



2019/2020

Documentation projet UF Active Directory

Baptiste ESTELA / Kévin SAUMADE/David
SOARES CAETANO
YNOV Aix en Provence

Table des matières



I.	Introduction :	I
II.	Convention de nommage :	I
III.	Structure du réseau :	2
IV.	Stratégies de groupes :	4
V.	Serveur de fichier :	7
VI.	Sauvegarde Windows.....	10
VII.	Mise en place de la réplication DFS :	11

I. Introduction :

Pour la réalisation de notre projet nous avons choisis de nous tourner vers des serveurs Windows 2016 pour ce qui est des deux active directory ainsi que du serveur de backup, et pour ce qui est des serveurs Linux nous avons optés pour de l'Ubuntu 18.04 (mise à jour ultérieurement)

2 contrôleurs de domaine seront donc installés afin de maintenir le service d'annuaire dans le SI de GSB.







Nos contrôleurs de domaine sont donc des machines virtuelles :

-  GSB-SRV-AD1 172.16.0.1
-  GSB-SRV-AD2 172.16.0.2

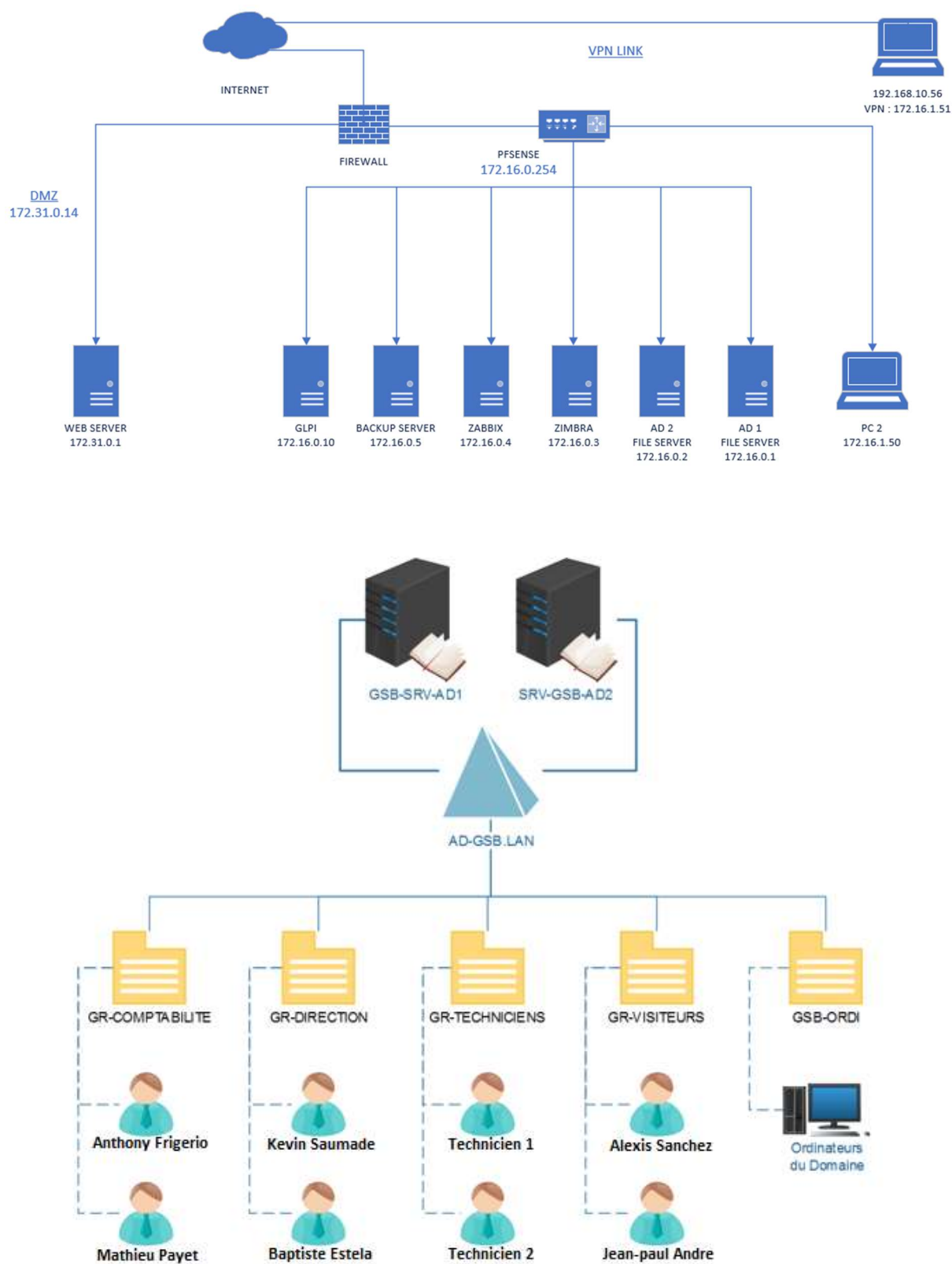
II. Convention de nommage :

Notre convention de nommage pour la structure GSB sera GSB.LAN.

Nous avons donc choisi les conventions suivantes :

-  Pour le nom NETBIOS des serveurs :
Nom de l'entreprise - SRV- Rôle du serveur ex : « GSB-SRV-AD 1 »
-  Pour le nom NETBIOS des postes clients :
Nom de l'entreprise - client -chiffre du système d'exploitation ex : « GSB-CLIENT-WIN10 »
-  Pour les utilisateurs :
 - Prénom.Nom :
 - Pour le service direction : kevin.saumade et Baptiste.estela
 - Pour le service visiteurs : alexis.sanchez et jean-paul.andre
 - Pour le service comptabilité : anthony.frigerio et mathieu.payet
-  Pour les administrateurs linux :
 - admingsb
-  Pour les groupes :
 - Nom du service :
 - GR_COMPTABILITE
 - GR_DIRECTION
 - Gr_VISITEURS
-  Pour les mots de passes :
Etant donné que l'infrastructure présente est une maquette tous les mots de passe Windows sont : Formation13@ et les mots de passe linux sont GSB

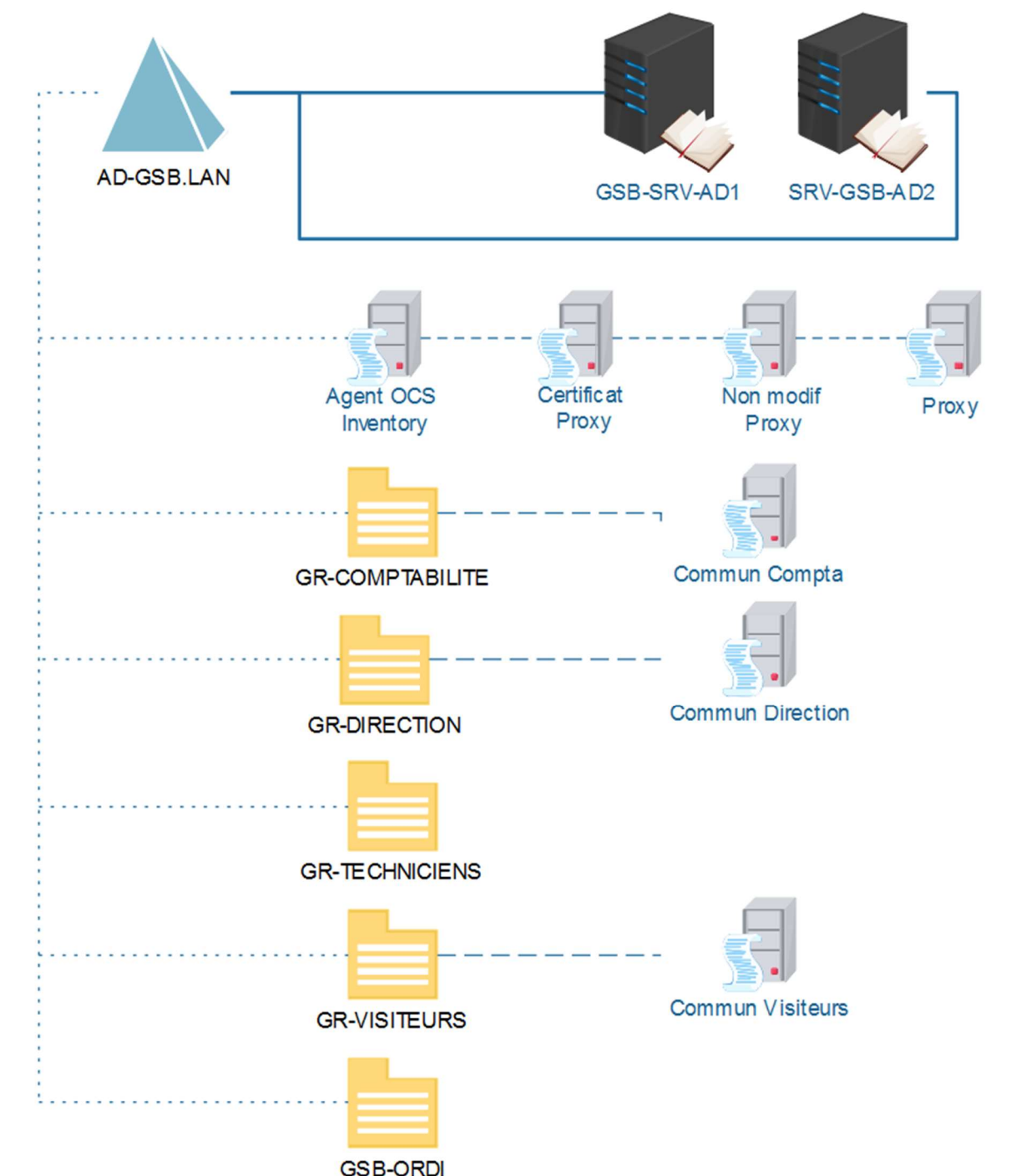
III. Structure du réseau :



Ci-dessous une capture d'écran de l'arborescence des UO du domaine :

Utilisateurs et ordinateurs Active Directory [GSB-SRV-AD1.GSB.LAN]																																									
<ul style="list-style-type: none"> Requêtes enregistrées GSB.LAN <ul style="list-style-type: none"> Builtin Computers Domain Controllers ForeignSecurityPrincipals GR_COMPTABILITE GR_DIRECTION GR_TECHNICIENS GR_VISITEURS GSB_ORDI LostAndFound Managed Service Accounts Microsoft Exchange Security Groups Program Data System Users Microsoft Exchange System Objects NTDS Quotas TPM Devices 	<table> <tr> <th>Nom</th><th>Type</th></tr> <tr><td>Builtin</td><td>builtinDomain</td></tr> <tr><td>Computers</td><td>Conteneur</td></tr> <tr><td>Domain Controllers</td><td>Unité d'organisation</td></tr> <tr><td>ForeignSecurityPrincipals</td><td>Conteneur</td></tr> <tr><td>GR_COMPTABILITE</td><td>Unité d'organisation</td></tr> <tr><td>GR_DIRECTION</td><td>Unité d'organisation</td></tr> <tr><td>GR_TECHNICIENS</td><td>Unité d'organisation</td></tr> <tr><td>GR_VISITEURS</td><td>Unité d'organisation</td></tr> <tr><td>GSB_ORDI</td><td>Unité d'organisation</td></tr> <tr><td>LostAndFound</td><td>lostAndFound</td></tr> <tr><td>Managed Service Accounts</td><td>Conteneur</td></tr> <tr><td>Microsoft Exchange Security Groups</td><td>Unité d'organisation</td></tr> <tr><td>Program Data</td><td>Conteneur</td></tr> <tr><td>System</td><td>Conteneur</td></tr> <tr><td>Users</td><td>Conteneur</td></tr> <tr><td>Microsoft Exchange System Objects</td><td>msExchSystemObjectsContainer</td></tr> <tr><td>NTDS Quotas</td><td>msDS-QuotaContainer</td></tr> <tr><td>TPM Devices</td><td>msTPM-InformationObjectsContainer</td></tr> <tr><td>Infrastructure</td><td>infrastructureUpdate</td></tr> </table>	Nom	Type	Builtin	builtinDomain	Computers	Conteneur	Domain Controllers	Unité d'organisation	ForeignSecurityPrincipals	Conteneur	GR_COMPTABILITE	Unité d'organisation	GR_DIRECTION	Unité d'organisation	GR_TECHNICIENS	Unité d'organisation	GR_VISITEURS	Unité d'organisation	GSB_ORDI	Unité d'organisation	LostAndFound	lostAndFound	Managed Service Accounts	Conteneur	Microsoft Exchange Security Groups	Unité d'organisation	Program Data	Conteneur	System	Conteneur	Users	Conteneur	Microsoft Exchange System Objects	msExchSystemObjectsContainer	NTDS Quotas	msDS-QuotaContainer	TPM Devices	msTPM-InformationObjectsContainer	Infrastructure	infrastructureUpdate
Nom	Type																																								
Builtin	builtinDomain																																								
Computers	Conteneur																																								
Domain Controllers	Unité d'organisation																																								
ForeignSecurityPrincipals	Conteneur																																								
GR_COMPTABILITE	Unité d'organisation																																								
GR_DIRECTION	Unité d'organisation																																								
GR_TECHNICIENS	Unité d'organisation																																								
GR_VISITEURS	Unité d'organisation																																								
GSB_ORDI	Unité d'organisation																																								
LostAndFound	lostAndFound																																								
Managed Service Accounts	Conteneur																																								
Microsoft Exchange Security Groups	Unité d'organisation																																								
Program Data	Conteneur																																								
System	Conteneur																																								
Users	Conteneur																																								
Microsoft Exchange System Objects	msExchSystemObjectsContainer																																								
NTDS Quotas	msDS-QuotaContainer																																								
TPM Devices	msTPM-InformationObjectsContainer																																								
Infrastructure	infrastructureUpdate																																								

IV. Stratégies de groupes :

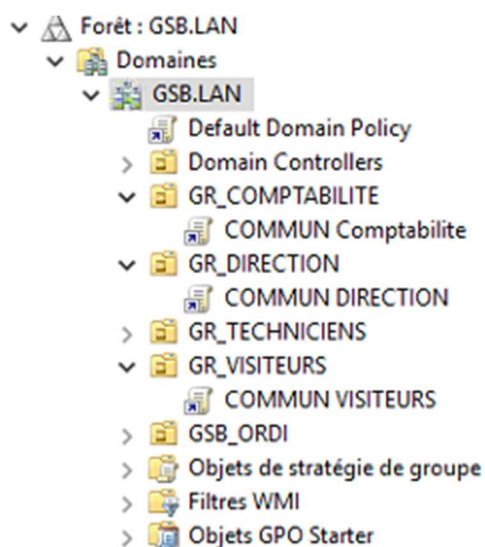


Des GPO sont mises en place afin d'automatiser certaines tâches ou d'interdire l'accès à certaines fonctionnalités.

Nous avons donc mis en place :

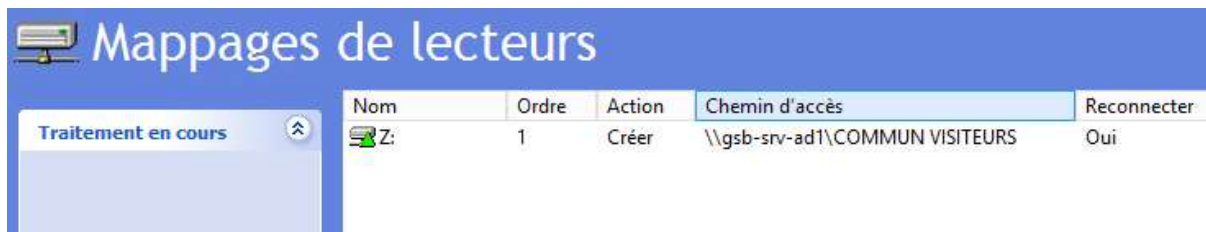
- Des GPO de mappage de lecteur pour les visiteurs, les comptables et les directeurs.

Ci-dessus on peut voir les différentes GPO listées conformément au cahier des charges.



Concernant les GPO en rapport avec le serveur de fichier et ses accès nous avons créé une GPO pour chaque groupe utilisant ce serveur à savoir le groupe visiteurs, le groupe comptable et le groupe direction (le groupe technicien concerne la partie supervision et tickets GLPI, il sera donc évoqué plus tard dans la documentation en rapport).

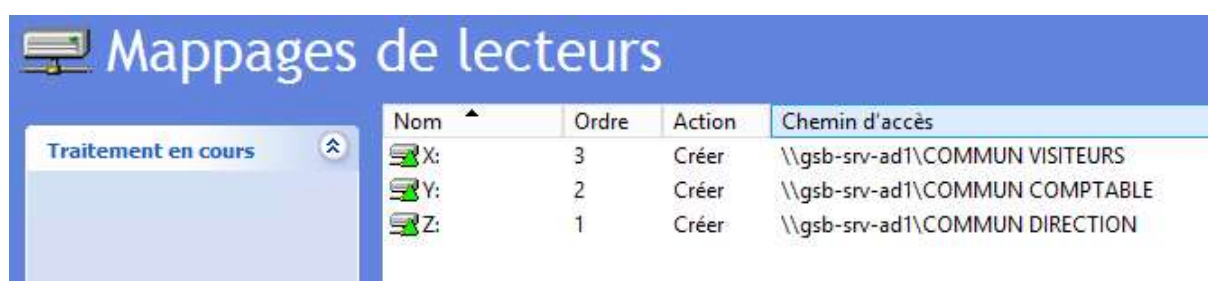
Le groupe visiteurs doit pouvoir avoir accès à un dossier COMMUN VISITEURS mappé par GPO et ne voir que le dossier commun des visiteurs :



Le groupe comptable doit pouvoir avoir un accès à un dossier COMMUN COMPTABLE mappé par GPO et ne voir que le dossier commun des comptable et visiteurs :



Le groupe direction doit pouvoir quant à lui avoir un accès au dossier COMMUN DIRECTION mappé par GPO et voir tous les autres COMMUN :

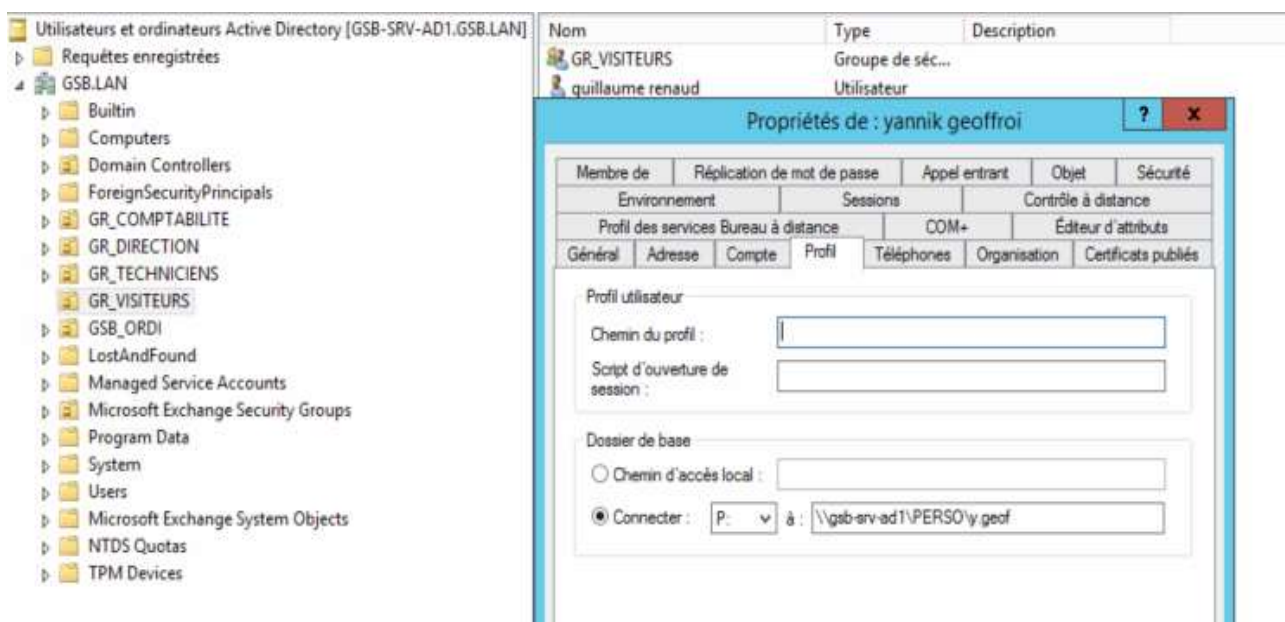


V. Serveur de fichier :

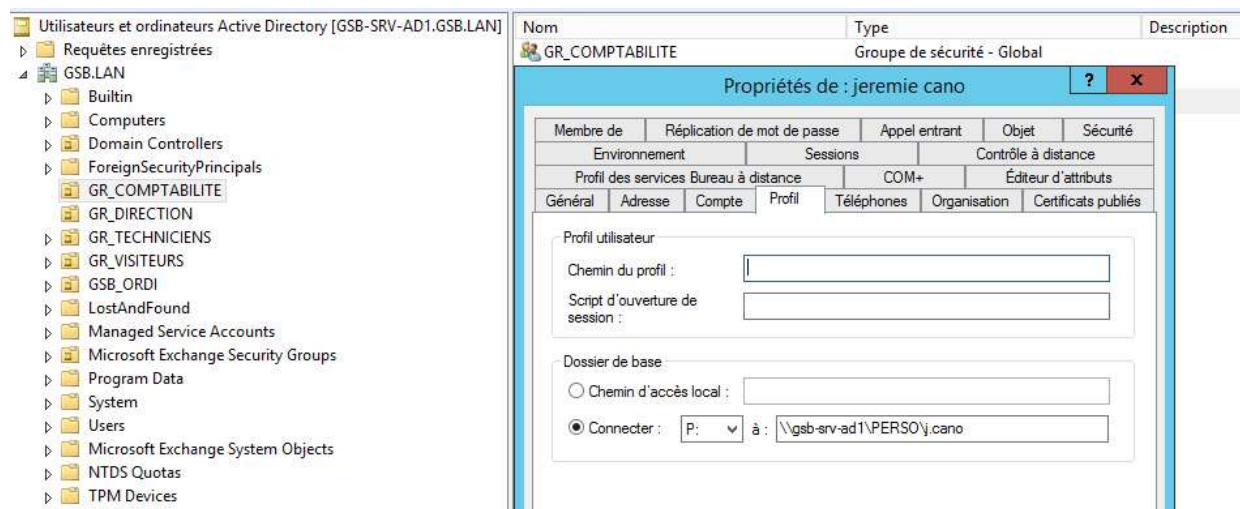
Pour le serveur de fichier le cahier des charges nous demande d'intégrer un disque dur (ou un serveur) supplémentaire qui permettra de créer des partages réseaux entre les différents services de l'entreprise.

Pour répondre à ce besoin nous avons donc ajouté un disque dur que l'on a intégré à nos SRV-AD1 et SRV-AD2 pour une redondance assurée par rôle DFS assurant une réplication des données.

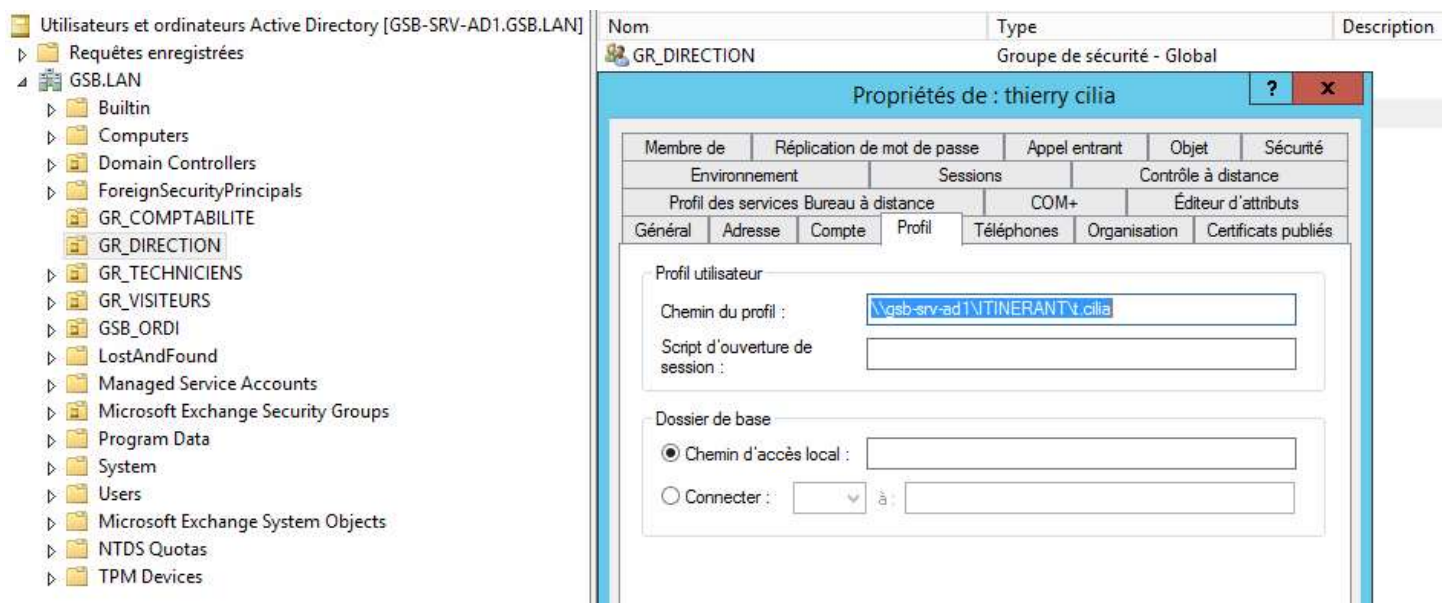
- Les visiteurs doivent avoir un dossier personnel nous avons donc utilisé pour le dossier personnel la fonction dossier de base sur la fiche de l'utilisateur. Seul le propriétaire pourra alors y accéder et modifier, ajouter ou supprimer ce dont il a besoin.



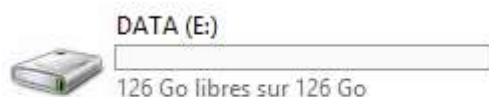
- Les comptables doivent avoir un dossier personnel nous avons donc utilisé pour le dossier personnel la fonction dossier de base sur la fiche de l'utilisateur. Seul le propriétaire pourra alors y accéder et modifier, ajouter ou supprimer ce dont il a besoin.



- Les directeurs doivent à la différence des autres services, avoir un profil itinérant ce qui signifie que lorsqu'il se connecteront avec leur session sur un poste client par exemple du domaine, ils retrouveront leur bureau ce qui leur permettra de travail plus simplement. Pour cela nous avons utilisé la fonction profil itinérant dans les propriétés du profil des directeurs.



Architecture du serveur de fichiers :



Le lecteur E est le disque dur faisant office de serveur de fichier, il contient les dossiers ci-dessous :

ITINERANT	06/10/2017 16:24	Dossier de fichiers
PARTAGES	06/10/2017 15:11	Dossier de fichiers
PERSO	06/10/2017 15:55	Dossier de fichiers

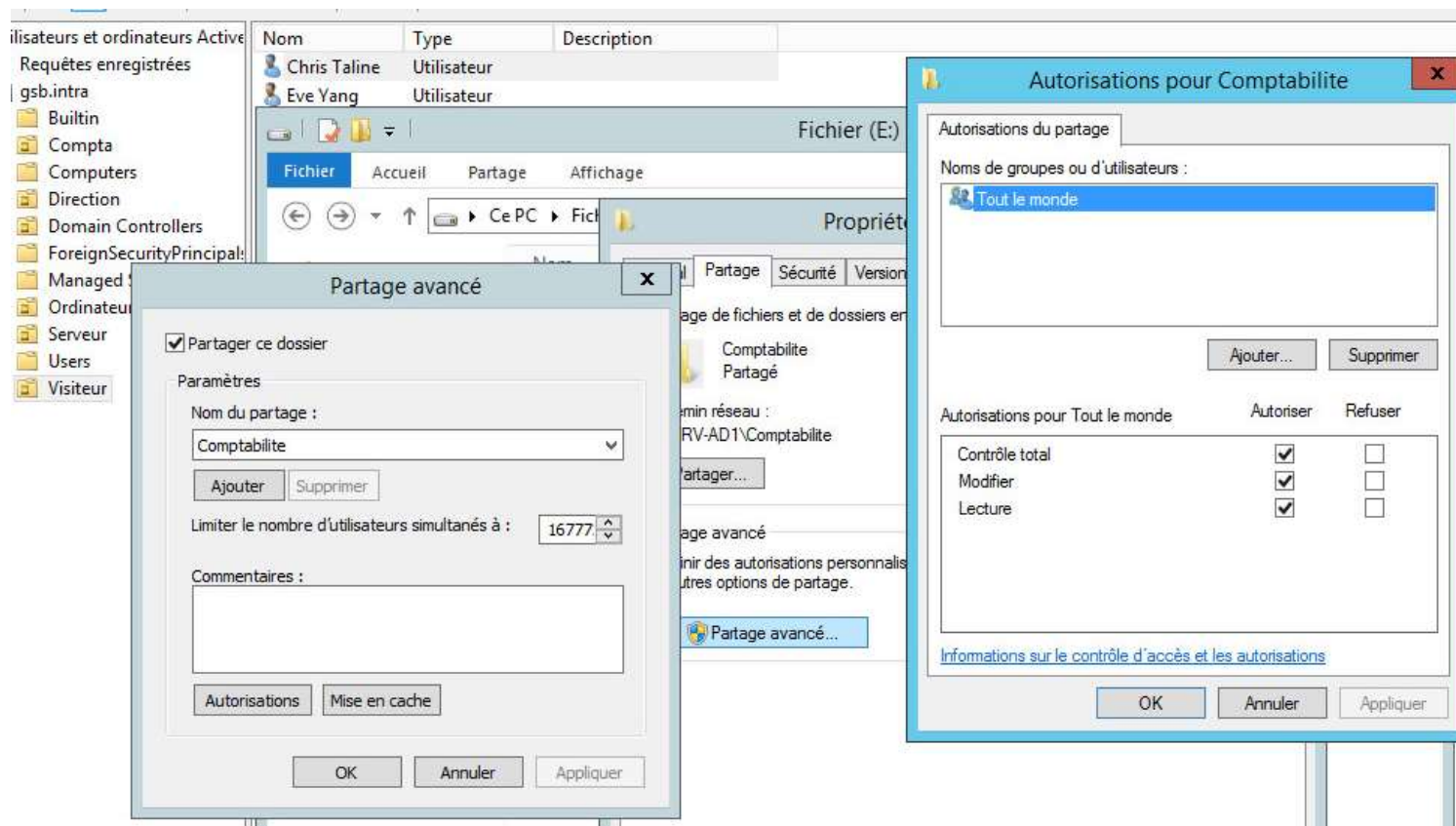
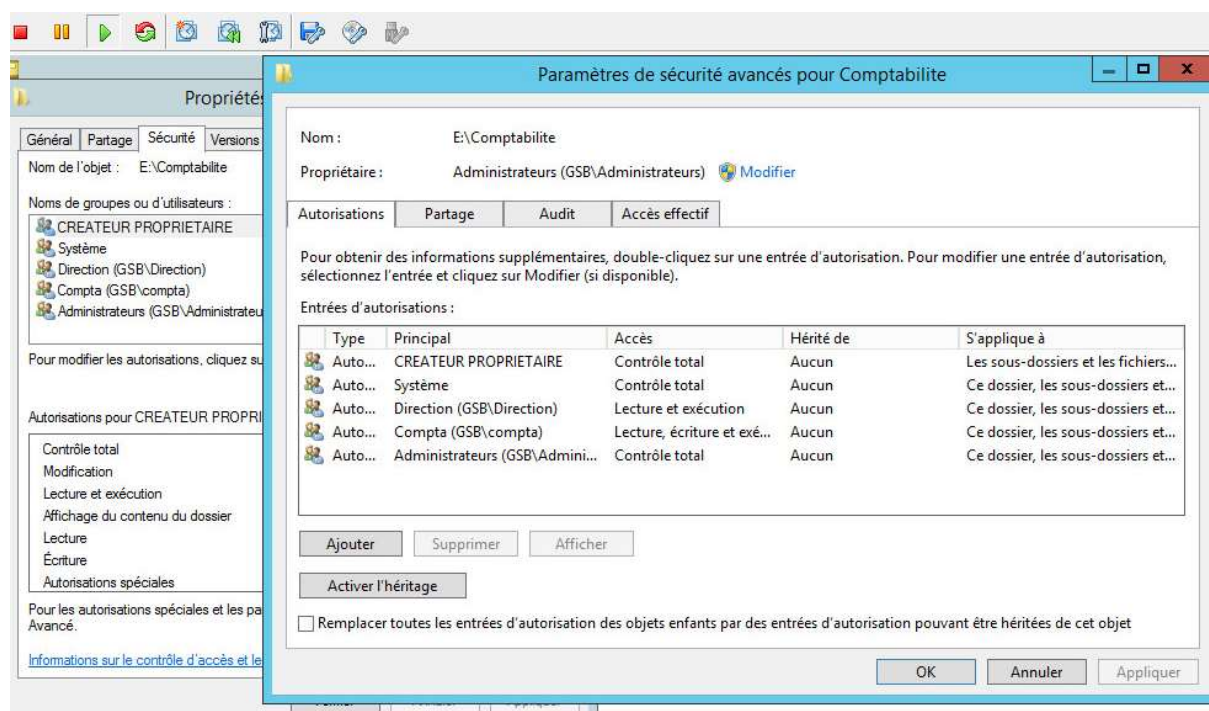
Le dossier PARTAGES contient les dossiers ci-dessous à savoir les COMMUN de chaque services :

COMMUN COMPTABLE	06/10/2017 16:11	Dossier de fichiers
COMMUN DIRECTION	06/10/2017 15:11	Dossier de fichiers
COMMUN VISITEURS	06/10/2017 16:59	Dossier de fichiers

Les dossiers ITINERANT et PERSO contiennent les dossier des utilisateurs bénéficiant d'un profils itinérant (les directeurs) et de les visiteurs / comptables qui eux on leur dossier personnel à leur nom.

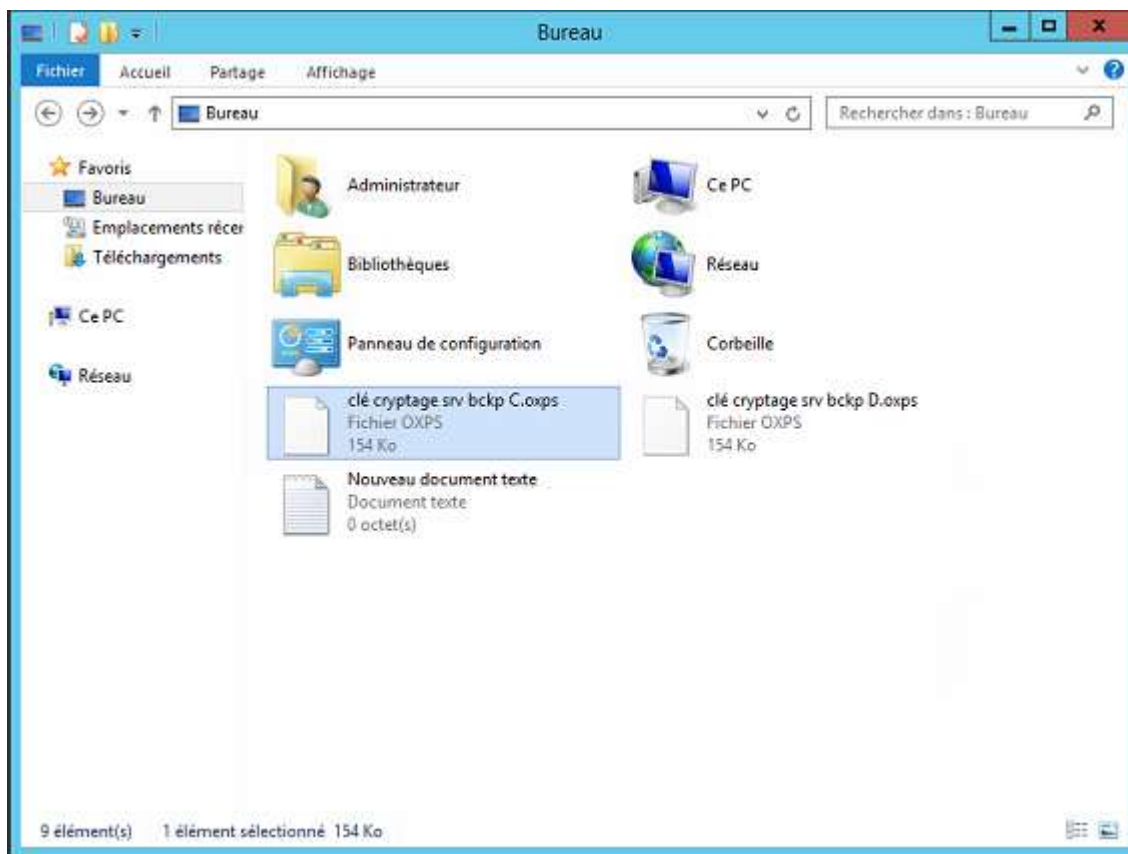
Droits et partages :

Nous avons commencé par établir un partage total sur tous les dossiers pour ensuite y établir des règles de sécurité (ajouts de droits, désactivation de l'héritage) c'est à ce moment-là que nous avons donné les droits d'accès en fonction des exigences du cahier des charges évoqué plus haut.



VI. Sauvegarde Windows

Nous avons mis en place également un Serveur de Backup GSB-SRV-BCKP, Ce serveur nous permet de copier l'intégralité de GSB-SRV-ADI (Disque C et le Disque DATA). Protégé par des clefs de cryptage :

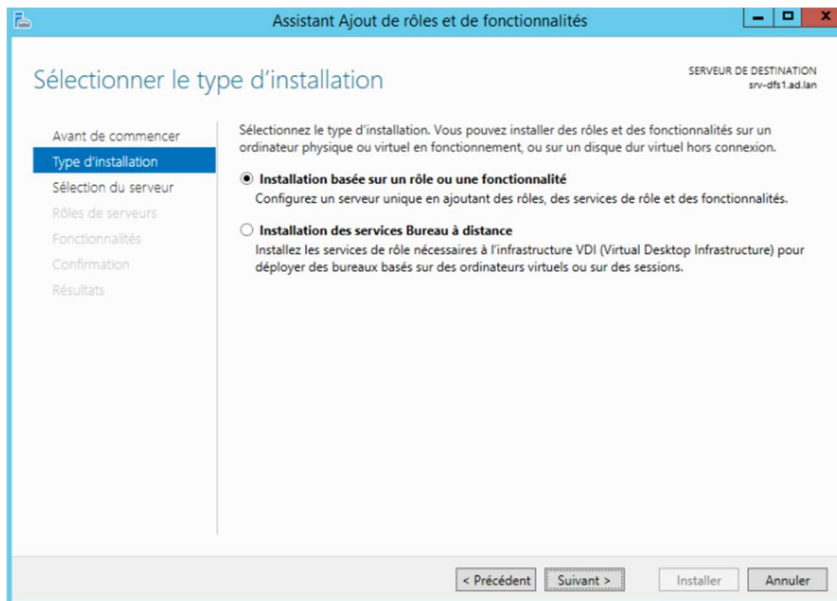
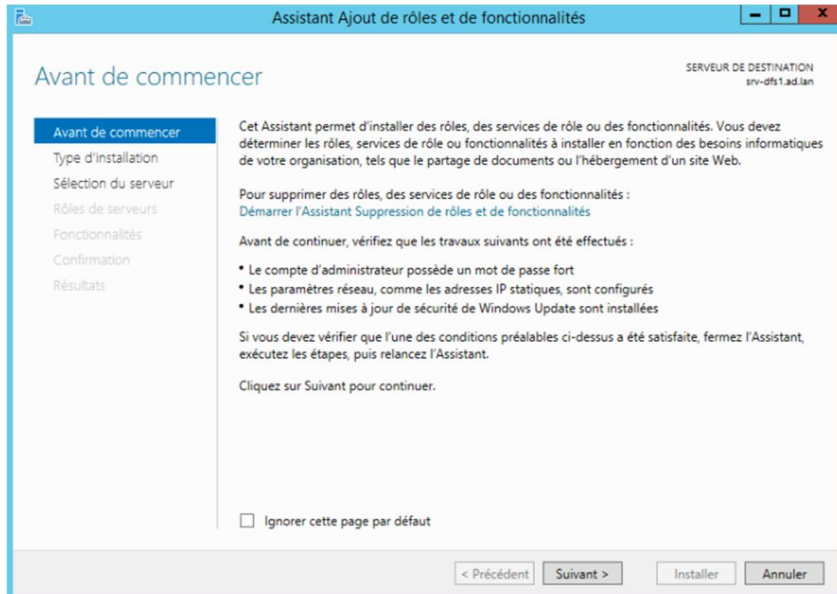


Numéro	Disque virt...	État	Capacité	Non alloué	Partition	Lecture se...	En cluster	Sous-systè...	Type de...	Nom
SRV-GSB-BCKP (2)										
0		En ligne	127 Go	0,00 O	GPT				SAS	Disque virtuel Microsoft
1		En ligne	127 Go	0,00 O	GPT				SAS	Disque virtuel Microsoft

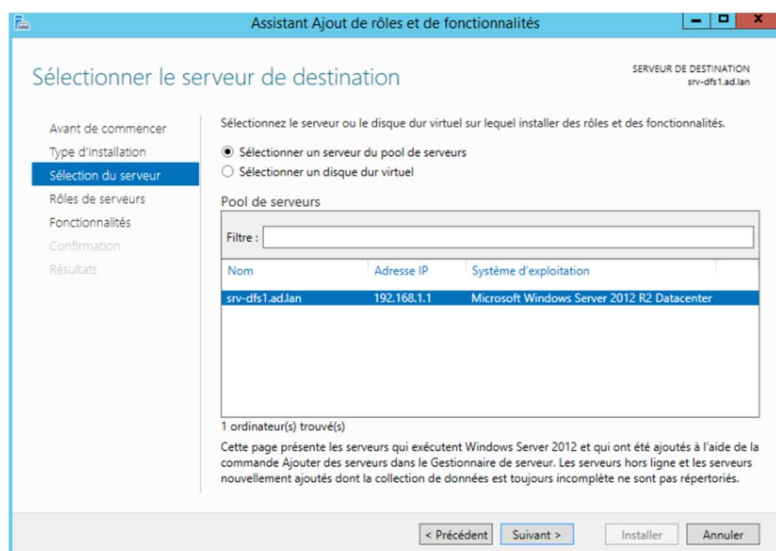
Pour le cryptage nous avons utilisé BitLocker qui permet le chiffrement de partition et prend en charge le chiffrement XTS-AES en 128 et 256 bits.

VII. Mise en place de la réplication DFS :

Donc il faut commencer par installer le rôle DFS sur chaque serveur participant (donc pour nous DC1 et DC2) la réplication. C'est en fait un sous rôle (service de rôle) du service de fichier.

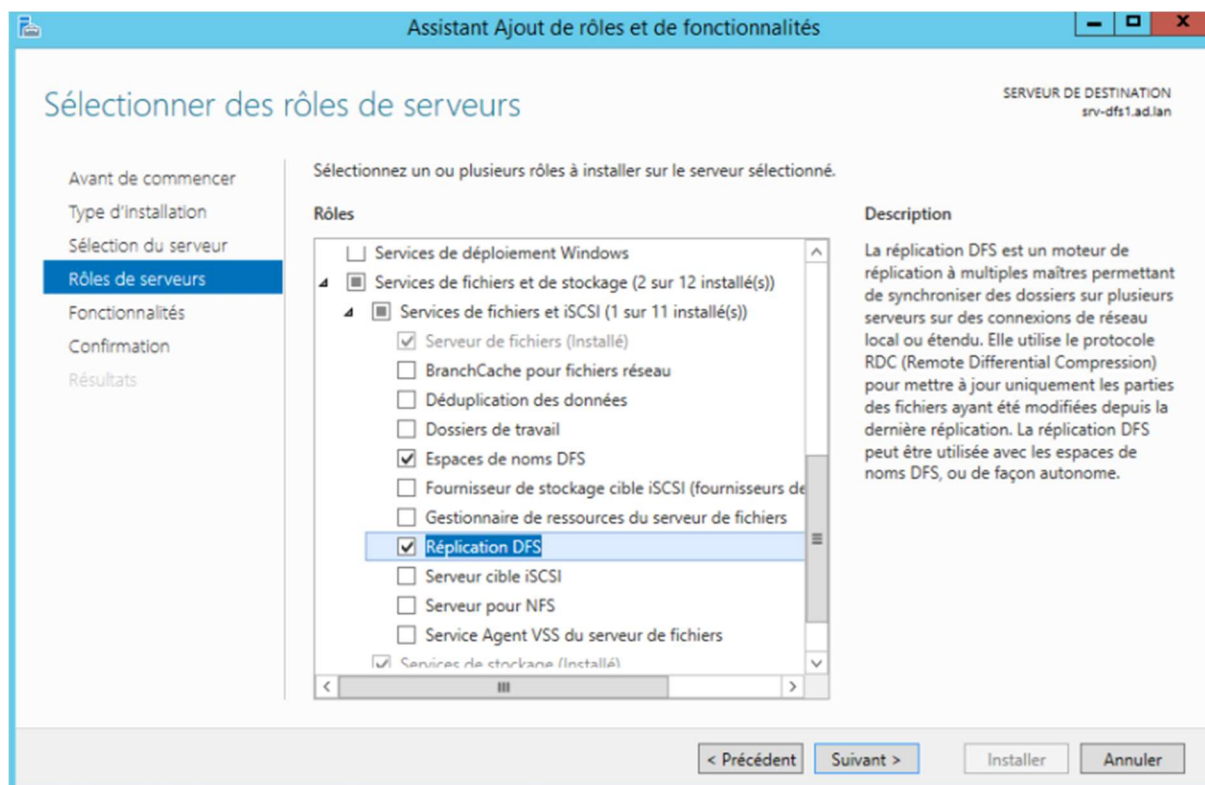


Mise en place de l'Annuaire, Serveur de fichier, Sauvegarde Windows (DFS), Service DNS,



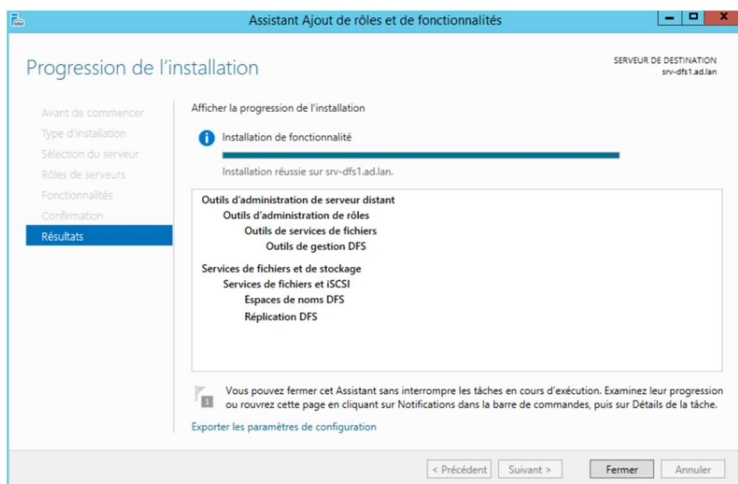
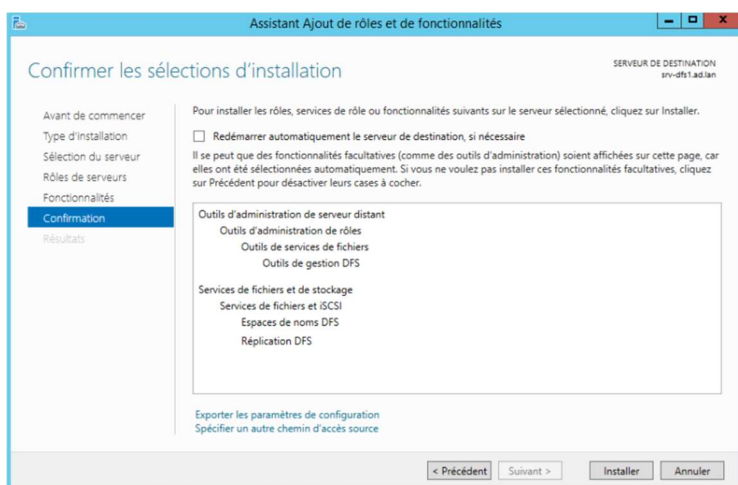
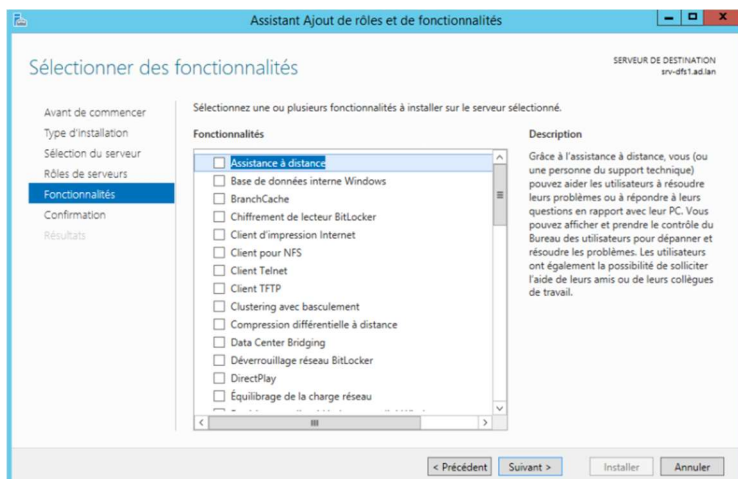
On choisit donc le service de rôle « **Réplication DFS** ».

Attention, l'espace de nom DFS permet de créer des racines DFS dans un domaine, ce qui permet de simplifier l'accès aux partages réseaux. Il n'est plus nécessaire alors de taper le chemin UNC de chaque serveur hébergeant les partages. Il suffit de taper le nom du domaine et on accède alors à tous les partages publiés dans la racine.

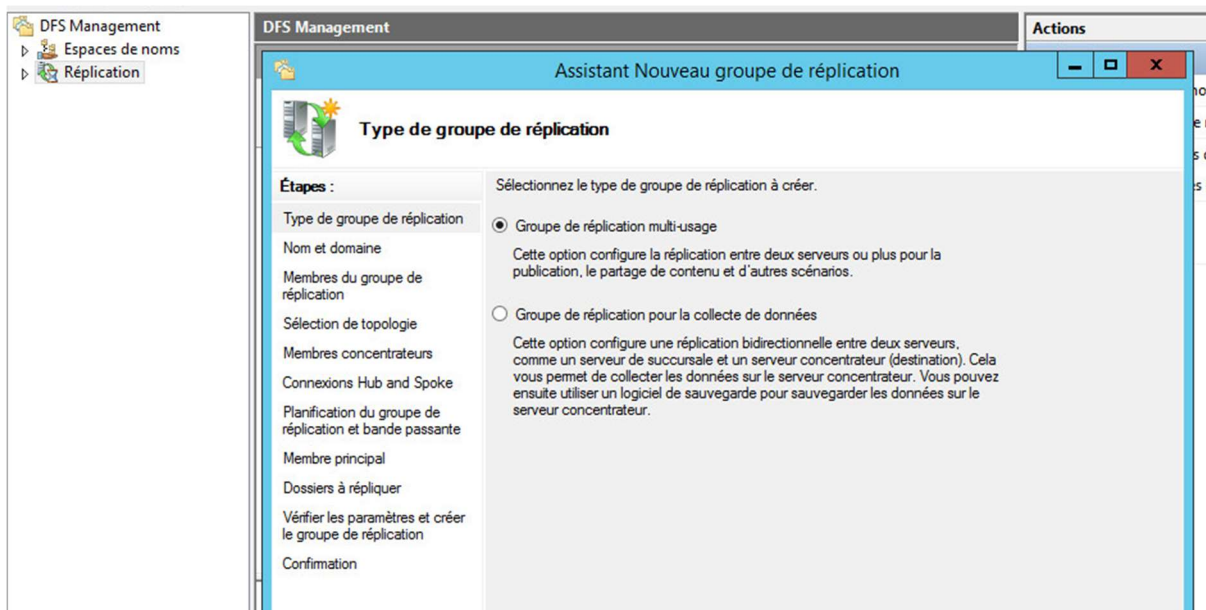


Mise en place de l'Annuaire, Serveur de fichier, Sauvegarde Windows (DFS), Service DNS,

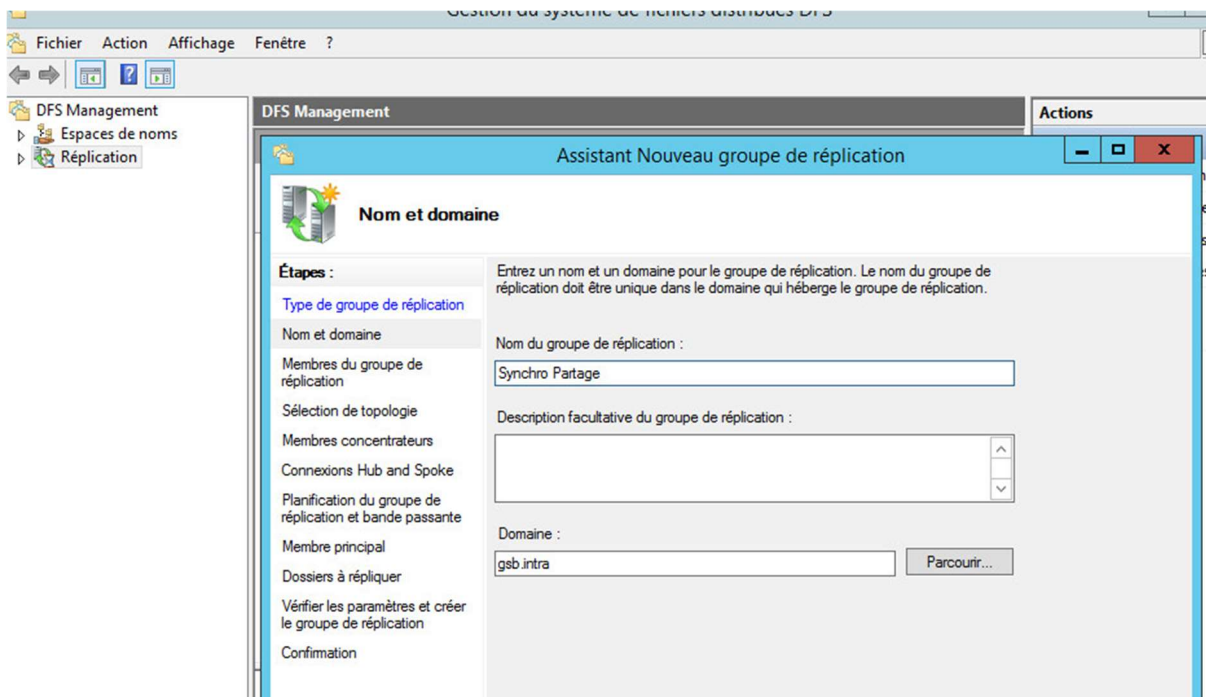
Pas besoin de sélectionner de fonctionnalités, l'installation peut se lancer.



Une fois le service installé, on peut accéder à la console « **DFS management** » à partir des rôles, clic de droite sur « **nouveau groupe de réplication** », Sélectionner un groupe de réplication multi usage.



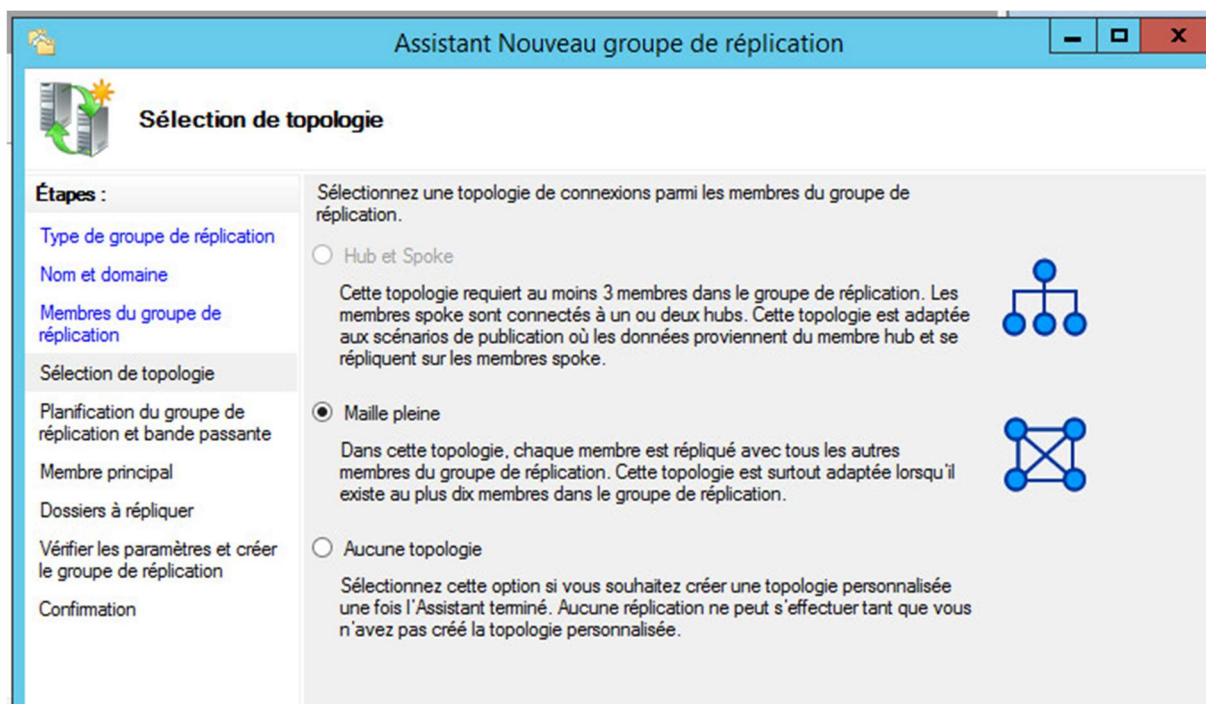
Donner un nom au groupe de réplication.



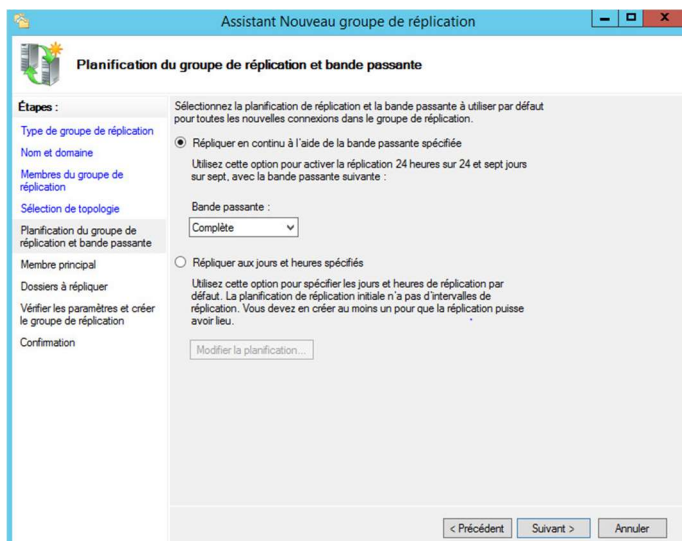
Ajouter tous les serveurs concernés par la réplication. Dans mon cas ce sont mes deux AD.



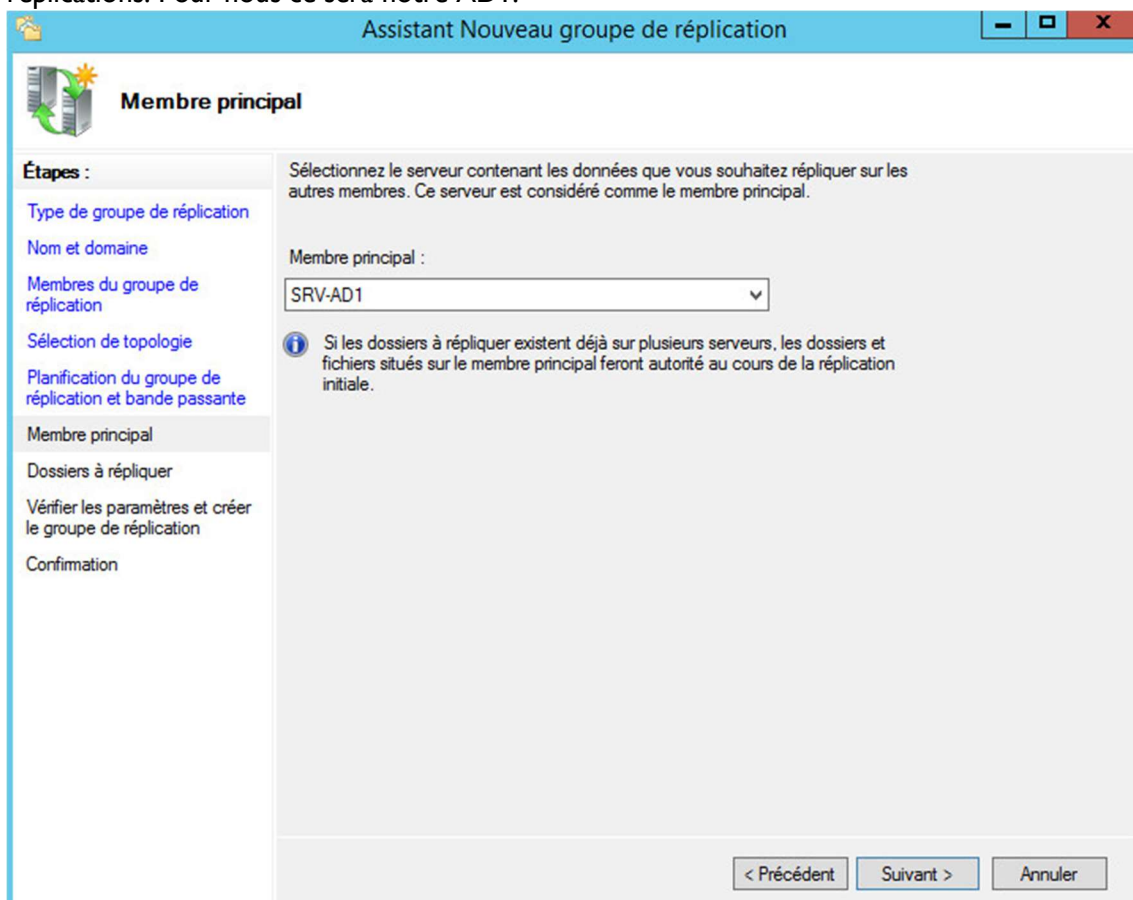
Sélectionner une topologie en maille pleine, ce qui permettra à mon dossier de partage de mon AD1 de se synchroniser avec celui de mon AD2 et inversement.



Ici, on peut régler les fréquences de réplication et limiter la bande passante de celle-ci. Pour nos tests nous laisserons « complète ».



La prochaine étape consiste à définir un membre principal de réplication. C'est à partir de lui que la première réplication va se faire vers les autres serveurs. Ensuite, le principe de la maille pleine fait que, peu importe le serveur qui va être modifié, la réplication se fera sur tous les partenaires de réplications. Pour nous ce sera notre ADI.



Mise en place de l'Annuaire, Serveur de fichier, Sauvegarde Windows (DFS), Service DNS,

Il faut ensuite sélectionner le dossier qui devra être répliqué.

The screenshot shows the 'Assistant Nouveau groupe de réplication' window at the 'Dossiers à répliquer' step. The left sidebar lists the steps: Type de groupe de réplication, Nom et domaine, Membres du groupe de réplication, Sélection de topologie, Planification du groupe de réplication et bande passante, Membre principal, Dossiers à répliquer (selected), Chemin d'accès local de E sur les autres membres, Vérifier les paramètres et créer le groupe de réplication, and Confirmation. The main area contains instructions: 'Cliquez sur Ajouter pour sélectionner un dossier du membre principal que vous souhaitez répliquer sur les autres membres du groupe de réplication.' Below this is a table titled 'Dossiers répliqués :'. The table has three columns: 'Chemin d'accès local', 'Nom du dossier répliqué', and 'Autorisations NT...'. One row is visible with 'E:\' in the first column, 'E' in the second, and 'Utiliser les autori...' in the third. At the bottom of the table are buttons 'Ajouter...', 'Modifier...', and 'Supprimer'. At the bottom of the window are buttons '< Précédent', 'Suivant >', and 'Annuler'.

Chemin d'accès local	Nom du dossier répliqué	Autorisations NT...
E:\	E	Utiliser les autori...

Il faut également sélectionner le deuxième serveur et stipuler également le dossier qui partagera la réplication avec le serveur principal. C'est donc le même dossier.

The screenshot shows the 'Assistant Nouveau groupe de réplication' window at the 'Chemin d'accès local de E sur les autres membres' step. The left sidebar is the same as the previous screenshot, with 'Chemin d'accès local de E sur les autres membres' selected. The main area contains instructions: 'Pour spécifier le chemin d'accès local du dossier répliqué ou l'état de lecture seule du dossier, sélectionnez le membre approprié, puis cliquez sur Modifier.' Below this is a table titled 'Détails du membre :'. The table has three columns: 'Membre', 'Chemin d'accès local', and 'Statut de l'appar...'. One row is visible with 'SRV-AD2' in the first column, '<Non défini>' in the second, and 'Désactivé' in the third. Below the table is a 'Modifier...' button. At the bottom of the window are buttons '< Précédent', 'Suivant >', and 'Annuler'.

Membre	Chemin d'accès local	Statut de l'appar...
SRV-AD2	<Non défini>	Désactivé