PIELCO

FOOTWEAR COMPANY

Projet Evolution 2018
Charles GOUYETTE, Louis FRU, Antoine VERDIER

Sommaire

I. Présentation 1

A. Projet 1

B. Le cahier des charges 1

C. Organisation 1

II. Propositions 3

A. L'infrastructure : 4

1. Système 4
2. Matériel 4

B. Les serveurs 6

1. Adresses IP des machine 6
2. VMware ESXi 6
3. Windows Serveur 2016 15
4. Linux CentOS 68

C. Système de sauvegarde 79

1. Installation 80
2. Configuration 84

D. Licences 88

E. Conclusion 88

III. Annexes 89

A. Scripts 89

B. Devis 92

IV. Glossaire 93

I. Présentation

A. Projet

Nous sommes trois techniciens informatiques travaillants pour l'entreprise Pielco.

Cela fait désormais 6 mois que nous sommes au sein de cette société. Nous avons précédemment procédé à la conception et au renouvellement de l'infrastructure informatique qui comprend, le câblage, l'installation des postes informatique, des copieurs ainsi que toute l'infrastructure réseau. De plus nous avions déjà prévu les futurs serveurs, donc nous possédons déjà les armoires à serveur et les onduleurs.

Nous avons relevé avec notre DAF différents dysfonctionnements au sein du service informatique et des solutions doivent être apportées afin d'y remédier.

Ce document a pour but de détailler la solution retenue par notre équipe. Les mots en **gras*** seront présents dans le glossaire.

B. Le cahier des charges

Voici les recommandations du DAF qui souhaite des propositions concrètes sur les sujets suivants :

- L'équipe informatique court partout et se trompe souvent de lieu pour dépanner les utilisateurs. 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 à besoin d'un serveur **FTP*** pour y récupérer des fichiers ;

- Il faut implémenter un **Active Directory*** dans l'entreprise ;

- Il veut un compte rendu mensuel sur notre avancé ;

- 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.

C. Organisation

Pour mener à bien ce projet, nous nous sommes organisés en répartissant les tâches et en planifiant des rendez-vous avec notre DAF.

Avant tout, avons commencé par lister nos ressources puis à lister les travers à éviter :

Les ressources : Informations / connaissances :	Les ressources : organisation :	Les ressources : attitudes & comportement :
• Intervenants CESI • Cours • Projets précédents • Compétences individuelles / expériences ce chacun • Ressources de l'entreprise (tuteur, collègues…) • Echanges avec le DAF • Ressources externes (documentation, internet…)	• Planification • Utilisation des supports fournis (Office 365, etc.) • Préparation de l'oral • Organisation • Définition d'un chef d'équipe • Compréhension et application de nos objectifs • Répartition des tâches • Temps passé ensemble	• Tenue correcte • Relationnel de qualité (communication de groupe, partage des connaissances et compétences) • Travail • Rigueur (être ambitieux sans devenir perfectionniste – sans perdre de temps) • Assiduité • Savoir distinguer les éléments importants des détails

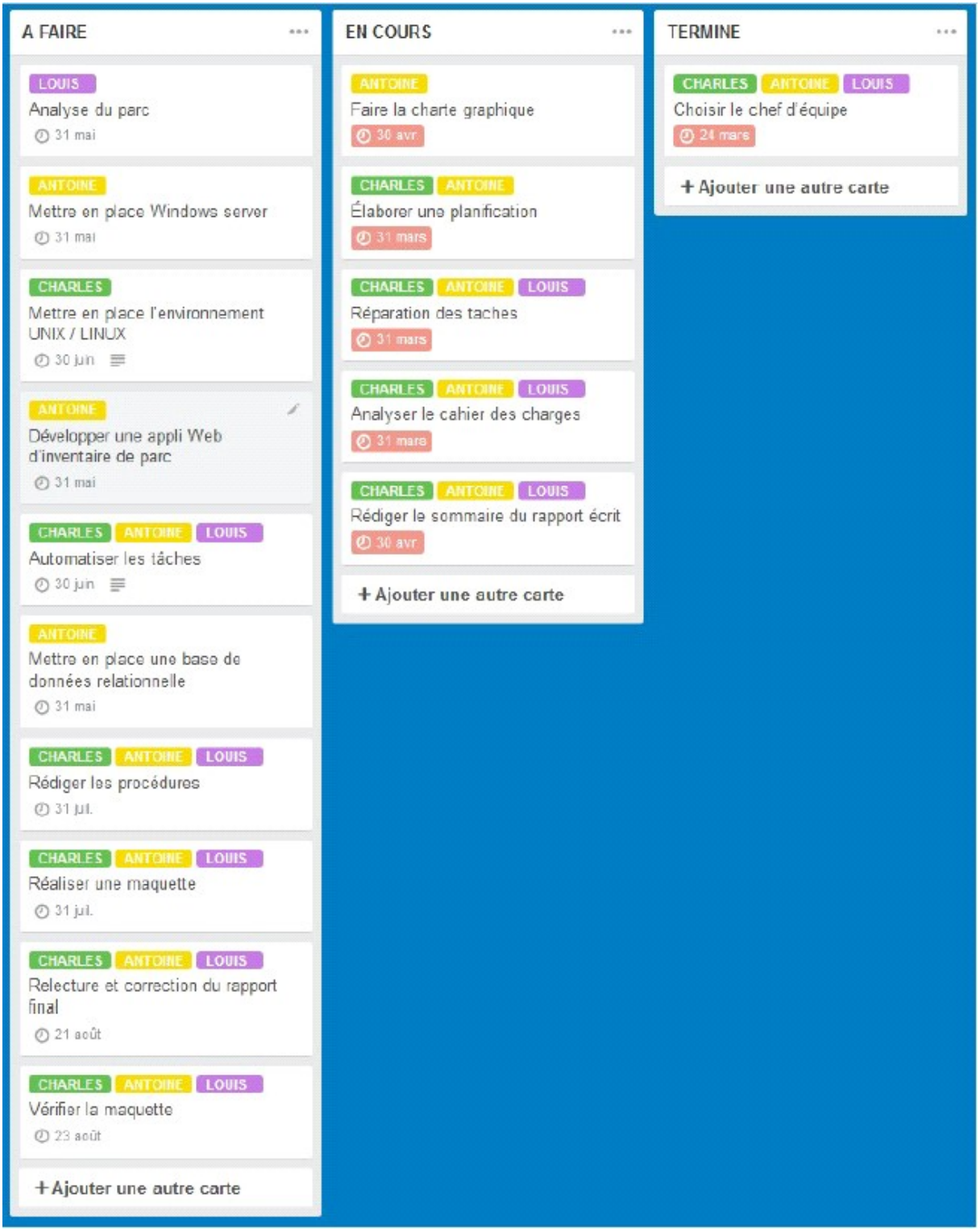
Les freins :	Les récifs :
• mauvaise organisation • manque de connaissances • manque de travail • mauvaise prise d'informations • intervenant CESI inefficace • mauvaise cohésion de groupe • mauvaise évaluation du temps • mauvaise répartition des tâches • mauvais chef d'équipe • non exploitation des ressources	• Problèmes matériels • absence d'un participant • absence de planification

Nous avons ensuite fais un planning mensuel de ce qui devait être fait :

Etapes & planification :

	Mars	Avril	Mai	Juin	Juillet	Aout
Livrables à rendre Echéances		CR mensuel	CR mensuel	CR mensuel	CR mensuel	CR mensuel 21 août : Restitution rapport écrit 23 août : Oral
Etapes / actions **(à développer et à affiner)** **+ rajouter la distribution des tâches : qui fait quoi ?**	Choisir le chef d'équipe Analyser le cahier des charges Répartir les tâches Elaborer une planification Choisir les outils collaboratifs	Faire la charte graphique Rédiger le sommaire du rapport écrit	Identifier les matériels à acheter Justifier les coûts Définir / recenser l'existant Mettre en place Windows server Développer une appli Web d'inventaire de parc Mettre en place une base de données relationnelle Poser les bonnes questions au DAF	Automatiser les tâches Mettre en place l'environnement UNIX / LINUX	Rédiger les procédures Réaliser une maquette	Relecture et correction du rapport final Vérifier la maquette Vérifier que le projet répond aux attentes du DAF Préparation d'un support visuel (convaincre l'auditoire) Faire le point final : transmission des connaissances entre les membres du groupe Entrainement à l'oral

Et pour finir, nous avons mis en place un planning nominatif avec qui doit faire quoi :



II. Propositions

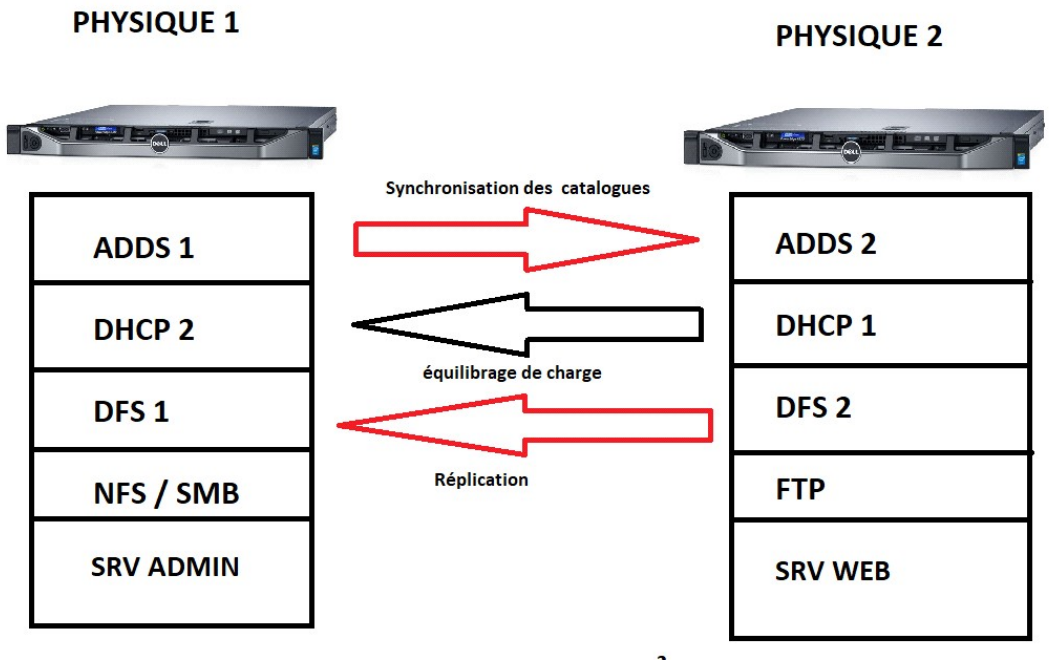
A. L'infrastructure :

1. Système

Afin de mener à bien de nouveau projet, nous proposons la mise en place de l'infrastructure système suivante :

5 Machines virtuelles sous Windows serveur 2016 :
- Deux **contrôleurs de domaine***
- Deux serveur de partage **DFS***
- Un Serveur d'administration + service d'impression

5 Machines sous Linux (CentOS)
- Deux serveur **DHCP***
- Un serveur **FTP***
- Un serveur WEB
- Un serveur NFS + SMB



2. Matériel

Le tout sera hébergé sur deux serveurs Dell Power Edge R330 équipés d'un processeur Xeon E3-1280V6 possédant 4 cœurs physiques ainsi que 64 Go de ram et 4 baies 3.5 pour le stockage. Nous avons choisi de mettre en place la fonctionnalité **Raid 5*** pour permettre de répartir les données sur tous les disques, d'améliorer les performances et de fournir une sécurité supplémentaire en cas de défaillance d'un disque.

La solution d'Hypervision retenue sera l'OS VMWare **ESXI***.

Figure 1 Power Edg R330

Notre outil de sauvegarde, Veeam, que nous verrons plus bas, sera hébergé sur un serveur Dell PowerEdge T130.

Figure 2 Dell PowerEdge t310

B. Les serveurs

1. Adresses IP des machine

Nos machines respectent un plan IP que nous avions préalablement défini, le voici :

IP MACHINES	
ADDS1	192.168.0.40
ADDS2	192.168.0.41
DHCP	192.168.0.42
DHCP2	192.168.0.43
FTP	192.168.0.44
WEB	192.168.0.45
DFS1	192.168.0.46
DFS2	192.168.0.47
NFS / SMB	192.168.0.48
SRV administration	192.168.0.49

2. VMware ESXi

Comment mentionné plus haut, toutes les machines virtuelles que nous proposons de mettre en place seront gérées via un ESX. Nous allons couvrir le rôle et l'installation de ce système d'exploitation. Il y aura deux ESX installés sur deux machines physiques différentes.

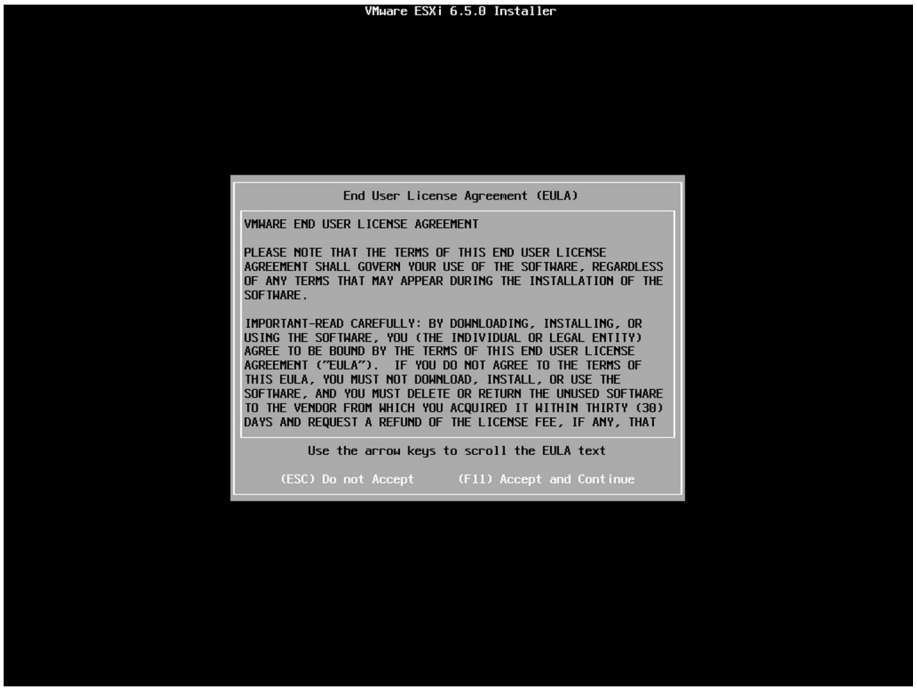
a) Rôle

Un ESX est outil qui permet la gestion précise d'un parc de machines virtuelles. Il s'agit d'un hyperviseur de type 1. Dans notre cas, il va nous permettre d'installer et de gérer des machines tournant avec Windows Serveur 2016 et CentOS.

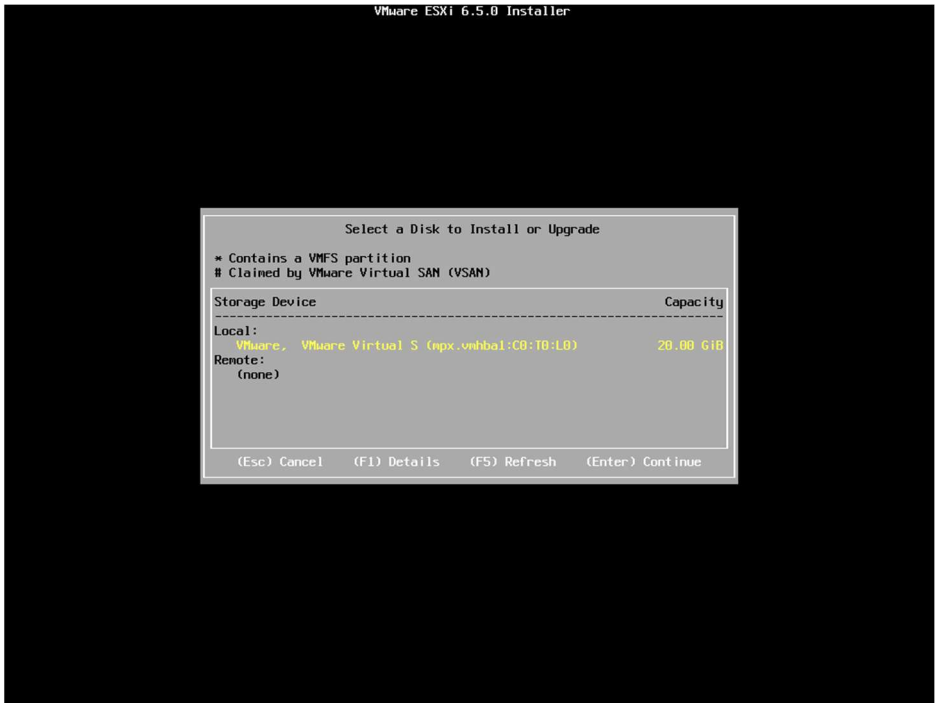
b) Installation

Voici les différentes étapes d'installation d'un ESX sur un serveur :

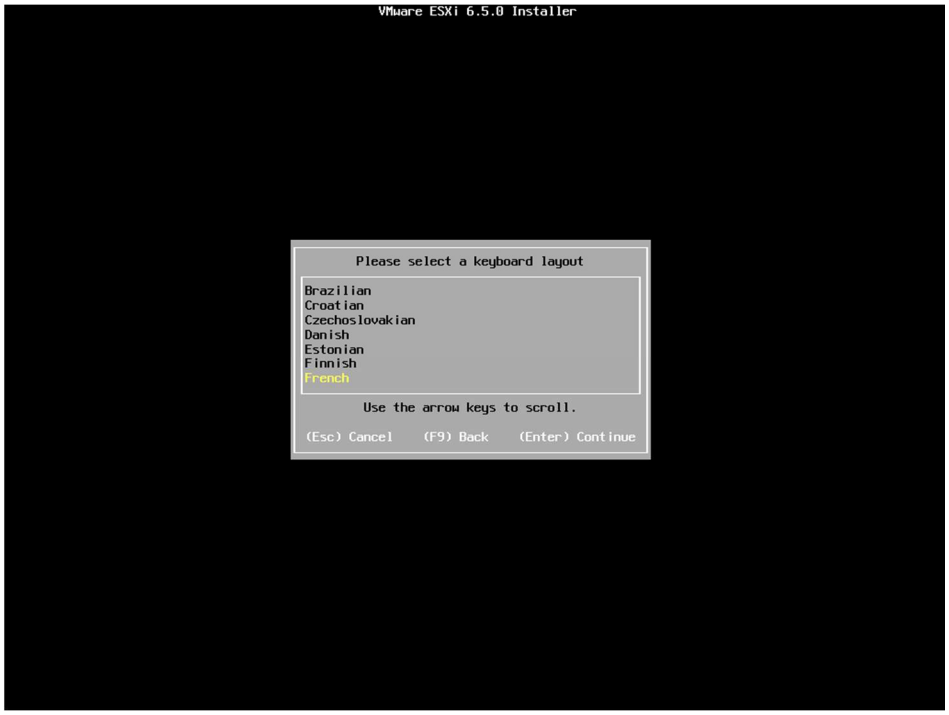
Voici la première page après le chargement des fichiers d'installations de l'ISO.



Avant de commencer, il faut accepter les conditions d'utilisations du logiciel.



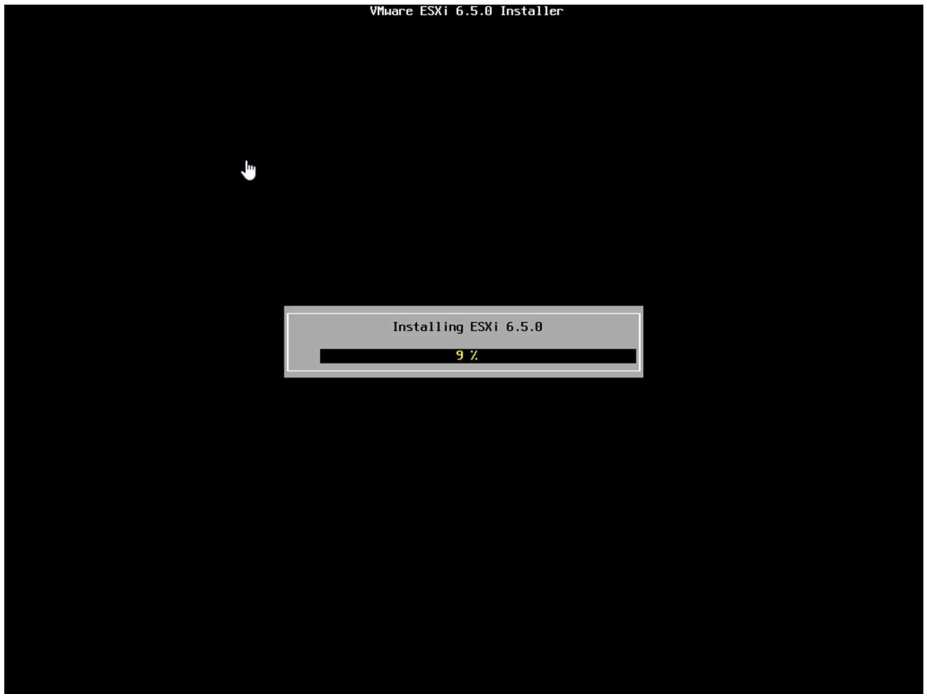
Ici il faut choisir le disque qui accueillera l'installation de l'ESX.



Sur la page suivante, il faut choisir la langue d'installation.

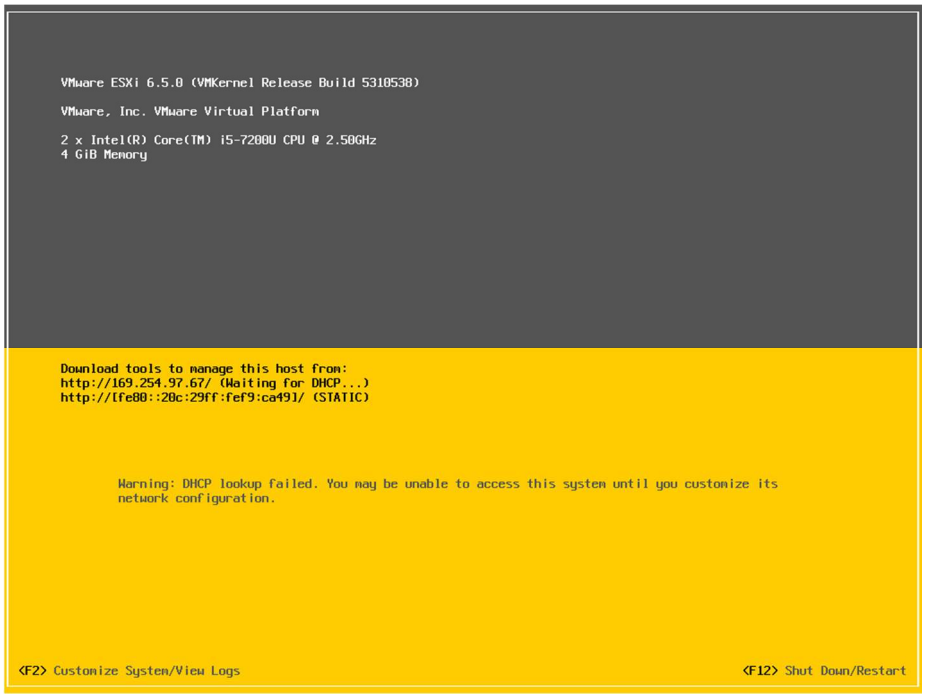
Ici, il faut renseigner le mot de passe de l'utilisateur ROOT pour l'administration du serveur.

Voici la page de confirmation avant l'installation.

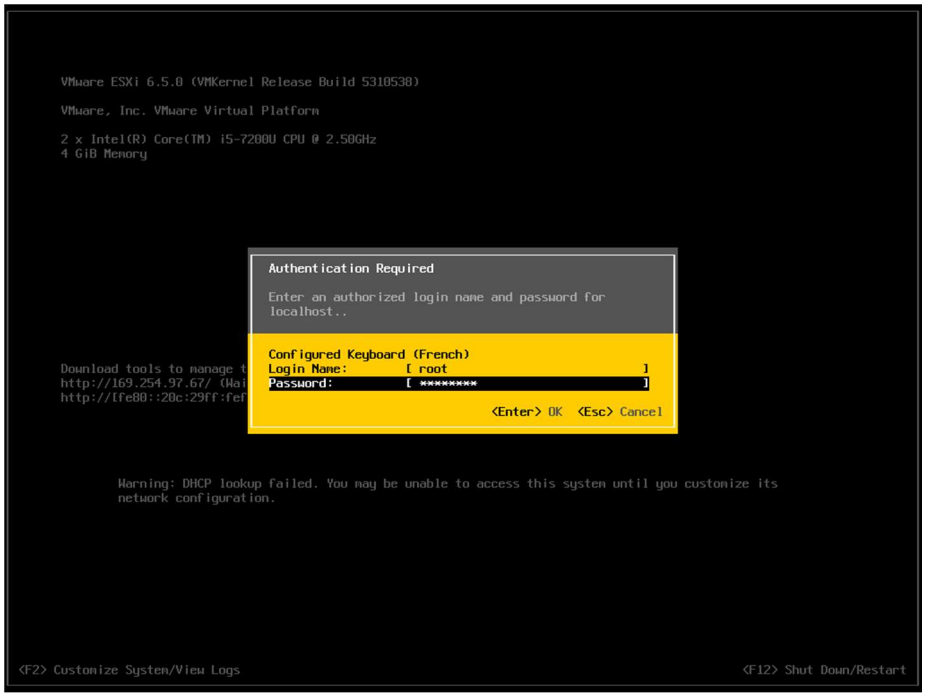


L'installation est lancée.

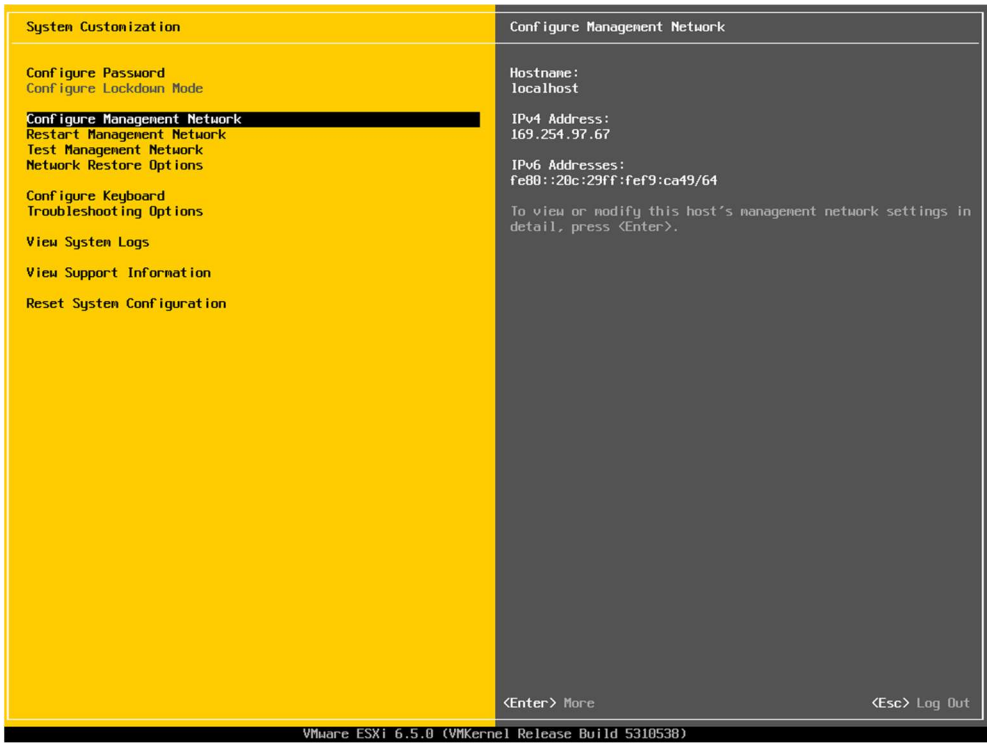
Une fois l'installation terminé, il faut retirer le media d'installation de l'ESXI et accepter le redémarrage.



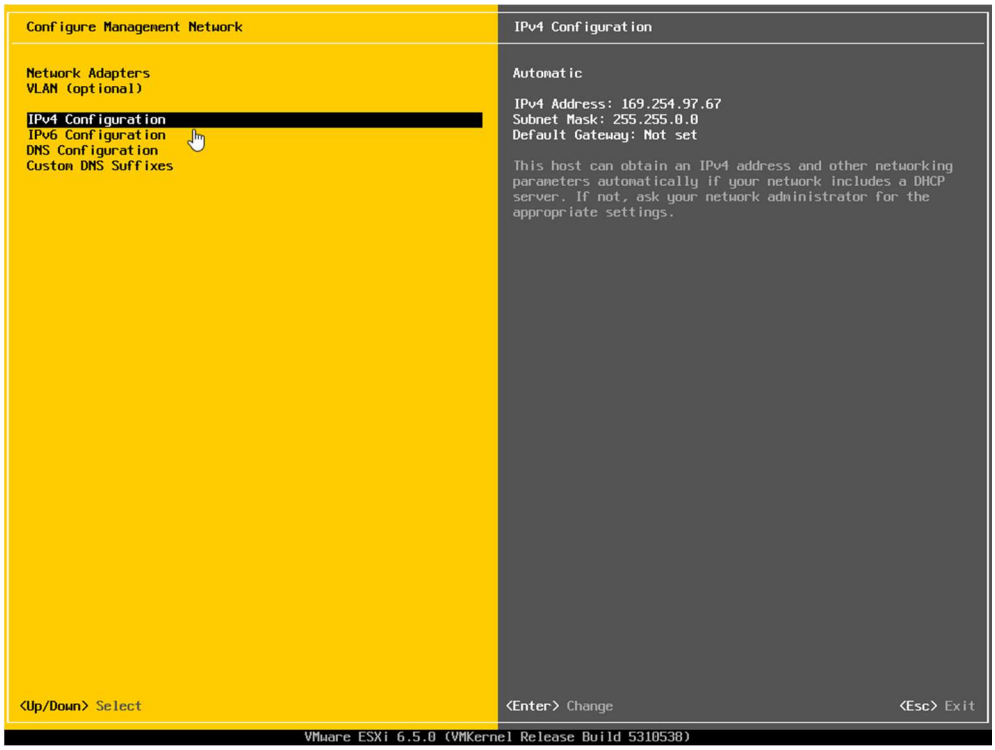
Apres redémarrage, nous arrivons sur la ou nous allons devoir configurer le réseau.



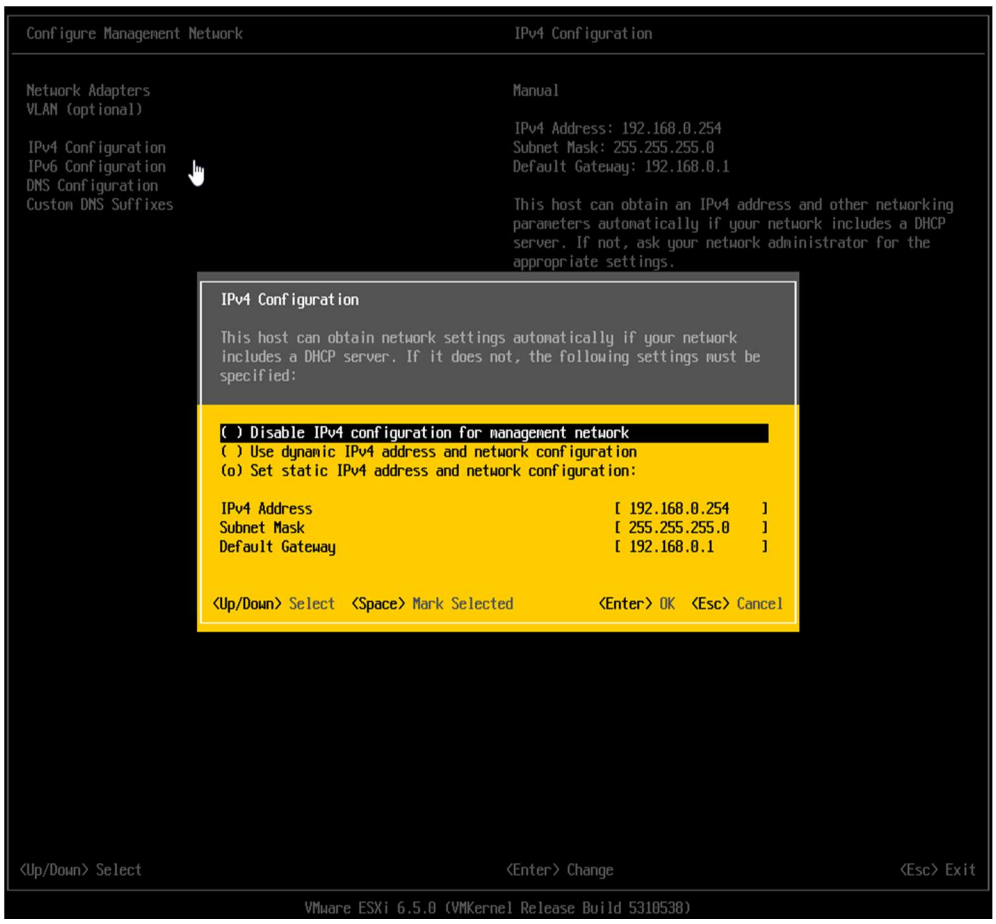
Il faudra donc appuyer sur « F12 » et se logger avec le mot de passe créer lors de l'installation.



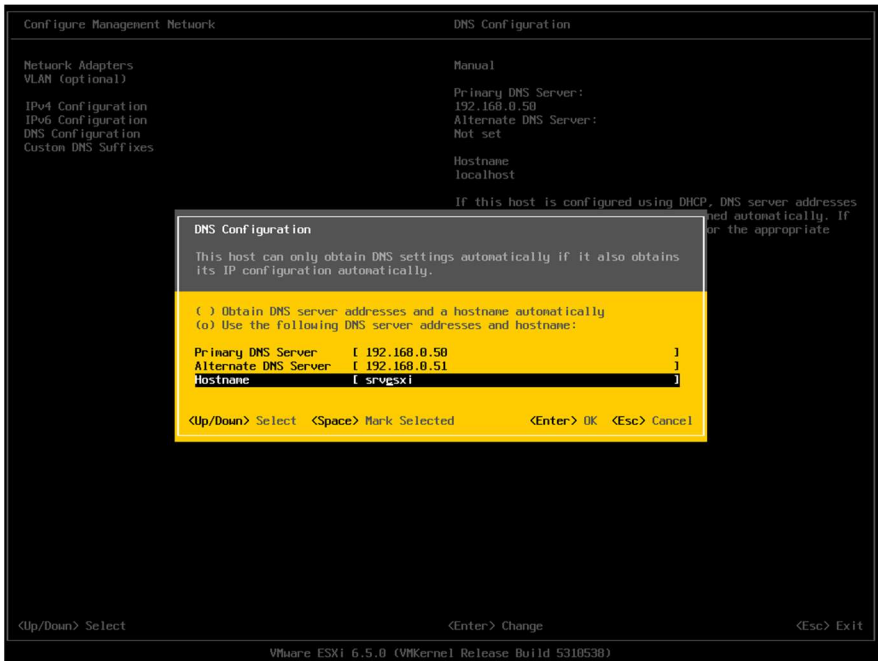
Sur la page de configuration, nous allons dans un premier temps, configurer l'adresse IP de la machine pour qu'elle soit accessible sur via le réseau.



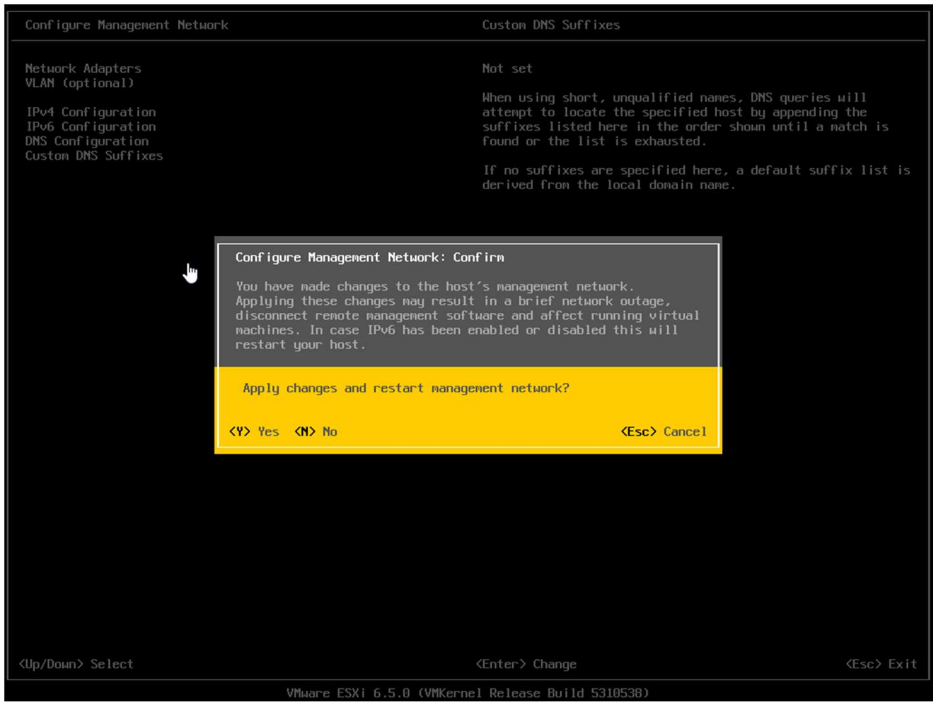
Nous sélectionnons IPV4.



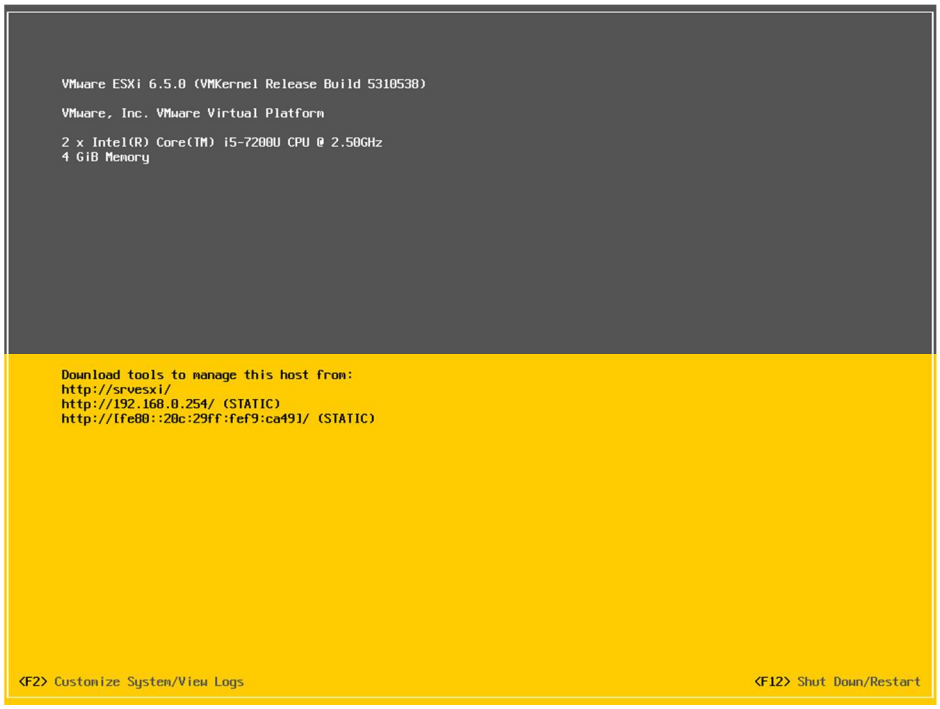
Ici il faut désactiver le DHCP en sélectionnant « SET STATIC IPV4 ADRESS AND NETWORK CONFIGURATION » et remplir comme souhaités l'IP, le masque réseau et la passerelle.



Ensuite, il faut effectuer la même manipulation en la configuration DNS.



En quittant les pages de configuration, le serveur nous propose de redémarrer immédiatement pour la prise ne compte des changements réseau.



Apres redémarrage, on peut constater que l'IP du serveur a bien été pris en compte.

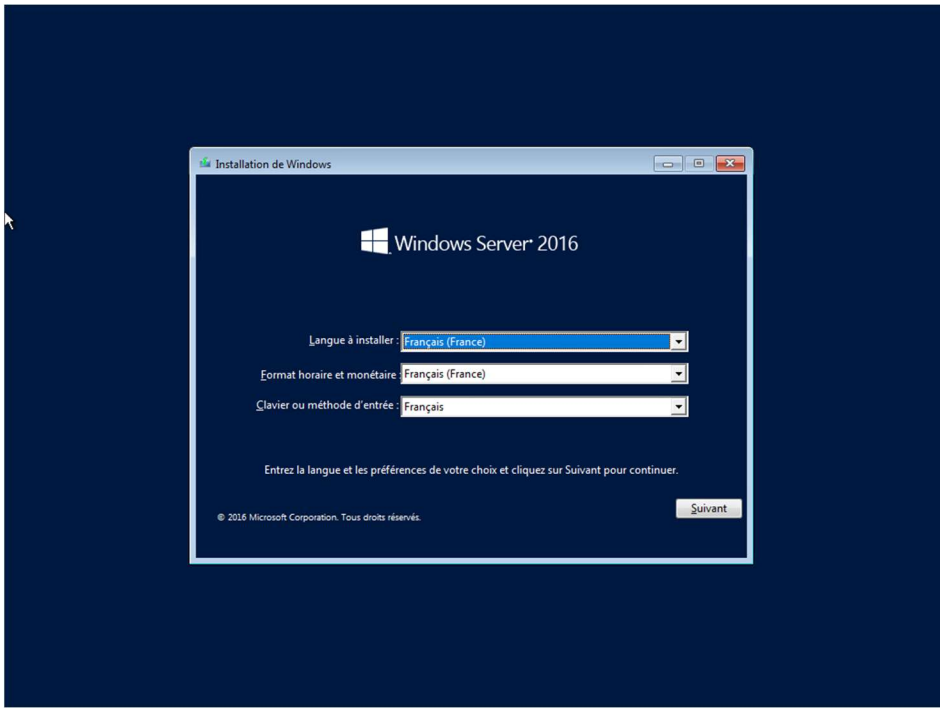
La configuration du serveur est maintenant terminée, on peut s'y connecter via le navigateur WEB d'un ordinateur sur le réseau via l'IP renseignée : https://192.168.0.254

3. Windows Serveur 2016

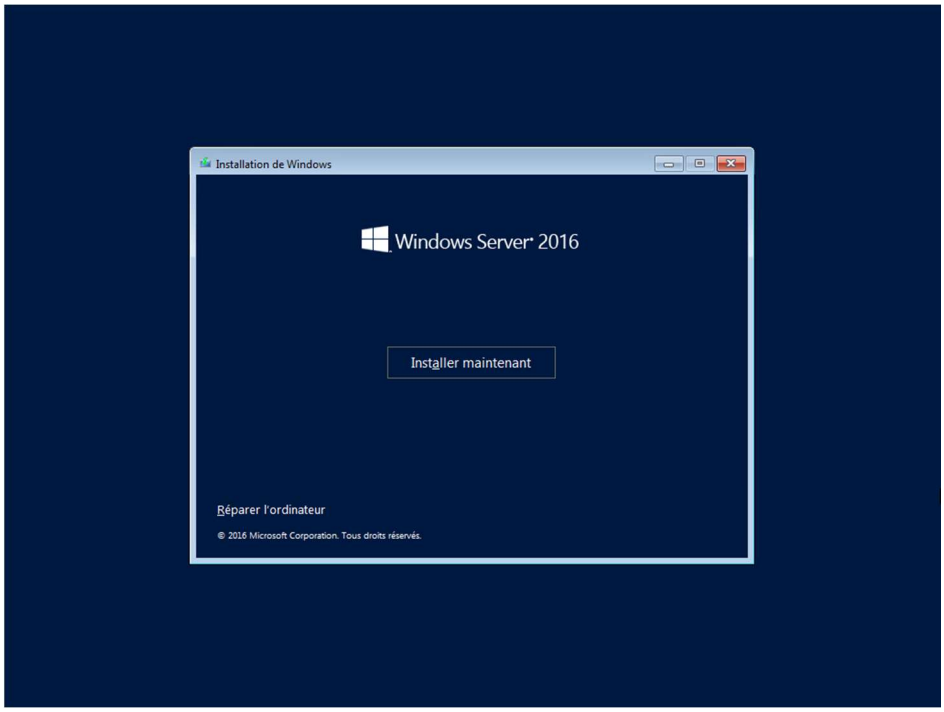
Nous avons décidé d'installer 5 machines virtuelles sous Windows Serveur. Deux pour l'AD, deux pour **SAMBA*** et un pour le service d'impression et la gestion des autres serveurs Windows.

a) Installation

Voici les différentes étapes d'installation de Windows Serveur 2016 Core :

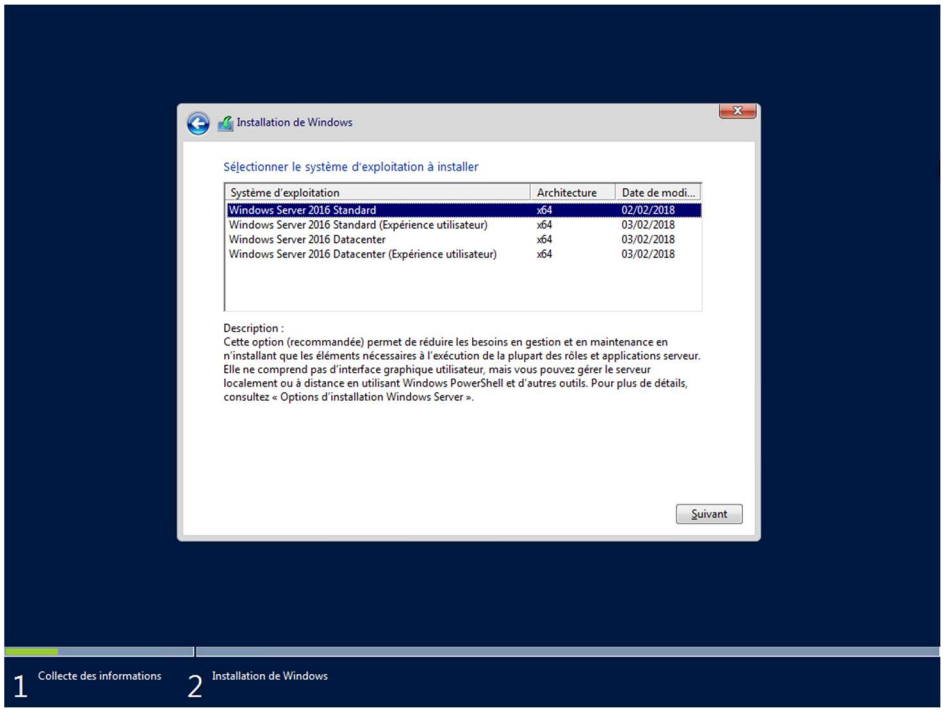


Après avoir booté sur l'image disque (ISO) de Windows serveur, voici la première page sur laquelle nous arrivons.

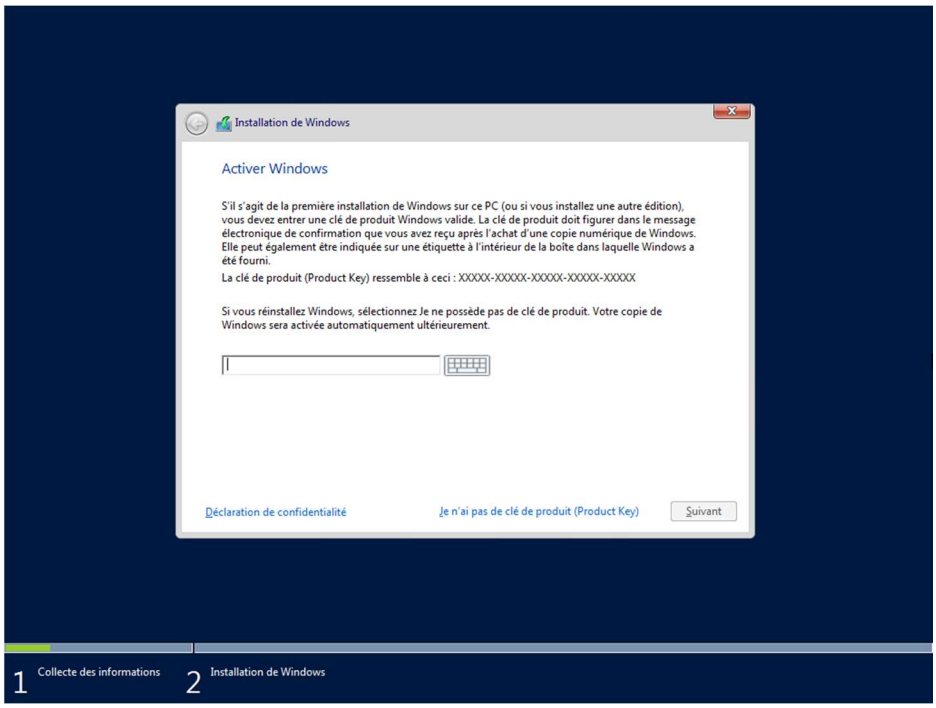


Ici sont proposé les différents langages disponibles. Nous sélectionnons le Français.

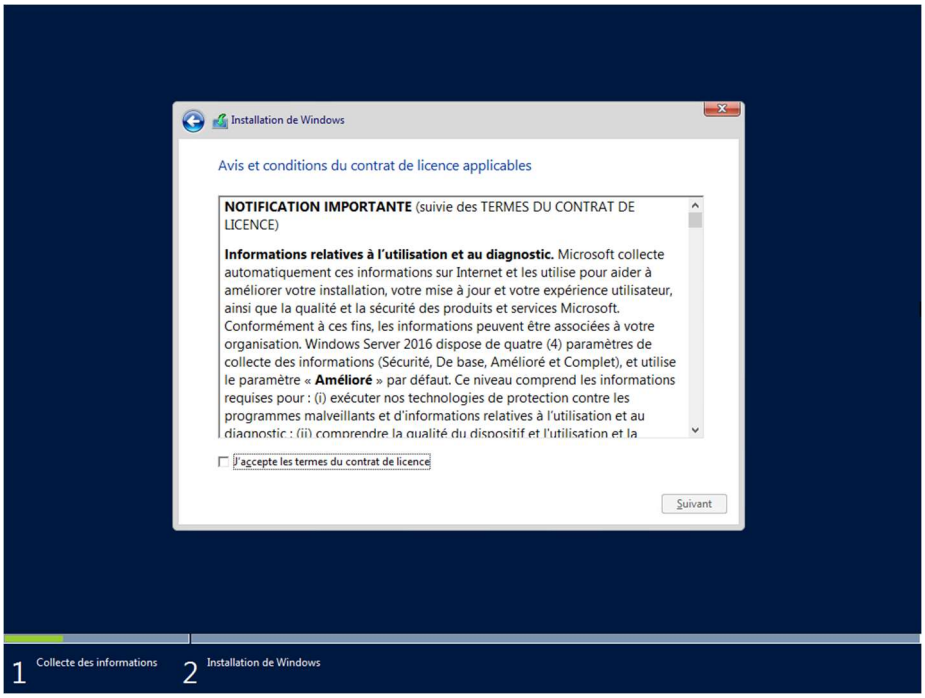
L'installation va maintenant pouvoir être lancée.



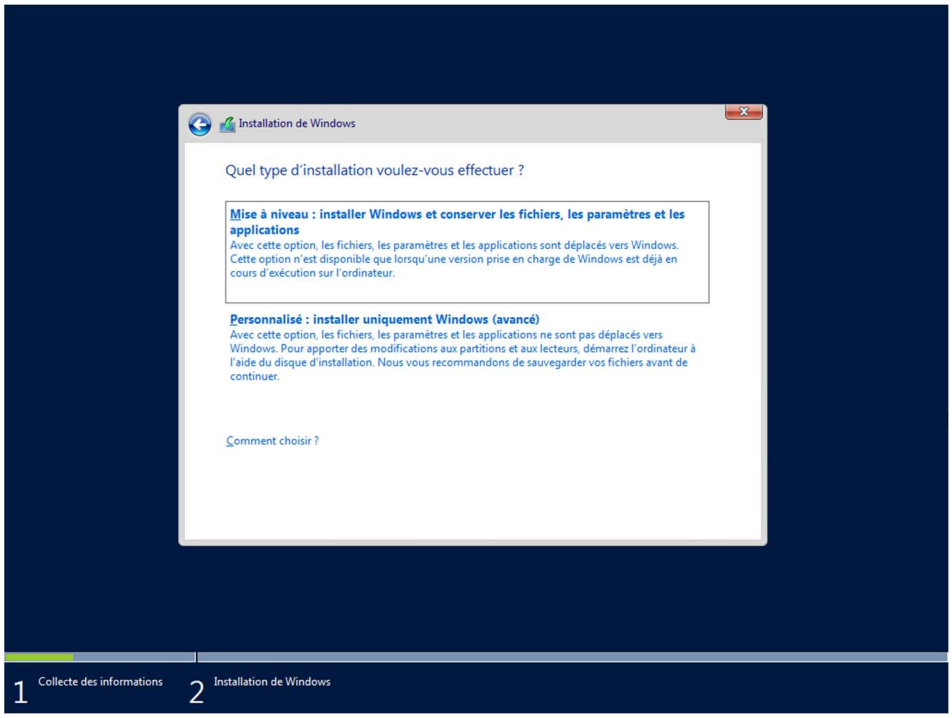
Ici, nous pouvons sélectionner la version du Windows server à installer (Standard ou Datacenter) ainsi que s'on mode d'installation, avec ou sans « Expérience utilisateur » ce qui signifie, avec ou sans interface graphique. Nous choisirons sans, car ce mode requiert beaucoup moins de ressource matérielle, est plus sécurisé et requiert moins de mise i u i à jour.



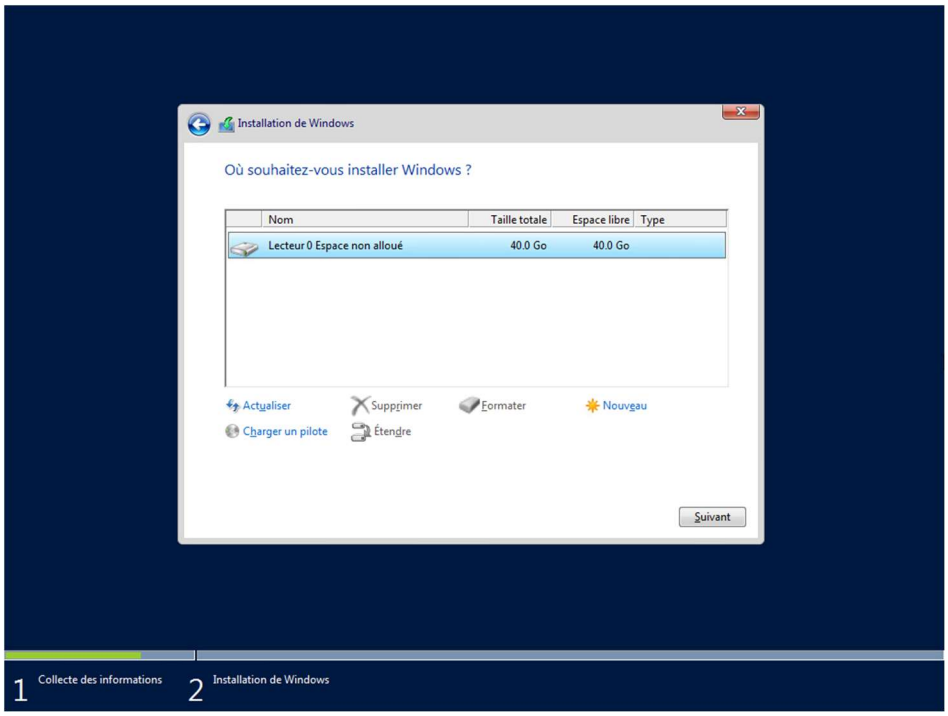
Cette étape vous demande la clé d'activation pour l'utilisation du produit.

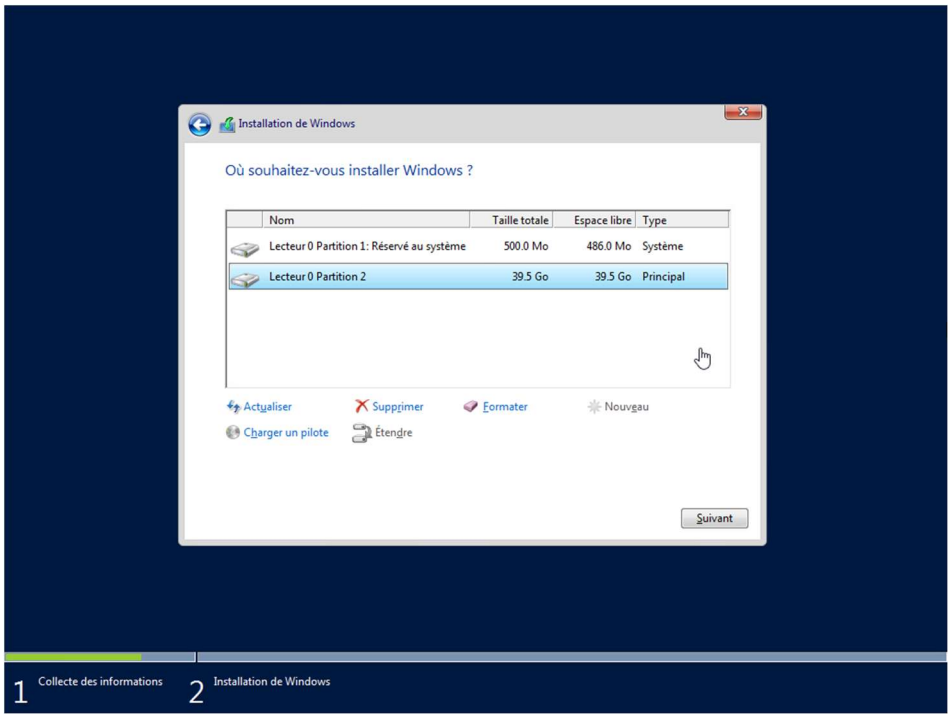


Voici les conditions d'utilisations de la licence Windows serveur à accepter pour continuer le produit Microsoft.



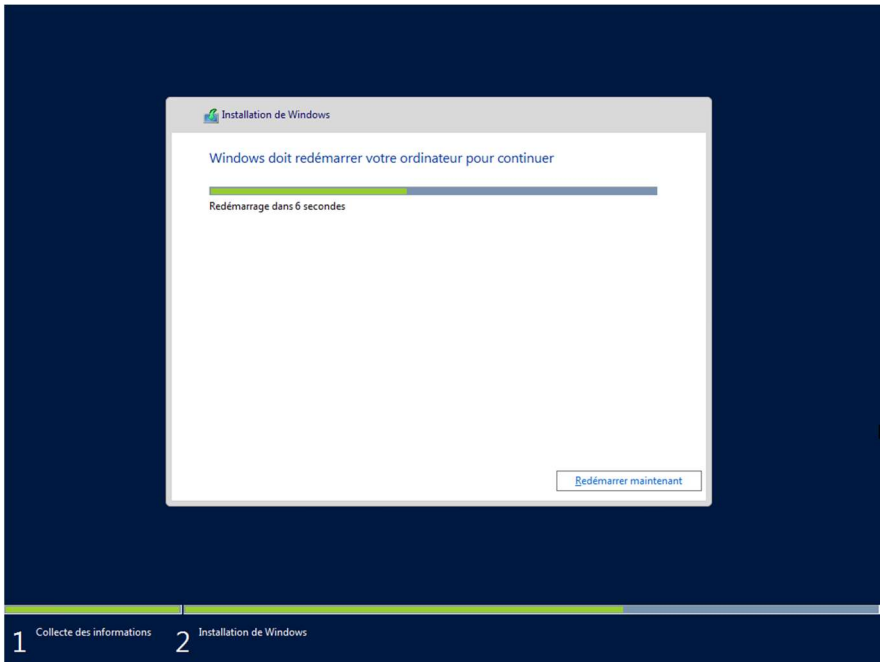
Cette étape concerne le type d'installation à effectuer. Nous allons choisir personnalisé car ceci et une installation fraiche et non pas une mise à jour du produit.

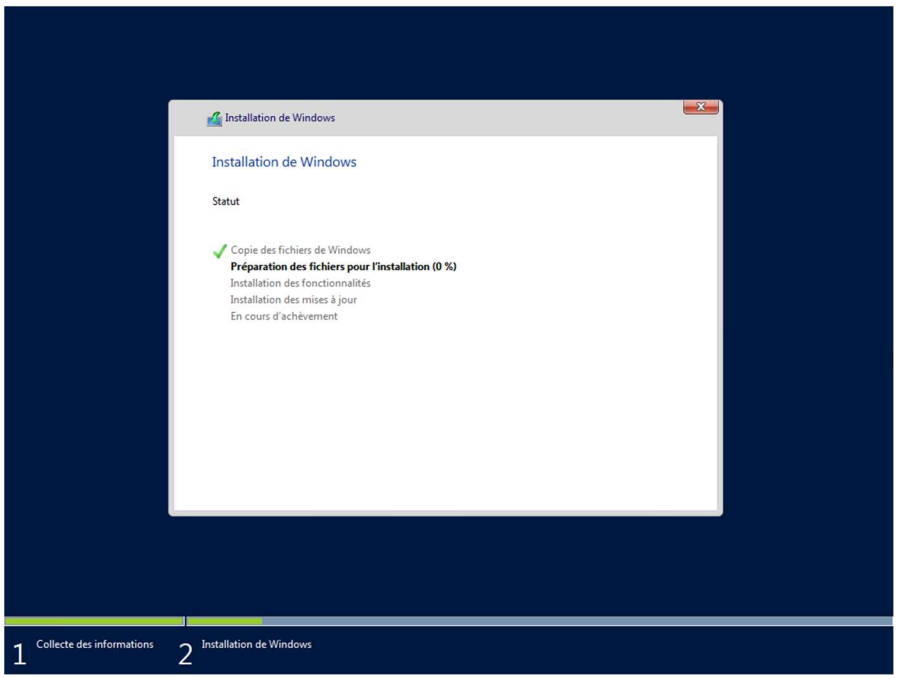




Nous allons donc paramètre le disque dur ou sera installer Windows Serveur.

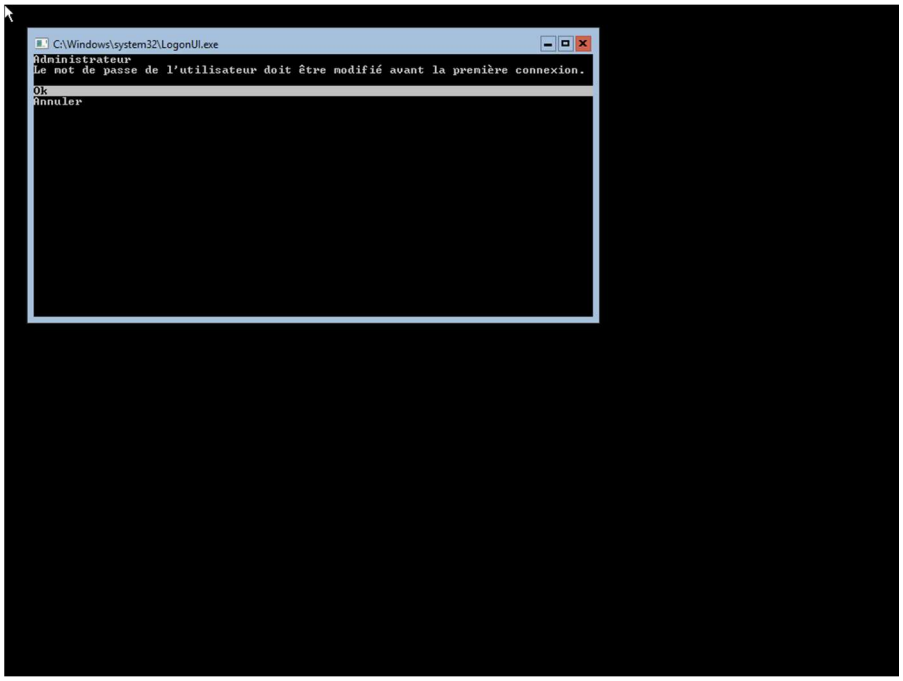
Voici le partitionnement de base proposé automatique par l'installeur. Il suffit amplement, rien besoin de changer.



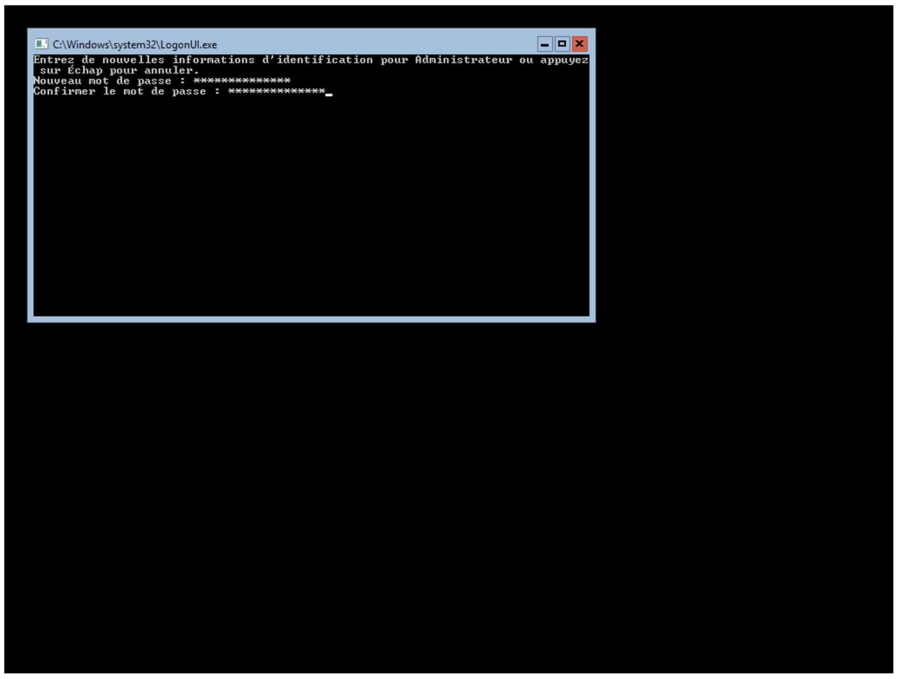


L'installation est désormais lancée. En mode Core, il suffit de quelque minute pour que l'installation se termine.

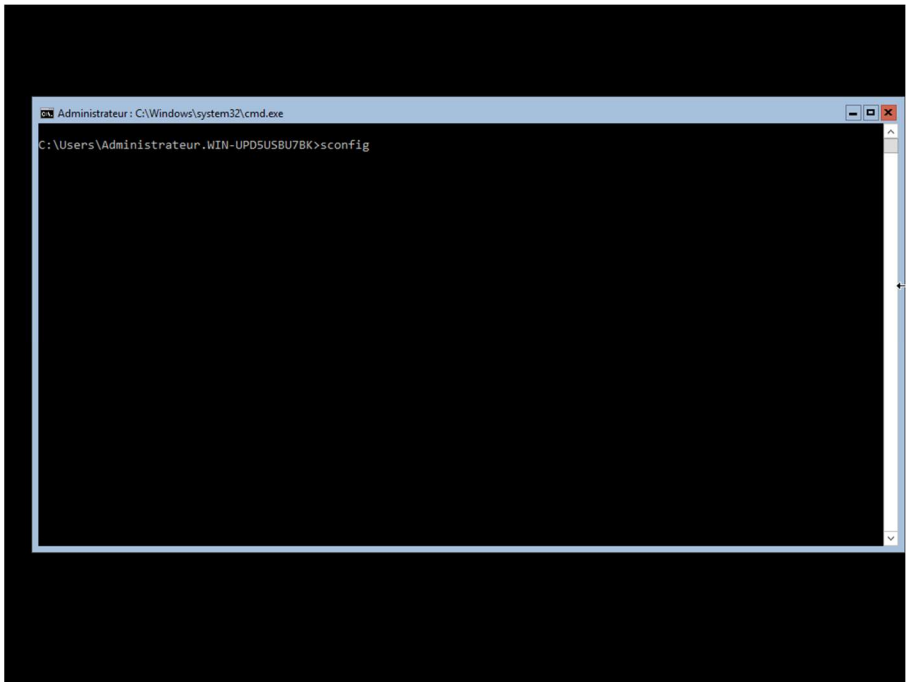
Lorsque l'installation est terminée, Windows serveur redémarrera automatiquement.



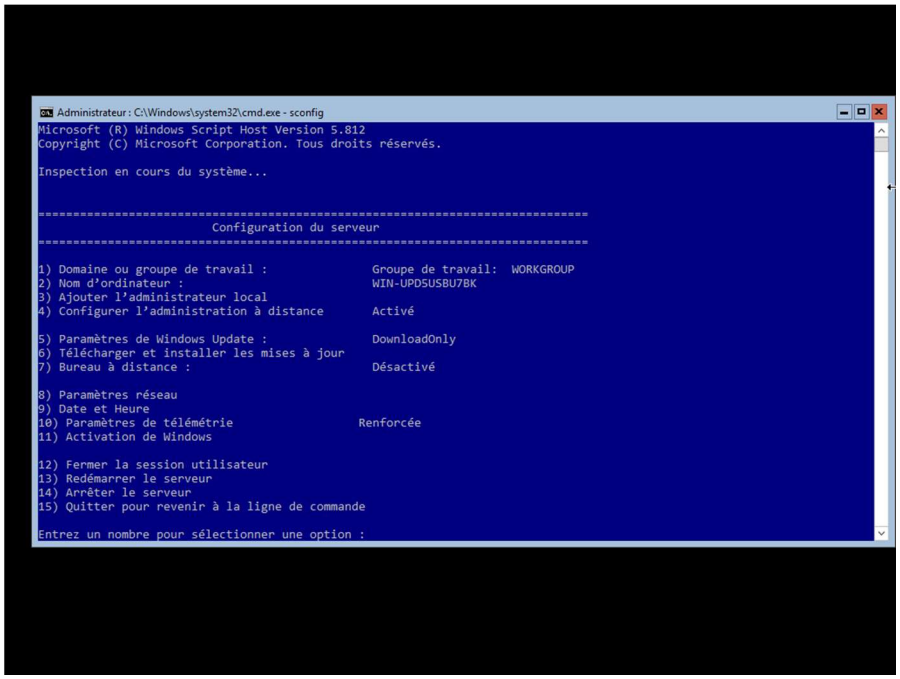
Configuration type d'un serveur.



Lors du premier démarrage, après installation, il est demandé de créer le mot de passe administrateur.



Ensuite, pour configurer le minimum sur un serveur, (le nom, l'IP, la jonction au domaine, etc.)



En mode Core la ligne de commande est : sconfig

Voici l'interface de configuration de serveur qui nous permet de modifier l'adresse IP de serveur, le domaine, nom de la machine, l'accès à distance, etc.

b) Active Directory // DNS

Afin de respecter les bonnes pratiques Microsoft et jouer la carte de la sécurité nous allons donc mettre en place deux serveurs contrôleur de domaine. En cas de panne du premier contrôleur de domaine le second le remplacera et ce en toute transparence pour les utilisateurs.

Nous installerons aussi un autre rôle sur nos deux contrôleurs de domaine nécessaire à son bon fonctionnement, celui de DNS pour Domain Name Server ou système de noms de domaine qui sera utilisé pour traduire les noms de domaine Internet et local en adresse IP ou autres enregistrements.

Les services Active Directory et DNS sont installés via scripts (voir annexe). Ce qui nous permet d'automatiser l'installation des services et de ne pas faire d'erreur.

De plus, si besoin est, ces scripts permettront d'installer ces services sur de nouvelles VM rapidement.

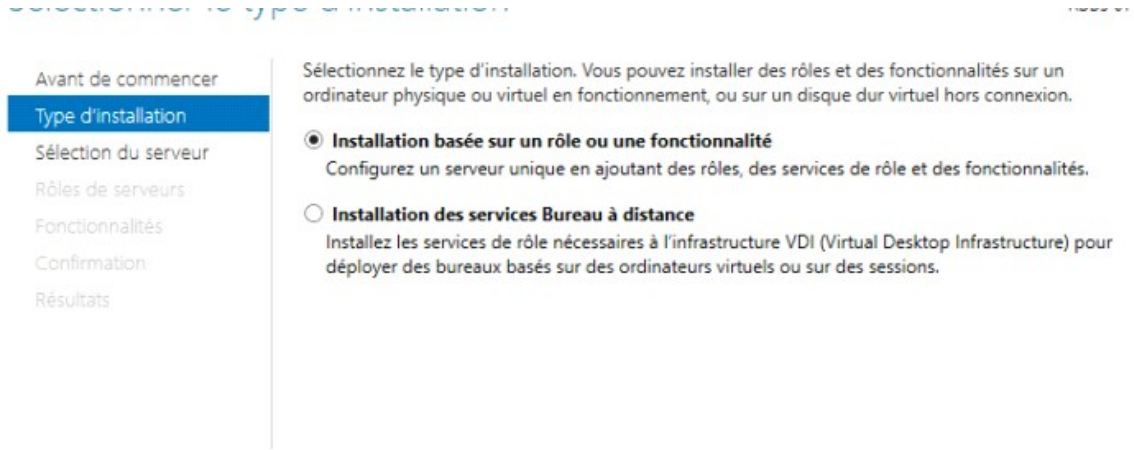
(1) Installation

Pour installer notre premier contrôleur de domaine, nous devons installer Active Directory.
Pour ce faire nous avons utilisé le script PowerShell suivant :

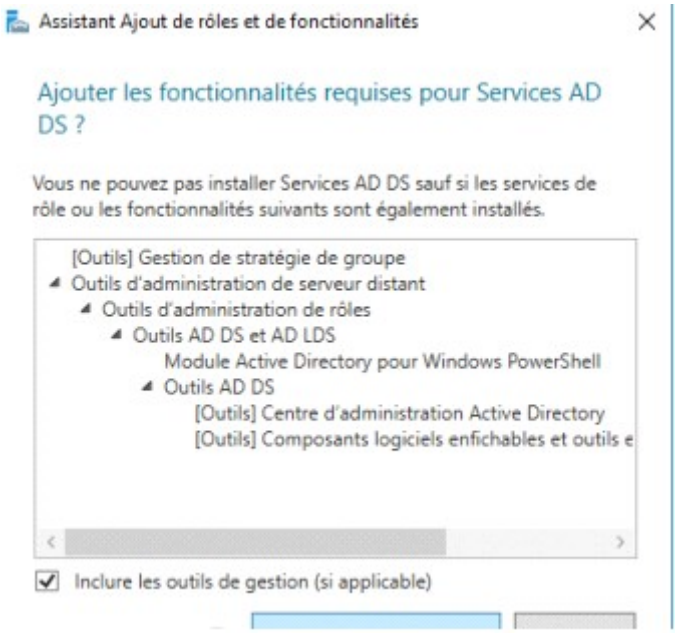
```
Install-windowsfeature AD-Domain-Services
Install-ADDSForest -CreateDnsDelegation:$false  `
DatabasePath "B:\NTDS"  `
DomainMode « 7"  `
DomainName "pielco.lan"  `
DomainNetbiosName "PIELCO"  `
ForestMode « 7"  `
InstallDns:$true  `
LogPath "L:\NTDS"  `
NoRebootOnCompletion:$false  `
SysvolPath "S:\SYSVOL"  `
Force:$true
```

Une fois l'AD installé, nous devons faire la même chose sur un deuxième serveur pour avoir le deuxième DC de notre forêt.

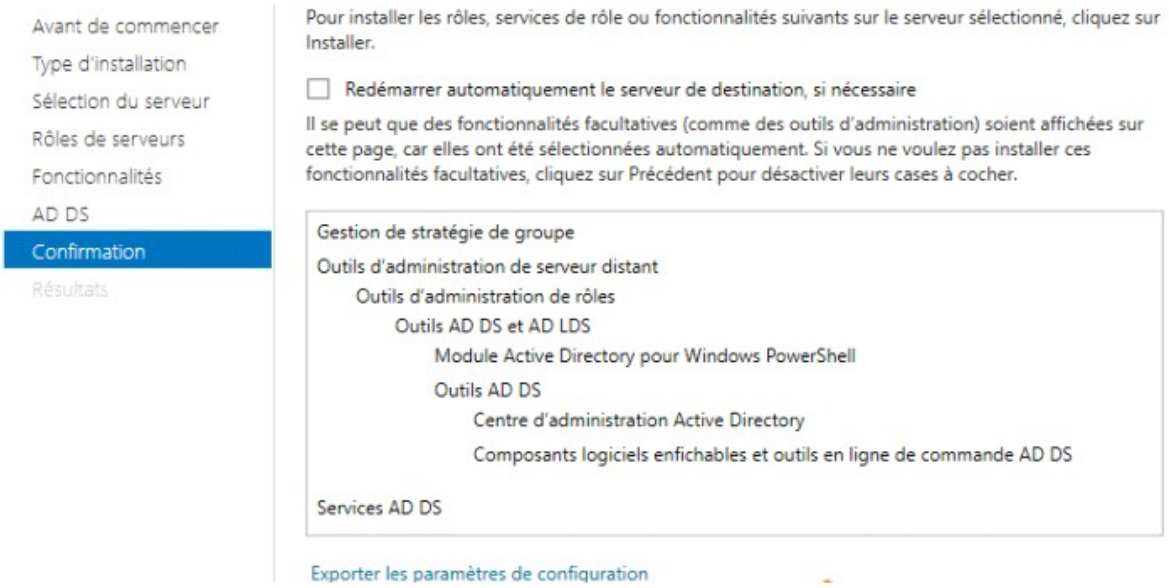
Pour ce faire, nous avons réinstallé l'AD en graphique de la manière suivante :



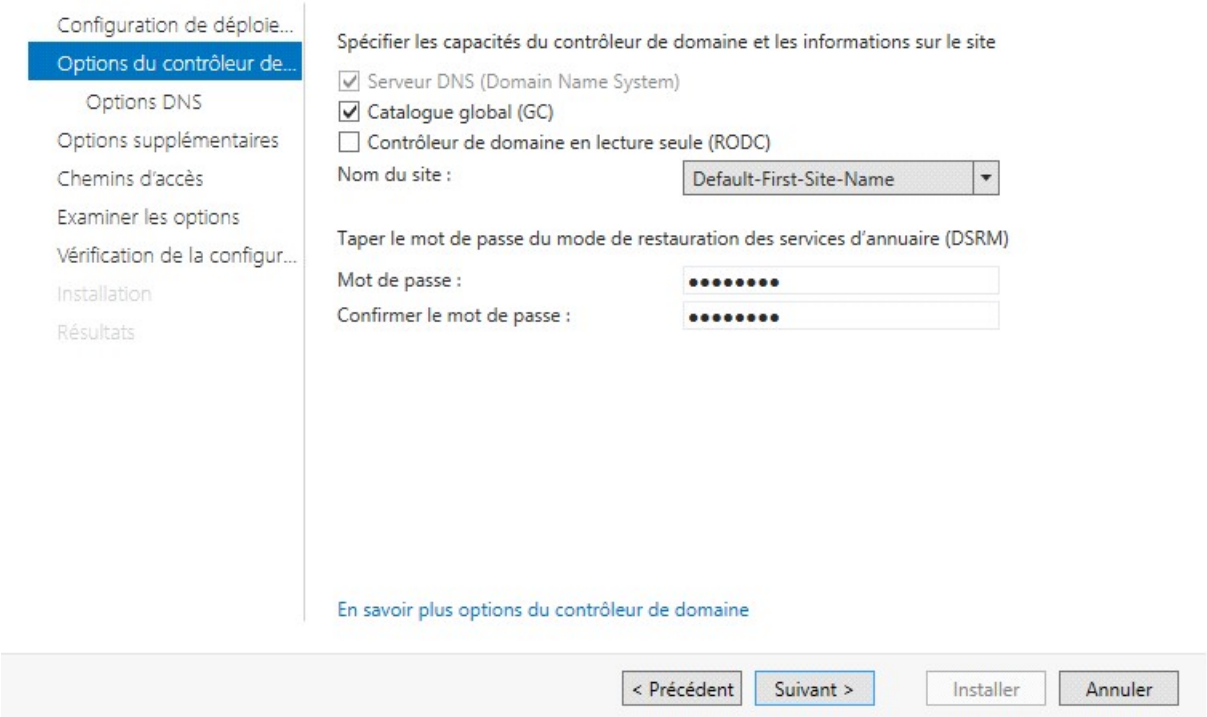
Installation d'un nouveau rôle



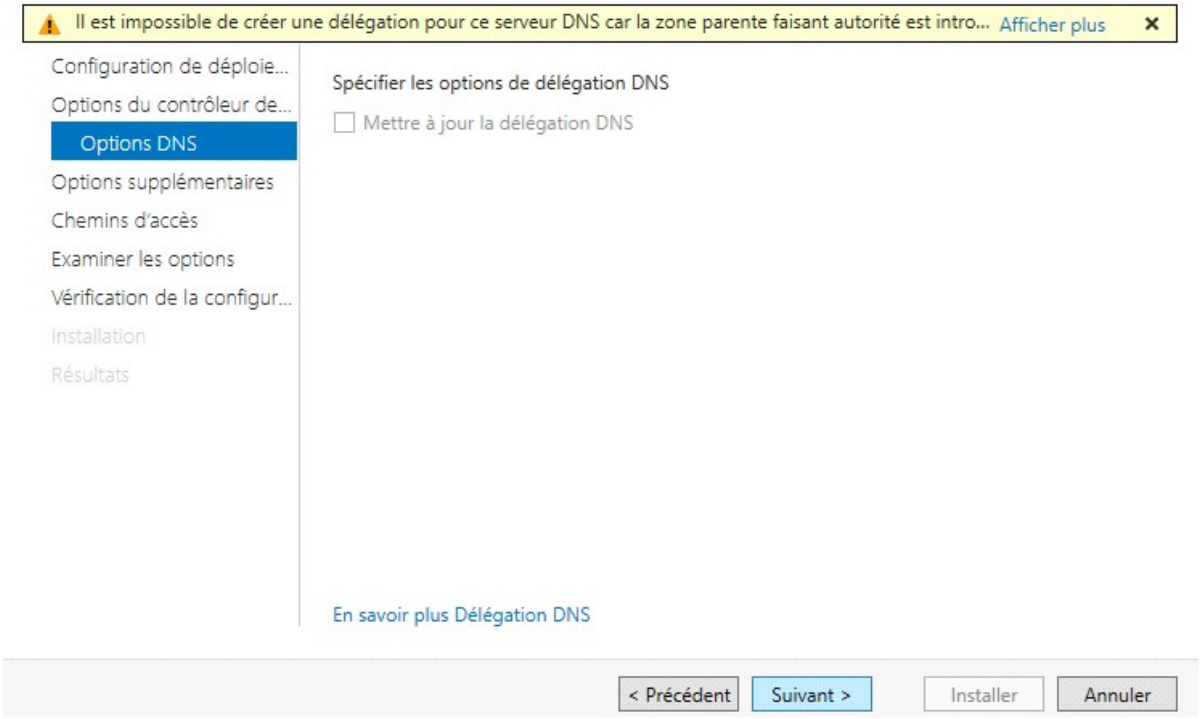
On ajoute les outils de gestion pour ADDS



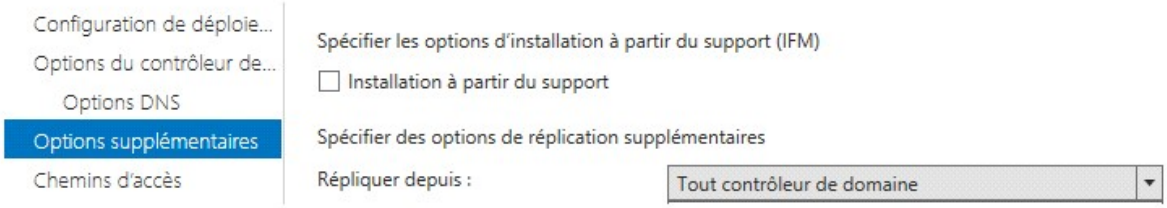
On confirme sans redémarrer le serveur



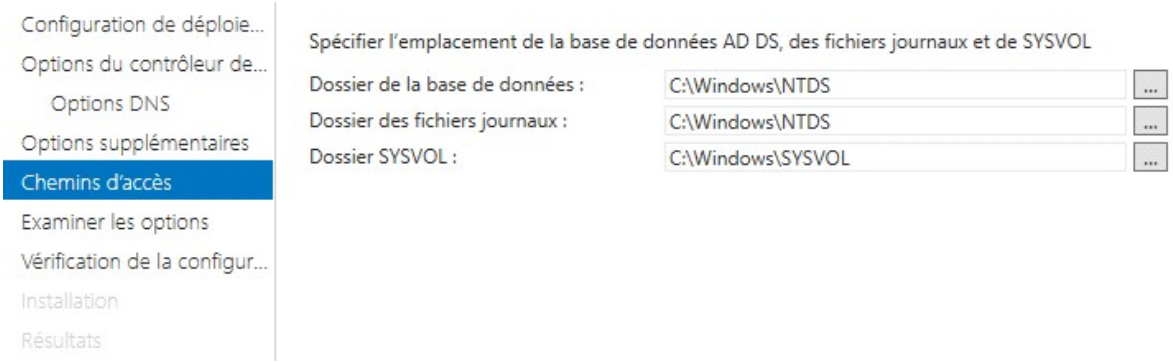
On coche catalogue global et on indique le mot de passe de restauration des services d'annuaire



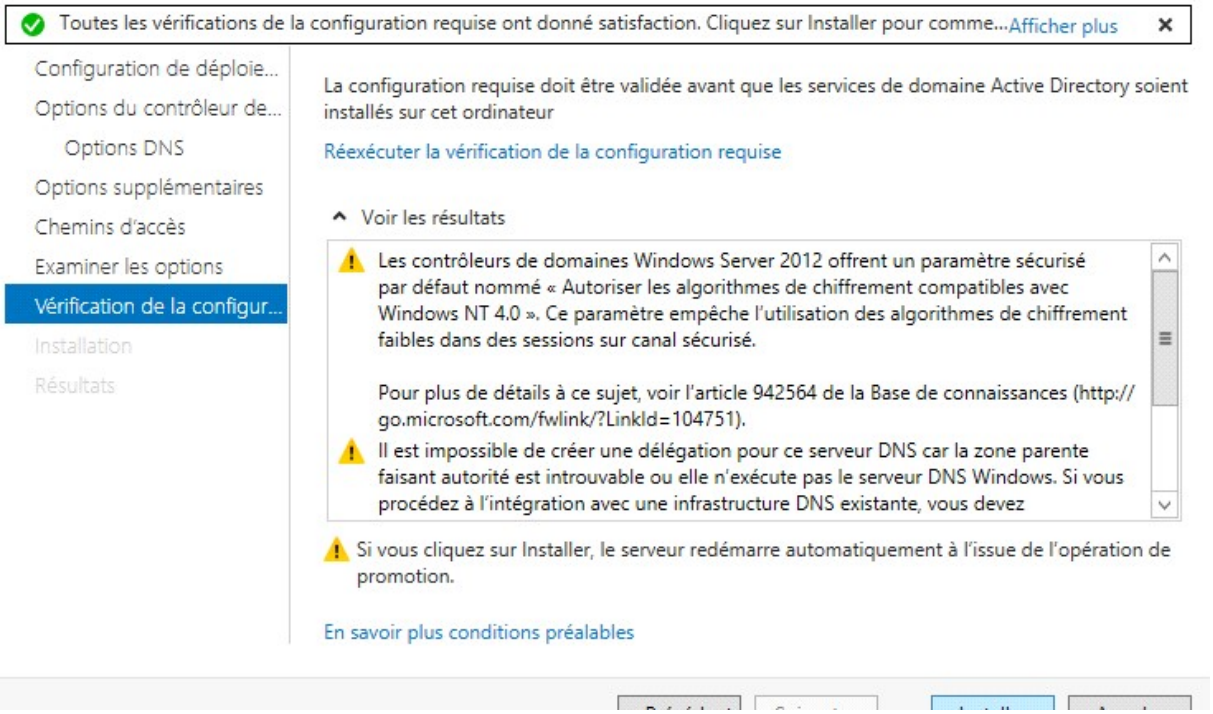
Suivant



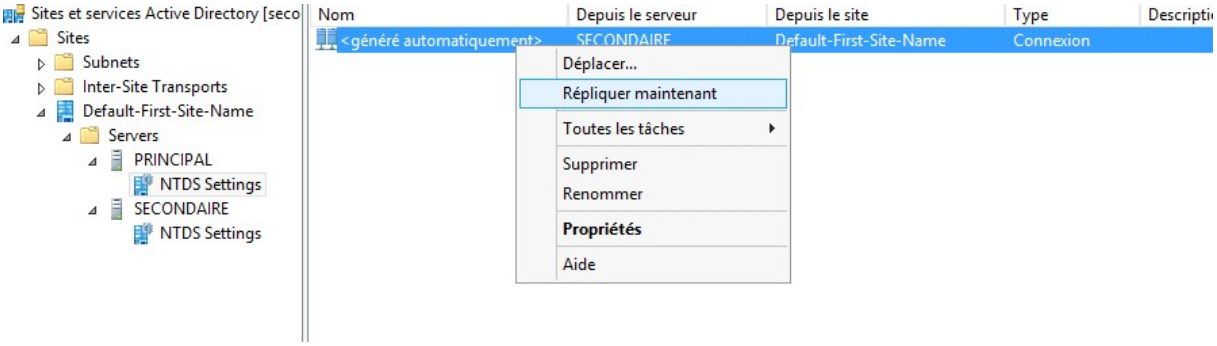
En sélectionnant cette option on réplique à partir du DC1



On indique ici les chemins d'accès des dossiers



On vérifie que les paramètres sont bons



Dans la console AD, on active la réplication entre les deux AD.

(2) Création des utilisateurs

Pour créer les utilisateurs, nous avons fait un script PowerShell qui s'appuie sur un CV contenant la liste des employés de Pielco. Cette solution par script est encore une fois rapide à mettre en place et permet un gain de temps conséquent. De plus, une fois sûr, ce script nous permet d'éviter de faire des erreurs.

Voir les annexes pour les deux fichiers.

(3) Mise en place des GPO

De manière à bien gérer les utilisateurs nous avons mis en places plusieurs GPO, les voici :

Nom	État GPO	Filtre WMI
bloque DVD/FLOPPY	Activé	Aucun(e)
Bloque install logiciels	Activé	Aucun(e)
deco user	Activé	Aucun(e)
Default Domain Controllers Policy	Activé	Aucun(e)
Default Domain Policy	Activé	Aucun(e)
Print	Activé	Aucun(e)
Quota	Activé	Aucun(e)

Liste des GPO appliquées aux utilisateurs

bloque DVD/FLOPPY

Étendue | Détails | Paramètres | Délégation | État

bloque DVD/FLOPPY

Données recueillies le : 20/08/2018 11:15:04 — afficher tout

Général — masquer

- **Détails** — afficher
- **Liaisons** — afficher
- **Filtrage de sécurité** — afficher
- **Délégation** — afficher

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	Désactivé	
CD et DVD : refuser l'accès en lecture	Désactivé	
Lecteurs de disquettes : refuser l'accès en écriture	Désactivé	
Lecteurs de disquettes : refuser l'accès en lecture	Désactivé	

La GPO pour bloquer l'utilisation du lecteur CD et de disquette

Bloque install logiciels

Étendue | Détails | Paramètres | Délégation | État

Bloque install logiciels

Données recueillies le : 20/08/2018 11:15:42 — afficher tout

Général — masquer

- **Détails** — afficher
- **Liaisons** — afficher
- **Filtrage de sécurité** — afficher
- **Délégation** — afficher

Configuration ordinateur (activée) — masquer

Stratégies — masquer

Modèles d'administration — masquer

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

Composants Windows/Windows Installer — masquer

Stratégie	Paramètre	Commentaire
Autoriser les utilisateurs à appliquer des correctifs sur des installations avec privilèges élevés	Désactivé	
Empêcher la suppression des mises à jour	Activé	
Interdire les installations par les utilisateurs	Activé	
Comportement de l'installation par l'utilisateur :	Masquer l'installation par l'utilisateur	

Configuration utilisateur (activée) — masquer

Aucun paramètre n'est défini.

GPO bloquant la possibilité d'installer des logiciels

deco user

Étendue | Détails | Paramètres | Délégation | État

deco user

Données recueillies le : 20/08/2018 11:14:14

afficher tout

Général — afficher

Configuration ordinateur (activée) — masquer

Aucun paramètre n'est défini.

Configuration utilisateur (activée) — masquer

Préférences — masquer

Paramètres du Panneau de configuration — masquer

Tâches planifiées — masquer

Tâche planifiée (nom : deco user) — masquer

deco user (ordre : 1) — masquer

Général — masquer

Action	Créer
Tâche	
Nom	deco user
Exécuter	shutdown.exe
Arguments	/l /f
Démarrer dans	C:\Windows\System32
La tâche planifiée s'exécute à l'heure spécifiée.	Activé
Planification	
1. À 19:00 tous les jours. Cette tâche débute le 16/08/2018	
Paramètres	
Supprimer la tâche si son exécution n'est plus planifiée	Non
Arrêter la tâche si l'ordinateur n'est plus inactif	Non
Ne pas démarrer la tâche si l'ordinateur utilise les batteries	Activé
Arrêter la tâche si l'ordinateur passe en mode batterie	Activé
Sortir l'ordinateur du mode veille pour exécuter cette tâche	Désactivé

Commun — masquer

Options	
Interrompre le traitement des éléments sur cette extension si une erreur se produit sur cet élément	Non
Exécuter dans le contexte de sécurité de l'utilisateur connecté (option de la stratégie utilisateur)	Non
Supprimer cet élément lorsqu'il n'est plus appliqué	Non
Appliquer une fois et ne pas réappliquer	Non

GPO paramétrant les déconnexions des utilisateurs

deco user

Étendue | Détails | Paramètres | Délégation | État

Configuration utilisateur (activée) — masquer

Préférences — masquer

Paramètres du Panneau de configuration — masquer

Tâches planifiées — masquer

Tâche planifiée (nom : deco user) — masquer

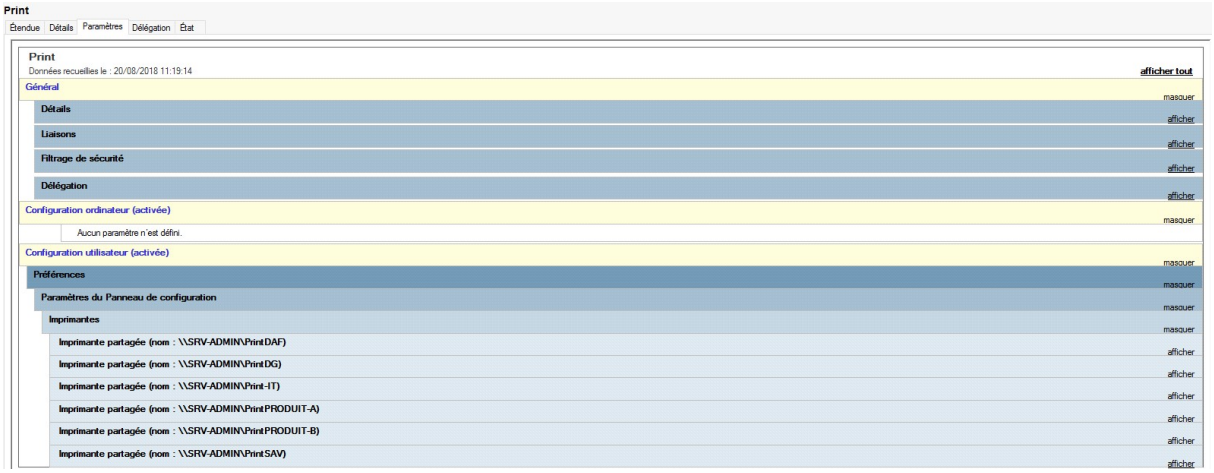
deco user (ordre : 1) — masquer

Général — masquer

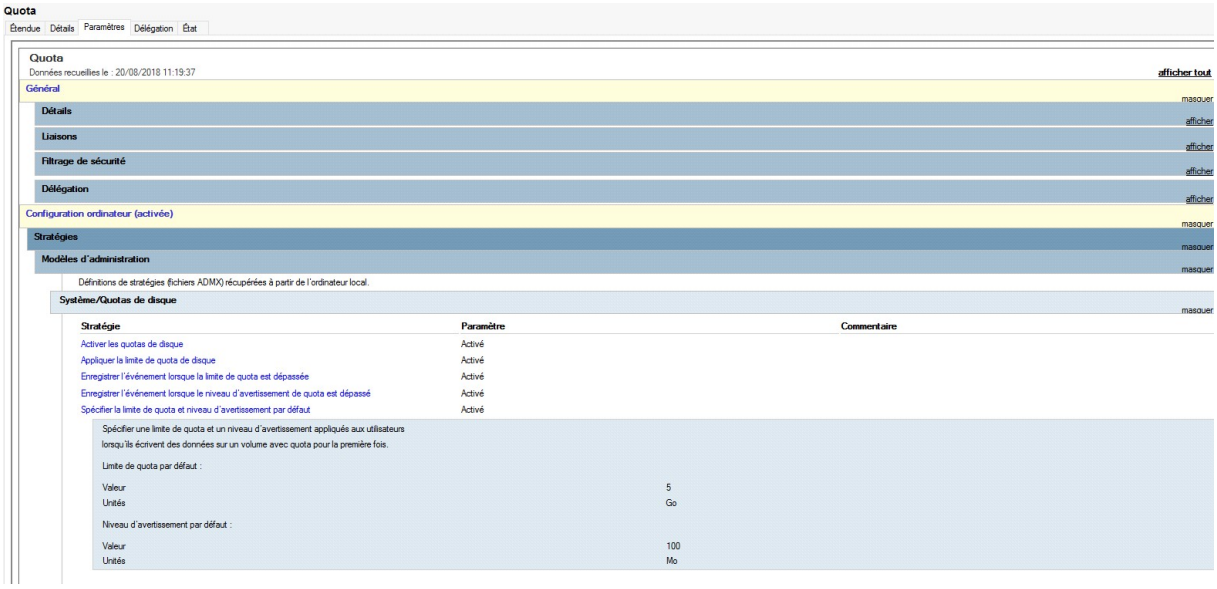
Commun — afficher

Options	
Interrompre le traitement des éléments sur cette extension si une erreur se produit sur cet élément	Non
Exécuter dans le contexte de sécurité de l'utilisateur connecté (option de la stratégie utilisateur)	Non
Supprimer cet élément lorsqu'il n'est plus appliqué	Non
Appliquer une fois et ne pas réappliquer	Non
Cible niveau élément : Utilisateur	
Attribut	Valeur
bool	AND
not	0
name	PIELCO\pauline.ayo
sid	S-1-5-21-1710135193-1661715509-3856782548-2123
Cible niveau élément : Utilisateur	
Attribut	Valeur
bool	AND
not	0
name	PIELCO\martine.beziat
sid	S-1-5-21-1710135193-1661715509-3856782548-2124
Cible niveau élément : Utilisateur	
Attribut	Valeur
bool	AND
not	0
name	PIELCO\adeline.ella
sid	S-1-5-21-1710135193-1661715509-3856782548-2122
Cible niveau élément : Utilisateur	
Attribut	Valeur
bool	AND
not	0
name	PIELCO\sophie.acien
sid	S-1-5-21-1710135193-1661715509-3856782548-2125

Suite de la GPO déconnexion utilisateur



GPO faisant remonter les imprimantes



GPO limitant l'espace disque de chaque utilisateur sur les serveurs

Default Domain Policy

Étendue Détails Paramètres Délégation État

Délégation — afficher

Configuration ordinateur (activée) — masquer

Stratégies — masquer

Paramètres Windows — masquer

Paramètres de sécurité — masquer

Stratégies de comptes/Stratégie de mot de passe — masquer

Stratégie	Paramètre
Antériorité maximale du mot de passe	365 jours
Antériorité minimale du mot de passe	1 jours
Appliquer l'historique des mots de passe	3 mots de passe mémorisés
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé
Le mot de passe doit respecter des exigences de complexité	Activé
Longueur minimale du mot de passe	8 caractères

Stratégies de comptes/Stratégie de verrouillage du compte — masquer

Stratégie	Paramètre
Seuil de verrouillage de comptes	0 tentative d'ouverture de session non valides

Stratégies de comptes/Stratégie Kerberos — masquer

Stratégie	Paramètre
Appliquer les restrictions pour l'ouverture de session	Activé
Durée de vie maximale du ticket d'utilisateur	10 heures
Durée de vie maximale du ticket de service	600 minutes
Durée de vie maximale pour le renouvellement du ticket utilisateur	7 jours
Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur	5 minutes

GPO de paramétrage de mot de passe.

Préférences — masquer

Paramètres Windows — masquer

Mappages de lecteurs — masquer

Mappage de lecteur (lecteur : S) — masquer

S: (ordre : 1) — masquer

Général — masquer

Action	Créer
Propriétés	
Lettre US (215,9 x 279,4 mm)	S
Emplacement	\\pielco.lan\data\services
Reconnecter	Activé
Intituler	Services
Utiliser le premier disponible	Désactivé
Masquer/Afficher ce lecteur	Afficher
Masquer/Afficher les lecteurs	Aucune modification

Commun

GPO pour le mappage des lecteurs réseaux des utilisateurs

Nous avons choisi d'utiliser le **Remote Desktop Protocol** de Windows pour prendre la main sur les postes des salariés. Voici la GPO activant le service sur leur poste :

Default Domain Policy

Étendue Détails Paramètres Délégation État

Default Domain Policy — afficher tout

Données recueillies le : 20/08/2018 11:18:49

Général — masquer

Détails — afficher

Liaisons — afficher

Filtrage de sécurité — afficher

Délégation — afficher

Configuration ordinateur (activée) — masquer

Stratégies — masquer

Paramètres Windows — masquer

Paramètres de sécurité — afficher

Modèles d'administration — masquer

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

Composants Windows/OneDrive — afficher

Composants Windows/Services Bureau à distance/Hôte de la session Bureau à distance/Connexions — masquer

Stratégie	Paramètre	Commentaire
Autoriser les utilisateurs à se connecter à distance à l'aide des services Bureau à distance	Activé	

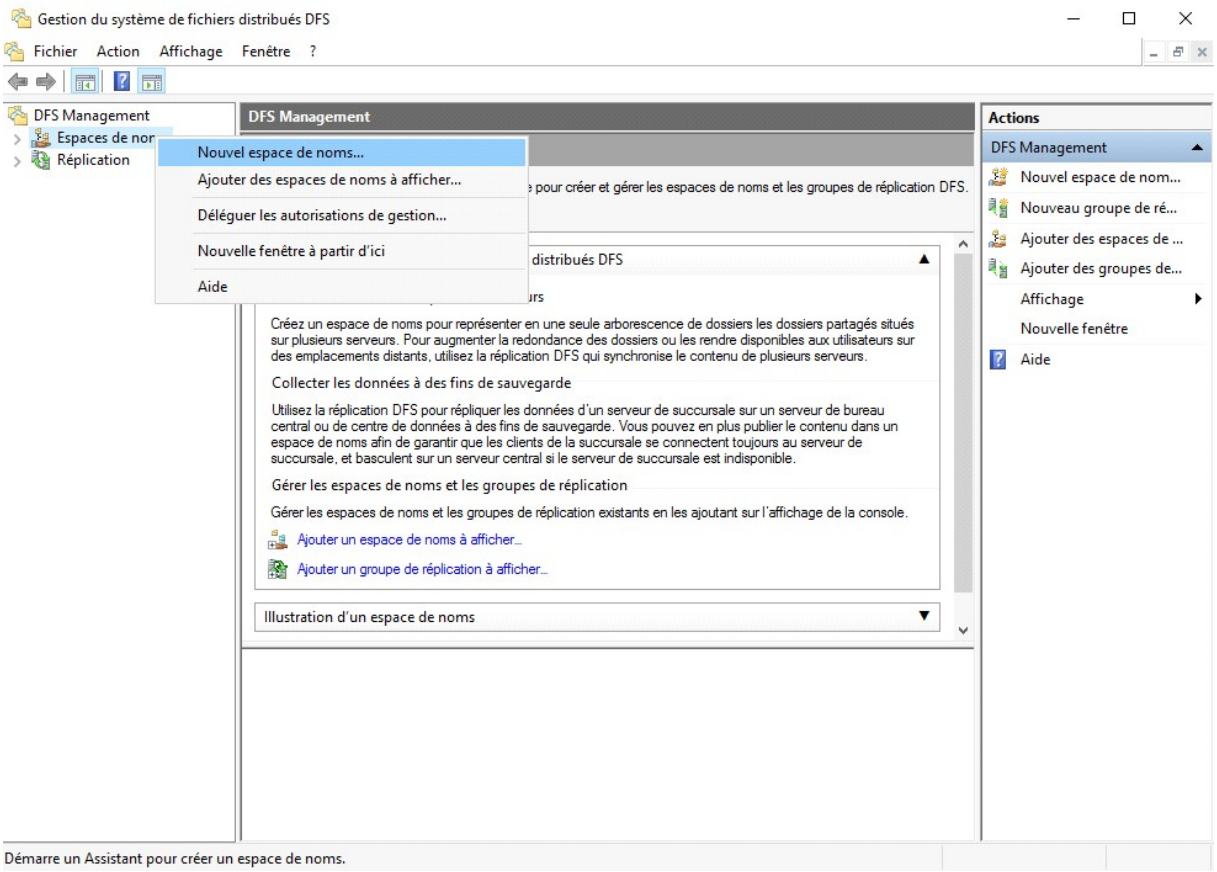
c) DFS

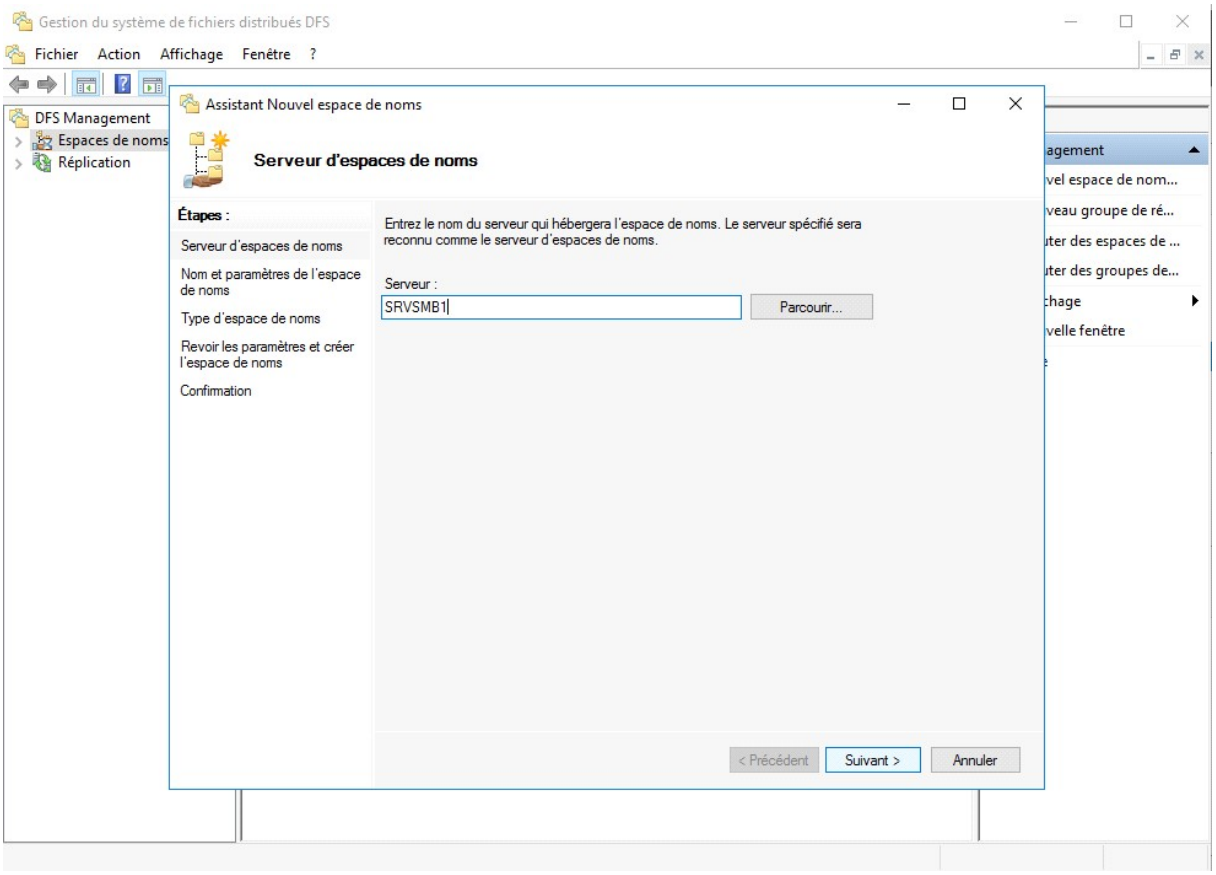
La technologie Distributed File System (DFS), en français «Système de fichiers distribué » est un ensemble de services client et serveur permettant :

- de fournir une arborescence logique aux données partagées depuis des emplacements différents,
- de rassembler différents partages de fichiers à un endroit unique de façon transparente,
- d'assurer la redondance et la disponibilité des données grâce à la réplication. (source Wikipédia)

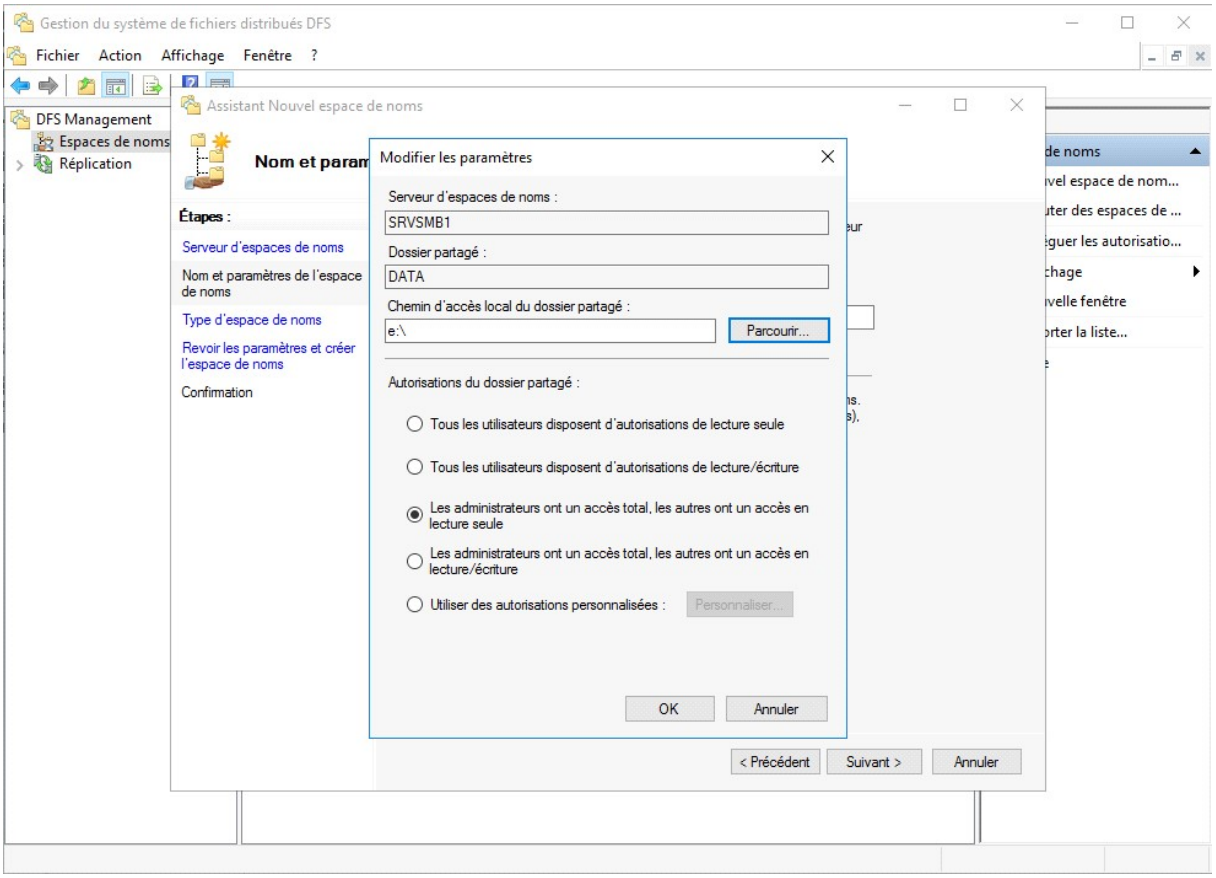
Les utilisateurs Windows vont utiliser le DFS pour pouvoir travailler sur des dossiers communs avec les utilisateurs Linux qui eux utiliseront le NFS. Nous y reviendrons plus tard.

(1) Installation NFS

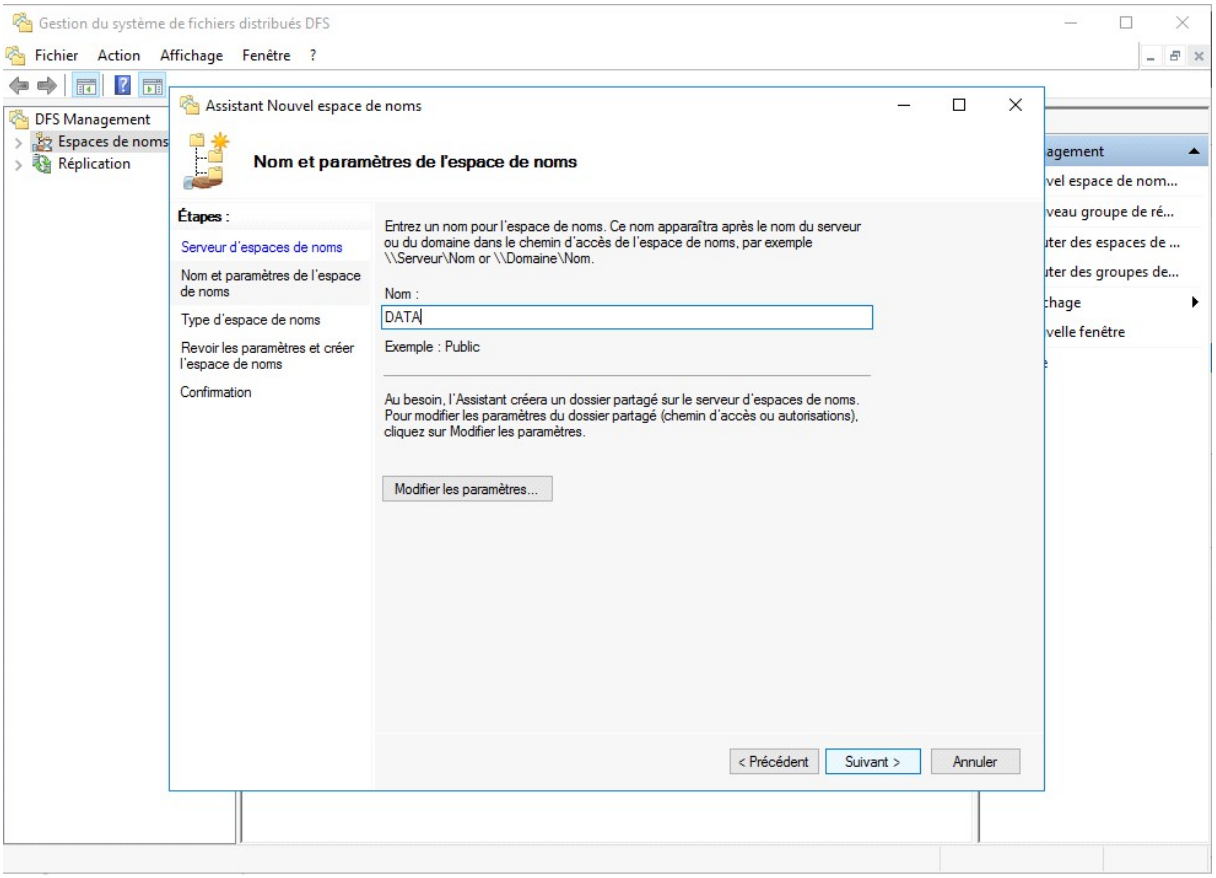




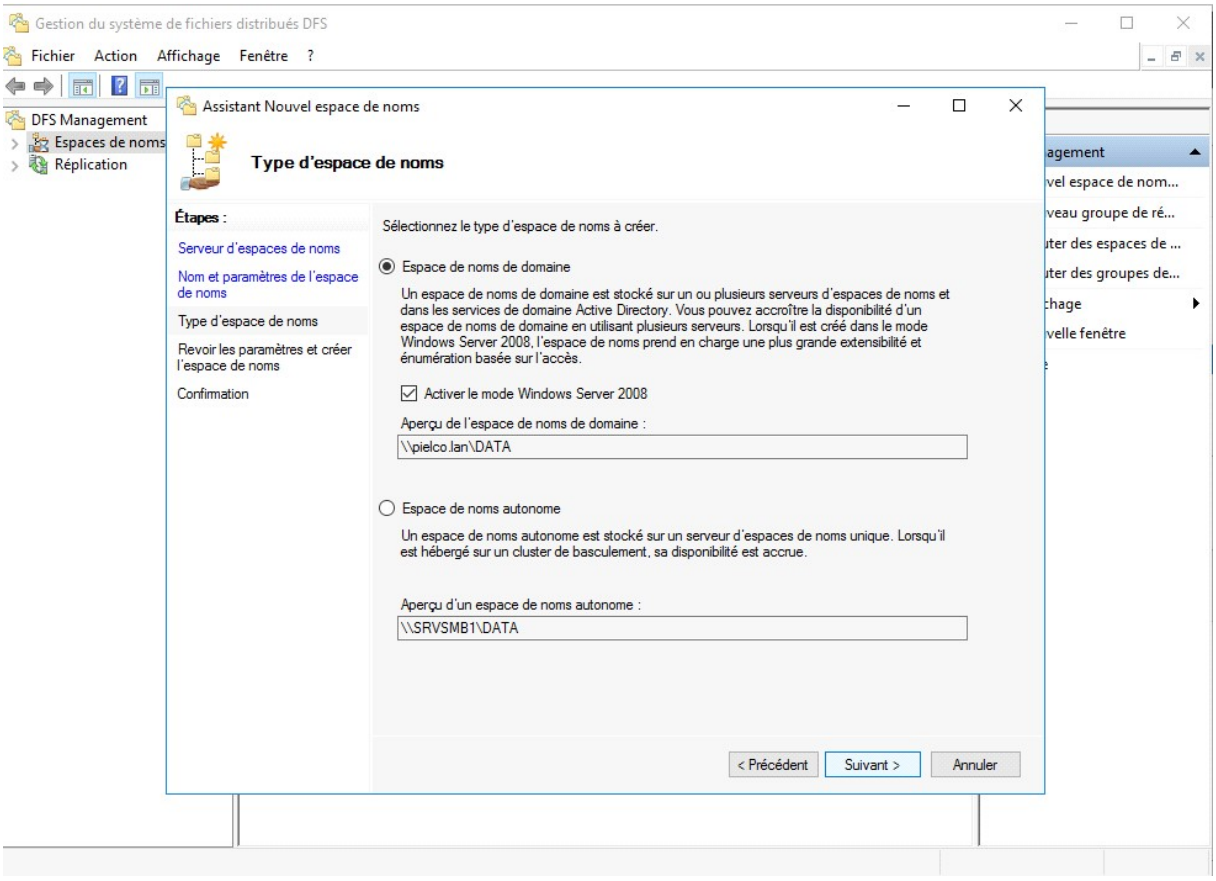
On indique le nom du serveur qui hébergera l'espace de nom



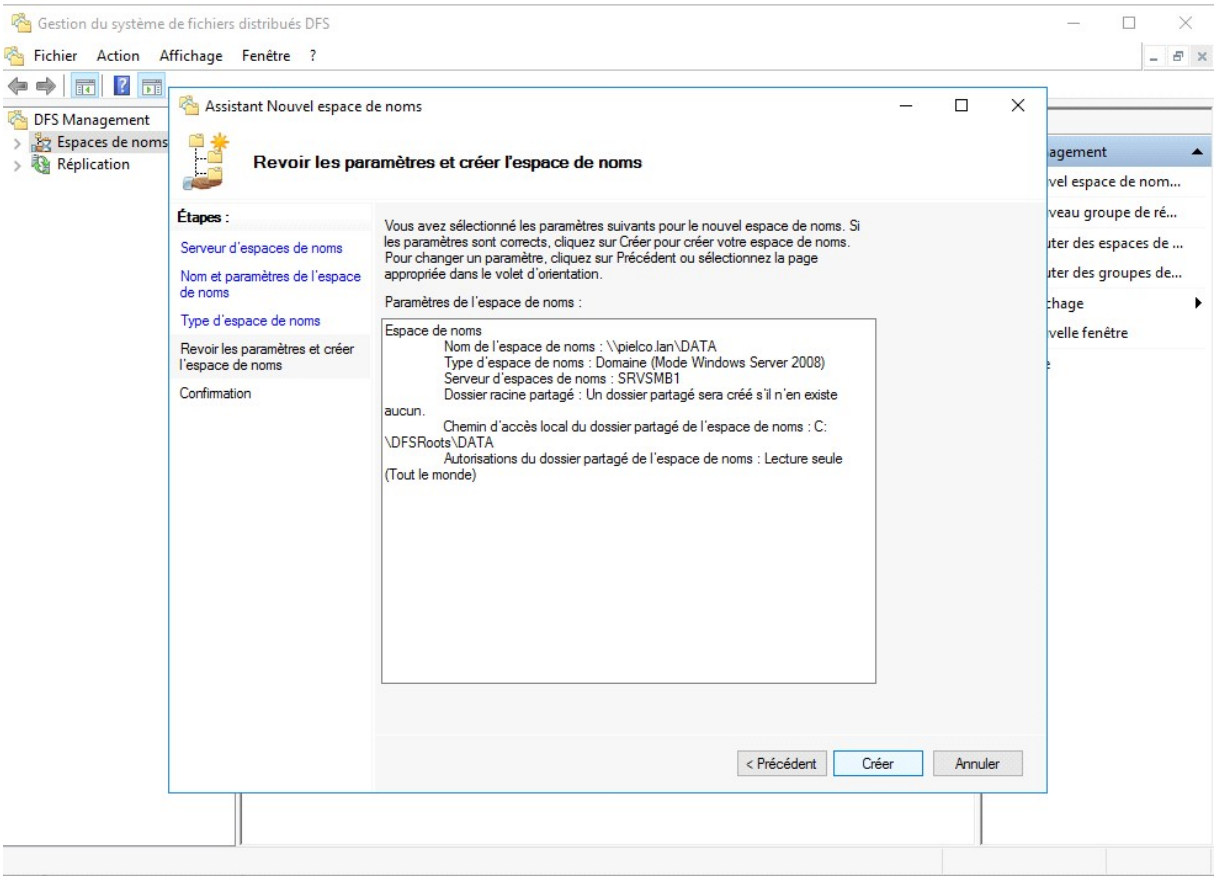
On y renseigne le chemin d'accès et les droits



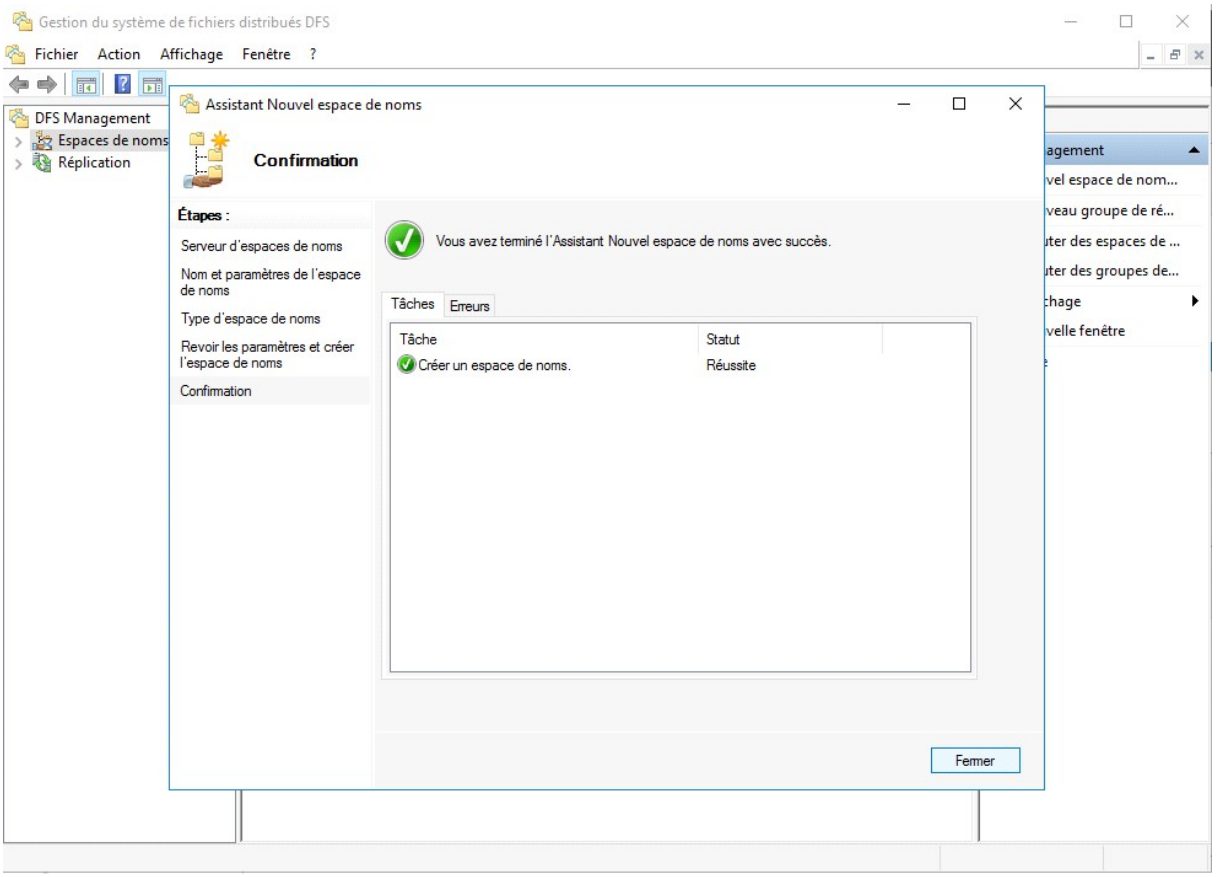
On donne un nom à l'espace de nom



On coche espace de nom de domaine et on y renseigne les bonnes données correspondant à notre infrastructure.



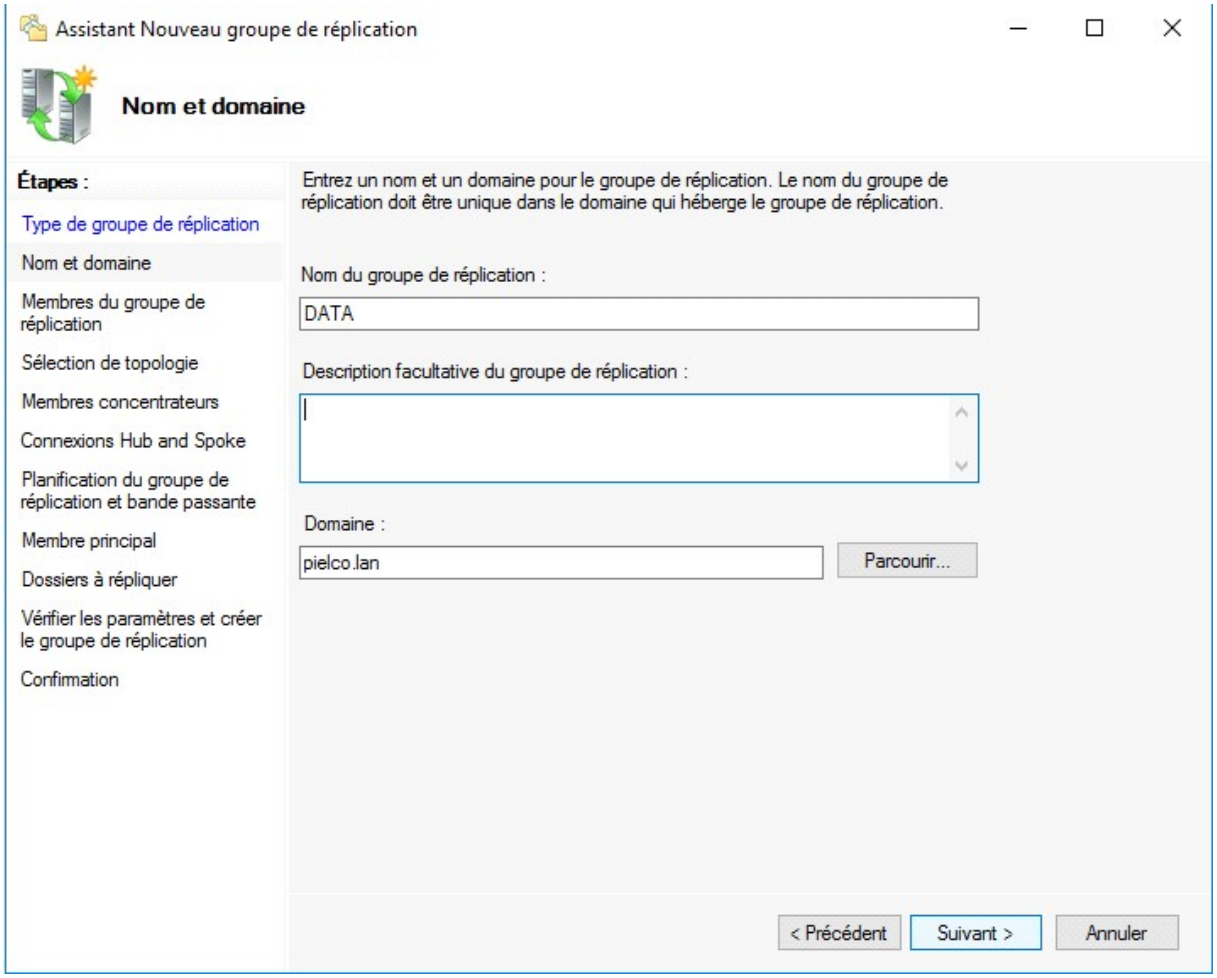
On vérifie une dernière fois que tout est conforme



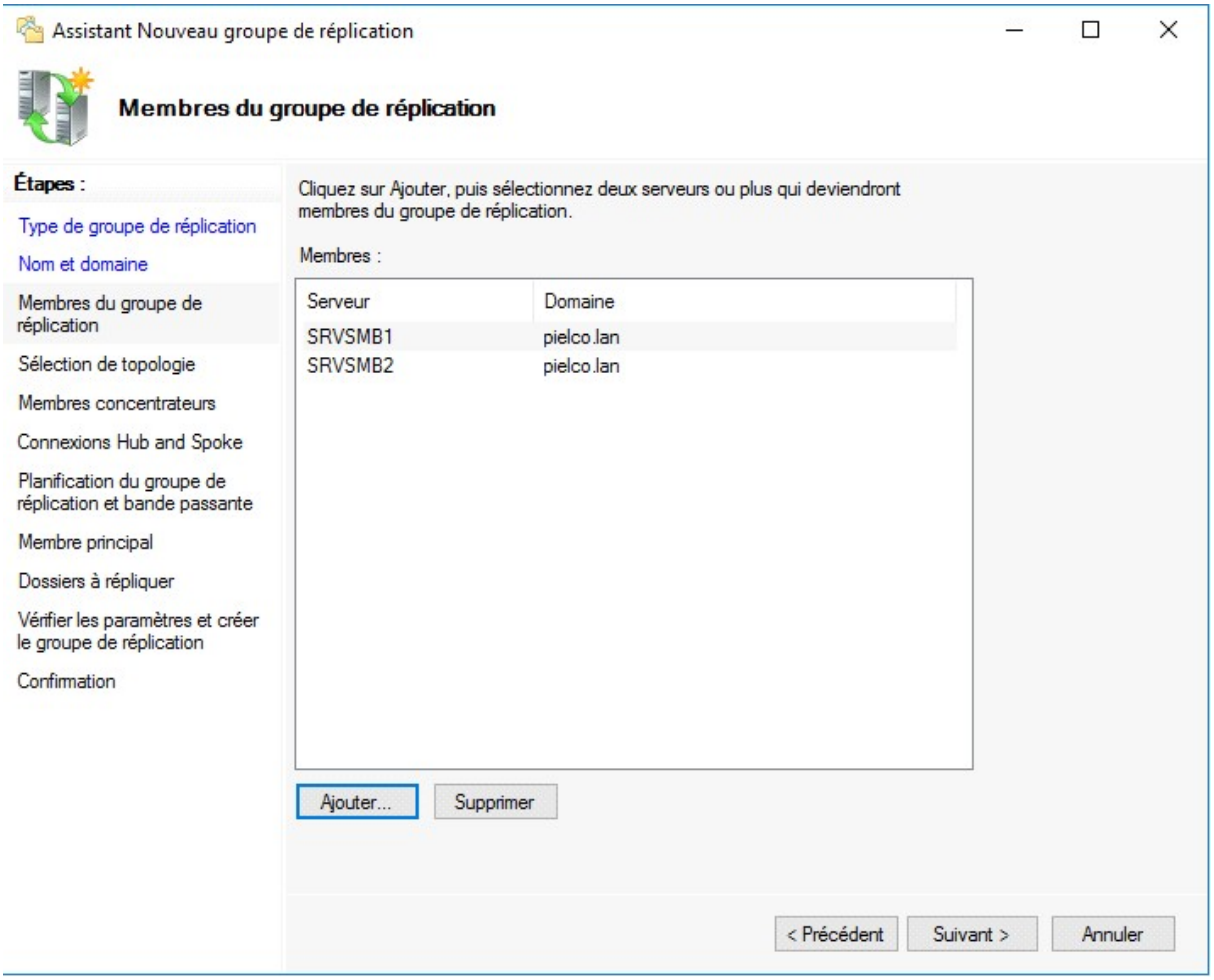
Une fois que tout est ok, nous un avons paramétré un service DFS avec espace de nom

(2) Réplication

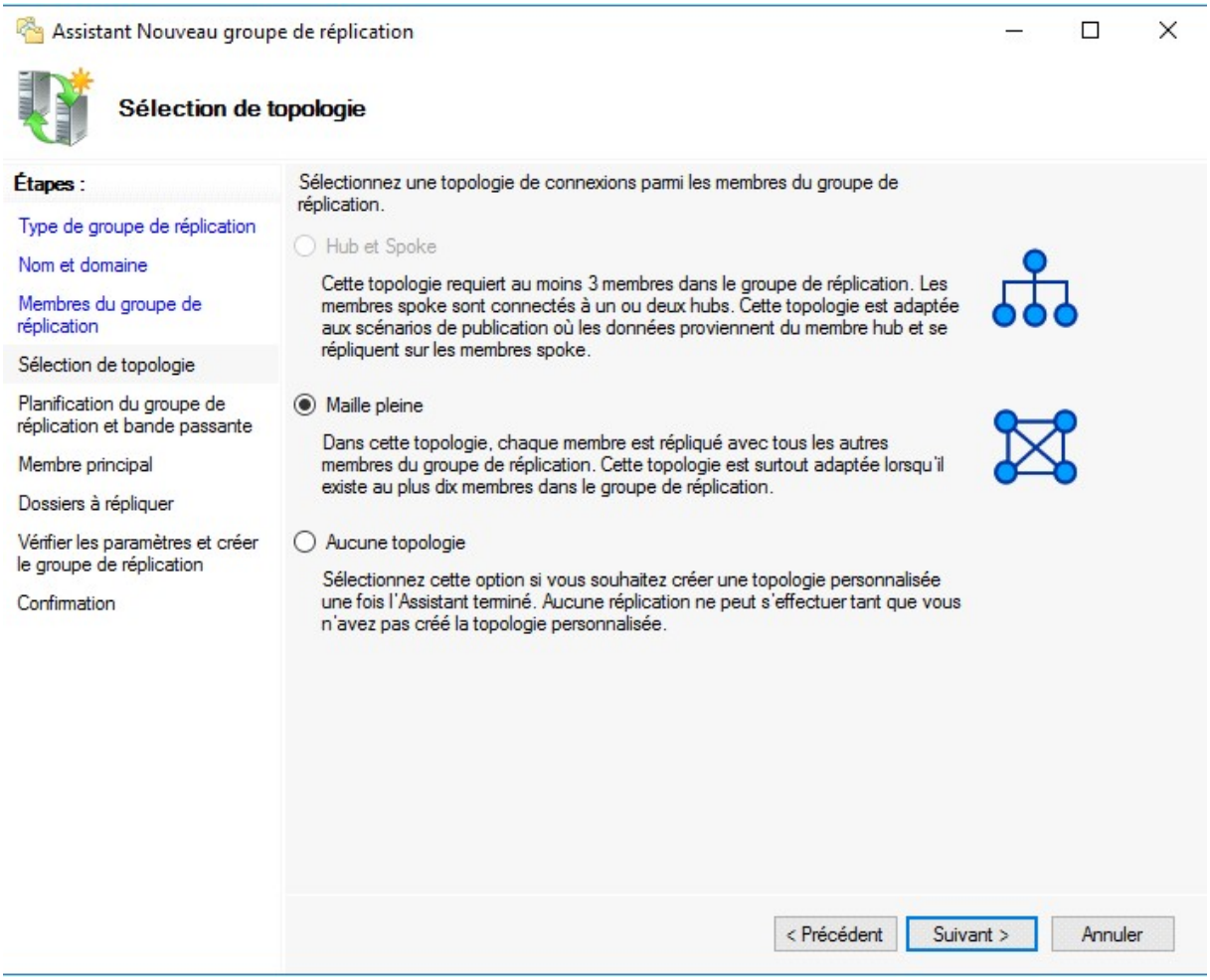
Une fois paramétré, par sécurité nous faisons une réplication du DFS. Toujours dans l'optique de répondre au cahier des charges et d'avoir un uptime du service maximal.



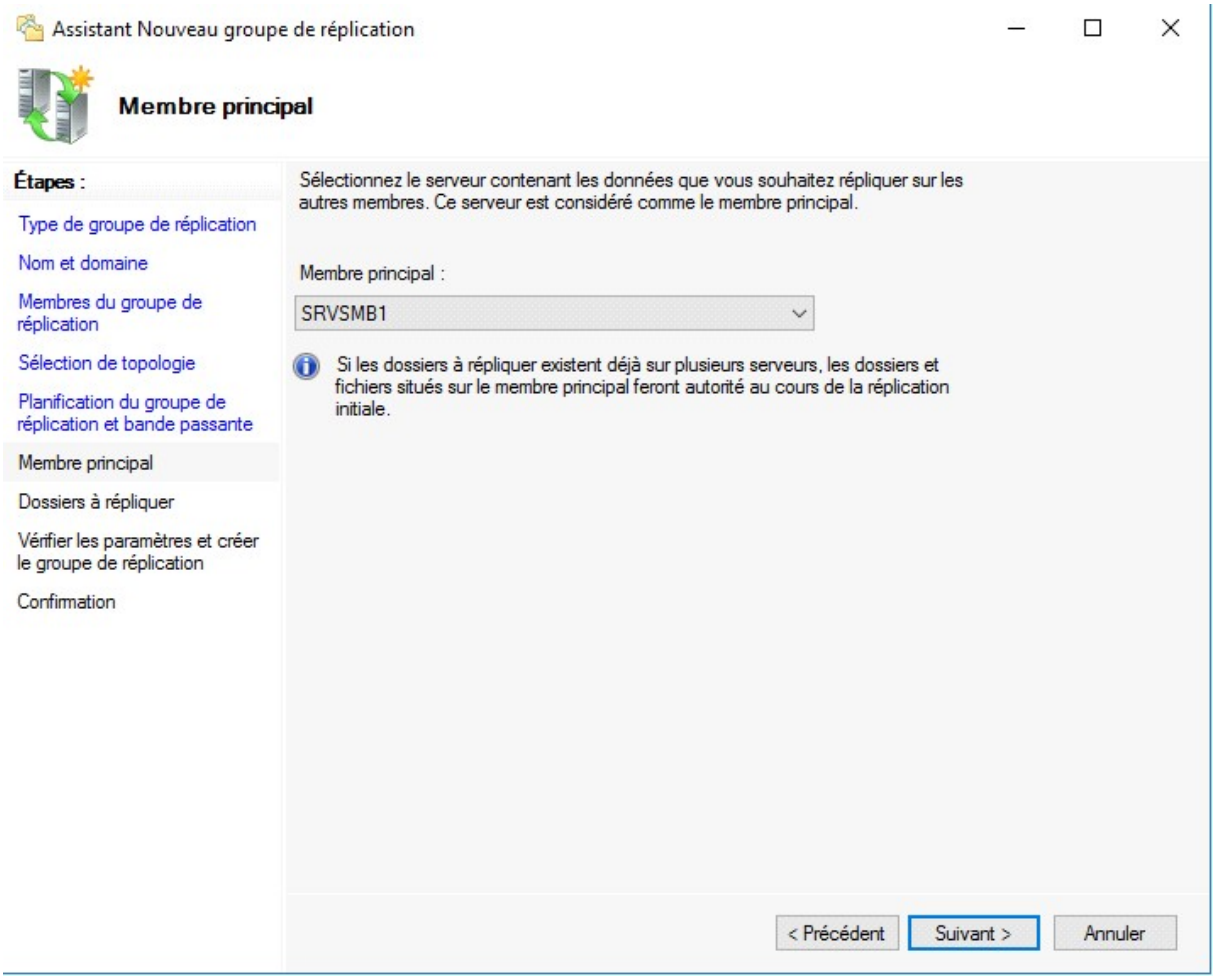
On donne un nom au groupe de réplication



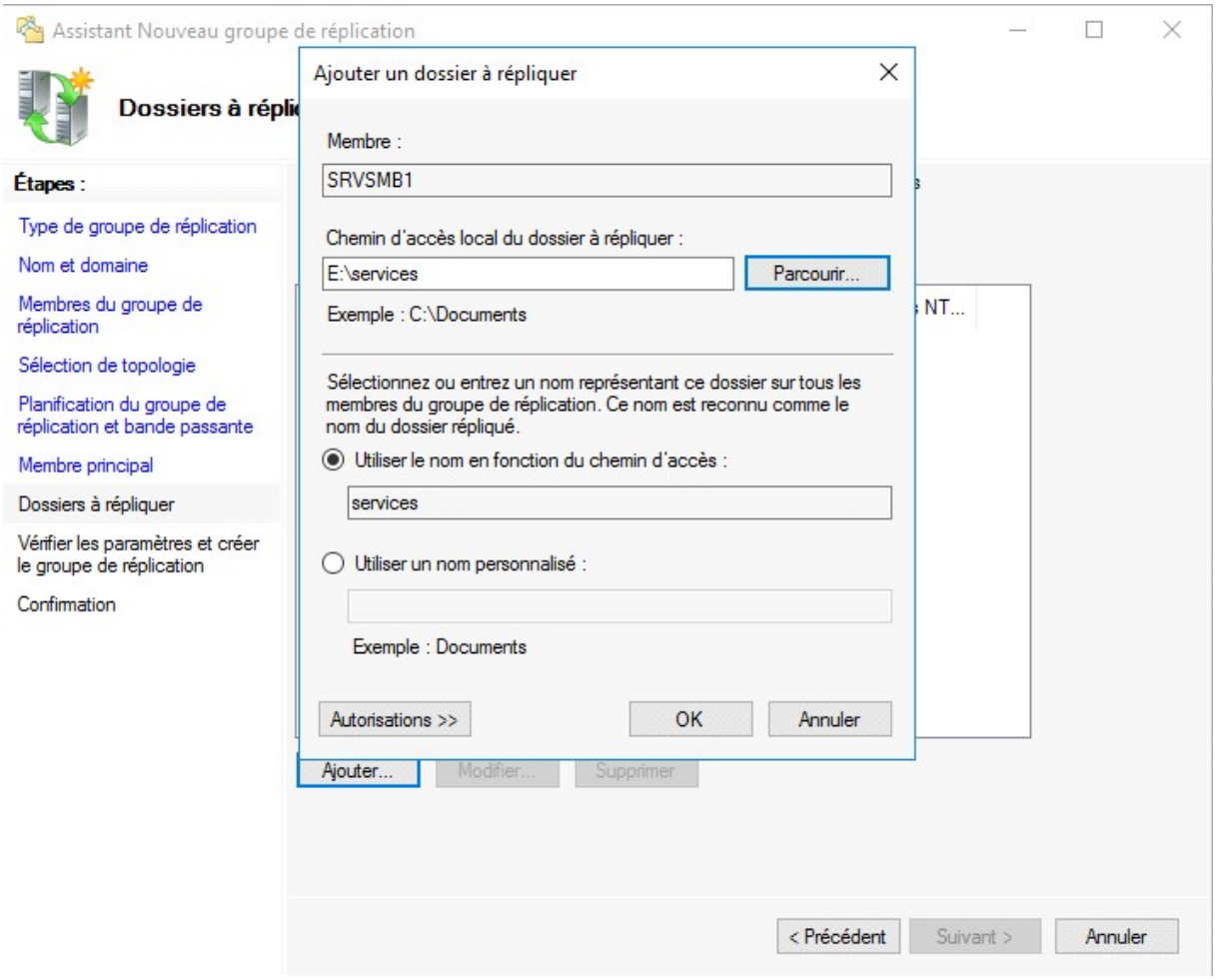
On indique quel serveur est à rajouter à ce groupe de réplication



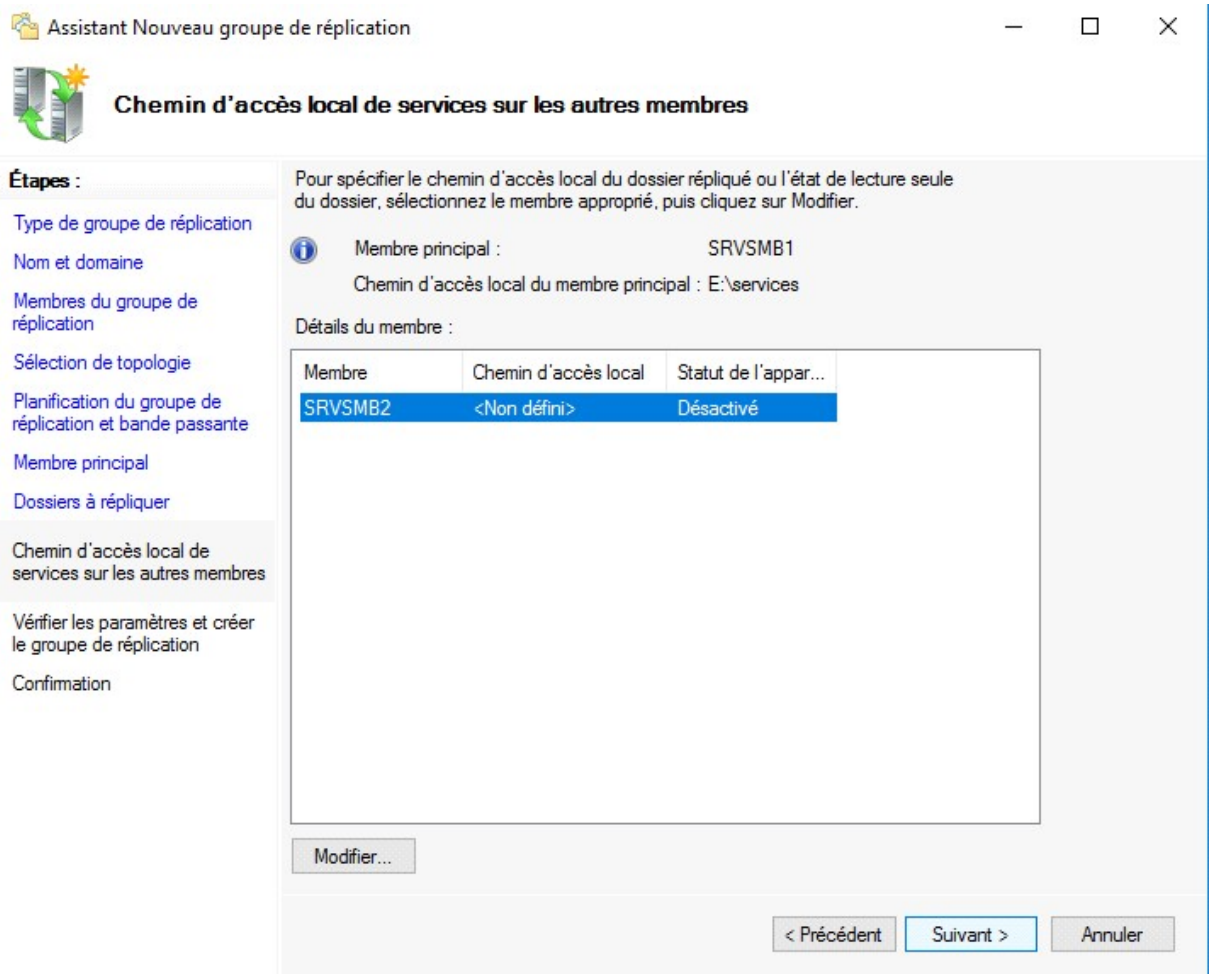
Ici on choisit la topologie souhaitée. En choisissant Maille pleine, son s'assure une réplication efficace correspondant à nos besoins.



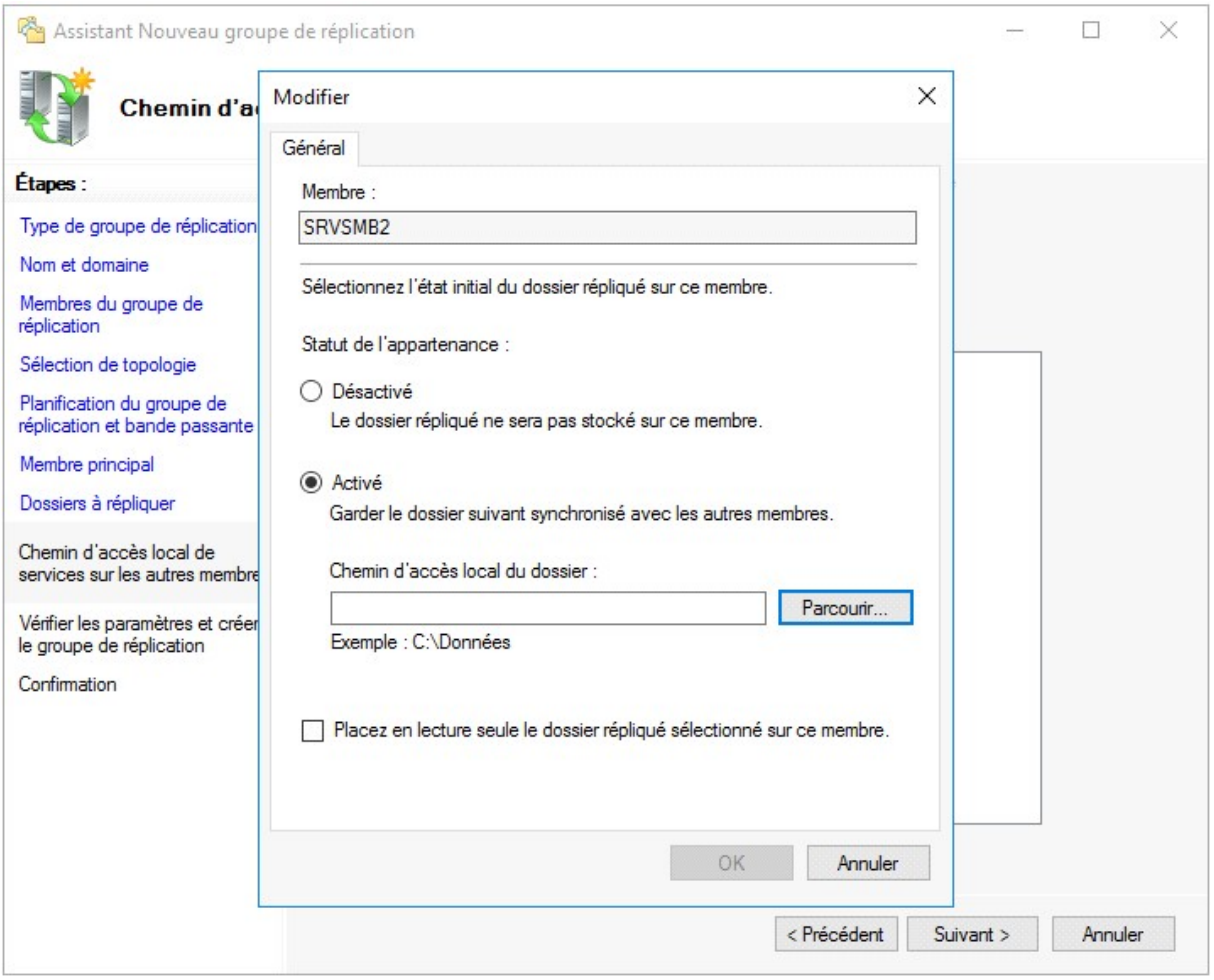
On indique le serveur principal à partir duquel les données vont être répliquées. Dans notre cas, le serveur Samba 1.



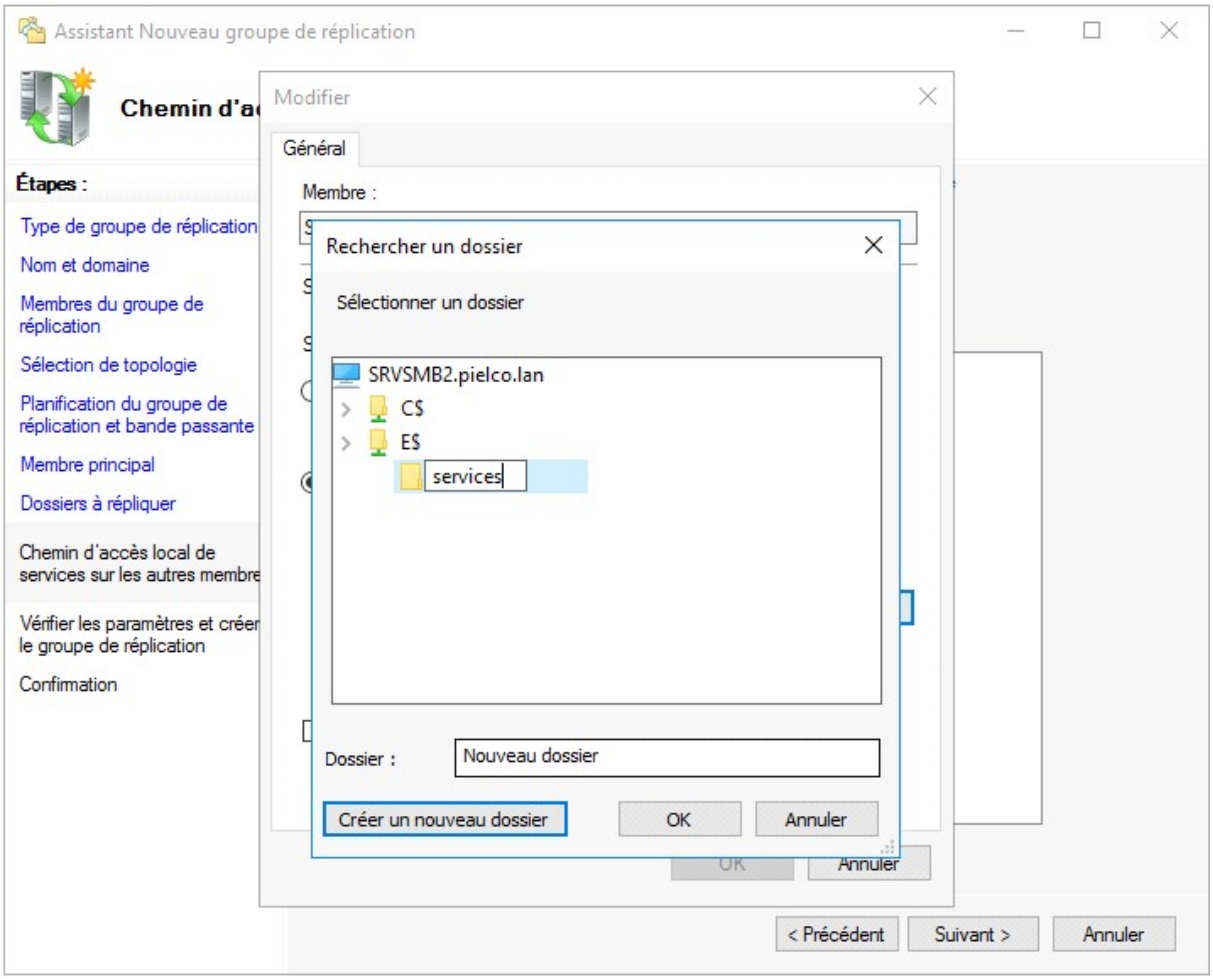
On ajouter un dossier à répliquer



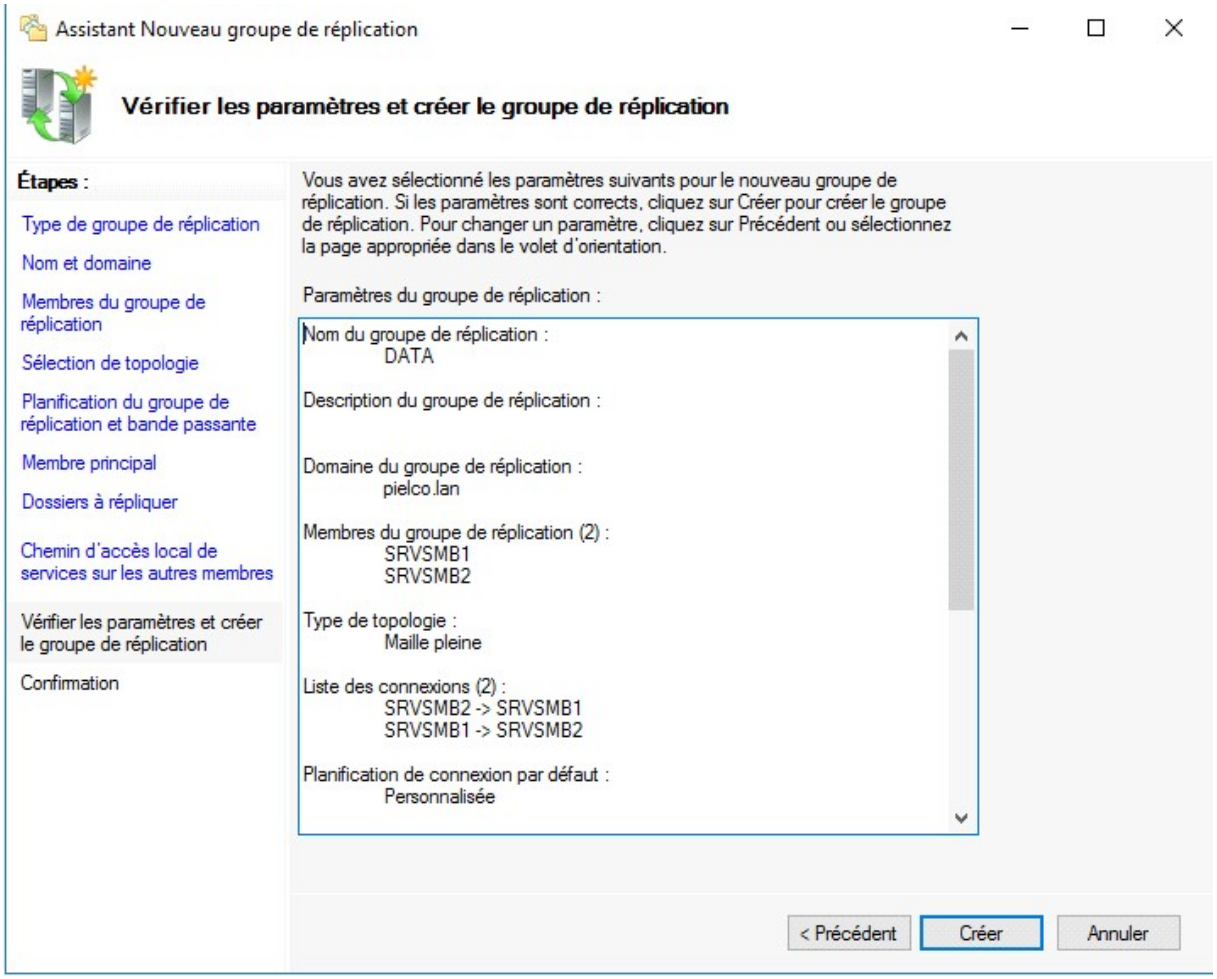
On indique le chemin de réplication



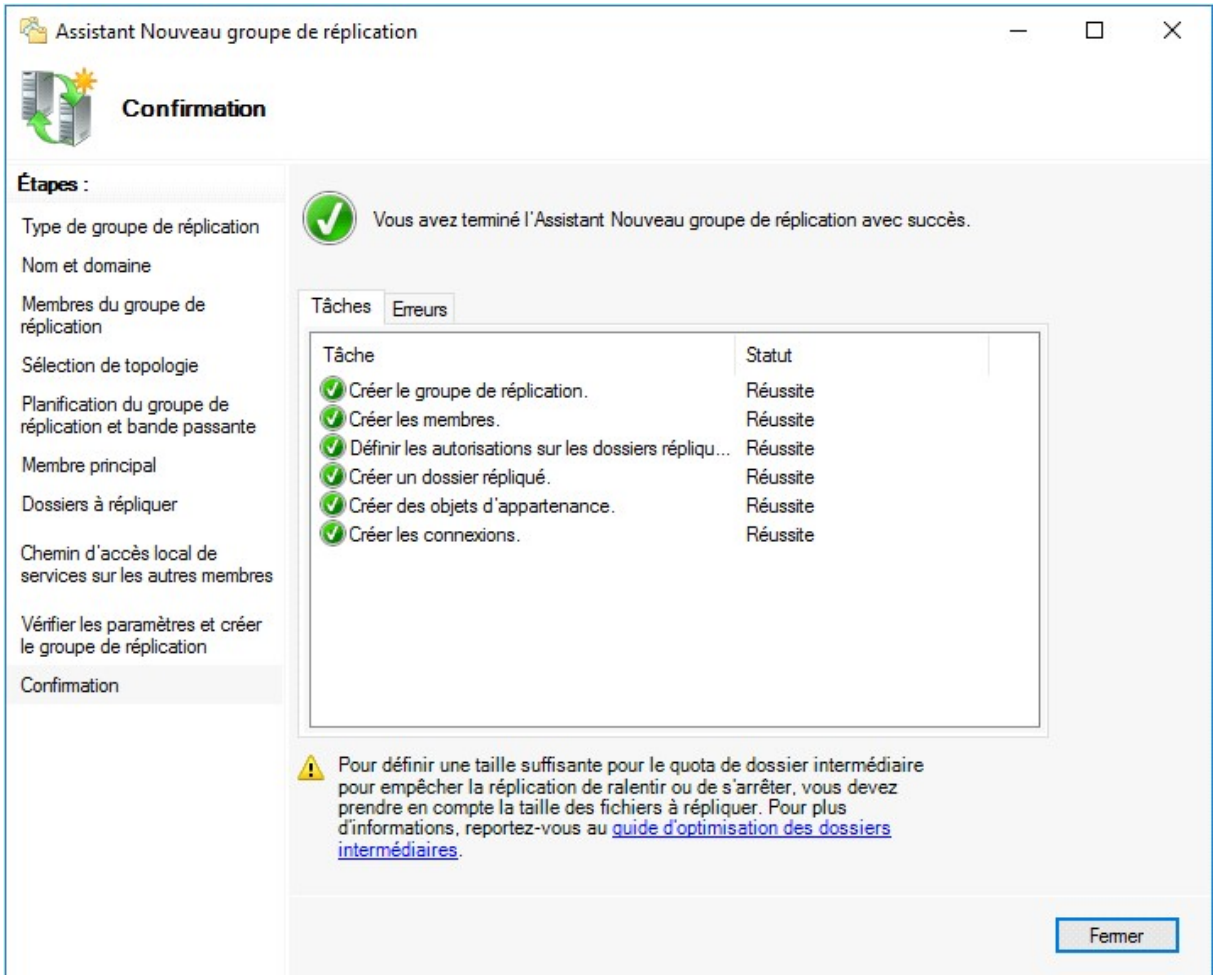
On active la synchronisation avec les autres membres



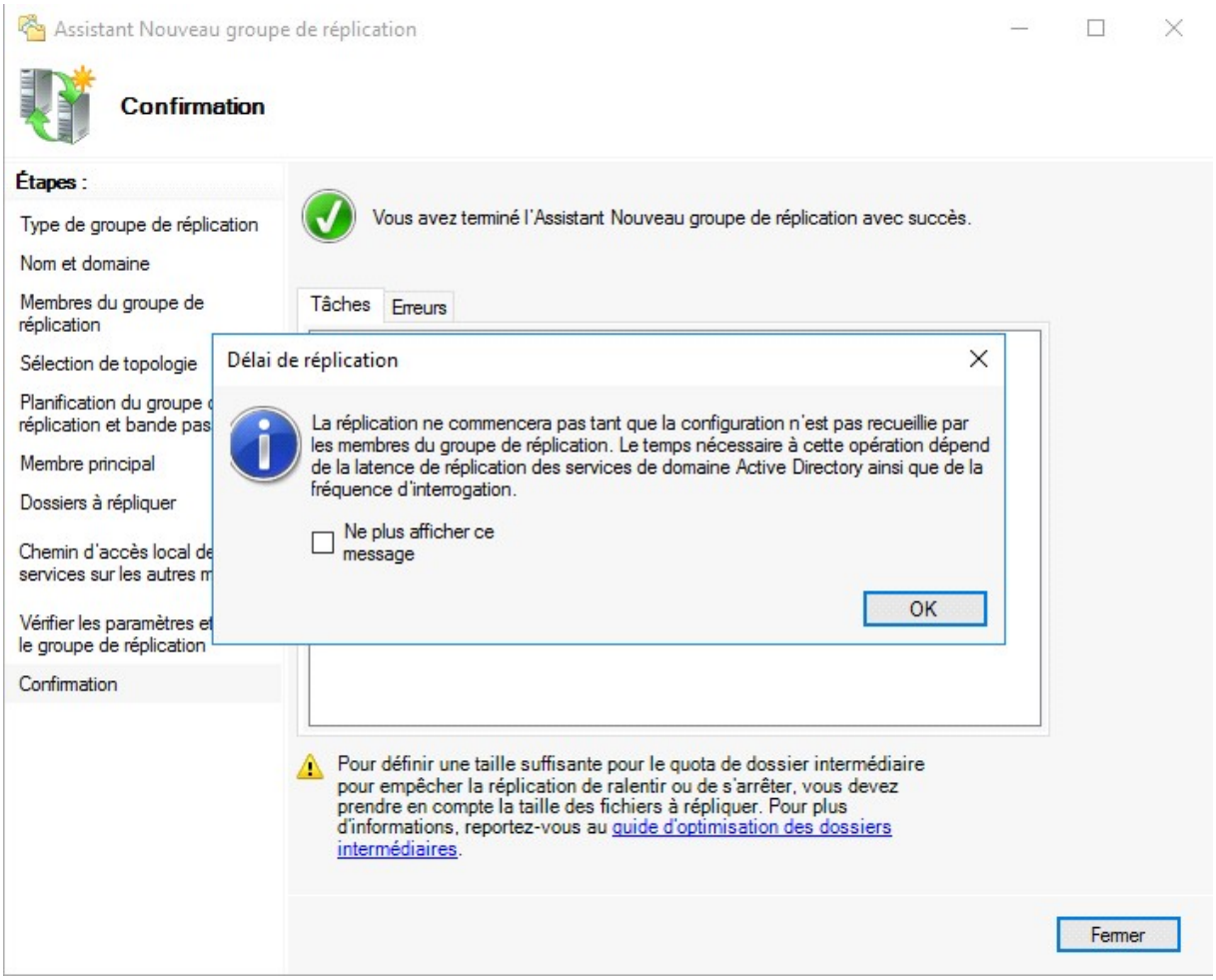
On indique le chemin de destination



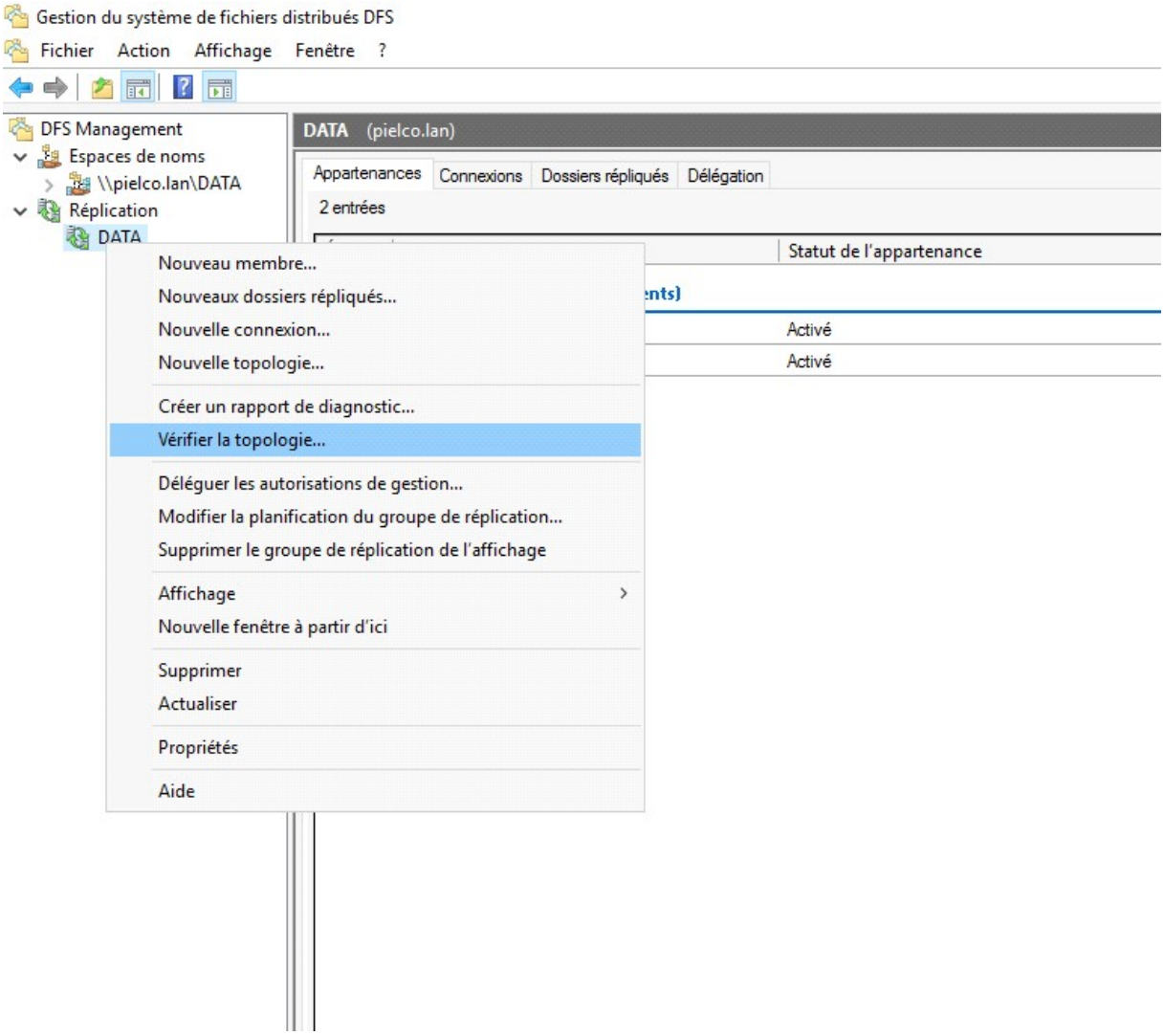
Nous avons un récapitulatif des paramètres de groupe de réplication



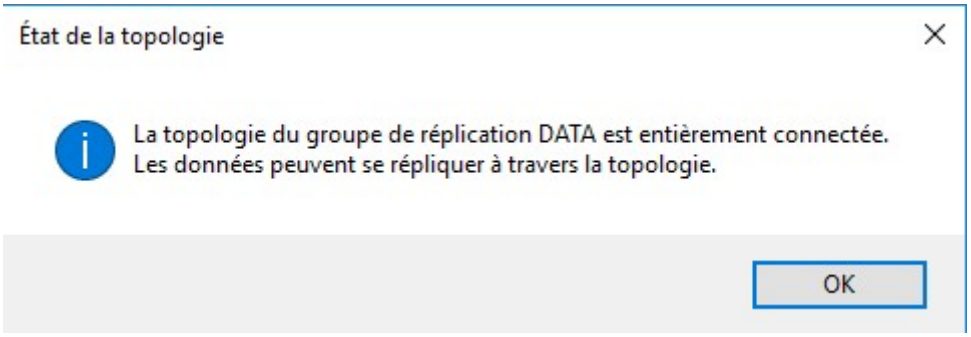
La réplication s'est bien faite, cependant on doit définir un quota suffisant afin de ne pas ralentir la réplication



L'assistant de réplication nous indique qu'une latence entre les premières réplications dépend de



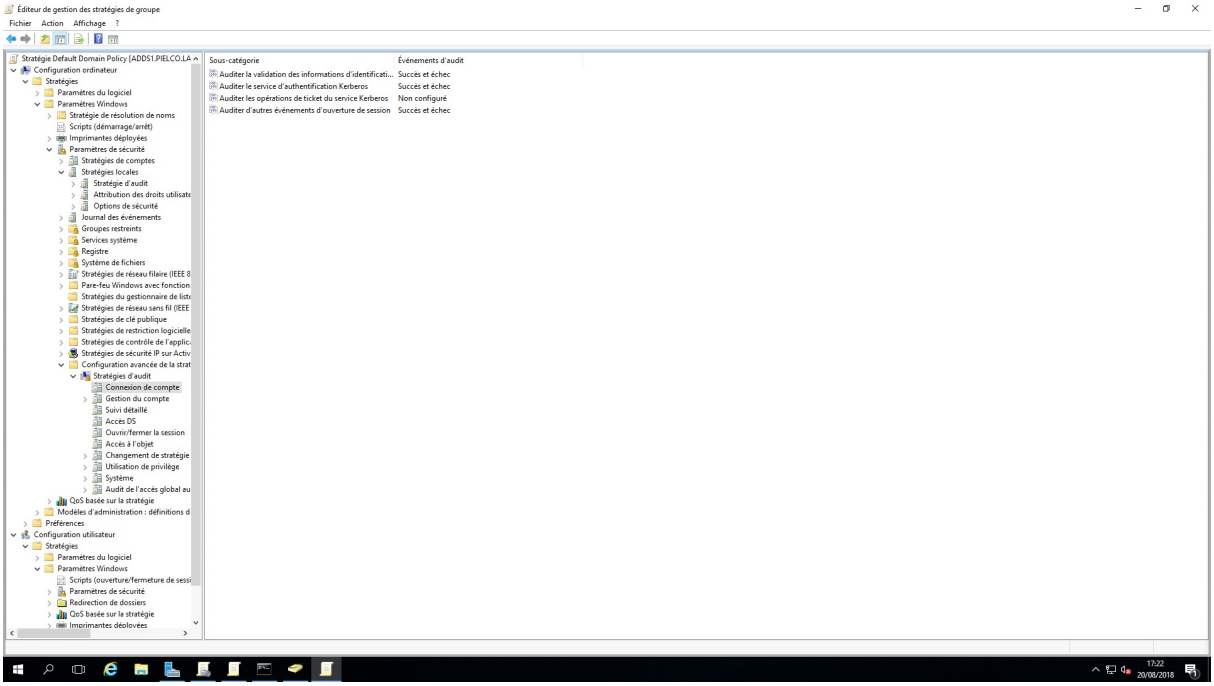
On vérifie l'état de la topologie pour savoir si la réplication est ok.

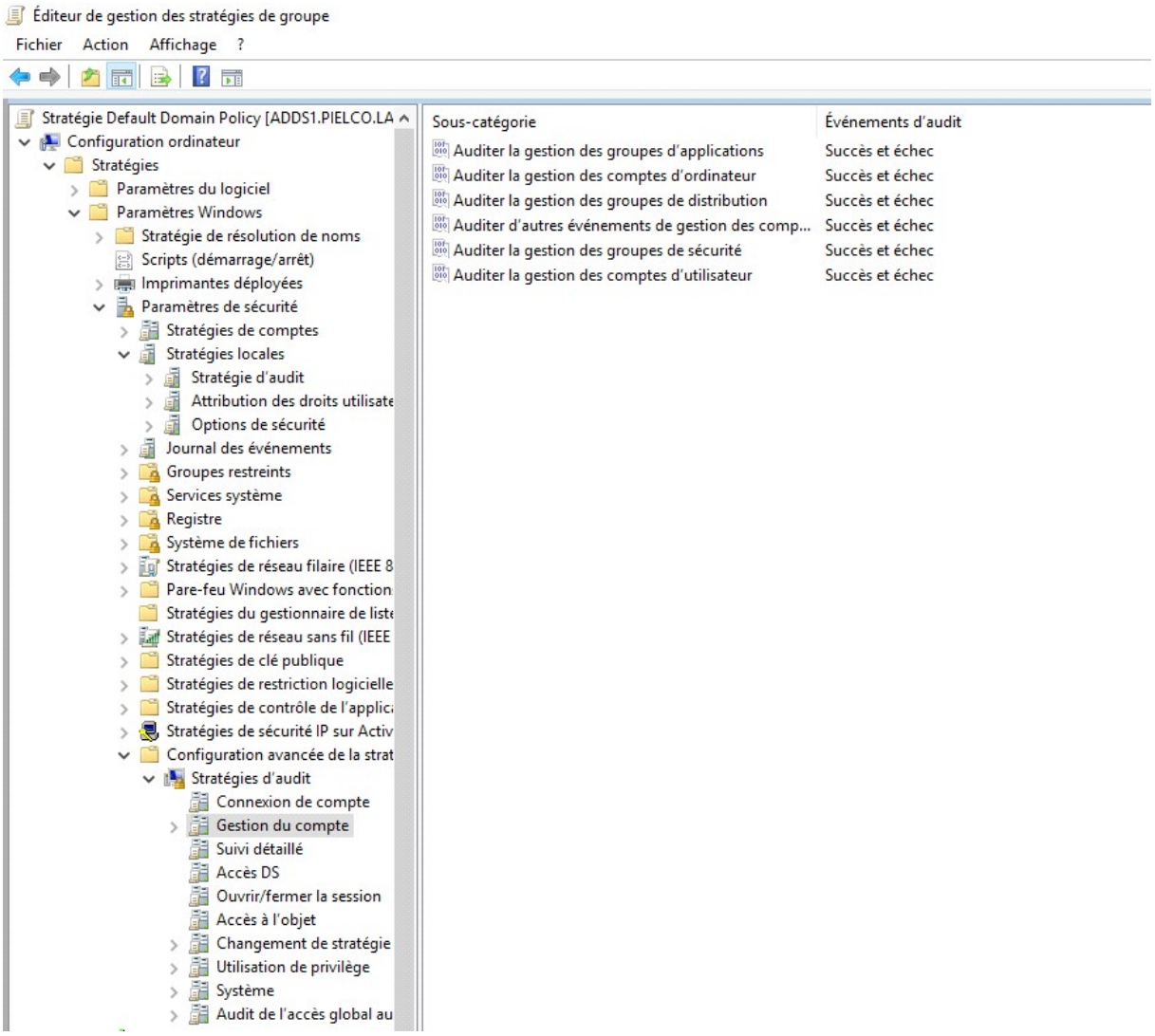


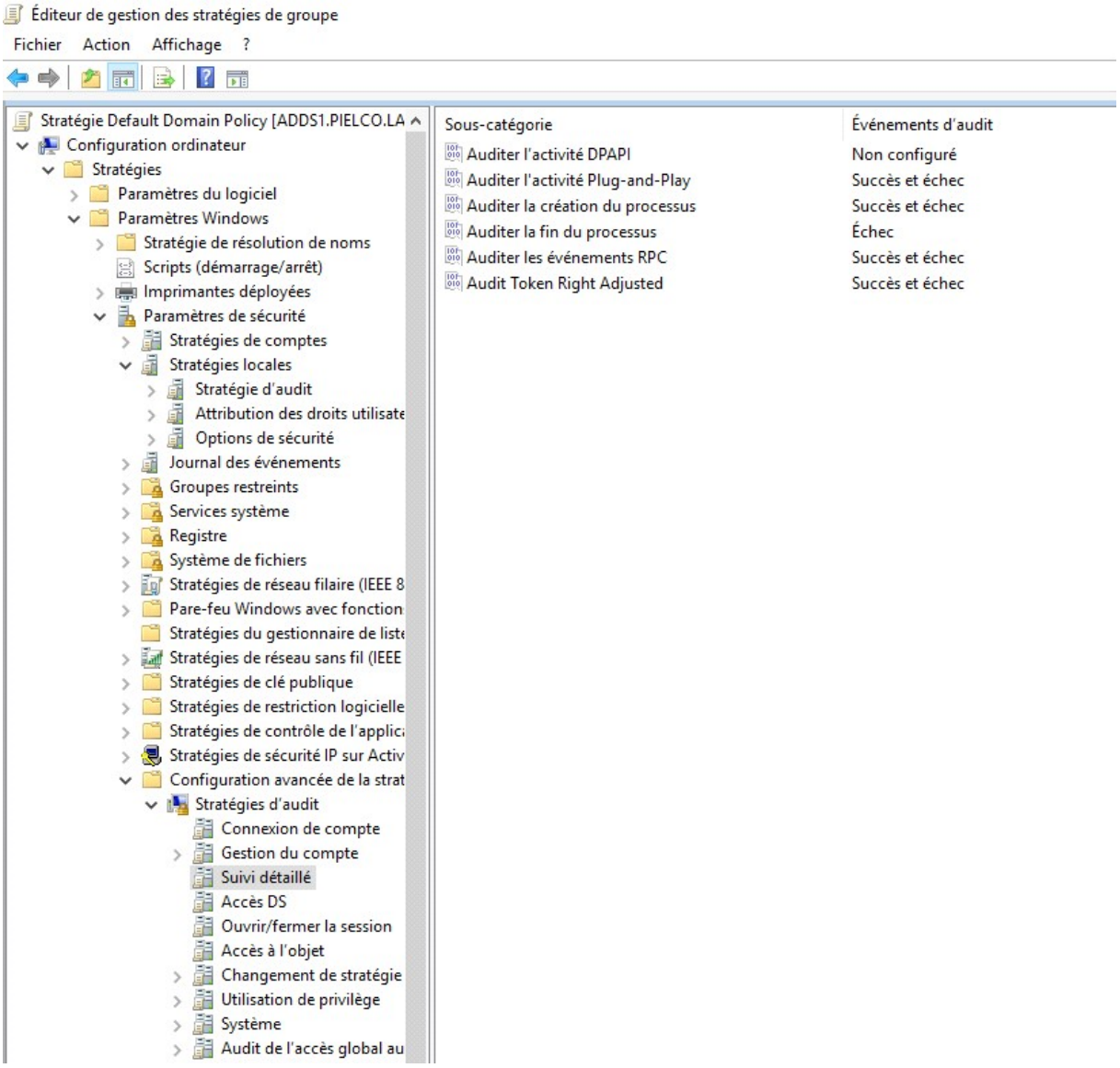
Fini, la réplication est effective.

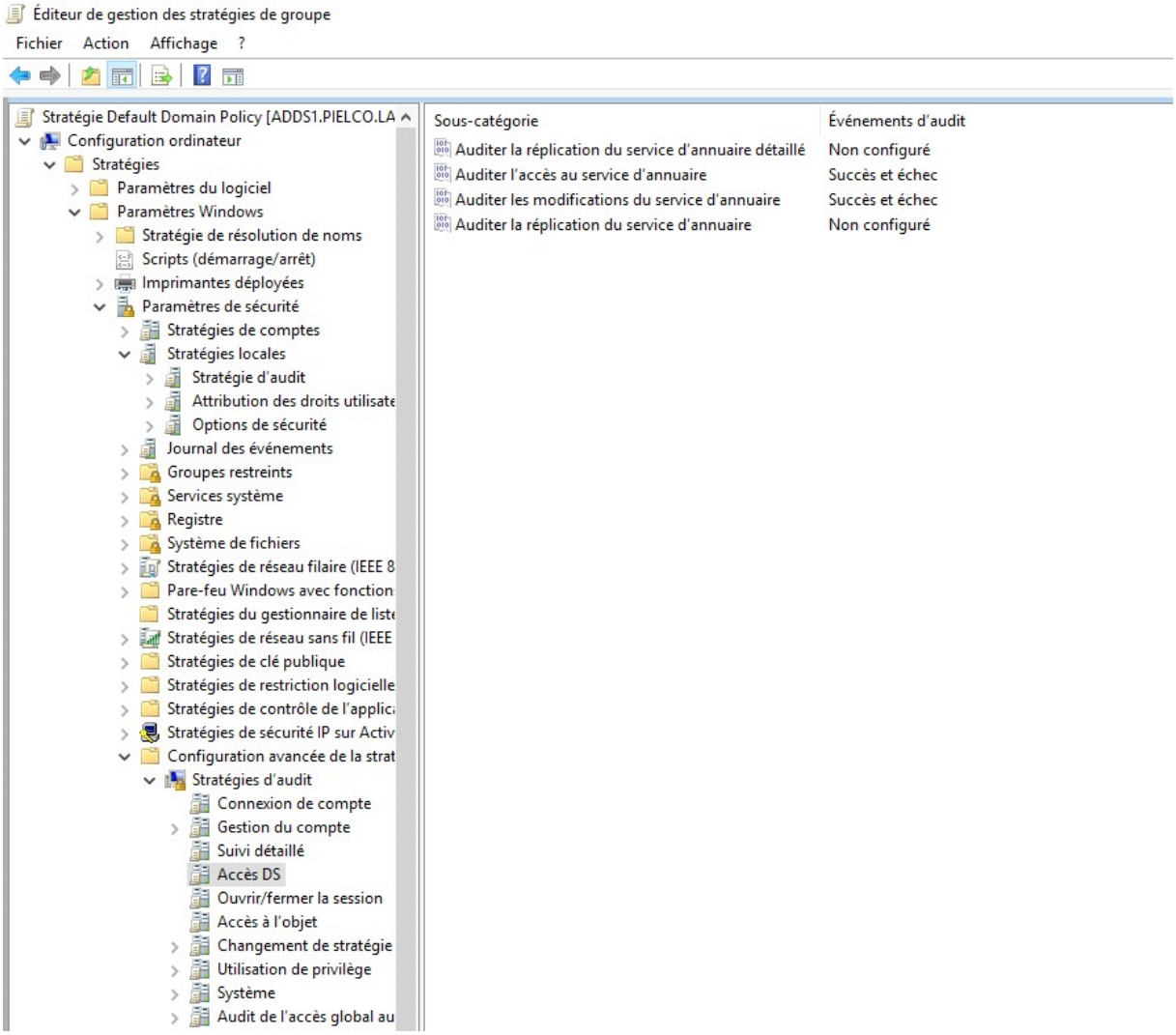
(3) Audits

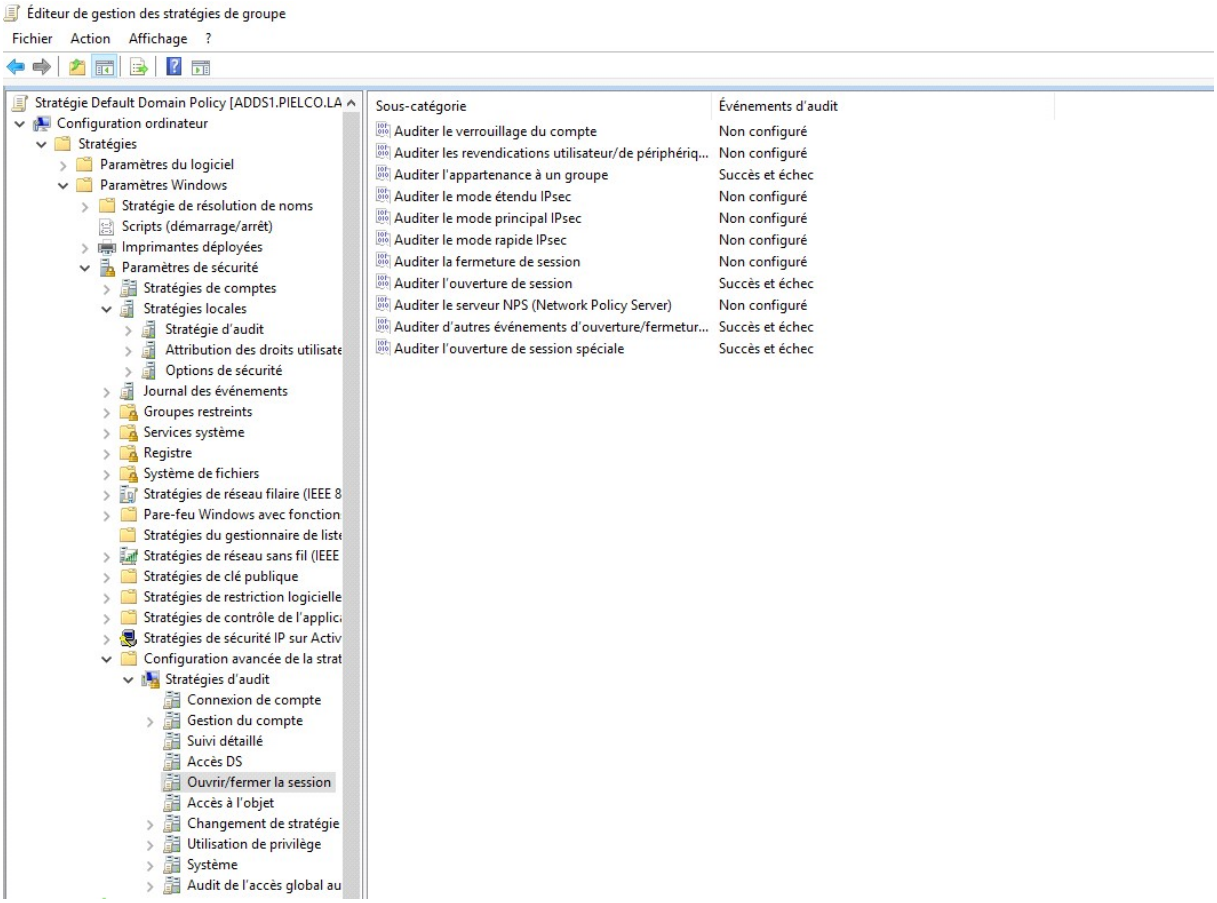
Dans le cahier des charges il nous est demandé de prévoir au hasard des audits afin de générer des logs pour chaque évènement fait par un ou plusieurs groupes d'utilisateurs choisis pour des actions, des dossiers / fichiers préalablement identifiés.

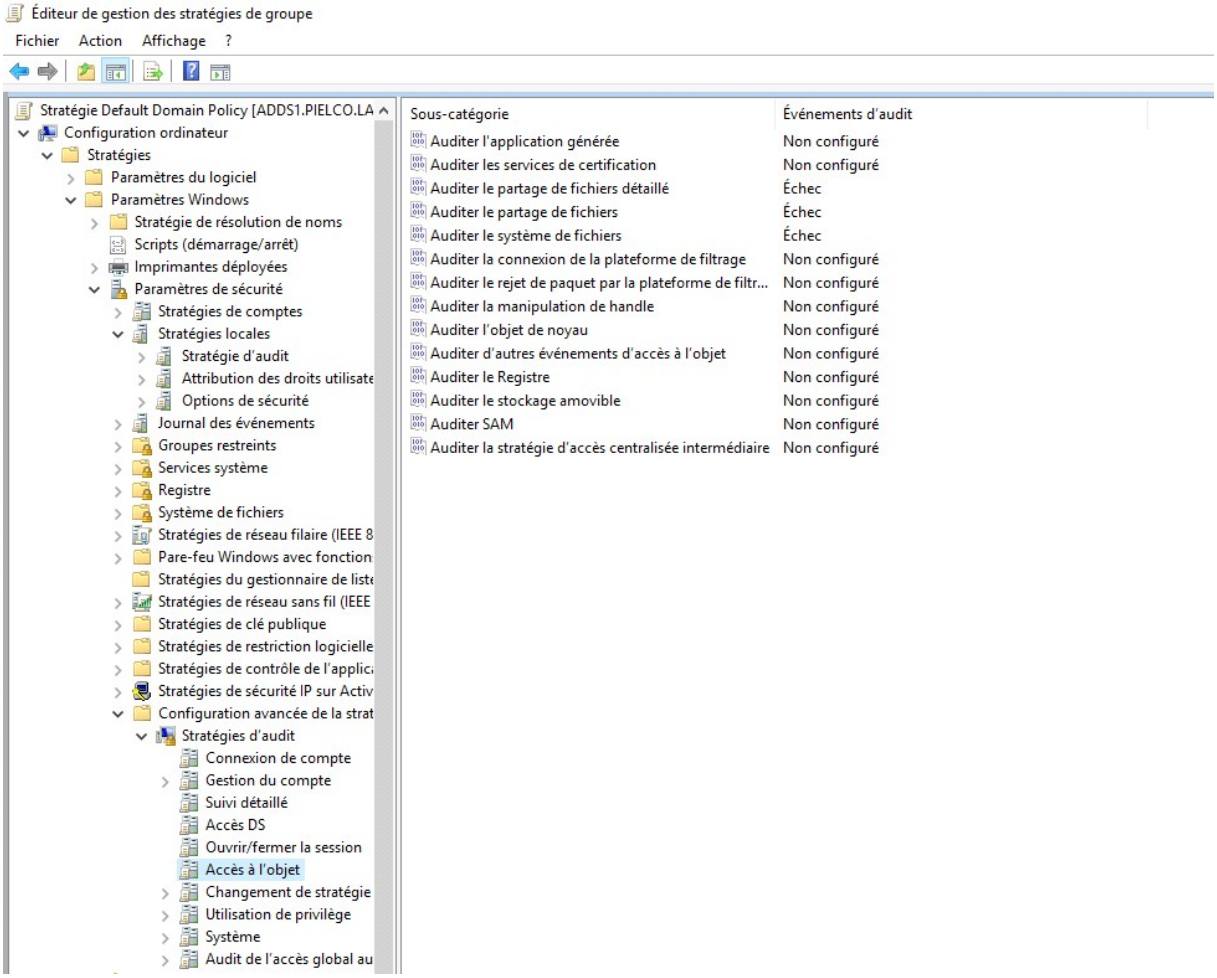


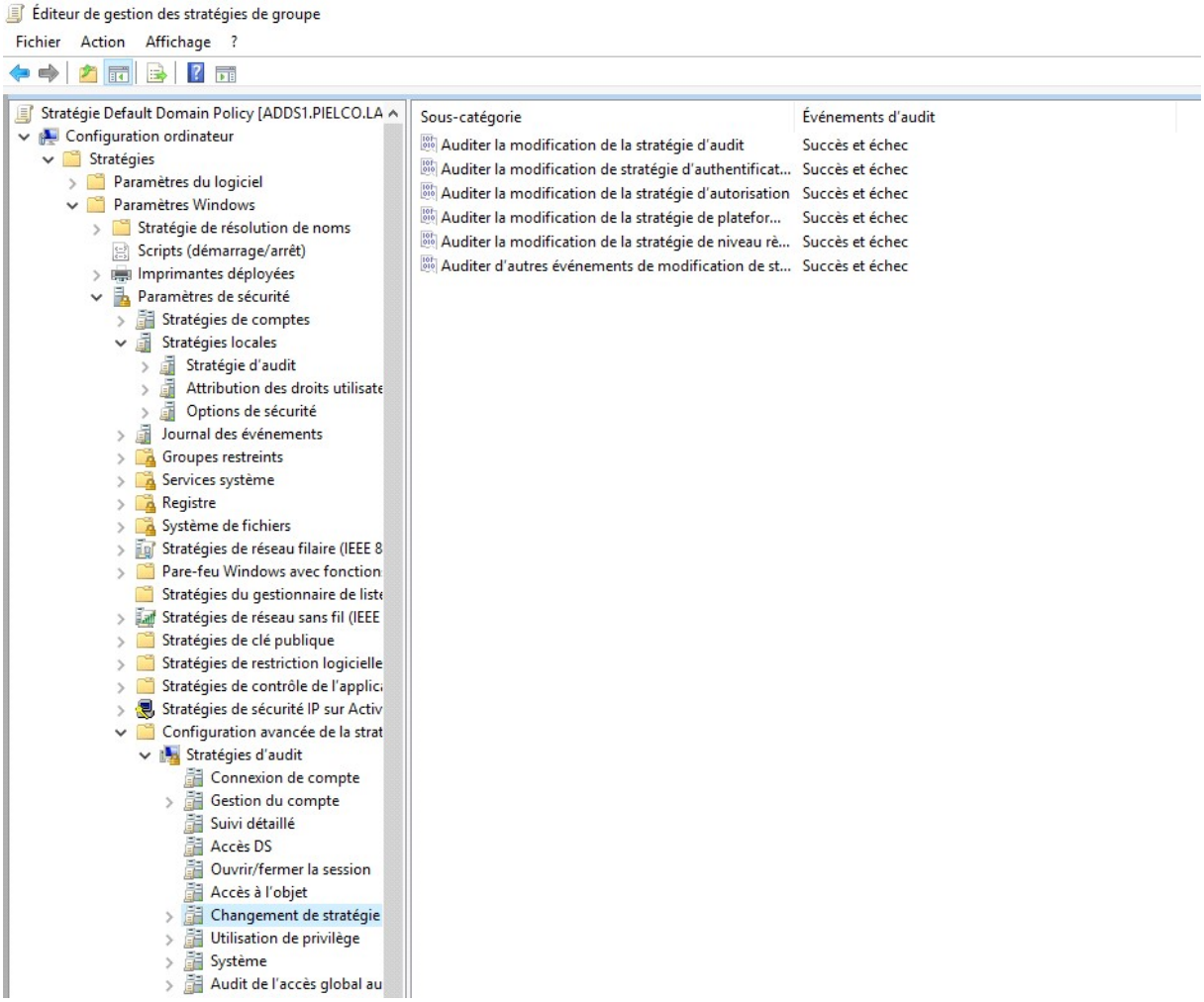

Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie Default Domain Policy [ADDS1.PIELCO.LA
Configuration ordinateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Stratégie de résolution de noms
Scripts (démarrage/arrêt)
Imprimantes déployées
Paramètres de sécurité
Stratégies de comptes
Stratégies locales
Stratégie d'audit
Attribution des droits utilisate
Options de sécurité
Journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de réseau filaire (IEEE 8
Pare-feu Windows avec fonction
Stratégies du gestionnaire de liste
Stratégies de réseau sans fil (IEEE
Stratégies de clé publique
Stratégies de restriction logicielle
Stratégies de contrôle de l'applic
Stratégies de sécurité IP sur Activ
Configuration avancée de la strat
Stratégies d'audit
Connexion de compte
Gestion du compte
Suivi détaillé
Accès DS
Ouvrir/fermer la session
Accès à l'objet
Changement de stratégie
Utilisation de privilège
Système
Audit de l'accès global au
Sous-catégorie
Événements d'audit
Auditer la gestion des groupes d'applications
Succès et échec
Auditer la gestion des comptes d'ordinateur
Succès et échec
Auditer la gestion des groupes de distribution
Succès et échec
Auditer d'autres événements de gestion des comp...
Succès et échec
Auditer la gestion des groupes de sécurité
Succès et échec
Auditer la gestion des comptes d'utilisateur
Succès et échec

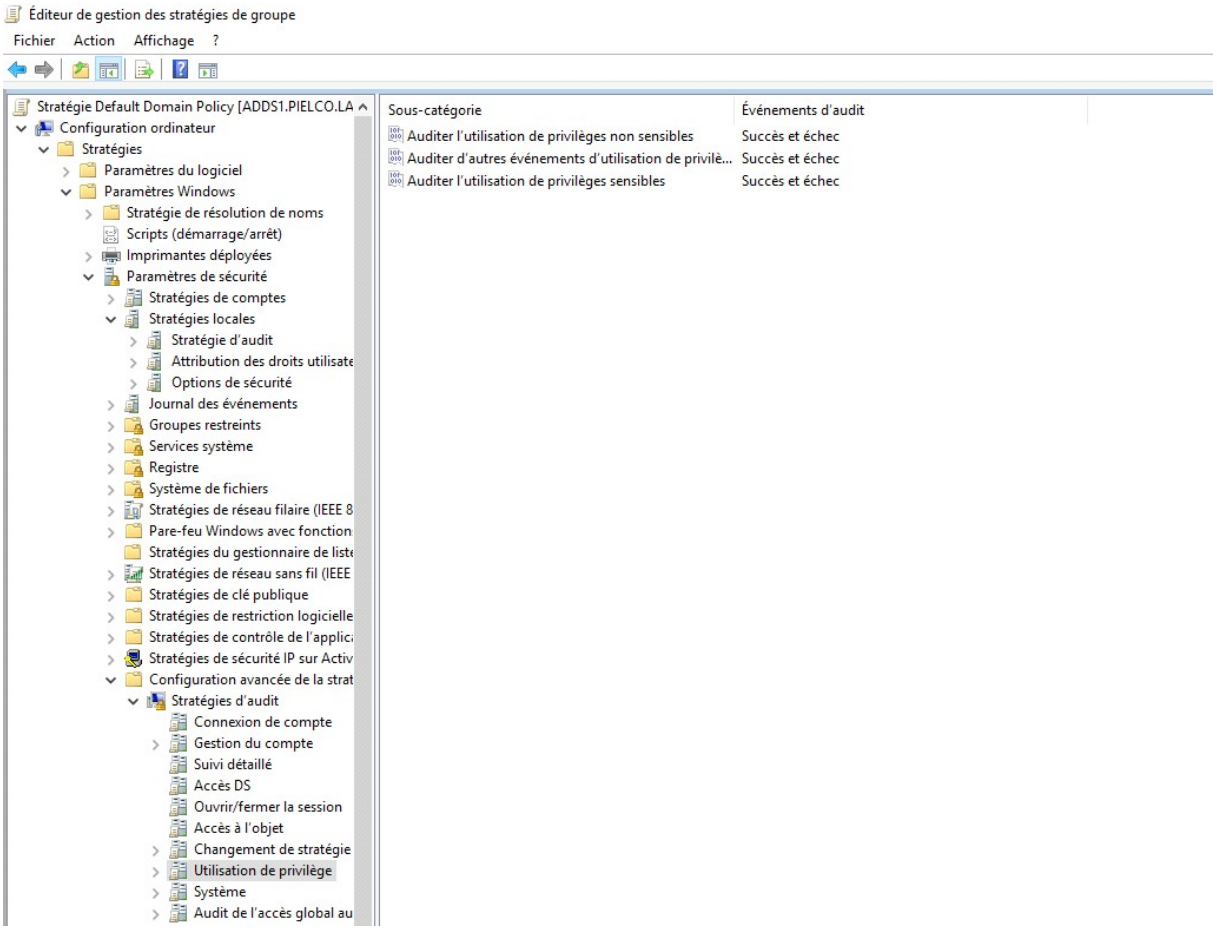

Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie Default Domain Policy [ADDS1.PIELCO.LA
Configuration ordinateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Stratégie de résolution de noms
Scripts (démarrage/arrêt)
Imprimantes déployées
Paramètres de sécurité
Stratégies de comptes
Stratégies locales
Stratégie d'audit
Attribution des droits utilisate
Options de sécurité
Journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de réseau filaire (IEEE 8
Pare-feu Windows avec fonction
Stratégies du gestionnaire de liste
Stratégies de réseau sans fil (IEEE
Stratégies de clé publique
Stratégies de restriction logicielle
Stratégies de contrôle de l'applica
Stratégies de sécurité IP sur Activ
Configuration avancée de la strat
Stratégies d'audit
Connexion de compte
Gestion du compte
Suivi détaillé
Accès DS
Ouvrir/fermer la session
Accès à l'objet
Changement de stratégie
Utilisation de privilège
Système
Audit de l'accès global au
Sous-catégorie
Événements d'audit
Auditer l'activité DPAPI
Non configuré
Auditer l'activité Plug-and-Play
Succès et échec
Auditer la création du processus
Succès et échec
Auditer la fin du processus
Échec
Auditer les événements RPC
Succès et échec
Audit Token Right Adjusted
Succès et échec

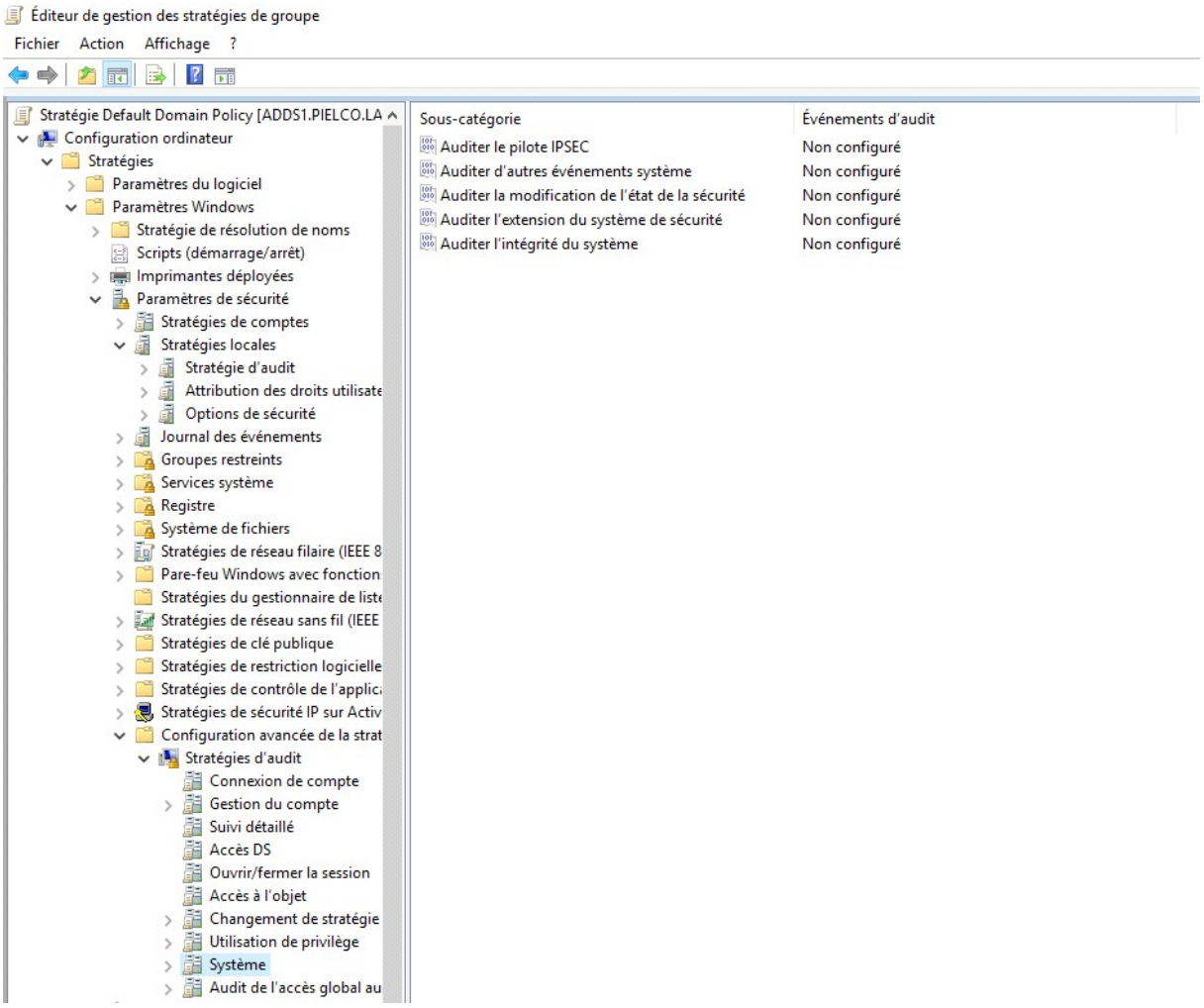

Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie Default Domain Policy [ADDS1.PIELCO.LA
Configuration ordinateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Stratégie de résolution de noms
Scripts (démarrage/arrêt)
Imprimantes déployées
Paramètres de sécurité
Stratégies de comptes
Stratégies locales
Stratégie d'audit
Attribution des droits utilisate
Options de sécurité
Journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de réseau filaire (IEEE 8
Pare-feu Windows avec fonction
Stratégies du gestionnaire de liste
Stratégies de réseau sans fil (IEEE
Stratégies de clé publique
Stratégies de restriction logicielle
Stratégies de contrôle de l'applic
Stratégies de sécurité IP sur Activ
Configuration avancée de la strat
Stratégies d'audit
Connexion de compte
Gestion du compte
Suivi détaillé
Accès DS
Ouvrir/fermer la session
Accès à l'objet
Changement de stratégie
Utilisation de privilège
Système
Audit de l'accès global au
Sous-catégorie
Événements d'audit
Auditer la réplication du service d'annuaire détaillé
Non configuré
Auditer l'accès au service d'annuaire
Succès et échec
Auditer les modifications du service d'annuaire
Succès et échec
Auditer la réplication du service d'annuaire
Non configuré

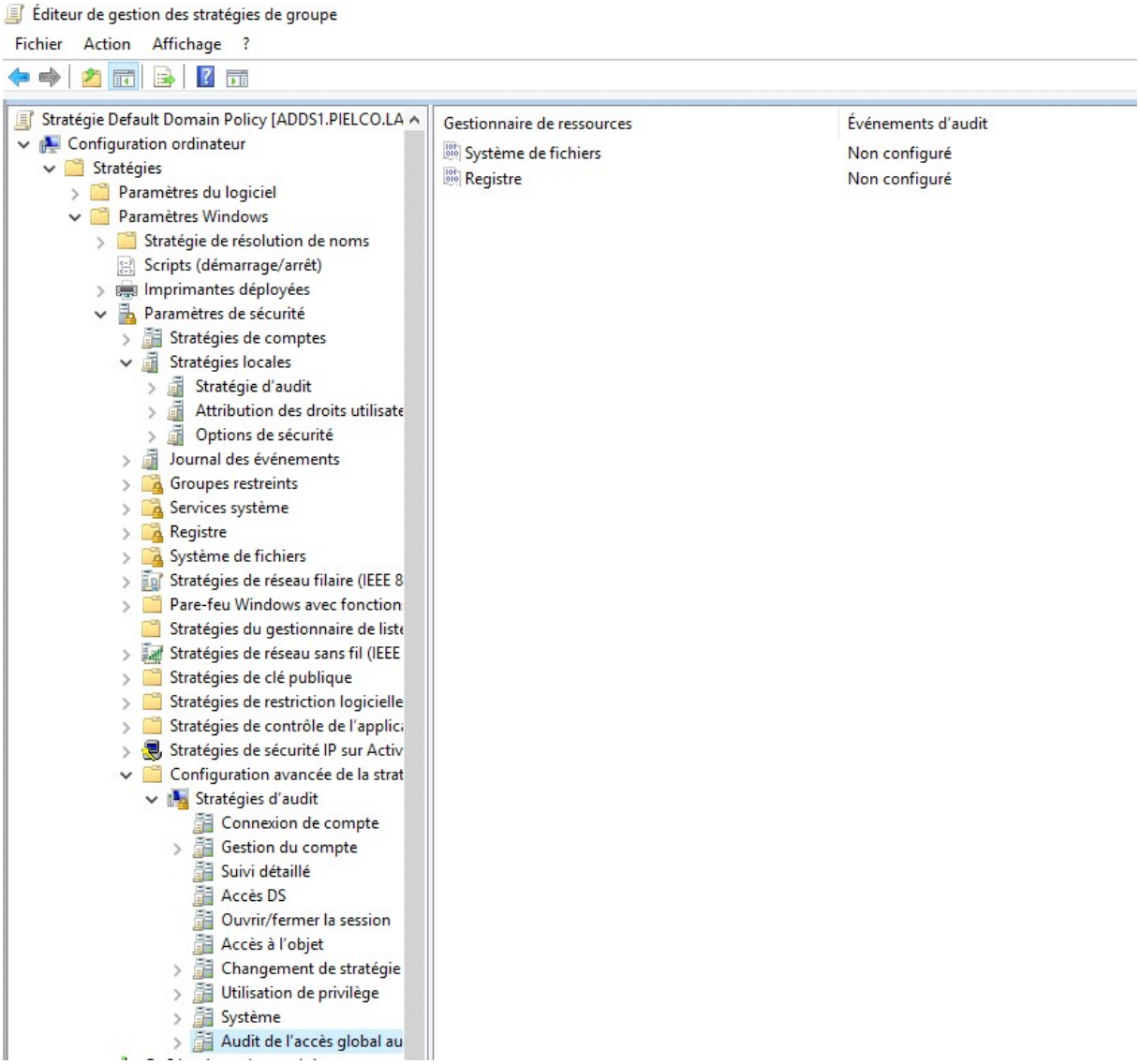

Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie Default Domain Policy [ADDS1.PIELCO.LA
Configuration ordinateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Stratégie de résolution de noms
Scripts (démarrage/arrêt)
Imprimantes déployées
Paramètres de sécurité
Stratégies de comptes
Stratégies locales
Stratégie d'audit
Attribution des droits utilisate
Options de sécurité
Journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de réseau filaire (IEEE 8
Pare-feu Windows avec fonction
Stratégies du gestionnaire de liste
Stratégies de réseau sans fil (IEEE
Stratégies de clé publique
Stratégies de restriction logicielle
Stratégies de contrôle de l'applic
Stratégies de sécurité IP sur Activ
Configuration avancée de la strat
Stratégies d'audit
Connexion de compte
Gestion du compte
Suivi détaillé
Accès DS
Ouvrir/fermer la session
Accès à l'objet
Changement de stratégie
Utilisation de privilège
Système
Audit de l'accès global au
Sous-catégorie
Événements d'audit
Auditer le verrouillage du compte
Non configuré
Auditer les revendications utilisateur/de périphériq...
Non configuré
Auditer l'appartenance à un groupe
Succès et échec
Auditer le mode étendu IPsec
Non configuré
Auditer le mode principal IPsec
Non configuré
Auditer le mode rapide IPsec
Non configuré
Auditer la fermeture de session
Non configuré
Auditer l'ouverture de session
Succès et échec
Auditer le serveur NPS (Network Policy Server)
Non configuré
Auditer d'autres événements d'ouverture/fermetur...
Succès et échec
Auditer l'ouverture de session spéciale
Succès et échec

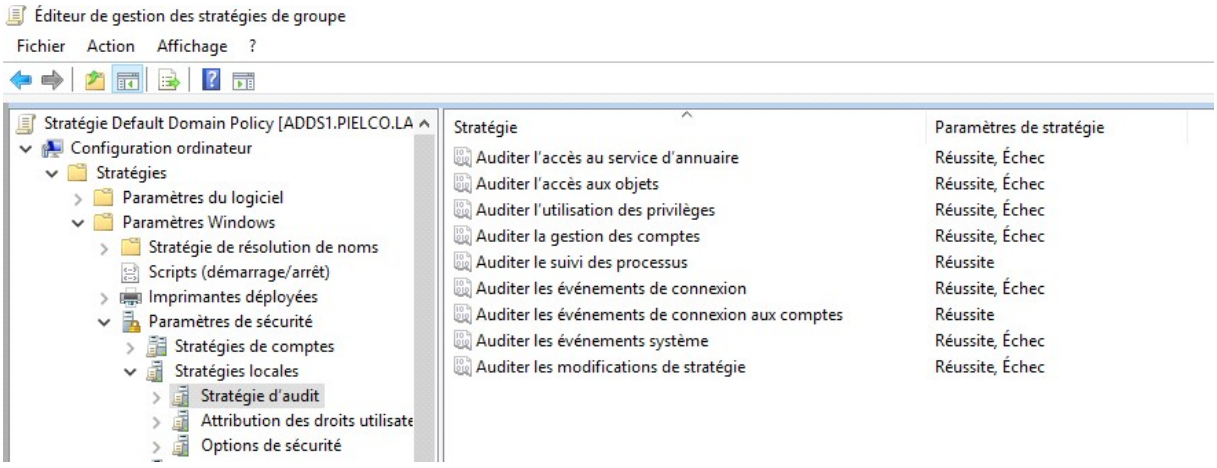

Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie Default Domain Policy [ADDS1.PIELCO.LA
Configuration ordinateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Stratégie de résolution de noms
Scripts (démarrage/arrêt)
Imprimantes déployées
Paramètres de sécurité
Stratégies de comptes
Stratégies locales
Stratégie d'audit
Attribution des droits utilisate
Options de sécurité
Journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de réseau filaire (IEEE 8
Pare-feu Windows avec fonction
Stratégies du gestionnaire de liste
Stratégies de réseau sans fil (IEEE
Stratégies de clé publique
Stratégies de restriction logicielle
Stratégies de contrôle de l'applic
Stratégies de sécurité IP sur Activ
Configuration avancée de la strat
Stratégies d'audit
Connexion de compte
Gestion du compte
Suivi détaillé
Accès DS
Ouvrir/fermer la session
Accès à l'objet
Changement de stratégie
Utilisation de privilège
Système
Audit de l'accès global au
Sous-catégorie
Événements d'audit
Auditer l'application générée Non configuré
Auditer les services de certification Non configuré
Auditer le partage de fichiers détaillé Échec
Auditer le partage de fichiers Échec
Auditer le système de fichiers Échec
Auditer la connexion de la plateforme de filtrage Non configuré
Auditer le rejet de paquet par la plateforme de filtr... Non configuré
Auditer la manipulation de handle Non configuré
Auditer l'objet de noyau Non configuré
Auditer d'autres événements d'accès à l'objet Non configuré
Auditer le Registre Non configuré
Auditer le stockage amovible Non configuré
Auditer SAM Non configuré
Auditer la stratégie d'accès centralisée intermédiaire Non configuré


Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie Default Domain Policy [ADDS1.PIELCO.LA
Configuration ordinateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Stratégie de résolution de noms
Scripts (démarrage/arrêt)
Imprimantes déployées
Paramètres de sécurité
Stratégies de comptes
Stratégies locales
Stratégie d'audit
Attribution des droits utilisate
Options de sécurité
Journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de réseau filaire (IEEE 8
Pare-feu Windows avec fonction
Stratégies du gestionnaire de liste
Stratégies de réseau sans fil (IEEE
Stratégies de clé publique
Stratégies de restriction logicielle
Stratégies de contrôle de l'applica
Stratégies de sécurité IP sur Activ
Configuration avancée de la strat
Stratégies d'audit
Connexion de compte
Gestion du compte
Suivi détaillé
Accès DS
Ouvrir/fermer la session
Accès à l'objet
Changement de stratégie
Utilisation de privilège
Système
Audit de l'accès global au
Sous-catégorie
Événements d'audit
Auditer la modification de la stratégie d'audit
Succès et échec
Auditer la modification de stratégie d'authentificat...
Succès et échec
Auditer la modification de la stratégie d'autorisation
Succès et échec
Auditer la modification de la stratégie de platefor...
Succès et échec
Auditer la modification de la stratégie de niveau rè...
Succès et échec
Auditer d'autres événements de modification de st...
Succès et échec


Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie Default Domain Policy [ADDS1.PIELCO.LA
Configuration ordinateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Stratégie de résolution de noms
Scripts (démarrage/arrêt)
Imprimantes déployées
Paramètres de sécurité
Stratégies de comptes
Stratégies locales
Stratégie d'audit
Attribution des droits utilisate
Options de sécurité
Journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de réseau filaire (IEEE 8
Pare-feu Windows avec fonction
Stratégies du gestionnaire de liste
Stratégies de réseau sans fil (IEEE
Stratégies de clé publique
Stratégies de restriction logicielle
Stratégies de contrôle de l'applic
Stratégies de sécurité IP sur Activ
Configuration avancée de la strat
Stratégies d'audit
Connexion de compte
Gestion du compte
Suivi détaillé
Accès DS
Ouvrir/fermer la session
Accès à l'objet
Changement de stratégie
Utilisation de privilège
Système
Audit de l'accès global au
Sous-catégorie
Événements d'audit
Auditer l'utilisation de privilèges non sensibles
Succès et échec
Auditer d'autres événements d'utilisation de privilè...
Succès et échec
Auditer l'utilisation de privilèges sensibles
Succès et échec

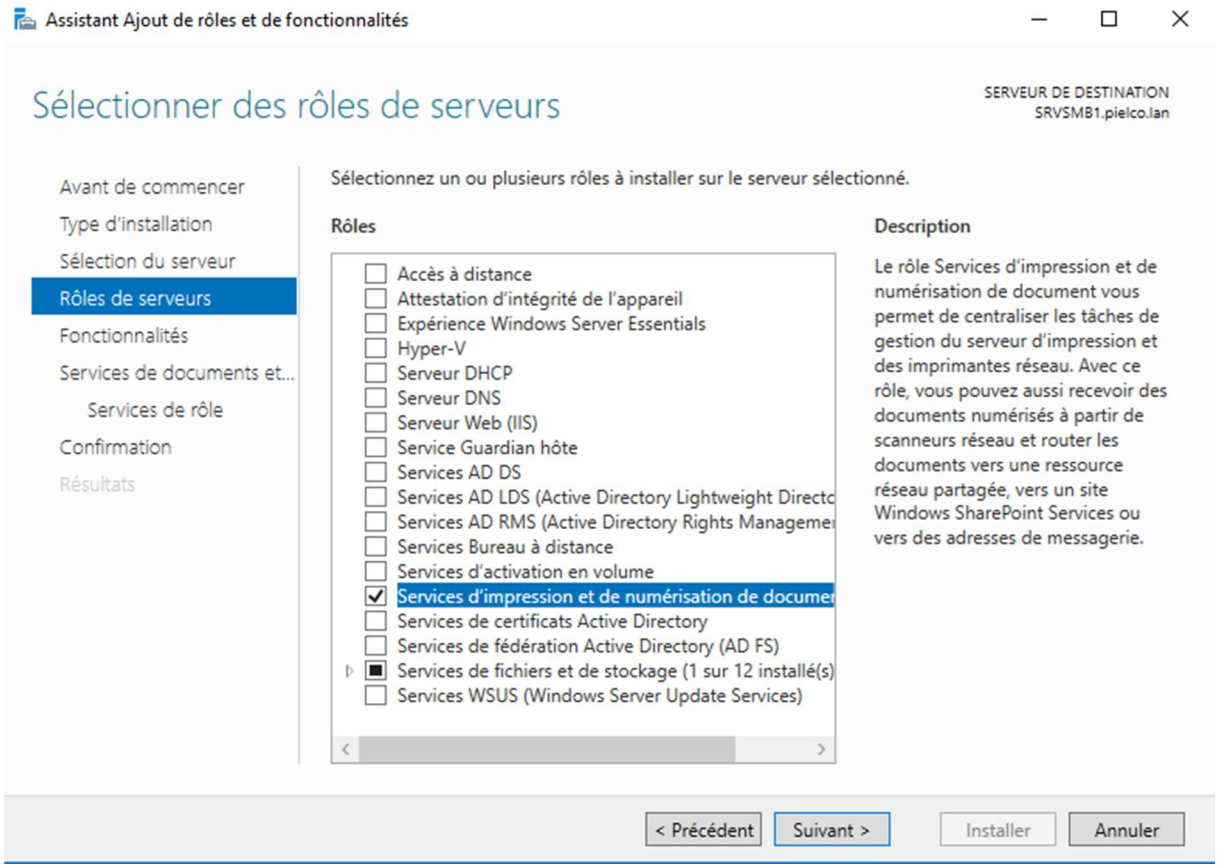

Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie Default Domain Policy [ADDS1.PIELCO.LA
Configuration ordinateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Stratégie de résolution de noms
Scripts (démarrage/arrêt)
Imprimantes déployées
Paramètres de sécurité
Stratégies de comptes
Stratégies locales
Stratégie d'audit
Attribution des droits utilisate
Options de sécurité
Journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de réseau filaire (IEEE 8
Pare-feu Windows avec fonction
Stratégies du gestionnaire de liste
Stratégies de réseau sans fil (IEEE
Stratégies de clé publique
Stratégies de restriction logicielle
Stratégies de contrôle de l'applic
Stratégies de sécurité IP sur Activ
Configuration avancée de la strat
Stratégies d'audit
Connexion de compte
Gestion du compte
Suivi détaillé
Accès DS
Ouvrir/fermer la session
Accès à l'objet
Changement de stratégie
Utilisation de privilège
Système
Audit de l'accès global au
Sous-catégorie
Événements d'audit
Auditer le pilote IPSEC
Non configuré
Auditer d'autres événements système
Non configuré
Auditer la modification de l'état de la sécurité
Non configuré
Auditer l'extension du système de sécurité
Non configuré
Auditer l'intégrité du système
Non configuré


Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie Default Domain Policy [ADDS1.PIELCO.LA
Configuration ordinateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Stratégie de résolution de noms
Scripts (démarrage/arrêt)
Imprimantes déployées
Paramètres de sécurité
Stratégies de comptes
Stratégies locales
Stratégie d'audit
Attribution des droits utilisate
Options de sécurité
Journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de réseau filaire (IEEE 8
Pare-feu Windows avec fonction
Stratégies du gestionnaire de liste
Stratégies de réseau sans fil (IEEE
Stratégies de clé publique
Stratégies de restriction logicielle
Stratégies de contrôle de l'applica
Stratégies de sécurité IP sur Activ
Configuration avancée de la strat
Stratégies d'audit
Connexion de compte
Gestion du compte
Suivi détaillé
Accès DS
Ouvrir/fermer la session
Accès à l'objet
Changement de stratégie
Utilisation de privilège
Système
Audit de l'accès global au
Gestionnaire de ressources
Événements d'audit
Système de fichiers
Non configuré
Registre
Non configuré

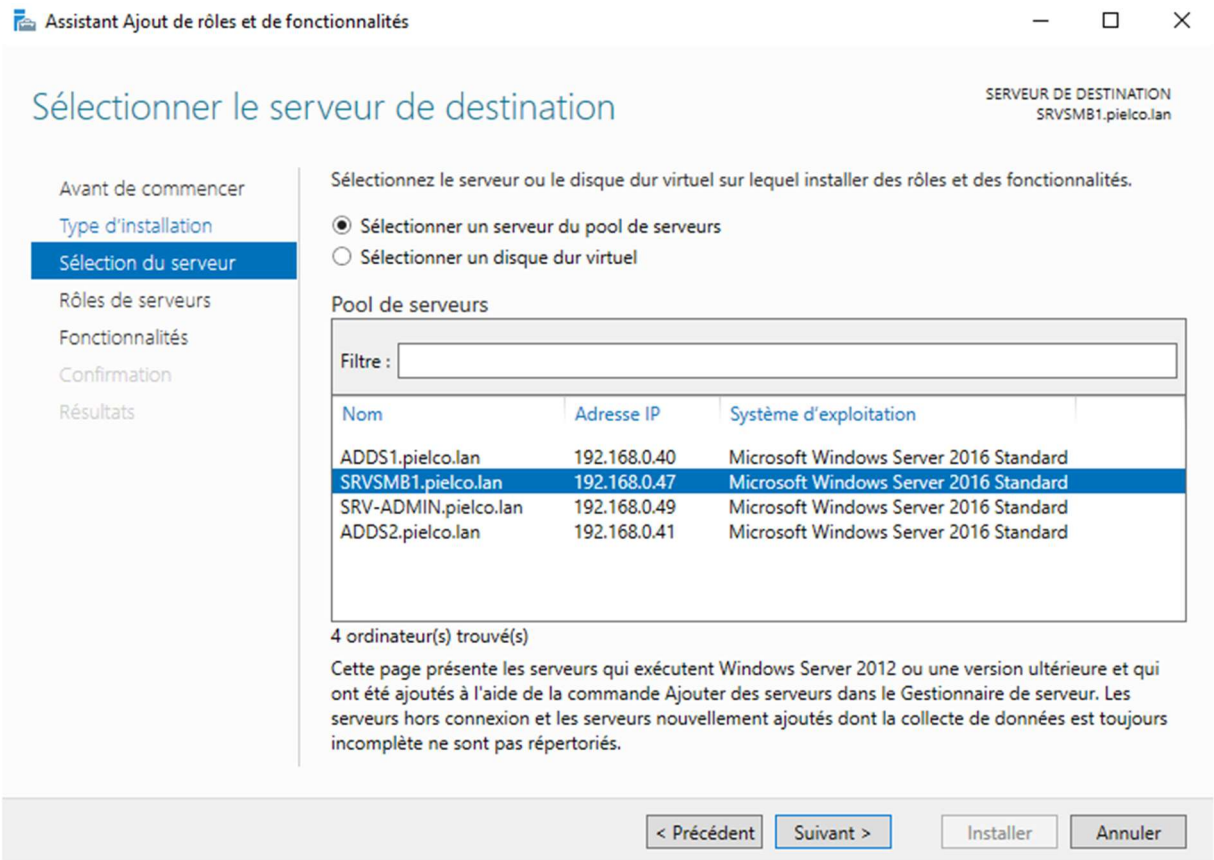

Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie Default Domain Policy [ADDS1.PIELCO.LA
Configuration ordinateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Stratégie de résolution de noms
Scripts (démarrage/arrêt)
Imprimantes déployées
Paramètres de sécurité
Stratégies de comptes
Stratégies locales
Stratégie d'audit
Attribution des droits utilisate
Options de sécurité
Stratégie
Paramètres de stratégie
Auditer l'accès au service d'annuaire
Réussite, Échec
Auditer l'accès aux objets
Réussite, Échec
Auditer l'utilisation des privilèges
Réussite, Échec
Auditer la gestion des comptes
Réussite, Échec
Auditer le suivi des processus
Réussite
Auditer les événements de connexion
Réussite, Échec
Auditer les événements de connexion aux comptes
Réussite
Auditer les événements système
Réussite, Échec
Auditer les modifications de stratégie
Réussite, Échec

d) Service d'impression

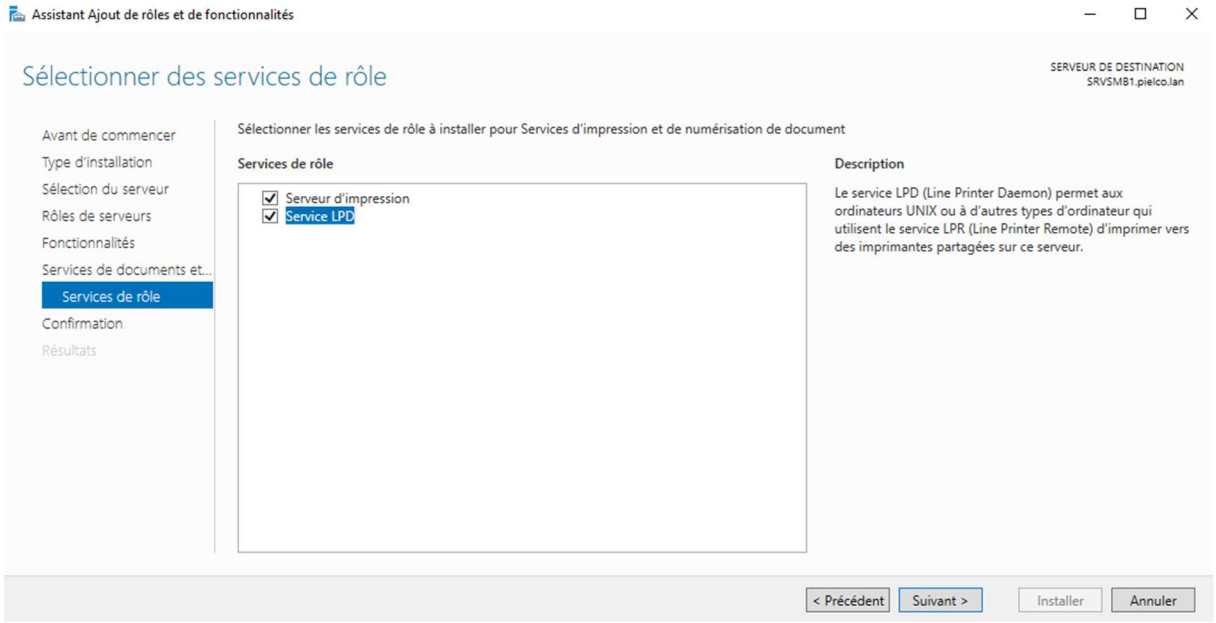
Pour installer le service d'impression nous permettant de gérer les imprimantes sur le réseau, il faut procéder comme suit :



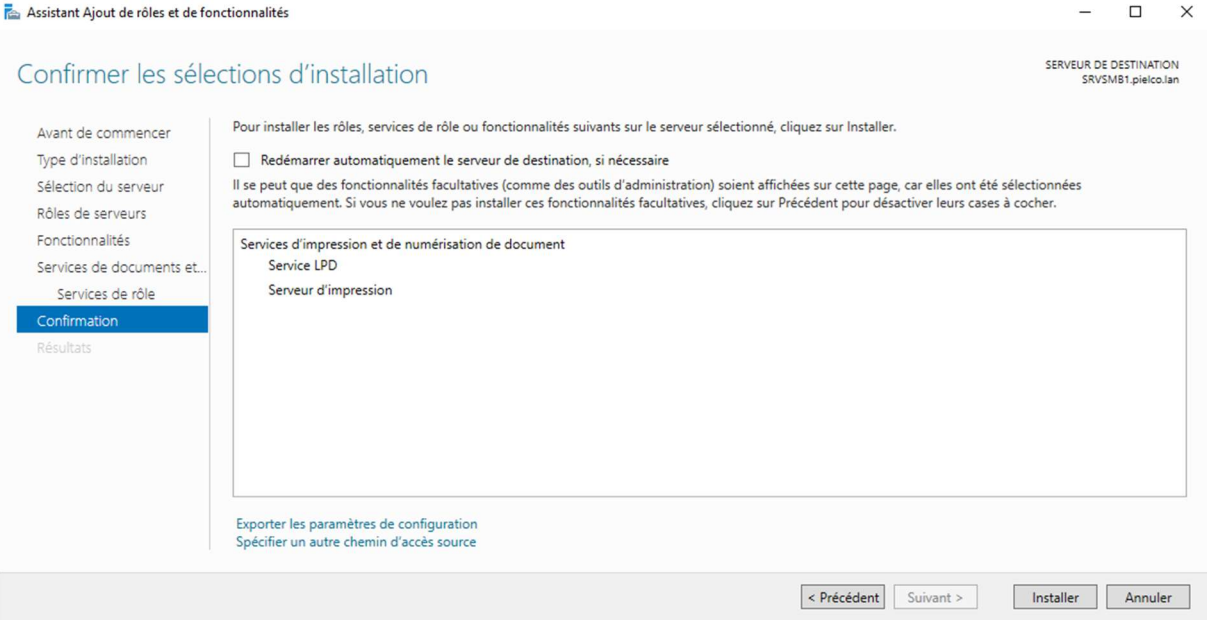
Choisir le rôle voulu



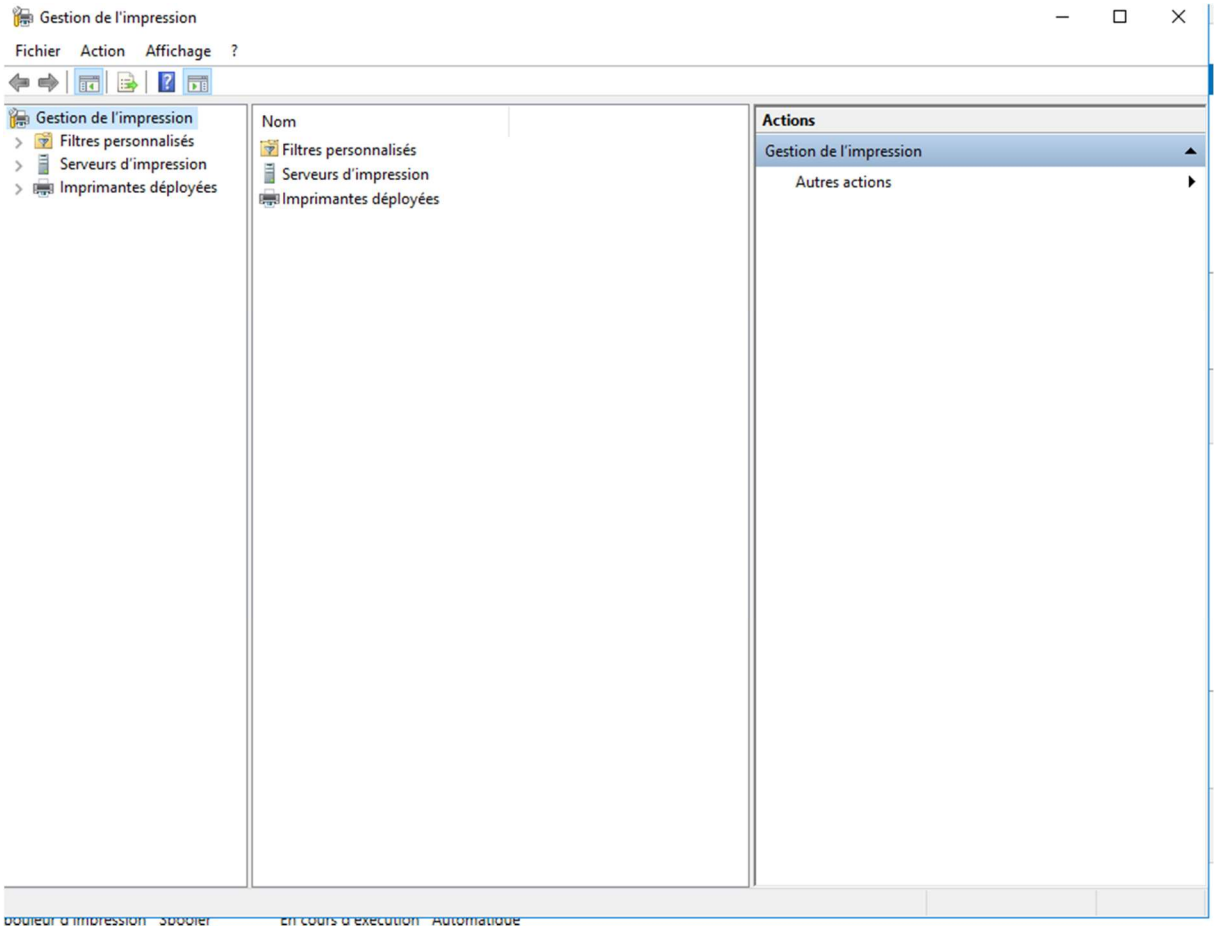
Il faut sélectionner le serveur de destination. Ici nous avons choisi d'installer sur notre serveur de gestion.



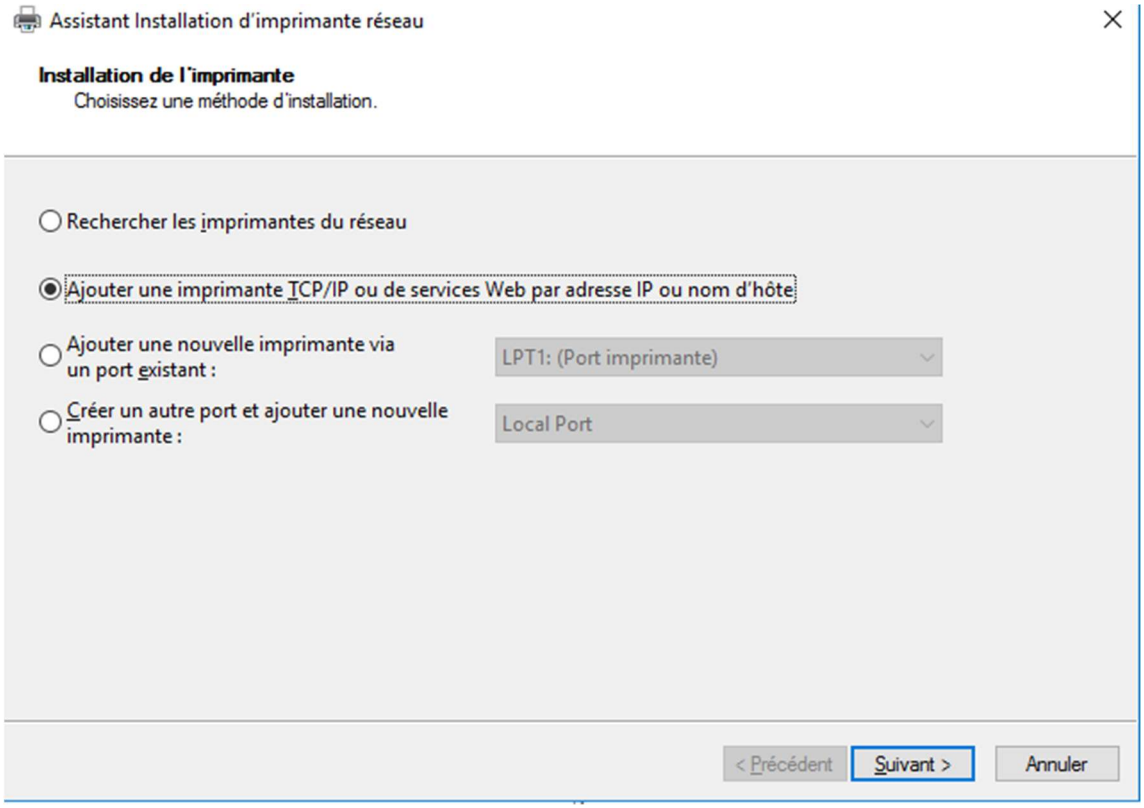
A cette étape, il faut sélectionner Service LPD car nous avons des clients linux sur le par ce service est nécessaire dans leur configuration.



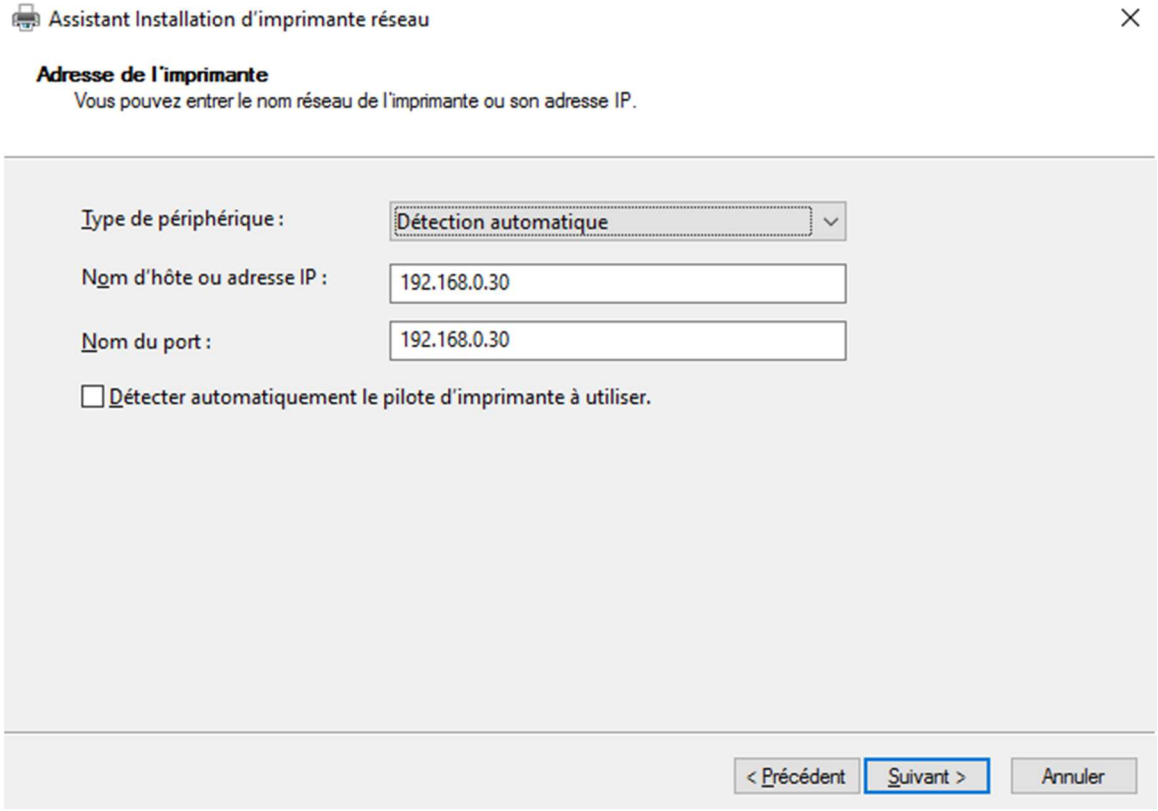
Ceci est la dernière étape, un récapitulatif des services qui vont être installés.



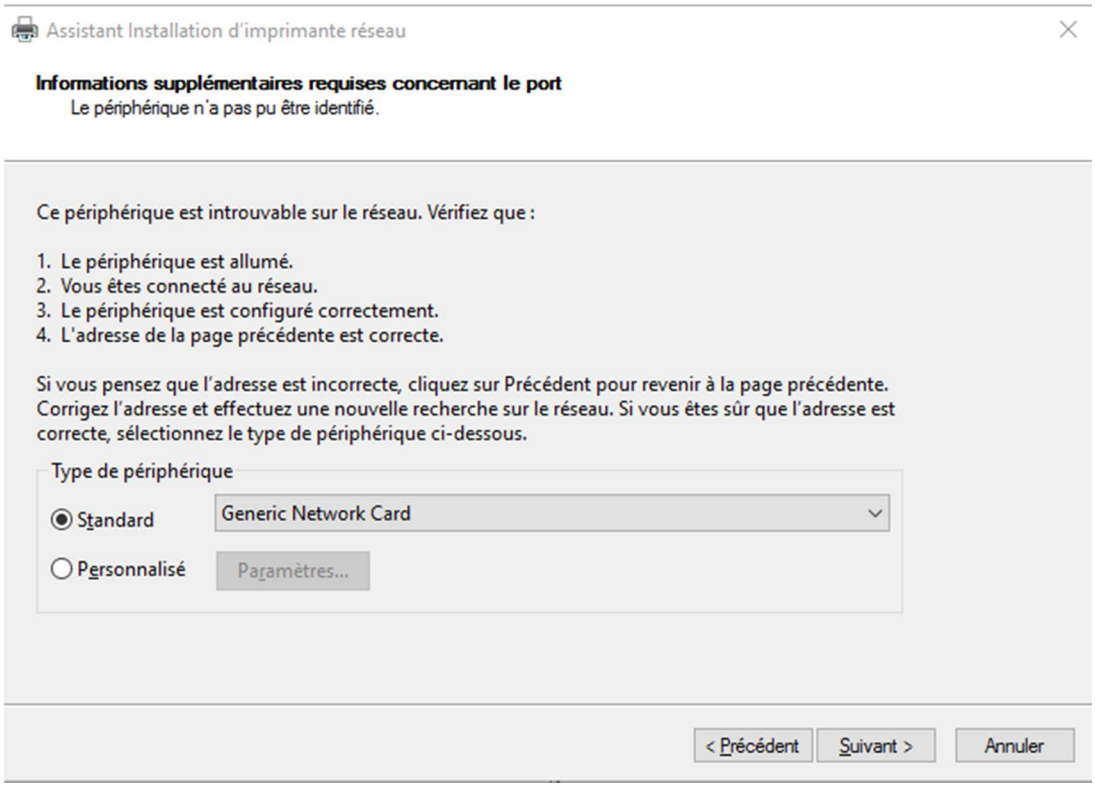
Voici l'installation terminé. Cela se présente comme n'importe quelle console de gestion d'impression sous un client Windows.



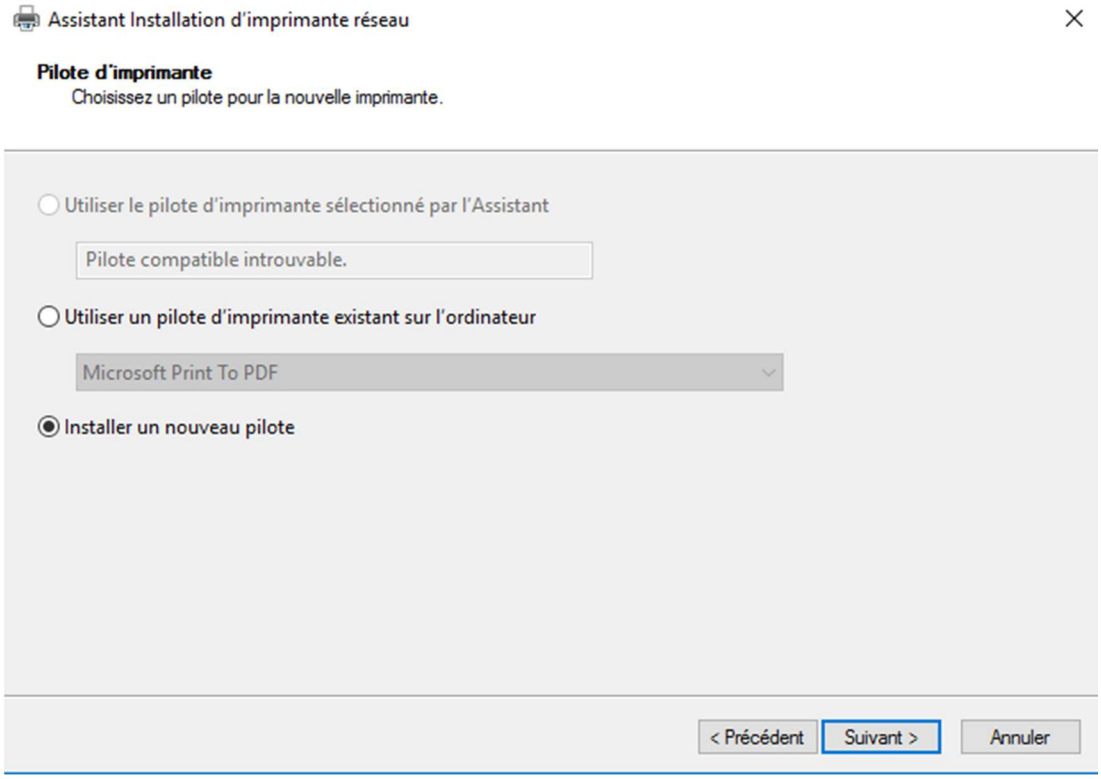
Nous allons maintenant rajouter nos imprimantes en **TCP/IP*** car elles seront en réseau



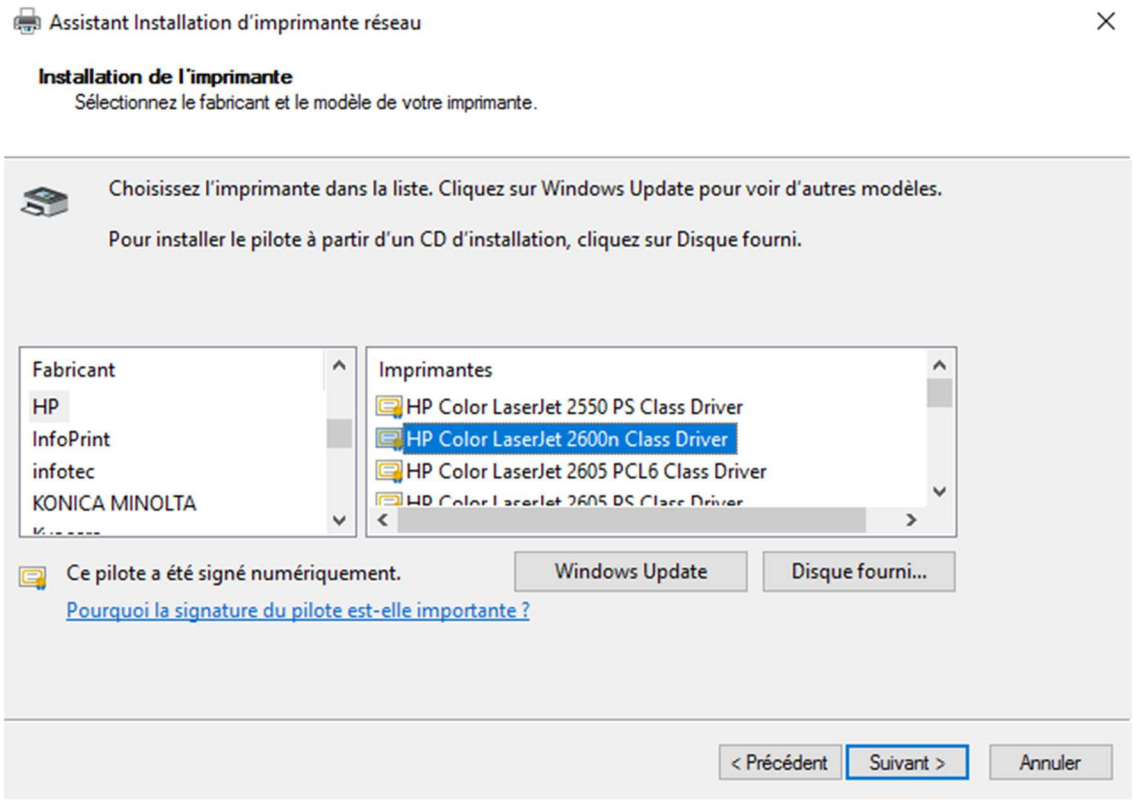
Ici il faut entrer l'adresse IP de notre Imprimante.

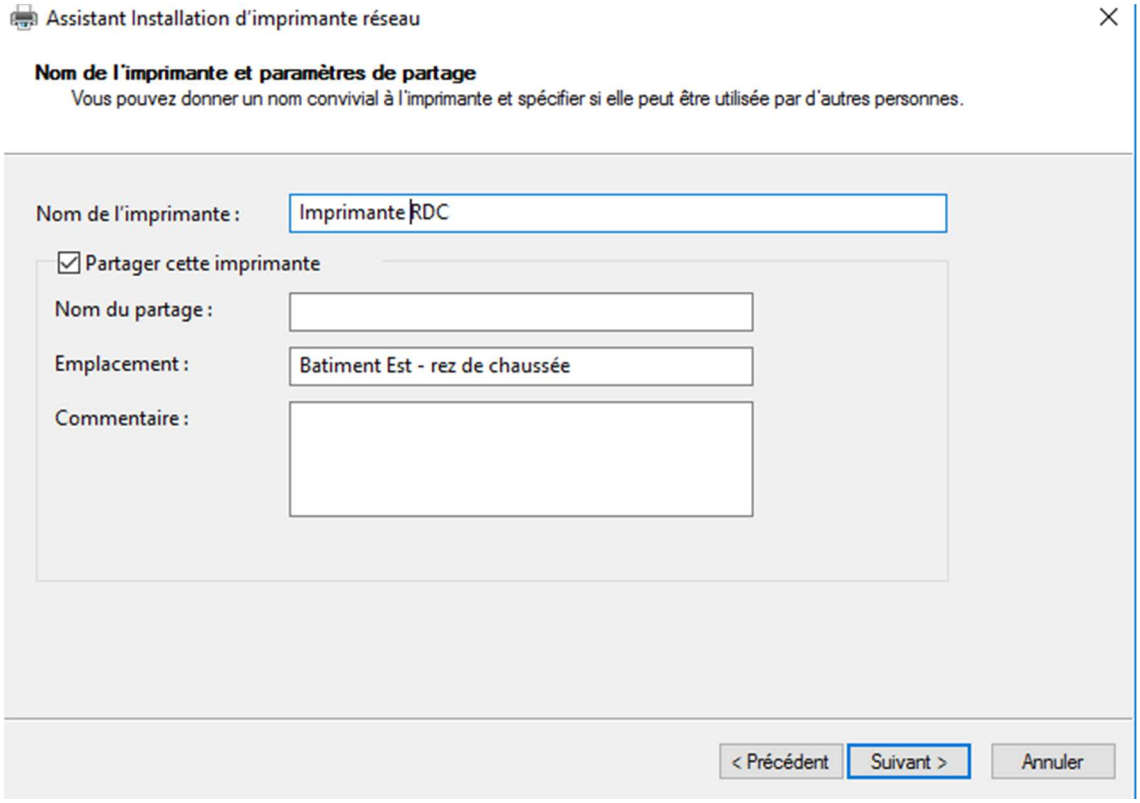


Ici rien de spécial à sélectionner, suivant

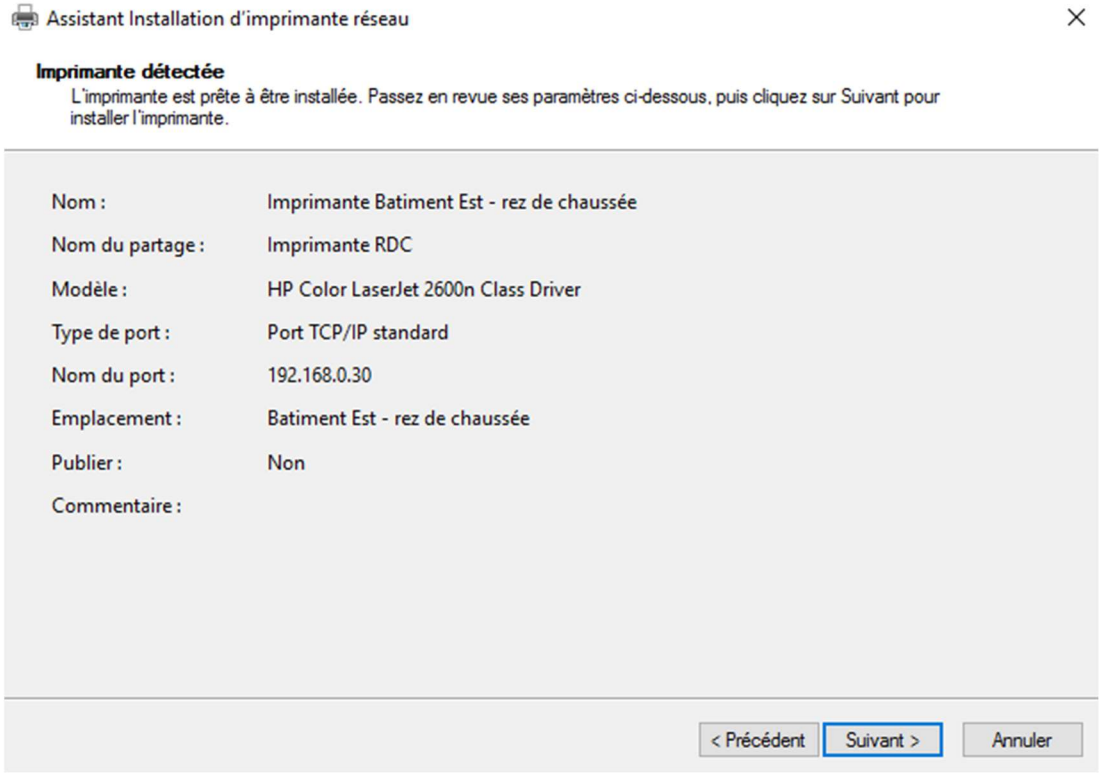


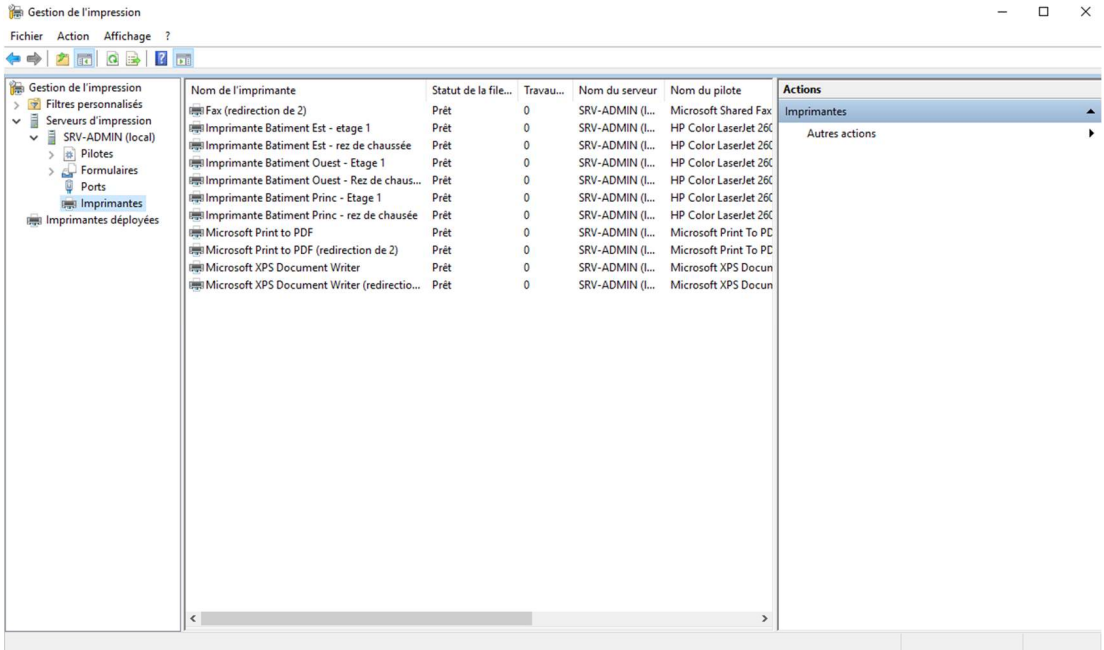
Nous allons maintenant sélectionner notre pilote pour nos imprimantes.





Ici il faut bien remplir les différents champs qui nous permettrons de retrouver notre imprimante plus tard les 6 a installer.





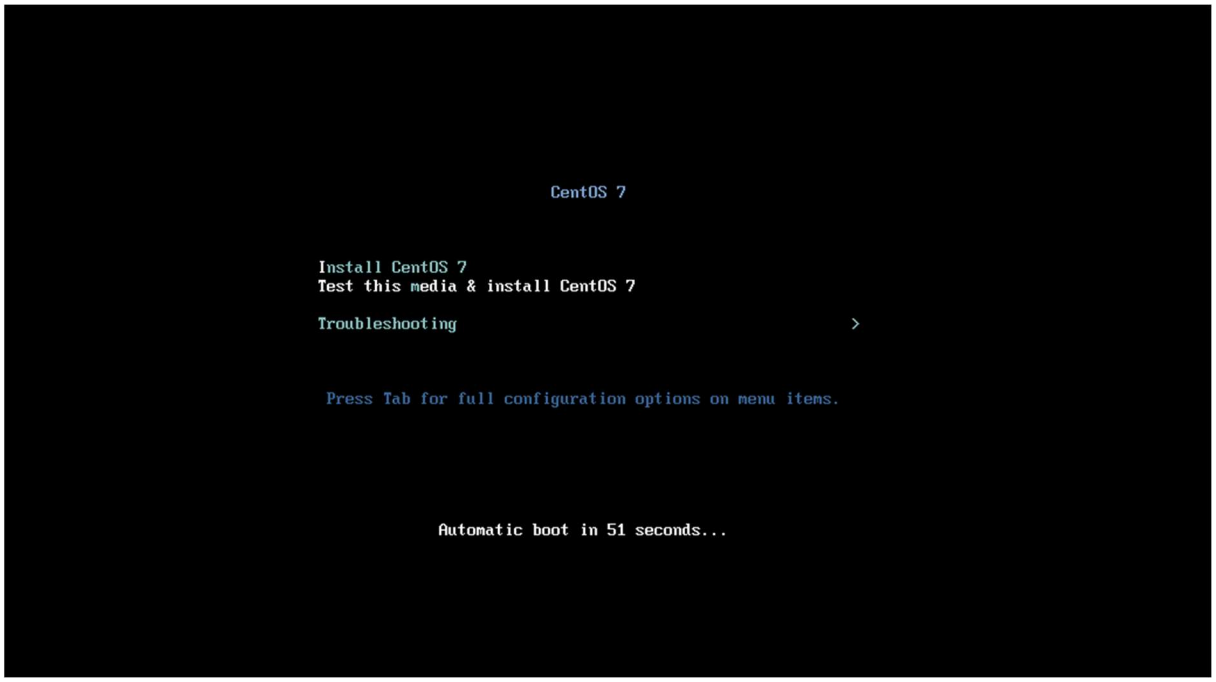
Et voici nos imprimantes installées.

4. Linux CentOS

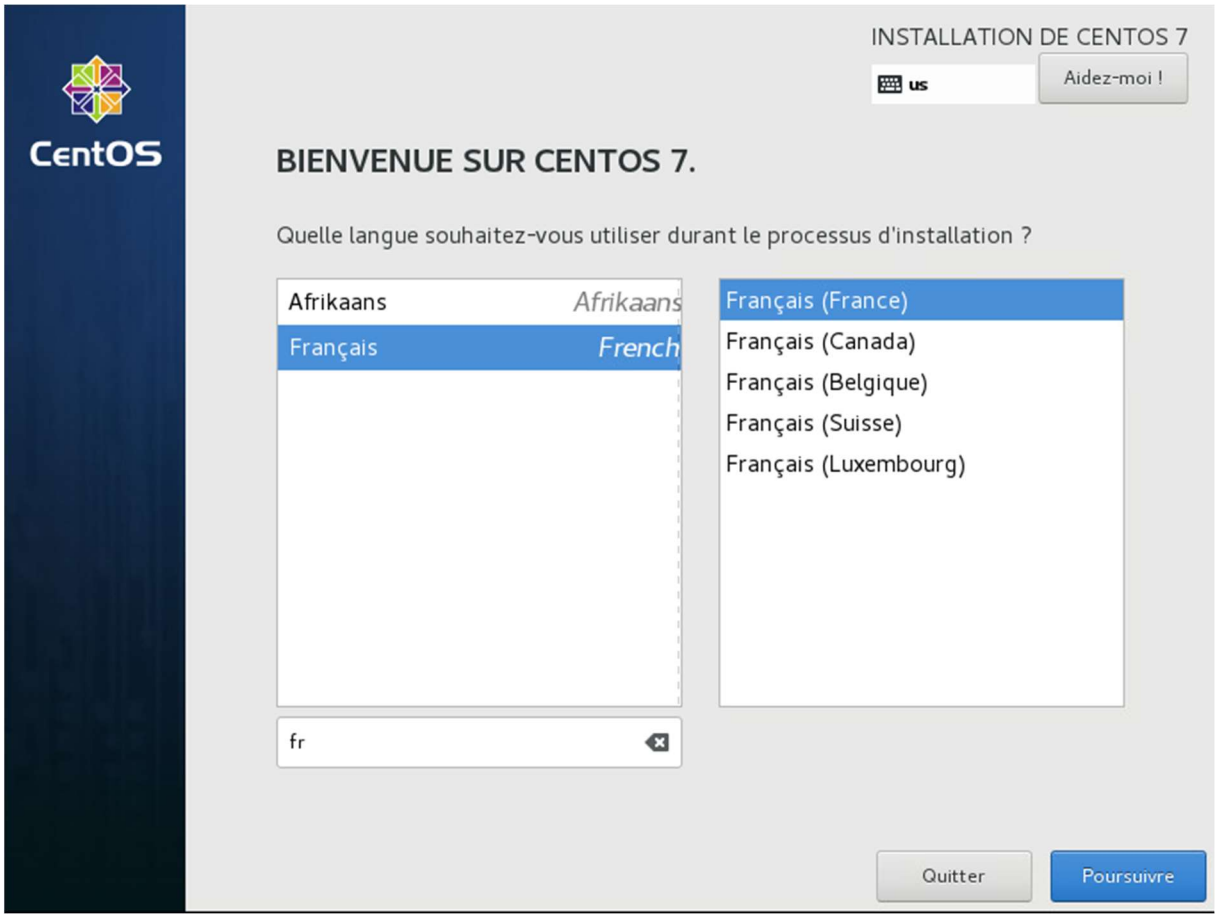
En adéquation avec le cahier des charges, nous avons installé 5 machines virtuelles tournant avec CentOS. Deux pour le DHCP, une pour le FTP, une pour le NFS et Samba et une pour le serveur Web.

a) Installation

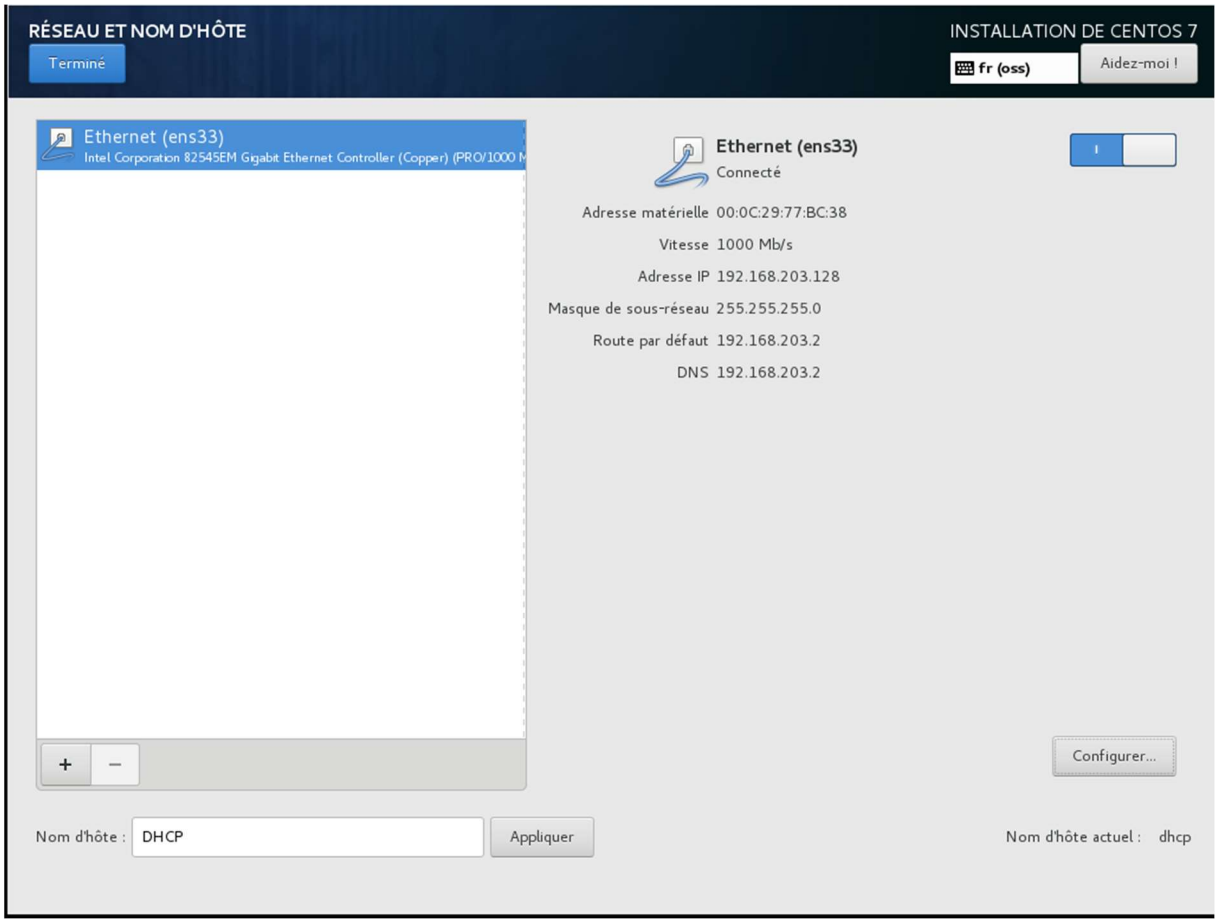
Voici la procédure à suivre pour installer CentOS :



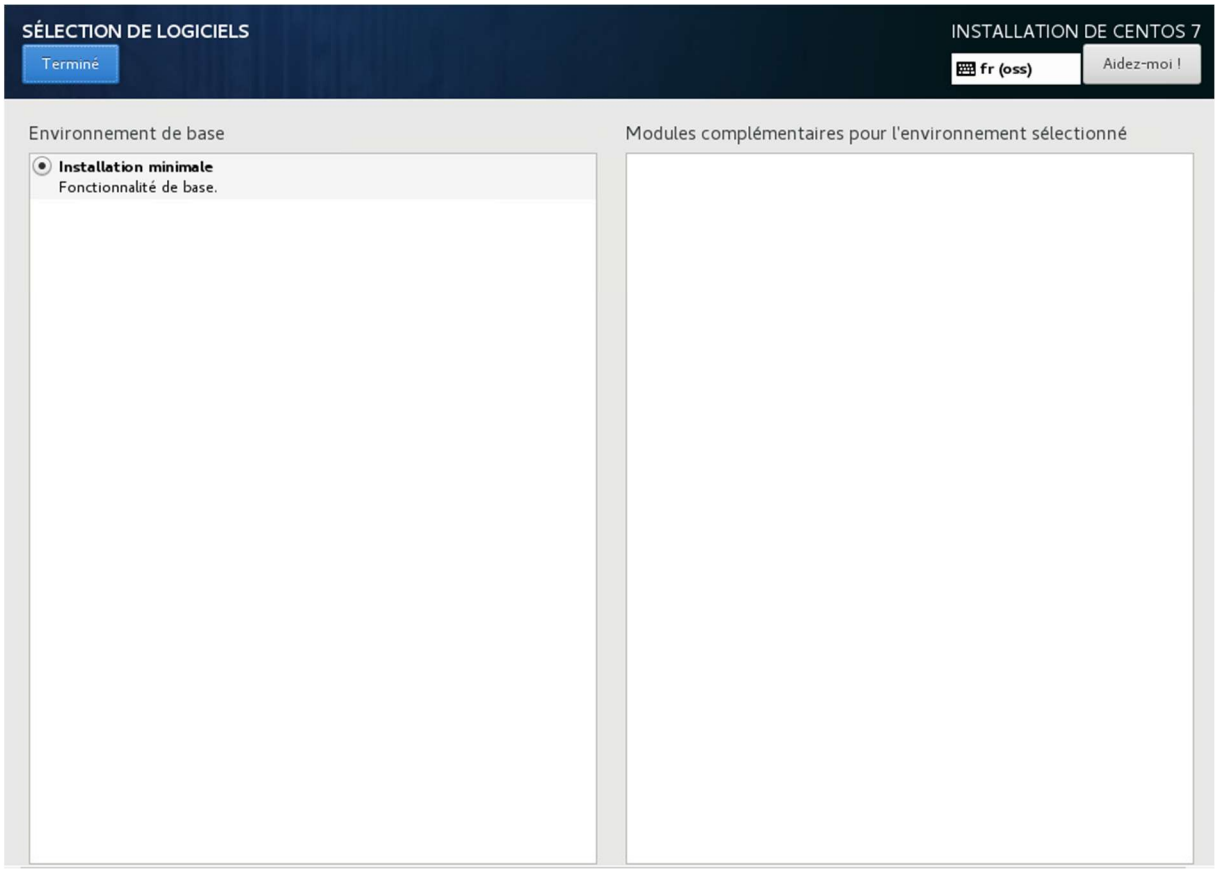
Premier écran au démarrage de l'OS.



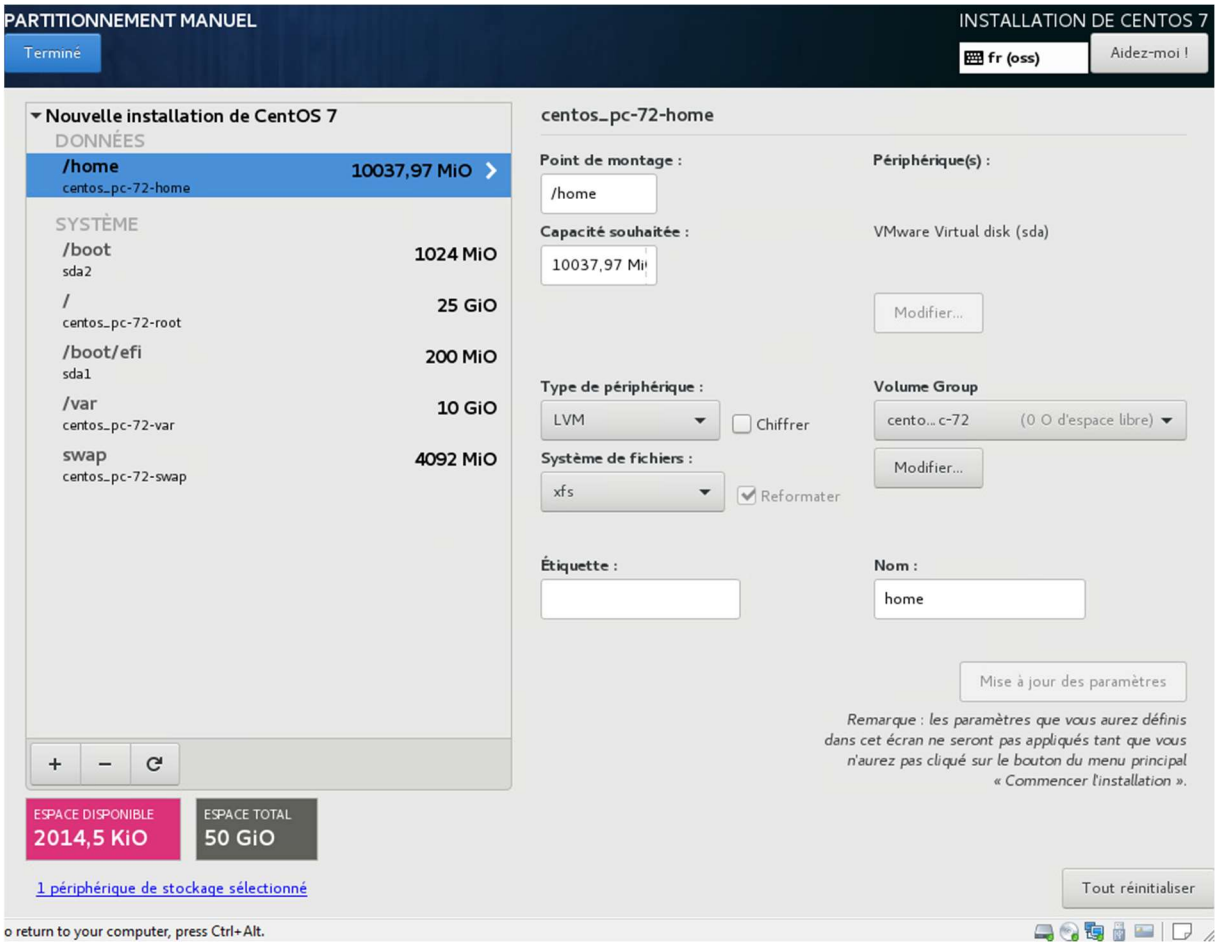
Nous choisissons la langue du système



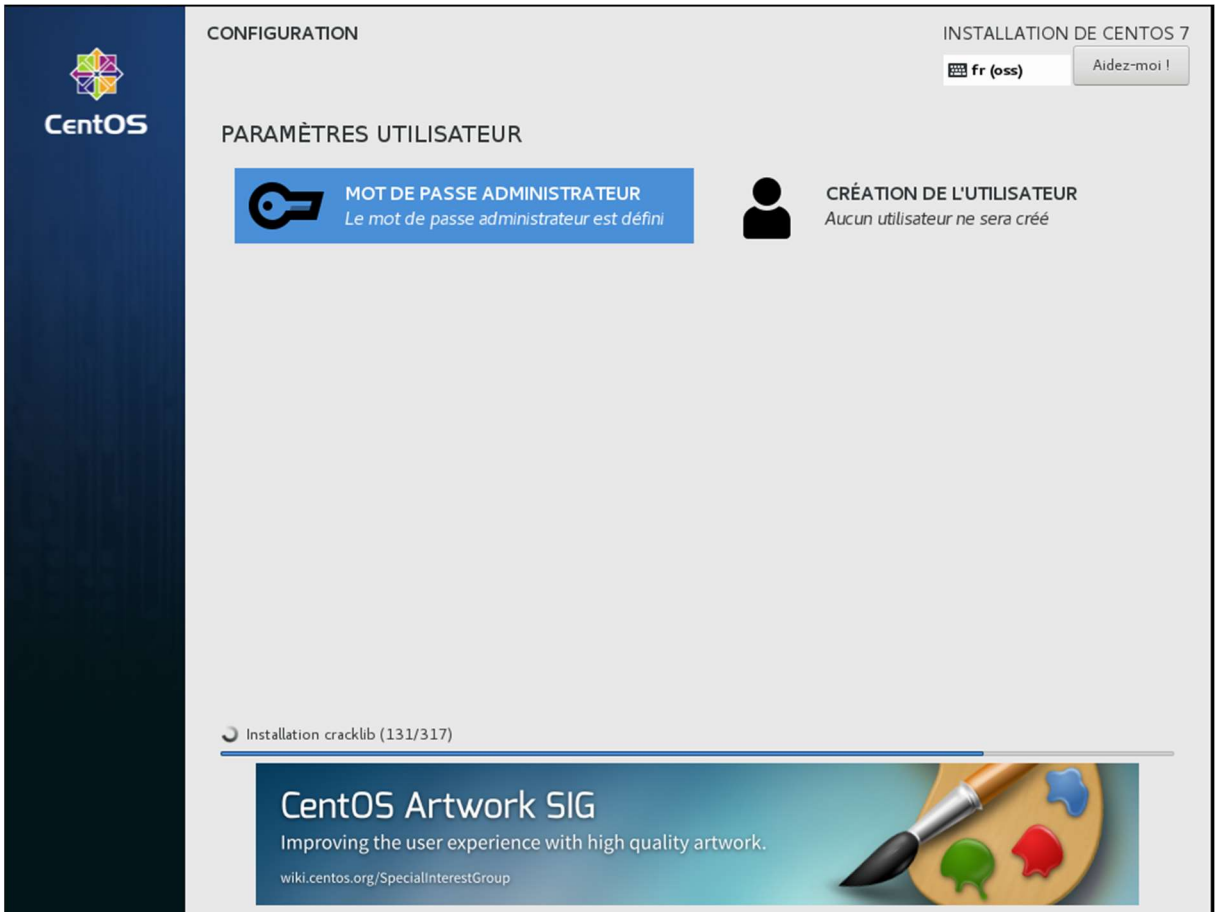
Pour ne pas oublier plus tard, on active la carte Ethernet pour qu'elle se lance automatiquement au démarrage (on peut aussi désactiver l'**IPV**6* si besoin)



Ici, pour ne pas nous encombre de services et applications inutiles, nous choisissons l'installation minimale



Nous paramétrons ensuite les différentes partitions du serveur en prenant bien soin de séparer le /home, le /var et la partition SWAP. Nous les séparons de la partition « principale » pour éviter de paralyser notre serveur si elle venait à saturer le « / ». En cas d'attaque **DDOS*** par exemple.



Une fois les paramétrages de bases faits, nous pouvons lancer l'installation de CentOS. Ici nous avons la possibilité de créer un utilisateur supplémentaire ou d'attribué un mot de passe à l'administrateur du système. (**Root*** par défaut).

b) DHCP

L'installation et le paramétrage d'un serveur DHCP se fait en deux étapes :

- L'installation du service DHCP : **yum install dhcp**
- La mise à jour des fichiers de configurations en faisant attention quant au rôle du DHCP (master ou slave) : **vi /etc/sysconfig/dhcpd**

Par sécurité, nous en avons installé deux. Les DHCP travaillent simultanément et mettre en continue à jour leur base de données de baux. Si un serveur n'est plus disponible, l'autre connaissant les baux distribués par son « peer », il peut prendre le relais en attendant la prochaine synchronisation.

Voici leur fichier de configuration :

(1) DHCP 1

Config DHCP-1.txt

```
authoritative;

failover peer "dhcp-failover" {
primary              ; # Déclare ce serveur comme master.
address 192.168.0.42      ; # Adresse du serveur master.
port 647          ; # Port d'écoute du serveur master.
peer address 192.168.0.43 ; # Adresse du serveur slave.
peer port 647          ; # Port d'écoute du serveur slave.
max-response-delay 60      ; # Temps de non réponse en secondes.
max-unacked-updates 10      ;
mclt 3600          ;
split 110          ; # Répartition des plages d'adresses.
load balance max seconds 3;
}

# Paramétrage de la configuration à distribuer aux postes clients
subnet 192.168.0.0 netmask 255.255.255.0 {
pool{
failover peer "dhcp-failover";                # Indique la configuration du failover
option routers 192.168.0.1;        # Passerelle par défaut
option domain-name-servers 192.168.0.40 ;    # Serveur DNS
range 192.168.0.100 192.168.0.254;    # Plage d'adresses IP
default-lease-time 21600 ;         # Bail de 6 heures par défaut
max-lease-time 36000 ;         # Bail pouvant aller jusqu'à 10 heures
```

(2) DHCP 2

Config DHCP-2.txt

```
failover peer "dhcp-failover" {
secondary          ; # Déclare ce serveur comme slave.
address 192.168.0.43      ; # Adresse du serveur slave.
port 647          ; # Port d'écoute du serveur slave.
peer address 192.168.0.42 ; # Adresse du serveur master.
peer port 647          ; # Port d'écoute du serveur master.
max-response-delay 60      ; # Temps de non réponse en secondes.
max-unacked-updates 10      ; # Nombre de mises à jour avant de déclarer le pair en échec
load balance max seconds 3; # Durée max avant de décharger la requête vers le pair
}

# Paramétrage de la configuration à distribuer aux postes clients
subnet 192.168.0.0 netmask 255.255.255.0 {
pool{
failover peer "dhcp-failover";                # Indique la configuration du failover
option routers 192.168.0.1;        # Passerelle par défaut
option domain-name-servers 192.168.0.40;    # Serveur DNS
range 192.168.0.100 192.168.0.254;    # Plage d'adresses IP
default-lease-time 21600 ;         # Bail de 6 heures par défaut
max-lease-time 36000 ;         # Bail pouvant aller jusqu'à 10 heures
```

c) FTP

Le cahier des charges stipule la mise en place d'un FTP sécurisé et anonyme pour l'échange de fichiers.

Une fois le service FTP installé sur le serveur avec la commande : **yum install vsftpd**, il faut paramétrer le fichier **vi /etc/vsftpd/vsftpd.conf**.

config ftp.txt

```
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_std_format=YES
chroot_local_user=YES
listen=NO
listen_ipv6=YES
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
allow writeable chroot=YES
pasv enable=YES
pasv min port=40000
pasv max port=40100
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_sslv2=NO
ssl_sslv3=NO
ssl_tlsv1=YES
```

d) NFS

Network File System (ou NFS), littéralement *système de fichiers en réseau*, est à l'origine un protocole que permet à un ordinateur d'accéder via un réseau à des fichiers distants.

Ce système de fichiers en réseau permet de partager des données principalement entre systèmes UNIX. Il est le penchant Unix du DFS de Windows.

Nous l'avons installé sur un serveur CentOS en tapant les commandes suivantes :

install nfs.txt

```
#Ajouter une règle dans le firewall
firewall-cmd --add-service=nfs --permanent
firewall-cmd --reload

#Installation du serveur NFS
yum install nfs-utils

#ajouter une disque dur et le partitionner
#Créer une partition sdb1 de type xfs
fdisk /dev/sdb
#Formater la partition
mkfs.xfs /dev/sdb1

#Créer un dossier destiné au montage de la nouvelle partition
mkdir /nfs

#Ajouté le montage de la nouvelle parartion au démarrage de la machine
vi /etc/fstab
#ajouter ligne suivantes
/dev/sdb1 /nfs  xfs defaults 0 0

#Changer les droits du dossier
chmod -R 755 /nfs

#Changer les groupes propriétaires
chown nfsnobody:nfsnobody /nfs

#Créer le partage
vi /etc/exports
#Ajouter
/nfs 192.168.0.*/24(rw,sync,no_root_squash,no_all_squash)

```

e) Samba

Samba est un logiciel qui s'appuie sur les protocoles propriétaires Windows SMB/CIFS installé sur une machine Unix qui permet l'interopérabilité entre des machines Windows et Unix. Ce protocole est en général utilisé pour partager des fichiers ou des imprimantes.

Nous nous servons de Samba pour faire en sorte que les utilisateurs Windows et Linux puissent avoir des dossiers partagés.

Nous l'avons installé sur notre serveur NFS en utilisant ces lignes de commandes :

On installe Samba **:**

yum install samba.x86_64

On édite le fichier de configuration : ***vi /etc/samba/smb.conf***

[data]
path = /nfs
browseable = yes
writable = yes
guest ok = yes
read only = no

On créé les droits **SELinux*** pour samba :

chcon -t samba_share_t /nfs

On modifie les droits du dossier:

chmod -R 0777 /nfs

chown -R nobody:nobody /nfs

On donne accès aux partage Home des utilisateurs avec la configuration par défaut :

chcon -t samba_share_t /home –R

On créé un compte pour authentifier l'utilisateur :

smbpasswd -a smbuser

On autorise le programme Samba à passer le firewall :

firewall-cmd --permanent --zone=public --add-service=samba

f) Serveur Web

Nous avions besoin d'avoir une solution de gestion de parc via le web. Pour se faire nous proposons d'installer un serveur Web puis nous avons développé notre propre solution s'appuyant sur une base de données relationnelle nous permettant entre autres de :

- Consulter la liste des postes par noms de l'utilisateur, prénoms, nom du local…
- Consulter les caractéristiques d'un matériel et voir ses éventuelles connexions avec d'autres matériels
- Enregistrer, modifier et supprimer des postes, des utilisateurs, …

Le tout sera accessible à tout le monde, avec des droits de consultation ou de gestion suivant le profil.

En attendant nous gérons toutes les entrées et sorties de stock, les lieux d'intervention sur gestion papier.

C. Système de sauvegarde

Afin de sauvegarder toutes notre infrastructure système, nous avons opté pour le logiciel « Veeam Backup and Replication ». Ce système de sauvegarde possède plusieurs avantages :

- Il a été éprouvé par de nombreuses entreprises avant la nôtre, ce qui fait que nous ne manquons pas de documentations pour travailler et résoudre les éventuels problèmes ;
- Il existe une version gratuite correspondant à la taille de notre infrastructure et à nos besoins ;
- Le logiciel est déjà connu de notre équipe.

Veeam tournera sur serveur Dell PowerEdge T130 se trouvant dans la salle serveur.

Nous avons configuré la sauvegarde des deux ESX **tous les soirs à 20H**. Cette fréquence élevée hors heures de travail nous permet de nous assurer qu'en cas de problème sur notre infrastructure, nous avons la capacité de répondre efficacement et rapidement en récupérant les données de la veille pour les remettre en production.

Pour rappel, ces données seront stockées sur un des NAS déjà présent sur site et lui-même redondé sur un autre NAS situé dans bâtiment différent.

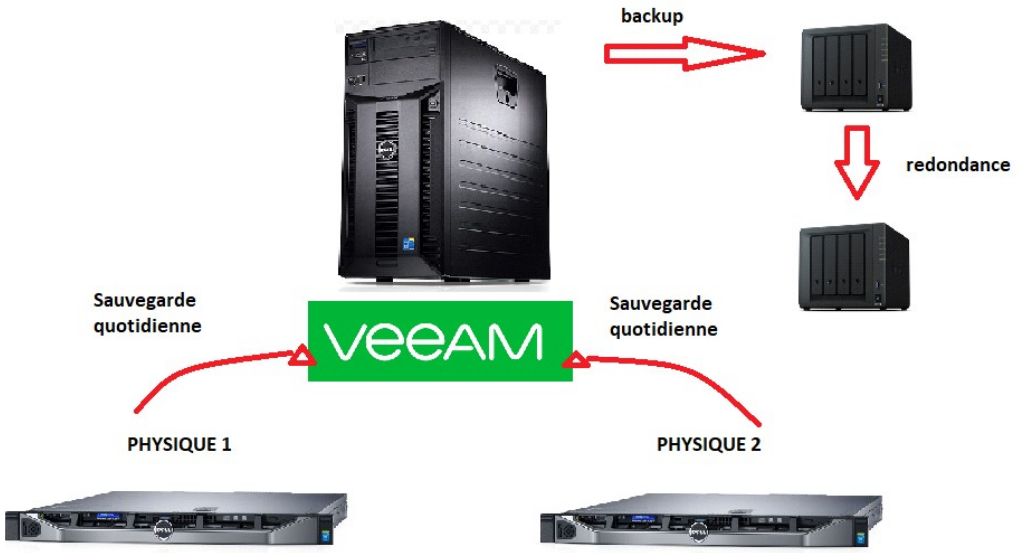
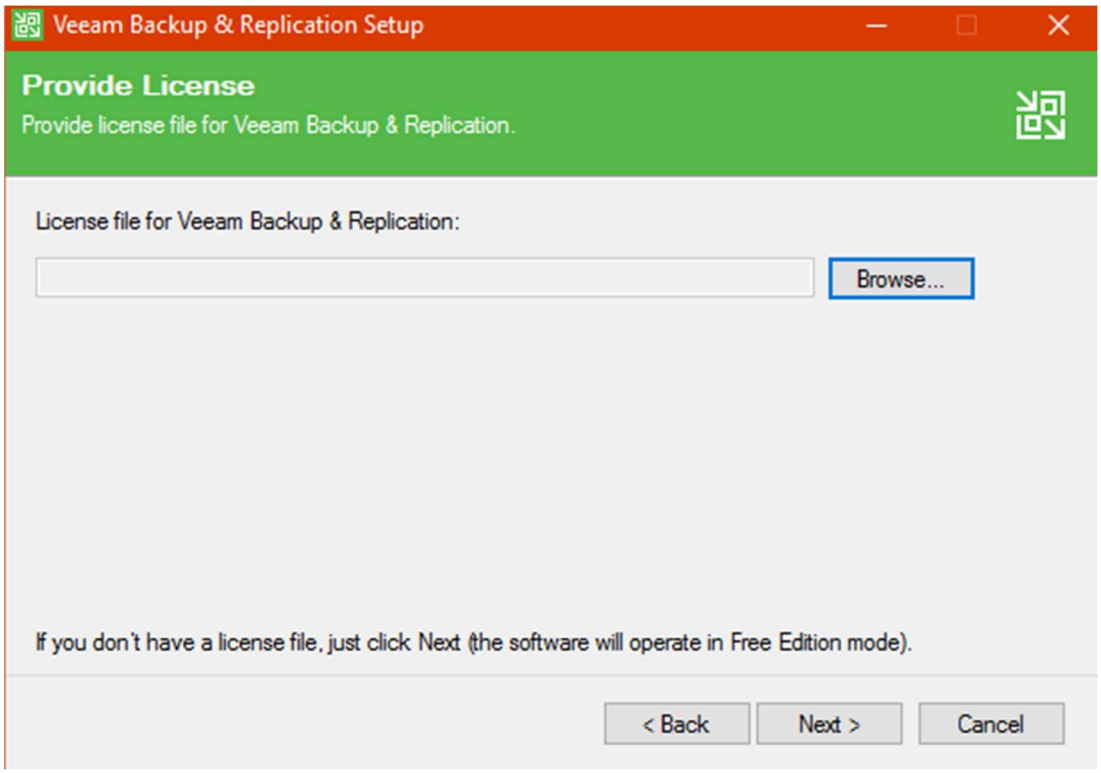


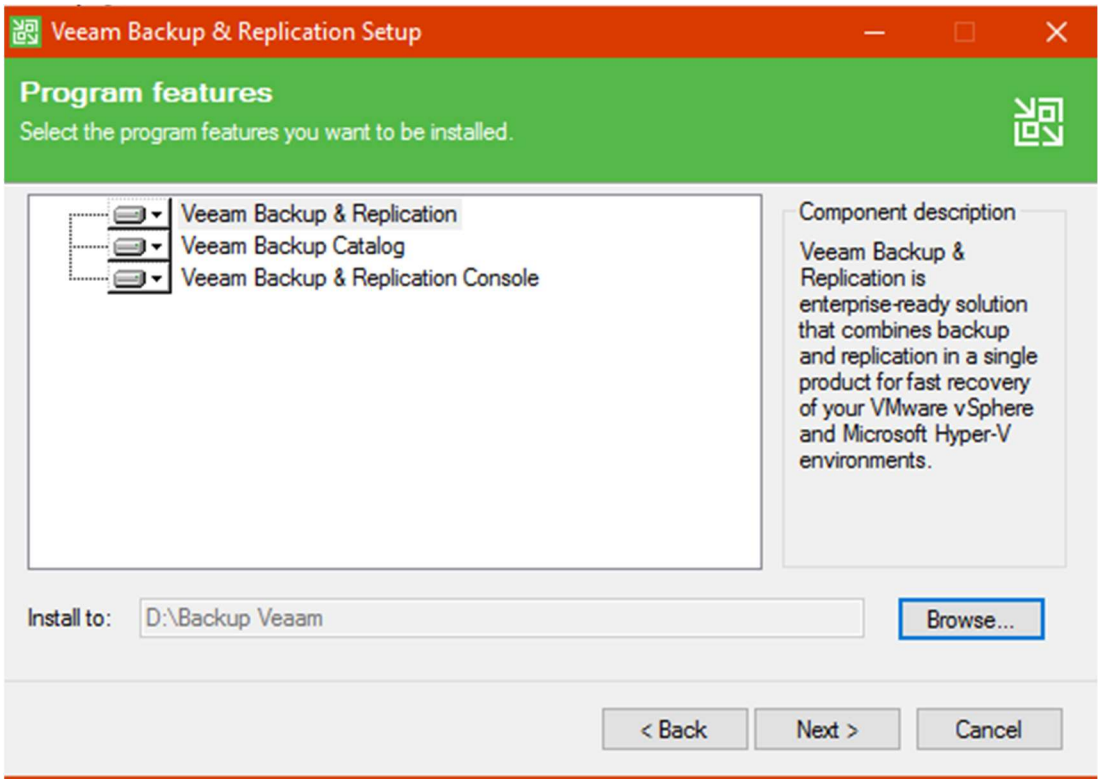
Schéma de notre système de sauvegarde.

1. Installation

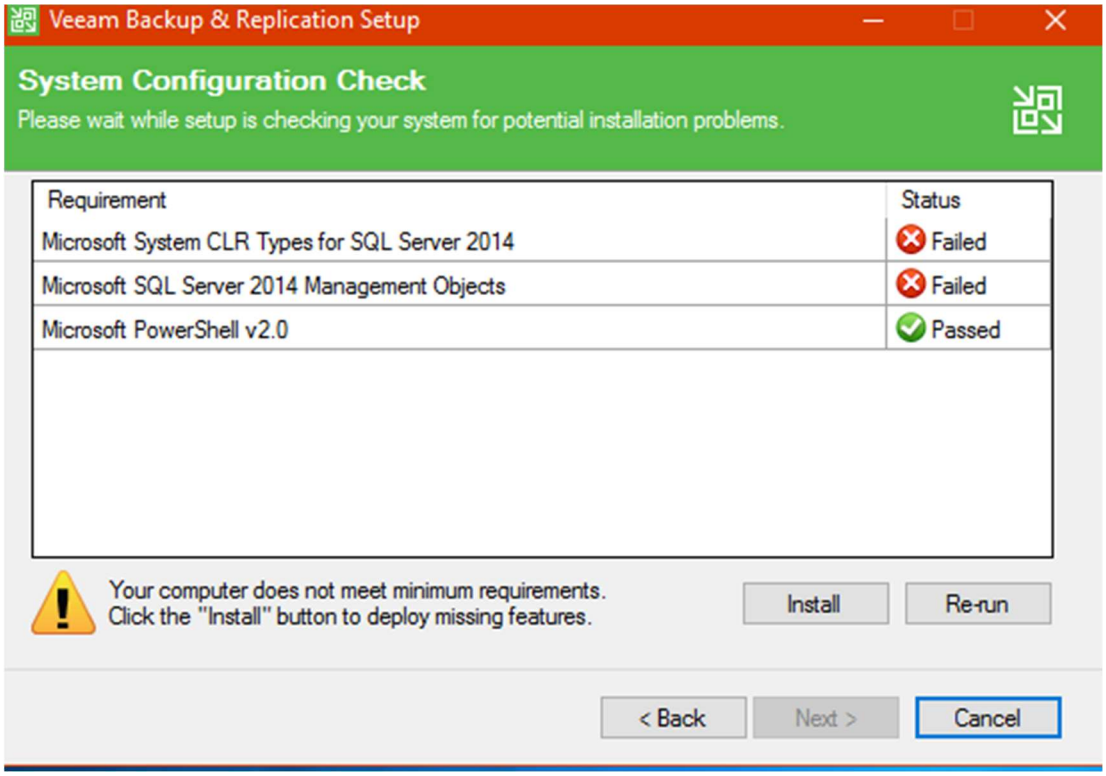
Voici comment nous avons procédé pour l'installation de Veeam :



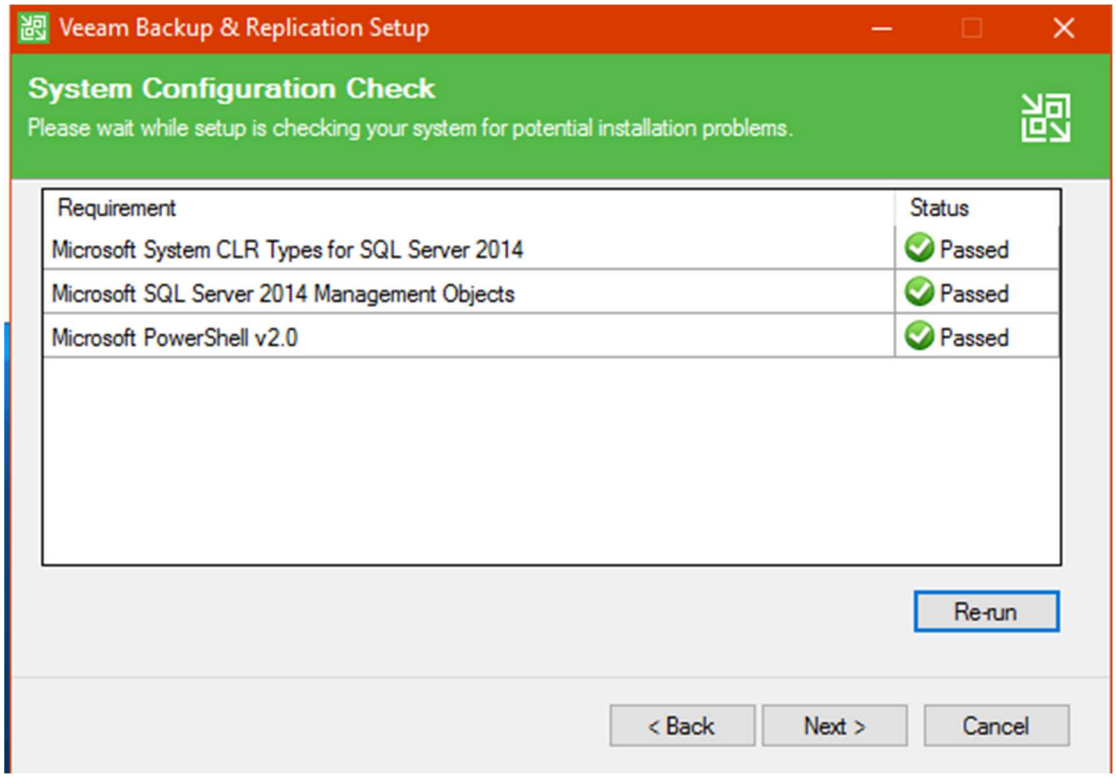
Au début de l'installation, Veeam nous demande la licence de lui fournir la licence d'utilisation du logiciel ou de partir sur une version gratuite.



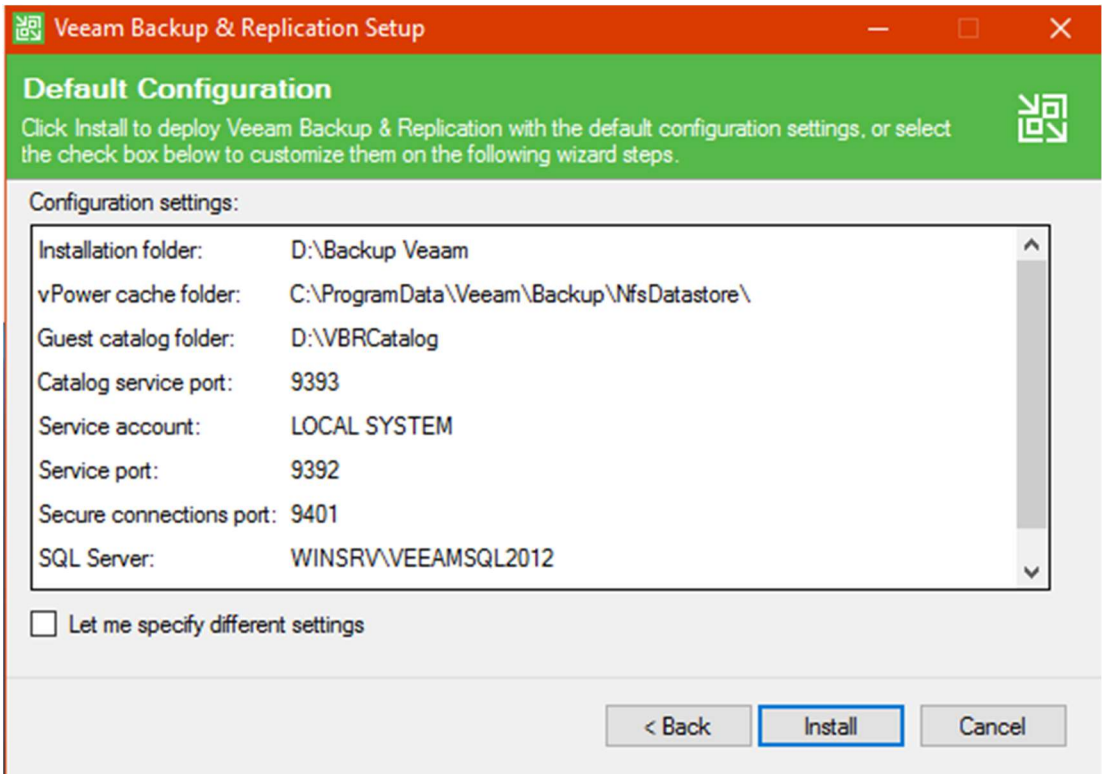
Voici les différents composants qui seront installés.



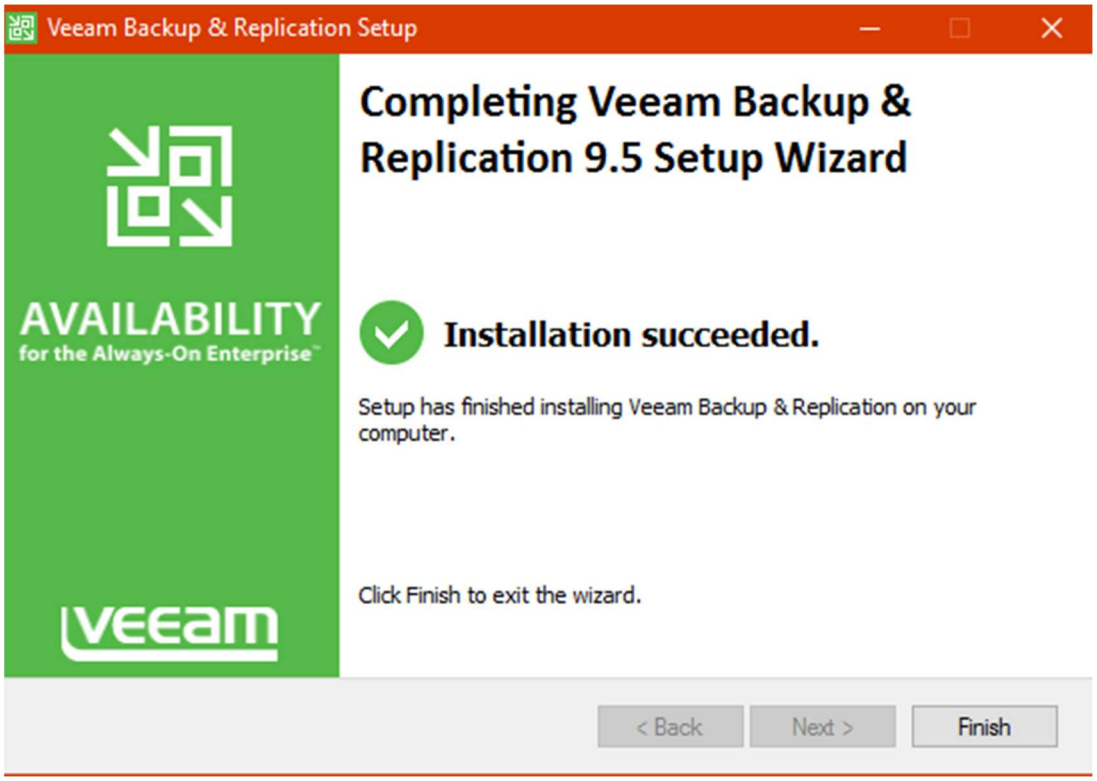
L'installation nécessite la solution Microsoft SQL server 2014 pour fonctionner. Il propose donc de l'installer pour nous. Il suffit de sélectionner « Install ».



Une fois les autres composants installés, Next.

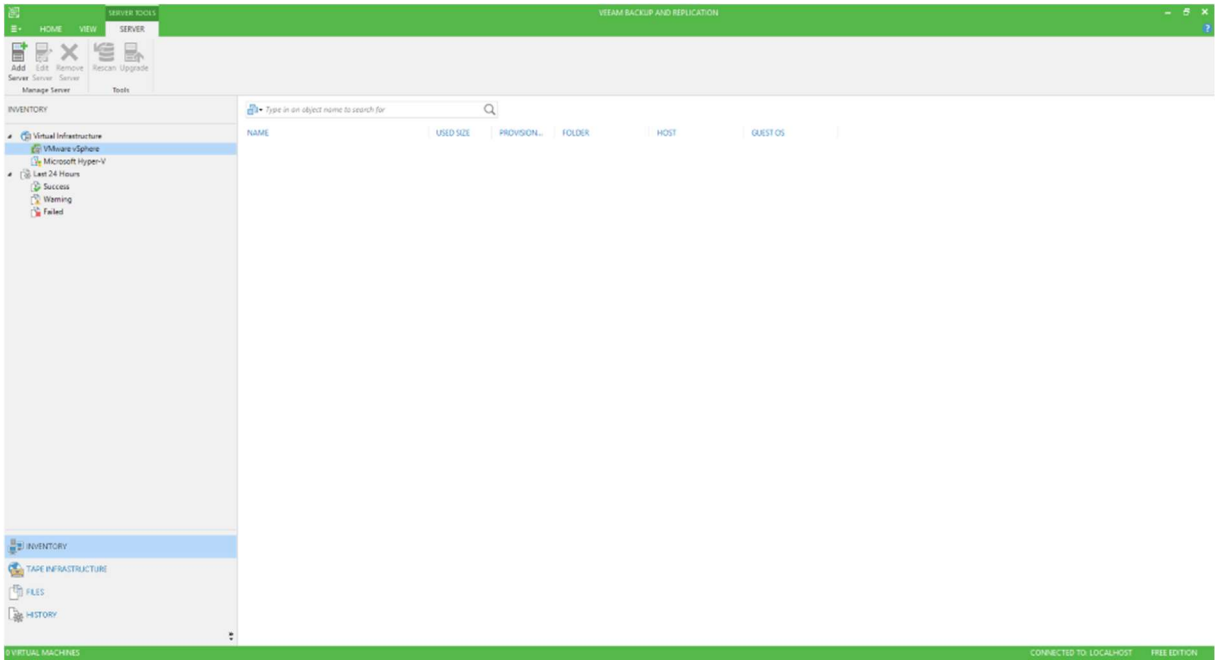


Ici est la dernière étape avant l'installation, ici nous pouvons modifier les ports utilisés par le logiciel, la base de données SQL etc.

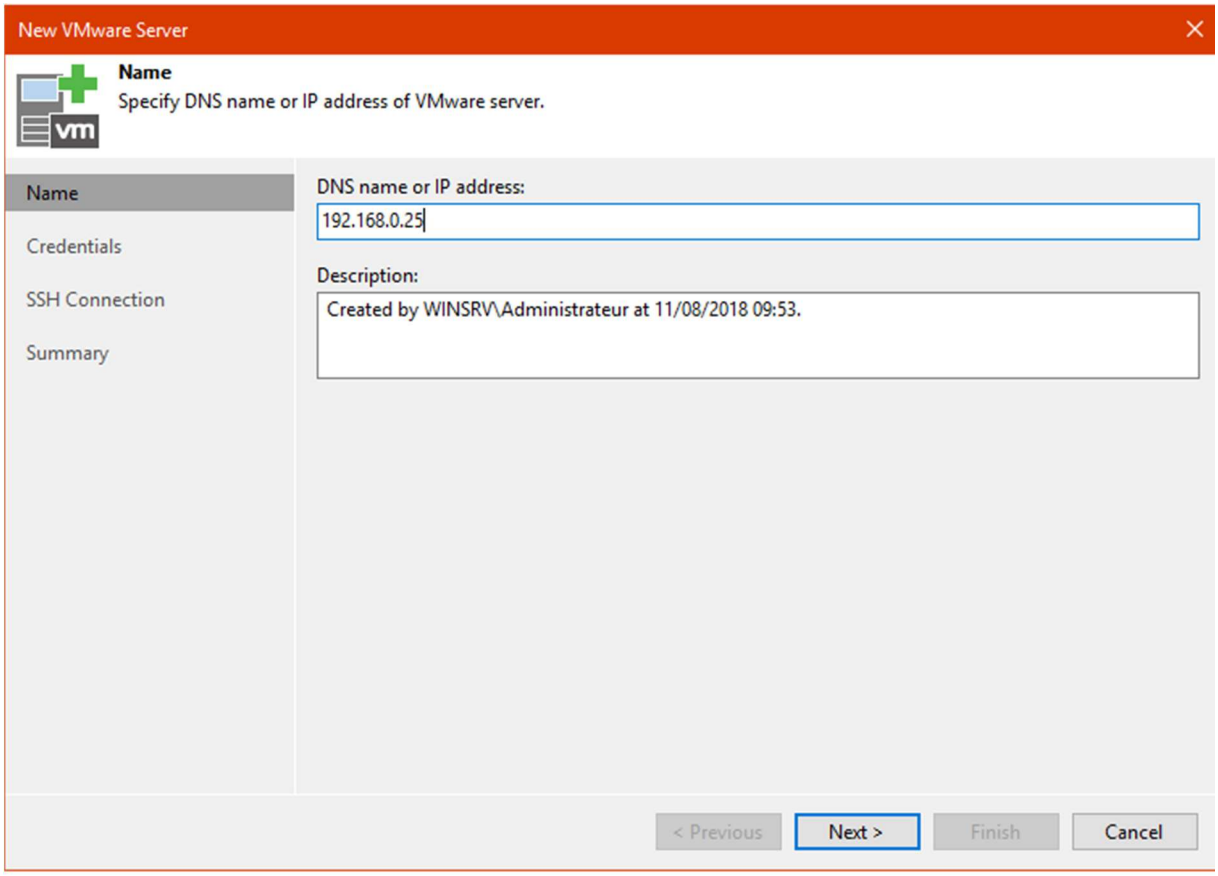


Une fois l'installation terminée, il est demandé de redémarrer le serveur.

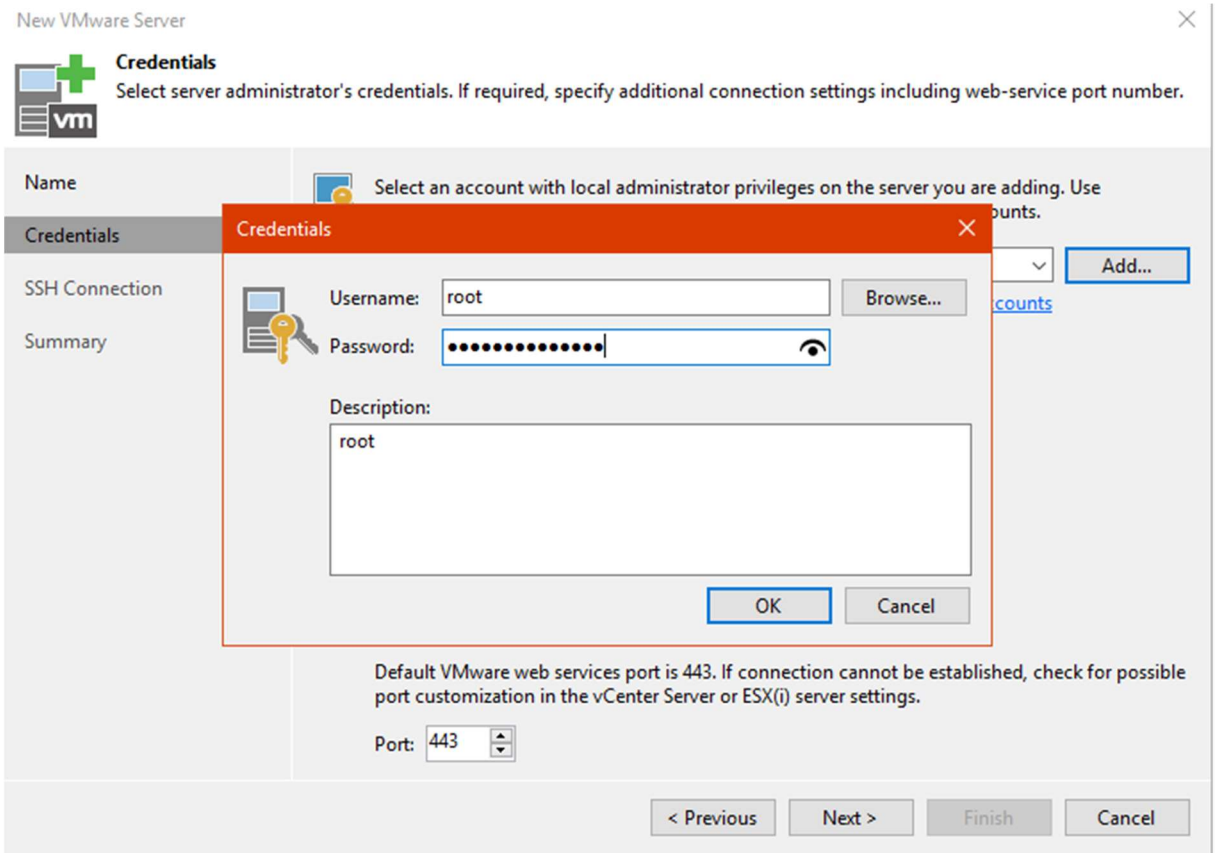
2. Configuration



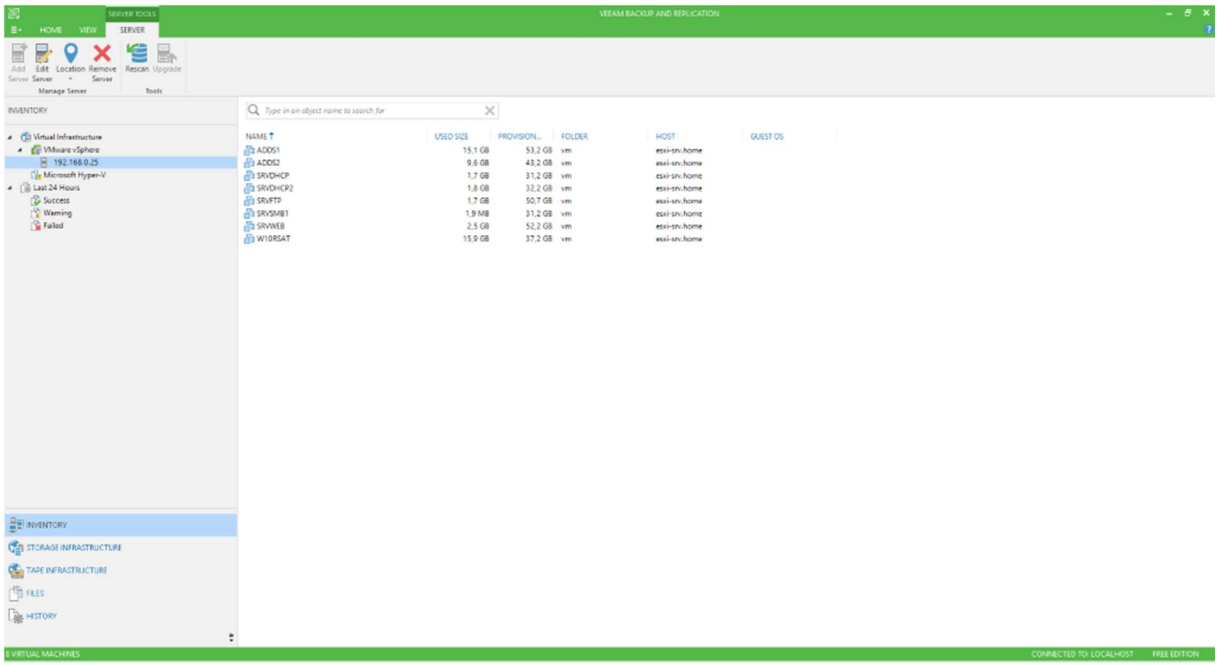
Une fois Veeam installé, nous pouvons le configurer.



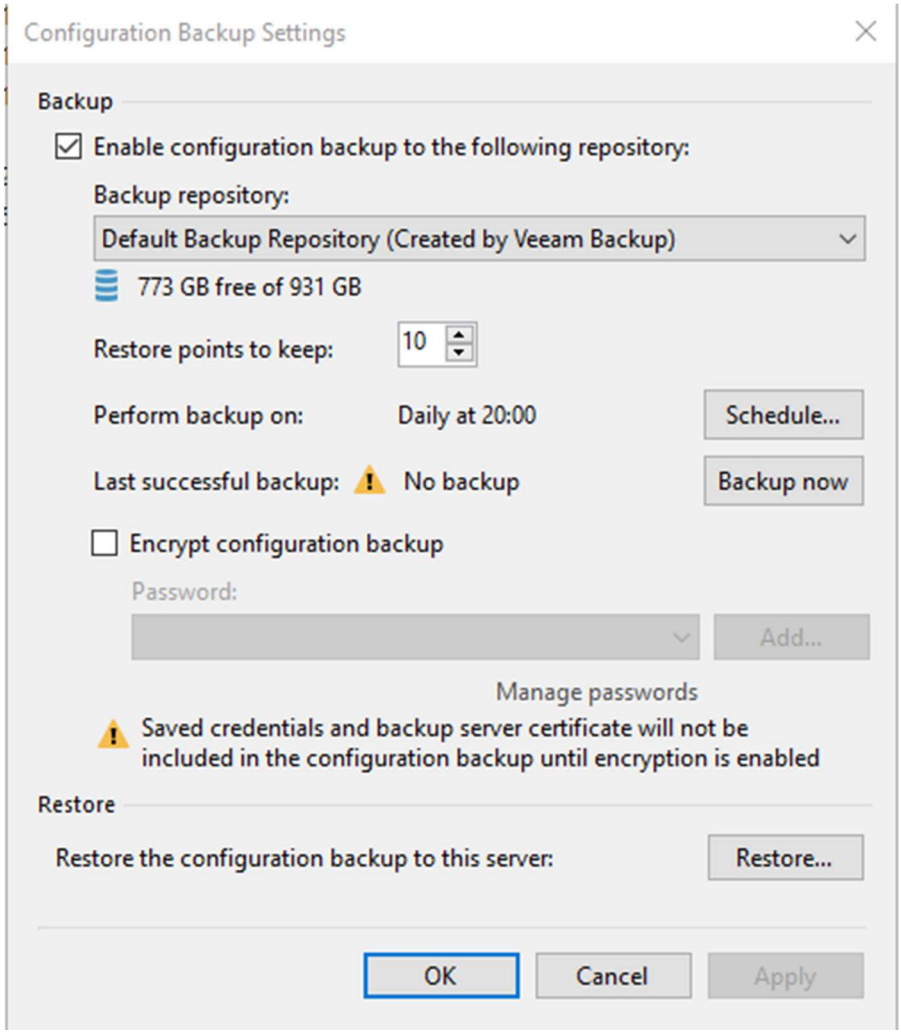
Pour configurer sauvegarder notre serveur, il faut au préalable ajouter notre serveur ESXI



Pour ajouter le serveur, il est demandé les identifiants de l'ESXI.



Voici le récapitulatif de l'ajout de notre serveur.



Voici le récapitulatif de l'ajout de notre serveur.

SRVWEB_2018-08-11T10024...	Backup	0% completed	11/08/2018 10:02
SRVSMB1_2018-08-11T1002...	Backup	0% completed	11/08/2018 10:02
SRVFTP_2018-08-11T100231...	Backup	0% completed	11/08/2018 10:02
SRVDHCP2_2018-08-11T100...	Backup	0% completed	11/08/2018 10:02
SRVDHCP_2018-08-11T1002...	Backup	0% completed	11/08/2018 10:02
ADDS2_2018-08-11T100209...	Backup	0% completed	11/08/2018 10:02
ADDS1_2018-08-11T100159...	Backup	23% completed	11/08/2018 10:02

Voici notre liste de serveur. Nous allons maintenant configurer notre système de backup. Ici nous pouvons modifier l'endroit où sera créé le backup de nos VM.

D. Licences

Nous ne pouvons pas terminer cette section sur les serveurs sans mentionner les licences nécessaires à la légalité de leur fonctionnement.

Nous devons acheter des licences pour l'ESX, Windows Server 2016 Standard, 2016 (CAL), pour la prise en main sur les serveurs et les postes utilisateurs par le SI, et Veeam Backup and Replication Entreprise.

Pour rappel nous avons 5 serveurs Windows Serveur 2016 dont les licences sont payantes et dépendent du nombre de cœurs de nos serveurs physiques en plus du nombre de machines virtuelles que nous avons.

Le devis se trouve en annexe du document.

E. Conclusion

Le DAF nous a demandé de réfléchir à une solution concernant le lieu de dépannage, les noms des utilisateurs, etc. Nous travaillons encore sur une solution viable de système de gestion de parc.

Nous avons mis en place une gestion de droits utilisateurs avec un Active Directory, le siège social voulait un FTP pour récupérer des fichiers et nous leur avons mis à disposition. Nous avons mis en place un système de partage de fichier entre Windows et Linux.

Les utilisateurs voient maintenant leur utilisation sur les postes cadrées par des GPO afin de leur garantir une meilleure qualité d'utilisation (imprimantes et lecteurs réseaux qui remontent automatiquement, sécurité en phase avec les exigences de l'entreprise).

Nous avons aussi fait en sorte de garantir un temps de rétablissement minime et nous avons élaboré un plan de sauvegarde physique et logique efficace.

Nous pensons pouvoir dire que l'infrastructure système que nous proposons en réponse à ce cahier des charges est certes simple mais surtout pensée et cohérente au regard de Pielco.

De plus, elle n'est pas verrouillée aux futurs changements qui nous attendent.

III. Annexes

A. Scripts

```
51          New-ADOrganizationalUnit -name $ou -path $cheminusers `
52          -ProtectedFromAccidentalDeletion $false -Verbose}
53          catch{}
54      }
55  }
56
57
58  ########################
59  #### MENU GENERAL #####
60  ########################
61  function menu()
62  {
63
64  write-host "########################## PROJET EVOLUTION ################################################ "
65  Write-Host "#################################################################################################### "
66  Write-Host "######################  Votre Choix SVP ? ################################################### "
67  Write-Host "#################################################################################################### "
68  Write-Host "1 : Création Unités d'organisation"
69  Write-Host "2 : Création des groupes"
70  Write-Host "3 : Création des users"
71  Write-host "4 : Suppression totale"
72  Write-Host "0 : Quitter le projet"
73  $choix=read-host "Choix ? "
74
75      switch ($choix)
76      {
77          1 {creation_ous;menu}
78          2 {creation_groupes;menu}
79          3 {creation_users;menu}
80          4 {suppression;menu}
81          0 {exit}
82          default {menu}
83      }
84  }
85
86   ################################ GROUPES ####################
87  function creation_groupes()
88  {
89      foreach ($i in $csv)
90      {
91          $service=$i.service.toUpper()
92          $GG="GG_"+$service
93          $GU="GU_"+$service
94          $GDL_R="GDL_R_"+$service
95          $GDL_RW="GDL_RW_"+$service
96          $GDL_F="GDL_F_"+$service
97          $chemingroup="OU="+$service+","+$chemingroupes
98
99  try{New-ADGroup -Name $GG -path $chemingroup -GroupCategory Security -GroupScope Global -Verbose}
```

```
99  try{New-ADGroup -Name $GG -path $chemingroup -GroupCategory Security -GroupScope Global -Verbose}
100 catch{}
101 try{New-ADGroup -Name $GU -path $chemingroup -GroupCategory Security -GroupScope Universal -Verbose}
102 catch{}
103 try{New-ADGroup -Name $GDL_R -path $chemingroup -GroupCategory Security -GroupScope DomainLocal -Verbose}
104 catch{}
105 try{New-ADGroup -Name $GDL_RW -path $chemingroup -GroupCategory Security -GroupScope DomainLocal -Verbose}
106 catch{}
107 try{New-ADGroup -Name $GDL_F -path $chemingroup -GroupCategory Security -GroupScope DomainLocal -Verbose}
108 catch{}
109
110 Add-ADGroupMember $GU -Members $GG
111 Add-ADGroupMember $GDL_R -Members $GU
112 Add-ADGroupMember $GDL_RW -Members $GU
113 Add-ADGroupMember $GDL_F -Members $GU
114   }
115 }
116
117 ######################   USERS ############################
118 function creation_users()
119
120     {  $pass=ConvertTo-SecureString("Formation2018!") -AsPlainText -Force
121
122        foreach ($i in $csv)
123        {
124 $nom=$i.nom.Toupper()
125 $prenom=$i.prenom.substring(0,1).toUpper()+$i.prenom.substring(1).tolower()
126 $nomcomplet=$nom+" "+$prenom
127 $login=$prenom.tolower()+"."+$nom.tolower()
128 $upn=($login+"@"+$env:userdnsdomain).ToLower()
129 $description=$i.description
130 $fonction=$i.fonction
131 $service=$i.service
132 $chemin="OU="+$service+","+$cheminusers
133 $groupe="GG_"+$service
134
135  new-aduser -name $nomcomplet -GivenName $prenom -Surname $nom `
136  -DisplayName $nomcomplet -SamAccountName $login -UserPrincipalName $upn `
137  -path $chemin -Department $service -Description $description `
138  -AccountPassword $pass -Title $fonction -ChangePasswordAtLogon $true `
139  -Enabled $true -EmailAddress $upn -Verbose
140
141  Add-ADGroupMember $groupe -Members $login
142  creation_dossiers($login,$service)
143  permissions
144     }
145     }
146
```

```
146
147  function creation_dossiers()
148  {
149      $dossierperso=$dfspath+"\Perso\"
150      $dossierservice=$dfspath+"\Services\"
151
152      New-Item -name $login -ItemType Directory -path $dossierperso
153
154  try {
155      New-Item -name $service -ItemType Directory -path $dossierservice
156      }
157  catch
158  { write-host "Les dossiers "+$dossierservice + "Existe déjà"
159          }
160  }
161
162  function suppression()
163  {
164  Remove-ADOrganizationalUnit -Identity $cheminbase -Recursive -Confirm:$false -Verbose
165
166  $dossierperso=$dfspath+"\perso\"
167  $listedossierperso=get-childitem -Directory -path $dossierperso
168  $dossierservice=$dfspath+"\services\"
169  $listedossierservice=get-childitem -Directory -path $dossierservice
170
171  foreach ($i in $listedossierperso)
172      { $nomdossier=$dossierperso+$i.name
173        remove-item -Path $nomdossier -Recurse -Verbose
174      }
175  foreach ($i in $listedossierservice)
176      { $nomdossierserv=$dossierservice+$i.name
177        remove-item -Path $nomdossierserv -Recurse -Verbose
178      }
179  }
180
181   function permissions()
182  {  $cheminperso=$dfspath+"\perso\"
183      $cheminservice=$dfspath+"\services\"
184  $listedossierperso=Get-ChildItem -Directory -path $cheminperso
185  $listedossierservice=Get-ChildItem -Directory -path $cheminservice
186      foreach ($dossier in $listedossierperso)
187       {
188        $chemindossier=$dossier.fullname
189        $acl=(get-item $chemindossier).GetAccessControl('Access')
190        $username=$dossier.name
191  $ar=new-object security.accesscontrol.filesystemAccessRule($username,'Modify','ContainerInherit,ObjectInherit','none','Allow')
192        $acl.SetAccessRule($ar)
193        set-acl -Path $chemindossier -AclObject $acl
194        }
195  foreach ($dossier in $listedossierservice)
```

```
194       }
195  foreach ($dossier in $listedossierservice)
196       {
197        $chemindossier=$dossier.fullname
198        $acl=(get-item $chemindossier).GetAccessControl('Access')
199        $gdl="GDL_RW_"+$dossier.name
200        $ar=new-object security.accesscontrol.filesystemAccessRule($gdl,'Modify','ContainerInherit,ObjectInherit','none','Allow')
201        $acl.SetAccessRule($ar)
202        set-acl -Path $chemindossier -AclObject $acl
203        }
204  }
205
206
207  ######################### CORPS DU PROGRAMME ##################
208  menu
```

B. Devis

Devis en EUR
N° DEV0001

Émis le 21/08/18 expire le 24/09/18

Licences nouvelle infrastructure

DESCRIPTION	QUANTITÉ	PRIX UNITAIRE	MONTANT	TVA
Veeam Backup and Replication Entreprise + 3 ans support	2	1 522,00	3 044,00	1
Windows Server 2016 Standard	4	889,00	3 556,00	1
Virtual Machine ESX + 3 ans support	2	2 096,00	4 192,00	1
Dell PowerEdge R330	2	1 790,00	3 580,00	1
Dell PowerEdge T310	1	650,00	650,00	1
Disques durs WD Red 3To	10	109,00	1 090,00	1
Windows Server 2016 (CAL)	5	130,00	650,00	1

	%	MONTANT	TVA
1	20	16 762,00	3 352,40

TOTAL HT	16 762,00
TOTAL TVA	3 352,40
TOTAL TTC	20 114,40
A LA COMMANDE	0,00
A ÉCHÉANCE	20 114,40

Devis LDLC pour notre nouvelle infrastructure.

IV. Glossaire

Active directory : service d'annuaire centralisé d'identification et d'authentification à un réseau d'ordinateurs Il permet également l'attribution et l'application de stratégies, l'installation de mises à jour critiques par les administrateurs. *Active Directory* répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées (Wikipédia)

Contrôleur de domaine : Un serveur informatique hébergeant l'annuaire Active Directory est appelé « **contrôleur de domaine** ». Active Directory stocke ses informations et paramètres dans une base de données distribuée sur un ou plusieurs **contrôleurs de domaine**, la réplication étant prise en charge nativement (Wikipédia)

DDOS : Attaque par dénis de service consiste à rendre un service indisponible en lui faisant un trop gros nombre de requêtes simultanées.

DHCP : Dynamic Host Configuration Protocol, permet d'automatiser l'attribution des adresses IP au sein d'un réseau.

DNS : Le Domain Name System, généralement abrégé **DNS**, est un système permettant de traduire les noms de domaines (privés ou publiques) en adresses IP, on parle alors de résolution de nom de domaine.

ESXI : C'est un système d'exploitation qui permet de gérer des machines virtuelles.

FTP : File Transfer Protocol, c'est un protocole de communication permettant de partager des fichiers en sur un réseau TCP/IP.

Raid 5 : C'est une technique de répartition de stockage répartissant les données sur plusieurs disques durs afin d'améliorer les performances, la sécurité et la tolérance aux pannes. Ce système ne supporte que la perte d'un disque d'un à la foi, auquel cas les données deviennent irrécupérables.

Root : Désigne un utilisateur occupant un rôle d'administrateur sur Unix.

SElinux : Security-Enhanced-Linux est un module de sécurité linux permettant de définir une politique de contrôle d'accès obligatoire aux éléments d'un système issu de linux (Wikipédia).