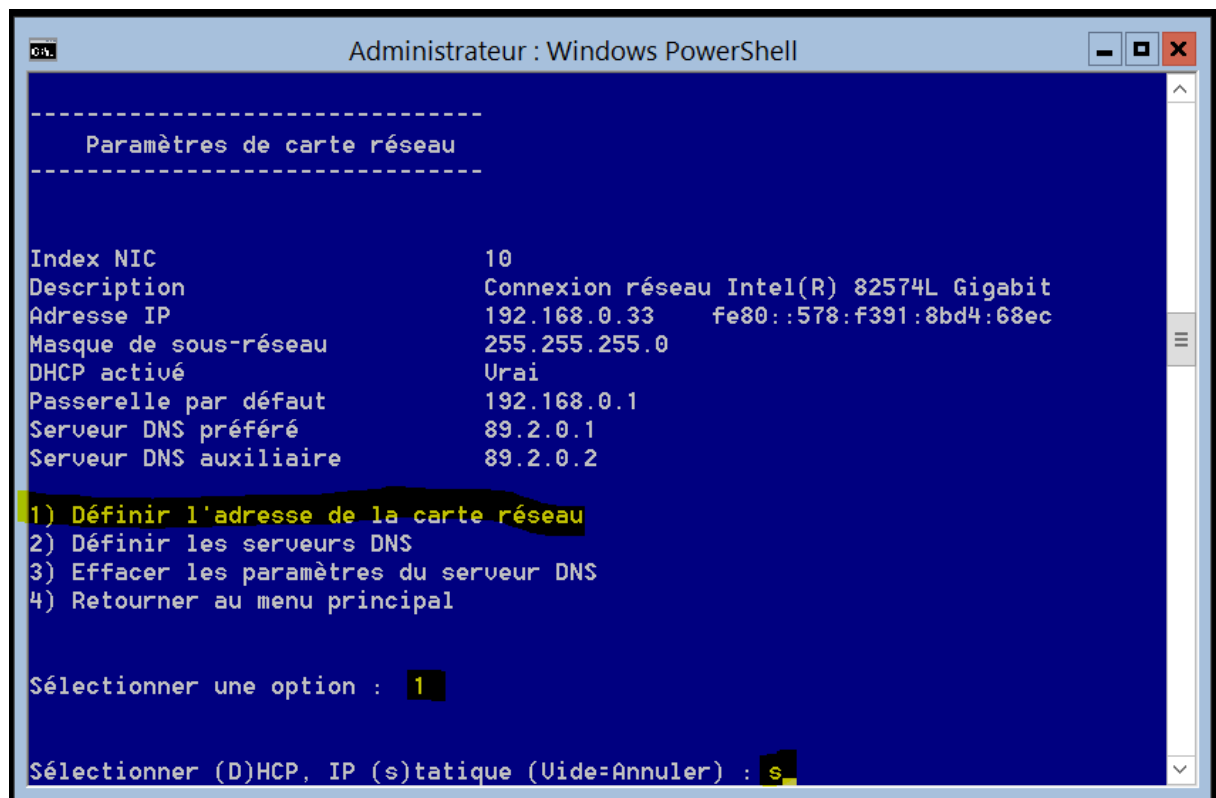
-----
Paramètres réseau
-----

Cartes réseau disponibles

Index#  Adresse IP      Description
-----
10      192.168.0.33    Connexion réseau Intel(R) 82574L Gigabit

Sélectionner Index# de la carte réseau (Vide=Annuler) : 10
  
```

Tapez « 1 » pour définir l'adresse de la carte, le masque et la passerelle.



```

Administrateur : Windows PowerShell

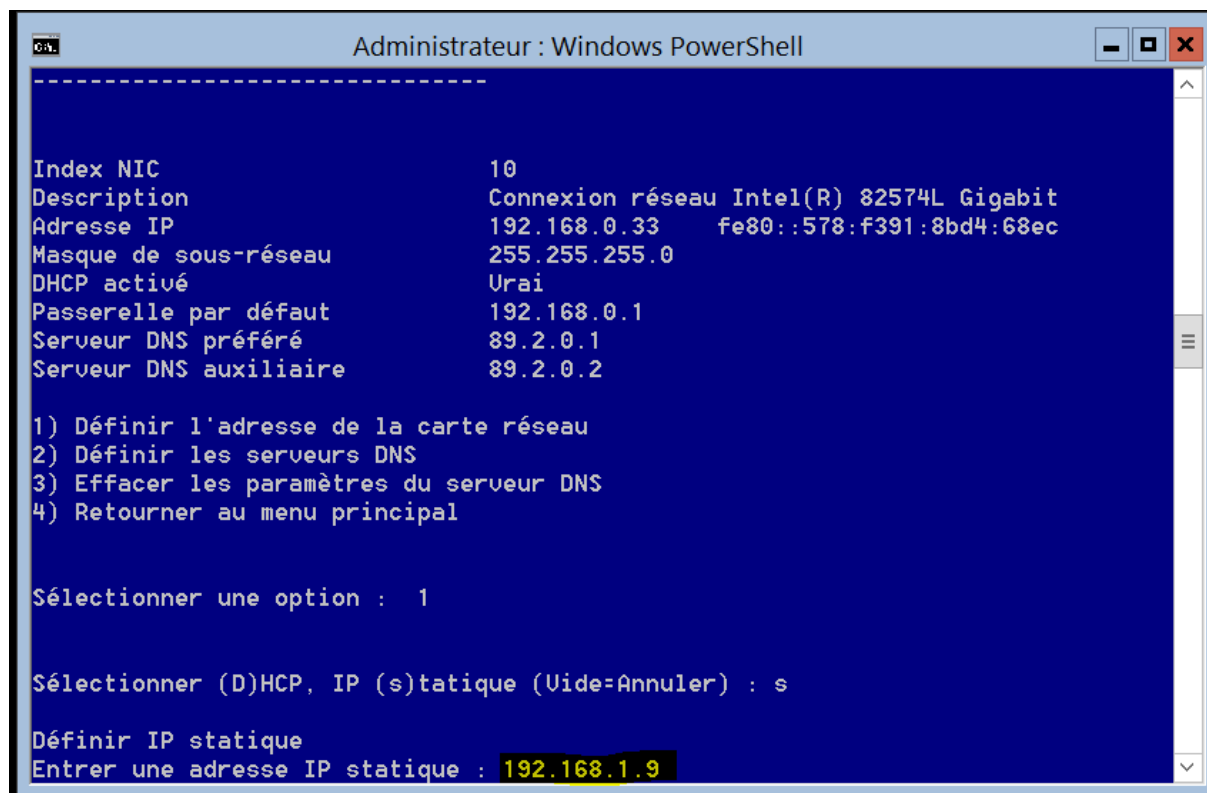
-----
Paramètres de carte réseau
-----

Index NIC      10
Description    Connexion réseau Intel(R) 82574L Gigabit
Adresse IP     192.168.0.33    fe80::578:f391:8bd4:68ec
Masque de sous-réseau 255.255.255.0
DHCP activé    Urai
Passerelle par défaut 192.168.0.1
Serveur DNS préféré 89.2.0.1
Serveur DNS auxiliaire 89.2.0.2

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
  
```



```
-----
Index NIC                10
Description              Connexion réseau Intel(R) 82574L Gigabit
Adresse IP               192.168.0.33    fe80::578:f391:8bd4:68ec
Masque de sous-réseau    255.255.255.0
DHCP activé              Urai
Passerelle par défaut    192.168.0.1
Serveur DNS préféré      89.2.0.1
Serveur DNS auxiliaire   89.2.0.2

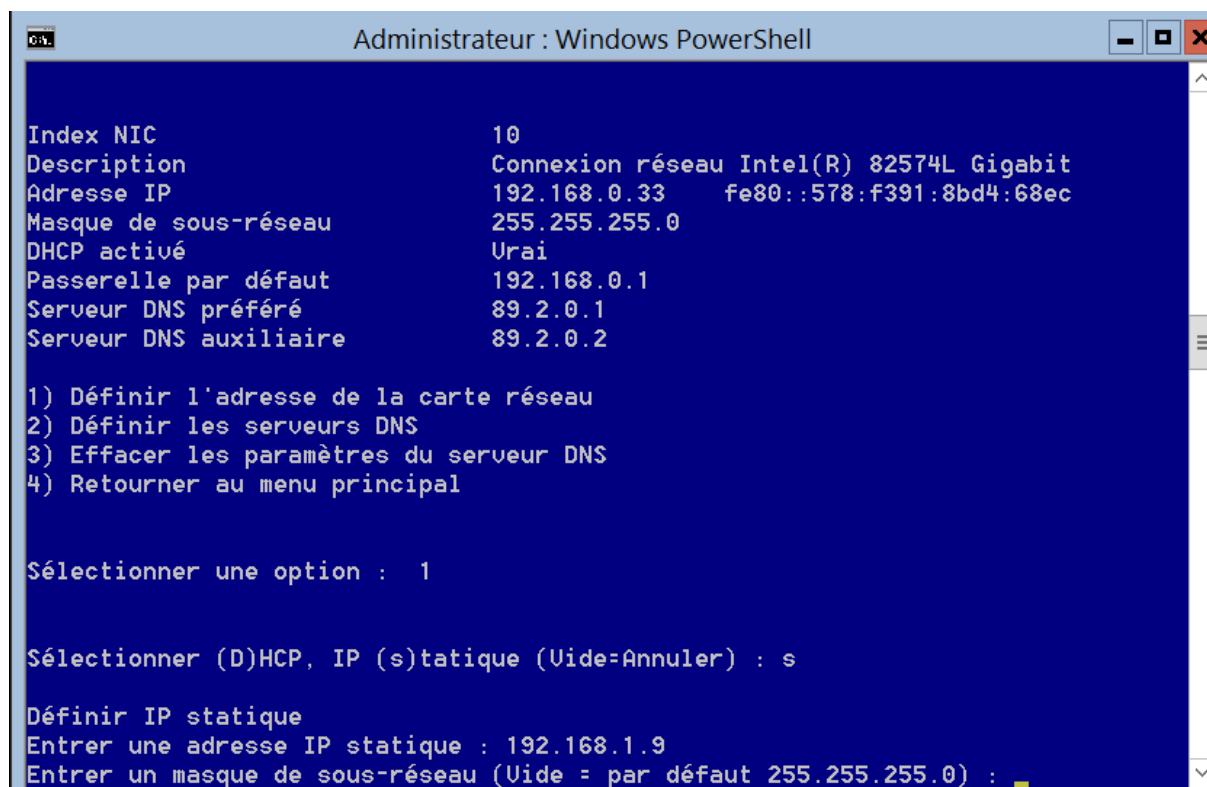
1) Définir l'adresse de la carte réseau
2) Définir les serveurs DNS
3) Effacer les paramètres du serveur DNS
4) Retourner au menu principal

Sélectionner une option : 1

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

Définir IP statique
Entrer une adresse IP statique : 192.168.1.9
```

Renseignez le masque de sous réseau



```
Index NIC                10
Description              Connexion réseau Intel(R) 82574L Gigabit
Adresse IP               192.168.0.33    fe80::578:f391:8bd4:68ec
Masque de sous-réseau    255.255.255.0
DHCP activé              Urai
Passerelle par défaut    192.168.0.1
Serveur DNS préféré      89.2.0.1
Serveur DNS auxiliaire   89.2.0.2

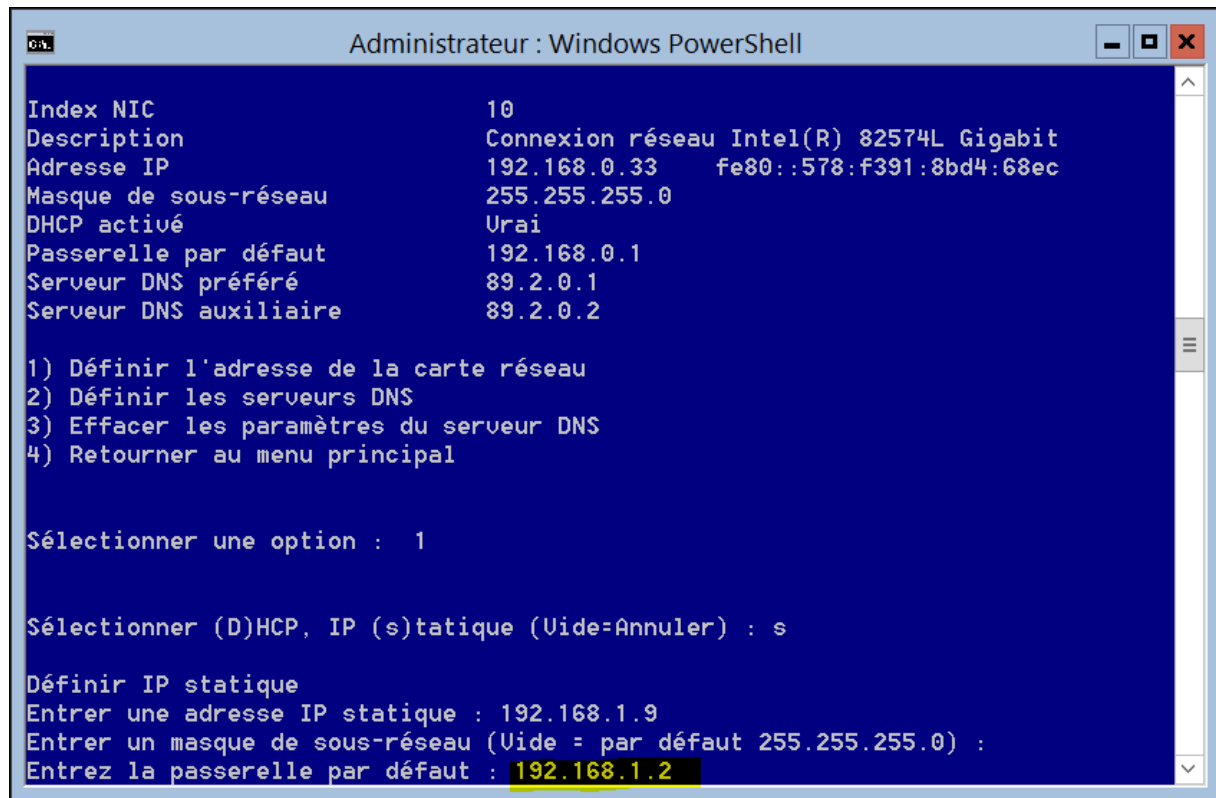
1) Définir l'adresse de la carte réseau
2) Définir les serveurs DNS
3) Effacer les paramètres du serveur DNS
4) Retourner au menu principal

Sélectionner une option : 1

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

Définir IP statique
Entrer une adresse IP statique : 192.168.1.9
Entrer un masque de sous-réseau (U)ide = par défaut 255.255.255.0) : 
```

Faire de même pour la passerelle



Administrateur : Windows PowerShell

```
Index NIC                10
Description              Connexion réseau Intel(R) 82574L Gigabit
Adresse IP               192.168.0.33    fe80::578:f391:8bd4:68ec
Masque de sous-réseau    255.255.255.0
DHCP activé              Urai
Passerelle par défaut    192.168.0.1
Serveur DNS préféré      89.2.0.1
Serveur DNS auxiliaire   89.2.0.2

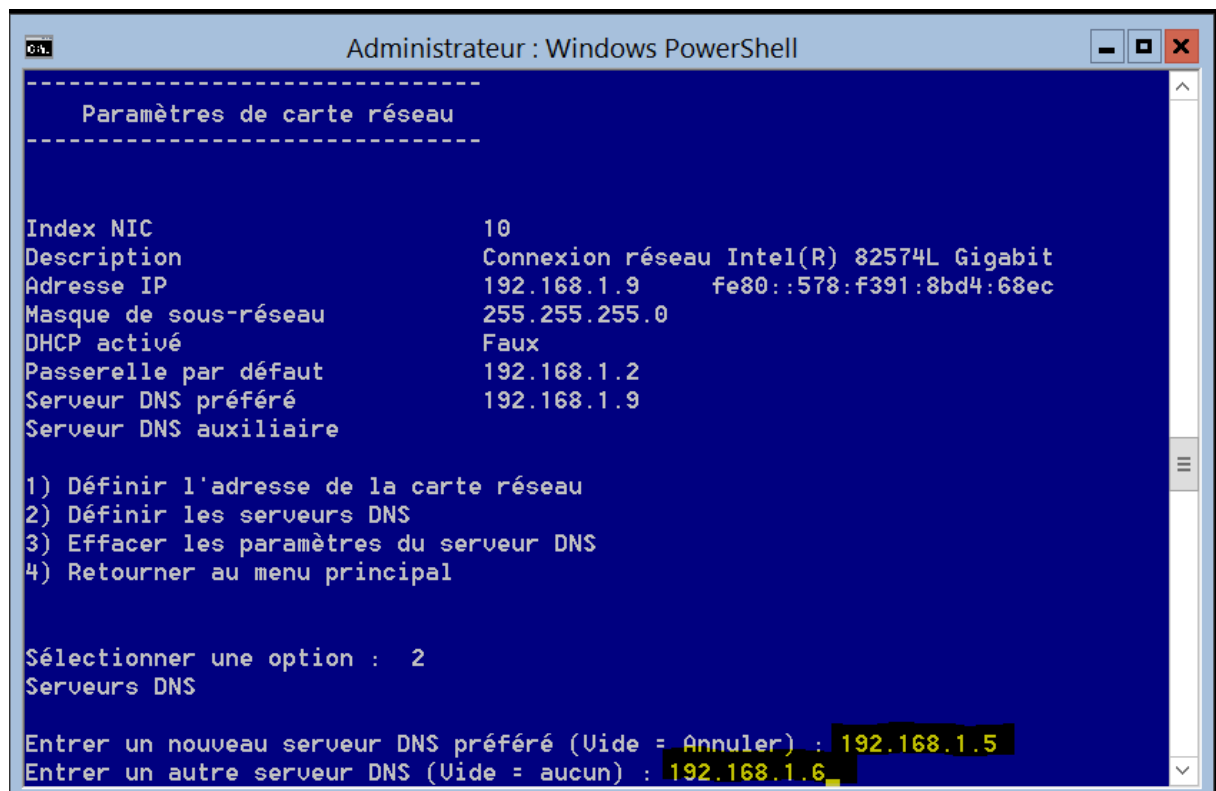
1) Définir l'adresse de la carte réseau
2) Définir les serveurs DNS
3) Effacer les paramètres du serveur DNS
4) Retourner au menu principal

Sélectionner une option : 1

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

Définir IP statique
Entrer une adresse IP statique : 192.168.1.9
Entrer un masque de sous-réseau (Vide = par défaut 255.255.255.0) :
Entrez la passerelle par défaut : 192.168.1.2
```

Tapez « 2 » pour renseigner l'adresse des serveurs DNS.



Administrateur : Windows PowerShell

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

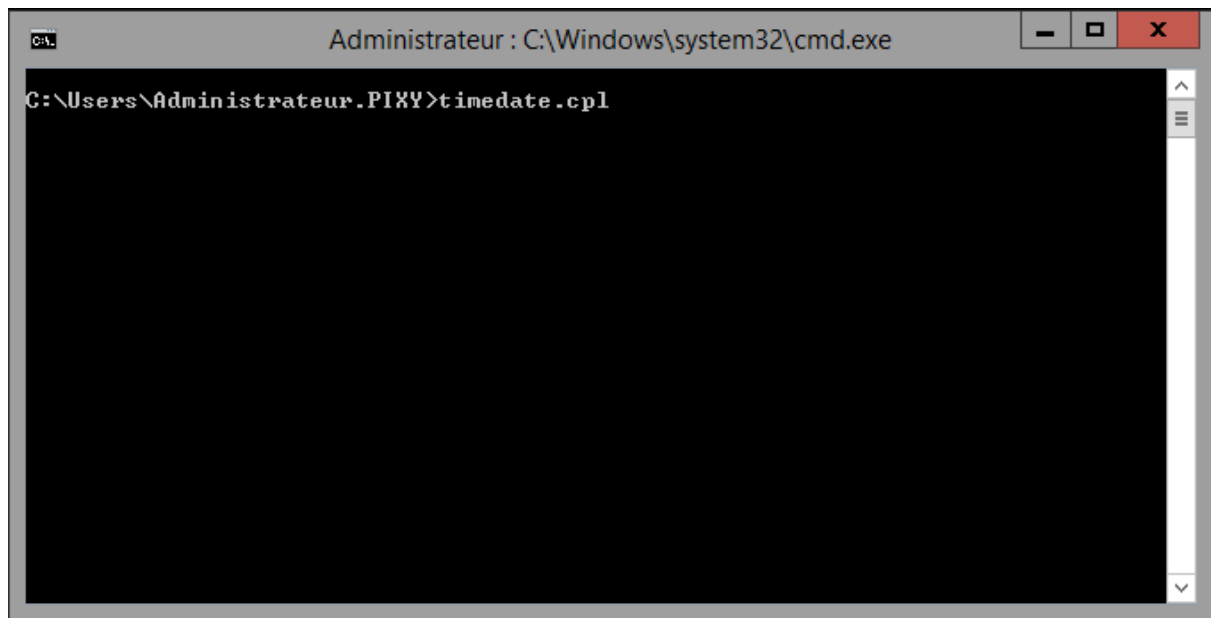
Index NIC                10
Description              Connexion réseau Intel(R) 82574L Gigabit
Adresse IP               192.168.1.9    fe80::578:f391:8bd4:68ec
Masque de sous-réseau    255.255.255.0
DHCP activé              Faux
Passerelle par défaut    192.168.1.2
Serveur DNS préféré      192.168.1.9
Serveur DNS auxiliaire   192.168.1.9

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

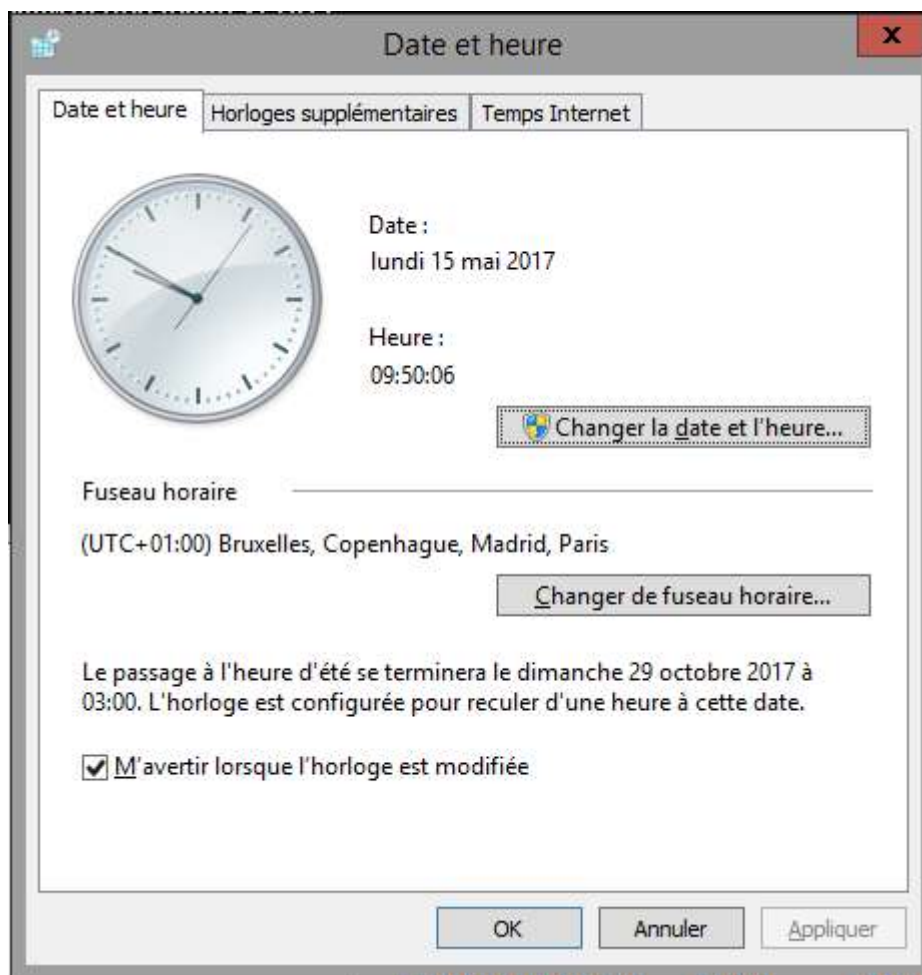
Sélectionner une option : 2
Serveurs DNS

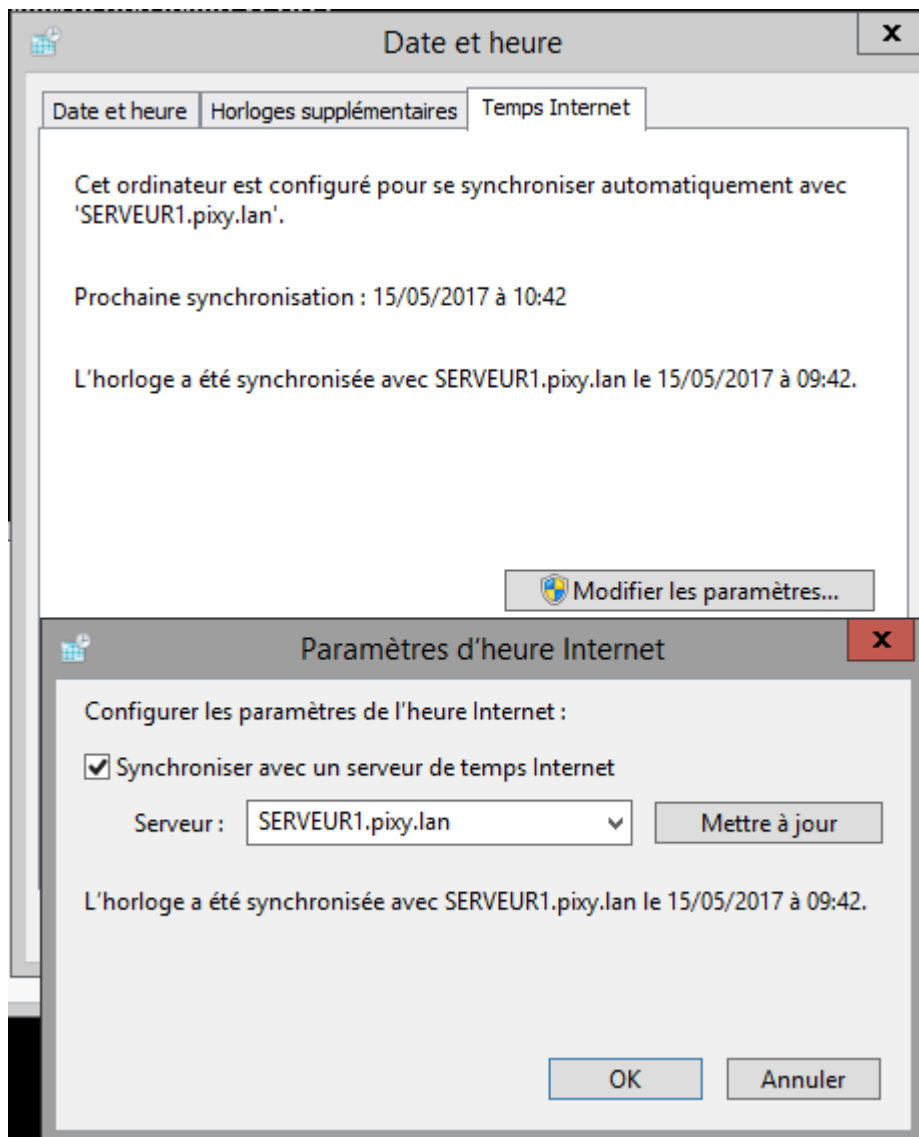
Entrer un nouveau serveur DNS préféré (Vide = Annuler) : 192.168.1.5
Entrer un autre serveur DNS (Vide = aucun) : 192.168.1.6
```

Configurer le serveur de temps et indiquer le serveur 1

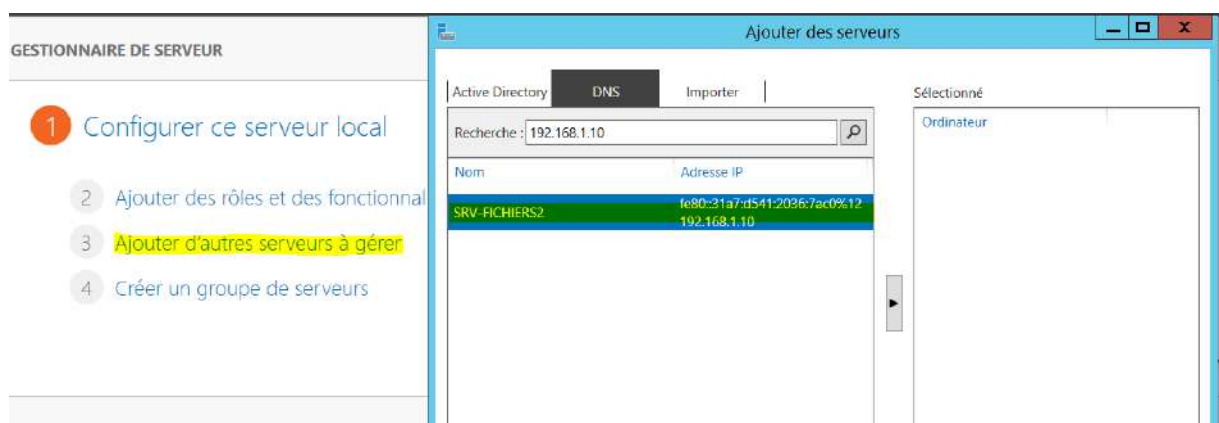


Cliquez sur "Temps Internet"





Afin de pouvoir administrer le serveur core à distance, nous allons l'ajouter dans le gestionnaire de serveur du SRV-FICHIERS1 et configurer winRM



Configurez les hôtes depuis lesquelles on autorise la connexion en tapant “Set-Item WsMan:\localhost\Client\TrustedHosts *” dans powershell, puis taper “o”

```
Configuration de la sécurité WinRM.
Cette commande modifie la liste TrustedHosts pour le client WinRM. Les ordinateurs figurant dans la liste TrustedHosts
ne sont pas nécessairement authentifiés. Or, le client risque d'envoyer des informations d'identification à destination
de ces ordinateurs. Êtes-vous sûr de vouloir modifier cette liste ?
[0] Oui [N] Non [S] Suspendre [?] Aide (la valeur par défaut est « 0 ») : 0
PS C:\Users\Administrateur> Restart-Service WinRM
```

Tapez “Restart-Service winrm” pour redémarrer le service winRM

```
Administrateur : Windows PowerShell
[SRV-FICHIERS2.pixy.lan]: PS C:\Users\Administrateur.PIXY\Documents> Restart-Service winrm
```

Consultez la configuration de WinRM pour vérifier que l'entrée est bien prise en compte. Pour cela on utilisera la commande suivante :

```
Administrateur : Windows PowerShell
[SRV-FICHIERS2.pixy.lan]: PS C:\Users\Administrateur.PIXY\Documents> winrm get winrm/config/client
Client
  NetworkDelays = 5000
  URLPrefix = wsman
  AllowUnencrypted = false
  Auth
    Basic = true
    Digest = true
    Kerberos = true
    Negotiate = true
    Certificate = true
    CredSSP = false
  DefaultPorts
    HTTP = 5985
    HTTPS = 5986
  TrustedHosts = *
```

Voici ce qu'il faut renseigner pour se connecter à la machine distante, pensez à préciser un identifiant avec des droits élevés :

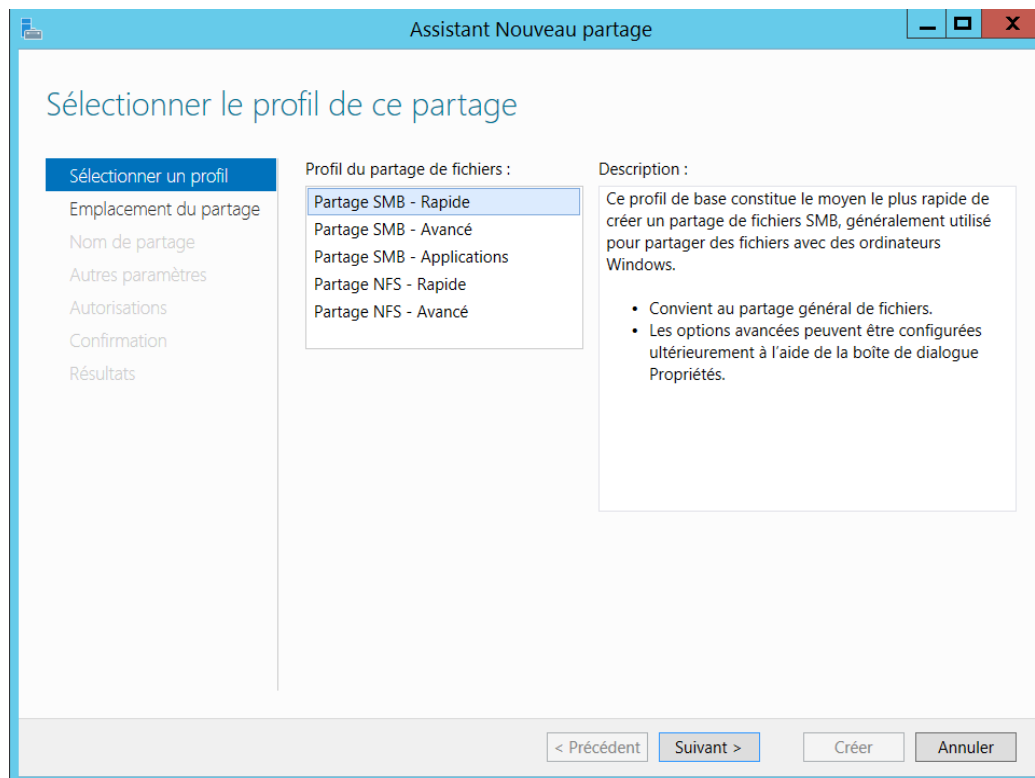
Enter-PSSession -ComputerName SRV-FICHIERS2.pixy.lan -Credential
PIXY\Administrateur

Lorsque la connexion sera établie, vous obtiendrez un shell PowerShell sur la machine distante.

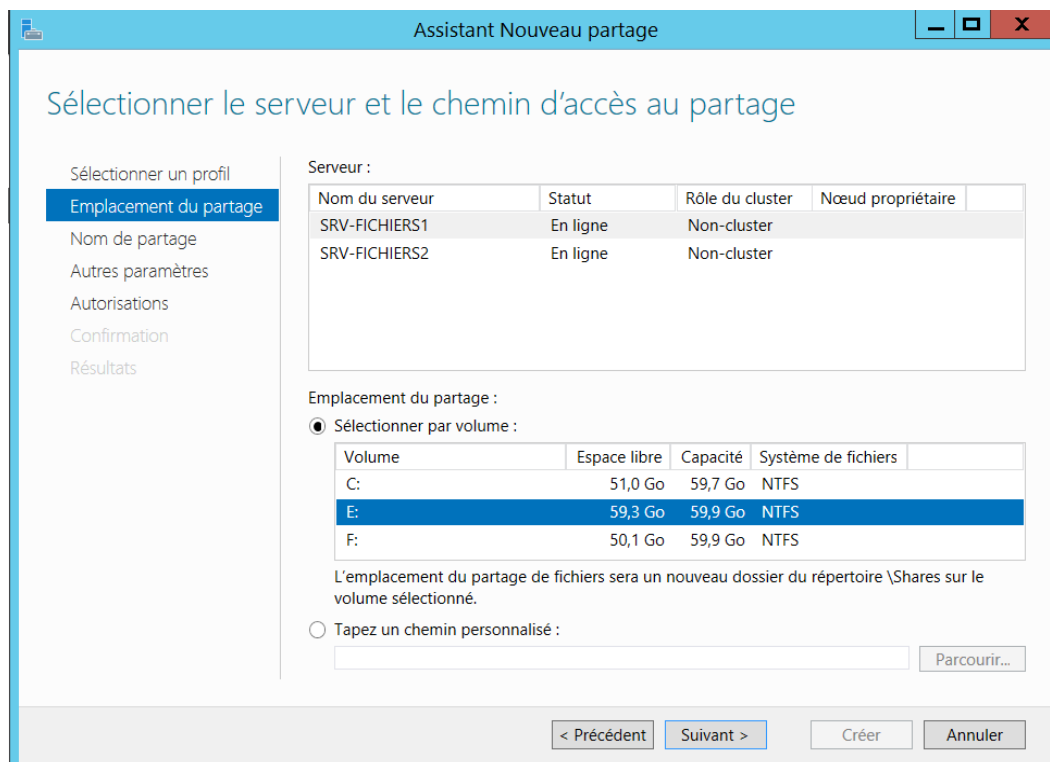
```
Sélectionner Administrateur : Windows PowerShell
pixy.lan]: PS C:\Users\Administrateur.PIXY\Documents> Enter-PSSession -ComputerName SRV-FICHIERS2.pixy.lan -Credential PIXY\Administrateur
```

Pour quitter la session PowerShell distante, il suffira d'entrer la commande suivante : Exit-PSSession Vous reviendrez alors sur la console PowerShell de votre machine locale.

Création d'un nouveau partage. Faire clique droit dans "Serveur de fichiers\Partage" et choisissez "nouveau partage"



Sélectionnez le disque où vous souhaitez créer le partage



Indiquez le nom du partage

The screenshot shows the 'Assistant Nouveau partage' window with the title bar 'Assistant Nouveau partage'. The main heading is 'Indiquer le nom de partage'. On the left, a sidebar lists steps: 'Sélectionner un profil', 'Emplacement du partage', 'Nom de partage' (highlighted), 'Autres paramètres', 'Autorisations', 'Confirmation', and 'Résultats'. The main area contains the following fields and options:

- 'Nom du partage :' with the text 'Communservice' entered.
- 'Description du partage :' with an empty text box.
- 'Chemin d'accès local au partage :' with the text 'E:\Shares\Communservice'.
- A blue information icon followed by the text: 'Si le dossier n'existe pas, il est créé.'
- 'Chemin d'accès distant au partage :' with the text '\\SRV-FICHIERS1\Communservice'.

At the bottom, there are four buttons: '< Précédent', 'Suivant >', 'Créer', and 'Annuler'.

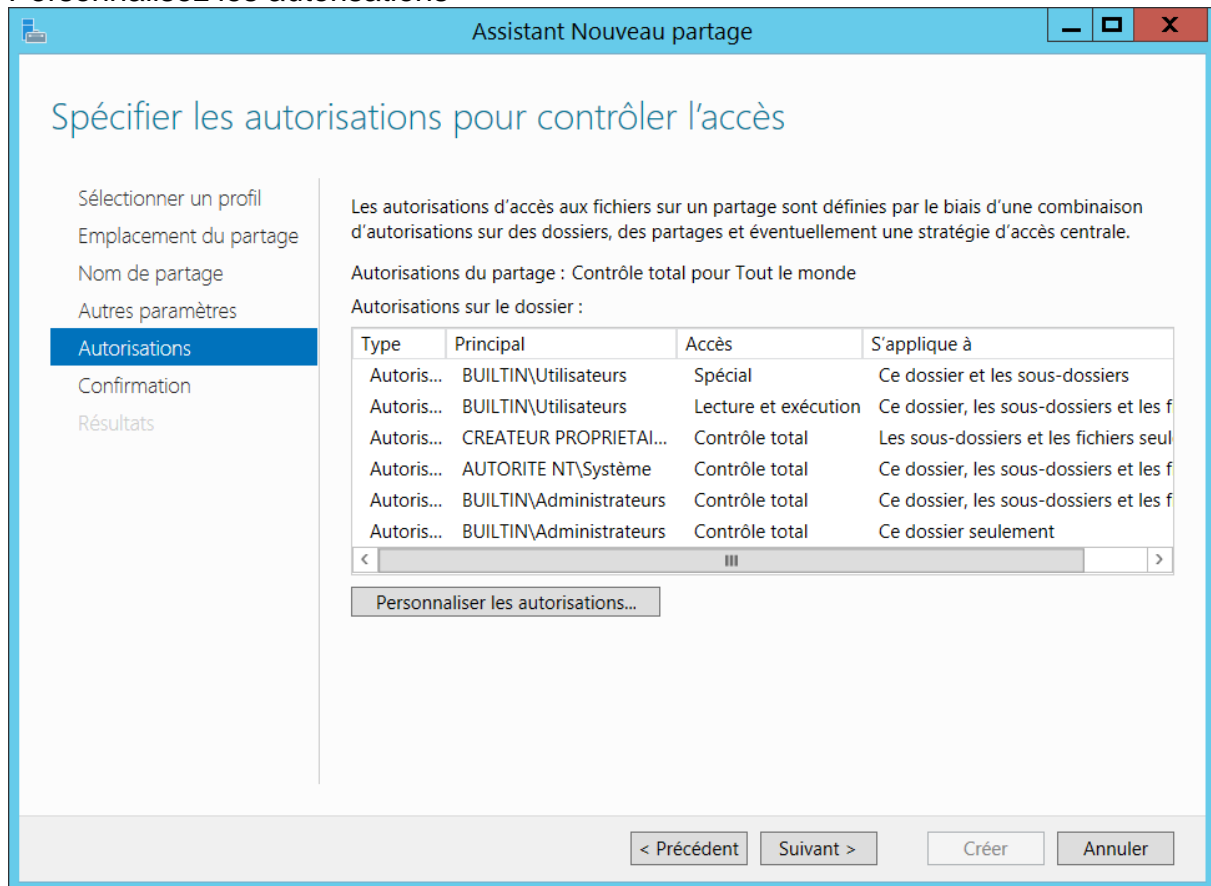
Activer l'énumération basée sur l'accès

The screenshot shows the 'Assistant Nouveau partage' window with the title bar 'Assistant Nouveau partage'. The main heading is 'Configurer les paramètres de partage'. On the left, the sidebar lists steps: 'Sélectionner un profil', 'Emplacement du partage', 'Nom de partage', 'Autres paramètres' (highlighted), 'Autorisations', 'Confirmation', and 'Résultats'. The main area contains the following options and text:

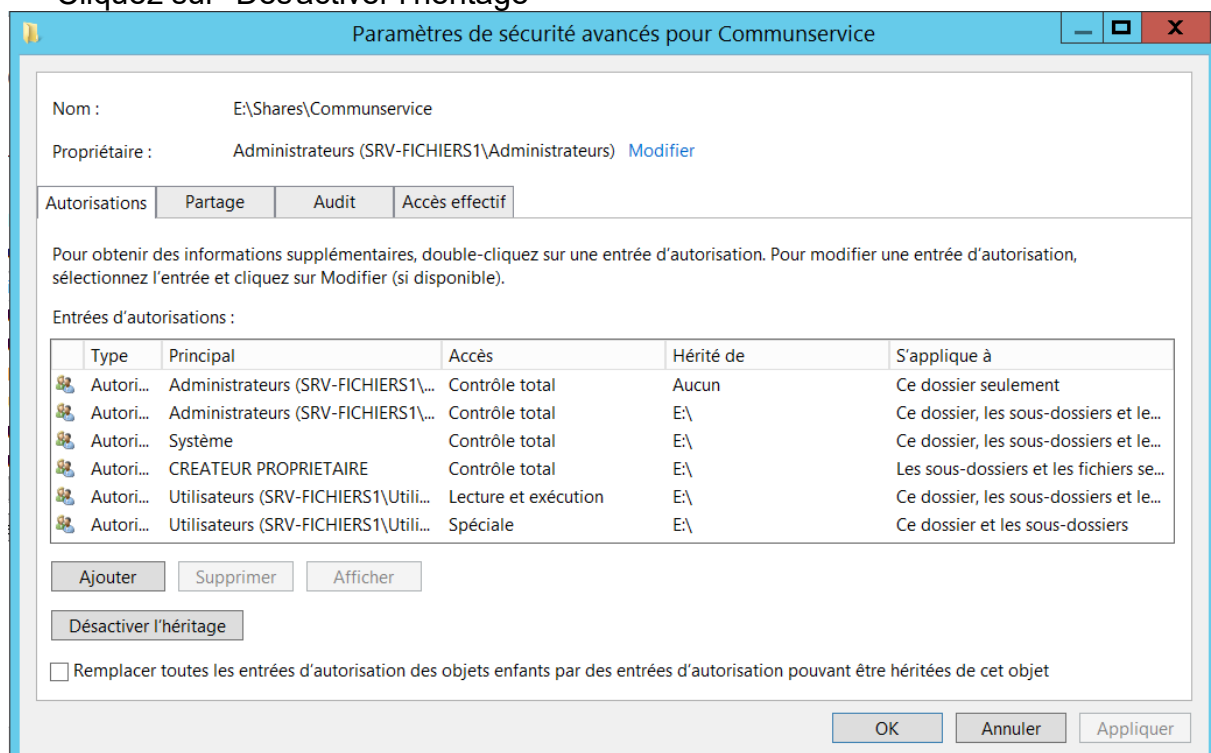
- ☒ 'Activer l'énumération basée sur l'accès'. Below it, a paragraph: 'L'énumération basée sur l'accès n'affiche que les fichiers et les dossiers dont un utilisateur possède les autorisations d'accès. S'il ne bénéficie pas d'autorisations en lecture (ou équivalentes) sur un dossier, Windows cache alors ce dernier de l'utilisateur.'
- ☐ 'Autoriser la mise en cache du partage'. Below it, a paragraph: 'La mise en cache met le contenu du partage à la disposition des utilisateurs hors connexion. Si la fonctionnalité BranchCache du service de rôle Fichiers réseau est installée, vous pouvez activer BranchCache sur le partage.'
- ☐ 'Activer le cache de filiale (BranchCache) sur le partage de fichiers'. Below it, a paragraph: 'BranchCache permet aux ordinateurs d'une succursale de mettre en cache les fichiers téléchargés à partir de ce partage, puis de les rendre disponibles en toute sécurité pour les autres ordinateurs de la succursale.'
- ☐ 'Chiffrer l'accès aux données'. Below it, a paragraph: 'Lorsqu'il est activé, l'accès distant aux fichiers de ce partage est chiffré. Cela a pour effet de sécuriser les données contre tout accès non autorisé lors de leur transfert vers ou depuis le partage. Si cette case à cocher est activée et grisée, cela signifie qu'un administrateur a activé le chiffrement pour l'ensemble du serveur.'

At the bottom, there are four buttons: '< Précédent', 'Suivant >', 'Créer', and 'Annuler'.

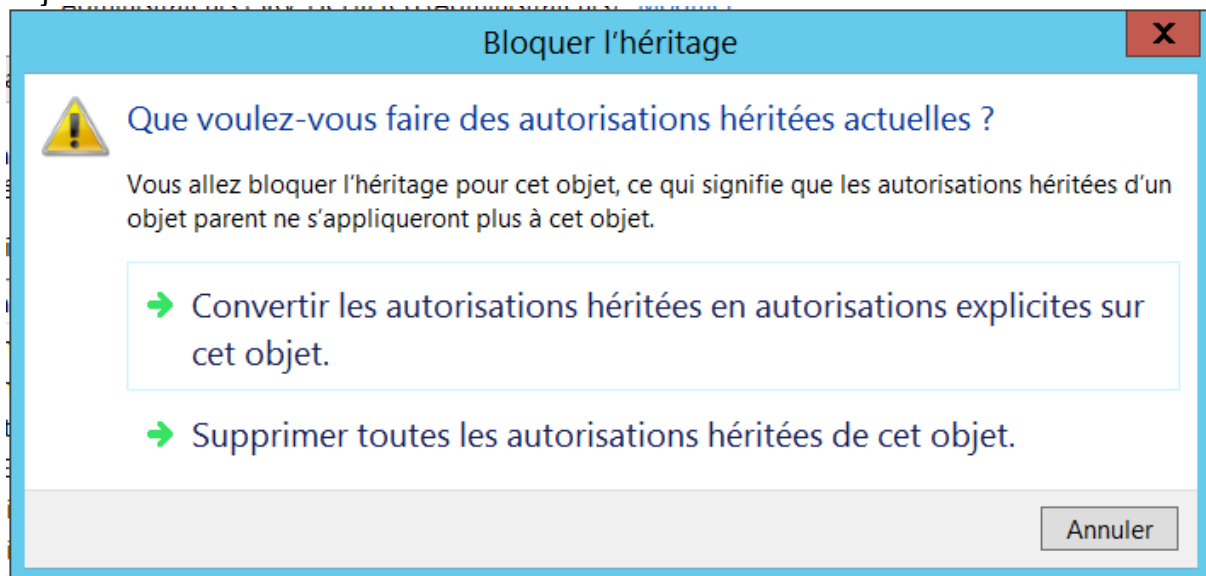
Personnalisez les autorisations



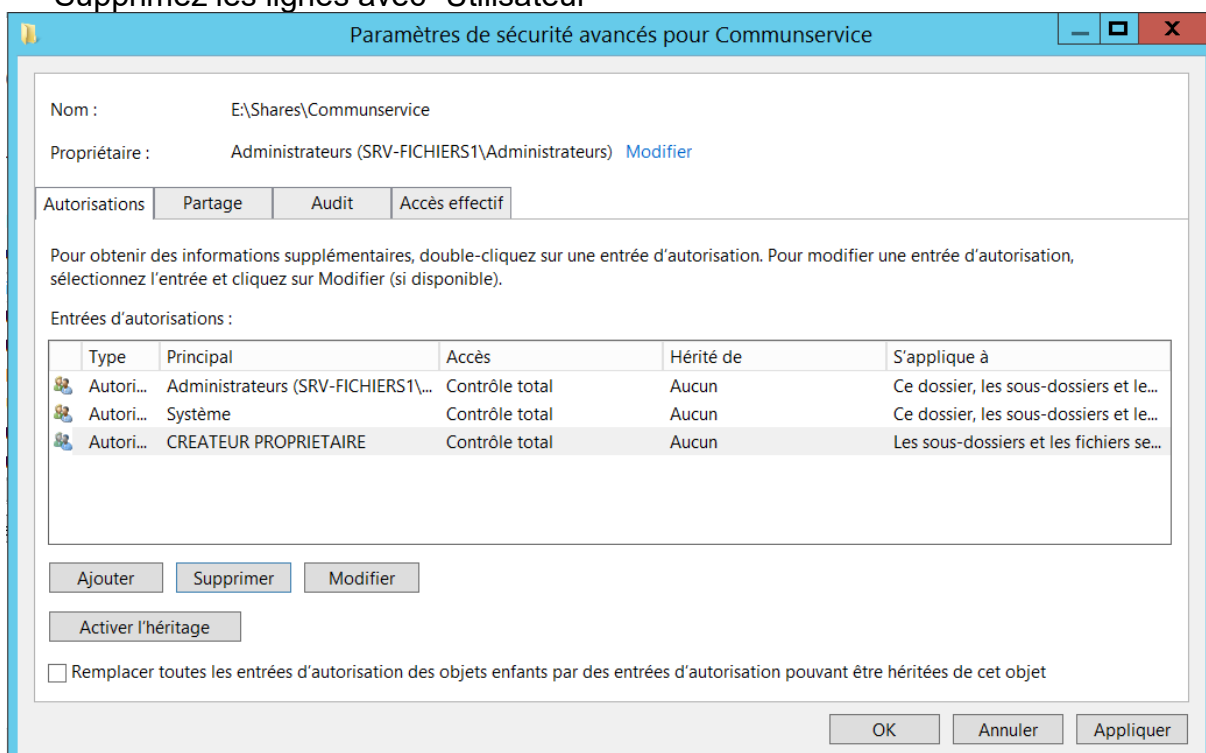
Cliquez sur "Désactiver l'héritage"



Sélectionnez “ Convertir les autorisations héritées en autorisation explicites sur cet objet”



Supprimez les lignes avec “Utilisateur”



Autorisations pour Communservice

Principal : Sélectionnez un principal

Type : Autoriser

S'applique à : Ce dossier, les sous-dossiers et les fichiers

Autorisations de base :

- ☐ Contrôle total
- ☐ Modification
- ☒ Lecture et exécution
- ☒ Affichage du contenu du dossier
- ☒ Lecture
- ☒ Écriture
- ☐ Autorisations spéciales

☐ Appliquer ces autorisations uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur

Ajouter une condition

Impossible de contacter Active Directory pour accéder aux types de revendications ou pour les vérifier.

OK Annuler

Sélectionnez les “utilisateurs du domaine” puis “ok”

Autorisations pour Communservice

Principal : Utilisateurs du domaine (PIXY\\Utilisateurs du domaine) Sélectionnez un principal

Type : Autoriser

S'applique à : Ce dossier, les sous-dossiers et les fichiers

Autorisations de base :

- ☐ Contrôle total
- ☐ Modification
- ☒ Lecture et exécution
- ☒ Affichage du contenu du dossier
- ☒ Lecture
- ☒ Écriture
- ☐ Autorisations spéciales

☐ Appliquer ces autorisations uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur

Ajouter une condition

Impossible de contacter Active Directory pour accéder aux types de revendications ou pour les vérifier.

OK Annuler

Cliquez sur “créer”

Assistant Nouveau partage

Confirmer les sélections

Sélectionner un profil
Emplacement du partage
Nom de partage
Autres paramètres
Autorisations
Confirmation
Résultats

Vérifiez que les paramètres suivants sont corrects, puis cliquez sur Créer.

EMPLACEMENT DU PARTAGE

Serveur :	SRV-FICHIERS1
Rôle du cluster :	Non-cluster
Chemin d'accès local :	E:\Shares\Communservice

PROPRIÉTÉS DU PARTAGE

Nom du partage :	Communservice
Protocole :	SMB
Énumération basée sur l'accès :	Activé
Mise en cache :	Désactivé
BranchCache :	Désactivé
Chiffrer les données :	Désactivé

< Précédent Suivant > Créer Annuler

Votre nouveau partage est maintenant créé et configuré.

Nous allons maintenant configurer l'espace de nom. Nous renseignerons "SRV-FICHIERS1"

The screenshot shows the 'Assistant Nouvel espace de noms' window. The title bar is 'Assistant Nouvel espace de noms'. The main title is 'Serveur d'espaces de noms'. On the left, under 'Étapes :', the steps are: 'Serveur d'espaces de noms' (selected), 'Nom et paramètres de l'espace de noms', 'Type d'espace de noms', 'Revoir les paramètres et créer l'espace de noms', and 'Confirmation'. The main area contains the instruction: 'Entrez le nom du serveur qui hébergera l'espace de noms. Le serveur spécifié sera reconnu comme le serveur d'espaces de noms.' Below this, there is a 'Serveur :' label and a text box containing 'srv-fichiers1'. To the right of the text box is a 'Parcourir...' button. At the bottom right, there are three buttons: '< Précédent', 'Suivant >', and 'Annuler'.

Nommez l'espace de nom

The screenshot shows the 'Assistant Nouvel espace de noms' window. The title bar is 'Assistant Nouvel espace de noms'. The main title is 'Nom et paramètres de l'espace de noms'. On the left, under 'Étapes :', the steps are: 'Serveur d'espaces de noms', 'Nom et paramètres de l'espace de noms' (selected), 'Type d'espace de noms', 'Revoir les paramètres et créer l'espace de noms', and 'Confirmation'. The main area contains the instruction: 'Entrez un nom pour l'espace de noms. Ce nom apparaîtra après le nom du serveur ou du domaine dans le chemin d'accès de l'espace de noms, par exemple \\Serveur\Nom or \\Domaine\Nom.' Below this, there is a 'Nom :' label and a text box containing 'Communservice'. Below the text box is the text 'Exemple : Public'. Further down, there is a paragraph: 'Au besoin, l'Assistant créera un dossier partagé sur le serveur d'espaces de noms. Pour modifier les paramètres du dossier partagé (chemin d'accès ou autorisations), cliquez sur Modifier les paramètres.' Below this paragraph is a 'Modifier les paramètres...' button. At the bottom right, there are three buttons: '< Précédent', 'Suivant >', and 'Annuler'.

Indiquer le chemin d'accès local du dossier

Modifier les paramètres

Serveur d'espaces de noms :
srv-fichiers1

Dossier partagé :
Communservice

Chemin d'accès local du dossier partagé :
E:\Shares\Communservice Parcourir...


Autorisations du dossier partagé :

- ☒ Tous les utilisateurs disposent d'autorisations de lecture seule
- ☐ Tous les utilisateurs disposent d'autorisations de lecture/écriture
- ☐ Les administrateurs ont un accès total, les autres ont un accès en lecture seule
- ☐ Les administrateurs ont un accès total, les autres ont un accès en lecture/écriture
- ☐ Utiliser des autorisations personnalisées : Personnaliser...

OK Annuler

Cliquez sur "Oui"

Avertissement

 Un dossier partagé nommé « Communservice » existe déjà sur le serveur « srv-fichiers1 ». Si le dossier partagé existant est utilisé, le paramètre de sécurité défini dans la boîte de dialogue Modifier les paramètres ne s'appliquera pas. Pour qu'un dossier partagé soit créé avec ces paramètres, vous devez d'abord supprimer le dossier partagé existant.

Voulez-vous utiliser le dossier partagé existant et ses paramètres de sécurité actuels ?

Oui Non

Sélectionnez “espace de nom de domaine” puis “suivant” et “créer”

Assistant Nouvel espace de noms

Type d'espace de noms

Étapes :

- Serveur d'espaces de noms
- Nom et paramètres de l'espace de noms
- Type d'espace de noms
- Revoir les paramètres et créer l'espace de noms
- Confirmation

Sélectionnez le type d'espace de noms à créer.

☒ Espace de noms de domaine

Un espace de noms de domaine est stocké sur un ou plusieurs serveurs d'espaces de noms et dans les services de domaine Active Directory. Vous pouvez accroître la disponibilité d'un espace de noms de domaine en utilisant plusieurs serveurs. Lorsqu'il est créé dans le mode Windows Server 2008, l'espace de noms prend en charge une plus grande extensibilité et énumération basée sur l'accès.

☒ Activer le mode Windows Server 2008

Aperçu de l'espace de noms de domaine :

\\pixy.lan\Communservice

☐ Espace de noms autonome

Un espace de noms autonome est stocké sur un serveur d'espaces de noms unique. Lorsqu'il est hébergé sur un cluster de basculement, sa disponibilité est accrue.

Aperçu d'un espace de noms autonome :

\\srv-fichiers1\Communservice

< Précédent Suivant > Annuler

Assistant Nouvel espace de noms

Revoir les paramètres et créer l'espace de noms

Étapes :

- Serveur d'espaces de noms
- Nom et paramètres de l'espace de noms
- Type d'espace de noms
- Revoir les paramètres et créer l'espace de noms
- Confirmation

Vous avez sélectionné les paramètres suivants pour le nouvel espace de noms. Si les paramètres sont corrects, cliquez sur Créer pour créer votre espace de noms. Pour changer un paramètre, cliquez sur Précédent ou sélectionnez la page appropriée dans le volet d'orientation.

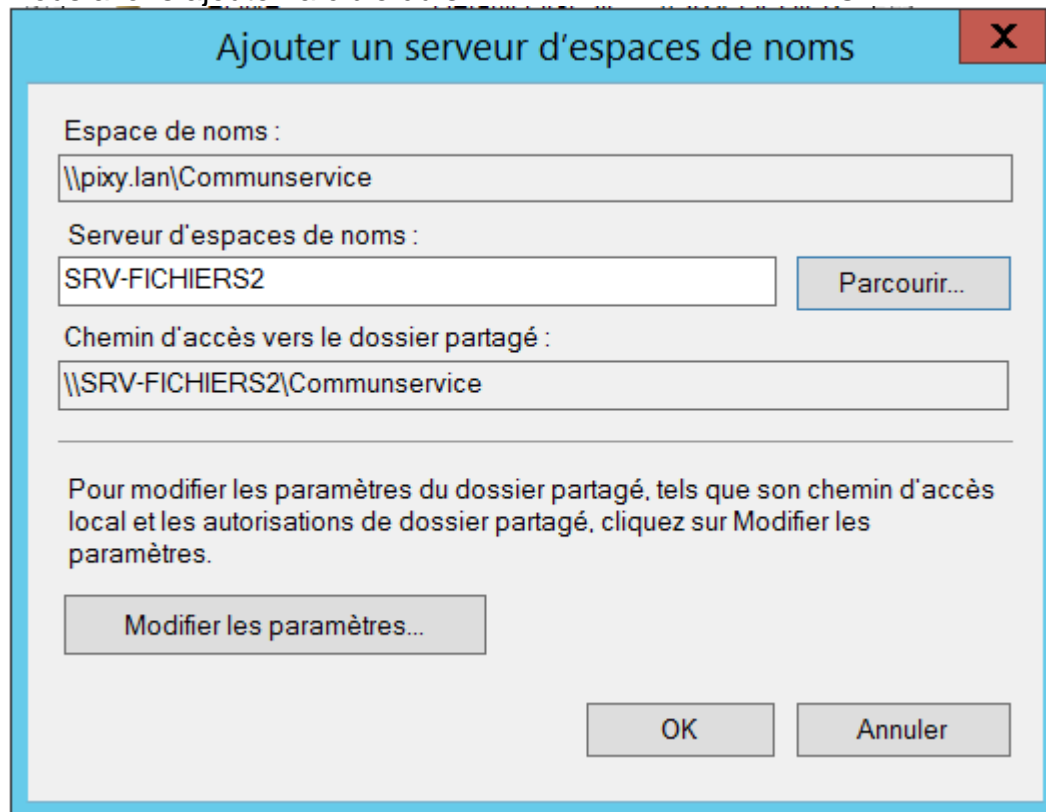
Paramètres de l'espace de noms :

Espace de noms

- Nom de l'espace de noms : \\pixy.lan\Communservice
- Type d'espace de noms : Domaine (Mode Windows Server 2008)
- Serveur d'espaces de noms : srv-fichiers1
- Dossier racine partagé : Ne pas créer de dossier partagé.

< Précédent Créer Annuler

Nous allons ajouter la cible du srv-fichiers2 sur le dossier “Communservice”



Ajouter un serveur d'espaces de noms [X]

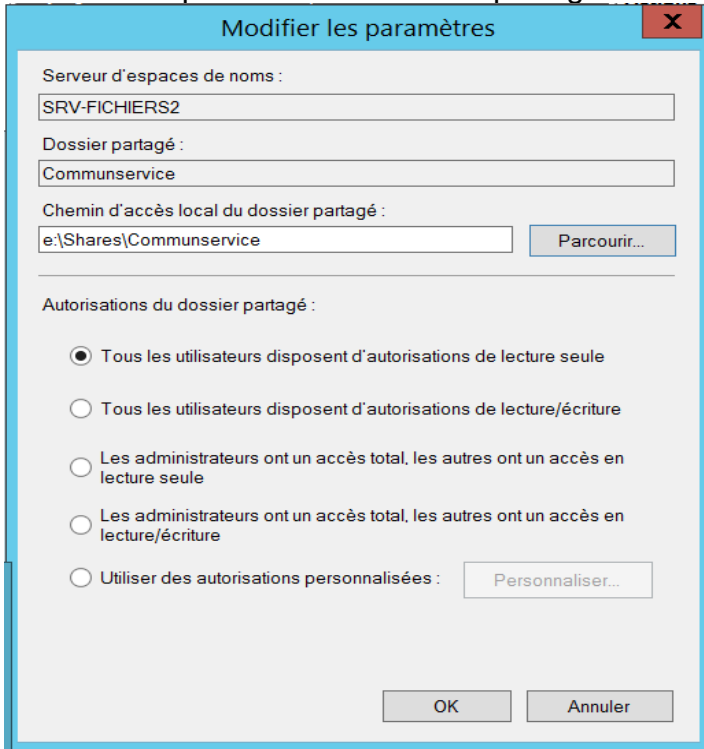
Espace de noms :

Serveur d'espaces de noms :

Chemin d'accès vers le dossier partagé :

Pour modifier les paramètres du dossier partagé, tels que son chemin d'accès local et les autorisations de dossier partagé, cliquez sur Modifier les paramètres.

Modifiez les paramètres du dossier partagé en indiquant la première option



Modifier les paramètres

Serveur d'espaces de noms :
SRV-FICHIERS2

Dossier partagé :
Communservice

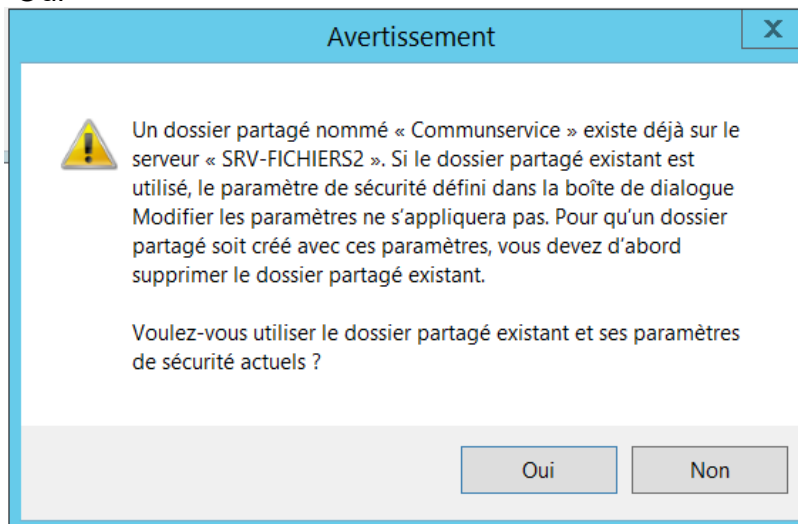
Chemin d'accès local du dossier partagé :
e:\Shares\Communservice Parcourir...

Autorisations du dossier partagé :


- ☒ Tous les utilisateurs disposent d'autorisations de lecture seule
- ☐ Tous les utilisateurs disposent d'autorisations de lecture/écriture
- ☐ Les administrateurs ont un accès total, les autres ont un accès en lecture seule
- ☐ Les administrateurs ont un accès total, les autres ont un accès en lecture/écriture
- ☐ Utiliser des autorisations personnalisées : Personnaliser...

OK Annuler

“Oui”



Avertissement

 Un dossier partagé nommé « Communservice » existe déjà sur le serveur « SRV-FICHIERS2 ». Si le dossier partagé existant est utilisé, le paramètre de sécurité défini dans la boîte de dialogue Modifier les paramètres ne s'appliquera pas. Pour qu'un dossier partagé soit créé avec ces paramètres, vous devez d'abord supprimer le dossier partagé existant.

Voulez-vous utiliser le dossier partagé existant et ses paramètres de sécurité actuels ?

Oui Non

Création du groupe de réplication

The screenshot shows the 'Assistant Nouveau groupe de réplication' window. The title bar is blue with standard window controls. The main area is titled 'Type de groupe de réplication'. On the left, a list of steps is shown, with 'Type de groupe de réplication' selected. The main content area contains two radio button options. The first option, 'Groupe de réplication multi-usage', is selected. Below it, a description states: 'Cette option configure la réplication entre deux serveurs ou plus pour la publication, le partage de contenu et d'autres scénarios.' The second option, 'Groupe de réplication pour la collecte de données', is unselected. Below it, a description states: 'Cette option configure une réplication bidirectionnelle entre deux serveurs, comme un serveur de succursale et un serveur concentrateur (destination). Cela vous permet de collecter les données sur le serveur concentrateur. Vous pouvez ensuite utiliser un logiciel de sauvegarde pour sauvegarder les données sur le serveur concentrateur.' At the bottom right, there are three buttons: '< Précédent', 'Suivant >', and 'Annuler'.

Assistant Nouveau groupe de réplication

Type de groupe de réplication

Étapes :

- Type de groupe de réplication
- Nom et domaine
- Membres du groupe de réplication
- Sélection de topologie
- Membres concentrateurs
- Connexions Hub and Spoke
- Planification du groupe de réplication et bande passante
- Membre principal
- Dossiers à répliquer
- Vérifier les paramètres et créer le groupe de réplication
- Confirmation

Sélectionnez le type de groupe de réplication à créer.

☒ Groupe de réplication multi-usage

Cette option configure la réplication entre deux serveurs ou plus pour la publication, le partage de contenu et d'autres scénarios.

☐ Groupe de réplication pour la collecte de données

Cette option configure une réplication bidirectionnelle entre deux serveurs, comme un serveur de succursale et un serveur concentrateur (destination). Cela vous permet de collecter les données sur le serveur concentrateur. Vous pouvez ensuite utiliser un logiciel de sauvegarde pour sauvegarder les données sur le serveur concentrateur.

< Précédent Suivant > Annuler

Nommez le groupe de réplication

The screenshot shows the 'Assistant Nouveau groupe de réplication' window, Step 2: 'Nom et domaine'. The title bar is blue. The main area is titled 'Nom et domaine'. On the left, the list of steps shows 'Nom et domaine' as the current step. The main content area contains instructions: 'Entrez un nom et un domaine pour le groupe de réplication. Le nom du groupe de réplication doit être unique dans le domaine qui héberge le groupe de réplication.' Below this, there are three input fields. The first is 'Nom du groupe de réplication :', which contains the text 'Communservice'. The second is 'Description facultative du groupe de réplication :', which is empty. The third is 'Domaine :', which contains the text 'pixy.lan'. To the right of the 'Domaine' field is a button labeled 'Parcourir...'. At the bottom right, there are three buttons: '< Précédent', 'Suivant >', and 'Annuler'.

Assistant Nouveau groupe de réplication

Nom et domaine

Étapes :

- Type de groupe de réplication
- Nom et domaine
- Membres du groupe de réplication
- Sélection de topologie
- Membres concentrateurs
- Connexions Hub and Spoke
- Planification du groupe de réplication et bande passante
- Membre principal
- Dossiers à répliquer
- Vérifier les paramètres et créer le groupe de réplication
- Confirmation

Entrez un nom et un domaine pour le groupe de réplication. Le nom du groupe de réplication doit être unique dans le domaine qui héberge le groupe de réplication.

Nom du groupe de réplication :

Communservice

Description facultative du groupe de réplication :

Domaine :

pixy.lan Parcourir...

< Précédent Suivant > Annuler

Ajoutez SRV-FICHIERS1 et SRV-FICHIERS2

Assistant Nouveau groupe de réplication

Membres du groupe de réplication

Étapes :

- Type de groupe de réplication
- Nom et domaine
- Membres du groupe de réplication
- Sélection de topologie
- Membres concentrateurs
- Connexions Hub and Spoke
- Planification du groupe de réplication et bande passante
- Membre principal
- Dossiers à répliquer
- Vérifier les paramètres et créer le groupe de réplication
- Confirmation

Cliquez sur Ajouter, puis sélectionnez deux serveurs ou plus qui deviendront membres du groupe de réplication.

Membres :

Serveur	Domaine
SRV-FICHIERS1	pixy.lan
SRV-FICHIERS2	pixy.lan

Ajouter... Supprimer

< Précédent Suivant > Annuler

Assistant Nouveau groupe de réplication

Sélection de topologie

Étapes :

- Type de groupe de réplication
- Nom et domaine
- Membres du groupe de réplication
- Sélection de topologie
- Planification du groupe de réplication et bande passante
- Membre principal
- Dossiers à répliquer
- Vérifier les paramètres et créer le groupe de réplication
- Confirmation

Sélectionnez une topologie de connexions parmi les membres du groupe de réplication.

☐ Hub et Spoke

Cette topologie requiert au moins 3 membres dans le groupe de réplication. Les membres spoke sont connectés à un ou deux hubs. Cette topologie est adaptée aux scénarios de publication où les données proviennent du membre hub et se répliquent sur les membres spoke.

☒ Maille pleine

Dans cette topologie, chaque membre est répliqué avec tous les autres membres du groupe de réplication. Cette topologie est surtout adaptée lorsqu'il existe au plus dix membres dans le groupe de réplication.

☐ Aucune topologie

Sélectionnez cette option si vous souhaitez créer une topologie personnalisée une fois l'Assistant terminé. Aucune réplication ne peut s'effectuer tant que vous n'avez pas créé la topologie personnalisée.

< Précédent Suivant > Annuler

Indiquez le chemin local du dossier répliqué

Assistant Nouveau groupe de réplication

Dossiers à répliquer

Étapes :

- Type de groupe de réplication
- Nom et domaine
- Membres du groupe de réplication
- Sélection de topologie
- Planification du groupe de réplication et bande passante
- Membre principal
- Dossiers à répliquer**
- Chemin d'accès local de Communservice sur les autres membres
- Vérifier les paramètres et créer le groupe de réplication
- Confirmation

Cliquez sur Ajouter pour sélectionner un dossier du membre principal que vous souhaitez répliquer sur les autres membres du groupe de réplication.

Dossiers répliqués :

Chemin d'accès local	Nom du dossier répliqué	Autorisations NTFS
E:\Shares\Communservice	Communservice	Utiliser les autoris...

Ajouter... Modifier... Supprimer

Activer Windows

< Précédent Suivant > Annuler

Indiquez le serveur sur lequel répliquer

Modifier

Général

Membre :
SRV-FICHIERS2

Sélectionnez l'état initial du dossier répliqué sur ce membre.

Statut de l'appartenance :

☐ Désactivé
Le dossier répliqué ne sera pas stocké sur ce membre.

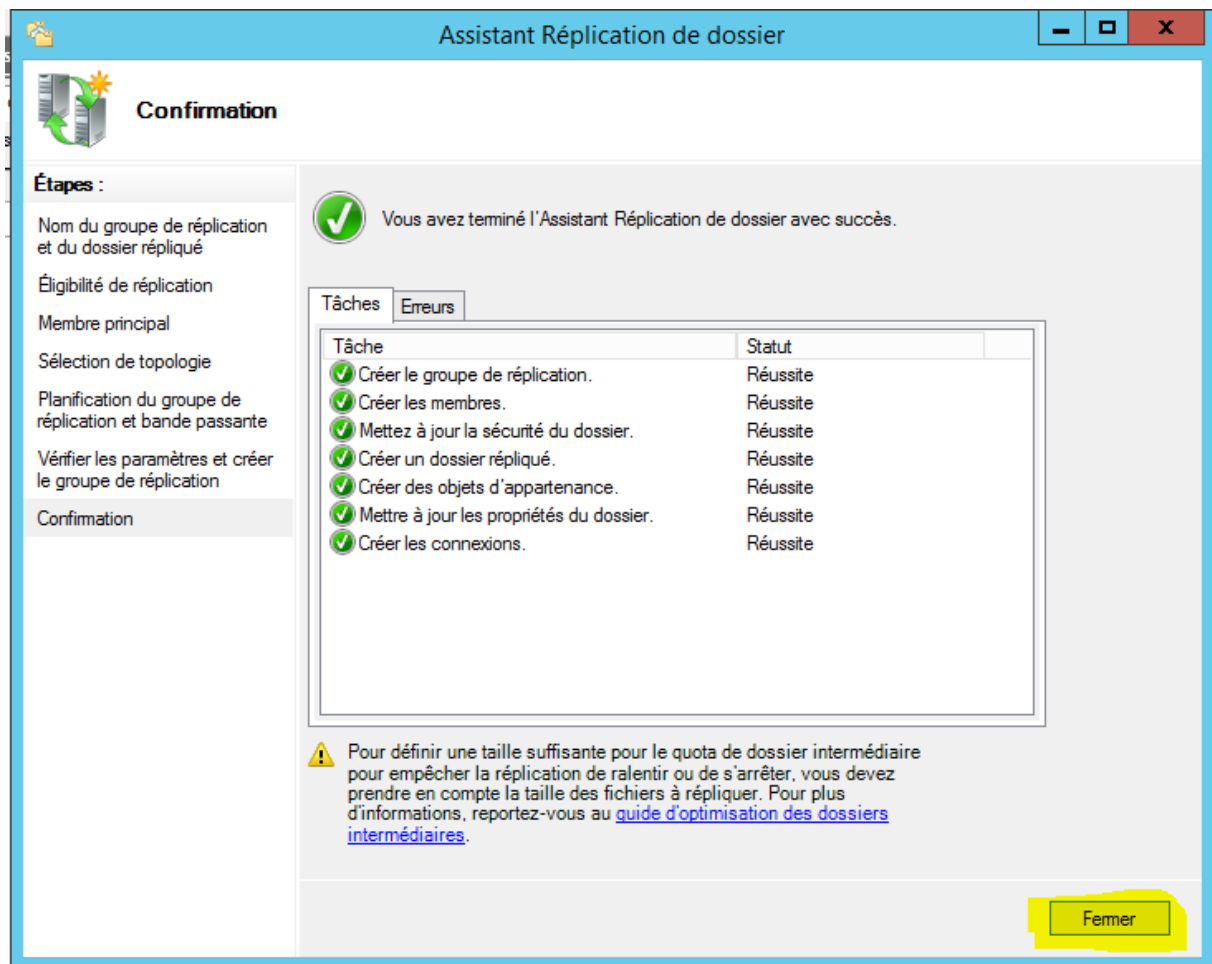
☒ Actif
Garder le dossier suivant synchronisé avec les autres membres.

Chemin d'accès local du dossier :
E:\Shares\Communservice Parcourir...

Exemple : C:\Données

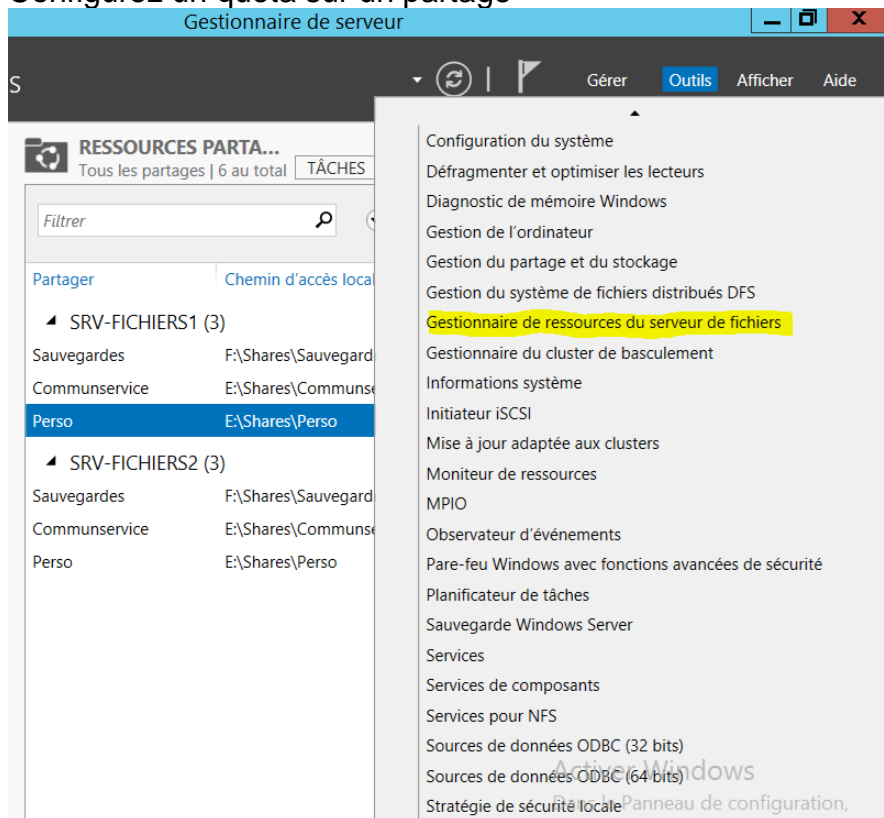
☐ Placez en lecture seule le dossier répliqué sélectionné sur ce membre.

OK Annuler

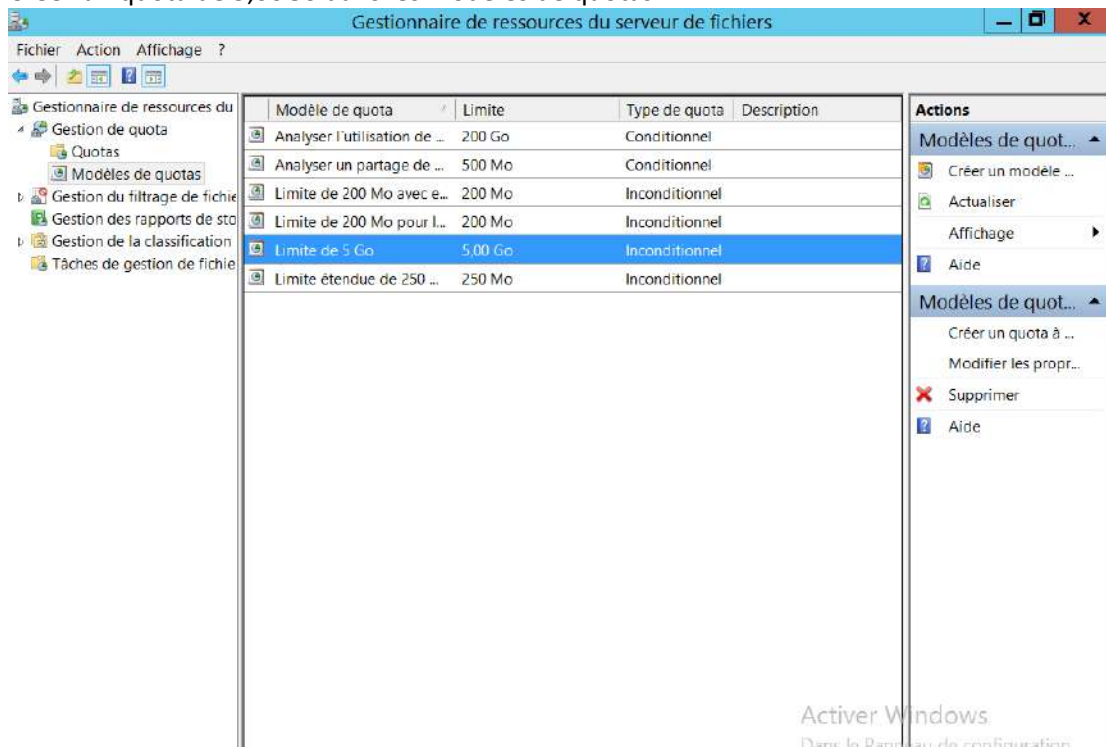


Faire de même pour le partage "Perso" et le "Sauvegardes"

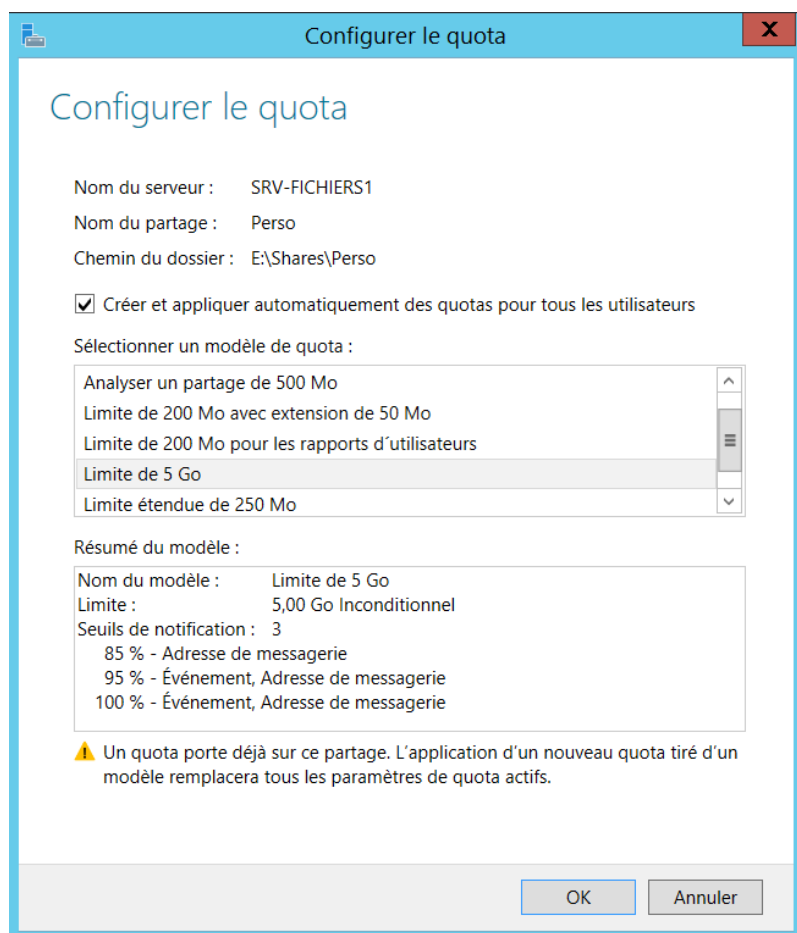
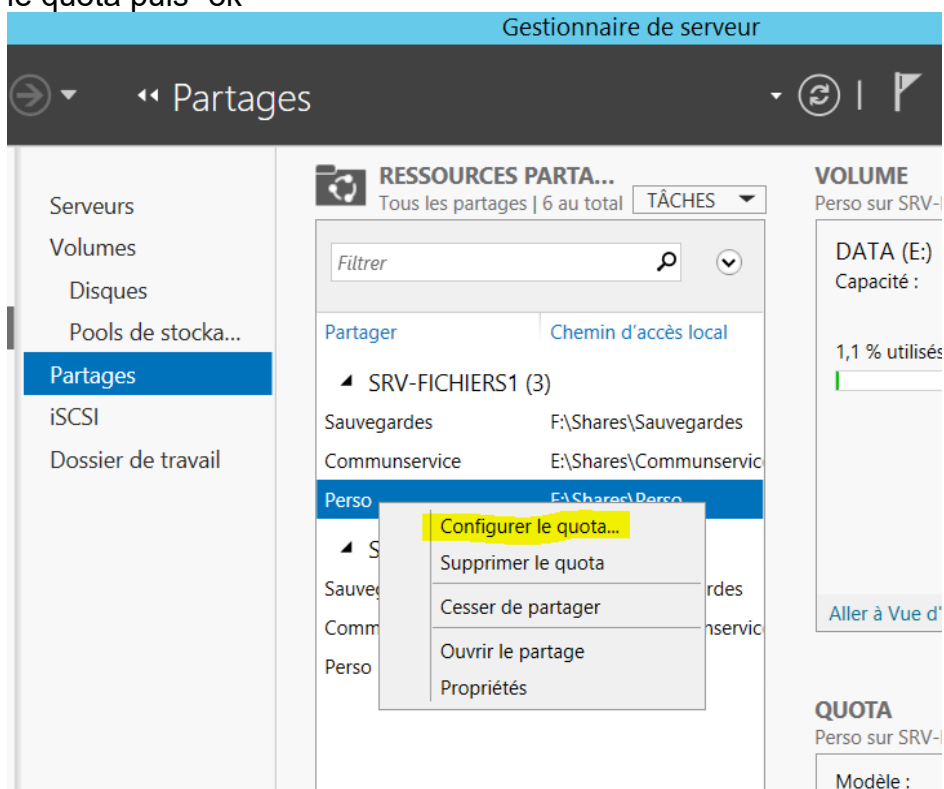
Configurez un quota sur un partage



Créez un quota de 5,00Go dans les modèles de quotas



Appliquez le quota aux dossiers perso des utilisateurs en cliquant sur “configurer le quota puis “ok”



SCRIPT Création des OU, Groupes et Users

```

1  $Schemin="DC=PIXY,DC=LAN"
2  $utils=import-csv -path "C:\Users\Administrateur\Documents\utilisateurs.csv" -Delimiter ";" -Encoding UTF8
3
4  $dossierperso="\pixy.tan\stockage\communservice\service"
5  $dossierperso="\pixy.tan\stockage\perso\"
6
7  ##### INDIV #####
8
9  function creation_ou()
10 {
11     $nomou-read-host "saisir un nom d'ou?"
12     New-ADOrganizationalUnit -Name $nomou -Path $Schemin -
13     -ProtectedFromAccidentalDeletion $false
14     Write-Host "OU $nomou a été créée"
15 }
16
17 function suppression_ou()
18 {
19     $identity="OU=$nomou", "$Schemin"
20     Remove-ADOrganizationalUnit -Identity $identity
21     Write-Host "OU $nomou a été supprimée"
22 }
23
24 function affichage_ou()
25 {
26     $listeou=get-ADOrganizationalUnit -Filter * -SearchBase $Schemin -SearchScope OneLevel
27     Write-Host "Listes des ou's 1er niveau"
28     foreach ($i in $listeou)
29     {
30         Write-Host $i.name
31     }
32     $choix2-read-host "Retour Menu? ( 1 pour OUI ou 2 pour NON ) : "
33     if ($choix2 -eq 1)
34     {
35         menu1
36     }
37     else {
38         exit
39     }
40 }
41
42 function creation_user()
43 {
44     $oubase-read-host "Ou de base ?"
45     $Scheminbase="OU=$oubase,DC=PIXY,DC=LAN"
46     $nom-read-host "Nom utilisateur ?"
47     $prenom-read-host "Prénom utilisateur ?"
48     $noncomplet=$prenom+"-$nom"
49     $login=$prenom.Tolower()+"$nom.Tolower()"
50     $supn=("$login"+"$serv:USER@DOMAIN").Tolower()
51     $titre-read-host "Fonction ?"
52     $service-read-host "Service ?"
53     $Scheminuser="OU=$service", $Scheminbase
54     $groupe="GC=$service"
55     $pass-ConvertTo-SecureString("BlancheFort1") -AsPlainText -Force
56
57     New-ADUser -Name $noncomplet -DisplayName $noncomplet -GivenName $prenom -Surname $nom -sAMAccountName $login -userPrincipalName $supn -Title $titre -Department $service -Path $Scheminuser -ChangePasswordAtLogon $true -Enabled $true
58     Add-ADGroupMember $groupe -Members $login
59     Write-Host $noncomplet a bien été créé
60 }

```

Activer Windows

Dans le Panneau de configuration: ouvrir Système pour

```

32
33
34
35
36
37
38
39
40
41
42 DC=LAN"
43
44
45 IF ?"
46 $Lower()
47 .Tolower()
48
49
50
51 $inbase
52
53 $efort1") -AsPlainText -Force
54 $yName $noncomplet -GivenName $prenom -Surname $nom -sAMAccountName $login -userPrincipalName $supn -Title $titre -Department $service -Path $Scheminuser -ChangePasswordAtLogon $true -Enabled $true -AccountPassword $pass -EmailAddress $supn
55
56 $login
57
58
59

```

Activer Windows

```

58     write-Host $noncomplet a bien été créé
59 }
60 }
61 }
62 ##### LOTS #####
63 function creation_ou_lot()
64 {
65     $oubase=Read-Host "Créez votre OU de base ?"
66     New-ADOrganizationalUnit -name $oubase -path $chemin -ProtectedFromAccidentalDeletion $false
67     $cheminbase="OU="+$oubase+",DC=PIXY,DC=LAN"
68     New-ADOrganizationalUnit -name GROUPES -path $cheminbase -ProtectedFromAccidentalDeletion $false
69     foreach ($i in $utils)
70     {
71         $ou=$i.service
72         try {
73             New-ADOrganizationalUnit -name $ou -path $cheminbase
74             -ProtectedFromAccidentalDeletion $false
75         }
76         catch {}
77     }
78     creation_groupes($chemin, $cheminbase)
79     return $cheminbase
80 }
81 function creation_groupes()
82 {
83     foreach ($i in $utils)
84     {
85         $sgg="GG_"+$i.service
86         $sgdlr="GDL_"+$i.service+"_R"
87         $sgdlrw="GDL_"+$i.service+"_RW"
88         $sgdlf="GDL_"+$i.service+"_F"
89         $chemingroupe="OU=GROUPES,"+$cheminbase
90         try {
91             New-ADGroup -Name $sgg -GroupCategory Security -GroupScope Global -Path $chemingroupe
92             New-ADGroup -Name $sgdlr -GroupCategory Security -GroupScope DomainLocal -Path $chemingroupe
93             New-ADGroup -Name $sgdlrw -GroupCategory Security -GroupScope DomainLocal -Path $chemingroupe
94             New-ADGroup -Name $sgdlf -GroupCategory Security -GroupScope DomainLocal -Path $chemingroupe
95         }
96         catch {}
97         Add-ADGroupMember $sgdlr -Members $sgg
98         Add-ADGroupMember $sgdlrw -Members $sgg
99         Add-ADGroupMember $sgdlf -Members $sgg
100     }
101 }
102 }
103 }
104 }
105 }
106 }
107 }
108 }
109 }

```

```

1 function creation_users()
2 {
3     $oubase=Read-Host "OU BASE?"
4     $cheminbase="OU="+$oubase+",DC=PIXY,DC=LAN"
5     $pass=ConvertTo-SecureString("Blanquefort!") -AsPlainText -Force
6     foreach ($i in $utils)
7     {
8         $non-($i.non).toupper()
9         $prenon=$i.prenom.substring(0,1).toupper()+$i.prenom.substring(1).tolower()
10        $noncomplet=$prenon+" "+$non
11        $login=$prenon.tolower()+"."+$non.tolower()
12        $supn-($login+"@-serv:USER@DOMAIN").tolower()
13        $titre=$i.fonction
14        $service=$i.service
15        $cheminuser="OU="+$service+","+$cheminbase
16        $groupe="GG_"+$service
17        $description=$i.description
18        $cheminlecteur-("\\pixy.lan\stockage\perso\"+$login)
19        creation_dossiers($login,$service)
20        New-ADUser -Name $noncomplet -DisplayName $noncomplet -GivenName $prenon -Surname $non -sanAccountName $login -userprincipalName $supn -Title $titre -Department $service -Path $cheminuser -ChangePasswordAtLogon $true -Enabled $true -
21        Add-ADGroupMember $groupe -Members $login
22    }
23 }
24 function creation_dossiers()
25 {
26     try {
27         $dossierperso-("\\pixy.lan\stockage\communservice\service\")
28         $dossierperso-("\\pixy.lan\stockage\perso\")
29         New-Item -ItemType Directory -path $dossierperso -Name $service -Force
30         New-Item -ItemType Directory -path $dossierperso -name $login -Force
31     }
32     catch {}
33 }
34 }
35 }
36 }

```

-userprincipalName \$supn -Title \$titre -Department \$service -Path \$cheminuser -ChangePasswordAtLogon \$true -Enabled \$true -AccountPassword \$pass -EmailAddress \$supn -Description \$description -HomeDrive "P:" -HomeDirectory \$cheminlecteur


```

function ac1()
{
    $l1stedossier=Get-Childitem $dossier -Directory
    $l1stedossierperso=Get-Childitem $dossierperso -Directory
    Get-Acl -Path \\pixy.lan\stockage\Communserv\service | Set-Acl -Path \\pixy.lan\stockage\Communserv\service
    Get-Acl -Path \\pixy.lan\stockage\perso | Set-Acl -Path \\pixy.lan\stockage\perso
    foreach ($dossier in $l1stedossier)
    {
        $chemindossier=$dossier.FullName
        $acl=(Get-Item $chemindossier).GetAccessControl('Access')
        $gd1="GD1_" + $dossier.Name + "_Rn"
        Write-Host $gd1
        $sar=New-Object System.Security.AccessControl.FileSystemAccessRule($gd1, 'Modify', 'ContainerInherit, ObjectInherit', 'none', 'Allow')
        $acl.SetAccessRule($sar)
        Set-Acl -Path $chemindossier -AclObject $acl
    }

    foreach ($dossier in $l1stedossierperso)
    {
        $chemindossier=$dossier.FullName
        $acl=(Get-Item $chemindossier).GetAccessControl('Access')
        $user=$dossier.Name
        $sar=New-Object System.Security.AccessControl.FileSystemAccessRule($user, 'Modify', 'ContainerInherit, ObjectInherit', 'none', 'Allow')
        $acl.SetAccessRule($sar)
        Set-Acl -Path $chemindossier -AclObject $acl
    }
}

function suppression_totale()
{
    $oubase=Read-Host "OU BASE?"
    $cheminbase="OU="+$oubase+",DC=PIXY,DC=LAN"

    Set-ADOrganizationalUnit -Identity $cheminbase -ProtectedFromAccidentalDeletion $false
    Remove-ADOrganizationalUnit -Identity $cheminbase -Recursive -Confirm:$false

    $dossierperso="\\*\$env:USERDNSDOMAIN\stockage\services\*service\*"
    $dossierperso="\\*\$env:USERDNSDOMAIN\stockage\perso\*"
    Remove-Item $dossierperso -Recurse
    Remove-Item $dossierperso -Recurse
}

##### MENUS #####
function menu_general()
{
    cls
    write-host "*****"
    write-host "CHOIX MENU 1 ( création individuelle)?"
    write-host "CHOIX MENU 2 (création par lots)?"
    write-host "CHOIX 0 QUITTER LE SCRIPT"
    $choix=read-host "votre choix?"
    switch ($choix)
    {
        1 {menu1}
        2 {menu2}
        0 {exit}
        default {menu}
    }
}

function menu1()
{
    cls
    write-host "*****MENU 1 INDIVIDUEL *****"
    write-host "choix 1 : Création d'ou"
    write-host "choix 2 : Suppression d'ou"
    write-host "choix 3 : Affichage des OU de base"
    write-host "choix 4 : Création d'un user"
    write-host "choix 9 : Retour Menu Général"
    write-host "choix 0 : Quitter le script"
    $choix=read-host "votre choix ?"

    switch ($choix)
    {
        1 {creation_ou($chemin); menu1}
        2 {suppression_ou($chemin); menu1}
        3 {affichage_ou($chemin)}
        4 {creation_user($chemin, $cheminbase); menu1}
        9 {menu_general}
        0 {exit}
        default {menu1}
    }
}

```

```
249
250 function menu2()
251 {
252
253     write-host "*****MENU 2 PAR LOTS *****"
254     write-host "choix 1 : Création d'ou et des Groupes"
255     write-host "choix 2 : Création des Users"
256     write-host "choix 3 : permission NTFS sur dossier"
257     write-host "choix 4 : Suppression totale"
258     write-host "choix 9 : Retour Menu Général"
259     write-host "choix 0 : Quitter le script"
260     $choix=read-host "Votre choix ?"
261
262
263     switch ($choix)
264     {
265         1 {creation_ou_lot($chemin); menu2}
266         2 {creation_users($chemin); menu2}
267         3 {acl($dossierperso,$dossiersevice); menu2}
268         4 {suppresion_totale($chemin); menu2}
269         9 {menu_general}
270         0 {exit}
271         default {menu2}
272     }
273 }
274
275 menu_general
276
277
```

Glossaire

Active Directory : Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP 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, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs

Boot : Le boot (ou bootstrap), l'amorce, ou encore l'amorçage, est la procédure de démarrage d'un ordinateur, qui comporte notamment le chargement du programme initial.

Debian : C'est une organisation communautaire et démocratique, dont le but est le développement d'un système d'exploitation basé exclusivement sur des logiciels libres. On l'assimile généralement à sa version Debian GNU/Linux

DHCP : Dynamic Host Configuration Protocol (DHCP) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut

DNS : Le Domain Name System (ou DNS, système de noms de domaine) est un service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom.

FTP : File Transfer Protocol (protocole de transfert de fichiers), ou FTP, est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers.

GPO : Les stratégies de groupe (ou GP pour group Policy) sont des fonctions de gestion centralisée de la famille Microsoft Windows. Elles permettent la gestion des ordinateurs et des utilisateurs dans un environnement Active Directory. Les stratégies de groupe font partie de la famille des technologies IntelliMirror, qui incluent la gestion des ordinateurs déconnectés, la gestion des utilisateurs itinérants ou la gestion de la redirection des dossiers ainsi que la gestion des fichiers en mode déconnecté. Les stratégies de groupe sont gérées à travers des objets de stratégie de groupe communément appelés GPO (Group Policy Objects).

iSCSI : iSCSI est une abréviation de Internet Small Computer System Interface. C'est un protocole de stockage en réseau basé sur le protocole IP destiné à relier les installations de stockage de données.

ISO : Pour un disque, le logiciel de création d'image prendra une copie conforme («photo») du disque, et le réécrit sous la forme d'un code (qui peut être compressé) contenant tous les fichiers, la liste de ces fichiers, et la façon dont le disque a été gravé. L'ISO est le format le plus répandu, c'est la norme internationale ISO 9660.

MySQL : C'est un système de gestion de base de données (SGBD) Selon le type d'application, sa licence est libre ou propriétaire. Il fait partie des logiciels de gestion de base de données les plus utilisés au monde, autant par le grand public (applications web) que par des professionnel.

NFS : Network File System (ou NFS, système de fichiers en réseau) est à l'origine un protocole développé par Sun Microsystems en 19842 qui permet à un ordinateur d'accéder à des fichiers via un réseau. Il fait partie de la couche application du modèle OSI et utilise le protocole RPC.

Onduleur : Un onduleur est un dispositif d'électronique de puissance permettant de délivrer des tensions et des courants alternatifs à partir d'une source d'énergie électrique délivrant un courant continu. C'est la fonction inverse d'un redresseur. L'onduleur est un convertisseur statique de type continu/alternatif.

PHP : Un langage de scripts libre principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP, mais pouvant également fonctionner comme n'importe quel langage interprété de façon locale, en exécutant les programmes en ligne de commande.

Devis

Serveur hyperviseur

Dell PowerEdge R620.

Processeur : double Xeon E5-2667v2 3.30GHz 8 coeurs.

Mémoire : 4x 8Go 1866MHz.

RAID1 PERC H310 de 2 disques durs 900Go en SAS 10k 2.5" pour le système.

Alimentation redondé de 750W.

Carte iDRAC7.

Cartes réseaux : double cartes de 2 port Ethernet chacune.

Garantie 5 ans sur le site.

Serveur NAS

Dell PowerVault NX3200.

Processeur : Xeon E5-2609 2.40GHz 4 coeurs.

Mémoire : 2x 8Go 1600MHz.

RAID1 PERC H710 de 2 disques durs 300Go en SAS 10k 3.5" pour le système.

RAID6 PERC H710 de 9 disques durs 600Go en SAS 15k 3.5" pour les données (4.2To utile).

Alimentation redondé de 750W.

Cartes réseaux : double cartes de 2 port Ethernet chacune.

Garantie 5 ans sur le site.

Disques durs de spare

2x Disques durs 600Go SAS 15k 3.5" 308.29€
2x Disques durs 300Go SAS 10k 3.5" 158.29€
3x Disques durs 900Go SAS 10k 2.5" 541.63€

Total Security 2017

Kaspersky Total Security 2017 version Entreprise 13 propose des antivirus innovants pour entreprises.

Ce logiciel est un antivirus puissant et discret, efficace contre les virus, les vers, les rootkits, les logiciels espions, les composeurs et les chevaux de Troie.

Kaspersky Total Security for Business, notre solution de sécurité pour entreprises la plus complète, offre une protection efficace de votre réseau informatique. Outre la sécurité des ordinateurs de bureau, ordinateurs portables, serveurs de fichiers, avec des outils de chiffrement des données, de contrôle des terminaux et de sécurité mobile, elle protège les serveurs de messagerie, les serveurs collaboratifs et le trafic circulant à travers les passerelles Web. De plus, des outils étendus de gestion des systèmes automatisent un large éventail de tâches d'administration afin de vous faire gagner du temps et des ressources.

- Protection multi niveaux qui s'appuie sur une combinaison unique de big data et de surveillance des menaces, de Machine Learning et d'expertise humaine.
- La gestion granulaire de la sécurité facilite l'administration et le contrôle de l'ensemble des problèmes de sécurité, sans nécessité d'installer de solutions d'intégration et de gestion supplémentaires.
- Efficacité renforcée de l'entreprise grâce à la sécurisation des communications et de la collaboration.
- Sécurité et gestion des appareils mobiles plus efficaces pour protéger les données, quel que soit l'endroit où vous vous trouvez.
- La meilleure protection possible pour vos clients, comme des tests indépendants l'ont confirmé. Kaspersky Lab propose la protection la plus récompensée et la plus testée au monde, alliée aux taux de détection les plus élevés du secteur.

Inventaire logiciel et matériel du parc

Présentation détaillées des ordinateurs présents dans l'entreprise

Assistance technique: Chez G Data, développement et assistance sont deux notions indissociables, pour un meilleur support technique.

Extincteur

Extincteur à eau certifié Bureau Veritas pour les feux de liquides, de solides, de liquides de cuisson et les feux d'origine électriques. Extincteur avec additif AFFF. Garantie 1 an.

Onduleur

- Rendement exceptionnel, convivialité et mesure de la consommation.
- Convivialité
- Performance et Rendement
- Disponibilité et souplesse
- Le nouvel écran graphique LCD donne des informations claires sur l'état et les mesures de l'onduleur (en 7 langues). Fonctions évoluées de paramétrage disponibles grâce aux touches de navigation.
- Première dans l'industrie : le 5PX mesure la consommation énergétique jusqu'au niveau des groupes de prises. Ces valeurs (kWh) peuvent être gérées par l'écran LCD ou la suite logicielle Intelligent Power® Software d'Eaton.
- La segmentation de charge permet, lors d'une coupure prolongée du réseau, de couper les équipements les moins nécessaires pour réserver l'autonomie de la batterie aux équipements essentiels. Cette fonction est également, utilisée pour le reboot distant et le démarrage séquentiel des serveurs.
- Le 5PX possède des ports de communications Série (RS232) et USB, ainsi qu'un emplacement libre pour une carte optionnelle (carte réseau SNMP/Web ou carte contacts secs). La suite logicielle Intelligent Power® d'Eaton est compatible avec tous les principaux systèmes d'exploitation, y compris les environnements virtualisés tels que VMware et Hyper-V.
- Jusqu'à 99% de rendement : moindres dissipation calorifique et consommation d'énergie.
- Plus de puissance réelle grâce à son facteur de puissance de 0,9 en sortie. Le 5PX est compatible avec tous les équipements informatiques modernes.
- Lorsqu'il fonctionne sur batteries, le 5PX fournit un signal sinusoïdal d'une grande qualité, idéal pour l'alimentation des équipements sensibles, tels que les serveurs à PFC actif (facteur de puissance corrigé).
- Le 5PX est un système convertible rack/tour - pieds et glissières sont inclus pour tous les modèles sans coût additionnel.
- Prolonger la durée de vie de la batterie : la batterie est gérée par la technologie ABM® de Eaton qui ne recharge la batterie que si nécessaire, évitant ainsi sa corrosion et prolongeant considérablement sa durée de service.
- Les batteries sont remplaçables à chaud sans devoir couper les équipements connectés. Grâce à un module bypass de maintenance optionnel, vous pouvez même remplacer l'onduleur complet.
- Jusqu'à 4 coffrets batteries externes, remplaçables à chaud, peuvent porter son autonomie de quelques minutes à plusieurs heures. Ces coffrets batteries sont automatiquement détectés par l'onduleur.

Description du produit	Eaton 5PX 2200 Rack/Tower LCD - onduleur - 1980 Watt - 2200 VA
Type de périphérique	Onduleur - montable sur rack / externe
Dimension Rack	2U
Dimensions (LxPxH)	44.1 cm x 52.2 cm x 8.6 cm
Poids	28.5 kg
Tension d'entrée	CA 230 V
Tension de sortie	CA 200/208/220/230/240 V (50/60 Hz)
Capacité d'alimentation	1980 Watt / 2200 VA
Connecteur(s) de sortie	8 x alimentation IEC 320 EN 60320 C13 ? 1 x alimentation IEC 320 EN 60320 C19
Autonomie (jusqu'à)	3 min en pleine charge
Dimensions de la batterie	Module enfichable
Réseaux	RS-232, USB
Accessoires inclus	Pied tour
Garantie du fabricant	3 ans de garantie

Climatisation

Classe énergétique : A +
Puissance frigorifique : 2,6 W
Efficacité énergétique : EER pour le froid 3,1
Consommation d'énergie (Froid) 0,9 kWh
Fluide frigorigène : R410A
Niveau sonore : 64 dB
Programmable Jusqu'à 24h à l'avance
Type de commandes Electronique : LCD
Débit d'air : 413 m³/h
Fonctions Auto : Froid, Déshumidificateur, Ventilateur
Nombre de vitesses: 3
Ventilation seule : Oui
Accessoire(s) fourni(s) : Housse de protection
Hauteur : 76,4 cm
Largeur : 46,5 cm
Profondeur : 39,7 cm
Poids : 32 kg
Fonction chauffage : Non
Alimentation : 220-240 V
Prise : 10 A
Origine de fabrication : Corée
Programmable : Oui



Windows serveur

Nous avons choisi cette version : Windows server 2012 R2 standard.

Édition	Idéale pour...	Fonctionnalités	Mode de licence
 Windows Server 2012 Datacenter	Des environnements de Cloud hybride et à haute densité de virtualisation	Accès à toutes les fonctionnalités de Windows Server et à un droit de virtualisation illimitée	Par processeur + CAL
 Windows Server 2012 Standard	Des environnements à faible densité de virtualisation ou non virtualisés	Accès à toutes les fonctionnalités de Windows Server et à un droit pour deux machines virtuelles	Par processeur + CAL
 Windows Server 2012 Essentials	Les Petites et Moyennes Entreprises	Une interface plus simple, pas de droit pour virtualiser	Par serveur (limité à 25 utilisateurs) Pas de CAL
 Windows Server 2012 Foundation	Un premier serveur très abordable	Accès à toutes les fonctionnalités essentielles d'un premier serveur, pas de droit pour virtualiser	Par serveur (limité à 15 utilisateurs) Pas de CAL Disponible en OEM uniquement

Tableau récapitulatif des devis

Produit	Prix unitaire HT	Unité	Prix HT
Serveur hyperviseur	13 507,00 €	2	27 014,00 €
Serveur de fichier (NAS)	9 471,00 €	2	18 942,00 €
Spare 600Go SAS 15k 3.5"	308,29 €	2	616,58 €
Spare 6300Go SAS 10k 3.5"	158,29 €	2	316,58 €
Spare 900Go SAS 10k 2.5"	541,63 €	3	1 624,89 €
Licence antivirus	55 €	4	220 €
Licence Windows serveur	828 €	4	3 312 €
CAL Windows serveur	33,90 €	100	3 390,00 €
Extincteur	28,99 €	6	173,94 €
Climatisation mobile	599,00 €	3	1 797,00 €
Onduleur	745,31 €	6	4 471,86 €
Prix Total HT			61 877,99 €
Taxe			20,00%
Prix Total TTC			74 253,59 €

Charte graphique



Titre 1

Police : Arial
Taille de caractère : 18
Couleur : bleu
Gras
Italique
Sous-titré

Titre 2

Police : Arial
Taille de caractère : 16
Couleur : bleu clair
Gras
Italique

Titre 3

Police : Arial
Taille de caractère : 14
Couleur : bleu clair
Gras
Italique
Texte de base
Police : Arial
Taille de caractère : 12
Couleur : noir

Espace entre le titre et le texte : un retour à la ligne

Diagramme de Gantt

