



PROJET EVOLUTION

Stephen Dufour, Enzo Berard, Dylan Roche, Rémy Latzer

GMSI 44

Table des matières

I.	Introduction	4
A.	Présentation de VESTIGIO.....	4
B.	Objectifs du Projet EVOLUTION	5
1.	Cahier des charges	6
II.	Infrastructure Réseau	8
A.	Schéma réseau :	9
III.	Windows Server	10
A.	Installation de Windows Server 2016	10
B.	Active Directory et DNS.....	17
1.	Définition et rôles Active Directory :	17
2.	Définition et rôles du DNS.....	17
3.	Installation :	17
C.	Fonctionnalité serveur : Le DNS.....	22
D.	Les GPO	28
4.	Définition et rôles	28
5.	Les points forts.....	28
6.	Les besoins du cahier des charges :	29
E.	Outils RSAT	30
F.	DFS	31
G.	Serveur d'Impression	40
H.	Serveur WSUS	42
IV.	Linux Serveur.....	49
A.	Installation de CentOS 7.....	49
B.	NFS	55
1.	Serveur NFS.....	55
2.	Client NFS	55
C.	FTP.....	56
D.	Mise en place de Samba	57
E.	Mise en place du DHCP	59
F.	Intégration des Serveur Linux dans Active Directory.....	61
V.	Base de données	62
A.	Installation de GLPI	62

1.	Configuration du serveur web	62
2.	Interface GLPI.....	66
B.	Installation de Fusion Inventory	70
1.	Installation du plugin dans GLPI.....	70
2.	Installation de l'agent	71
VI.	Solution de sauvegarde.....	77
VII.	Prise en main à distance	78
VIII.	Conclusion.....	79
IX.	Annexes :.....	80
A.	Charte graphique	80
B.	Automatisation des tâches (Script Powershell)	81
C.	Devis.....	88
D.	Planning.....	89
E.	Lexique	90

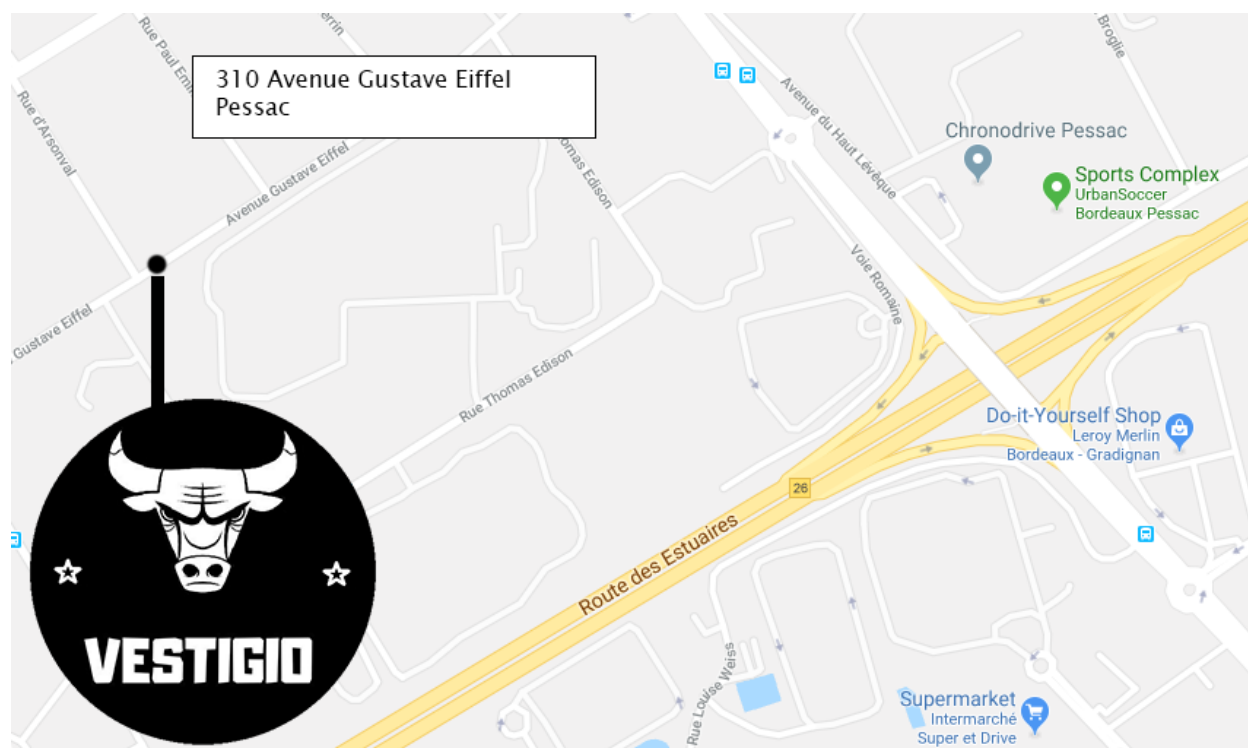
I. Introduction

A. Présentation de VESTIGIO

L'entreprise VESTIGIO est une centrale d'achat pour un regroupement de franchises. Elle fournit deux lignes de produits aux franchisés : une ligne de vêtements ainsi que du matériel sportif.

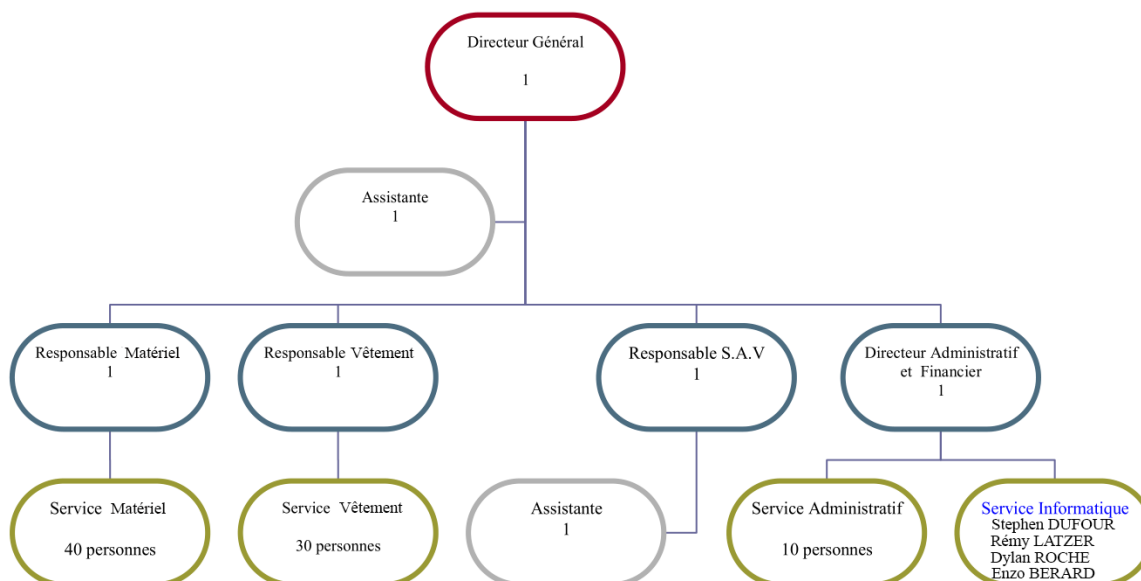
L'entreprise emploie actuellement 90 salariés. Elle dispose d'un capital de 425 000€ et d'un chiffre d'affaire de 1.9M€ pour l'année 2017.

Localisation de l'entreprise :



L'entreprise se situe à Pessac au 310 Avenue Gustave Eiffel. Son numéro SIRET est le 416 214 589.

Organigramme de l'entreprise :



Le service informatique est composé de 4 techniciens qui ont la charge du projet :

Stephen DUFOUR

Enzo BERARD

Rémy LATZER

Dylan ROCHE

B. Objectifs du Projet EVOLUTION

- Mettre en œuvre les outils d'administration de Windows Server 2016
- Mettre en œuvre les outils d'administration de UNIX/LINUX (dans notre projet : CentOS 7)
- Être capable de sécuriser l'accès aux réseaux et aux données de l'entreprise
- Rédiger des rapports écrits adaptés au contexte professionnel
- Être capable de créer et gérer une base de données relationnelle
- Être capable d'automatiser les tâches à l'aide d'un outil de programmation (Powershell)

1. Cahier des charges

À la suite d'une mise au point avec le Directeur Administratif et Financier, celui-ci nous a mentionné quelques idées et remarques.

Parmi ses idées, nous en avons retiré les points importants suivants :

- Manque d'information sur le parc informatique de l'entreprise, entraînant une perte de temps pour l'équipe informatique lors de ses interventions.
- Il y'a aucune gestion de droit d'utilisateurs.
- Le siège social a besoin d'un serveur FTP afin de récupérer des fichiers dessus.

Ces problématiques nous ont permis de mieux définir le cahier des charges. Il y'a un besoin important de stocker et centraliser les informations du parc informatique via une base de données mais également de mettre en place des outils d'administration du parc informatique avec une solution de tolérance aux pannes sécurisée.

Nous avons donc élaboré une liste de solutions techniques à mettre en œuvre pour notre entreprise :

- Windows Server 2016 :

• DNS

Configurer les zones (sur votre document, préciser le nombre de zones que vous avez)

Prévoir une solution de tolérance de panne et la justifier

• Sécurité

Le 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 est prioritaire sur toutes les impressions et les utilisent 24/24

Le service informatique a contrôle total sur toutes les impressions

Mme. LAPORTE et Mlle ADA (les assistantes des services SAV et direction peuvent imprimer chez les Services Informatique, Service Produit A et B.

• Les connexions réseaux

Mme BEZIAT, ELLA, AYO et ACIEN ne peuvent se connecter qu'entre 08 heures et 18 heures et à 19 heures elles doivent être déconnectées (elles sont du service Produit A)

Aucun salarié sauf la direction, le SAV et l'informatique ne peut se connecter entre 20 heures et 07 heures du matin.

- Stratégie locale

En dehors de la direction et du services informatique, personne ne peut installer de logiciels sur sa machine ni modifier l'heure

Les lecteurs disquette et 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.

A 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'évènements

- Accès à distance

Tous les postes doivent être accessibles à distance

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

Prévoir une solution de tolérance de panne, la justifier et l'expliquer

Donner une liste de matériels prévus et les coûts associés

- Créer des scripts facilitant l'administration des serveurs

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

- Serveurs Linux :

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

II. Infrastructure Réseau

Nomenclature des serveurs de l'infrastructure :

Serveurs			
Services	Versions	Adressage IP	Nom Netbios
AD-DS 1	Windows 2016 Core	192.168.10.1	ves-ad01
AD-DS 2	Windows 2016 Core	192.168.10.2	ves-ad02
DHCP1	CentOS 7	192.168.10.3	ves-dhcp01
DHCP2	CentOS 7	192.168.10.4	ves-dhcp02
NFS1 Server + Samba + FTP	CentOS 7	192.168.10.5	ves-cent01
NFS2 Client (Sauvegarde)	CentOS 7	192.168.10.6	ves-cent02
IMPR + WSUS + RSAT	Windows 2016 Graphique	192.168.10.7	ves-imp
Web	CentOs 7	192.168.10.8	ves-web01
DFS + DFSR	Windows 2016 Core	192.168.10.9	ves-file01
DFS + DFSR	Windows 2016 Core	192.168.10.10	ves-file02
Sauvegarde	Windows 2016 Graphique	192.168.10.18	ves-svg01

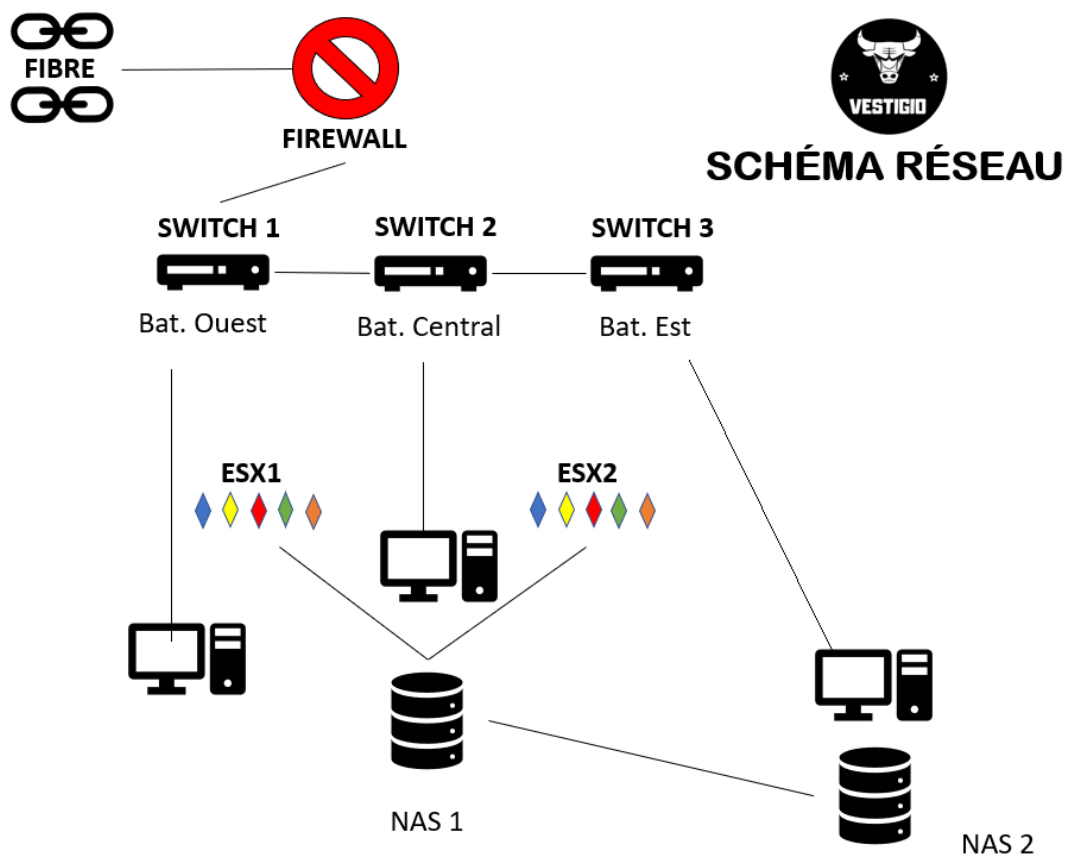
Nous avons effectué l'allocation des adresses IP comme ceci

Passerelle	192.168.10.254
Serveurs	10.1 -> 10.20
Switch	10.21 -> 10.30
DHCP	10.31-> 10.230
Imprimante	10.231 -> 10.240

Les ESX 1 et 2 auront respectivement les adresses 192.168.10.19 et 192.168.10.20.

Les IP des postes clients iront de 192.168.10.31 à 192.168.10.230.

A. Schéma réseau :



Les hôtes suivants seront présents dans ESX1:

Ves-ad01
 Ves-dhcp01
 Ves-cent01
 Ves-file01
 Ves-web01

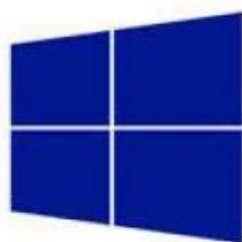
Les hôtes suivants seront présents dans ESX2

Ves-ad02
 Ves-dhcp02
 Ves-cent02
 Ves-file02
 Ves-svg01
 Ves-imp

III. Windows Server

Nous avons choisi la version Core de Windows Server 2016 pour des raisons de gain de performance, mais également de respect du cahier des charges (utiliser la dernière version de Windows Server).

Si besoin est nous aurons les outils RSAT afin de gérer les serveurs Windows via un poste client comme si nous étions sur une version graphique.



Windows Server 2016

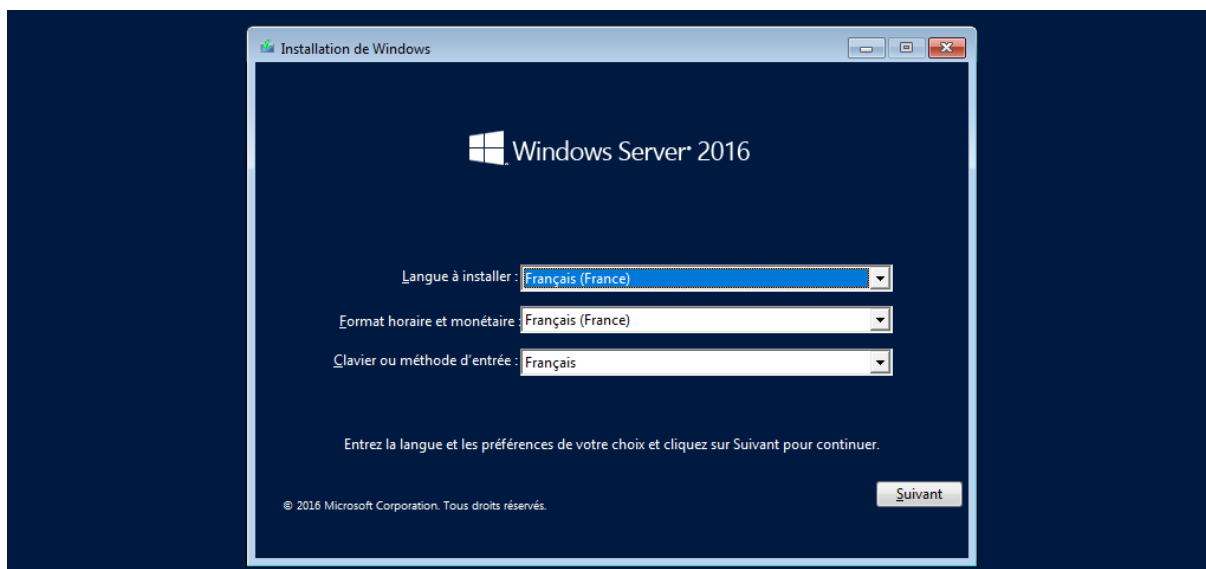
A. Installation de Windows Server 2016

Afin de traiter toutes les procédures utilisées lors du montage de notre projet tous en économisant de la place, nous allons décrire dans cette partie l'installation dite classique de Windows Server 2016.

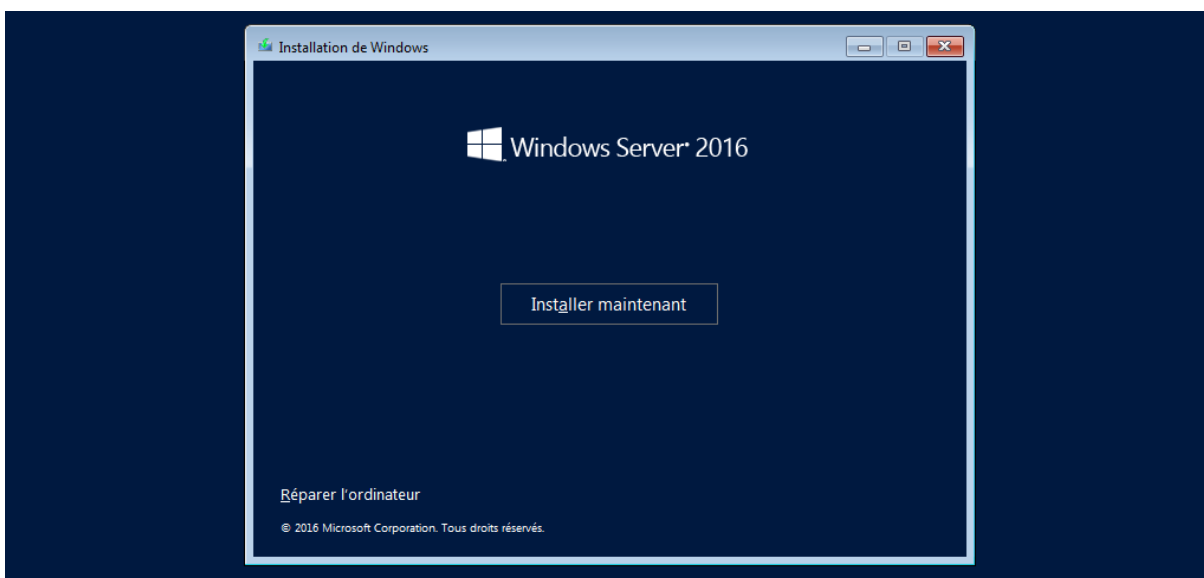
Tout d'abord, il nous faut intégrer dans le lecteur de notre machine un support comme une clé USB ou CD contenant l'image de Windows Server 2016.

Une fois cela fait, nous démarrons directement sur cette image afin d'arriver sur la première fenêtre.

Nous sélectionnons donc la langue française ainsi qu'un format horaire et un clavier français.

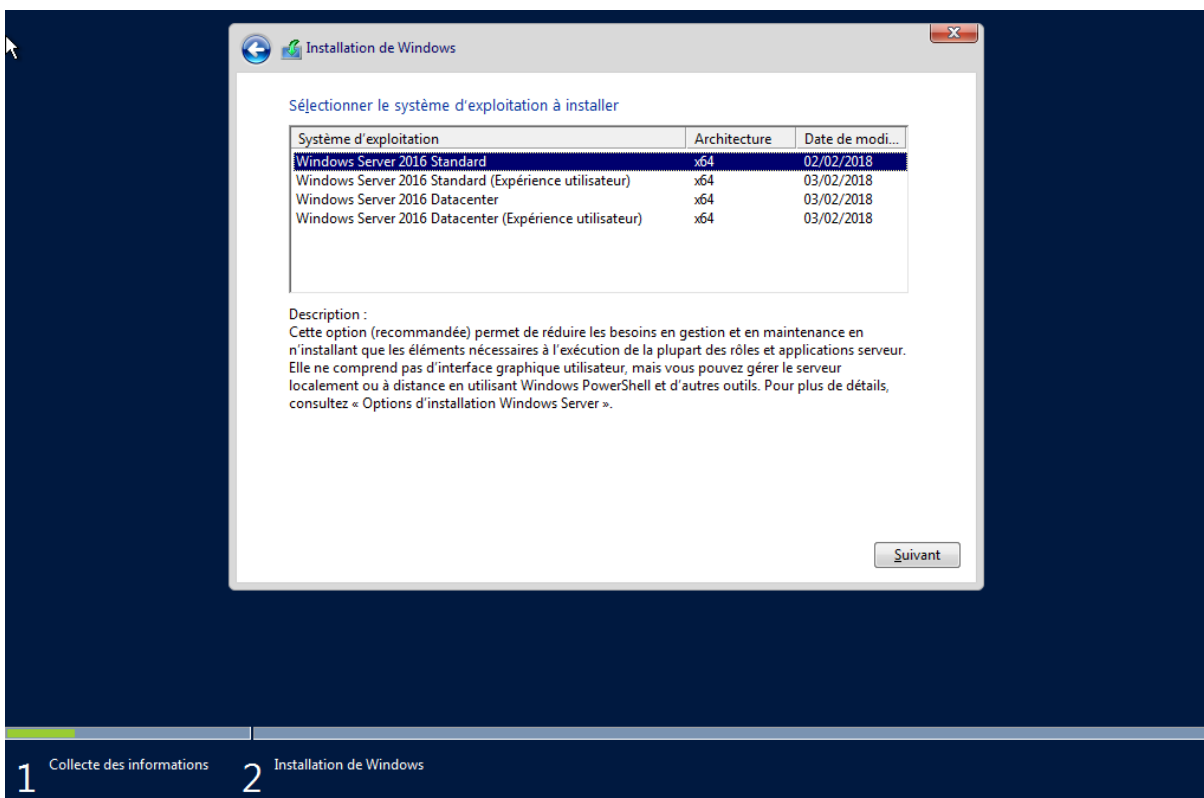


On clique donc sur installer maintenant.



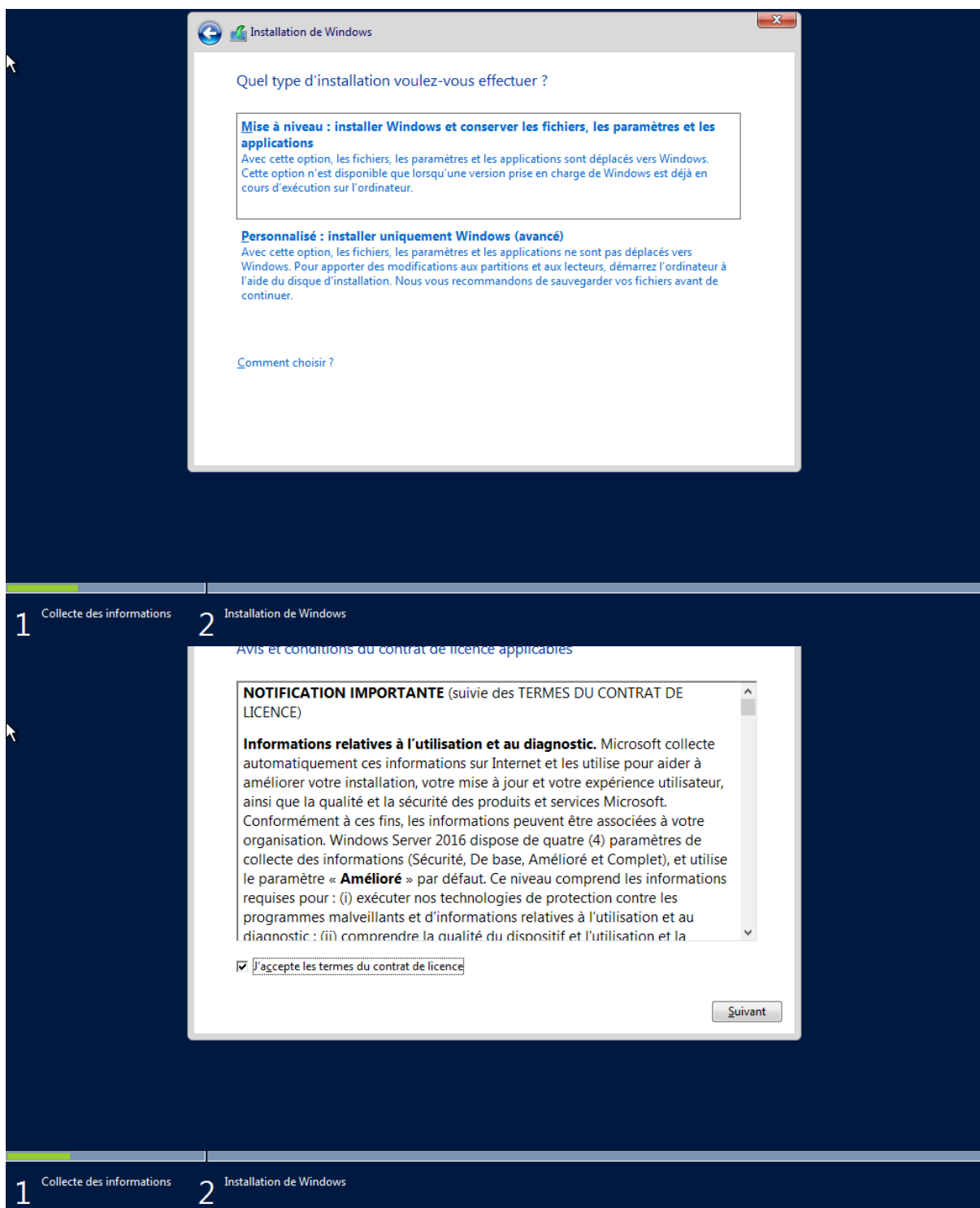
On sélectionne ensuite la version, ici Windows Server 2016 Standard ou Standard (Expérience utilisateur) la différence réside dans le fait que la version « expérience utilisateur » permet de bénéficier d'une interface graphique, utile pour l'administration par les RSAT, par exemple.

Cette version « Expérience Utilisateur » est cependant bien plus gourmande en ressources et c'est pour cela que nous privilégions, sauf en cas de nécessité, la version par défaut.

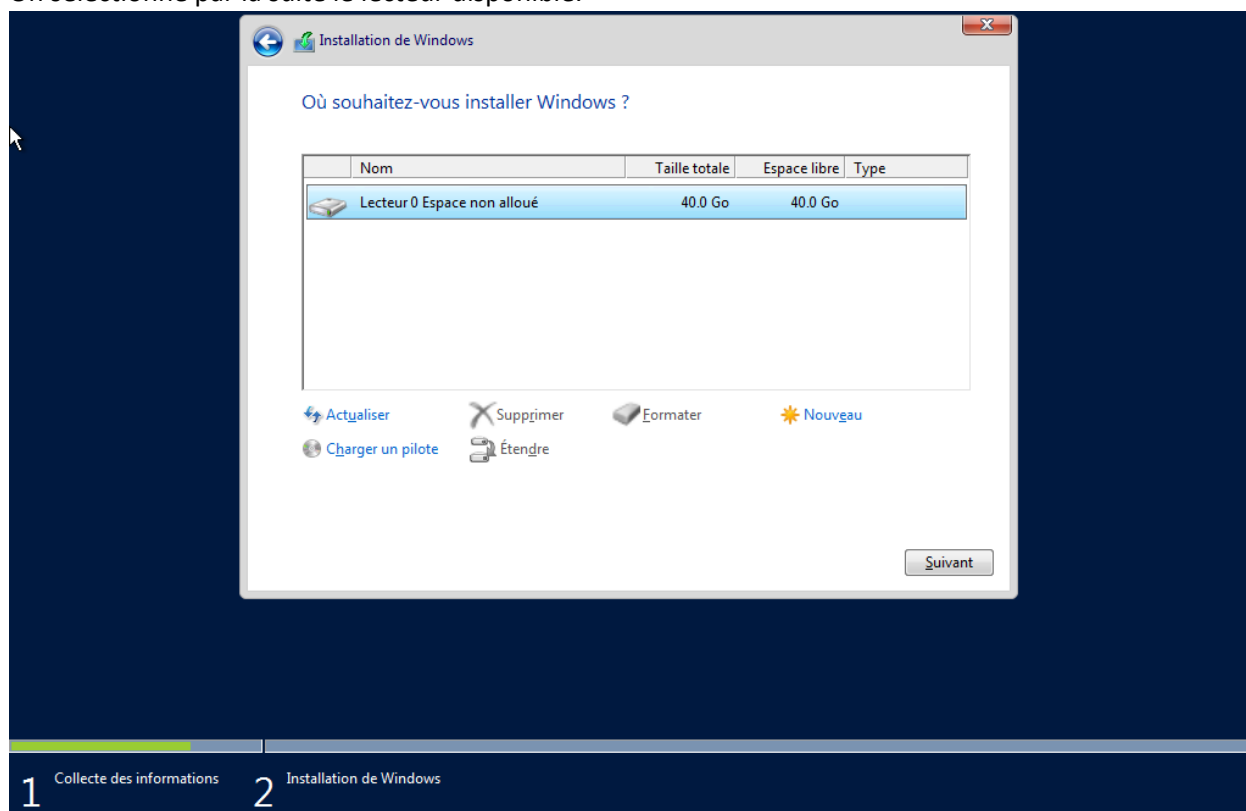


On accepte le contrat de licence.

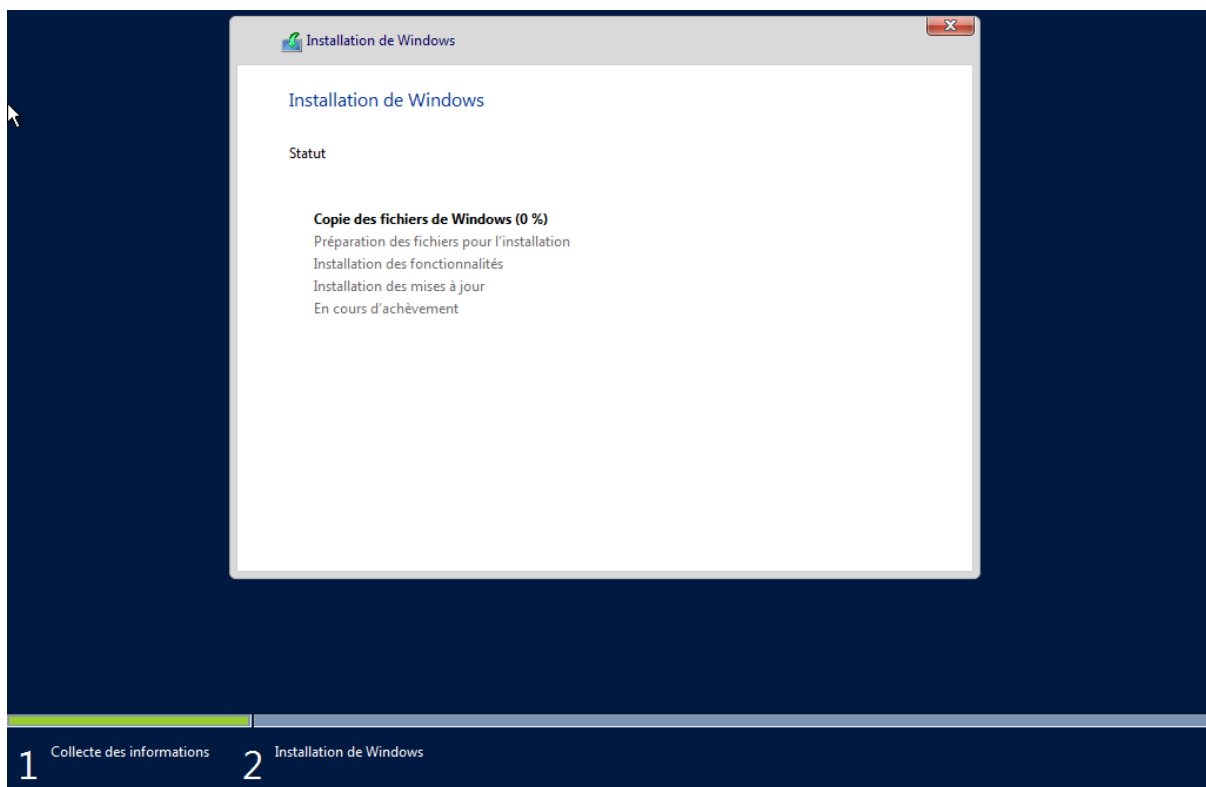
On choisit une installation personnalisée car nous installons un nouveau Windows Server sans mise à niveau.



On sélectionne par la suite le lecteur disponible.

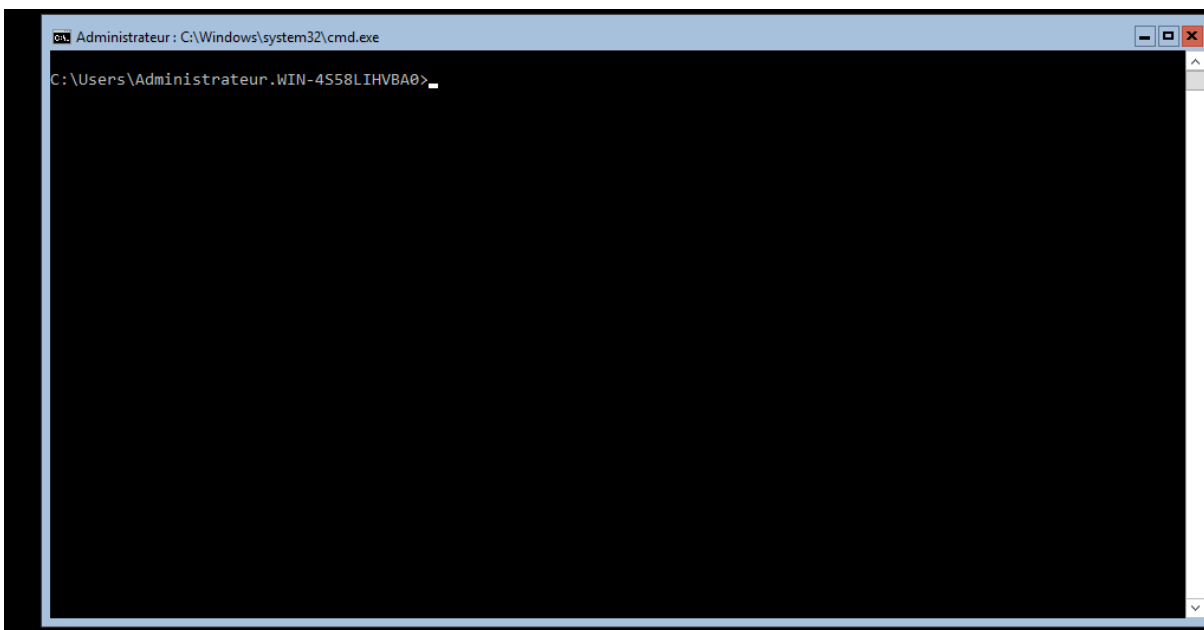
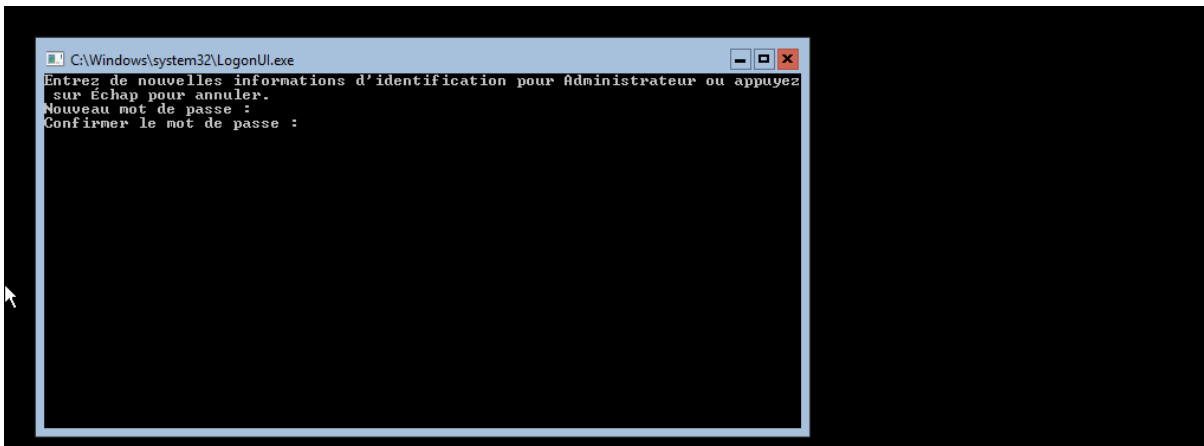


On attend la fin de l'installation.

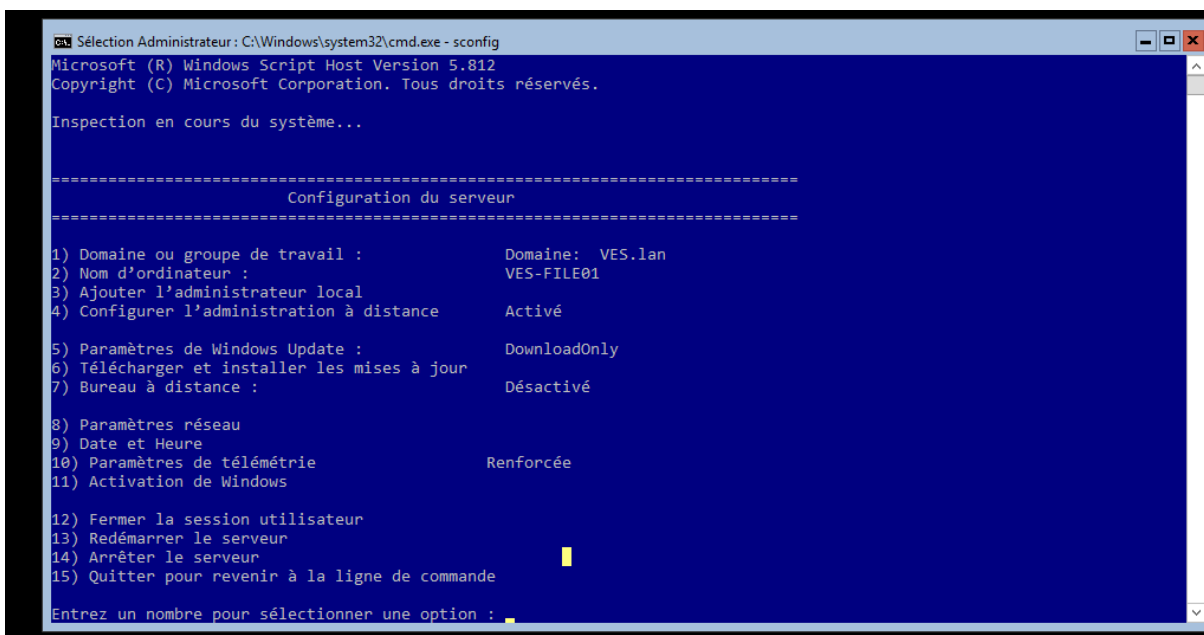


VERSION CLASSIQUE

Dans le cas de la version classique, au redémarrage, cette fenêtre nous demandera de configurer notre mot de passe administrateur, on l'entre donc pour arriver sur une invite de commande.



On va par la suite exécuter la commande sconfig afin d'accéder aux différents paramètres généraux de Windows Server.



Via cette commande sconfig :

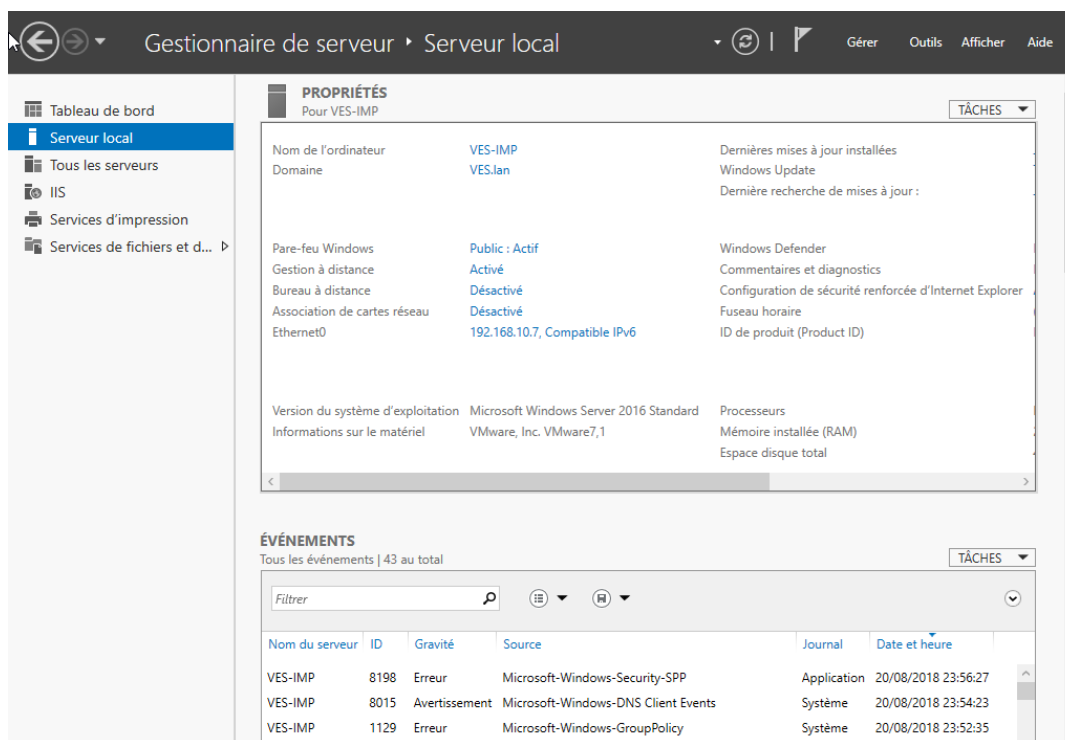
- Renseigner l'adresse Ip, le masque, la passerelle ainsi que les serveurs DFS que nous voulons appliquer à notre serveur ;
- Intégrer notre serveur au contrôleur de domaine, dans le cas où il ne l'est pas ;
- Renommer notre Serveur ;
- Autoriser l'administration à distance ;

Notre serveur est désormais prêt et nous n'avons plus qu'à installer les différents rôles et les configurer.

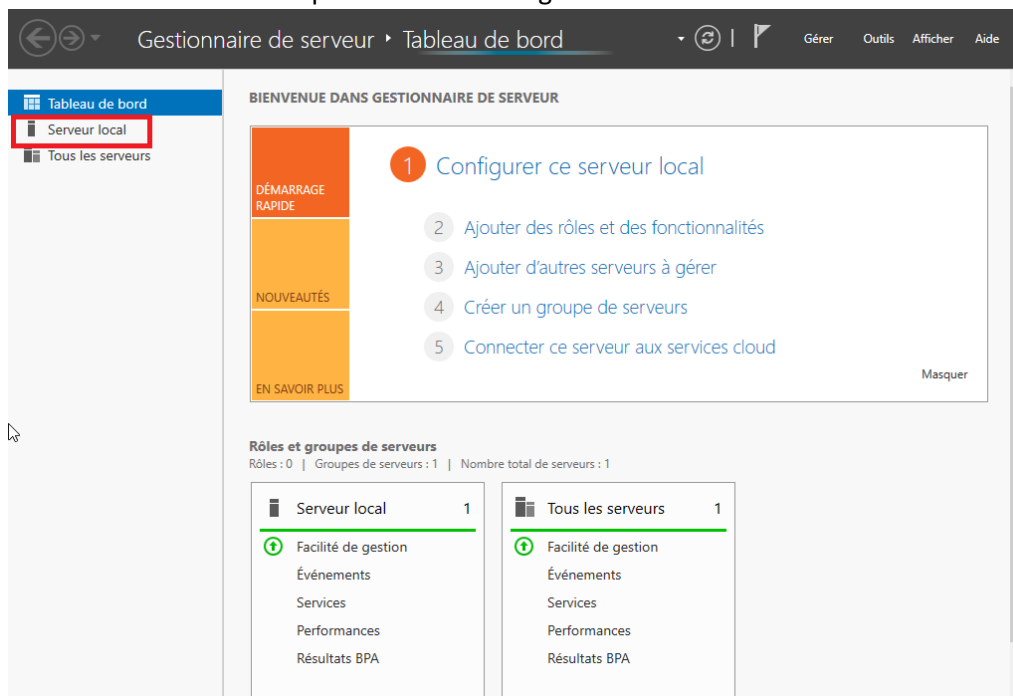
VERSION « EXPERIENCE UTILISATEUR »

Dans le cas de la version graphique, une fenêtre nous demande également au redémarrage de renseigner notre mot de passe administrateur.

On le fait donc et on arrive sur le bureau avec le gestionnaire de serveur qui se lance par défaut.



On va par la suite sur l'onglet « Serveur Local ».



Via cet onglet on va pouvoir :

- Renseigner l'adresse IP, le masque, la passerelle ainsi que les serveurs DFS que nous voulons appliquer à notre serveur ;
- Intégrer notre serveur au contrôleur de domaine, dans le cas où il ne l'est pas ;
- Renommer notre Serveur ;

- Autoriser l'administration à distance ;

Notre serveur est désormais prêt et nous n'avons plus qu'à installer les différents rôles et les configurer.

B. Active Directory et DNS

1. Définition et rôles Active Directory :

Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows. Il est apparu dans le système d'exploitation Microsoft Windows Server 2000 et est basé sur les standards TCP/IP. 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.

2. Définition et rôles du DNS

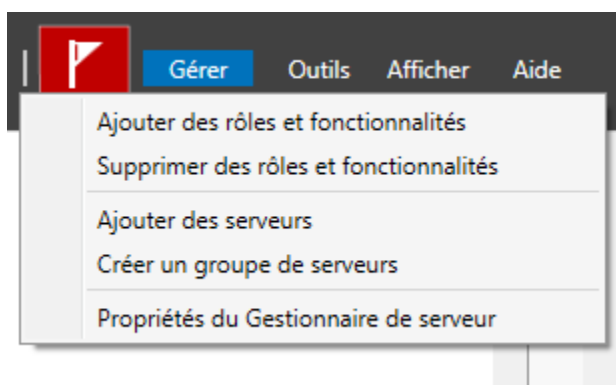
Le serveur DNS (Domain Name System, ou Système de noms de domaine en français) est un service dont la principale fonction est de traduire un nom de domaine en adresse IP. Pour simplifier, le serveur DNS agit comme un annuaire que consulte un ordinateur au moment d'accéder à un autre ordinateur via un réseau. Autrement dit, le serveur DNS est ce service qui permet d'associer à site web (ou un ordinateur connecté ou un serveur) une adresse IP, comme un annuaire téléphonique permet d'associer un numéro de téléphone à un nom d'abonné.

Le Domain Name System a donc été mis en place pour identifier de manière plus simple les différents site web ou serveur. On appelle ça la "Résolution de nom"

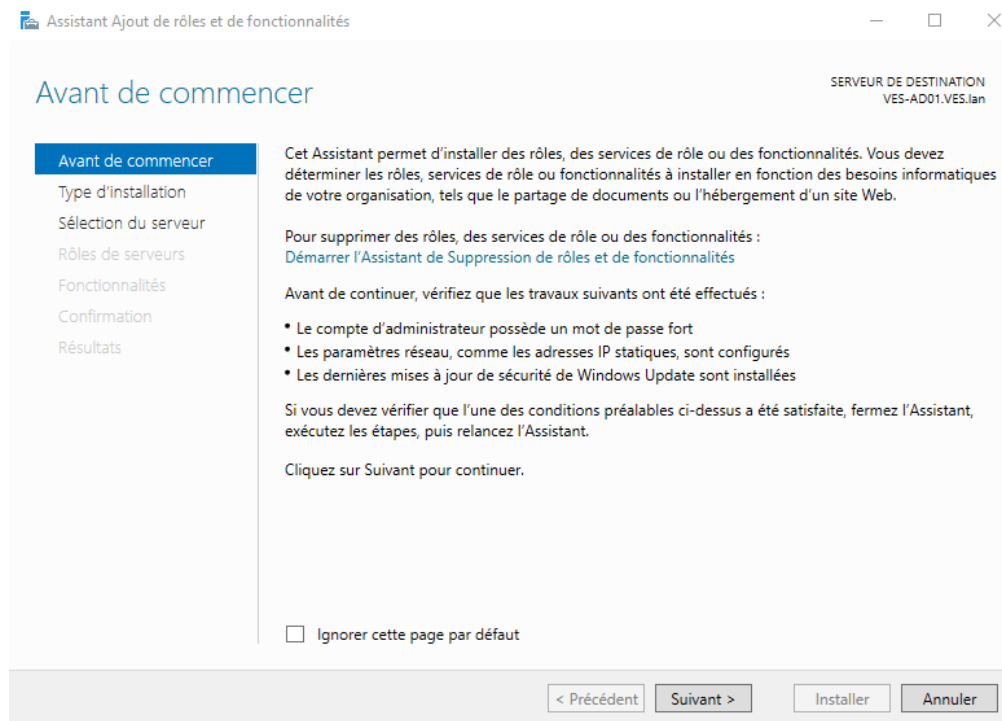
3. Installation :

A la suite de l'installation du Windows server Core 2016, j'ai installé les rôles via notre client lourd Win 10 en RSAT. Voir ci-dessous la procédure.

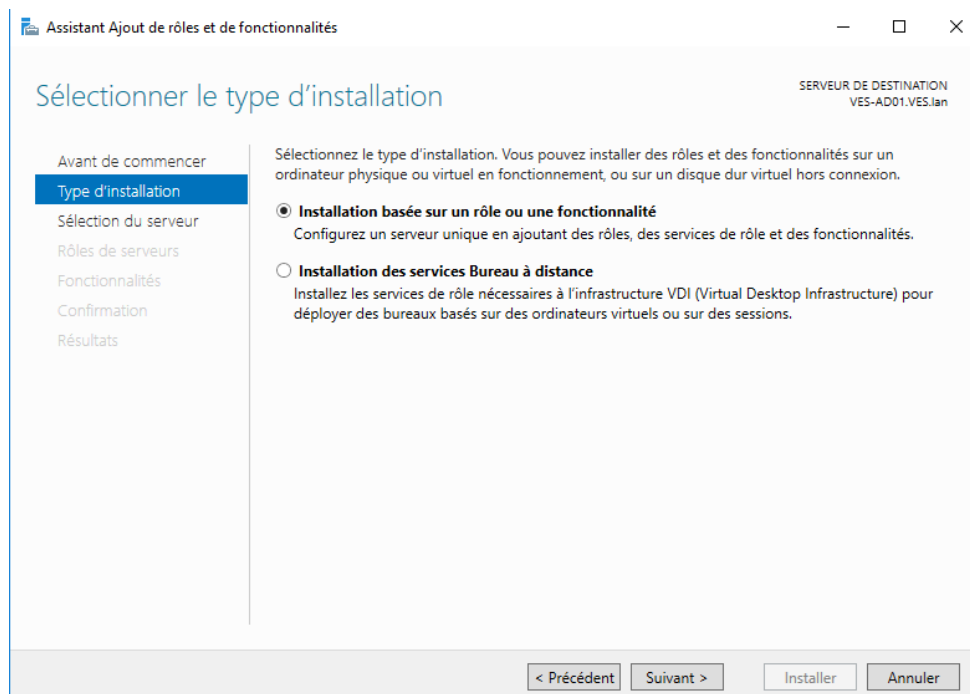
Cliquer sur "Gérer" et "Ajouter des rôles et fonctionnalités"



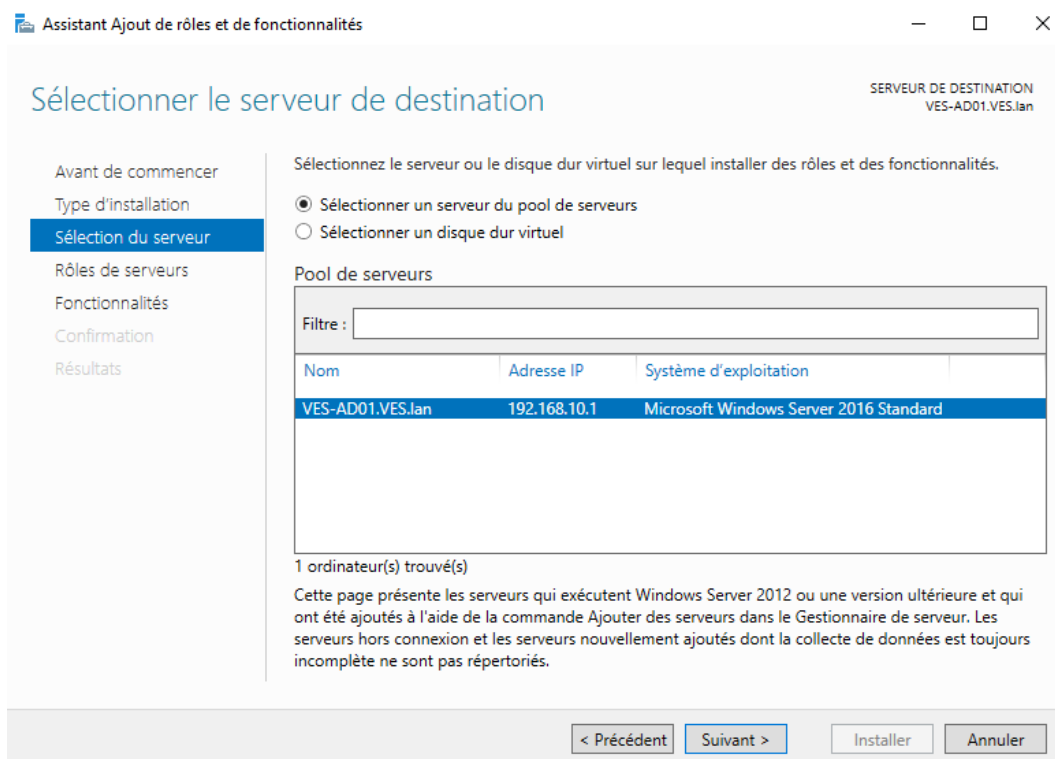
L'assistant d'installation se lance donc, cliquer sur “suivant”



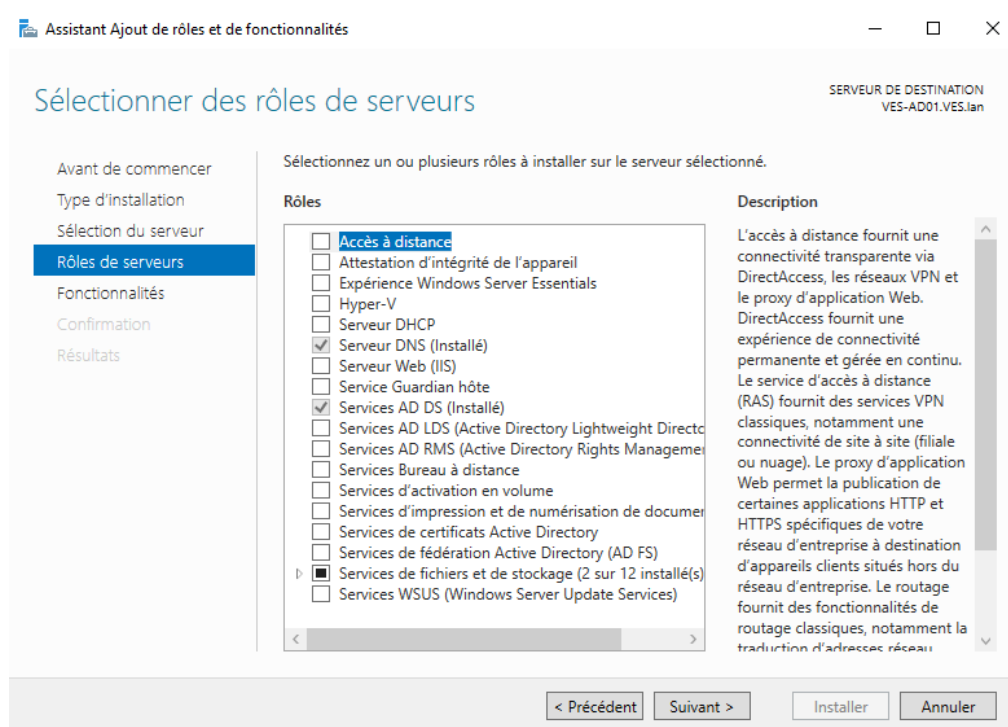
Choisir ensuite le type d'installation "Installation basée sur un rôle ou une fonctionnalité" pour configurer un seul serveur



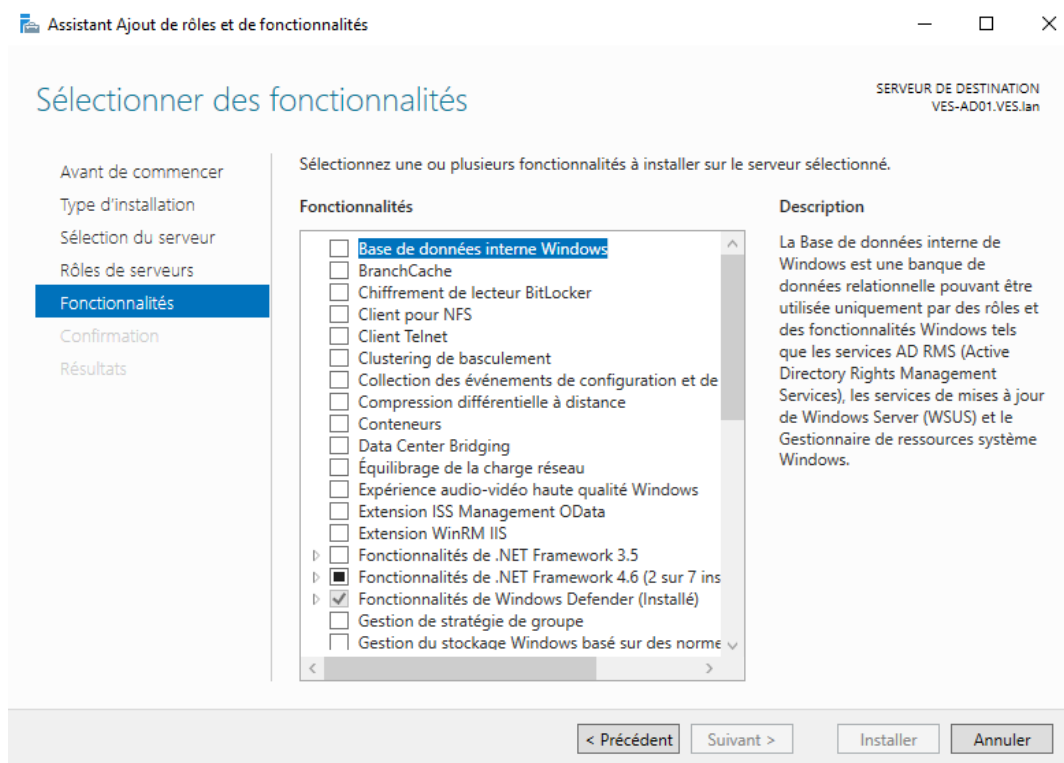
Choisir le serveur sur lequel nous souhaitons installer le rôle puis “Suivant”



Choisir les rôles Service ADDS



Nous n'avons pas besoin de fonctionnalités donc "Suivant"



Notre Active Directory n'est pas encore prêt, nous avons seulement installé le rôle. Il vous faut donc promouvoir ce serveur en tant que contrôleur de domaine. Cliquer donc sur Promouvoir ce serveur en contrôleur de domaine



Sélectionner "Ajouter une nouvelle forêt" dans notre cas c'est VES.lan.

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 :

Choisir le niveau fonctionnel, dans notre cas c'est Windows Server 2016. Il sera également serveur DNS. Nous avons aussi inscrit un mot passe de restauration des services d'annuaire par soucis de sécurité.

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 :

Un message d'erreur en jaune vient alerter de la délégation du serveur DNS. Il n'y a rien à faire à ce stade, cliquer simplement sur Suivant pour continuer.

Options DNS

 Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est intro

Configuration de déploie... Options du contrôleur de... Options DNS

Spécifier les options de délégation DNS

☐ Créer une délégation DNS

Vérifier le nom de domaine Net Bios du domaine pour notre cas : VES

Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire.

Le nom de domaine NetBIOS :

Spécifier l'emplacement de la base de données AD DS, des fichiers journaux et de SYSVOL

Dossier de la base de données :	<input type="text" value="C:\Windows\NTDS"/>	<input type="button" value="..."/>
Dossier des fichiers journaux :	<input type="text" value="C:\Windows\NTDS"/>	<input type="button" value="..."/>
Dossier SYSVOL :	<input type="text" value="C:\Windows\SYSVOL"/>	<input type="button" value="..."/>

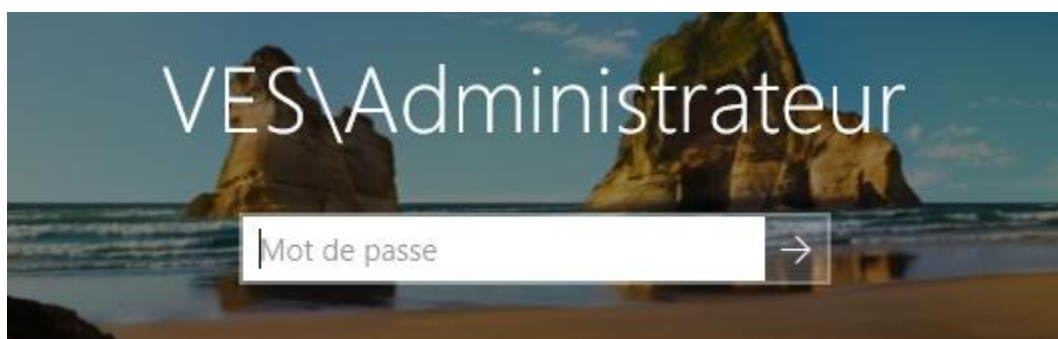
Valider l'emplacement de la base de données AD DS, des journaux d'historiques et pour SYSVOL.
Dans notre cas :

- Base de données : B:\Base
- Fichiers journaux : L:\Logs
- SYSVOL : S:\SYSVOL

Faire “suivant”

Une dernière vérification est effectuée, des notifications sont affichées mais cliquez sur Installer pour démarrer le processus.

L'ADDS est configuré.

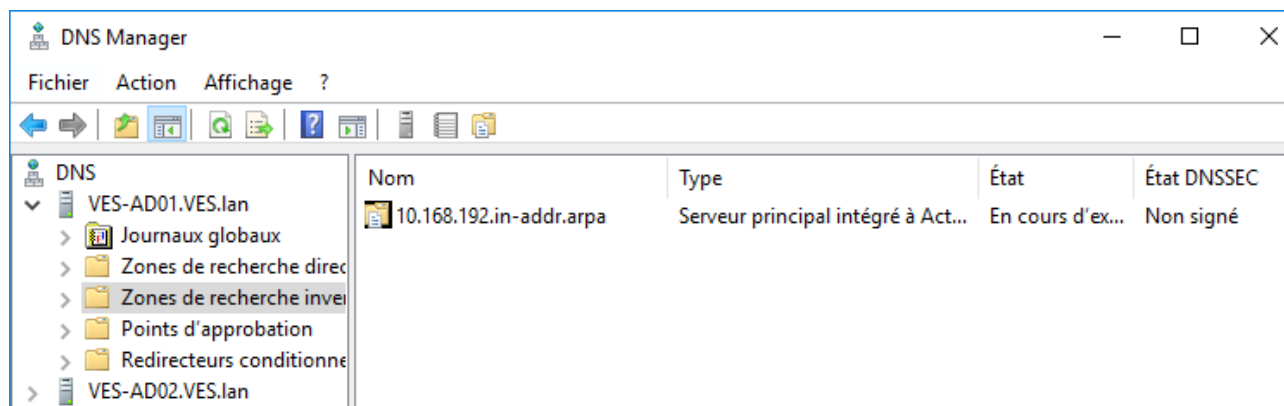


La même procédure est appliquée pour la réplique du serveur VES-AD02.

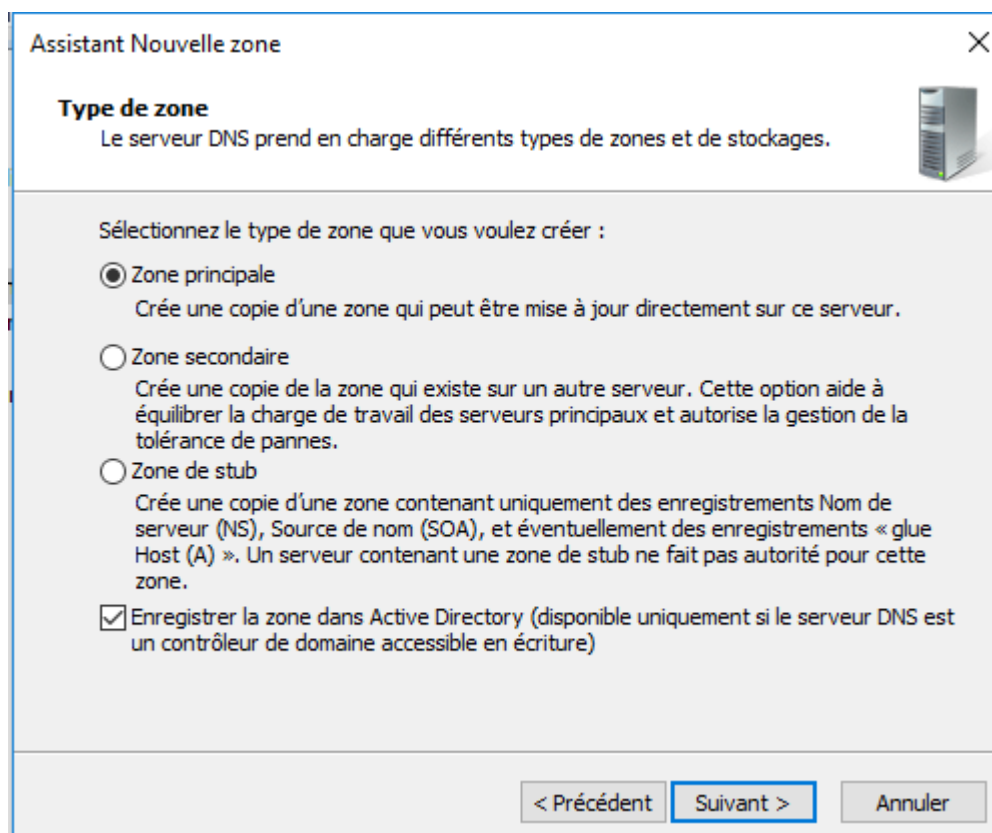
C. Fonctionnalité serveur : Le DNS

Ouvrir le gestionnaire DNS.

Allez maintenant sur “Zones de recherche inversés” faites clic droit et nouvelle zone



Sélectionner “Zone principale” et “Suivant”



A partir de cette fenêtre sélectionner “Zone de recherche inversée IPv4” puis 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

Nom de la zone de recherche inversée indiquer la plage d'adresse IP que nous utilisons.

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 .10

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 :

10.168.192.in-addr.arpa

< Précédent

Suivant >

Annuler

Sélectionner “N’autoriser que les mises à jour dynamiques sécurisées” 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 jour 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

Faire “Terminer”

Assistant Nouvelle zone

Fin de l’Assistant Nouvelle zone

L’Assistant Nouvelle zone s’est terminé correctement. Vous avez spécifié les paramètres suivants :

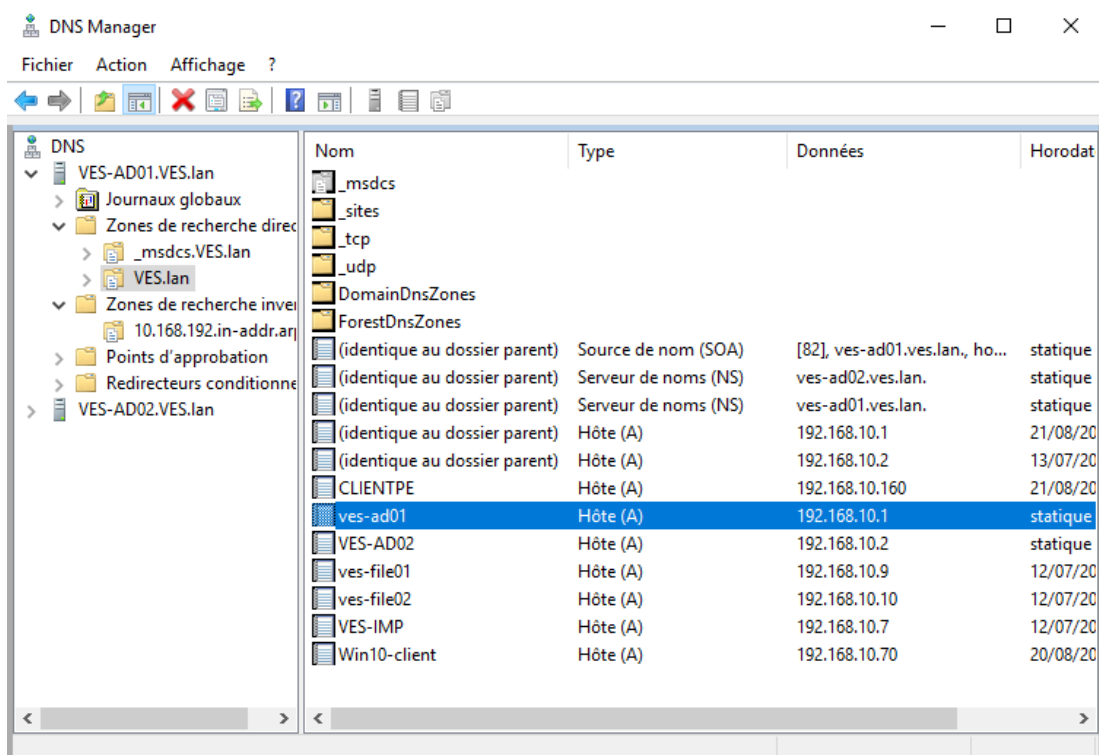
Nom :	10.168.192.in-addr.arpa
Type :	Serveur principal intégré à Active Directory
Type de recherche :	Inversée

Remarque : ajoutez des enregistrements à la zone, ou vérifiez que les enregistrements sont mis à jour de façon dynamique. Vous pourrez ensuite vérifier la résolution des noms avec nslookup.

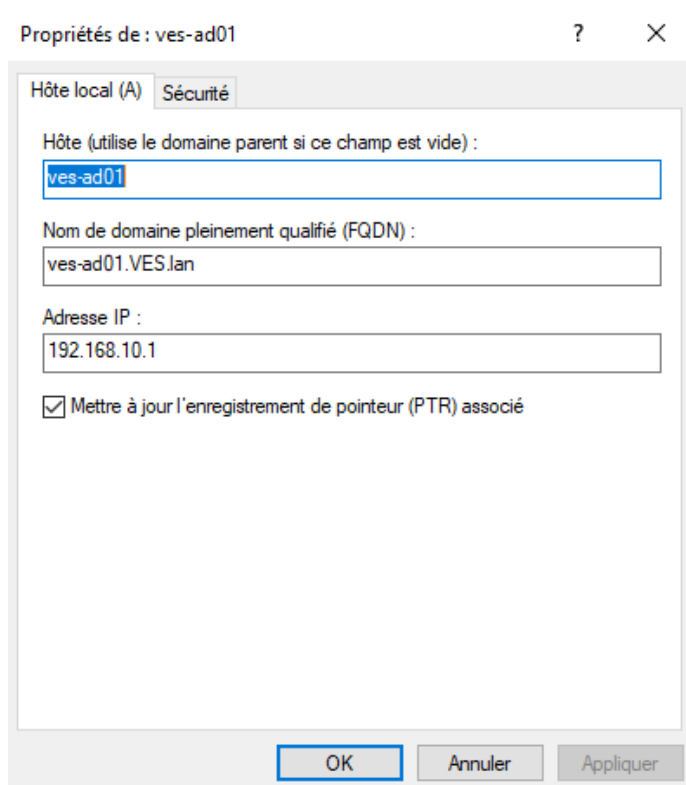
Pour fermer cet Assistant et créer une nouvelle zone, cliquez sur Terminer.

< Précédent **Terminer** Annuler

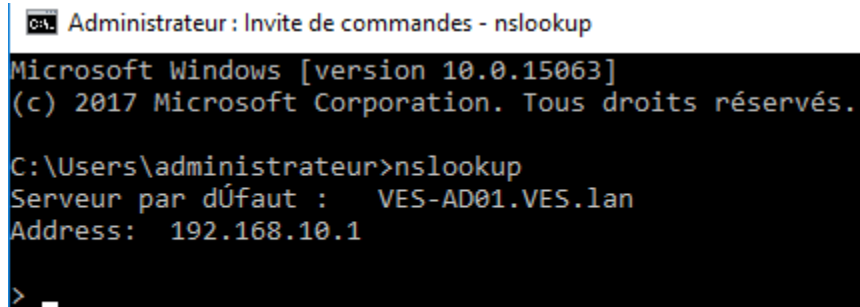
Ensuite aller dans Zones de recherche direct > VES.lan > VES-AD01 faites cliquer droit propriétés



Cocher “Mettre à jour l’enregistrement de pointeur (PTR) associée” et “Ok”



Pour vérifier la bonne configuration du DNS faites un Nslookup dans une invite de commande sur votre serveur AD.



```
Administrateur : Invite de commandes - nslookup
Microsoft Windows [version 10.0.15063]
(c) 2017 Microsoft Corporation. Tous droits réservés.

C:\Users\administrateur>nslookup
Serveur par défaut : VES-AD01.VES.lan
Address: 192.168.10.1

> _
```

Le DNS est répliqué sur le second active directory.

Nos adresses préférés DNS sont donc : 192.168.10.1 et 192.168.10.2.

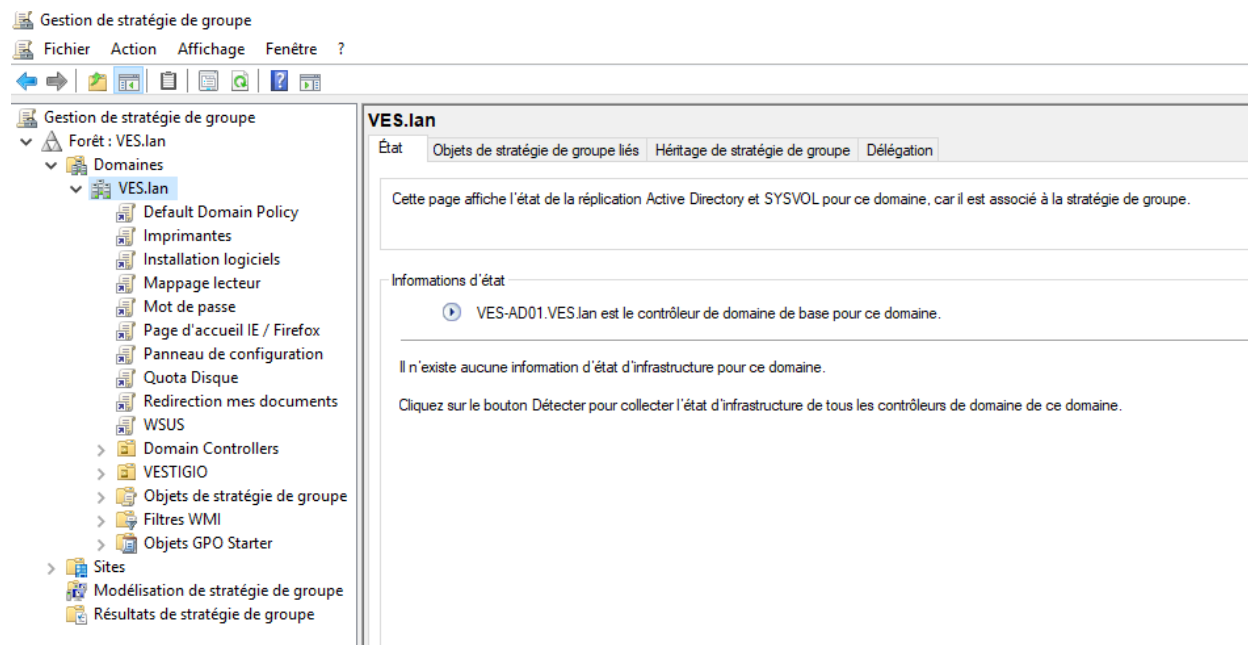
D. Les GPO

4. Définition et rôles

Une Stratégie de Sécurité (Group Policy Object) est définie comme un ensemble des configurations et paramètres permettant la gestion des ordinateurs et des utilisateurs répertoriés dans un annuaire Active Directory. Une GPO est la manière la plus simple de configurer des paramètres appelés "Stratégies de Sécurité" qui seront appliqués sur des utilisateurs et des ordinateurs.

5. Les points forts

- Gestion centralisée et dynamique des utilisateurs et ordinateurs.
- Contrôle efficace des actions des utilisateurs.
- Renforcement de la sécurité dans un domaine Active Directory
- Application d'une politique de sécurité commune à des utilisateurs et ordinateurs.
- Déploiement des applications sur des postes de travail ciblés.



6. Les besoins du cahier des charges :

- Mappage des lecteurs P : Perso T : Commun S : Services
- Page d'accueil personnalisé (GLPI)
- Panneau de configuration retirer pour les utilisateurs
- Redirection de mes documents
- Installation à l'ouverture de session des logiciels essentiels

- Imprimantes
- WSUS
- Complexité des mots de passe : Durée 90 jours, 8 caractères minimum avec une majuscule, et il ne peut pas être le même que le nom de l'utilisateur
- Quota de stockage : Gestion de stockage 5 go par utilisateur autorisé
- Heure de connexion
- Impossibilité d'installer des logiciels pour les utilisateurs excepter les admins

E. Outils RSAT

Les outils RSAT (Remove Server Administration Tools, en français « Outil d'Administration de Serveur Distant ») sont une collection complète d'outils fournie par Microsoft qui la gestion d'un serveur Windows (dans notre cas Windows 2016) depuis une machine cliente (Windows 10)

Nous utiliserons ces outils sur une machine cliente afin d'avoir un accès à distance à nos outils du serveur. Grâce à cette fonction, nous aurons un accès graphique sur nos serveurs Core.

Ci-dessous un exemple de la console d'administration avec les serveurs AD et les serveurs de fichier.

The screenshot shows the Windows Server Management console. The left sidebar contains navigation options: 'Tableau de bord', 'Tous les serveurs' (selected), 'AD DS', 'DNS', and 'Services de fichiers et d...'. The main area is divided into three sections: 'SERVEURS', 'ÉVÉNEMENTS', and 'SERVICES'.

SERVEURS
Tous les serveurs | 4 au total

Nom du serveur	Adresse IPv4	Facilité de gestion	Dernière mise à jour	Activation de Windows
DC1EVO	192.168.10.1	Opération en cours	12/07/2018 13:38:12	Non activé
DC2EVO	192.168.10.2	Opération en cours	12/07/2018 13:38:51	Non activé
SF1EVO	192.168.10.21	En ligne - Compteurs de performances non démarré	21/08/2018 11:40:31	Non activé
SF2EVO	192.168.10.22	En ligne - Compteurs de performances non démarré	21/08/2018 11:40:31	Non activé

ÉVÉNEMENTS
Tous les événements | 0 au total

Nom du serveur	ID	Gravité	Source	Journal	Date et heure
----------------	----	---------	--------	---------	---------------

SERVICES
Tous les services | 130 au total

Nom du serveur	Nom complet	Nom du service	Stat.
----------------	-------------	----------------	-------

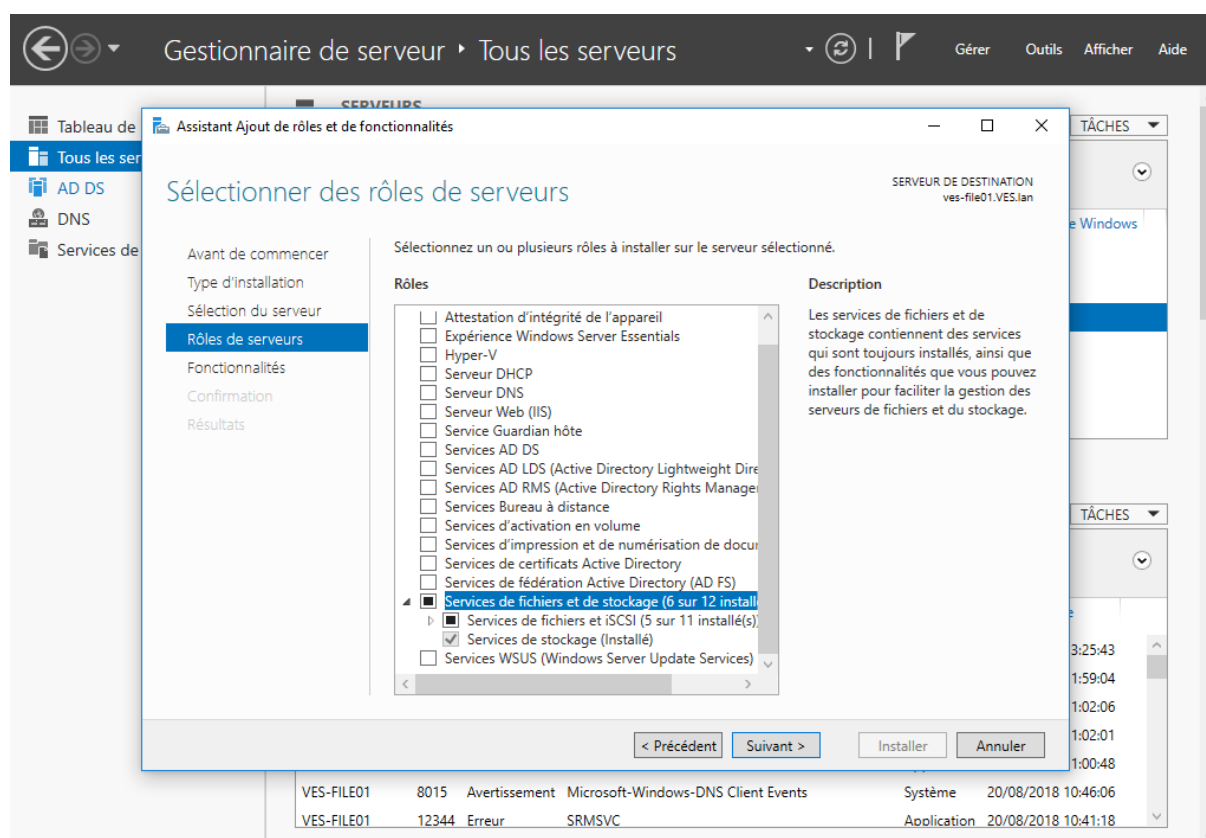
F. DFS

Notre Projet comprend, comme demandé dans le cahier des charges, un serveur et un client DFS, tout deux sous Windows Server 2016 Core.

Notre Serveur et notre Client DFS permettent la distribution d'un espace de stockage commun disponible même en cas de défaillance d'un serveur sur les deux.

L'installation des deux serveurs est classique à l'exception du choix de la version qui sera Windows Server 2016 Edition Standard.

Nous installerons par la suite le rôle DFS sur les deux serveurs.



Après installation, nous pouvons accéder au Gestionnaire DFS afin de configurer notre espace de noms et notre réplication.

Gestionnaire de serveur - Tous les serveurs

SERVEURS
Tous les serveurs | 4 au total

Nom du serveur	Adresse IPv4	Facilité de gestion	Dernière mise à jour	Activation de Windows
VES-AD01	192.168.10.1	En ligne - Compteurs de performances non démarré	20/08/2018 14:46:46	Non activé
VES-AD02	-	Ordinateur cible inaccessible	20/08/2018 14:27:25	-
VES-FILE01	192.168.10.9	En ligne - Compteurs de performances non démarré	20/08/2018 14:46:46	Non activé
VES-FILE02	192.168.10.10	En ligne - Compteurs de performances non démarré	20/08/2018 14:46:46	Non activé

ÉVÉNEMENTS
Tous les événements | 37 au total

Nom du serveur	ID	Gravité	Source	Journal	Date et heure
VES-FILE01	50	Avertissement	Microsoft-Windows-Time-Service	Système	20/08/2018 13:25:43
VES-FILE01	50	Avertissement	Microsoft-Windows-Time-Service	Système	20/08/2018 11:59:04
VES-FILE01	8015	Avertissement	Microsoft-Windows-DNS Client Events	Système	20/08/2018 11:02:06
VES-FILE01	8198	Erreur	Microsoft-Windows-Security-SPP	Application	20/08/2018 11:02:01
VES-FILE01	12344	Erreur	SRMSVC	Application	20/08/2018 11:00:48
VES-FILE01	8015	Avertissement	Microsoft-Windows-DNS Client Events	Système	20/08/2018 10:46:06
VES-FILE01	12344	Erreur	SRMSVC	Application	20/08/2018 10:41:18

« Serveurs

SERVEURS
Tous les serveurs | 3 au total

Nom du serveur	Adresse IPv4	Facilité de gestion	Dernière mise à jour	Activation de Windows
VES-AD01	192.168.10.1	En ligne - Compteurs de performances non démarré	20/08/2018 14:46:46	Non activé
VES-FILE01	192.168.10.9	En ligne - Compteurs de performances non démarré	20/08/2018 14:46:46	Non activé
VES-FILE02	192.168.10.10	En ligne - Compteurs de performances non démarré	20/08/2018 14:46:46	Non activé

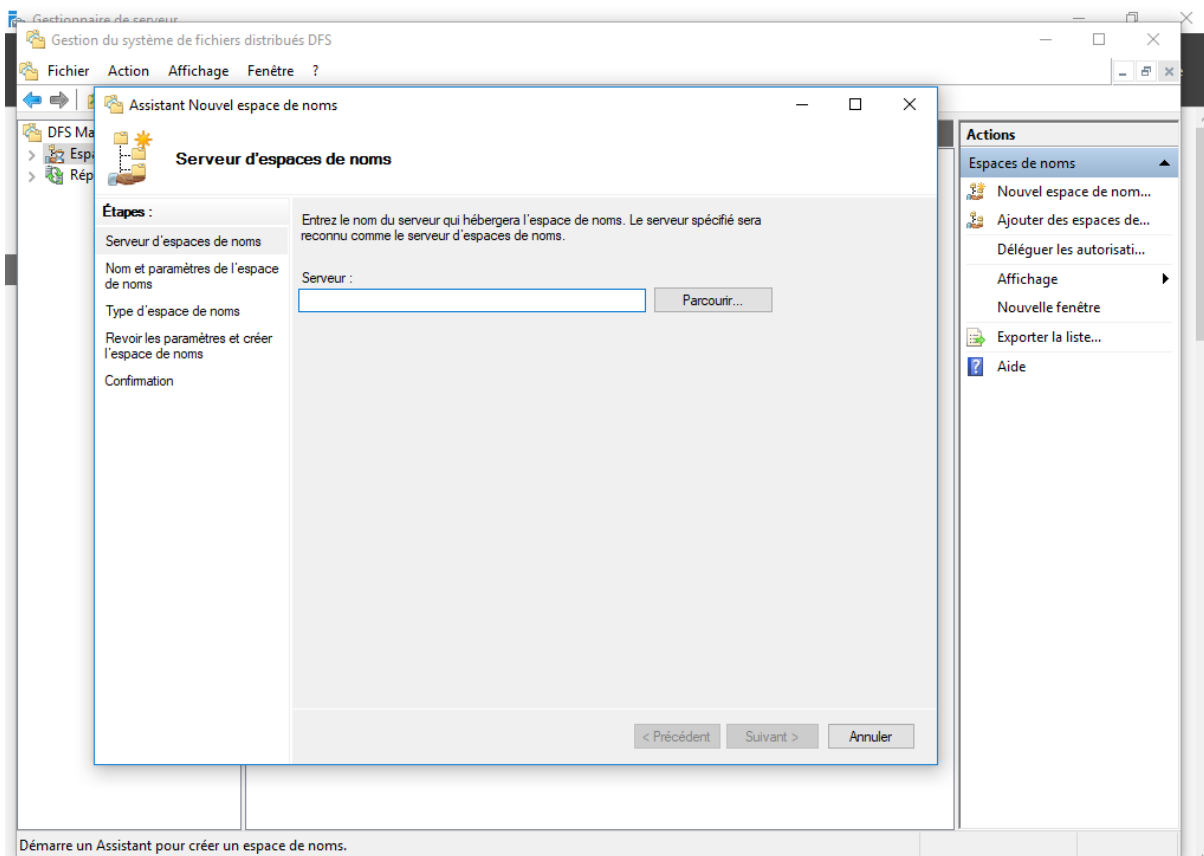
ÉVÉNEMENTS
Tous les événements

Nom du serveur	ID	Gravité	Source	Journal	Date et heure
VES-FILE01	5002	Erreur	DFSR Réplication DFS	Système	20/08/2018 11:39:15
VES-FILE01	12344	Erreur	SRMSVC Application	Application	20/08/2018 11:00:48
VES-FILE01	12344	Erreur	SRMSVC Application	Application	20/08/2018 10:41:18
VES-FILE01	8197	Erreur	SRMSVC Application	Application	20/08/2018 10:32:35

Planification de la déduplication
Gestionnaire de ressources du serveur de fichiers
Paramètres des Outils de gestion de ressources pour serveur de fichiers
Gestion du système de fichiers distribués DFS
Ajouter des rôles et fonctionnalités
Redémarrer le serveur
Gestion de l'ordinateur
Connexion Bureau à distance
Windows PowerShell
Configurer l'association de cartes réseau
Gérer en tant que...
Démarrer les compteurs de performances
Supprimer le serveur
Actualiser
Copier

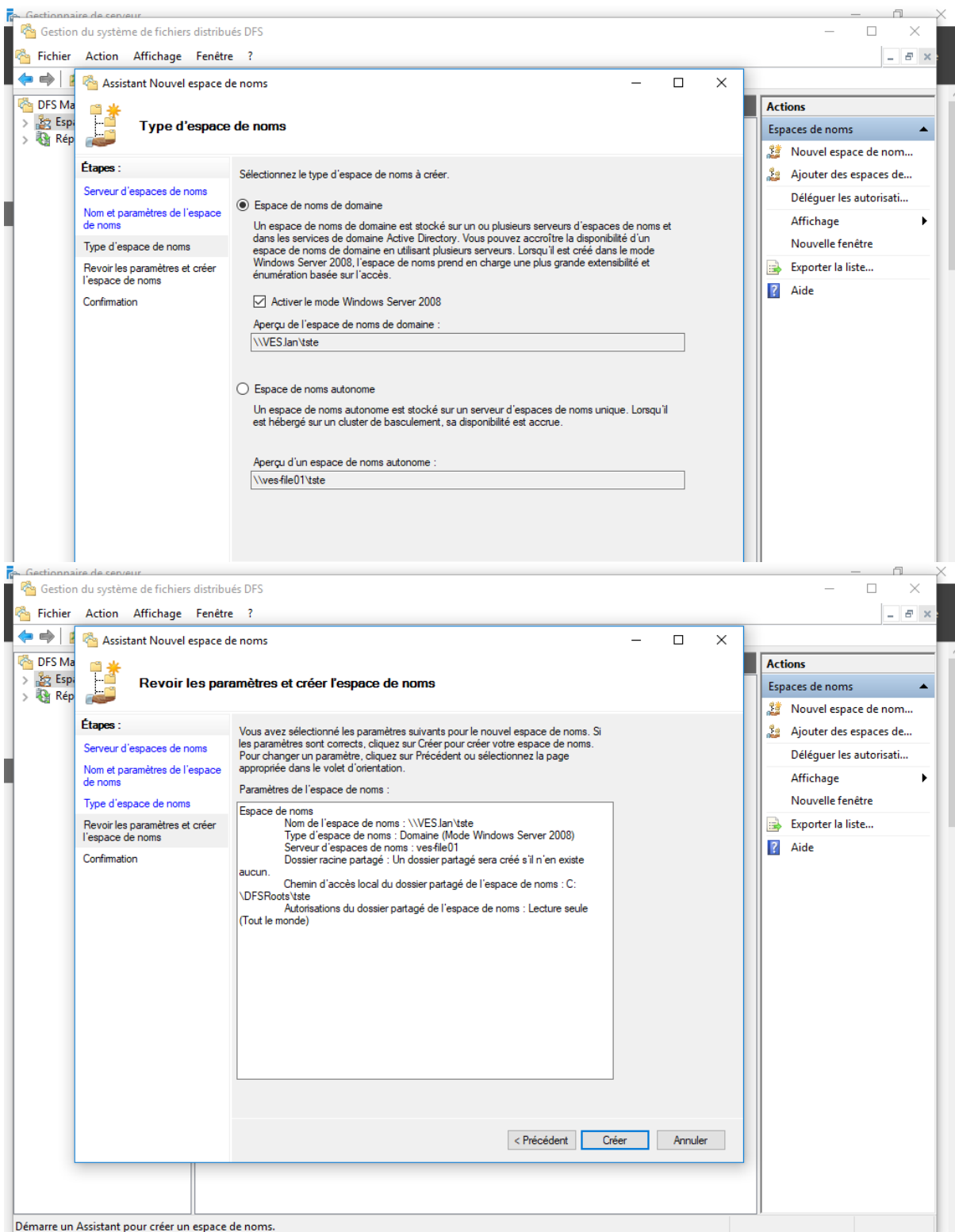
Ensuite, nous créons un nouvel espace de noms.

Nous choisissons notre serveur DFS principale, ici VES-FILE01.



Nous renommons ensuite notre Espace de noms en « DFS ».

Nous sélectionnons la coche « Espace de noms de domaine » et non « Espace de noms autonome » car dans notre cas, nous avons besoin de stocker cette espace de noms sur plusieurs serveurs, en l'occurrence VES-FILE01 et VES-FILE02.

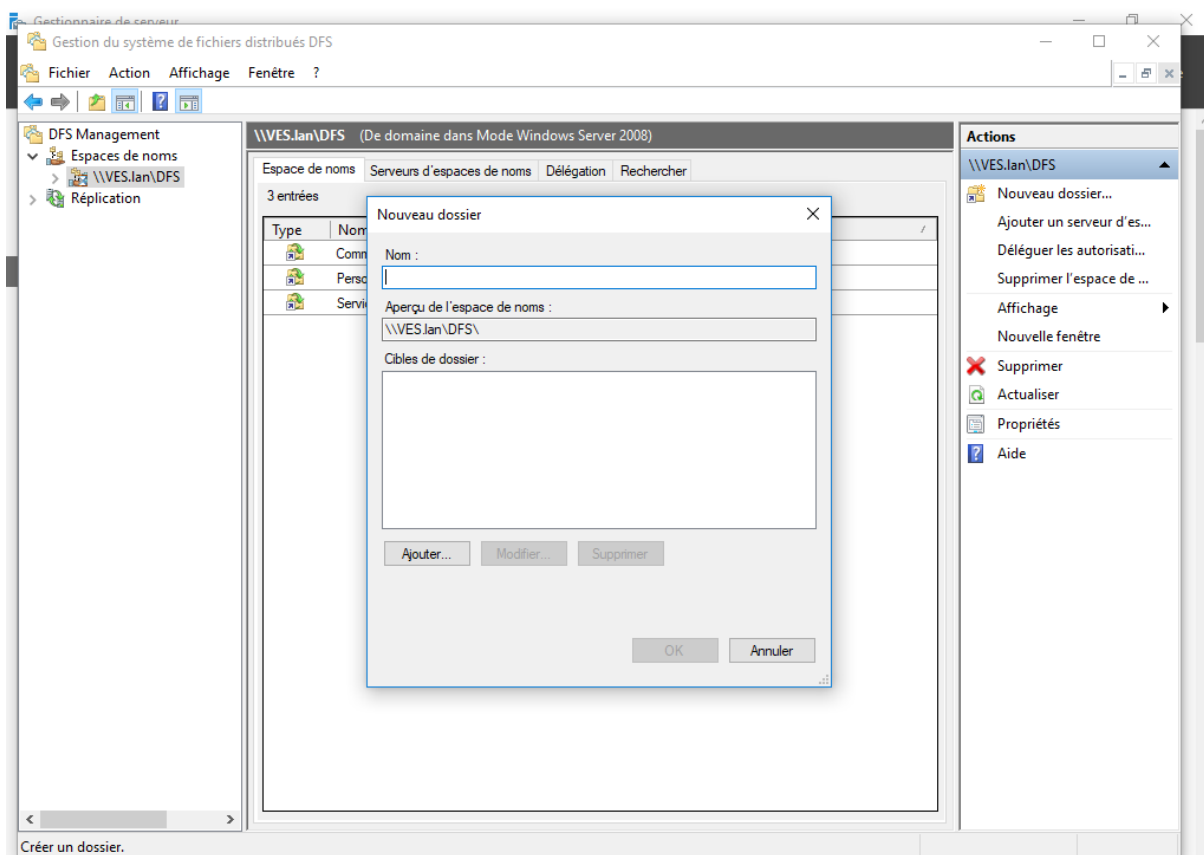


Nous pouvons finalement cliquer sur créer.

Notre espace de nom DFS est créé, nous pouvons désormais configurer les nouveau partages.

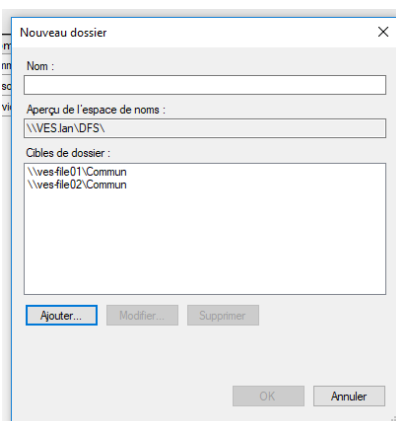
Nous allons créer 3 Partages nécessaires pour notre projet :

- Commun
- Services
- Perso

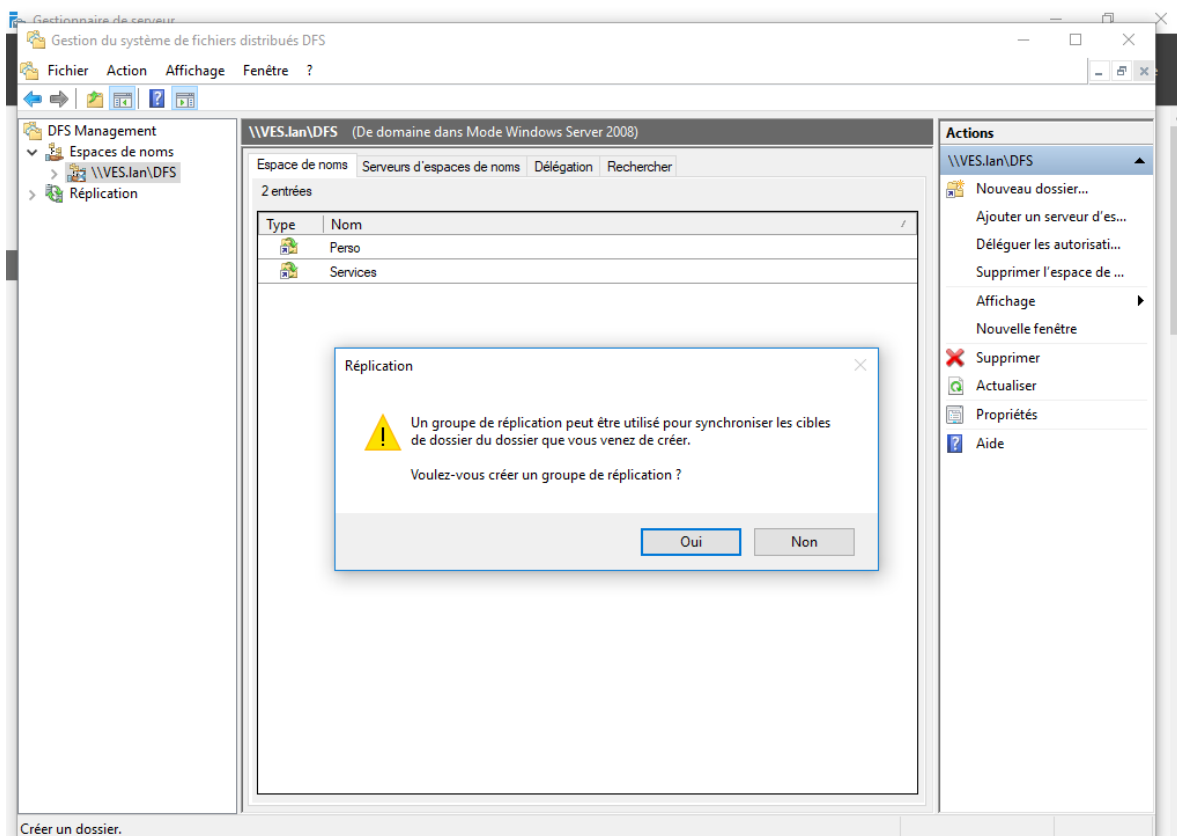


Une fois nos 3 partages créés, nous allons pouvoir créer nos 3 dossiers dans notre espace de noms.

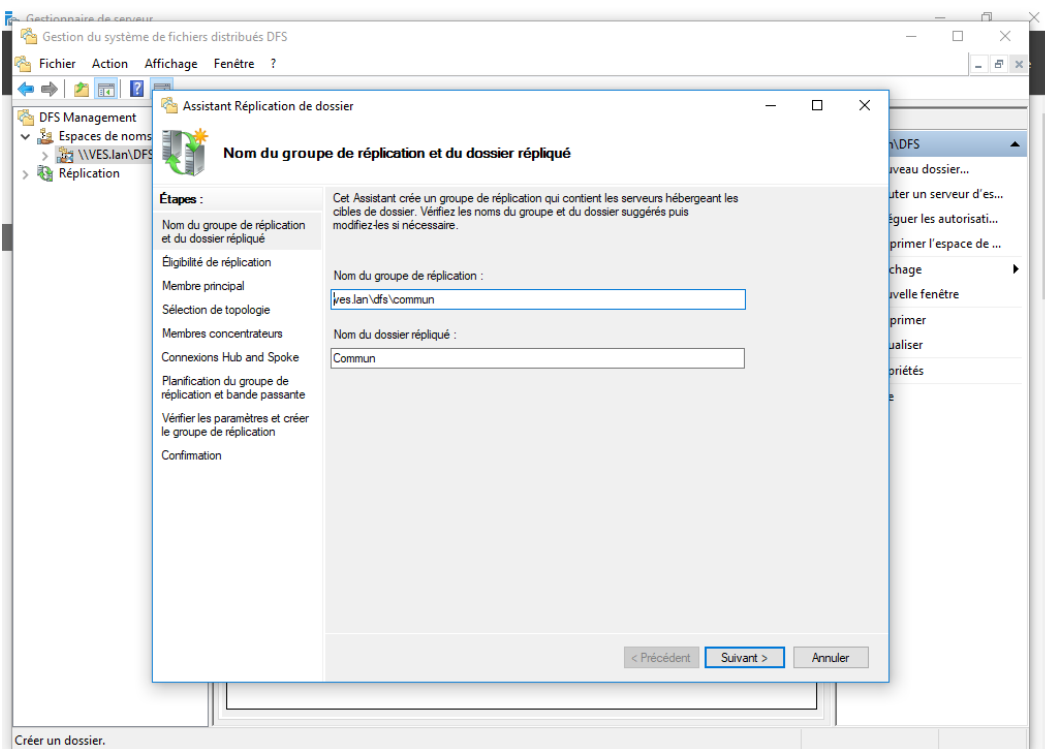
Nous renseignons donc le nom de notre partage ainsi que la cible sur VES-FILE01 ainsi que sur VES-FILE02 afin de permettre la réplication.



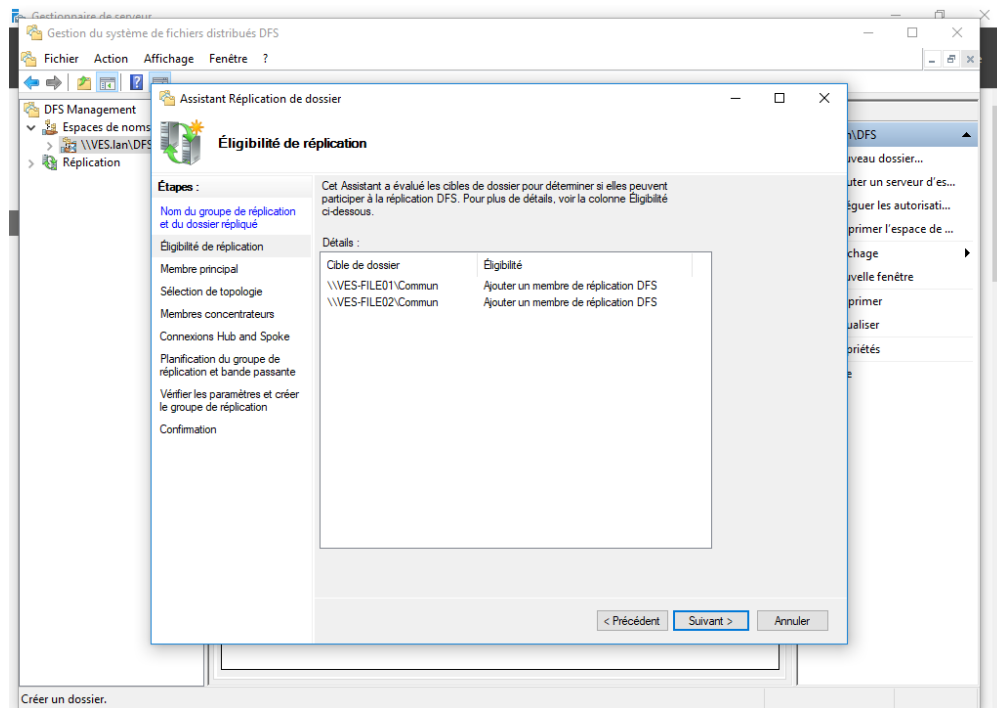
Par la suite un Pop UP apparait et nous demande si l'on veut créer un groupe de réplication, on répond oui.



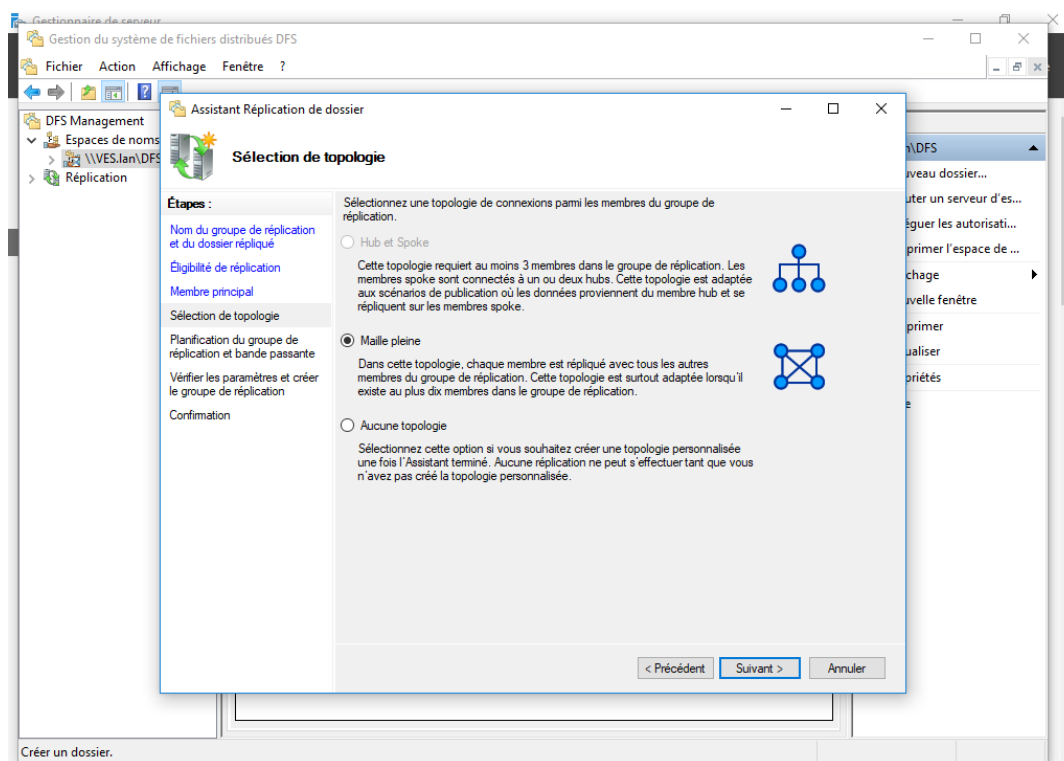
Nous laissons le nom par défaut.



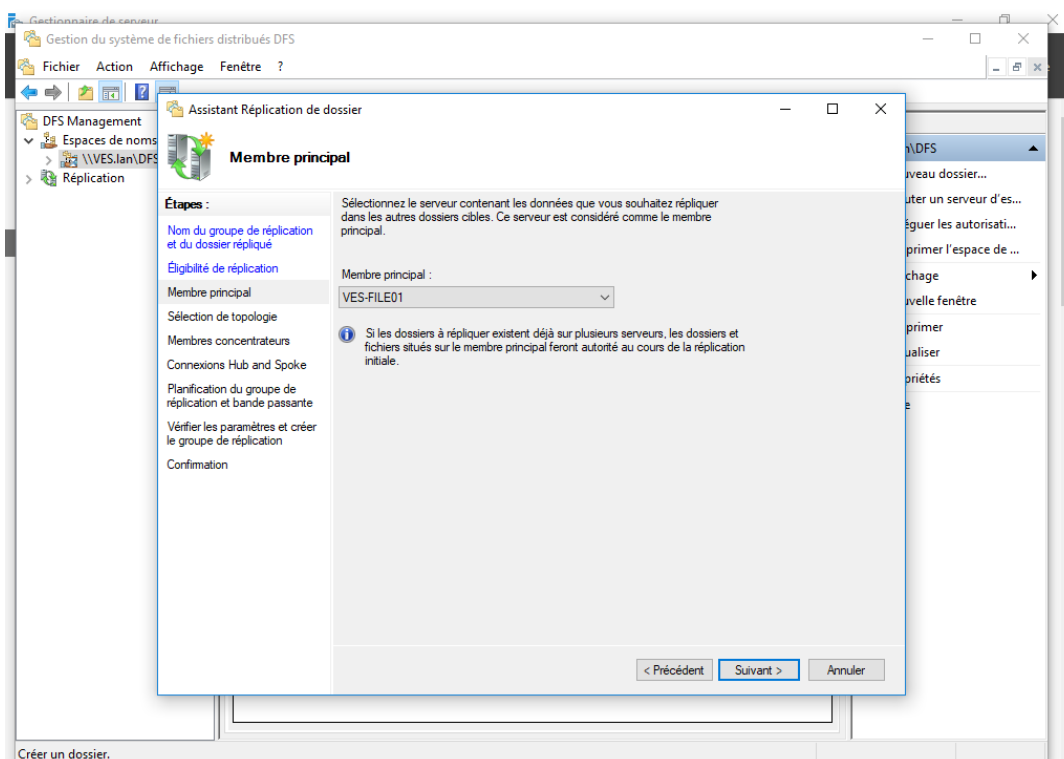
Nous vérifions les cibles : elles sont correctes.

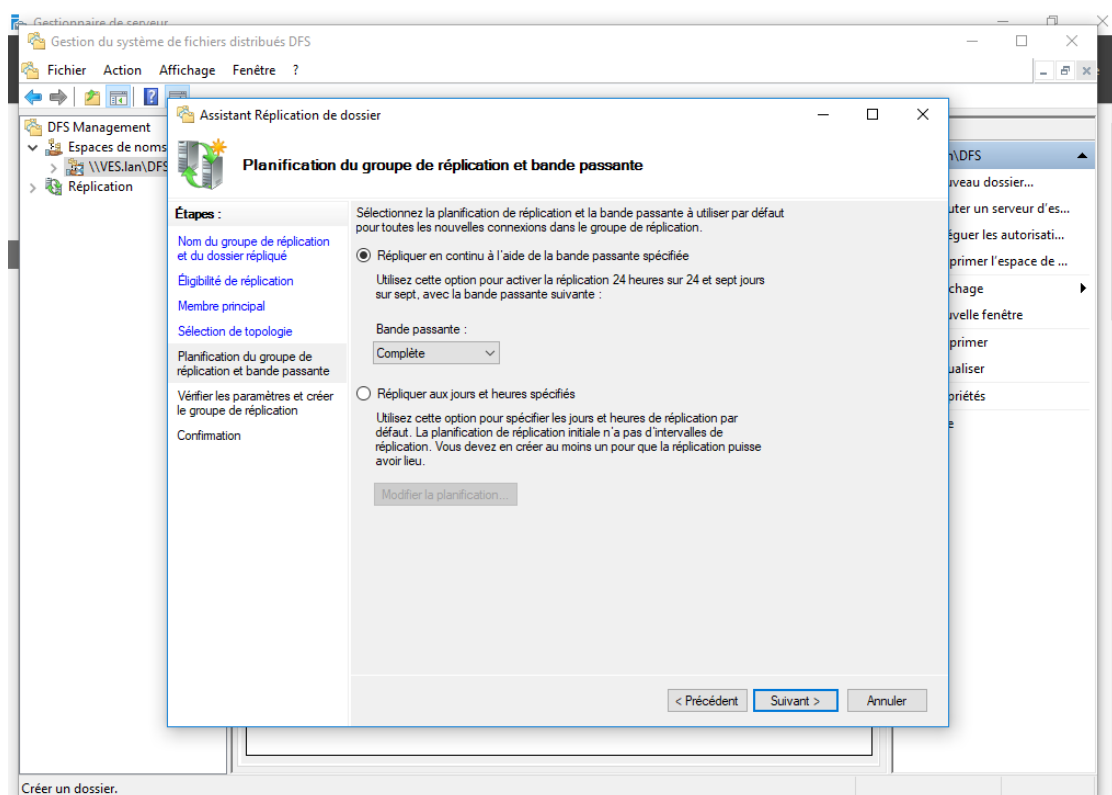


Nous sélectionnons en tant que membre principal notre serveur VES-FILE01.



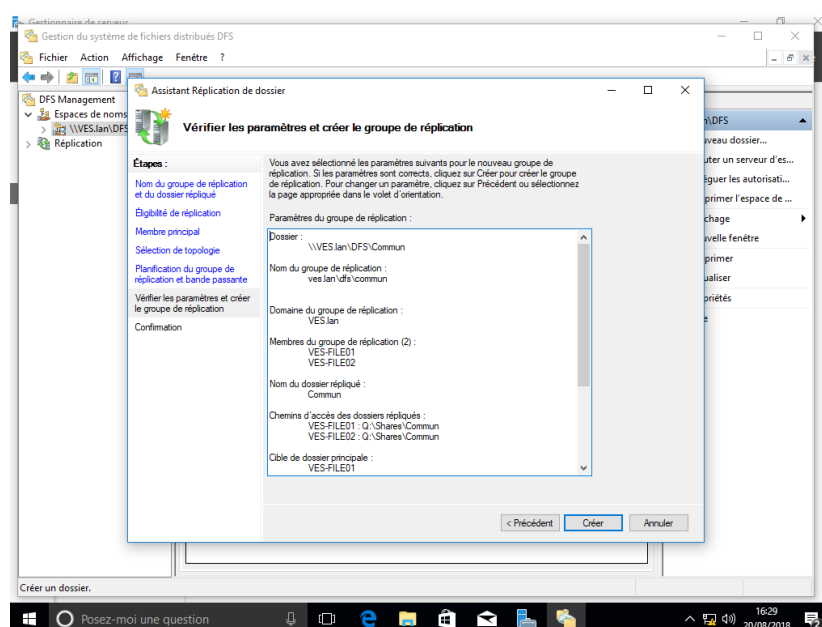
Nous sélectionnons comme topologie de réplication « Maille pleine » qui permet une réplication entre tous les serveurs DFS.





Nous choisissons une réplication en continue, adapté dans notre cas étant donné la nécessité de la haute disponibilité des différents partages.

Notre réplication est désormais fonctionnelle pour le dossier commun, il faut désormais réitérer ces étapes pour les 2 autres partages.

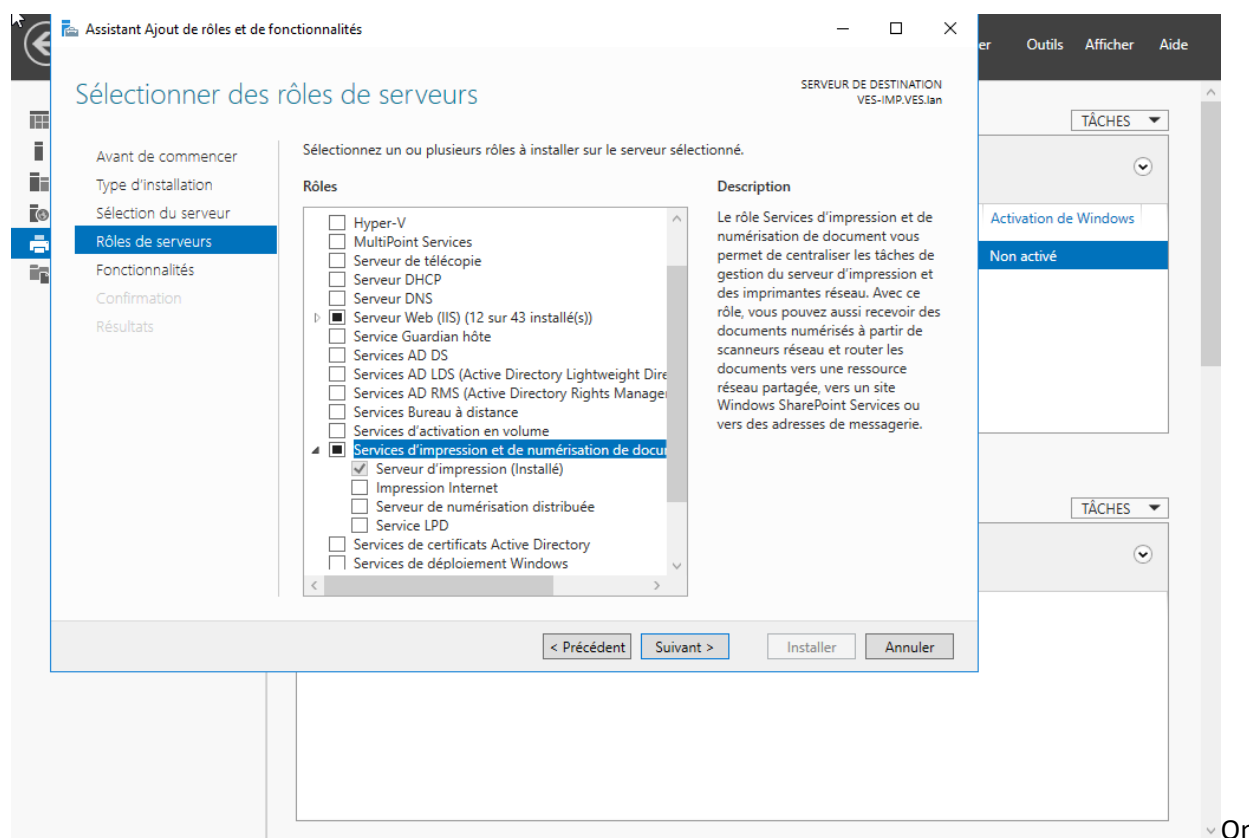


Nos serveurs DFS ainsi que nos partages sont désormais opérationnels.

G. Serveur d'Impression

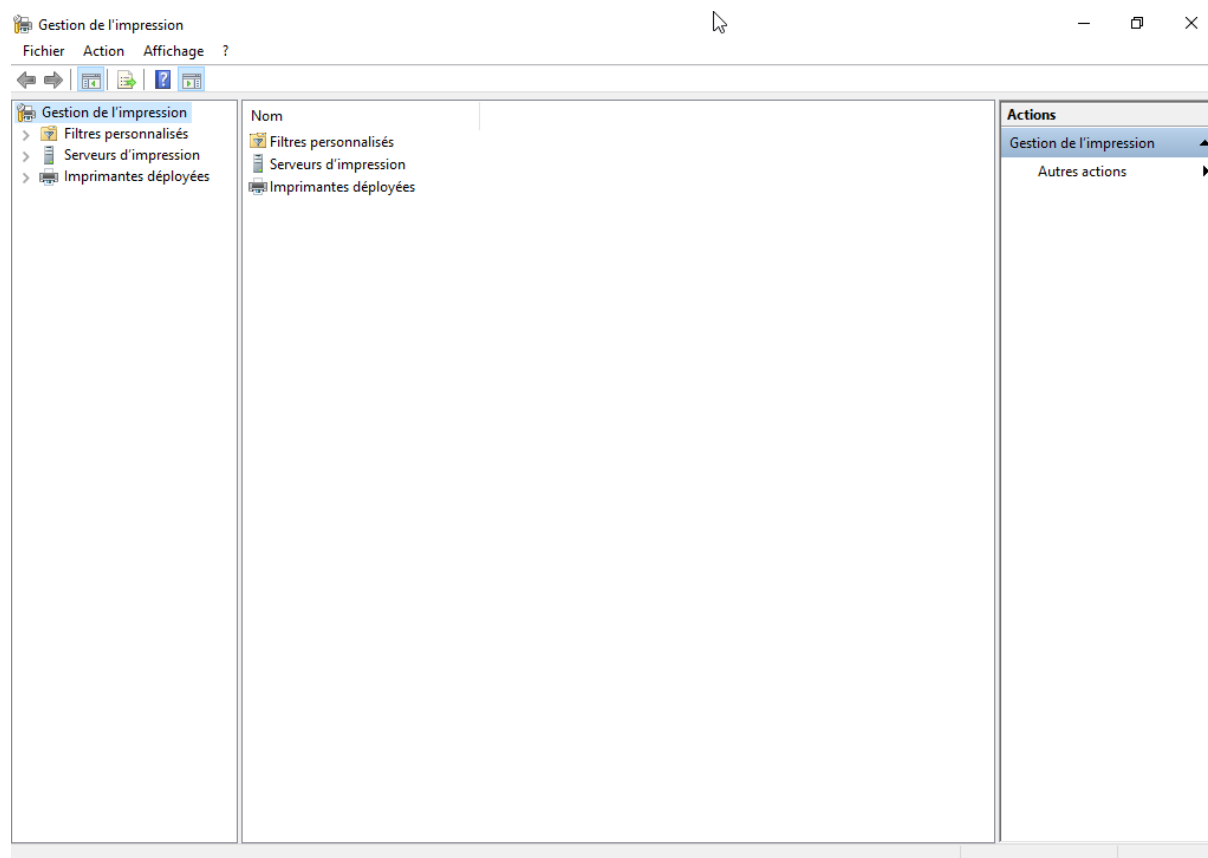
Le serveur d'impression, que nous mettons en place par notre propre initiative permet une centralisation de la gestion de l'impression afin de gagner du temps que ce soit lors du déploiement ou en cas de problème.

Notre serveur d'impression sera installé sur Windows Server 2016 (Expérience utilisateur) avec les rôles WSUS et RSAT, plus précisément sur le serveur VES-IMP qui a pour adresse IP 192.168.10.7.



On va donc commencer par installer le rôle permettant à notre serveur de devenir un serveur d'impression.

Une fois le rôle installé, nous allons accéder au gestionnaire d'impression afin de configurer nos imprimantes.



Via ce gestionnaire d'impression, on va ajouter, conformément au cahier des charges :

- Une imprimante par services nommé PrintService
- Une imprimante commune nommée PrintEveryone

Le plan d'adressage a donc été fait comme ci-dessous.

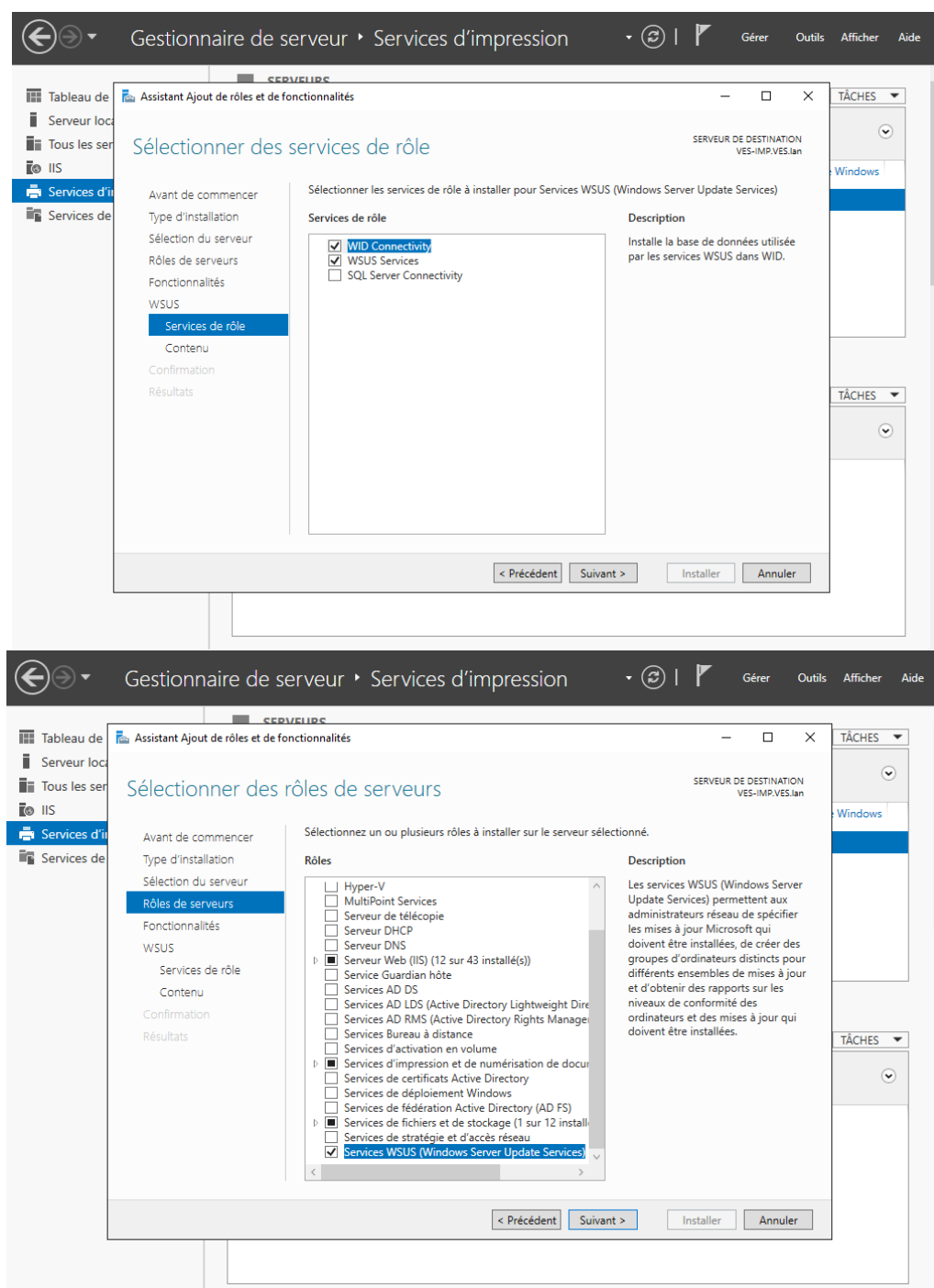
Services	Imprimantes	IP	
Matériel	PrintMatériel	192.168.10.231	Produit 1
Commercial	PrintCommercial	192.168.10.232	
Administratif	PrintAdministratif	192.168.10.233	
Direction	PrintDirection	192.168.10.234	Produit 2
Vêtements	PrintVêtements	192.168.10.235	
IT	PrintIT	192.168.10.236	
	PrintEveryone	192.168.10.237	

Une fois les imprimantes rajoutées, il faudra finaliser leur installation par la mise en place de GPO.

H. Serveur WSUS

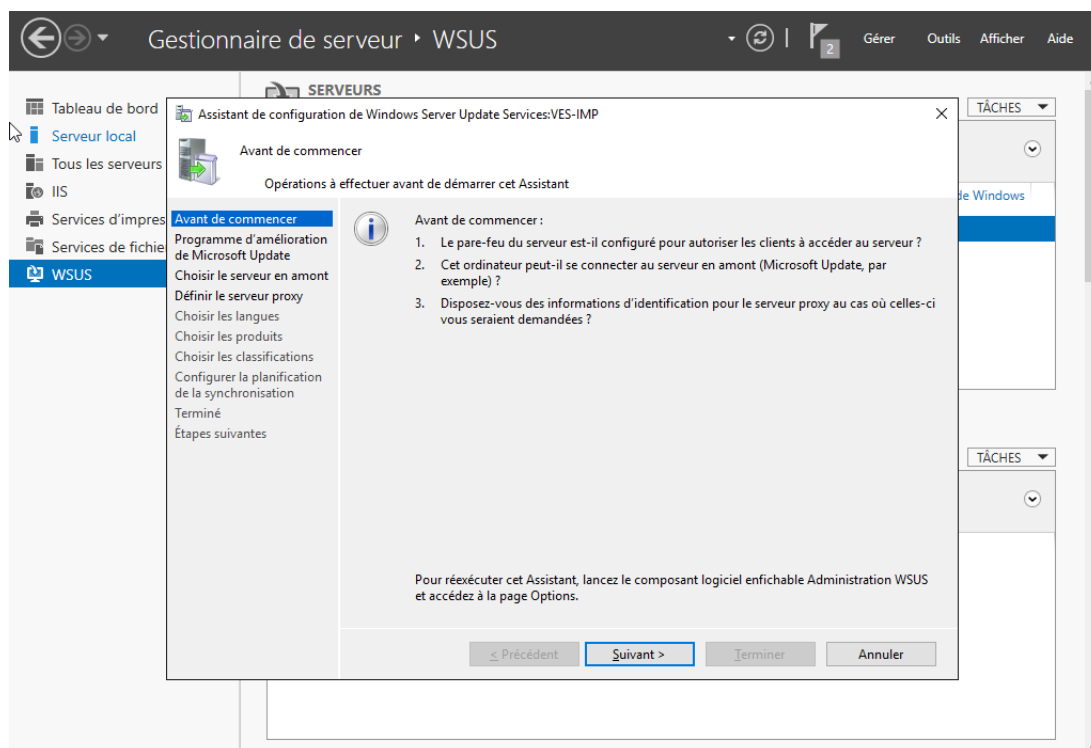
Afin de permettre la centralisation de la gestion des mises à jours ainsi qu'une économie de bande passante, nous avons pris l'initiative de mettre en place un serveur WSUS.

Il sera installé sur le serveur Windows Server 2016 sur lequel sont installés le serveur d'impression ainsi que les RSAT qui a pour nom VES-IMP avec comme adresse IP 192.168.10.7.

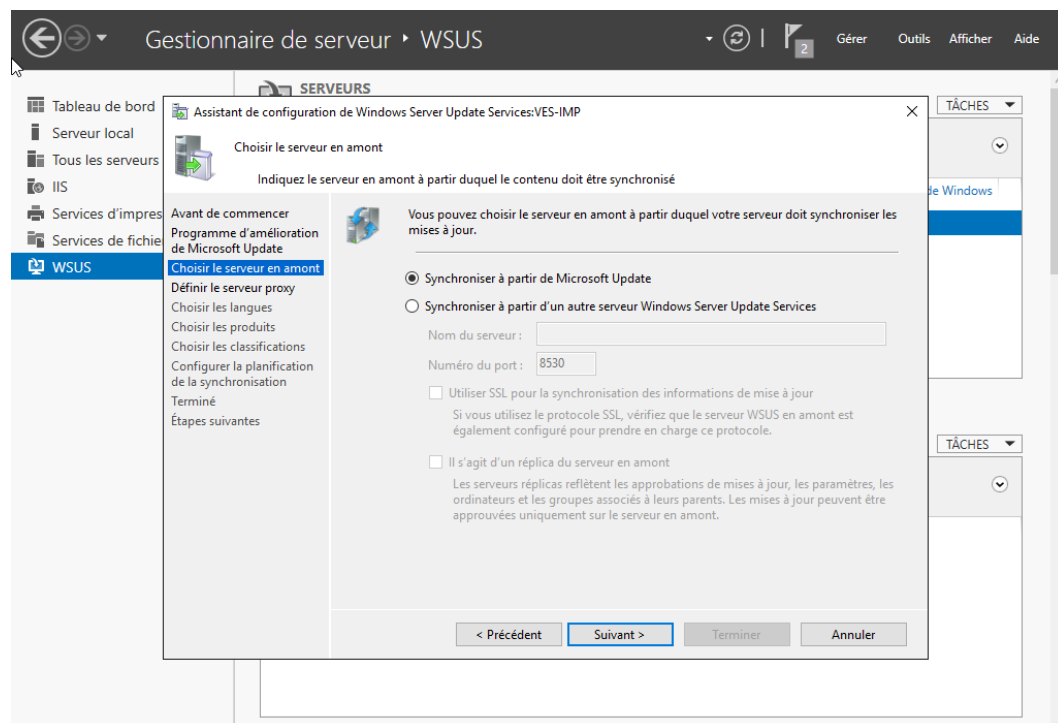


Nous installons d'abord le rôle WSUS via le gestionnaire des Rôles.

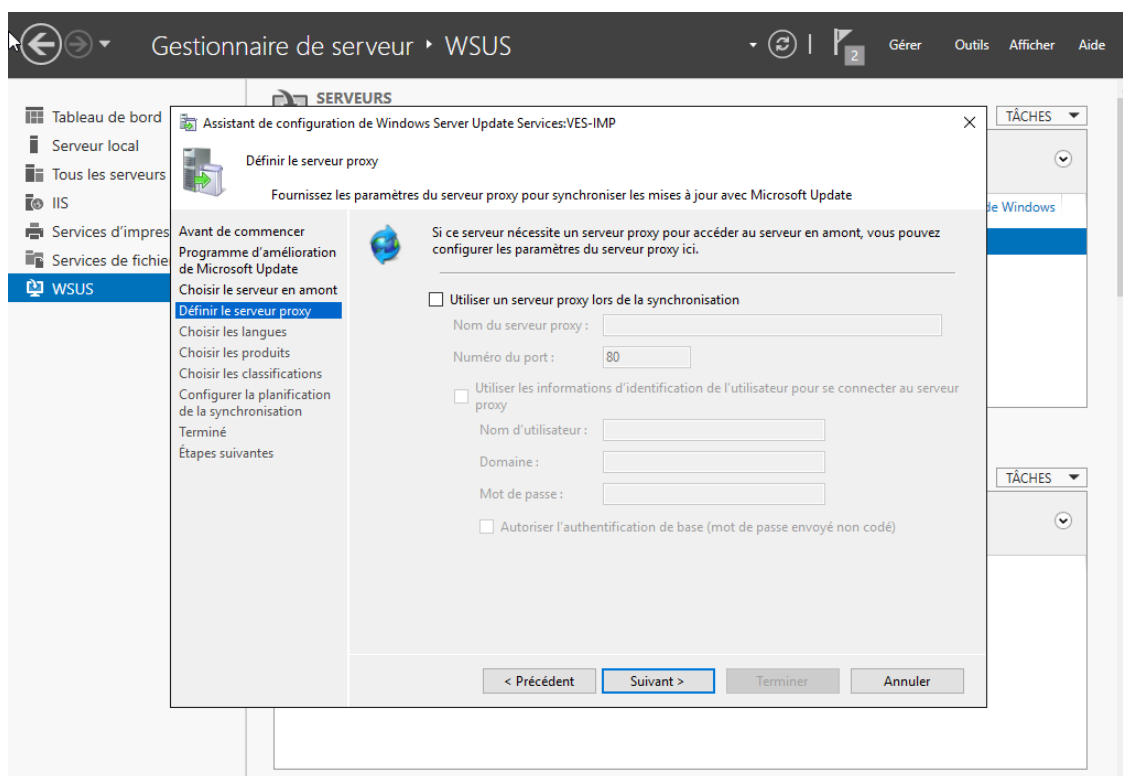
Une fois le rôle installé, une seconde fenêtre s'ouvre.



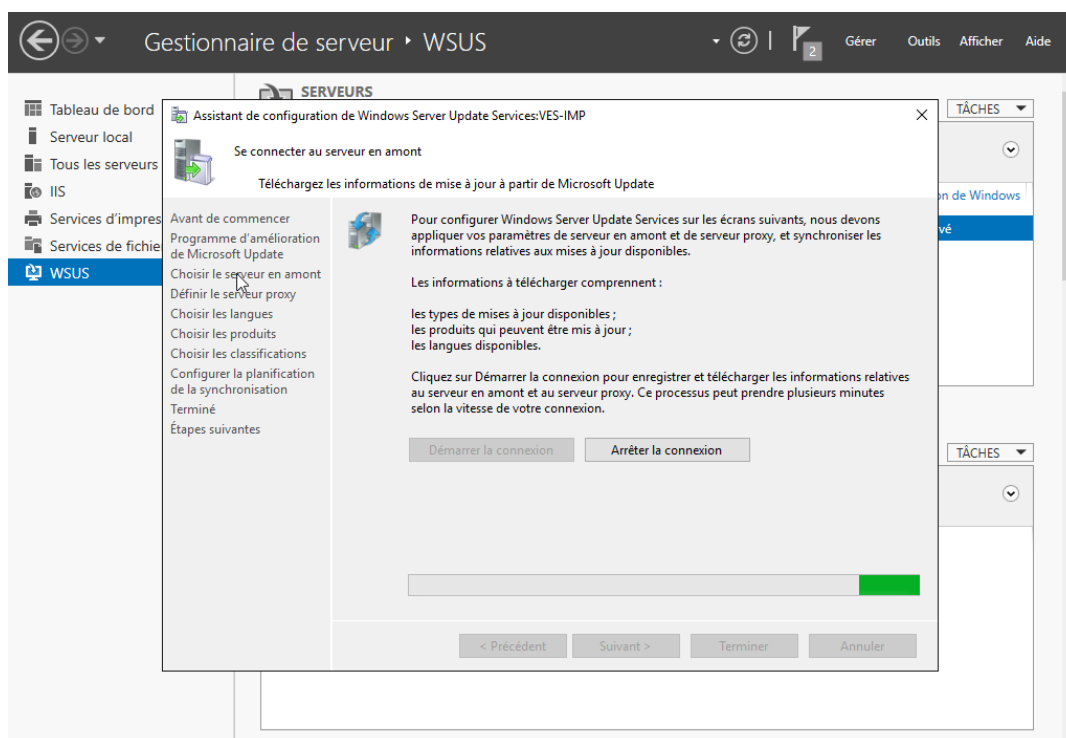
Nous allons donc cliquer sur suivant.



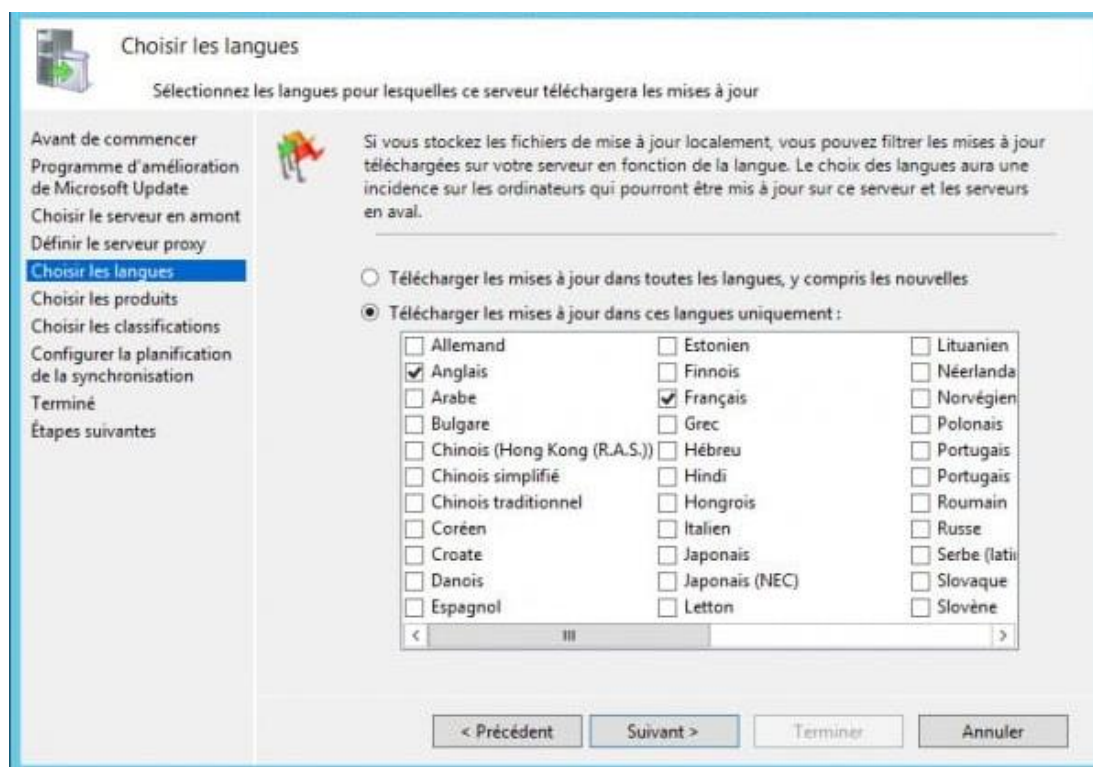
On sélectionne « Synchroniser à partir de Microsoft Update » car dans notre cas, nous ne possédons qu'un seul serveur WSUS et nous n'en aurons besoin que d'un seul.



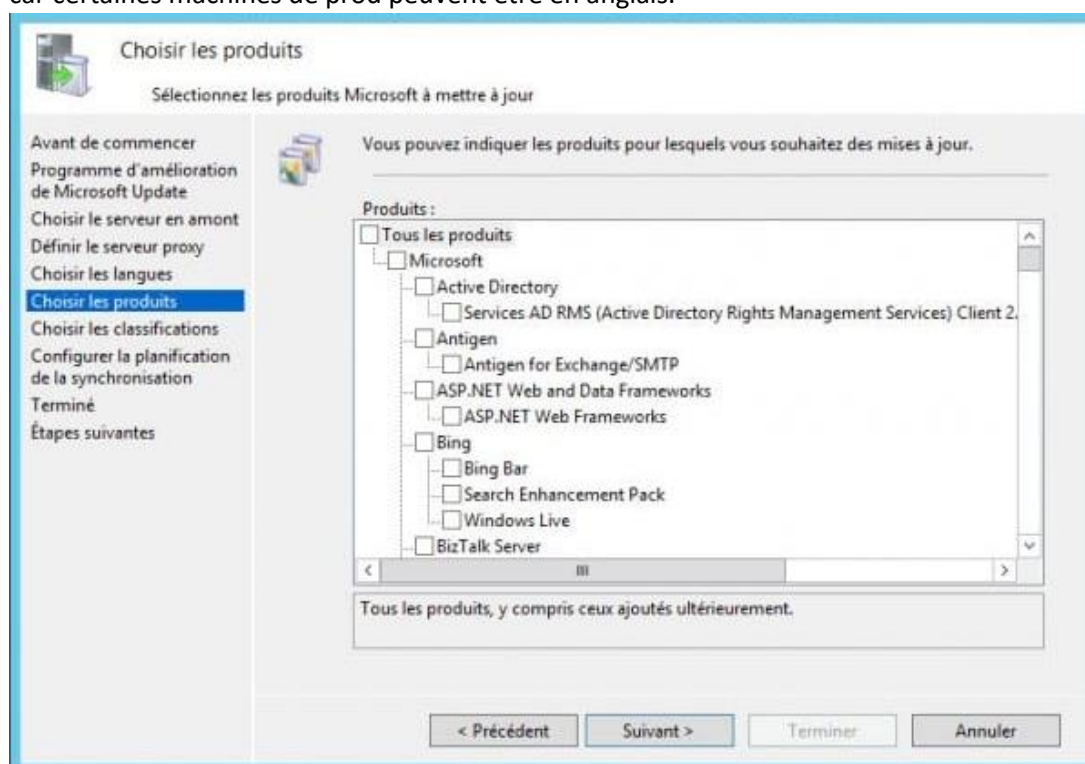
Nous n'avons pas de serveur proxy, nous ignorons donc cette étape.



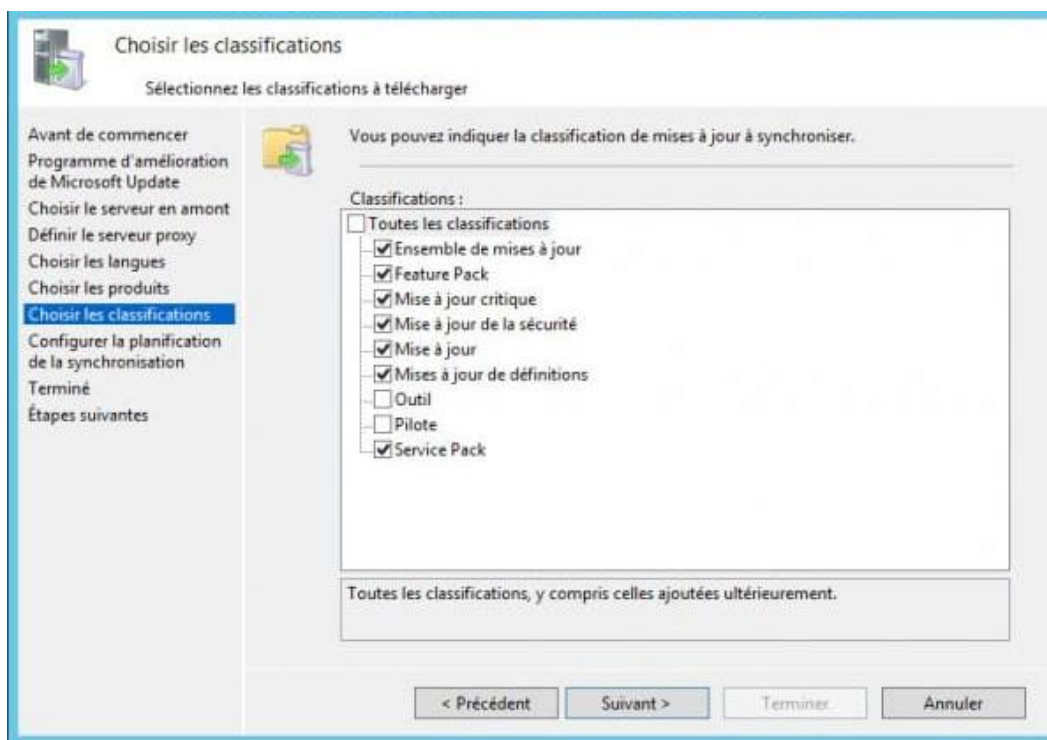
On va ensuite devoir télécharger les informations relatives au serveur de Microsoft Update.



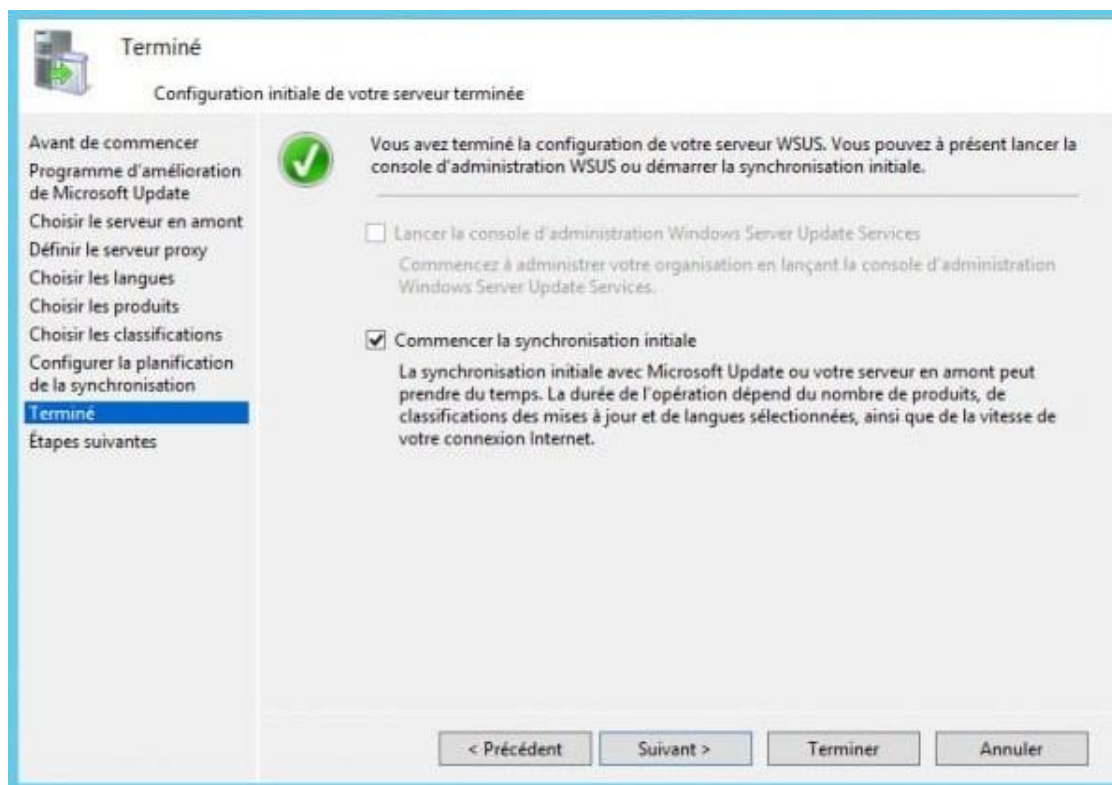
Une fois cela fait, nous allons choisir les langues d'installation pour les mises à jour, ici français et anglais car certaines machines de prod peuvent être en anglais.



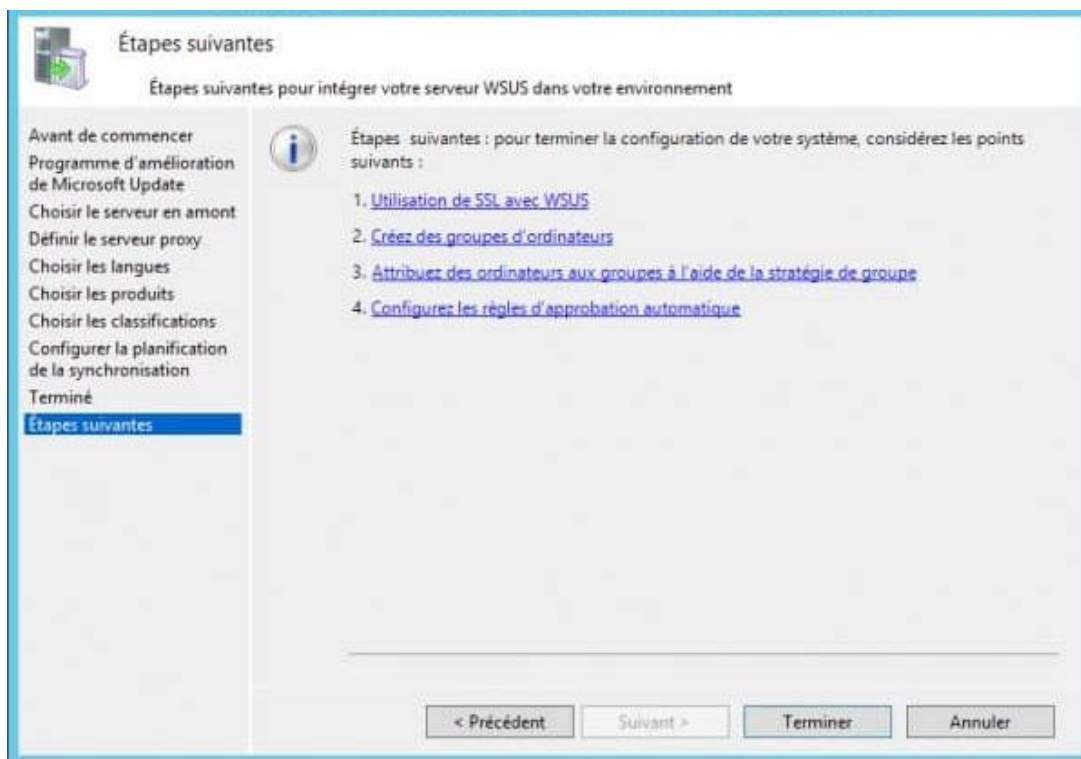
On installera aucun produit.



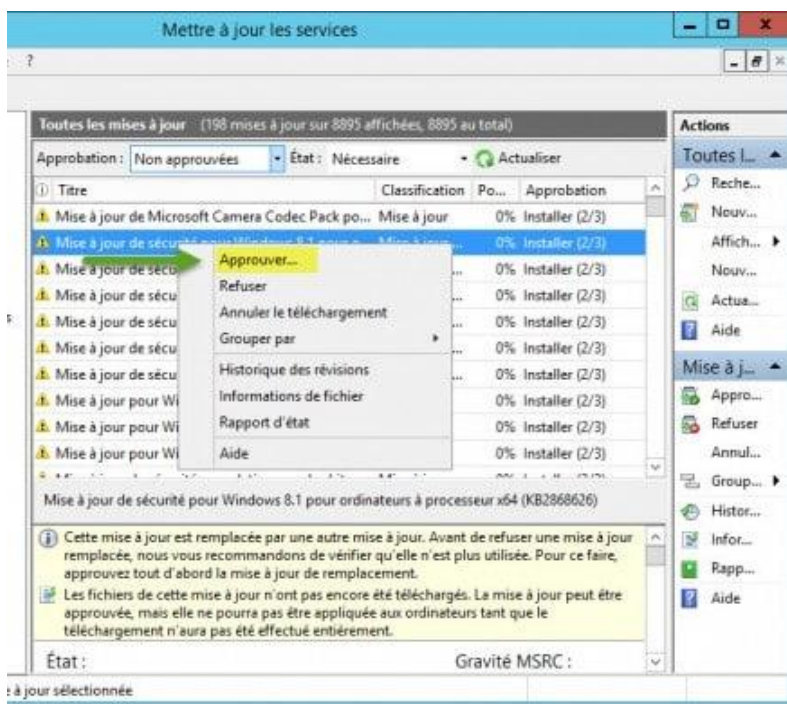
On choisira toutes les classifications sauf les Outils et les Pilotes que l'on installera à la main.

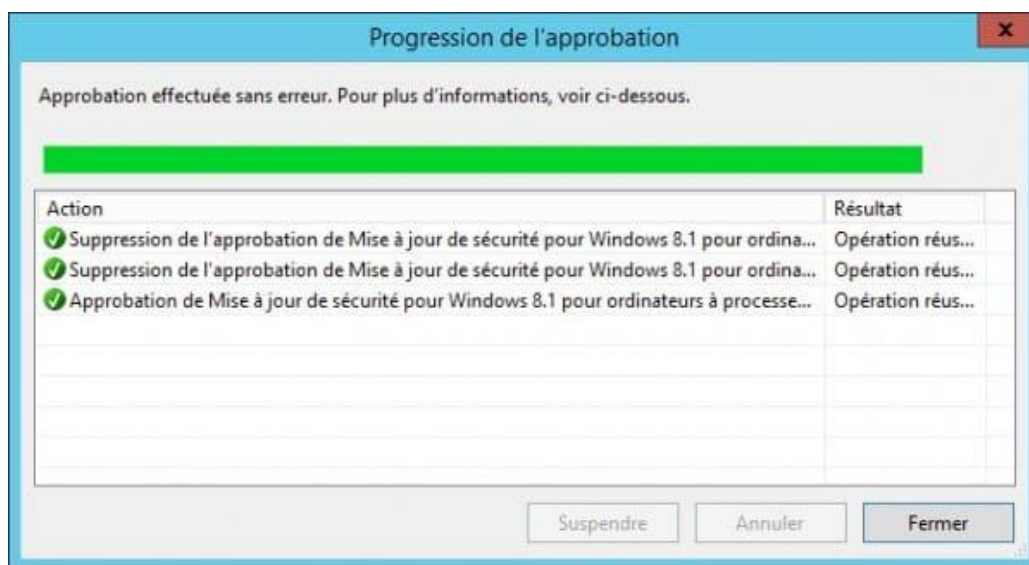


Dans notre cas, vu que personne n'est en production, j'ai effectué la synchronisation initiale.



On peut cliquer sur terminer. L'installation se termine par la mise en place de GPO permettant aux mises à jour de s'installer. Nous allons désormais devoir approuver les mises à jour afin qu'elles puissent s'installer.





Une fois l'approbation effectuée, les mises à jour peuvent s'installer sur les différents postes et serveur qui sont sur le domaine.

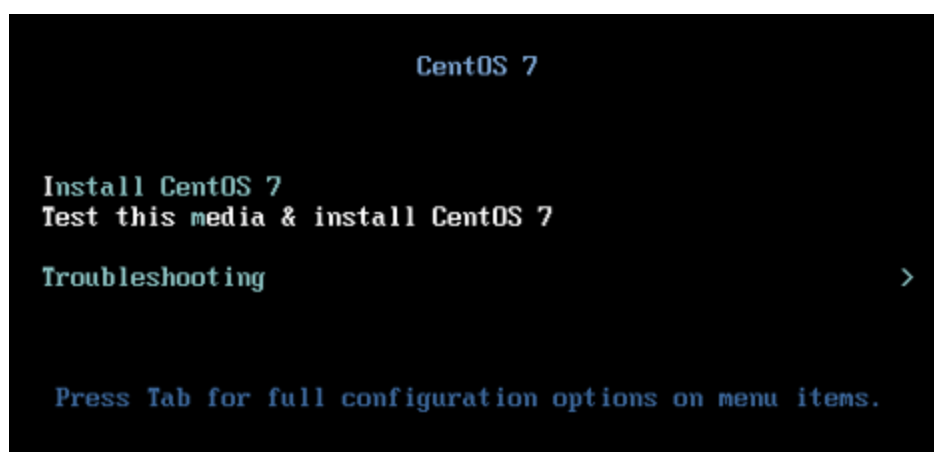
IV. Linux Serveur

Comme convenu avec le cahier des charges, nos serveurs Linux utiliseront le système d'exploitation CentOS 7. Cette distribution de Linux est gratuite et sera en version minimale (pas de partie graphique). Elle répond tout à fait à nos besoins et présente également un gain de performance.

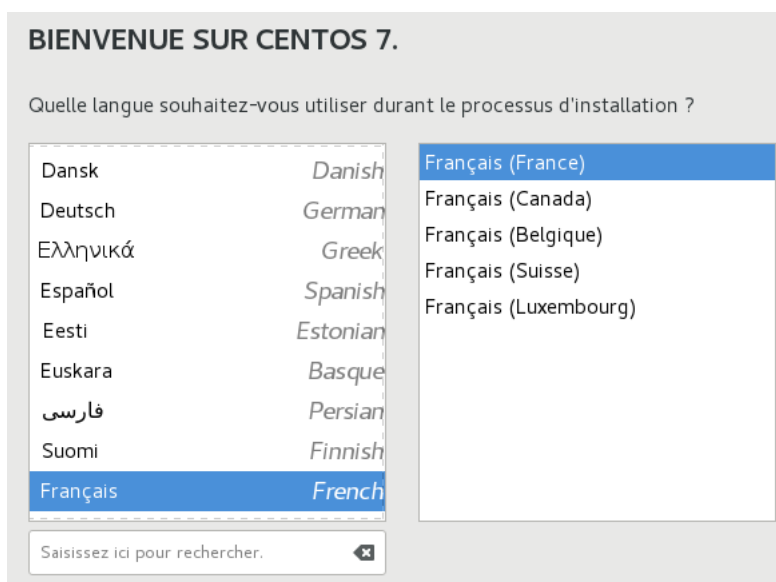
Notre infrastructure Linux assurera les fonctions DHCP, Samba, FTP, DFS, ainsi que notre serveur web. Nous allons tout d'abord procéder à l'installation du système d'exploitation.

A. Installation de CentOS 7

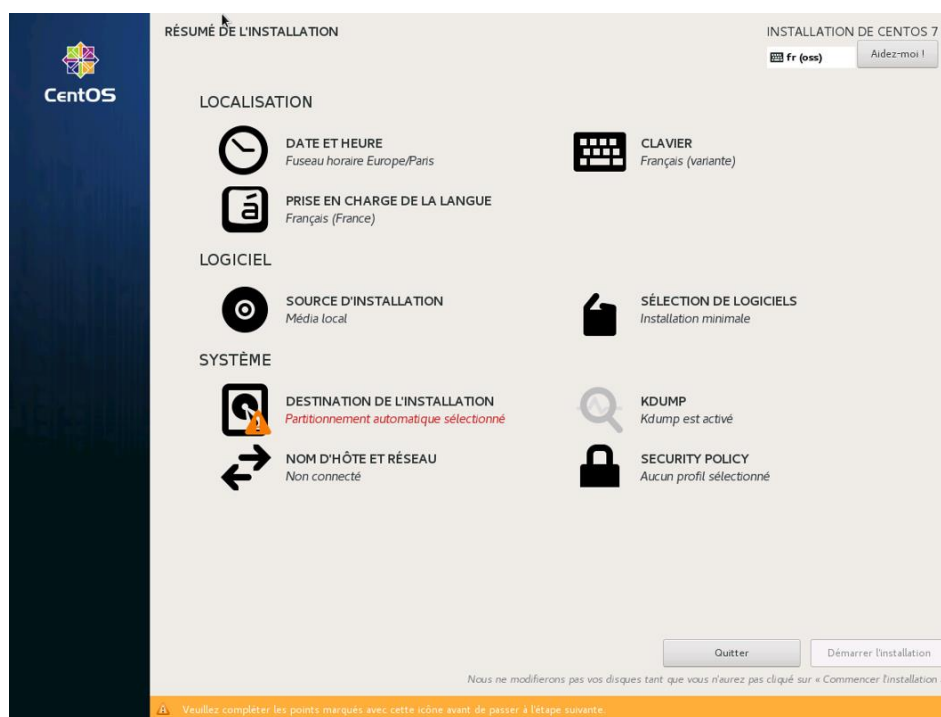
Afin d'optimiser les performances, nous effectuerons l'installation de CentOS en version minimale (core).



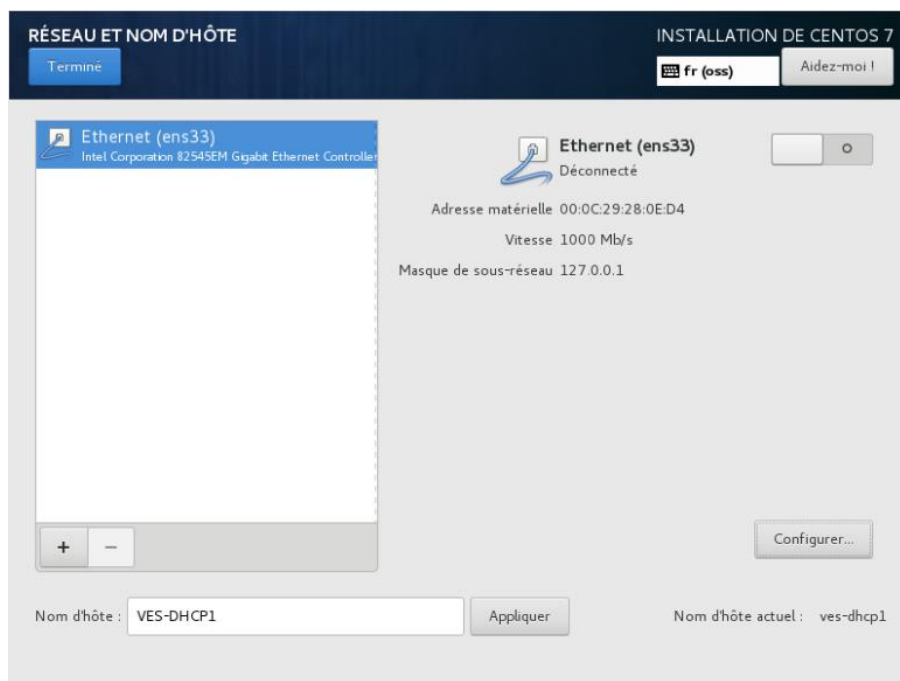
Choisir la langue qui sera utilisée pour l'installation, ici nous choisirons le français.



Un menu s'affichera ensuite :



Nous allons tout d'abord nous diriger vers « Nom d'hôte et réseau ». Dans cette fenêtre, nous allons pouvoir définir le nom d'hôte de la machine en bas à gauche de l'écran. Dans cet exemple nous utiliserons le nom d'hôte du premier DHCP : VES-DHCP01.



Ensuite, nous allons configurer la carte réseau. Dans un premier temps nous allons passer les paramètres IPv6 en « **ignorer** », puis dans l'onglet « **Général** », nous allons cocher la case « **Se connecter automatiquement à ce réseau si disponible** »

Modification de ens33

Nom de la connexion :

Général Ethernet Sécurité 802.1X DCB Proxy Paramètres IPv4 **Paramètres IPv6**

Méthode : Ignorer

Modification de ens33

Nom de la connexion :

Général Ethernet Sécurité 802.1X DCB Proxy Paramètres IPv4 **Paramètres IPv6**

☒ Se connecter automatiquement à ce réseau si disponible

Connection priority for auto-activation: - +

☒ Tous les utilisateurs peuvent se connecter à ce réseau

Cliquez sur « Terminé » pour revenir au menu principal. Nous irons ensuite dans « Destination de l'installation » pour configurer manuellement le partitionnement. Il faut donc cocher la case « Je vais configurer le partitionnement ».

CIBLE DE L'INSTALLATION INSTALLATION DE CENTOS 7

[Terminé](#) fr (oss) [Aidez-moi !](#)

Sélection des périphériques

Sélectionnez le périphérique sur lequel vous souhaitez faire l'installation. Il restera intact jusqu'à ce que vous cliquiez sur le bouton « Commencer l'installation » du menu principal.

Disques locaux standards

20 GiO

VMware, VMware Virtual S
sda / 20 GiO d'espace libre

Les disques décochés ne seront pas modifiés.

Disques spéciaux et réseau

Ajouter un disque...

Les disques décochés ne seront pas modifiés.

Autres options de stockage

Partitionnement

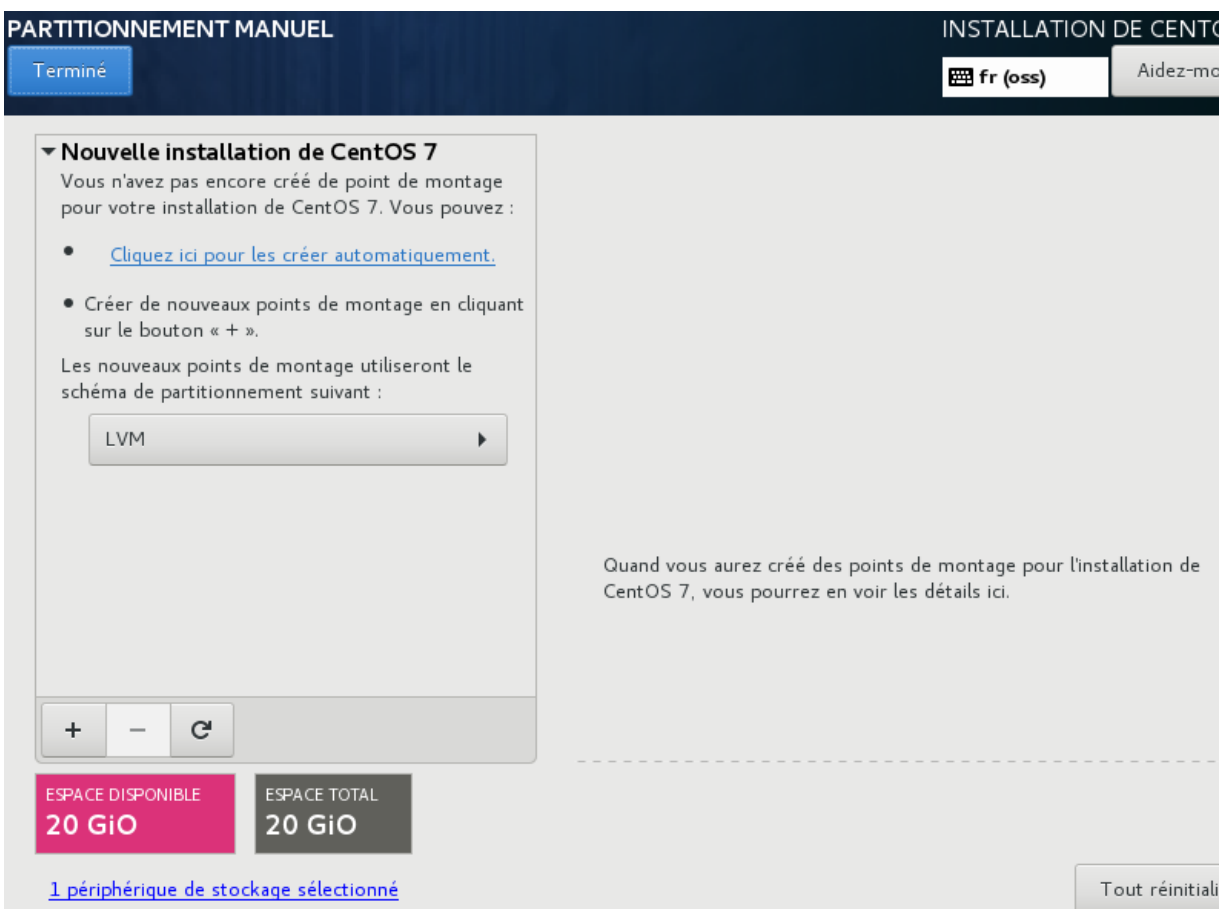
☐ Configurer automatiquement le partitionnement. ☒ Je vais configurer le partitionnement.

☐ Je voudrais libérer plus d'espace.

[Résumé complet du disque et du chargeur de démarrage...](#) 1 disque sélectionné ; 20 GiO de capacité ; 20 GiO d'espace libre [Rafraîchir.](#)

Cliquez sur « Terminé » pour afficher le menu de partitionnement manuel.

Nous allons créer automatiquement les points de montage en LVM :

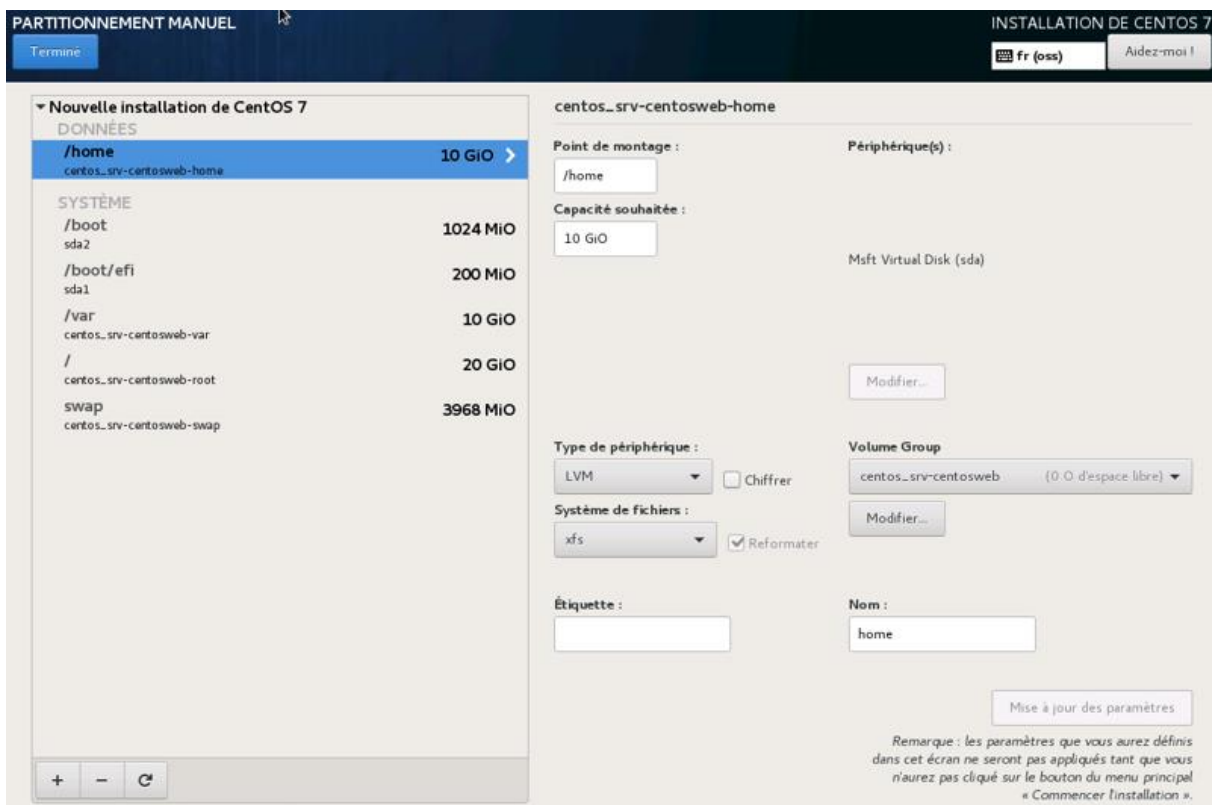


Nous allons utiliser 10 GiO pour la partition /var qui sert à stocker les fichiers variables (par exemple, les logs (journal du système)).

/home contiendra les données personnelles des utilisateurs, dans cet exemple nous allouerons 10 GiO à ce répertoire.

/swap constitue la mémoire virtuelle de la machine, il est utilisé pour décharger la RAM lorsque celle-ci arrive à saturation. On alloue généralement un espace correspondant au double de la mémoire RAM. Dans cet exemple 4GiO (3968 Mo) seront alloués.

Le partitionnement du disque devra être organisé comme dans l'image suivante.

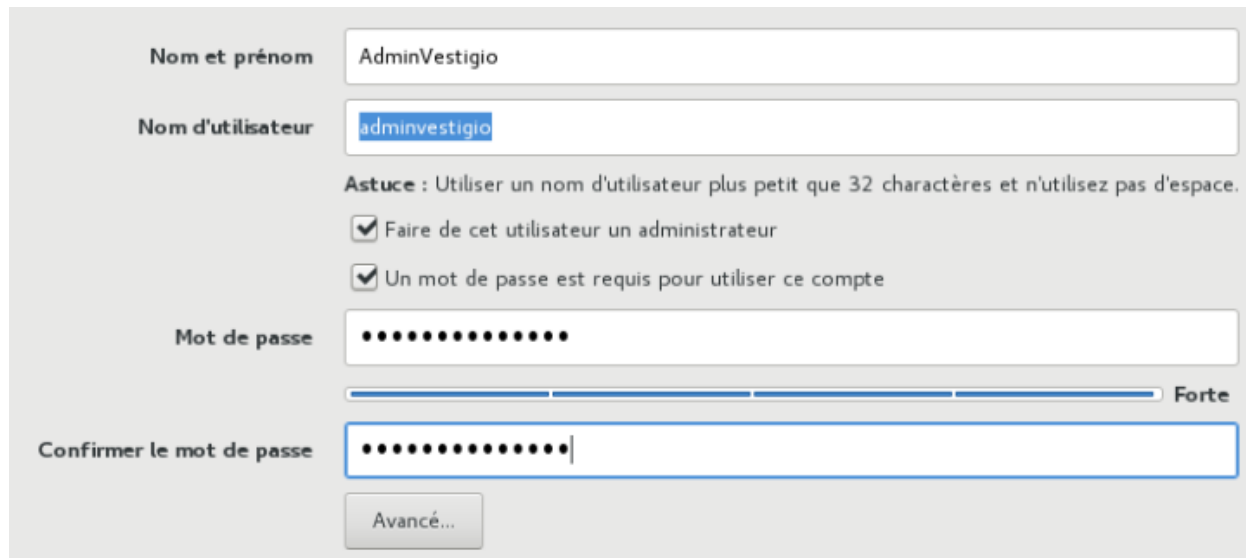


Cliquez ensuite sur « Terminé ».

Kdump est une fonctionnalité qui, après un éventuel crash du système d'exploitation, permet de sauvegarder le contenu de la mémoire système afin d'analyser les causes de ce crash.



Nous pouvons ensuite démarrer l'installation. Pendant cette installation nous pouvons créer un compte personnel qui sera utilisé comme compte administrateur. Le mot de passe sera « Formation2018 ! »



The screenshot shows a user creation form with the following fields and options:

- Nom et prénom:** AdminVestigio
- Nom d'utilisateur:** adminvestigio
- Astuce:** Utiliser un nom d'utilisateur plus petit que 32 caractères et n'utilisez pas d'espace.
- ☒ Faire de cet utilisateur un administrateur
- ☒ Un mot de passe est requis pour utiliser ce compte
- Mot de passe:** [masked with dots]
- Confirmer le mot de passe:** [masked with dots]
- Strength indicator:** A progress bar showing the password strength, labeled "Forte" (Strong).
- Button:** Avancé...

Lorsque l'installation sera terminée, nous aurons accès à la ligne de commande. Dans un premier temps, nous allons compléter l'installation des mises à jour (requiert une connexion internet), ce processus peut prendre quelques minutes supplémentaires :

```
[root@VES-DHCP1 ~]# yum upgrade -y
```

B. NFS

Afin de répondre au cahier des charges, nous intégrons à notre projet 2 machines sous Cent OS avec le rôle NFS afin de permettre une réplication des ressources.

L'installation de CentOS reste classique pour les 2 serveurs si ce n'est la configuration des disques sur lequel notre serveur principal comprend 2 disques pour séparer /var et le swap du reste de notre système alors que notre 2 ème serveur comprend 3 disques : 2 disques pour séparer /var et le swap du reste de notre système et un 3 ème disque pour permettre la sauvegarde des ressources du premier serveur sur un disque différent.

Par la suite nous ouvrons le port 2049 en TCP, utile pour le bon fonctionnement du NFS via la commande : `firewall-cmd --add-service=nfs --permanent`.

Une fois le pare-feu configuré, nous installons le rôle nfs sur nos 2 serveurs: **`Yum install nfs-utils -y`**

1. Serveur NFS

Nous allons créer une partition dédiée à notre serveur NFS via la commande `fdisk /dev/sdc`.

Ensuite, on va formater cette partition via la commande **`mkfs.xfs /dev/sdc1`**.

On va également ajouter le montage de la nouvelle partition au démarrage de la machine via la ligne **`/dev/sdc1 /nfs xfs defaults 0 0`** que l'on va placer dans le fichier situé sous la racine **`/etc/fstab`**.

Nous allons également changer les droits du dossier nfs ainsi que les groupes propriétaires via les commandes **`chmod -R 755 /nfs`** et **`chown nfsnobody :nfsnobody /nfs`**.

Nous allons finalement créer le partage qui va permettre à la machine cliente de se connecter via la ligne **`/nfs 192.168.10.6 (rw,sync,no_root_squash,no_all_squash)`**.

2. Client NFS

Pour permettre au client une connexion automatique au serveur nfs, il faut rentrer la ligne **`192.168.10.5:/nfs /mnt/nfs nfs defaults 0 0`**.

Notre serveur et notre client NFS sont désormais configurés et fonctionnels.

C. FTP

Notre Serveur FTP (Requis par le cahier des charges) sera sous Cent OS 7 sur le serveur qui as pour nom VES-CENTOS1 et pour IP 192.168.10.5.

L'installation sera donc classique à l'exception que nous activerons le lvm et nous sépareront sur 3 disques différent le système, les dossiers /var et swap ainsi que le dossier ftp afin de permettre une externalisation des données grâce au disque ftp et un maintien de fonctionnement même en cas de saturation du dossier /var ainsi qu'une rapidité d'exécution même en cas d'utilisation du dossier swap.

Nous installerons par la suite le rôle vsftpd permettant la mise en place d'un serveur ftp via la commande : **Yum install vsftpd -y** .

On autorise le ftp sur notre pare-feu via les commandes :

```
firewall-cmd --permanent --add-port=21/tcp  
firewall-cmd --permanent --add-port=40000-40100/tcp  
firewall-cmd --permanent --add-service=ftp
```

Une fois nos rôles installés, nous allons pouvoir configurés notre serveur ftp via le fichier vsftpf.conf située sous la racine **/etc/vsftpd/vsftpf.conf**.

Nous allons donc via ce fichier :

- Autorisé l'accès au Serveur FTP par les anonymes ;
- Forcer l'utilisation du protocole TLSV1 étant, a ce jour, le plus sécurisé ;
- Mettre en place un certificat permettant d'assurer sur la viabilité de notre serveur ftp ;
- Autoriser l'accès uniquement au dossier personnel pour chaque compte afin d'empêcher l'effacement d'un dossier compromettant ou nécessaire au bon fonctionnement de notre serveur ;

D. Mise en place de Samba

Conformément au cahier des charges, nous avons mis en place un Partage samba sous Cent OS afin de permettre à un ordinateur Windows de pouvoir importer / exporter des ressources depuis Cent OS.

Ce partage samba sera mis en place sur un Serveur Cent OS 7 avec le FTP et le NFS, plus précisément sur le serveur VES-CENTOS1 qui a comme adresse IP 192.168.10.5.

Nous allons dans un premier temps, sur notre Serveur Cent OS, installer samba via la commande `yum install samba.x86_64` et, par la même occasion, connecter notre serveur au domaine.

Nous pourrions désormais configurer samba via le fichier situé sous la racine `/etc/samba/smb.conf`.

Nous allons donc créer un partage pour Windows qui sera ouvert à tous.

On va nommer notre partage « Anonymous ».

On rentrera dans le fichier `smb.conf` située sous la racine `/etc/samba`.

On y intégrera les lignes: **[Anonymous]**

```
path = /samba/anonymous
browseable = yes
writable = yes
guest ok = yes
read only = no
```

On va par la suite créer un Dossier « Anonymous » via la commande **`mkdir /samba/anonymous`**.

Il faudra également éditer les permissions du dossier Anonymous afin que celui-ci puisse être modifié par n'importe qui via les lignes : **`cd /samba`**

```
chmod -R 0755 anonymous/
```

```
chown -R nobody:nobody anonymous/
```

Nous allons également autoriser SELinux pour notre dossier « Anonymous » via la commande

```
chcon -t samba_share_t anonymous/ .
```

Pour finir, nous avons désormais un Partage Anonyme accessible par tous.

Il nous faut désormais ouvrir le pare-feu afin de permettre à notre partage de pouvoir fonctionner.

Pour se faire, il faut rentrer la ligne : **`firewall-cmd --permanent --zone=public --add-service=samba`**.

Nous avons désormais un serveur samba anonyme fonctionnel.

Nous configurons également un Partage Sécurisé par un mot de passe, qui permettra, en cas de nécessité, un accès restreint a certaines ressources.

Pour ce faire, nous allons devoir, comme précédemment, créer un dossier pour notre partage que nous nommerons ici « vestigiosmb ».

On créer donc ce nouveau partage dans le fichier smb.conf avec les lignes :

```
[VESTIGIOSMB]
path = /samba/vestigiosmb
browseable =yes
writable = yes
guest ok = no
read only = no

Valid users =@smbves
```

On créer également un groupe que l'on appelle smbves tout en y intégrant un utilisateur nommé « utilisateur » avec pour mot de passe « V3stigio !! » via les commandes :

Groupadd smbves

Useradd utilisateur -G smbves

Smbpasswd -a utilisateur

On définit les permissions pour le dossier vestigiosmb via les commandes :

Cd /samba

chcon -t samba_share_t smbves/

On finit par autoriser SELinux pour notre dossier « vestigiosmb » et notre nouveau partage est désormais opérationnel.

E. Mise en place du DHCP

Le DHCP est un protocole réseau qui assure la configuration du paramétrage IP des hôtes du réseau de façon automatique. Dans notre projet nous allouerons une machine CentOS 7 qui aura un service DHCP installé et configuré afin qu'il effectue tout ce rôle. (Allouer une IP à un poste parmi une plage IP préférée). Cette machine sera redondée avec un deuxième serveur pour avoir une haute disponibilité (high availability)

Nous allons tout d'abord commencer par le téléchargement des paquets pour installer le service DHCP.

```
[root@VES-DHCP1 ~]# yum install dhcp -y_
```

Nous allons ensuite débloquer le firewall pour le service dhcpd et le rafraichir.

```
[root@VES-DHCP1 ~]# firewall-cmd --add-service=dhcp --permanent
success
[root@VES-DHCP1 ~]# firewall-cmd --reload
success
```

Après avoir répété les mêmes commandes sur le serveur ves-dhcp2, passons à la configuration du dhcp :

```
[root@VES-DHCP1 ~]# vi /etc/dhcp/dhcpd.conf
```

Ces lignes devront être entrées pour les deux serveurs. Les durées minimales et maximales des baux pour les hôtes du réseau seront configurées dans un premier temps.

Nous déclarerons ensuite le réseau avec le DNS, la passerelle, ainsi que la plage d'adresses que nous utiliserons pour les postes clients.

```
default-lease-time 86400; #Bail de 24H
max-lease-time 172800; #Bail maxi de 48h

#Déclaration du réseau
subnet 192.168.10.0 netmask 255.255.255.0 {
    option domain-name-servers 192.168.10.1; #DNS
    option routers 192.168.10.1; #Passerelle
    pool {
        failover peer "dhcp-failover";
        range 192.168.10.31 192.168.10.230;
    }
}
```

Les critères de haute disponibilité seront légèrement différents entre les deux serveurs.

Le premier serveur sera désigné comme « master » (primary), ce sera lui qui délivrera les adresses en priorité. Le deuxième serveur sera désigné comme « secondaire ».

Ci-dessous les critères de configuration de haute disponibilité pour le serveur dhcp1 :

```
failover peer "dhcp-failover" {
    primary;
    address 192.168.10.3;
    port 647;
    peer address 192.168.10.4;
    peer port 647;
    max-response-delay 60;
    max-unacked-updates 10;
    mclt 3600;
    split 128;
    load balance max seconds 3;
}
```

Le port 647 TCP est le port permettant le dhcp failover (en français « de basculement »). Le peer port constitue le port d'écoute pour le serveur secondaire.

Le peer address constitue l'adresse IP du DHCP partenaire.

max-response-delay correspond au temps de réponse entre les deux serveurs maximal (en secondes).

Max-unacked-updates est le nombre de messages de bail maximal qu'un serveur DHCP peut envoyer sans recevoir d'acquiescement de la part de son partenaire.

Mclt est le temps que le serveur DHCP peut assurer seul sa tâche suite à la défaillance de son partenaire.

Load balance max seconds est le temps limite de traitement de demande de dhcp. Si un client ne reçoit pas de réponse à son message de type « dhcpdiscover » ou « dhcprequest » par le serveur dhcp, le serveur partenaire prendra le relai pour traiter la demande du poste client.

La configuration des critères de haute disponibilité du deuxième serveur est presque identique, certains éléments ne sont cependant pas nécessaires.

```
failover peer "dhcp-failover" {
    secondary;
    address 192.168.10.4;
    port 647;
    peer address 192.168.10.3;
    peer port 647;
    max-response-delay 60;
    max-unacked-updates 10;
    load balance max seconds 3;
}
```

Une fois la configuration des fichiers de configuration terminée, il faudra redémarrer le service dhcpd pour prendre en compte les modifications. Ce service devra être redémarré à chaque modification.

Après avoir configuré nos deux serveurs DHCP nous allons pouvoir ouvrir le port 647 TCP pour permettre à nos serveurs de fonctionner en haute disponibilité.

F. Intégration des Serveur Linux dans Active Directory

Tout d'abord nous devons installer les paquets suivants pour permettre l'intégration de CentOS7

yum install realmd oddjob oddjob-mkhomedir sssd adcli openldap-clients polycoreutils-python samba-common samba-common-tools krb5-workstation ntp -y

Dans le fichier hosts (vi /etc/hosts), nous allons ajouter notre Active Directory/Contrôleur de Domaine :

```
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.10.1 ves-ad01.ves.lan ves-ad01
```

Nous devons ensuite synchroniser l'heure avec le contrôleur de domaine dans vi /etc/ntp.conf

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
#server 0.centos.pool.ntp.org iburst
#server 1.centos.pool.ntp.org iburst
#server 2.centos.pool.ntp.org iburst
#server 3.centos.pool.ntp.org iburst
server ves-ad01.ves.lan iburst
```

Lancer le service dès le démarrage avec **systemctl enable ntpd** et **systemctl start ntpd**

Une fois la vérification de la date et heure et que le serveur DNS de la carte réseau soit bien le contrôleur de domaine (avec les commandes nmcli et nmtui), nous pouvons ajouter la machine au domaine.

realm join --administrateur ves-ad01.ves.lan

Nous pouvons vérifier la liste des domaines avec **realm list** et une connexion avec :

Id administrateur@ves.lan

V. Base de données

Pour la gestion du parc nous avons choisi l'outil de gestion : GLPI.

Cet outil est un outil open source et nous servira à gérer les ordinateurs, imprimantes, utilisateurs.

Nous l'avons choisi car il est gratuit, simple d'utilisation et répond parfaitement au cahier des charges.

GLPI intègre de nombreuses fonctionnalités telles que :

- Inventaire des ordinateurs, périphériques (Clavier, souris..), imprimantes et autres consommable.
- Gestion des licences
- Gestion des réparations
- Gestions des fournisseurs, Contrats, documents (ex : bon de commande d'un poste)
- Réservation de matériel
- Help desk

Il dispose également d'un outil de ticketing permettant de garder un historique de tout incident pouvant survenir sur une machine afin d'optimiser nos méthodes de résolution.

Nous l'utiliserons en paire avec l'outil OCSNG qui lui permet de récupérer les caractéristiques système des PC puis nous importerons ces données pour la première entrée dans la base GLPI.

A. Installation de GLPI

La version de GLPI utilisée sera la 0.90.5. Celle-ci se fera sur un serveur CentOS 7. (voir l'installation dans IV)

1. Configuration du serveur web

Nous allons tout d'abord installer les modules requis pour l'outil, à savoir : SQL, PHP avec php-mysql, php-gg, php-mbstring et wget.

```
[root@ves-web01 html]# yum install httpd php php-{gd,mysql,mbstring} mariadb-server wget_
```

Une fois l'installation terminée vous devriez avoir le message de confirmation suivant :

```
Installé :
httpd.x86_64 0:2.4.6-80.el7.centos.1      mariadb-server.x86_64 1:5.5.56-2.el7      php.x86_64 0:5.4.16-45.el7
php-mbstring.x86_64 0:5.4.16-45.el7      php-mysql.x86_64 0:5.4.16-45.el7      wget.x86_64 0:1.14-15.el7_4.1
```

Nous allons ensuite démarrer les services httpd et mariadb et vérifier leur statut :

```
[root@ves-web01 ~]# systemctl start httpd mariadb
[root@ves-web01 ~]# systemctl is-active httpd mariadb
active
active
```

Toujours avec les mêmes services, nous allons les activer au démarrage et vérifier également s'ils le seront au prochain démarrage :

```
[root@ves-web01 ~]# systemctl enable httpd mariadb
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/mariadb.service to /usr/lib/systemd/system/mariadb.service.
```

```
[root@ves-web01 ~]# systemctl is-enabled httpd mariadb
enabled
enabled
```

Nous allons devoir autoriser les protocoles http et https dans le firewall. Un redémarrage du firewall sera nécessaire par la suite.

```
[root@ves-web01 ~]# firewall-cmd --zone=public --add-port=http/tcp --permanent
success
[root@ves-web01 ~]# firewall-cmd --zone=public --add-port=https/tcp --permanent
success
[root@ves-web01 ~]# firewall-cmd --reload
success
```

Nous pouvons ensuite vérifier la prise en compte des commandes ci-dessus.

```
[root@ves-web01 ~]# firewall-cmd --list-all
public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh dhcpv6-client
  ports: 80/tcp 443/tcp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

La ligne qui nous intéresse est « **ports : 80/tcp 443/tcp** »

Le port 80 correspond au http, tandis que le port 443 correspond au https. Ils sont ici bien pris en compte.

Nous allons ensuite créer la base de données ainsi qu'un utilisateur pour GLPI. Pour cela nous allons devoir utiliser MariaDB.

```
[root@ves-web01 ~]# mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 2
Server version: 5.5.56-MariaDB MariaDB Server

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

Création de la base de données ainsi que l'utilisateur :

```
MariaDB [(none)]> create database glpi;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> create user 'glpiuser'@'localhost' identified by 'glpipassword';
Query OK, 0 rows affected (0.00 sec)
```

Nous allons ensuite attribuer les droits à cet utilisateur :

```
MariaDB [(none)]> grant all privileges on glpi.* to 'glpiuser'@'localhost';
Query OK, 0 rows affected (0.00 sec)
```



```

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| glpi       |
| mysql      |
| performance_schema |
| test       |
+-----+
5 rows in set (0.00 sec)

MariaDB [(none)]> select host, user from mysql.user;
+-----+-----+
| host      | user      |
+-----+-----+
| 127.0.0.1 | root      |
| ::1       | root      |
| localhost |            |
| localhost | glpiuser   |
| localhost | root       |
| ves-web01 |            |
| ves-web01 | root       |
+-----+-----+
7 rows in set (0.00 sec)

```

Nous pouvons ensuite vérifier que la base et l'utilisateur ont bien été créés grâce à la commande ci-dessus.

Nous allons ensuite télécharger la version de GLPI qui nous intéresse (0.90.5) dans le répertoire /var/www/html :

```

[root@ves-web01 ~]# cd /var/www/html
[root@ves-web01 html]# wget https://github.com/glpi-project/glpi/releases/download/0.90.5/glpi-0.90.5.tar.gz
--2018-08-20 11:40:02-- https://github.com/glpi-project/glpi/releases/download/0.90.5/glpi-0.90.5.tar.gz

```

Décompression de l'archive puis suppression :

```

[root@ves-web01 html]# tar -zxvf glpi-0.90.5.tar.gz && rm -rf glpi-0.90.5.tar.gz

```

Nous allons modifier les permissions d'Apache sur le dossier GLPI

Nous allons créer un hôte virtuel pour donner un accès à GLPI.

Insérez les arguments ci-dessous dans : **vi /etc/httpd/conf.d/glpi.conf**

```
<VirtualHost 192.168.1.12:80>
    ServerName ves-web01
    DocumentRoot /var/www/html/glpi
    <Directory /var/www/html/glpi>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride All
        Require all granted
    </Directory>
    ServerSignature off
    ErrorLog /var/log/http.log
    CustomLog /var/log/access.log combined
</VirtualHost>
```

Enfin, afin de permettre au server web Apache de fonctionner. Nous allons configurer SELinux (module de sécurité) en permissive.

Allez dans le fichier de configuration de SELinux

```
[root@ves-web01 html]# vi /etc/selinux/config_
```

Modifiez la ligne SELinux=enforced en SELinux=permissive comme dans l'image ci-dessous :

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of three two values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Pour tester notre configuration ci-dessus, nous pouvons utiliser la commande **apachectl configtest**.

Si tout est convenable la commande vous retournera « **Syntax OK** »

Nous pouvons ensuite redémarrer le service httpd pour finaliser notre configuration.

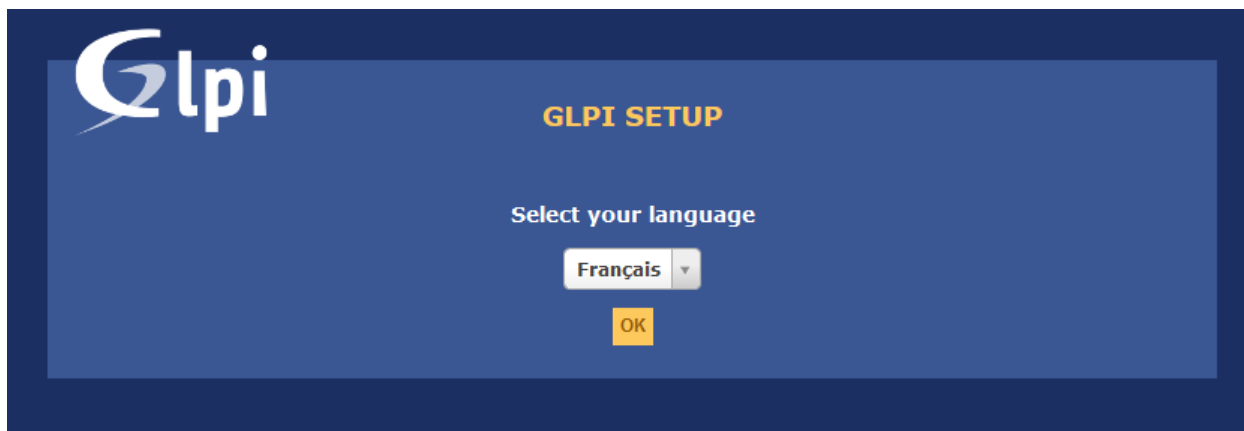
```
[root@ves-web01 html]# systemctl restart httpd
```

2. Interface GLPI

Pour accéder à l'interface GLPI nous allons rentrer l'URL « **http://192.168.10.8/glpi** » (l'adresse correspond l'IP du serveur web)

Nous arriverons ensuite dans l'installation de GLPI.

Sélection de la langue en Français :



Après avoir accepté les termes, nous avons deux choix, installer ou mettre à jour. Dans notre cas, nous allons procéder à une installation :



L'utilitaire va ensuite vérifier les droits d'accès pour assurer que l'exécution de GLPI soit compatible avec notre environnement Linux.

GLPI SETUP	
Étape 0	
Vérification de la compatibilité de votre environnement avec l'exécution de GLPI	
Tests effectués	Résultats
Test du Parseur PHP	✓
Test de l'extension MySQLi	✓
Test des sessions	✓
Test de l'utilisation de Session_use_trans_sid	✓
Test sur l'extension magic_quotes_sybase	✓
Test sur les fonctions ctype	✓
Test sur l'extension fileinfo	✓
Test sur les fonctions Json	✓
Test sur l'extension mbstring	✓
Test sur l'extension GD	✓
Test sur l'extension zlib	✓
Test de la mémoire allouée	✓
Test d'écriture du fichier de configuration	✓
Test d'écriture de fichiers documents	✓
Test d'écriture de fichiers dump	✓
Test d'écriture des fichiers de sessions	✓
Test d'écriture des fichiers des actions automatiques	✓
Test d'écriture des fichiers de graphiques	✓
Test d'écriture des fichiers de verrouillage	✓
Test d'écriture des documents des plugins	✓
Test d'écriture des fichiers temporaires	✓
Test d'écriture de fichiers rss	✓
Test d'écriture des fichiers téléchargés	✓
Test d'écriture de fichiers photos	✓
Test d'écriture des fichiers de journal	✓

- Renseignement des informations de connexion à la base de données MYSQL : les identifiants correspondent à ceux que nous avons entré lors de la création de la base de données. (glpivestigio/Formation2018)

-Sélection de la base de données que nous avons créé précédemment « glpi » :



La prochaine page vous affichera un message de confirmation de connexion à la base de données. Vous obtiendrez ensuite des logins de base selon le type de compte (administrateur, technicien, normal, postonly).

Lors de notre première connexion deux messages de sécurité s’afficheront sur le menu principal.

⚠ Pour des raisons de sécurité, veuillez changer le mot de passe par défaut pour le(s) utilisateur(s) : glpi post-only tech normal

⚠ Pour des raisons de sécurité, veuillez supprimer le fichier : install/install.php

Le premier est sur la sécurité des comptes, les mots de passes seront modifiés pour notre utilisation.

Le deuxième indique la présence du fichier d’installation dans `/var/www/html/glpi/install` . Nous allons le supprimer.

Sur la machine du serveur web, se rendre sur le dossier noté ci-dessus. Et vérifier la présence du fichier.

```
[root@ves-web01 ~]# cd /var/www/html/glpi/install
[root@ves-web01 install]# ls
index.php          update_0681_07.php  update_0782_080.php  update_0845_0846.php
install.php        update_07_071.php   update_080_0801.php  update_085_0853.php
mysql              update_071_0712.php update_0801_0803.php  update_0853_0855.php
update_031_04.php  update_0712_0713.php update_0803_083.php   update_0855_090.php
update_04_042.php  update_0713_072.php update_083_0831.php   update_090_0901.php
update_042_05.php  update_072_0721.php update_0831_0833.php  update_0901_0905.php
update_05_051.php  update_0721_0722.php update_0831_084.php   update_content.php
update_051_06.php  update_0722_0723.php update_084_0841.php   update.php
update_06_065.php  update_0723_078.php update_084_085.php    update_to_031.php
update_065_068.php update_078_0781.php  update_0841_0843.php
update_068_0681.php update_0781_0782.php update_0843_0844.php
```

Le fichier est donc bien présent dans le dossier. Procédez à sa suppression :

```
[root@ves-web01 install]# rm install.php
rm : supprimer fichier « install.php » ? y
```

B. Installation de Fusion Inventory

Fusion Inventory va nous servir de plugin de communication entre GLPI et les postes du réseau. Ce plugin permettra d'avoir une remontée automatique de notre inventaire informatique ainsi que de garder une traçabilité de ce dernier.

Tout comme GLPI ce logiciel est libre et donc gratuit d'utilisation.

En comparaison avec son alternative populaire OCS Inventory NG (Open Computer and Software Inventory New Generation) celui-ci est plus simple à mettre en œuvre.

L'installation du plugin se déroule en deux parties. Il faut tout d'abord installer le plugin dans GLPI dans le serveur avec une petite configuration dans GLPI. Pour les postes client Windows, il faudra installer un agent qui recueillera les informations.

Nous installerons cet agent automatiquement via GPO, mais nous allons néanmoins décrire le processus d'installation en utilisant une installation manuelle via l'exécutable dans ce document.

1. Installation du plugin dans GLPI

Sur le serveur web, nous nous positionnerons dans le dossier `/var/www/html/glpi/plugins` avec la commande `CD`.

Dans ce dossier nous téléchargerons le fichier archive `tar.gz` avec la commande `wget` :

```
wget https://github.com/fusioninventory/fusioninventory-for-glpi/releases/download/glpi090%2B1.4/fusioninventory-for-glpi_0.90.1.4.tar.gz
```

Il faudra ensuite décompresser cette archive :

```
[root@ves-web01 plugins]# tar -zxvf fusioninventory-for-glpi_0.90.1.4.tar.gz
```

Si vous n'étiez pas dans le bon répertoire vous pouvez déplacer le fichier `fusioninventory` après la décompression de l'archive.

```
[root@ves-web01 plugins]# mv fusioninventory /var/www/html/glpi/plugins/
```

Donnez les droits à `apache` sur ce dossier.

```
[root@ves-web01 plugins]# chown -R apache:apache /var/www/html/glpi/plugins/
```

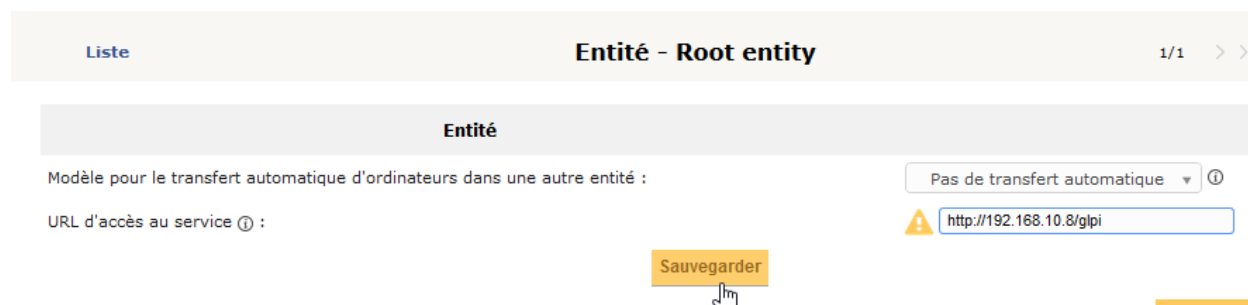
Après s'être connecté en tant qu'administrateur sur GLPI, dirigez-vous vers le menu déroulant « Configuration » puis « Plugins ».

Fusion Inventory sera ainsi détecté et vous aurez le choix de l'installer puis de l'activer.

Puisque c'est notre première installation de Plugin sur GLPI, un message s'affichera :



Cliquez sur le message pour configurer la page de connexion. Il faudra insérer l'adresse de notre GLPI, à savoir : <http://192.168.10.8/glpi>

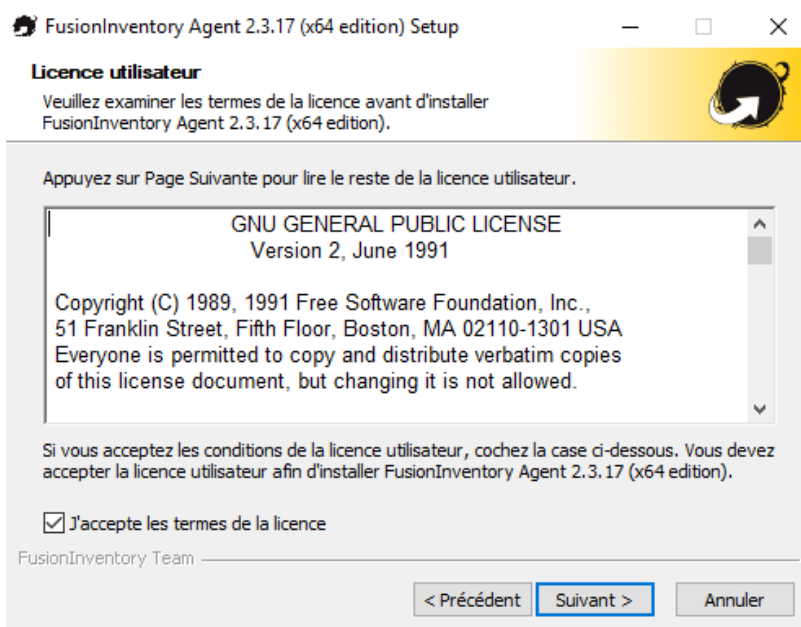
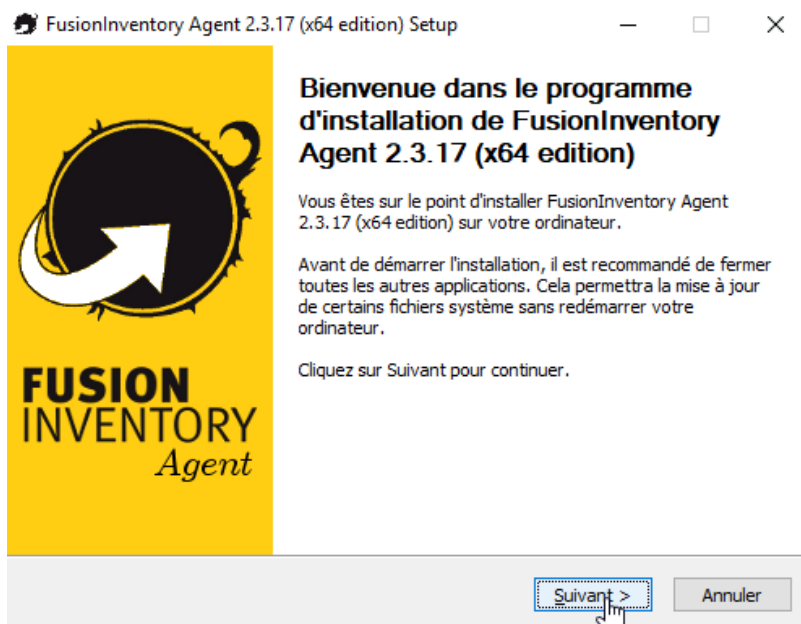


2. Installation de l'agent

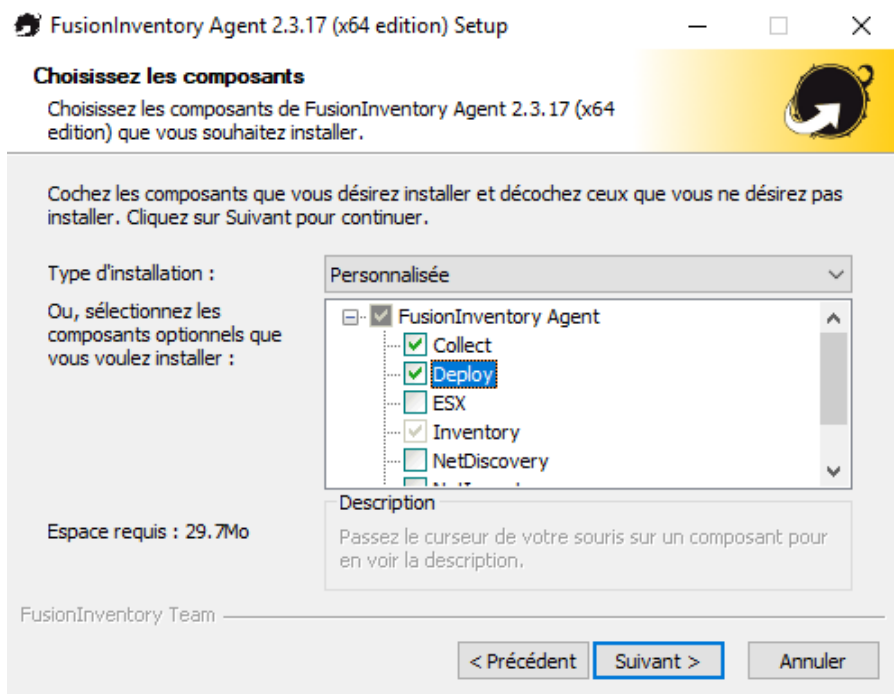
Vu que nous utiliserons l'agent pour les machines clientes des employés, nous utiliserons que la version Windows.

Cet Agent sera déployé par GPO, mais nous allons vous montrer l'installation manuelle avec un exécutable téléchargeable sur le site officiel.

Une fois l'exécutable lancé, sélectionnez la langue française et acceptez les conditions d'utilisation.

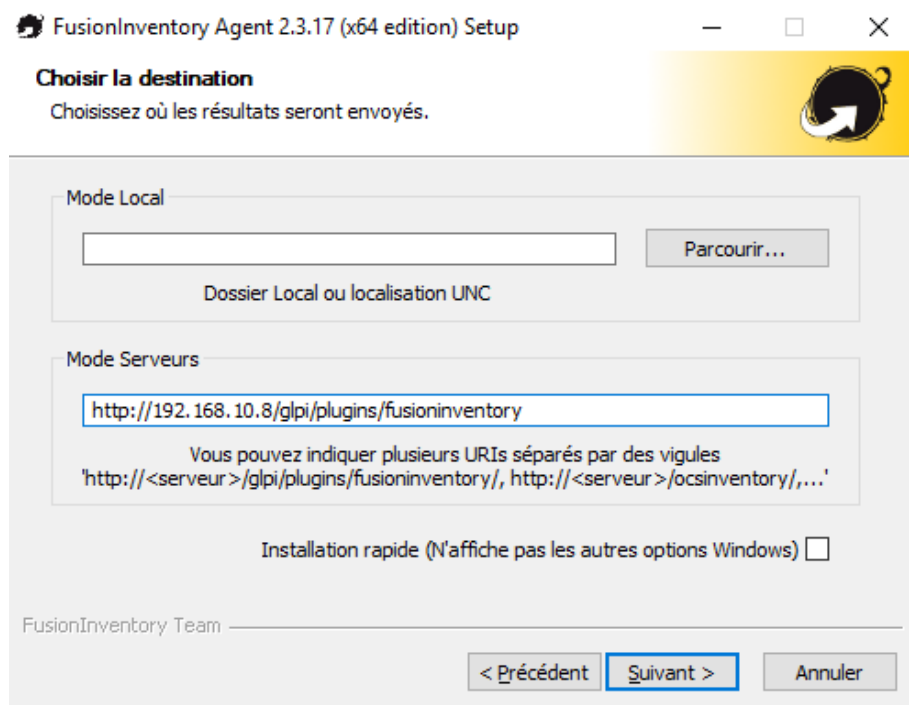


Cochez les cases « Collect » et « Deploy » pour les composants.



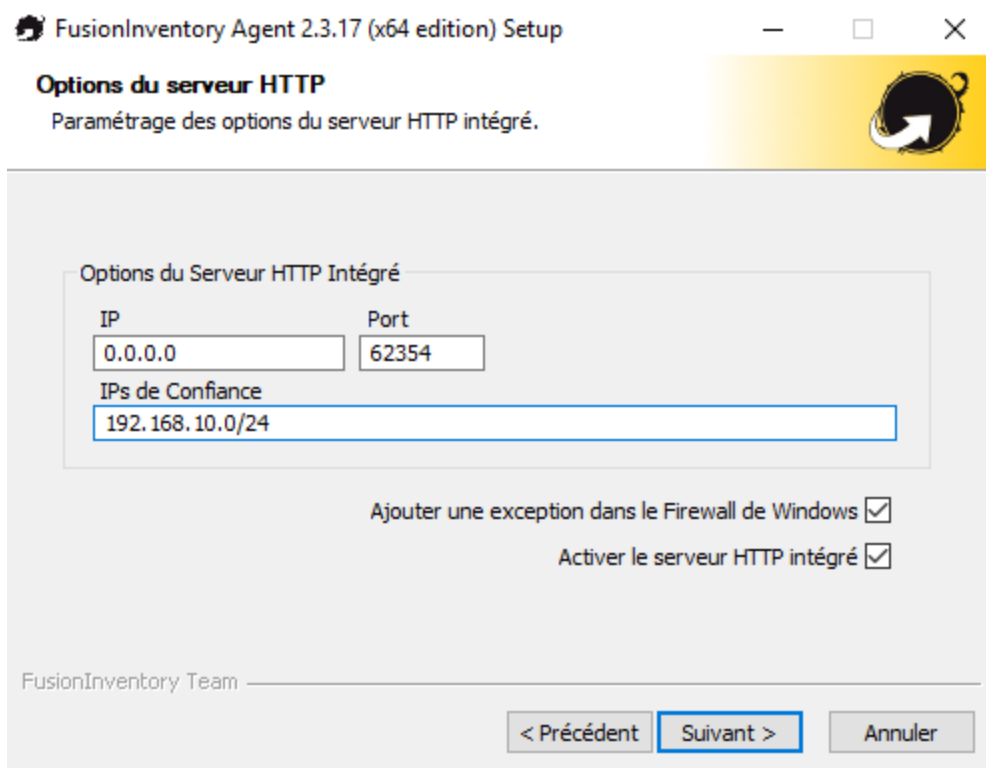
Gardez le dossier d'installation tel quel et faites suivant.

Nous allons spécifier ici notre serveur GLPI qui dispose du plugin.

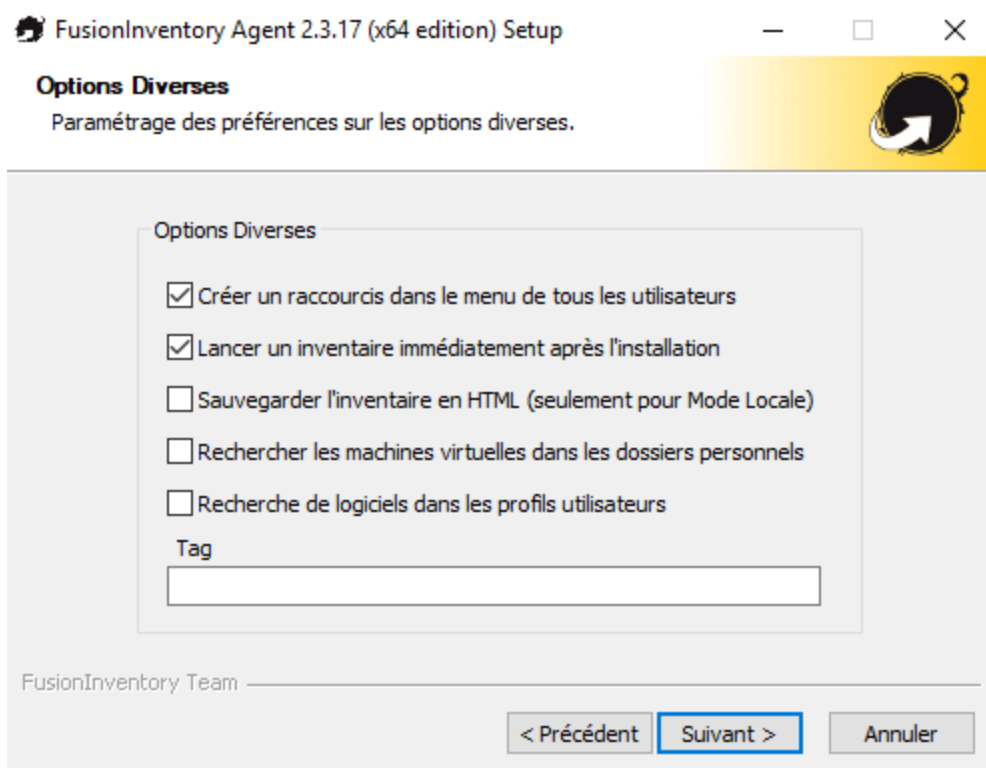


Cliquez sur « Suivant » pour le SSL et le proxy.

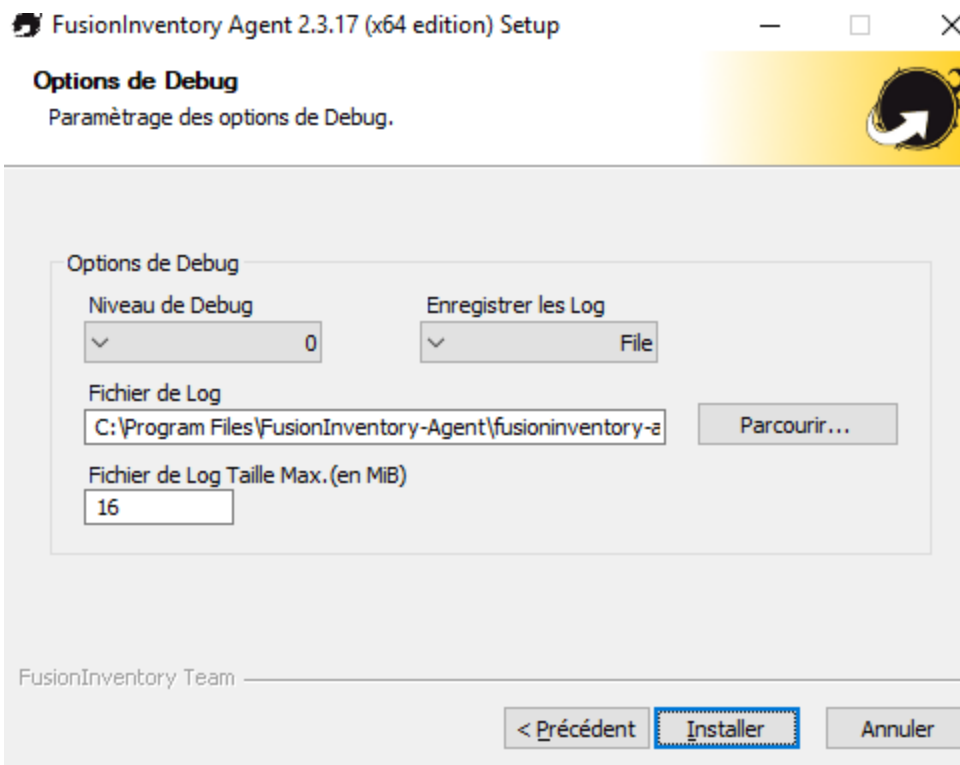
Nous allons préciser ici dans « IP de confiance » l'ensemble des machines de notre réseau.



Cochez la case « Lancer un inventaire immédiatement après l'installation ».



Laissez les options avancées et de debug préconfigurées et installez le programme.



Une fois l'installation terminée, on peut se connecter sur **http://IP_DE_LA_MACHINE:62354** afin de forcer l'inventaire sur le poste client.



FUSION INVENTORY

This is FusionInventory Agent 2.3.17

The current status is waiting

[Force an Inventory](#)

Next server target execution planned for:

- <http://192.168.10.8/plugins/fusioninventory>: Tue Aug 21 00:20:14 2018

De retour sur GLPI, allez dans Plugins > FusionInventory > Général > Gestion des Agents

The screenshot shows the Glpi FusionInventory Agent interface. The top navigation bar includes 'Accueil', 'Plugins', 'FusionInventory', and 'Agent'. Below this is a search bar with 'Rechercher' and a magnifying glass icon. A secondary navigation bar contains tabs for 'Général', 'Tâches', 'Règles', 'Réseau', 'Déployer', and 'Guide'. The main content area features a search filter 'Éléments visualisés' with a dropdown menu, a search button 'Rechercher', and a star icon. Below the search bar, there are options for 'Affichage (nombre d'éléments)' set to 20, a 'Page courante en PDF paysage' button, and a status 'De 1 à 1 sur 1'. A table with columns 'Nom', 'Entité', 'Dernier contact', 'Verrouillé', 'Device_id', 'Lié à l'ordinateur', 'Version', and 'Jeton' displays one entry: 'DESKTOP-3LPQM9M-2018-08-21-00-06-35' with 'Root entity' as the entity, '2018-08-20 22:07' as the last contact, 'Non' as locked status, 'DESKTOP-3LPQM9M-2018-08-21-00-06-35' as device ID, 'DESKTOP-3LPQM9M' as linked computer, 'INVENTORY : v2.3.17' as version, and '12345678' as token. Action buttons are visible above and below the table.

	Nom	Entité	Dernier contact	Verrouillé	Device_id	Lié à l'ordinateur	Version	Jeton
<input type="checkbox"/>	DESKTOP-3LPQM9M-2018-08-21-00-06-35	Root entity	2018-08-20 22:07	Non	DESKTOP-3LPQM9M-2018-08-21-00-06-35	DESKTOP-3LPQM9M	INVENTORY : v2.3.17	12345678

Nous pouvons donc apercevoir notre machine de test.

VII. Prise en main à distance

Le cahier des charges nous impose une prise en main à distance. Pour pallier également les problèmes d'organisation pour le dépannage du service informatique, nous avons opté pour une licence TeamViewer Corporate à base d'un abonnement mensuel à 124,90€ par mois.



Cela permettra au service informatique d'optimiser ses interventions sur des problèmes pouvant être réglés par un simple accès à distance sur leur poste informatique.

La version Corporate inclut 3 canaux, c'est-à-dire, 3 connexions simultanées sur le réseau, pouvant permettre plusieurs dépannages en même temps si cela est nécessaire.

Si besoin est, pour des frais supplémentaires, nous pouvons avoir accès à des canaux supplémentaires. Cependant nous allons rester à 3 canaux afin d'évaluer le besoin de nos utilisateurs.

Elle inclut également une option de déploiement en masse pour l'ensemble des postes du réseau.

VIII. Conclusion

Nous avons répondu à l'ensemble des demandes du cahier des charges avec la mise en œuvre d'outils d'administration Windows Server 2016 et de Linux via CentOS 7. Nous avons pu développer nos compétences techniques dans ces deux domaines.

Malgré des difficultés concernant la base de données, à la suite d'une réunion, nous avons décidé de créer un GLPI qui répond au cahier des charges.

Pour le matériel que nous avons acheté, c'est un investissement pour l'avenir, cela nous servira pour la création de nouveaux serveurs pour améliorer l'infrastructure.

IX. Annexes :

A. Charte graphique

Les documents provenant de la société Vestigio doivent respecter la charte graphique suivante :

En-tête de page :

- Police « Vestigio » :
- Couleurs logo : #000000 (Noir) et #F9F9F9 (Blanc)
- Couleurs « Vestigio » : #F9F9F9

Mise en page du texte :

I. Titre 1 : Arial 16

A Titre 2 : Arial 13

1. Titre 3 : Arial 12

a) Titre 4 : Arial 11

Texte Normal : Calibri (Body) 11

Pied de page :

Texte pied de page : Arial 8

B. Automatisation des tâches (Script Powershell)

Pour inclure un exemple d'automatisation des tâches dans les objectifs pédagogiques du projet. Nous avons réalisé un Script sur l'utilitaire Windows Powershell permettant la création automatique d'arborescence Active Directory :

```
### SCRIPT DE CREATION D'OBJETS AD ENTREPRISE VESTIGIO ###
##### OU/GROUPES/UTILISATEURS/DOSSIERS #####

##### CREATION DES VARIABLES GLOBALES #####
$nomoubase=Read-Host "Entrez le nom d'une OU"
$chemin1=(Get-ADDomain).distinguishedName
$chemin2="OU="+$nomoubase+","+$chemin1
$chemin3groupes="OU=GROUPES,"+$chemin2
$chemin3imprims="OU=IMPRIMANTES,"+$chemin2
$chemin3utils="OU=UTILISATEURS,"+$chemin2
$chemin3ordis="OU=ORDINATEURS,"+$chemin2
$dfspath=(get-dfsroot).path
$liste=import-csv -Path "./liste.csv" -Delimiter ";" -Encoding UTF8

####Function press()
####{
####Write-Host -NoNewline -Object 'Appuyer sur 1 touche pour continuer'
####$null = $Host.UI.RawUI.ReadKey('NoEcho,IncludeKeyDown')
####menu_principal
####}

function create_ous_base()
{echo "Creation des OUs"
New-ADOrganizationalUnit -Name $nomoubase -path $chemin1 -
ProtectedFromAccidentalDeletion $False -Verbose
New-ADOrganizationalUnit -Name "GROUPES" -path $chemin2 -
ProtectedFromAccidentalDeletion $False -Verbose
New-ADOrganizationalUnit -Name "IMPRIMANTES" -path $chemin2 -
ProtectedFromAccidentalDeletion $False -Verbose
New-ADOrganizationalUnit -Name "ORDINATEURS" -path $chemin2 -
ProtectedFromAccidentalDeletion $False -Verbose
New-ADOrganizationalUnit -Name "UTILISATEURS" -path $chemin2 -
ProtectedFromAccidentalDeletion $False -Verbose
create_ous_services
Start-Sleep -Seconds 5}

function create_ous_services()
{
    write-host "Création des ous services"
    foreach ($ligne in $liste)
    {
        $service=($ligne.service).ToUpper()
        try{New-ADOrganizationalUnit -Name $service -Path $chemin3groupes -
ProtectedFromAccidentalDeletion $false -Verbose}
        catch{}
        try{New-ADOrganizationalUnit -Name $service -Path $chemin3imprims -
ProtectedFromAccidentalDeletion $false -Verbose}
        catch{}
        try{New-ADOrganizationalUnit -Name $service -Path $chemin3utils -
ProtectedFromAccidentalDeletion $false -Verbose}
        catch{}
        try{New-ADOrganizationalUnit -Name $service -Path $chemin3ordis -
ProtectedFromAccidentalDeletion $false -Verbose}
        catch{}
    }

Start-Sleep -Seconds 5
}

function create_ous_groupes()
```

```

{
    Write-Host "Creation des groupes"
    foreach ($ligne in $liste)
    {
        $service=($ligne.service).ToUpper()
        $chemin4="OU="+$Service+", "+$chemin3groupes
        $GG="GG_"+$service
        $GU="GU_"+$service
        $GDL_R="GDL_"+$service+"_R"
        $GDL_Rw="GDL_"+$service+"_Rw"
        $GDL_M="GDL_"+$service+"_M"
        $GDL_F="GDL_"+$service+"_F"
        try{New-ADGroup -GroupCategory Security -GroupScope Global -Name $GG -Path
$chemin4}
        catch{}
        try{New-ADGroup -GroupCategory Security -GroupScope Universal -Name $GU -
Path $chemin4}
        catch{}
        try{New-ADGroup -GroupCategory Security -GroupScope DomainLocal -Name
$GDL_R -Path $chemin4}
        catch{}
        try{New-ADGroup -GroupCategory Security -GroupScope DomainLocal -Name
$GDL_Rw -Path $chemin4}
        catch{}
        try{New-ADGroup -GroupCategory Security -GroupScope DomainLocal -Name
$GDL_M -Path $chemin4}
        catch{}
        try{New-ADGroup -GroupCategory Security -GroupScope DomainLocal -Name
$GDL_F -Path $chemin4}
        catch{}

        Add-ADGroupMember $GU -Members $GG -Verbose
        Add-ADGroupMember $GDL_R -Members $GU -Verbose
        Add-ADGroupMember $GDL_Rw -Members $GU -Verbose
        Add-ADGroupMember $GDL_M -Members $GU -Verbose
        Add-ADGroupMember $GDL_F -Members $GU -Verbose
    }
    Start-Sleep -Seconds 5
}

function create_ous_utilisateurs()
{
    $pass=ConvertTo-SecureString("Formation2018!") -AsPlainText -Force
    Write-Host "Creation des utilisateurs"

    foreach ($ligne in $liste)
    {
        $service=($ligne.service).ToUpper()

        $prenom=($ligne.prenom).substring(0,1).ToUpper()+($ligne.prenom).substring(1).ToLower(
)
        $nom=($ligne.nom).ToUpper()
        $nomcomplet=$nom+" "+$prenom
        $description=$ligne.description
        $login=$nom.ToLower()+"."+$prenom.ToLower()
        $upn=($login+"@"+$env:USERDNSDOMAIN).ToLower()
        $chemin4user="OU="+$service+", "+$chemin3utils
        $fonction=$ligne.fonction
        $groupe="GG_"+$service

        New-ADUser -Enabled $true `
        -GivenName $prenom `
        -Name $nomcomplet `
        -Surname $nom `
        -DisplayName $nomcomplet `
        -Description $description `
        -EmailAddress $upn `
        -UserPrincipalName $upn `
        -Path $chemin4user `
        -SamAccountName $login `
        -ChangePasswordAtLogon $true `
        -AccountPassword $pass
    }
}

```

```

-Title $fonction -Department $service

Add-ADGroupMember $groupe -Members $login
creation_dossiers($login,$service)
#permissions
}
Start-Sleep -Seconds 5}

function creation_dossiers()
{
    $dossierperso=$dfspath+"\Perso\"
    $dossierservices=$dfspath+"\Services\"

    New-Item -name $login -ItemType Directory -path $dossierperso

    try {
        New-Item -name $service -ItemType Directory -path $dossierservices
    }
    catch {
        Write-Host -name "Les dossiers "+$dossierservices + "Existe déjà"
    }
}

function suppression()
{
    Remove-ADOrganizationalUnit -Identify $chemin1 -Recursive -Confirm:$false -Verbose

    $dossierperso=$dfspath+"\perso\"
    $listedossierperso=get-childitem -Directory -path $dossierperso
    $dossierservice=$dfspath+"\services\"
    $listedossierservices=get-childitem -Directory -path $dossierservices

    foreach ($i in $listedossierperso)
    {
        $nomdossierperso=$dossierperso+$i.name
        Remove-Item -Path $nomdossierperso -Recurse -Verbose
    }
    foreach ($i in $listedossierservices)
    {
        $nomdossierserv=$dossierservices+$i.name
        Remove-Item -Path $nomdossierserv -Recurse -Verbose
    }

    {echo "Suppression"}
}

function permissions()
{
    $cheminperso=$dfspath+"\perso\"
    $dossierpersoliste=get-childitem -Directory -path $cheminperso
    $cheminservice=$dfspath+"\services\"
    $dossierservicesliste=get-childitem -Directory -path $cheminservices

    foreach ($dossier in $dossierpersoliste)
    {
        $nomdossierperso=$dossierperso+$i.fullname
        $acl=(get-item $chemindossier).GetAccessControl('Access')
        $username=$dossier.name
        $ar=new-object security.accesscontrol.filesystemAccessRule
        ($username,'Modify','ContainerInherit,ObjectInherit','none','Allow')
        $acl.SetAccessRule($ar)
        set-acl -Path $chemindossier -AclObject $acl
    }

    foreach ($dossier in $dossierpersoservice)
    {
        $nomdossierperso=$dossierperso+$i.fullname
        $acl=(get-item $chemindossier).GetAccessControl('Access')
        $username=$dossier.name
        $ar=new-object security.accesscontrol.filesystemAccessRule
        ($username,'Modify','ContainerInherit,ObjectInherit','none','Allow')
        $acl.SetAccessRule($ar)
    }
}

```

```

        set-acl -Path $chemindossier -AclObj##### COURS GMSI Laurent Bureau
BLSI #####
##### POWERSHELL et ADDS #####
#Activation des privilèges et Importation des modules nécessaire
Set-ExecutionPolicy RemoteSigned
Import-Module ActiveDirectory
Import-Module GroupPolicy
#### CREATION DES VARIABLES GLOBALES #####
clear-host
$oubase=Read-Host "Votre OU de BASE SVP ?"
$domaindns=Get-ADDomain|select -ExpandProperty distinguishedname
try {
New-ADOrganizationalUnit -Name $oubase -path $domaindns `
-ProtectedFromAccidentalDeletion $false -Verbose
} catch {}
$csv=import-csv ".\liste.csv" -delimiter ";" -Encoding UTF8
$cheminbase="OU="+$oubase+","+$domaindns
$chemingroupes="OU=GROUPES,"+$cheminbase
$cheminimprims="OU=IMPRIMANTES,"+$cheminbase
$cheminusers="OU=UTILISATEURS,"+$cheminbase
$cheminordis="OU=ORDINATEURS,"+$cheminbase
$dfspath=(get-dfsroot).path

function creation_ous()
{
    try{New-ADOrganizationalUnit -name "GROUPES" -Path $cheminbase `
-ProtectedFromAccidentalDeletion $false -Verbose}
    catch{}
    try{New-ADOrganizationalUnit -name "IMPRIMANTES" -Path $cheminbase `
-ProtectedFromAccidentalDeletion $false -Verbose}
    catch{}
    try{New-ADOrganizationalUnit -name "ORDINATEURS" -Path $cheminbase `
-ProtectedFromAccidentalDeletion $false -Verbose}
    catch{}
    try{New-ADOrganizationalUnit -name "UTILISATEURS" -Path $cheminbase `
-ProtectedFromAccidentalDeletion $false -Verbose}
    catch{}

    foreach ($i in $csv)
    { $ou=$i.service.toupper()
        try{
            New-ADOrganizationalUnit -name $ou -path $chemingroupes `
-ProtectedFromAccidentalDeletion $false -Verbose}
        catch{}
        try{
            New-ADOrganizationalUnit -name $ou -path $cheminimprims `
-ProtectedFromAccidentalDeletion $false -Verbose}
        catch{}
        try {New-ADOrganizationalUnit -name $ou -path $cheminordis `
-ProtectedFromAccidentalDeletion $false -Verbose}
        catch{}
        try{
            New-ADOrganizationalUnit -name $ou -path $cheminusers `
-ProtectedFromAccidentalDeletion $false -Verbose}
        catch{}
    }
}

#####
#### MENU GENERAL ####
#####
function menu()
{

write-Host "##### PROJET EVOLUTION
##### "
Write-Host
"##### "
#### "
Write-Host "##### Votre Choix SVP ?
##### "

```

```

Write-Host
#####
##### "
Write-Host "1 : Création Unités d'organisation"
Write-Host "2 : Création des groupes"
Write-Host "3 : Création des users"
Write-Host "4 : Suppression totale"
Write-Host "0 : Quitter le projet"
$choix=read-host "Choix ? "

    switch ($choix)
    {
        1 {creation_ous;menu}
        2 {creation_groupes;menu}
        3 {creation_users;menu}
        4 {suppression;menu}
        0 {exit}
        default {menu}
    }
}

##### GROUPES #####
function creation_groupes()
{
    foreach ($i in $csv)
    {
        $service=$i.service.ToUpper()
        $GG="GG_"+$service
        $GU="GU_"+$service
        $GDL_R="GDL_R_"+$service
        $GDL_RW="GDL_RW_"+$service
        $GDL_F="GDL_F_"+$service
        $chemingroup="OU="+$service+", "+$chemingroupes

try{New-ADGroup -Name $GG -path $chemingroup -GroupCategory Security -GroupScope
Global -Verbose}
catch{}
try{New-ADGroup -Name $GU -path $chemingroup -GroupCategory Security -GroupScope
Universal -Verbose}
catch{}
try{New-ADGroup -Name $GDL_R -path $chemingroup -GroupCategory Security -GroupScope
DomainLocal -Verbose}
catch{}
try{New-ADGroup -Name $GDL_RW -path $chemingroup -GroupCategory Security -GroupScope
DomainLocal -Verbose}
catch{}
try{New-ADGroup -Name $GDL_F -path $chemingroup -GroupCategory Security -GroupScope
DomainLocal -Verbose}
catch{}

Add-ADGroupMember $GU -Members $GG
Add-ADGroupMember $GDL_R -Members $GU
Add-ADGroupMember $GDL_RW -Members $GU
Add-ADGroupMember $GDL_F -Members $GU
    }
}

##### USERS #####
function creation_users()
{
    $pass=ConvertTo-SecureString("Angouleme1") -AsPlainText -Force

    foreach ($i in $csv)
    {
        $nom=$i.nom.ToUpper()
        $prenom=$i.prenom.substring(0,1).ToUpper()+$i.prenom.substring(1).ToLower()
        $nomcomplet=$nom+" "+$prenom
        $login=$prenom.ToLower()+"."+ $nom.ToLower()
        $upn=($login+"@"+$env:userdnsdomain).ToLower()
        $description=$i.description
        $fonction=$i.fonction
        $service=$i.service
    }
}

```

```

$chemin="OU="+$service+", "+$cheminusers
$groupe="GG_"+$service

new-aduser -name $nomcomplet -GivenName $prenom -Surname $nom `
-DisplayName $nomcomplet -SamAccountName $login -UserPrincipalName $upn `
-path $chemin -Department $service -Description $description `
-AccountPassword $pass -Title $fonction -ChangePasswordAtLogon $true `
-Enabled $true -EmailAddress $upn -Verbose

Add-ADGroupMember $groupe -Members $login
creation_dossiers($login,$service)
permissions
}

function creation_dossiers()
{
    $dossierperso=$dfspath+"\Perso\"
    $dossierservice=$dfspath+"\Services\"

    New-Item -name $login -ItemType Directory -path $dossierperso

try {
    New-Item -name $service -ItemType Directory -path $dossierservice
}
catch {
    write-host "Les dossiers "+$dossierservice + "Existe déjà"
}

function suppression()
{
Remove-ADOrganizationalUnit -Identity $chemin2 -Recursive -Confirm:$false -Verbose

$dossierperso=$dfspath+"\perso\"
$listeddossierperso=get-childitem -Directory -path $dossierperso
$dossierservice=$dfspath+"\services\"
$listeddossierservice=get-childitem -Directory -path $dossierservice

foreach ($i in $listeddossierperso)
{
    $nomdossier=$dossierperso+$i.name
    remove-item -Path $nomdossier -Recurse -Verbose
}
foreach ($i in $listeddossierservice)
{
    $nomdossierserv=$dossierservice+$i.name
    remove-item -Path $nomdossierserv -Recurse -Verbose
}
}

function permissions()
{
    $cheminperso=$dfspath+"\perso\"
    $cheminservice=$dfspath+"\services\"
    $listeddossierperso=Get-ChildItem -Directory -path $cheminperso
    $listeddossierservice=Get-ChildItem -Directory -path $cheminservice
    foreach ($dossier in $listeddossierperso)
    {
        $chemindossier=$dossier.fullname
        $acl=(get-item $chemindossier).GetAccessControl('Access')
        $username=$dossier.name
    $ar=new-object
    security.accesscontrol.filesystemAccessRule($username,'Modify','ContainerInherit,Objec
tInherit','none','Allow')
    $acl.SetAccessRule($ar)
    set-acl -Path $chemindossier -AclObject $acl
    }
    foreach ($dossier in $listeddossierservice)
    {
        $chemindossier=$dossier.fullname
        $acl=(get-item $chemindossier).GetAccessControl('Access')
        $gdl="GDL_RW_"+$dossier.name
    }
}

```

```

        $ar=new-object
security.accesscontrol.filesystemAccessRule($gdl,'Modify','ContainerInherit,ObjectInhe
rit','none','Allow')
        $acl.SetAccessRule($ar)
        set-acl -Path $chemindossier -Aclobject $acl
    }
}

##### CORPS DU PROGRAMME #####
menu

ect $acl
    }
}
function menu_principal()
{
    clear-host
    write-host "Script de création des objets Active Directory"
    write-host "1 : Creation des OUS"
    write-host "2 : Creation des Groupes"
    write-host "3 : Creation des Utilisateurs"
    write-host "4 : Suppression Totale"
    write-host "0 : Sortir du script"
    $choix=Read-Host "Saisir votre choix (entre 0 et 4):"
    switch ($choix)
    {
        1 {create_ous_base;menu_principal}
        2 {create_ous_groupes;menu_principal}
        3 {create_ous_utilisateurs;menu_principal}
        4 {suppression;menu_principal}
        0 {exit}
        default {menu_principal}
    }
}
##### PROGRAMME PRINCIPAL #####
menu_principal

```

Nous avons également d'autres scripts pour avertir la fin de session pour les personnes devant se déconnecter avant une heure précise par exemple :

```
shutdown -c "Fermeture de la session dans 5 minutes. Prenez le temps
d'enregistrer tous vos documents !" /s /t 300
```

C. Devis

Invoice

Vestigio

310 Avenue Gustave Eiffel
05 57 56 55 54, contact@vestigio.com

Date: 08/21/2018
Invoice No.: 123455
Due Date: 09/20/2018
Customer PO No.:332546

Bill To:

Vestigio
310 Avenue Gustave Eiffel,
33600 PESSAC

Qty	Item	Description	Unit Price	TAX %	VAT	Total
2	Licence Windows Server 2016	Windows Server 2016	€5,390.00	0%	€0.00	€10,780.00
2	HPE ProLiant DL380 Gen9 - Xeon E5-2620V4 2.1 GHz - 16 Go - 0 Go	Serveur	€2,125.32	0%	€0.00	€4,250.64
2	Veeam Backup & Replication 9.5. STANDARD	Logiciel de sauvegarde	€652.50	0%	€0.00	€1,305.00
2	Licence VMWare ESX Support 3ans	Licence hyperviseur	€2,093.66	0%	€0.00	€4,187.32
1	Licence TeamViewer Corporate	Prise en main à distance, prix sur 1 an (abonnement mensuel)	€1,298.80	0%	€0.00	€1,298.80

Total €21,821.76
Balance Due €21,821.76

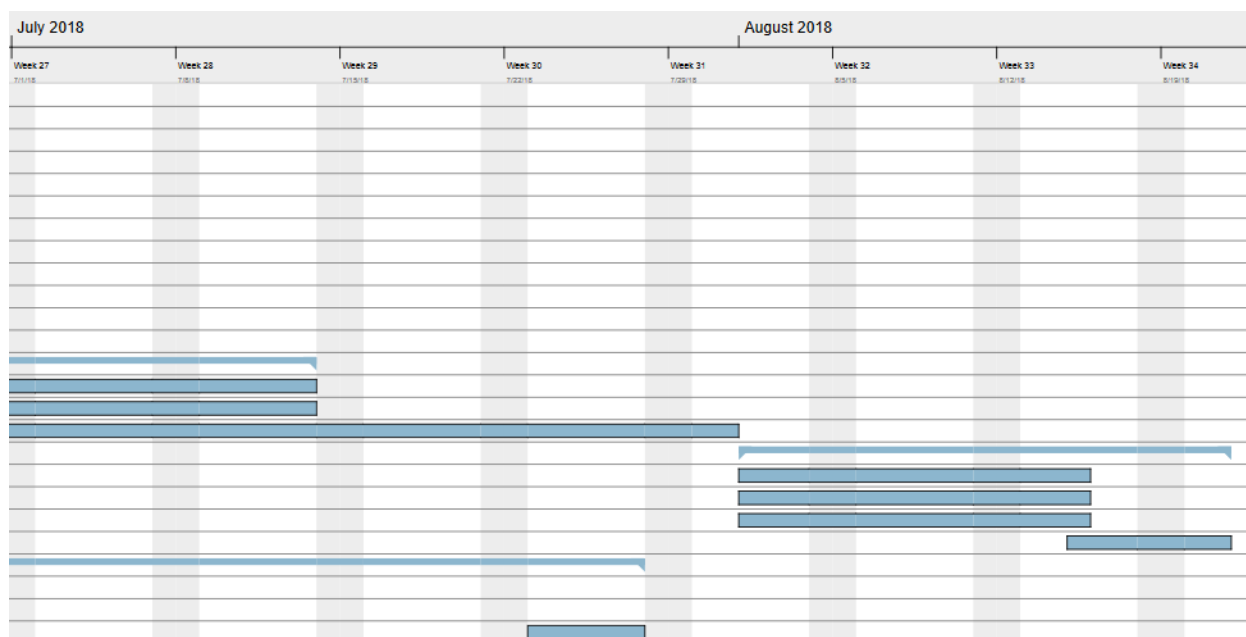
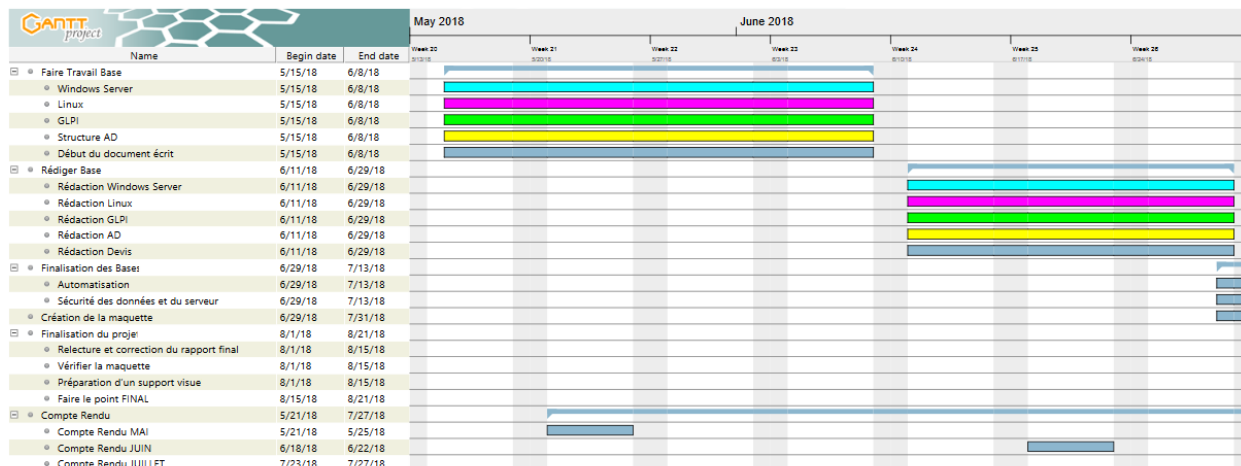
Please contact us for more information about payment options.

Thank you for your business.

D. Planning

Projet Evolution

Gantt Chart



E. Lexique

DFS : Distributed File System : ensemble de services client et serveur permettant de rassembler des partages de fichier à un endroit unique de façon transparente, d'assurer une redondance et disponibilité des données grâce à la réplication et de fournir une arborescence logique aux données depuis des emplacements différents.

DHCP : Dynamic Host Configuration Protocol (en français, protocole de configuration dynamique des hôtes) protocole réseau qui assure la configuration automatique du paramétrage IP d'une machine. (Attribution d'adresse IP, masque de sous-réseau, passerelle par défaut, serveurs de noms NDS etc...)

FTP : File Transfer Protocol (protocole de transfert de fichier). Protocole de communication sur un réseau TCP/IP permettant l'échange, la modification ou même la suppression de fichiers depuis un ordinateur vers un autre du même réseau.

GPO : Group Policy Object (en français, Stratégie de Groupe). Fonction de gestion des ordinateurs et utilisateurs dans un environnement Active Directory sous Microsoft Windows. Elles permettent aux entreprises de restreindre aux utilisateurs des actions présentant un risque potentiel (accès au panneau de configuration) ou d'assurer la configuration automatique des profils utilisateurs (ex : déploiement automatique d'un logiciel)

NFS : Network File System (en français système de fichiers réseau). Système de partage de fichiers en réseau principalement entre systèmes Linux.

Script : Programmation permettant de manipuler les fonctions d'un système informatique à travers un langage. Ils sont exécutés à partir de fichier contenant le code d'un programme qui sera ainsi interprété. Dans le cadre de notre projet, les scripts réalisés ont été produits sous l'utilitaire Windows Powershell pour pallier les soucis d'automatisation des tâches.