Procédure et documentation technique  
WINDOWS SERVEUR 2012 R2

# https://s1.qwant.com/thumbr/0x0/b/1/692fa2c8c38d8af7b7d8ffd57fbd86/b_1_q_0_p_0.jpg?u=http%3A%2F%2Flabs.supinfochina.com%2Fwp-content%2Fuploads%2F2014%2F08%2Fwindows-server-2012.jpg&q=0&b=1&p=0&a=1

TABLE DES MATIERES

DHCP…………………………………………………………..10

DFS……………………………………………………………..20

NPS RADIUS………………………………………………..25

TSE ……………………………………………………………..27

Groupes et Utilisateurs………………………………..60

GPO…………………………………………………………….65

Redondance………………………………………………..67

AD/DNS………………………………………………………67

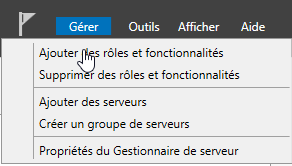
DHCP Failover……………………………………………..70

Radius…………………………………………………………72

DFS/DFSR…………………………………………………….73

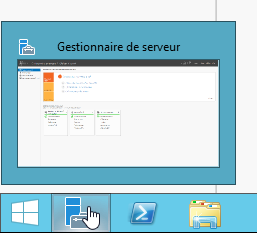
SERVEUR MAIL………………………………………….80

# Active Directory

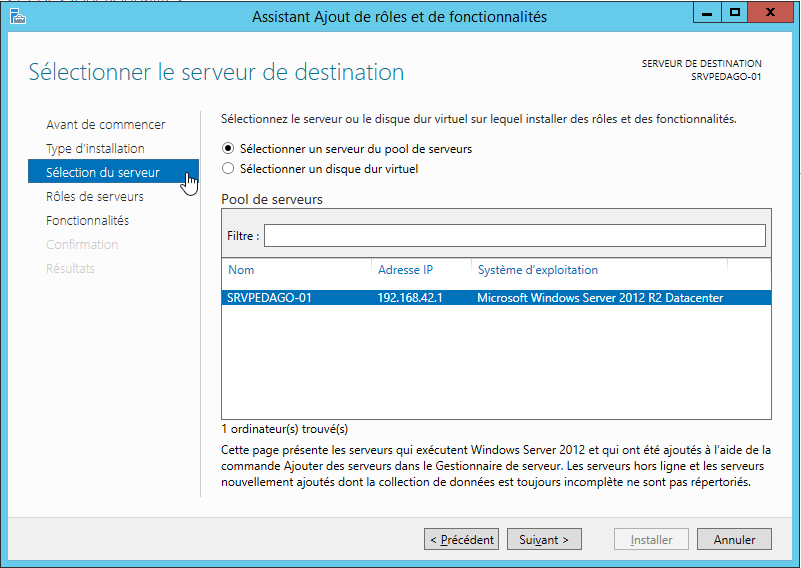


Sous **WINDOWS SERVER 2012 R2**, l’ajout de rôle ce fait via le menu *« Gérer », « Ajouter des rôles et des fonctionnalités »*.

Ce menu est disponible via l’application présente dans la barre de tâche : *« Gestionnaire de serveur »*.

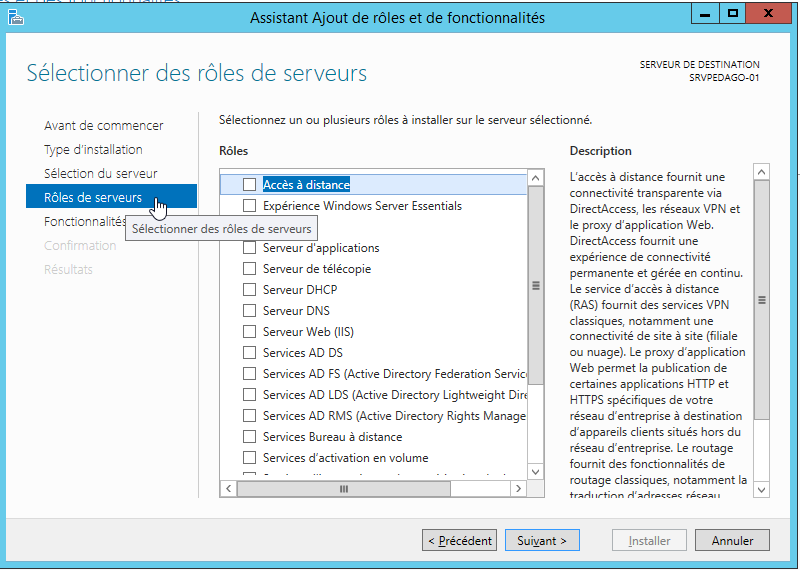
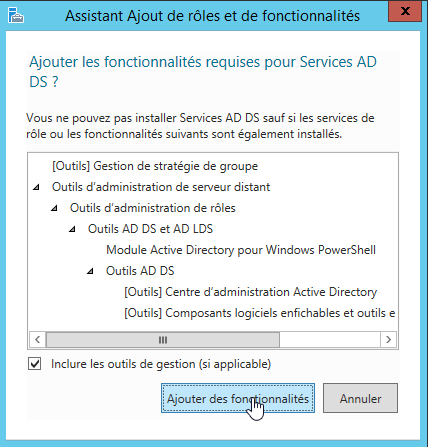


Une fois cliqué, une fenêtre d’assistance s’ouvre. Celle-ci a pour but de créer et préconfigurer le rôle de son choix.  
Comme on peut le voir ci-dessous, nous nous sommes rendus directement à la troisième étape. La première *« Avant de commencer »* fourni quelques indications à titre informatives. Le second : *« Type d’installation »* quant à lui, nous permet de choisir si l’on souhaite installer un rôle ou une fonctionnalité OU un service de bureau à distance.



Enfin, le menu *« Sélection du serveur »*, permet simplement de choisir où installer le rôle, ici : **SRVPEDAGO-01**.

À l’étape suivante, nous allons pouvoir cocher les rôles à installer sur le serveur.



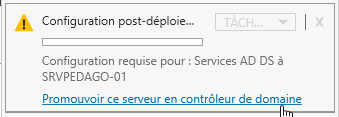
Une petite fenêtre vous préviens alors les prérequis nécessaires pour l’installation du rôle sélectionné.  


Pour commencer, nous installons le rôle « Active Directory ».  
Celui-ci aura pour fonction un « annuaire » regroupant l’ensemble des comptes utilisateurs sur le serveur via les « Contrôleurs de domaines » à travers le réseau.  
  
Dans « Fonctionnalités » nous ne sélectionnerons rien. Vient ensuite un petit « À propos » sur l’Active Directory et enfin, la confirmation de nos choix. *On peut également choisir de redémarrer serveur automatiquement.*

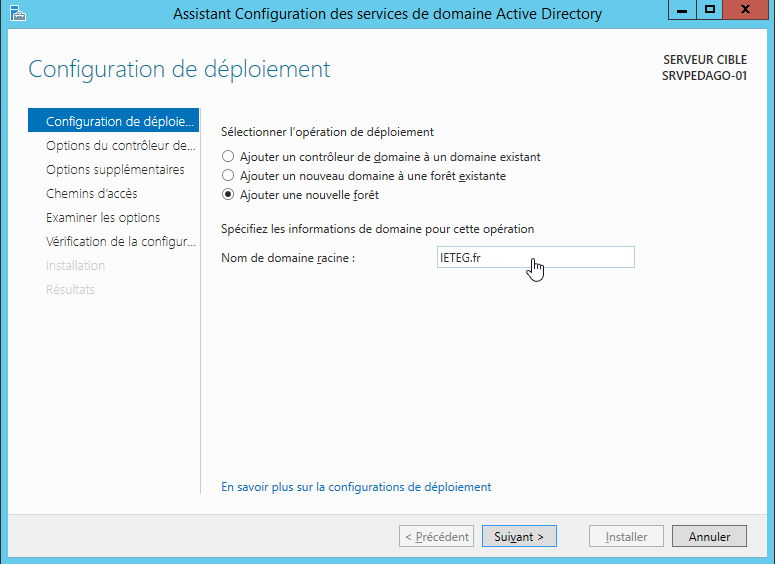


Puis une fois le rôle installé sur le serveur, une notification avec un point d’exclamation apparaît en haut à droite de la fenêtre du « Gestionnaire de serveur ».

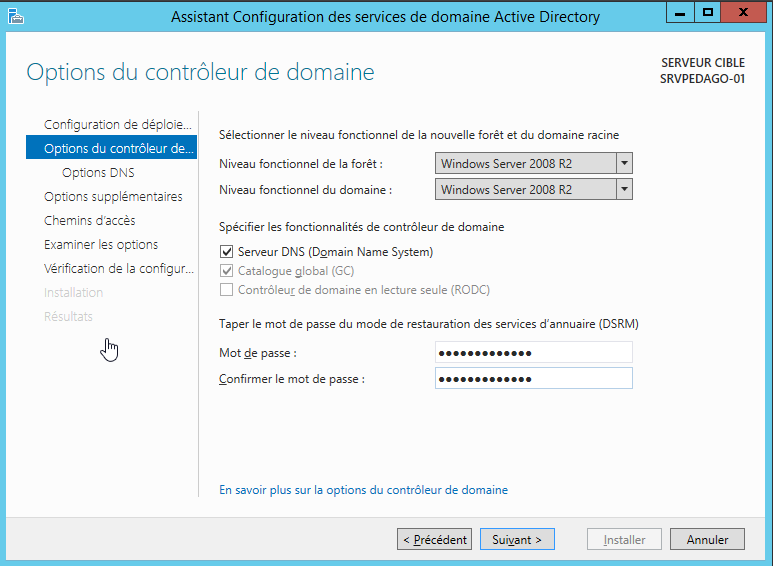


L’assistant vous propose alors de configurer le rôle.

Il faut ici choisir « Ajouter une nouvelle forêt ». Cela va permettre de créer un nouvel ensemble « Annuaire / Nom de domaine ».



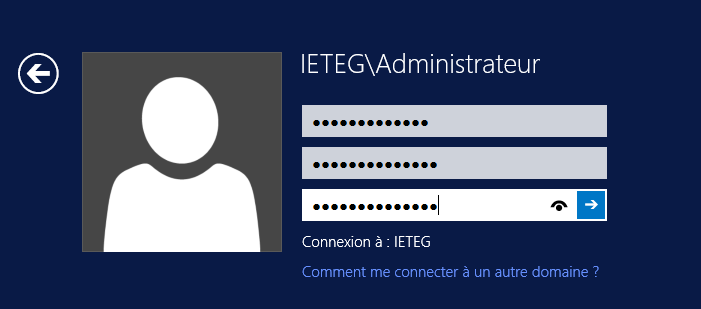
**Conformément au cahier de charges préalablement établi, le nom de domaine est : IETEG.fr**

Après quelques secondes, nous avons la possibilité de faire de petites modifications, comme la possibilité de changer le niveau du serveur (rétrograder le serveur en une version plus ancienne comme **WINDOWS SERVER 2008**) et de définir un mot de passe.  
**ATTENTION !** Afin de réaliser un « Cluster avec basculement » comme le demande le cahier des charges, il est nécessaire de choisir un niveau fonctionnel ***WINDOWS SERVER 2008 R2***. En effet, avec le niveau de **WINDOWS SERVER 2012 R2**, *le clustering est impossible avec des serveurs disposants le rôle « Active Directory ».*   
Dans l’optique d’économie financière, nous avons choisi de ne garder que deux serveurs (et donc d’avoir en cohabitation l’Active Directory avec le clustering).  


Comme aucun serveur DNS n’est existant sur le réseau, l’étape suivante est à ignorer.  
Enfin, nous gardons le *nom de domaine NetBIOS* **« IETEG »**.  
De même, les chemins d’accès ne sont pas à modifier. Nous pouvons donc faire « Suivant » jusqu’au la dernière étape où nous allons cliquer sur « Installer ».  
  
**Le serveur va redémarrer.**

**Maintenant, l’authentification sur le serveur s’effectue via « l’Active Directory » :**   


**Il sera cependant nécessaire de changer le mot de passe suite au passage dans le domaine.**



On peut observer à ce stade que sur le « Tableau de bord », les rôles « Active Directory » et « Domain Name Service » sont présent.  
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

À titre informatif, l’installation de l’  « Active Directory » peut aussi s’effectuer en script Powershell :

**Import-Module ADDSDeployment**

**Install-ADDSForest `**

**-CreateDnsDelegation:$false `**

**-DatabasePath "C:\Windows\NTDS" `**

**-DomainMode "Win2008R2" `**

**-DomainName "IETEG.fr" `**

**-DomainNetbiosName "IETEG" `**

**-ForestMode "Win2008R2" `**

**-InstallDns:$true `**

**-LogPath "C:\Windows\NTDS" `**

**-NoRebootOnCompletion:$false `**

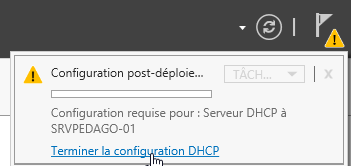
**-SysvolPath "C:\Windows\SYSVOL" `**

**-Force:$true**

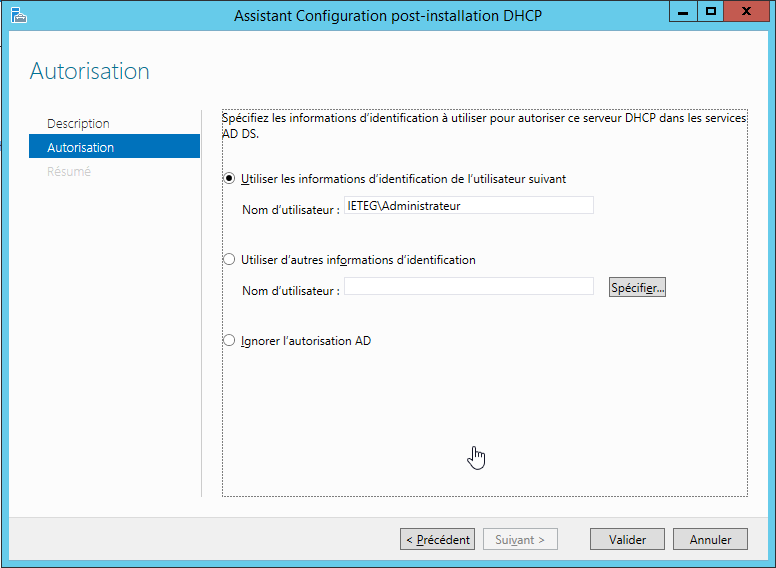
# DHCP

« L’Active Directory » maintenant installé et configurer, nous allons procéder à la mise en place du rôle et service DHCP. Les étapes sont les mêmes pour l’installation du rôle, il ne faut que sélectionner « Serveur DHCP » lors de l’étape « Rôles de serveur ».

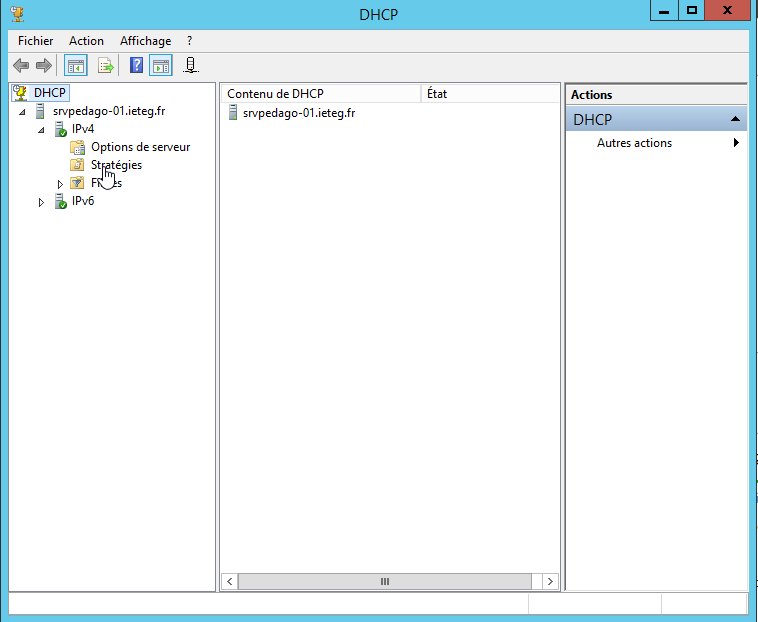


Une nouvelle notification vous propose alors de configurer le service.  
  


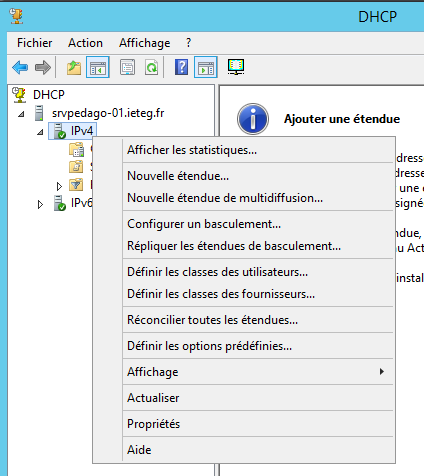
La première partie est une description du service.  
Puis, on choisit quel utilisateur va autoriser le DHCP dans l’AD. Evidemment, il s’agit de la session Administrateur.



Le rôle et le service est maintenant en place. Cependant, **il faut définir la plage d’adressage IP**.  
*Pour cela, il faut presser la touche WINDOWS du clavier ou cliquer en bas à gauche sur le logo Windows. Puis nous tapons DHCP pour accéder à la gestion de celui-ci.*

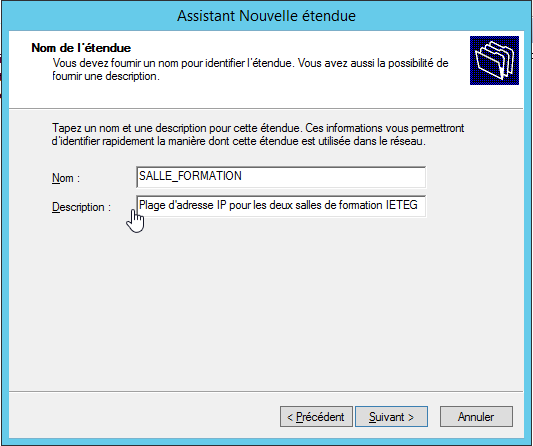


On développe le menu déroulant de notre serveur maintenant dénommé « srvpedago-01.ieteg.fr »  
Puis clic droit sur « Nouvelle étendue ».

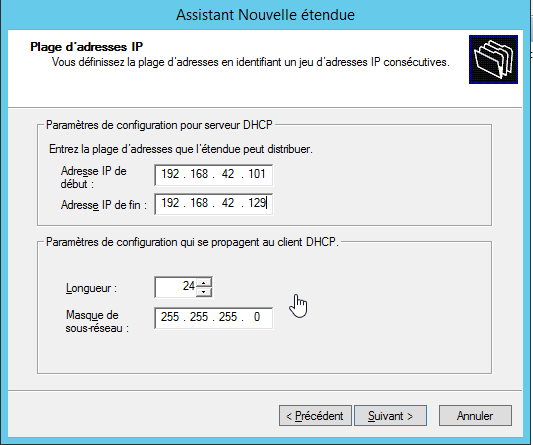


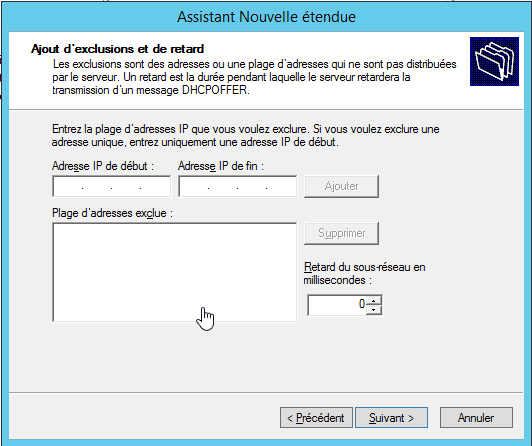
Un nouvel Assistant s’ouvre alors.

Il faut donc définir un nom à la nouvelle étendue (plage d’adressage IP) et lui donner sa description détaillant éventuellement à quoi elle correspond.

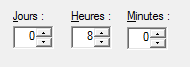


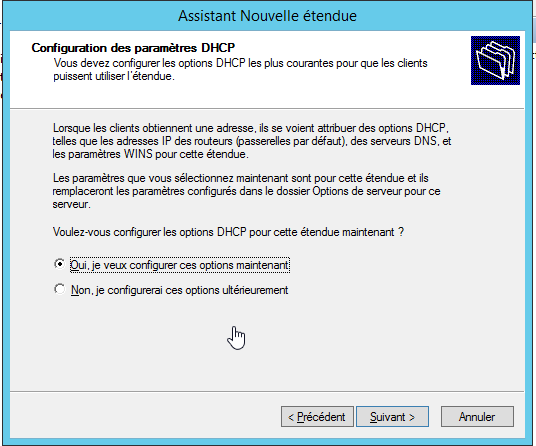
Il faut à présent établir la fameuse plage.

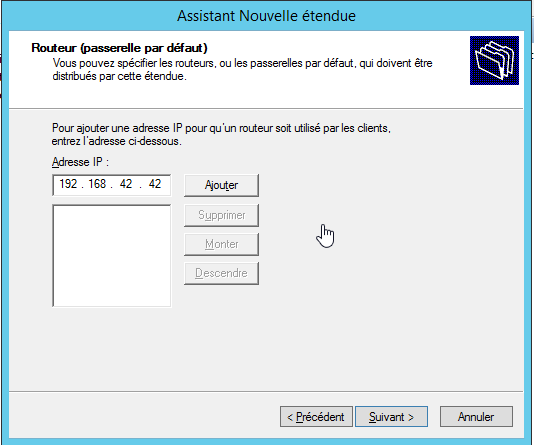


Comme exigé dans le cahier des charges, l’étendu est sous la forme « 192.168.42.X/24 » avec un masque de sous-réseau 255.255.255.0.  
Le choix de l’étendu : 192.168.42.101 à 192.168.42.129, résulte de 101 (première adresse IP de la plage) + 24 postes (donc IP) + 2 postes enseignants + une petite marge de 2 adresses en réserve. Cependant, par sécurité, la plage a été restreinte un maximum à 28 adresses possible.  
  


Nous avons la possibilité d’entrer des IP à exclure de la plage, nous ne le faisons pas, car nous n’en avons pas l’utilité ici.  
  
Puis nous attribuons un bail (durée à laquelle une IP est attribuée à un poste) de 8 heures, l’équivalent à une journée de formation.

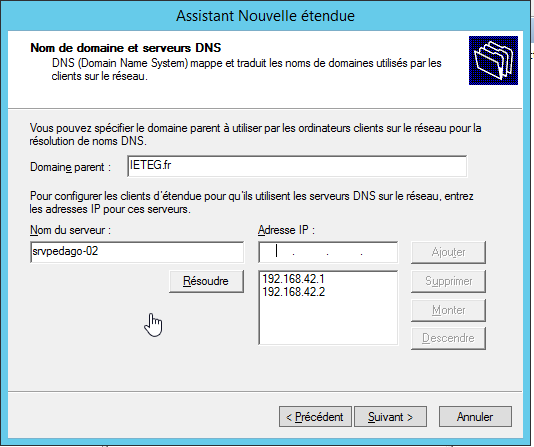


Nous choisissons de configurer les options maintenant : 

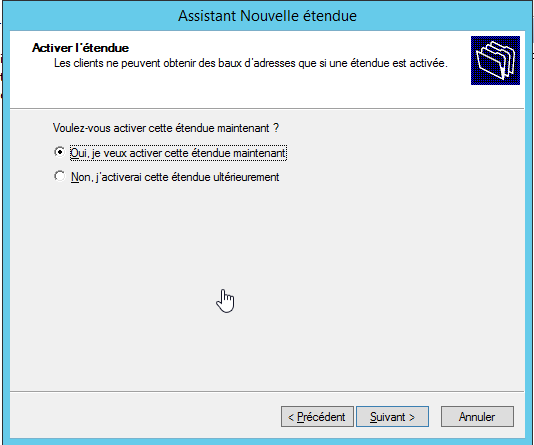
Etape suivante, nous entrons l’adresse IP de la passerelle.  
Pour des raisons de mnémotechnique, nous avons choisi d’attribuer l’adresse 192.168.42.42 comme passerelle.  
  


Il s’agira donc de l’adresse qu’aura notre serveur servant de routeur : **PfSense**.

*Il faut ensuite définir quel domaine et les serveurs DNS qui seront attribué automatiquement aux postes joignant le domaine IETEG.fr*  
Nous ajoutons à l’avance l’adresse du second serveur WINDOWS SERVER 2012 R2 qui viendra garantir la disponibilité des services : 192.168.42.2 (nom : SRVPEDAGO-02)



Nous n’avons pas de serveur WINS, l’étape suivante est donc à ignorer.

Puis, nous activons l’étendue et nous avons terminé.  
  


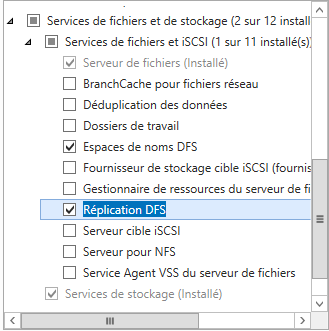
# DFS

« Distributed File System » est une fonctionnalité **WINDOWS SERVER** ayant plusieurs intérêts :

* *Fournir une arborescence logique aux données partagées depuis des emplacements différents ;*
* *Rassembler différents partages de fichiers à un endroit unique de façon transparente ;*
* *Assurer la redondance et la disponibilité des données grâce à la réplication ;*

Tout comme n’importe quel rôle, DFS s’installe via le « Gestionnaire de serveur » ; les premières étapes sont donc les mêmes.

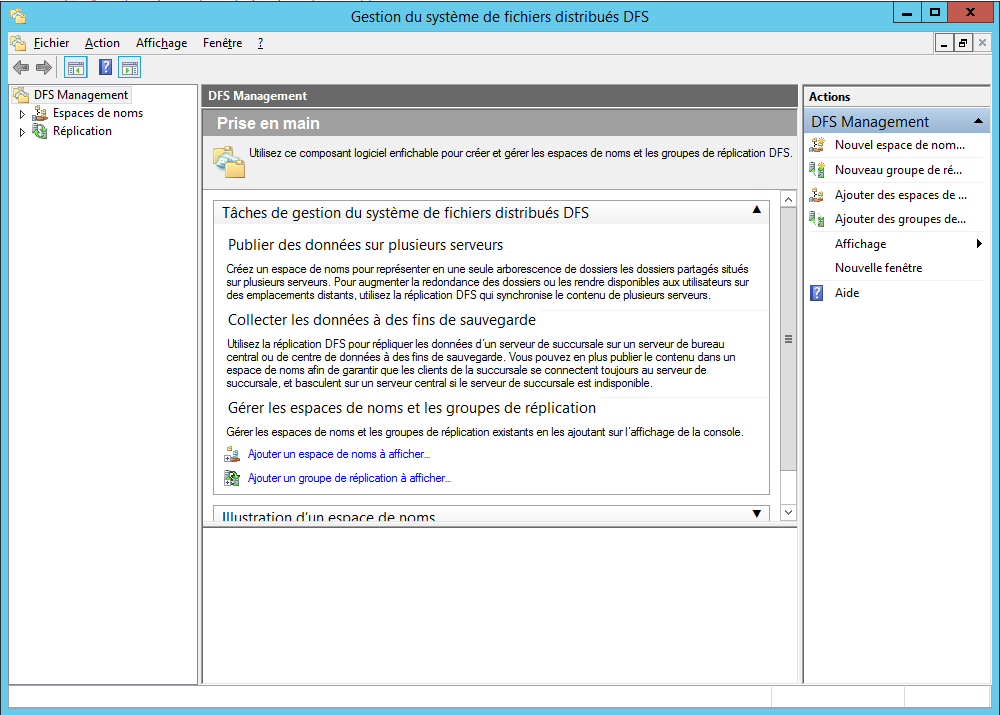
Lors de la quatrième étape d’installation, après avoir sélectionné notre serveur « SRVPEDAGO-01 », nous devons choisir le rôle à installer.  
Cependant, DFS n’est pas directement visible : il faut « développer » deux sous arborescences.



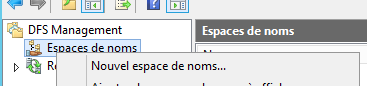
Le nom du rôle étant : « Espaces de noms DFS »  
Nous ajoutons la fonctionnalité « réplication DFS », puis nous pouvons confirmer et installer.  
  
*DFS est installable via Powershell avec la commande :*

**Install-WindowsFeature FS-DFS-Namespace**

À présent installer, il va falloir configurer le service.  
Pour cela, dans le « Gestionnaire de serveur », dans « Outils » (et non « Gérer » comme pour l’installation d’un rôle), cliquer sur « **Gestion du système de fichiers distribués DFS »  
Une page de management du rôle s’ouvre alors (semblable à celle permettant la configuration du service DHCP) :**

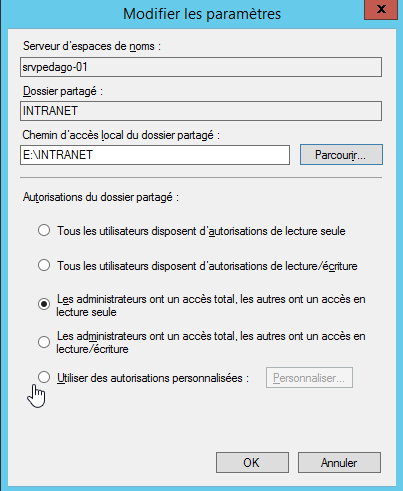


Enfin, clic droit sur « Espaces de noms » 🡪 « Nouvel espace de noms »



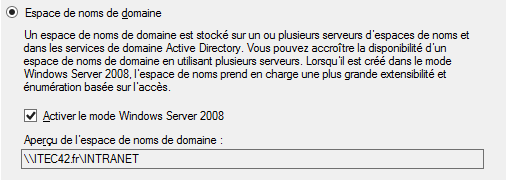
On choisit notre serveur qui va héberger le service, ici, SRVPEDAGO-01



Il faut ensuite créer les partages.  
Comme indiquer dans le cahier des charges, trois partages seront créés : **GRP1 (lecteur W), GRP2 (lecteur X) et TRANSFERT (lecteur Y)** ; ces trois répertoires étant **sur le disque « E:\DATAS » dans le répertoire « INTRANET ».**  
  


En accord avec le cahier des charges, nous créons alors le partage « INTRANET » où **l’ensemble des utilisateurs disposeront des droits de lecture seul sur la racine du partage (INTRANET) et les administrateurs de domaine avec un contrôle total.** *Les utilisateurs se verront avoir des droits supplémentaires sur des sous-répertoires du partage en fonction du cahier des charges.*

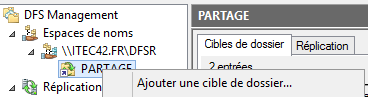
Il nous faudra, à l’étape suivante, choisir « Espace de noms de domaine » et non « Espace de noms autonome ». En effet, ce partage va devoir être le disponible un maximum et donc répliqué sur un serveur de basculement afin d’en garantir la disponibilité.   
Il faut donc enfaite choisir « Espace de noms de domaine ». (Suite à l’évolution technique)

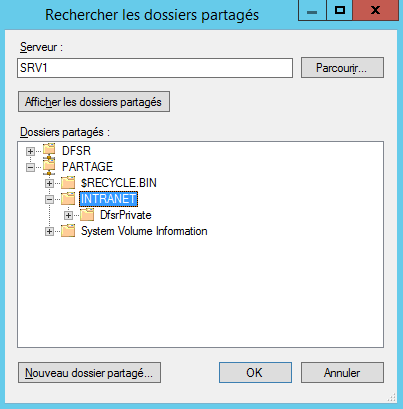


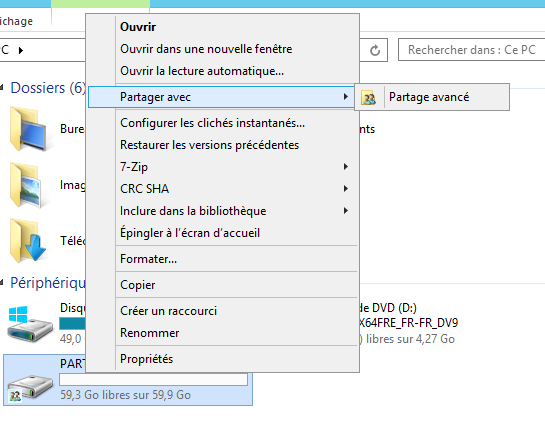
Nous pouvons le créer, et c’est terminé.  
Pour les prochains répertoires, il suffira dans ce même panneau de management, cliqué droit sur le nom de notre partage : « \\SRVPEDAGO-01\INTRANET » puis « Nouveau dossier » :

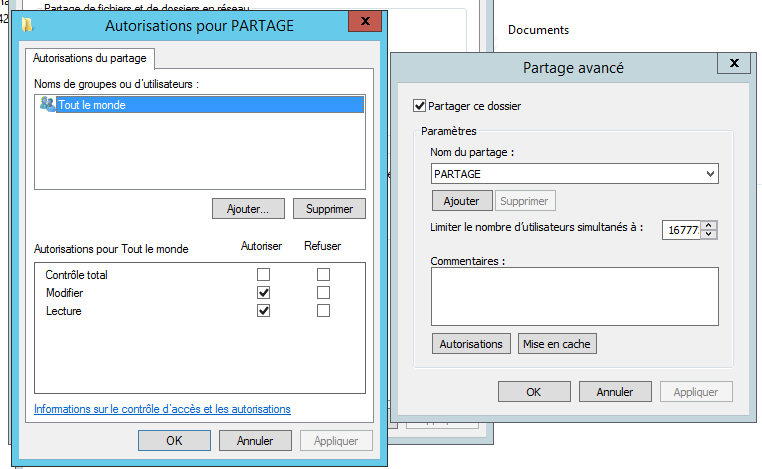


Nous avons à ce stade ceci :

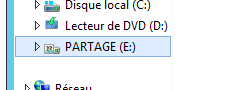


  
  
La remontée d’un répertoire en lecteur réseau est simple : clic droit sur « Ce PC » ou « Ordinateur » (cela dépend des versions du client Windows) dans l’explorateur de fichier.  
Puis, cliquer sur « Connecter un lecteur réseau… »



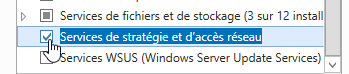


Il faudra ensuite choisir une lettre, par exemple « Y » pour « TRANSFERT » et indiquer le chemin d’accès au dossier. De même pour les autres lecteurs :



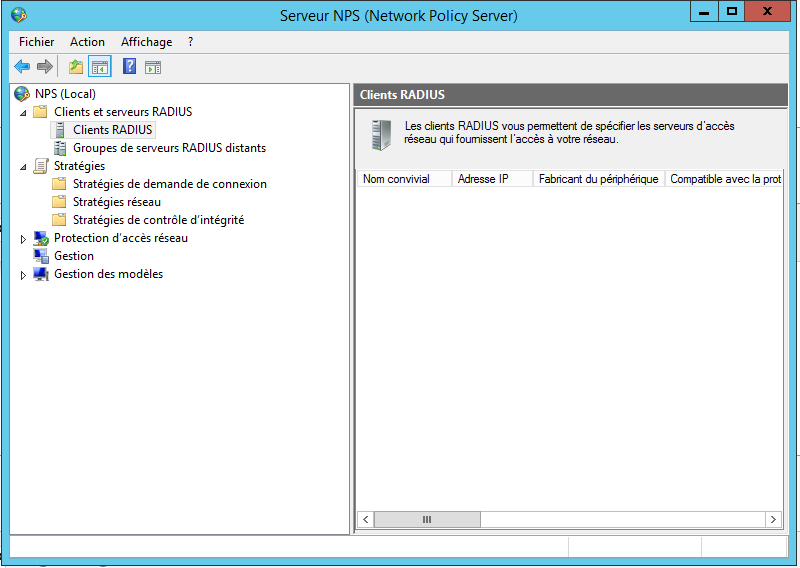
**Les utilisateurs se verront attribué leurs lecteurs par script de connexion et il n’y aura donc pas besoin de faire cette manipulation sur les postes clients.**

NPS RADIUS  
  
Le rôle NPS se nomme « Services de stratégie et d’accès réseau » dans l’utilitaire d’installation des rôles.

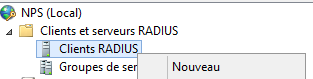


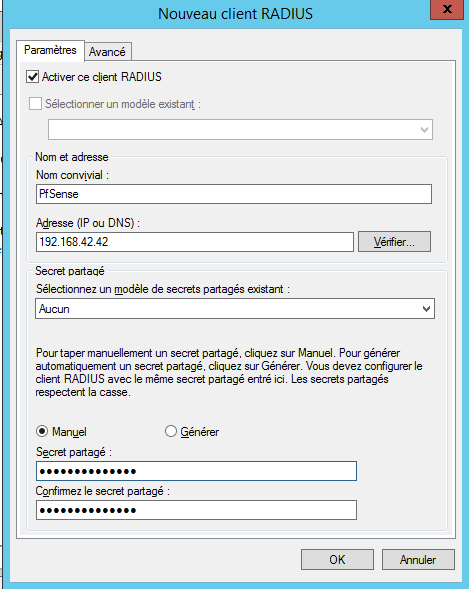
Puis suivant jusqu’à l’installation.  
Une fois installer, dans le « Gestionnaire de serveur », nous verrons apparaître un nouveau service : « NAP »

Il faut ensuite se rendre sur la fenêtre de configuration NPS. (Taper NPS dans la recherche Windows)



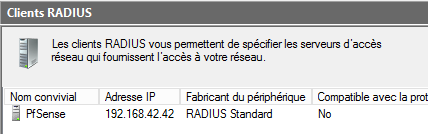
Puis, ajoutons **notre client RADIUS : PfSense** dont l’adresse IP, rappelons-le est : **192.168.42.42**





**Il est impératif de définir une clef secrète de partage avec de créer un jeton sur le client et garantir ainsi la sécurité du protocole.**

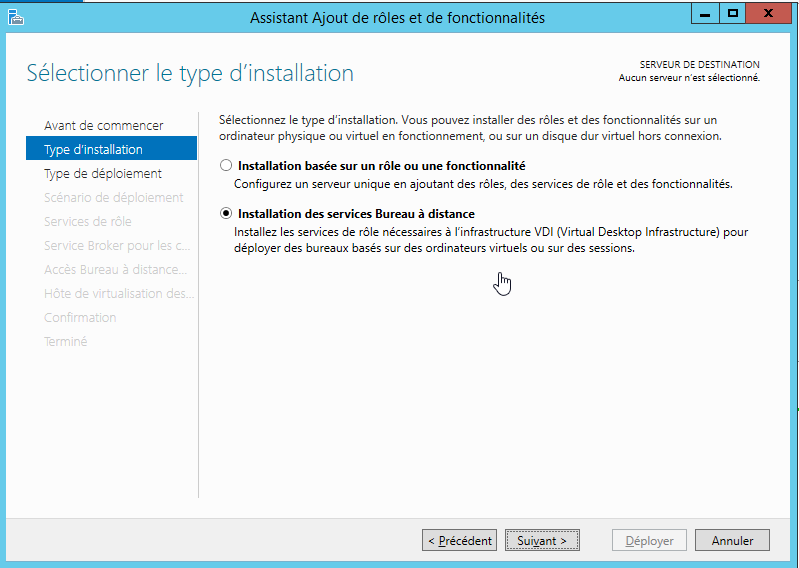
Nous pouvons alors observer le client :

  
  
Pour la suite, il faudra attendre l’installation et la configuration du serveur PfSense.

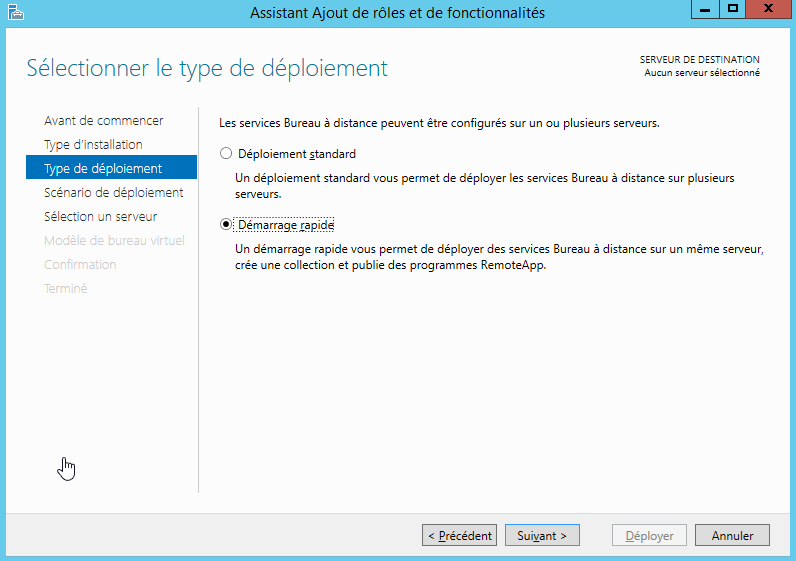
# TSE

Le rôle que nous allons installer se nomme « Terminal Server ».

Comme à l’accoutumé, l’installation de ce rôle s’effectue de la même façon que les autres à un détail près :

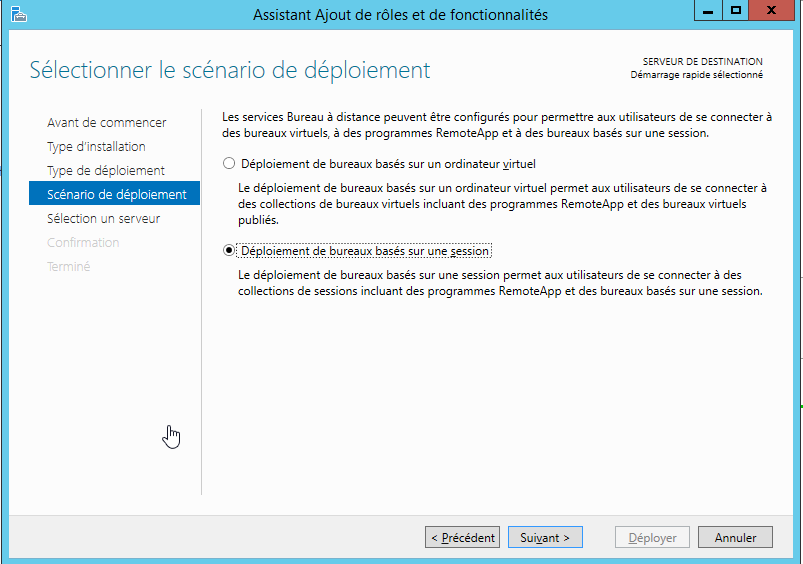
  
  
En effet, lors de la seconde étape d’installation du service**, il faut cette fois-ci choisir « Installation des services Bureau à distance » et non « Installation basée sur un rôle ou une fonctionnalité ».**

Les étapes vont ensuite être bien différentes de ce que nous avons vu précédemment.

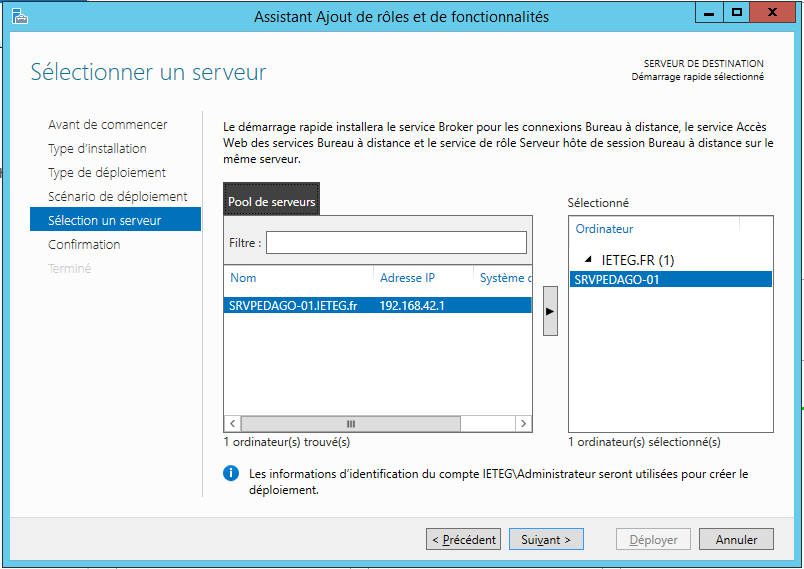


Il faut donc choisir « Démarrage rapide » à l’étape 3 car ici nous allons déployer ce service sur notre serveur.

Ensuite, **il faut choisir « Déploiement de bureaux basés sur une session » ainsi, les comptes Active Directory seront « lié » au service** et ces mêmes comptes pourront s’identifier dessus.

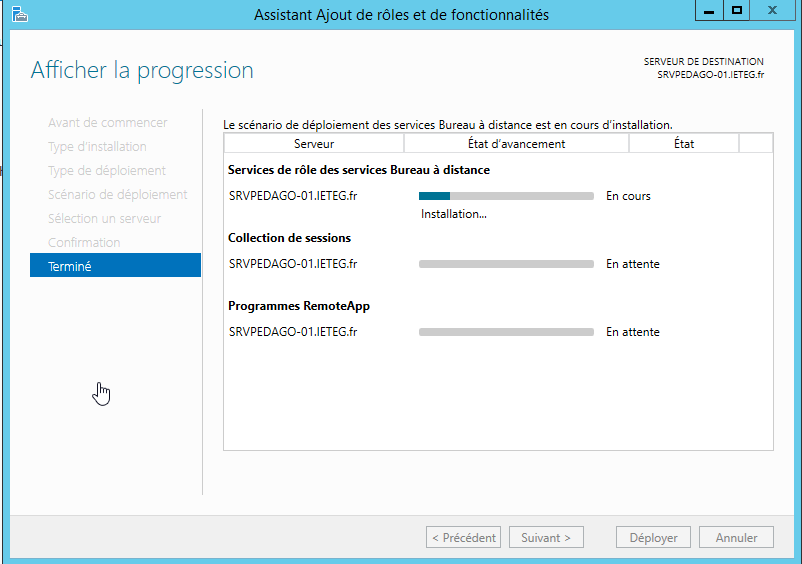


Puis nous faisons suivant, ne disposant que d’un seul serveur dans ce cas de figure :



Lors de l’étape « Confirmation », un message vous informant que le serveur devra redémarrer s’affiche. Il faudra alors cocher la case permettant le redémarrage automatique après l’installation du rôle.  
  
Cliquer sur « Déployer »

Nous obtenons une fenêtre semblable à celle-ci :



Il suffira alors d’attendre la fin de l’installation des « scénarios » par le serveur.

*À noter, l’installation des « scénarios » sont assez long : plusieurs minutes.*

**Au redémarrage, l’installation reprend rapidement et fini d’installer le service.**   
  
L’installation du rôle est terminée, à présent nous allons devoir activer la licence d’utilisation.

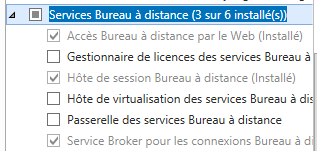
Afin d’entrer la licence, il nous est nécessaire d’installer un nouveau rôle : « Gestionnaire de licences des services de bureau à distance »

**/ ! \ ATTENTION ! Contrairement au rôle TSE, ce rôle-ci s’installe bel et bien en tant que « Rôle et fonctionnalité » sur le serveur ! Et non comme « Service de bureau à distance »**

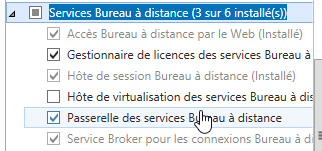
Pour l’installation, faire suivant jusqu’à l’étape 4 « Rôles de serveurs ».  
Ici, cocher « Service bureau à distance »  
  
Suite à l’installation du rôle précédent, nous voyons que certains services sont déjà présent sur le serveur :



Il suffit alors de cliquer sur la flèche afin de dérouler les options,

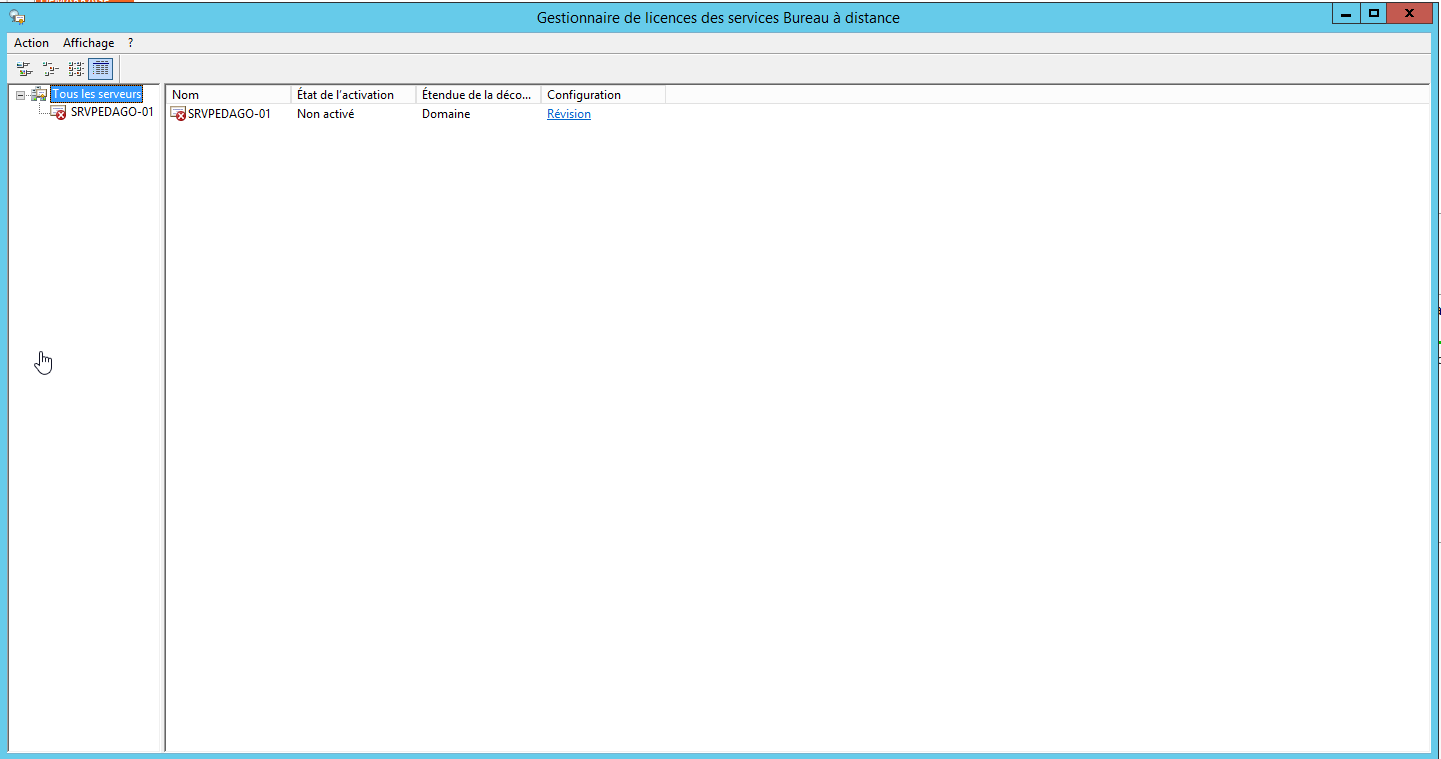


Il y a bien trois services d’installer.  
**Nous cochons alors « Gestionnaire de licences des services Bureau à Distance ». Il permet de gérer les licences « CAL (Client Access Licenses) ».**



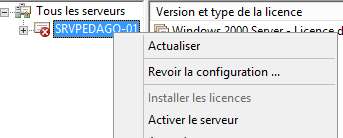
Puis suivant, car il n’y a pas de fonctionnalités à installer.  
Puis nous terminons l’installation du rôle.

Il faut donc se rendre sur le gestionnaire de licence, pour cela, il suffit de rechercher sur le serveur « Gestionnaire de licences de Bureau à distance ».  
  
Le manager ressemble à ceci :



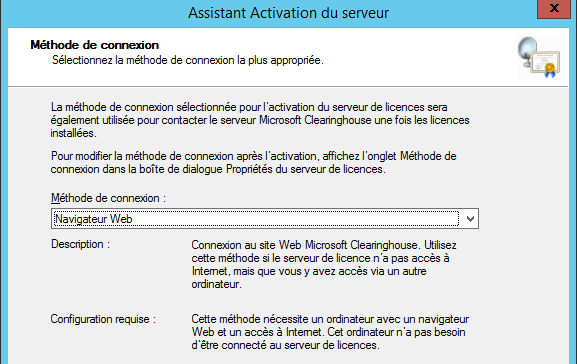
**Sans licence, l’utilisation de ce service est limitée à 120 jours. Il est donc impératif de disposer d’une licence.**

Clic droit sur notre nom de serveur, puis « Activer le serveur »



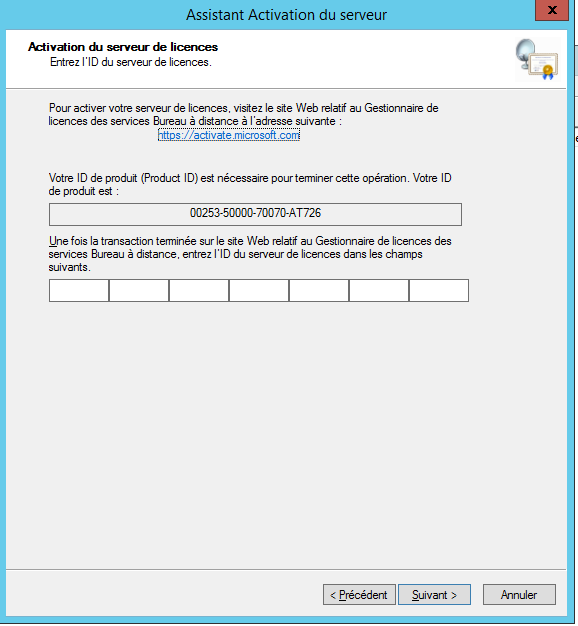
Puis suivant.

Ensuite, nous choisissons en « Méthode de connexion » « Navigateur Web »



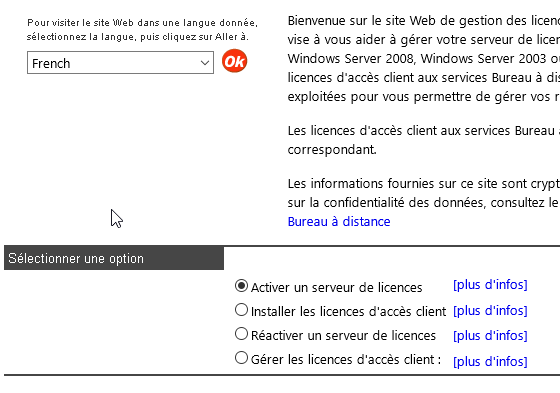
IMPORTANT

**La fenêtre suivante requiert une clef.  
Celle-ci s’obtient via le lien :** [**https://activate.microsoft.com/**](https://activate.microsoft.com/)

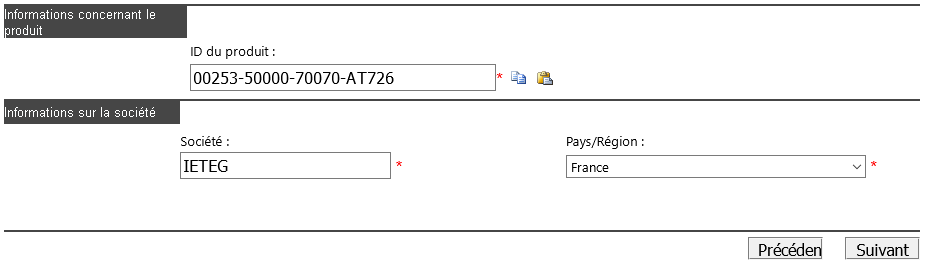


Il faut copier notre ID produit sur le site.

Pour cela, nous sélectionnons « Français » et « Activer un serveur de licences » puis suivant

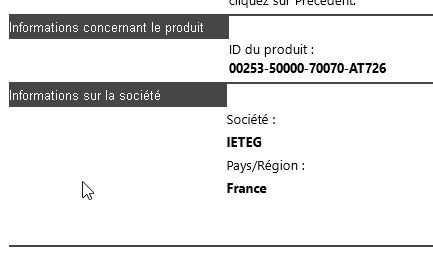


Puis nous entrons les informations demandé :

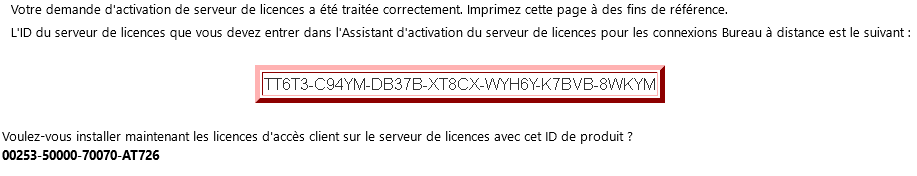


Suivant,

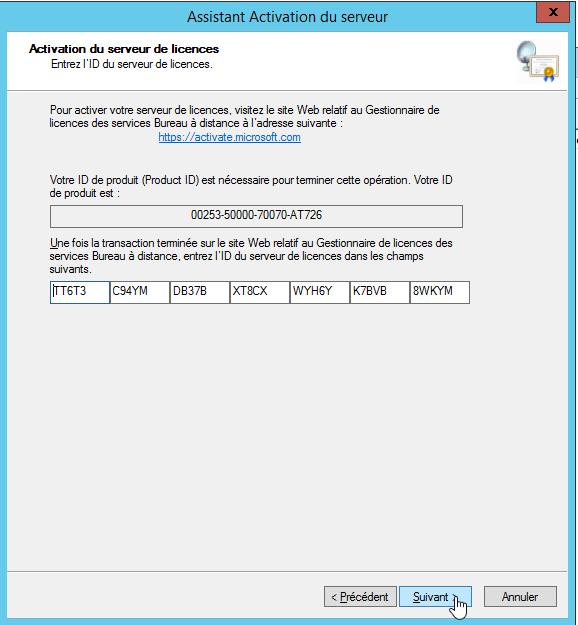
Petit récapitulatif :



Enfin, après avoir cliqué sur suivant, nous obtenons notre licence :

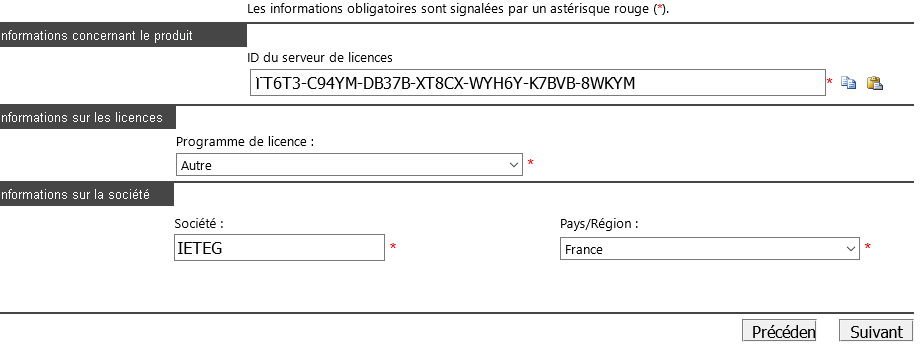


On retourne sur la fenêtre de l’assistant d’activation et on colle le numéro de licence fourni par MICROSOFT.

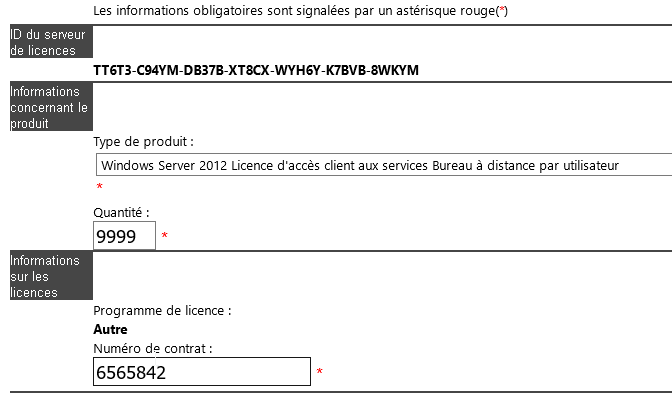


Suivant, l’installation et terminé, nous devons à présent retourner sur le site de MICROSOFT.  
Nous laissons alors coché « Démarrer l’Assistant Installation de licences ».

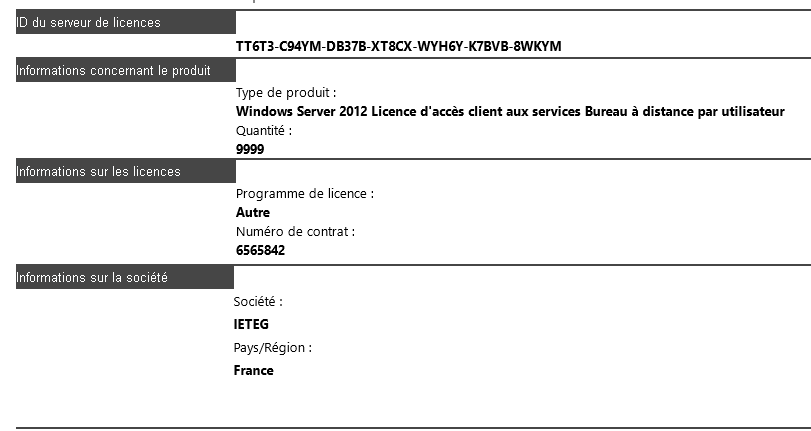
Sur le site, nous cliquons sur **OUI**, la page suivante apparaît et nous remplissons les champs nécessaires :



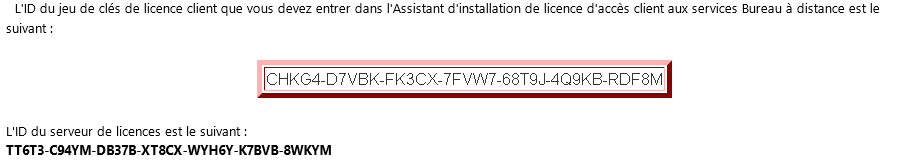
Et après,



Un second récapitulatif nous est donné

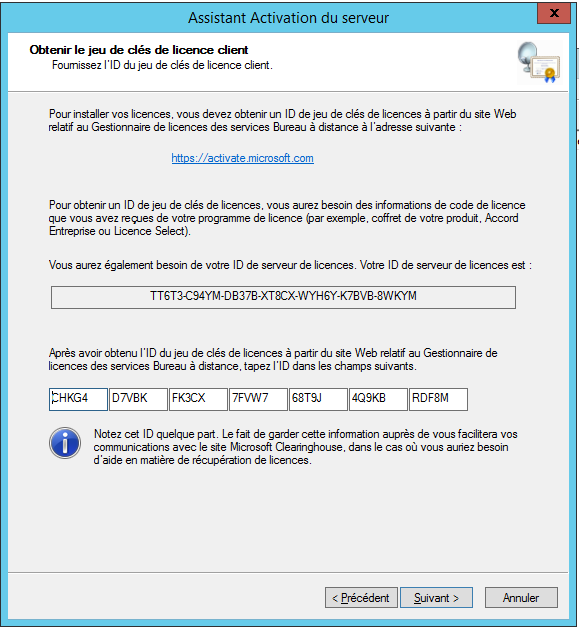


La page suivante nous fournit alors une licence :



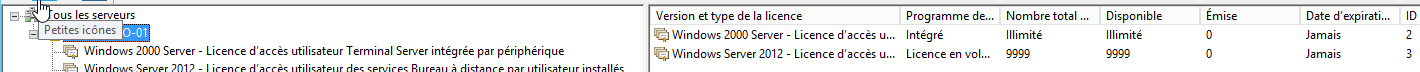
Terminé. On copie le numéro de licence et revenons sur le serveur.

On fait suivant sur la fenêtre d’assistance, puis, à l’étape « Fournissez l’ID du jeu de clés de licence client », on entre notre clef.

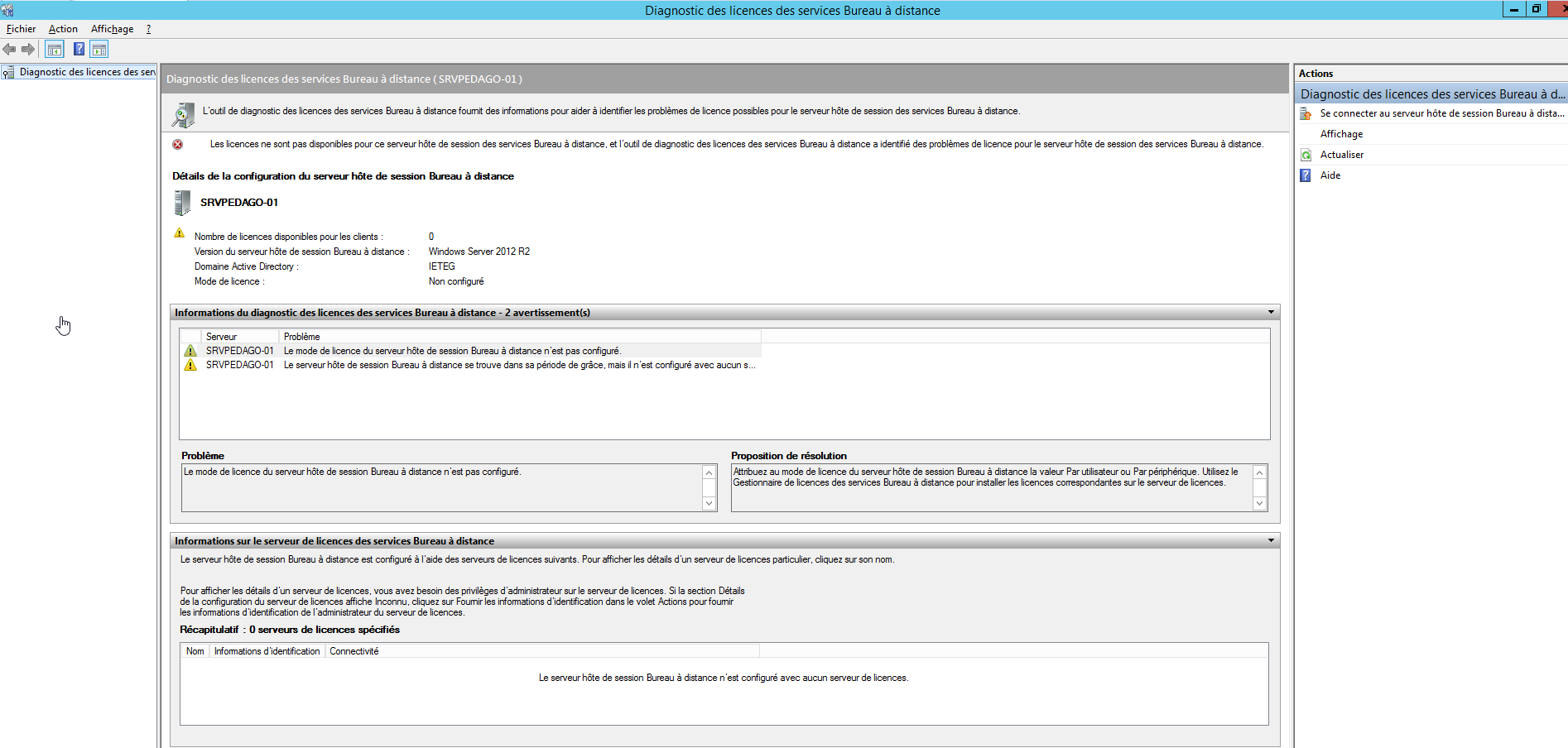


Suivant et c’est terminé.

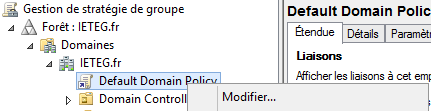
Cependant, quand bien même la licence est bonne, il nous reste à lier le service à l’Active Directory,



Il nous faut nous rendre sur le programme « Diagnostic des licences Bureau à distance »



Pour remédier au problème, **nous allons donc créer une stratégie de groupe (GPO) sur la stratégie principale.**  
Dans la recherche WINDOWS, nous tapons **« Gestion de stratégie de groupe »**, puis, dans la fenêtre de gestion, nous déroulons la forêt **« IETEG.fr »**, dans **« Domaine »**, **« IETEG.fr » et clic droit sur « Default Domain Policy » 🡪 modifier.**



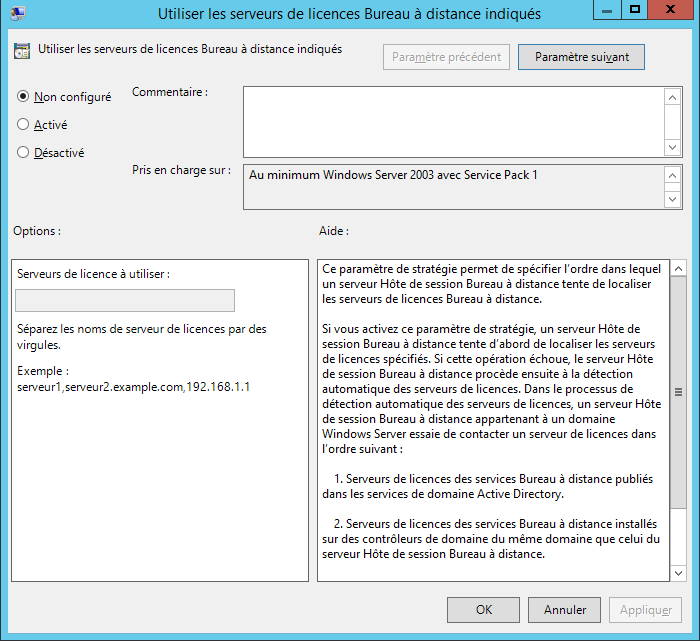
Enfin, il faut accéder au menu « Gestionnaire de licences » présent dans « Hôte de la session Bureau à distance ».  
Le chemin d’accès étant le suivant :

**Configuration de l’ordinateur\Stratégies\Modèles d’administration\Composants**

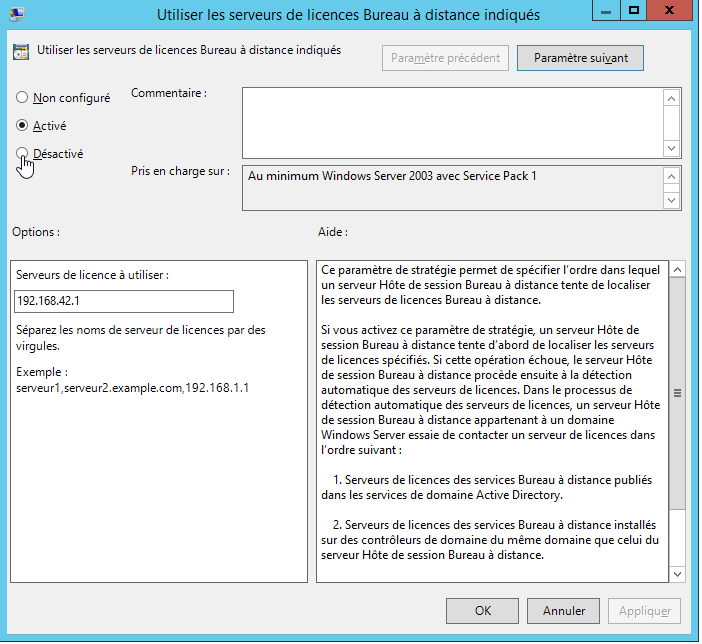
**Windows\Services Bureau à distance\Hôte de la session Bureau à distance\Gestionnaire de**

**Licences**

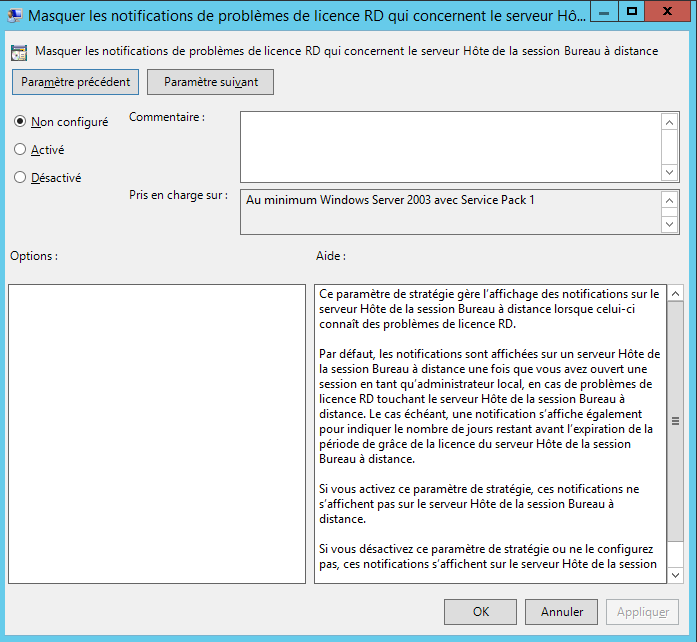
Il faut double-cliquer sur « Utiliser les serveurs de licences Bureau à Distance ».  
La fenêtre apparait ainsi :



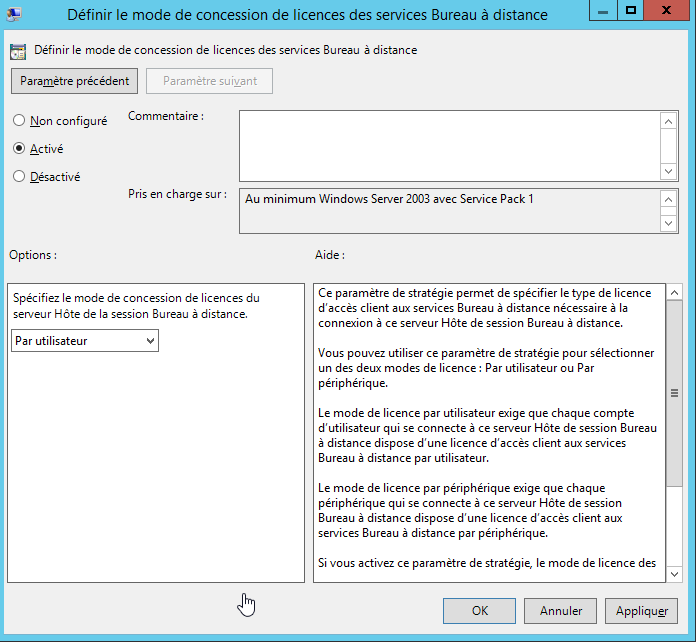
Enfin, suivre ces étapes :



« Paramètre suivant »

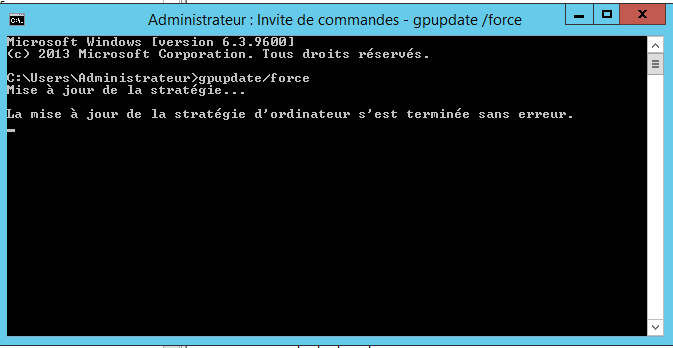


« Paramètre suivant »

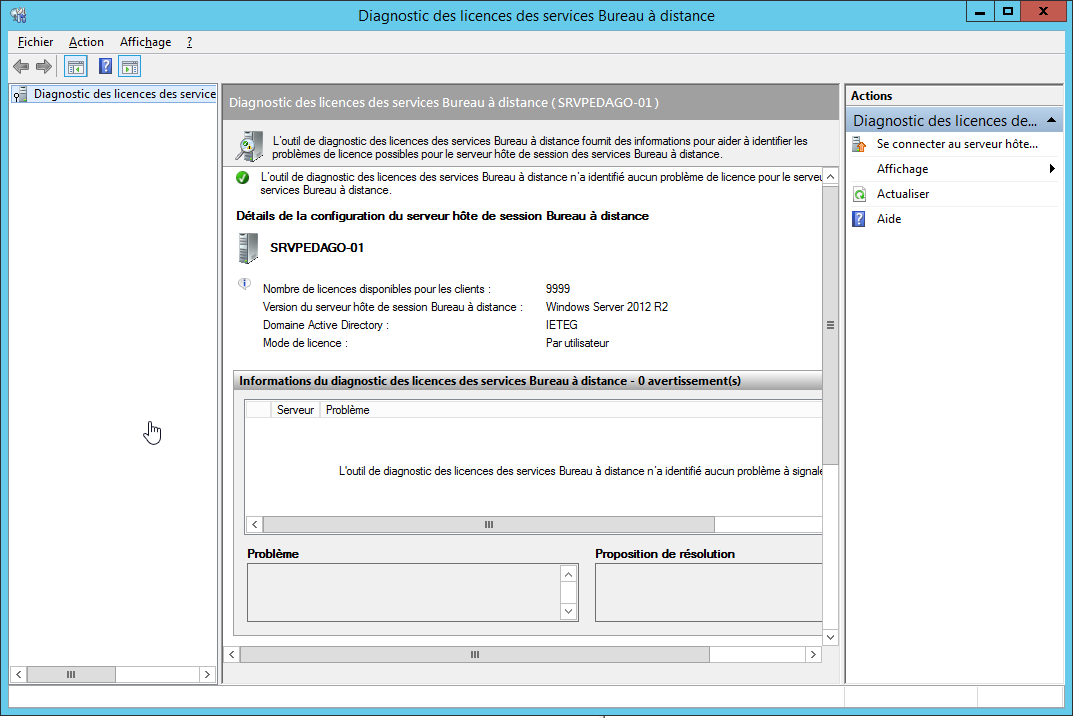


« OK »

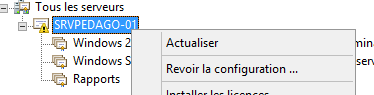
**Une fois ceci fait, nous devons ouvrir une invite de commande WINDOWS et lancer la commande suivante : « gpupdate/force » ; elle permet de forcer l’activation immédiate de la stratégie.**



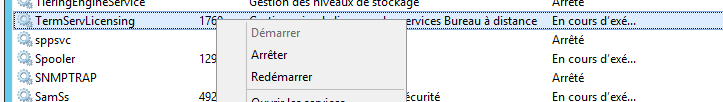
Maintenant, nous retournons sur la fenêtre de « Diagnostic des licences des services Bureau à distance » et actualisons avec « F5 » (la touche de fonction sur le clavier)   
Voici le résultat, tout est bon.



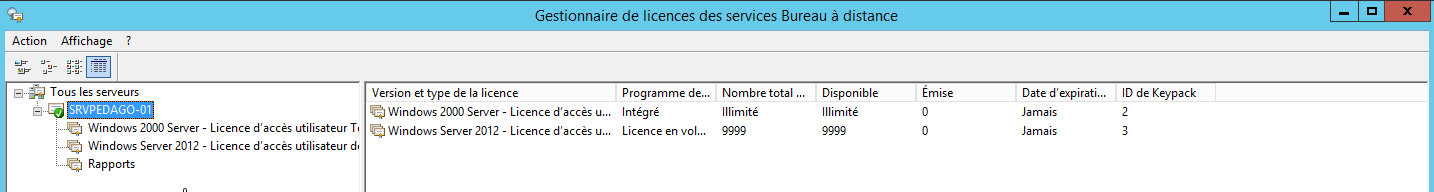
Par contre, il nous faut retourner sur le « Gestionnaire de licences des service de Bureau à distance », il reste une alerte.  
Clic droit sur notre serveur, et « Revoir la configuration »



Puis, on « Ajoute au groupe »  
  
C’est terminé.  
  
**Il ne reste plus qu’à redémarrer le service via le « Gestionnaire des tâches »  
Le service se nomme « TermServLicensing »**

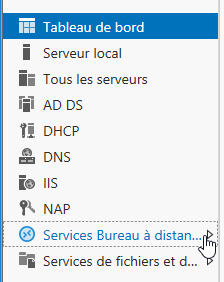


Tout est OK !

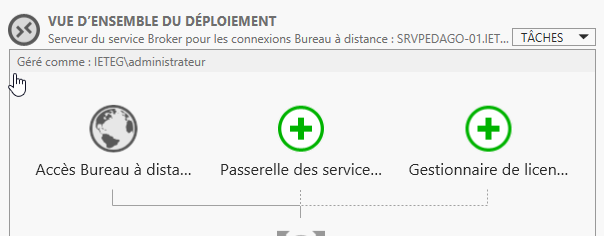


Il faut maintenant configurer les  « Services de Bureau à distance »

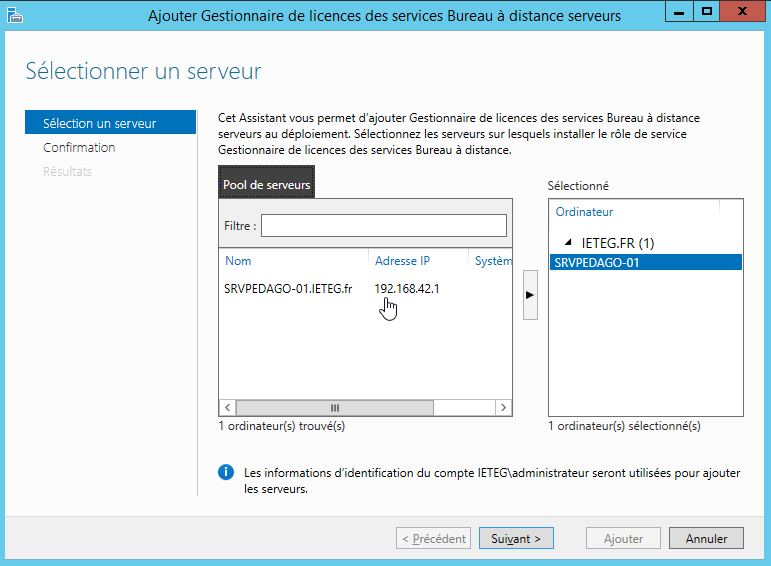
Sur le « Tableau de bord », nous pouvons donc observer l’apparition du service :



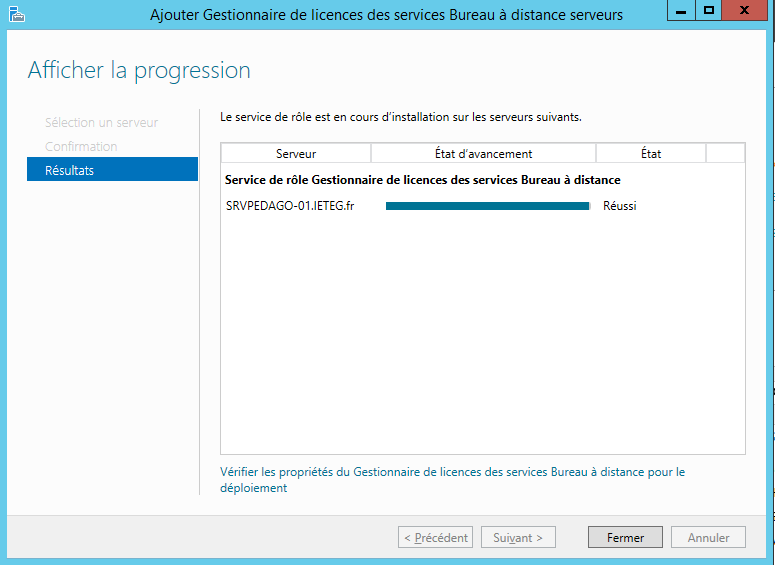
Nous pouvons voir ci-dessous, qu’il manque tout de même le « Gestionnaire de licence » et la « passerelle des Services Bureau à distance ».



On clique sur le + du gestionnaire de licence,



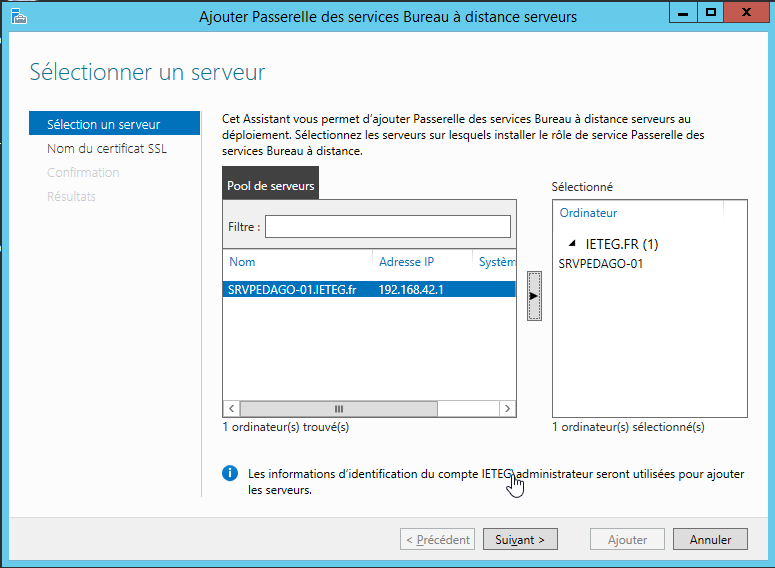
On sélectionne notre serveur puis suivant.



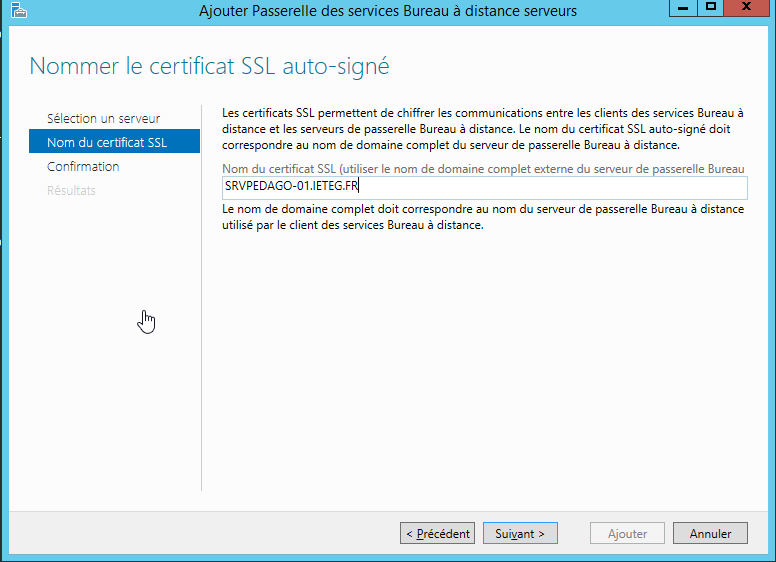
Et voilà ! Le gestionnaire de licence est présent.



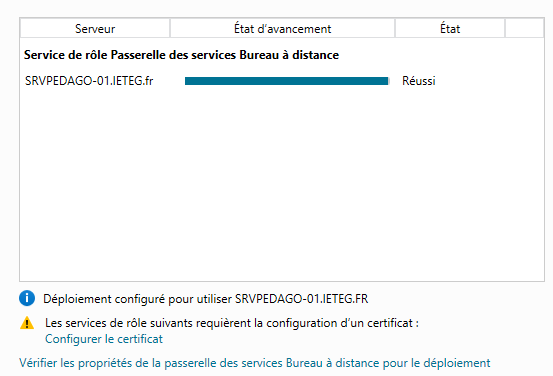
De même pour la passerelle 🡪



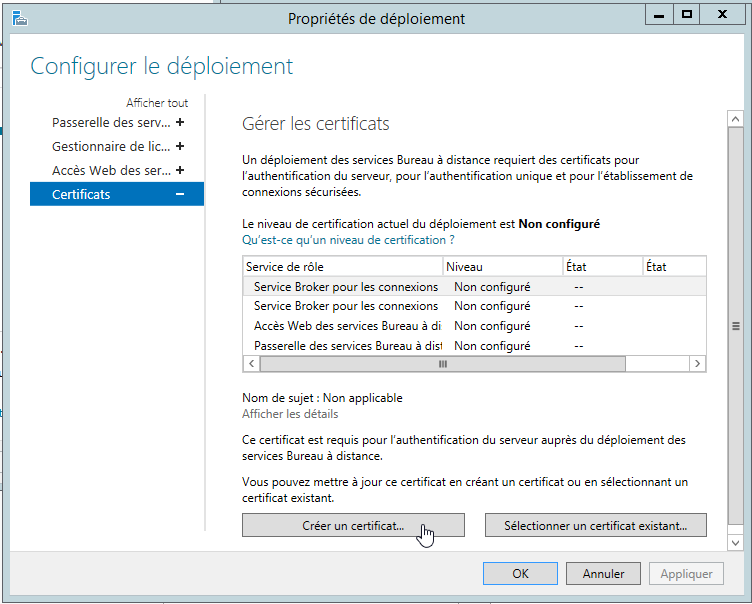
On sélectionne notre serveur,



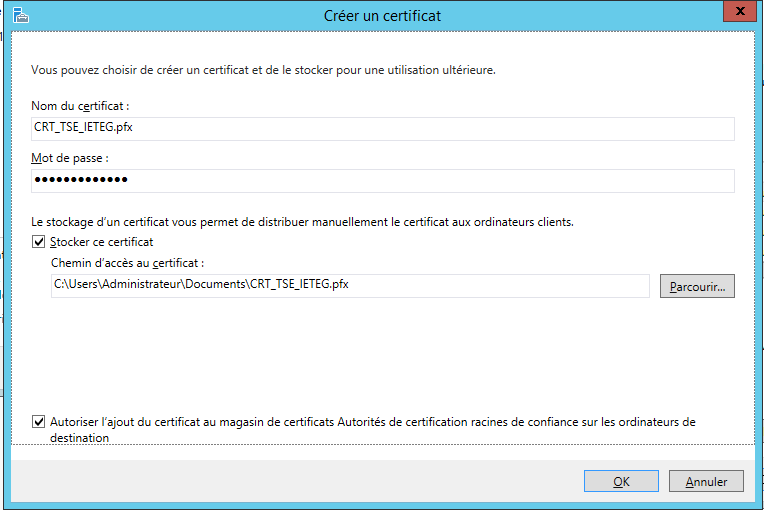
On nomme le certificat SLL avec le nom ENTIER du serveur (nom serveur + domaine complet)



Il manque cependant la configuration du certificat. On clique alors sur « Configurer le certificat »



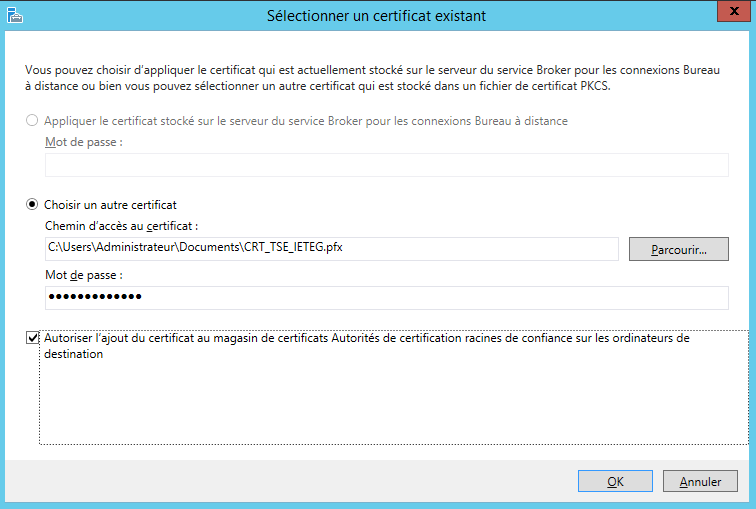
Nous n’avons pas de certificat, nous allons donc en créer un.



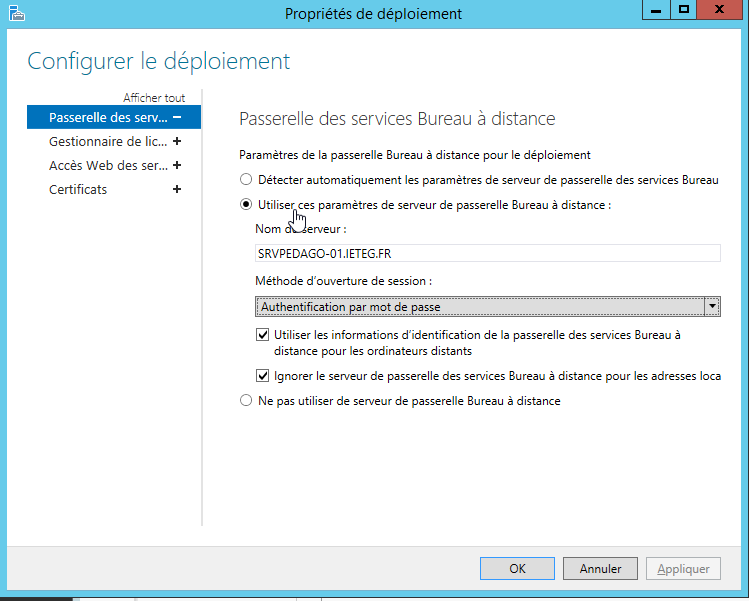
On le nomme par exemple « CRT\_TSE\_IETEG.pfx », on définit un mot de passe.

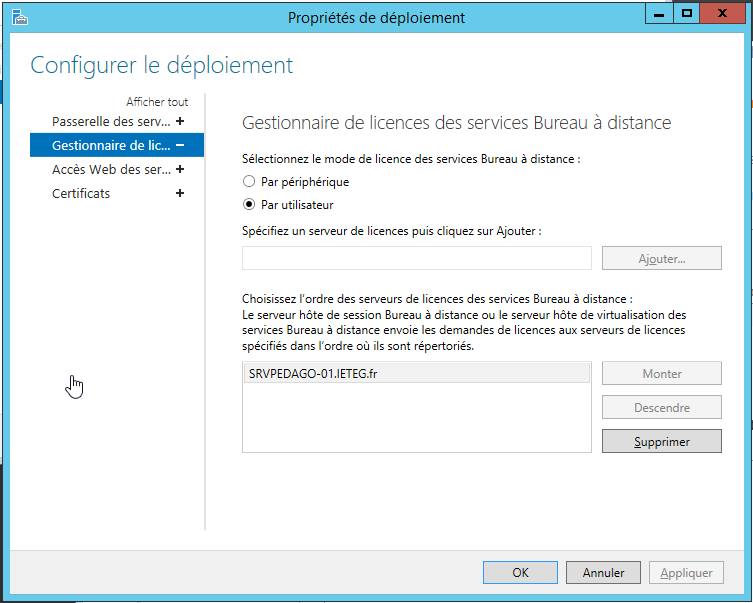
On choisit aussi de stocker ce certificat pour s’en resservir.

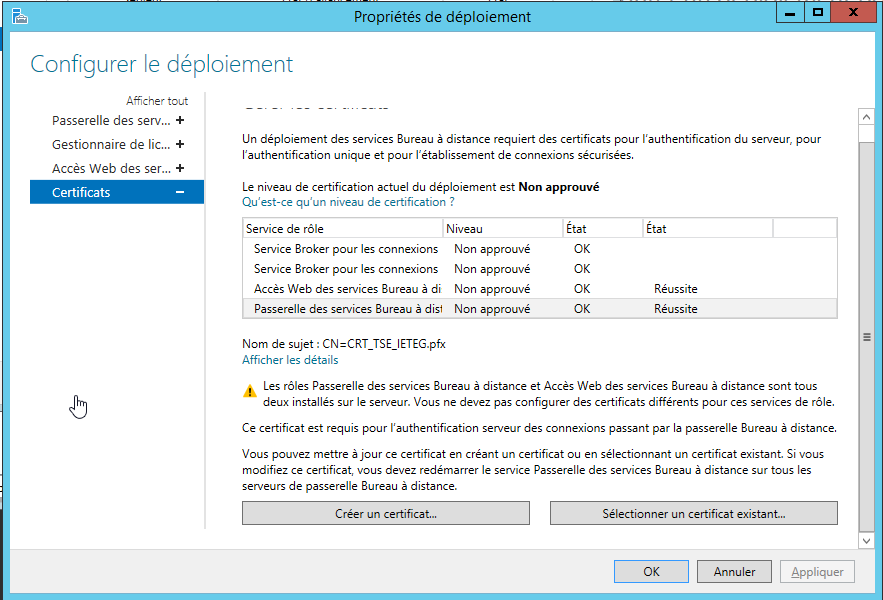
Il y a au total, quatre « rôles » demandant un certificat, il suffit de leur donner celui précédemment créé



Puis, à l’étape suivante, on choisit notre serveur comme serveur « Passerelle de connexion Bureau à distance ».



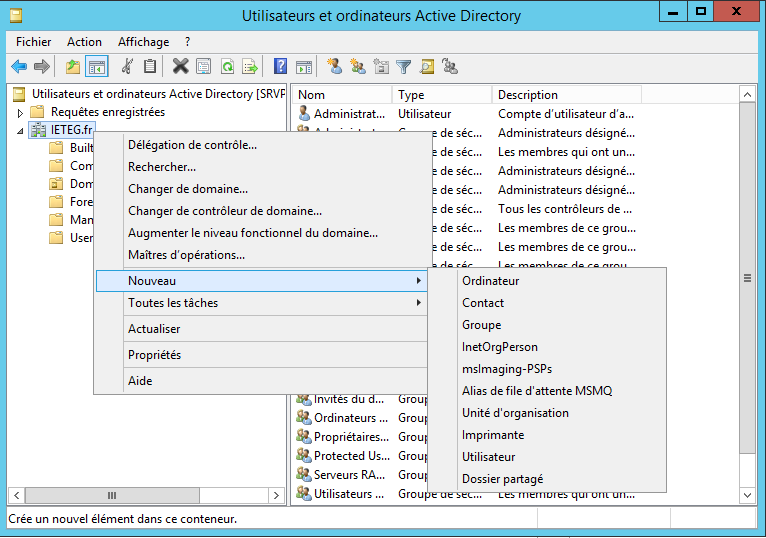
  
Enfin, on sélectionne le mode de licence. Ici nous choisissons de le gérer par utilisateurs car les personnes étant susceptible de venir sur site peuvent venir avec leur propre ordinateur.



Puis OK, tout est bon !

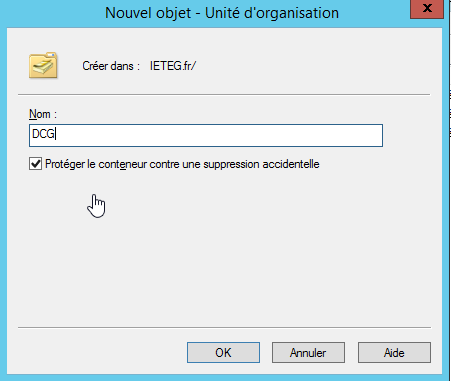
Puis nous allons choisir quel groupe de l’Active Directory disposera des accès. N’étant pas encore créé, nous allons devoir mettre en place un groupe « TSE ».

Groupes et Utilisateurs

Rendez-vous dans le gestionnaire de l’AD « Utilisateurs et ordinateurs Active Directory »  
  


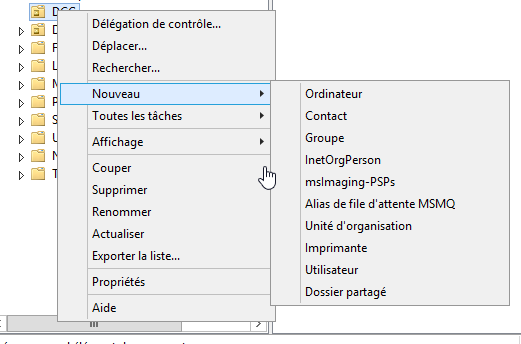
On déroule l’arborescence lié à notre domaine « IETEG.fr », clic droit 🡪 « Nouveau » 🡪 « Unité d’organisation ».

Dans un premier temps, nous allons créer une « UO » : « DCG ».  
Celle-ci aura pour fonction de gérer les droits de manière générale sur l’ensemble des utilisateurs du parc.

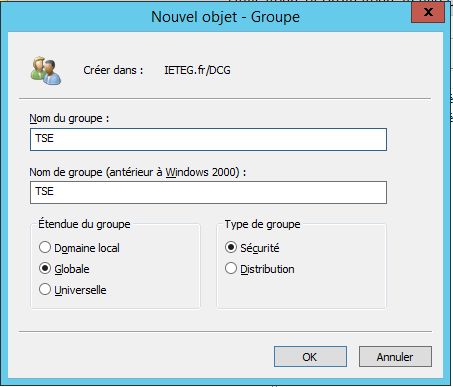


Cette « UO » se situe au même niveau dans l’arborescence que « Domain ».  
On laisse cocher l’option, elle permet d’éviter de supprimer accidentellement des données.

Il faut maintenant définir un groupe spécifique d’utilisateur qui pourra utiliser la prise en main à distance des Appliance.  
AU passage, nous créerons dans la même occasion, les trois groupes demandé dans le cahier des charges : GRP1 ; GRP2 ; et celui qui nous intéresse actuellement : TSE.

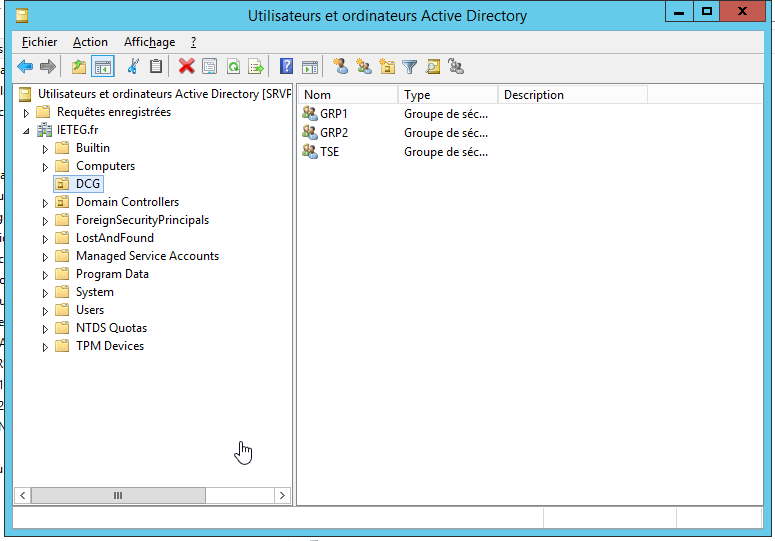


Clic droit sur notre « UO », dans « Nouveau » 🡪 « Groupe »



On laisse tout par défaut, puis on répète l’opération pour les deux groupes suivants.

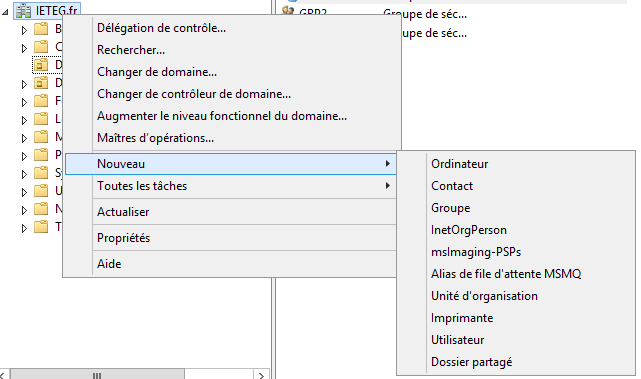
Nous obtenons alors le résultat suivant :

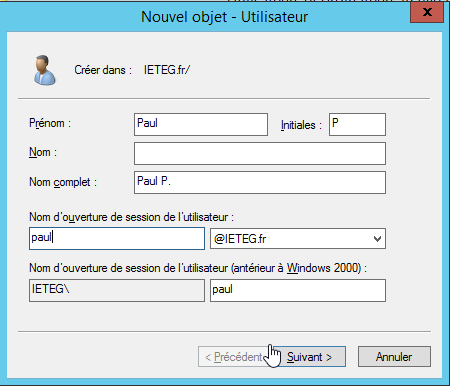


De la même façon, nous pouvons créer les utilisateurs :

Paul, Pierre, Isabelle, Nathalie, Jacques (qui sera dans l’UO DCG)  
  
Paul, Nathalie et Isabelle seront dans le groupe GRP1

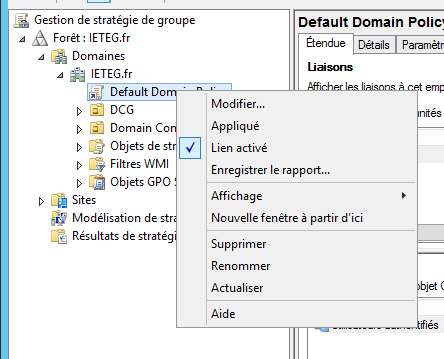
Jacques et Pierre dans le groupe GRP2  
Et l’ensemble des utilisateurs dans le groupe TSE.

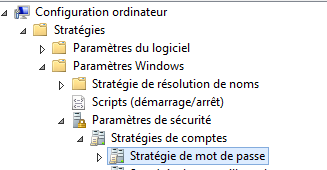




Il nous faut en revanche modifier notre stratégie de sécurité vis-à-vis des mots de passe. Dans le cahier des charges, il est demandé un minimum de 4 caractères et de ne pas gérer l’historique.

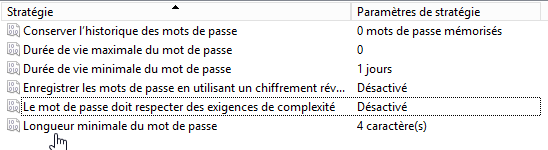
# GPO

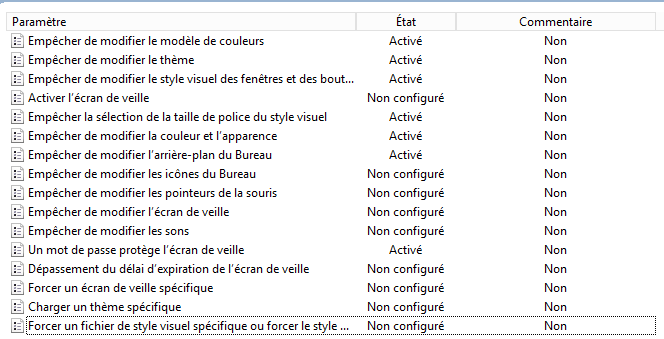
  
On clique sur « Modifier »



Puis on déroule les menus :

Configuration ordinateur 🡪 Stratégie 🡪 Paramètres Windows 🡪 Paramètres de sécurité 🡪 Stratégie des comptes 🡪 Stratégie de mot de passe.





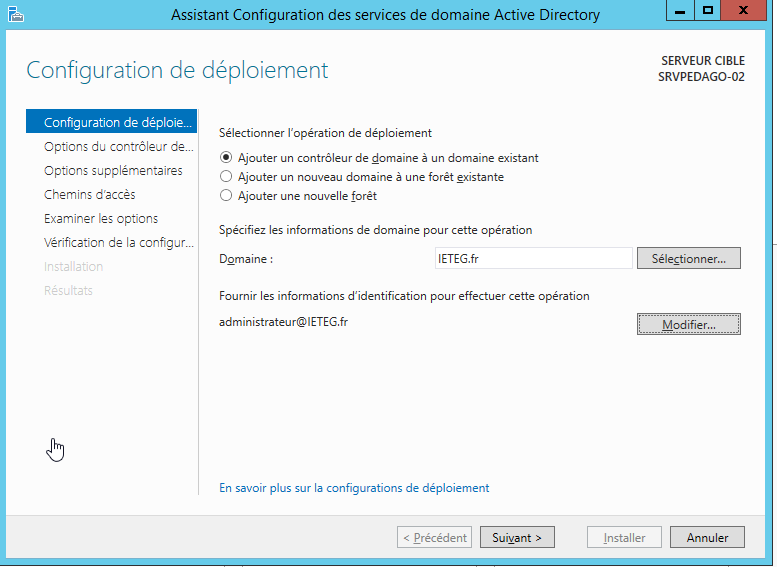
Dans les GPO (Stratégie de groupe) nous devons modifier quelques paramètres :

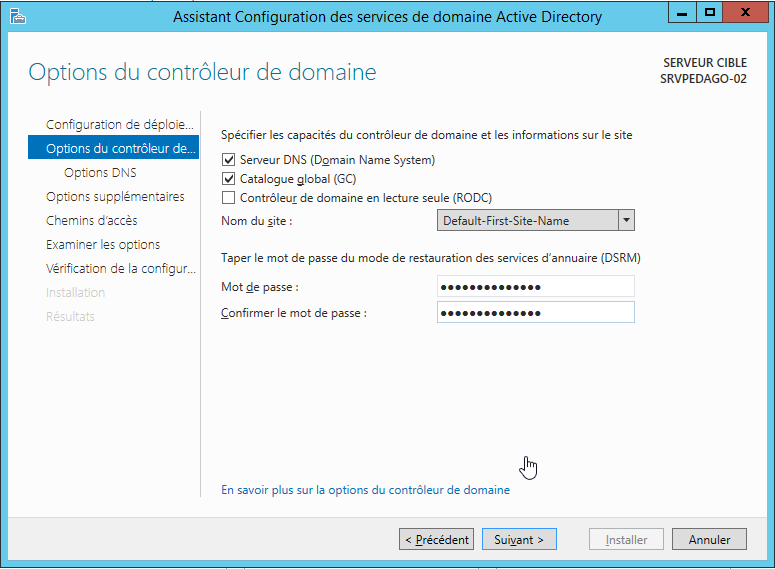
Interdire la modification des paramètres d’affichage,  
Toujours avoir le même fond d’écran,  
La menu démarrer et la panneau de configuration au format classique,  
Le login de l’utilisateur ne devra pas être apparent,

# Redondance sur le SRV 2 : SRVPEDAGO-02

## AD DNS

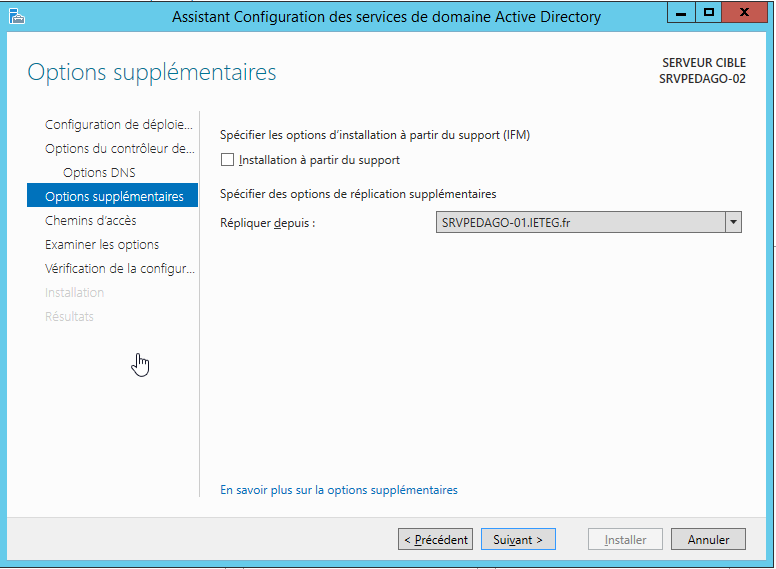
Pour assurer la redondance de l’Active Directory ainsi que du domaine, il suffit de configurer le rôle sur le serveur deux.  
  
En revanche, nous n’allons pas créer une nouvelle forêt mais bien rejoindre un domaine déjà existant !





On entre le mot de passe défini sur le serveur 1 ;

Puis on passe le menu suivant, et enfin :

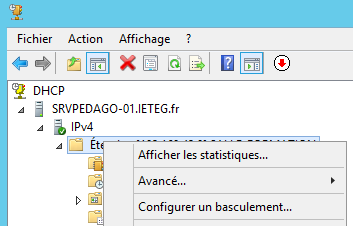


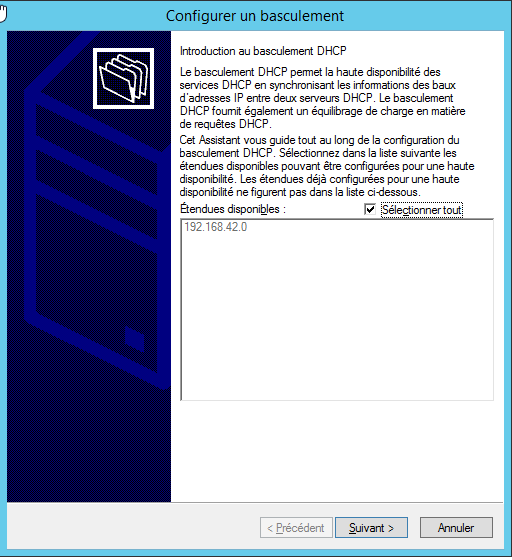
On choisit de répliquer l’AD du serveur 1.   
Et on installe le rôle.  
Et c’est tout. La réplication peut demander quelques minutes.

## DHCP FailOver :

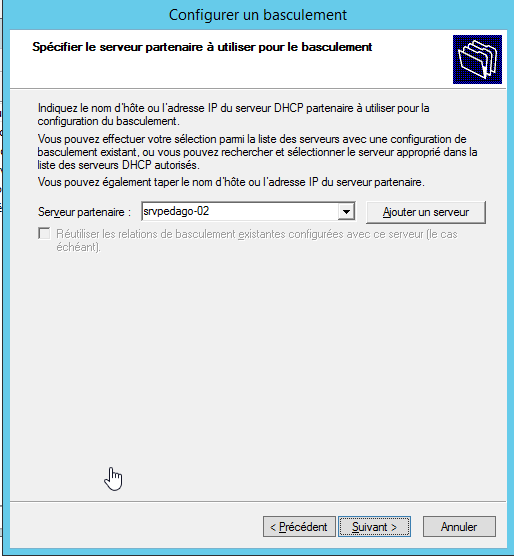
L’installation du rôle est identique au serveur 1.

Sur la gestion DHCP du serveur 1 ensuite, on clique sur « Configurer un basculement »

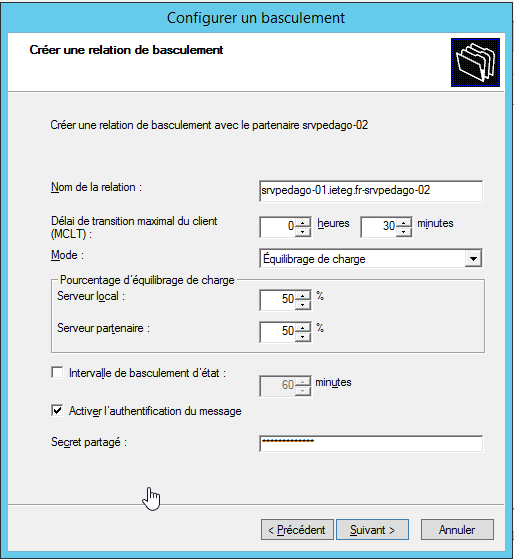




On entre le nom de notre second serveur :



Puis une petite configuration :



Et c’est fini, il n’y a plus qu’à attendre un peu.

RADIUS  
  
Il suffit d’ajouter le rôle et de le configurer comme dans le serveur 1

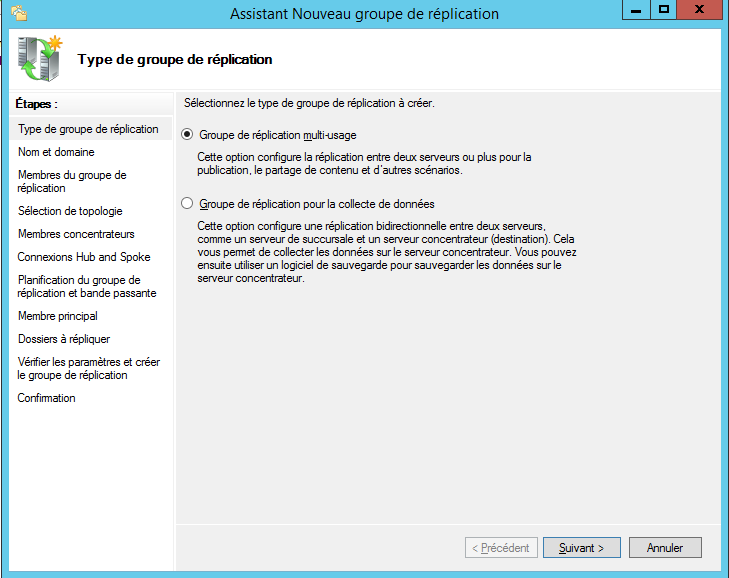
## DFS/DFSR

Il faut installer sur les deux serveurs le rôle « Réplication DFS » (en plus de DFS sur le second serveur).

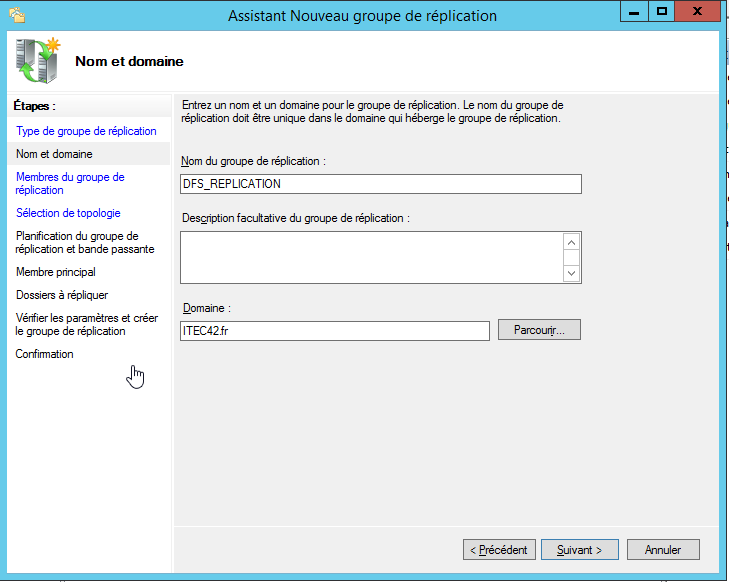
Sur le premier, rendez-vous dans le gestionnaire DFS puis :



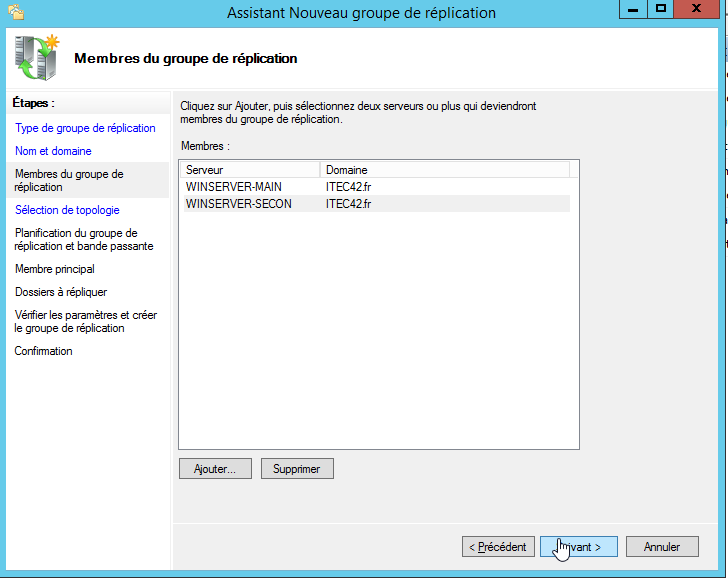
Clic droit sur « Réplication », « Nouveau groupe de réplication »

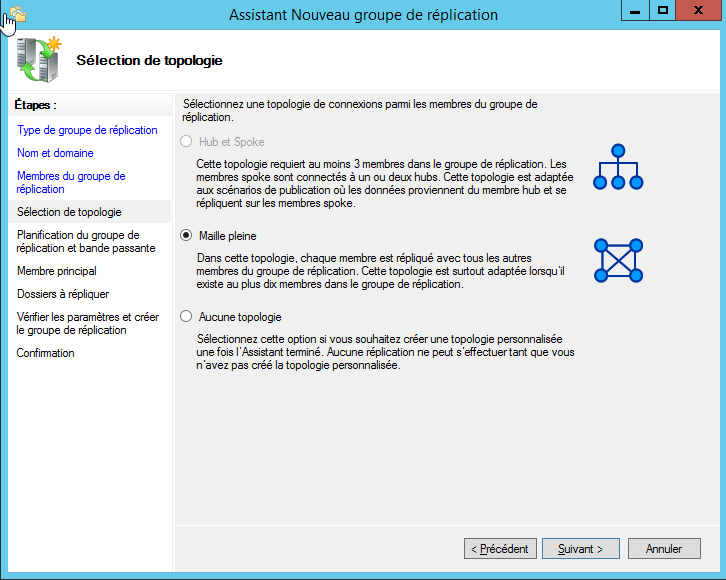
On sélectionne « Groupe de réplication multi-usage » 

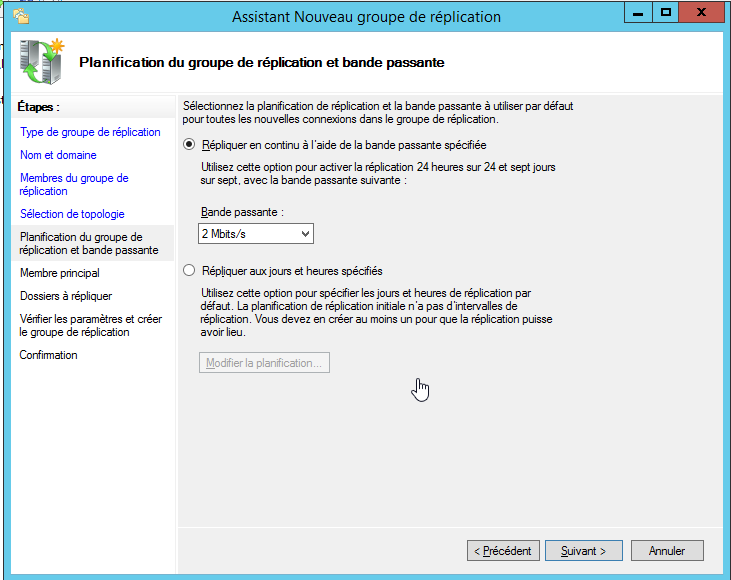
On donne un nom à la réplication :

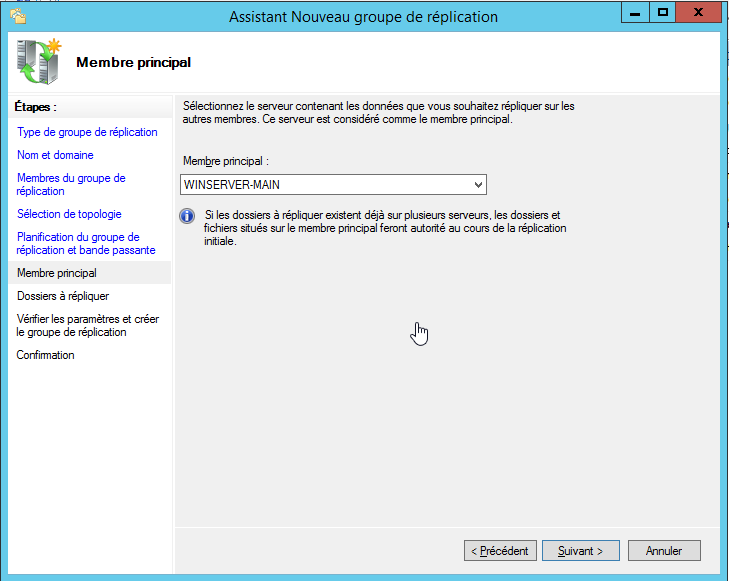


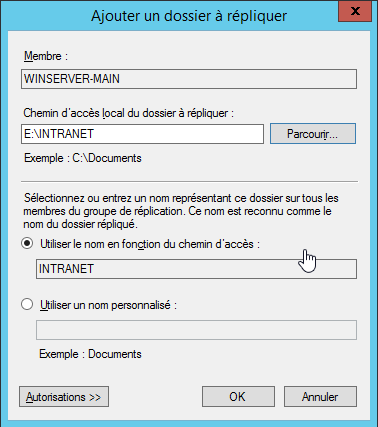
On choisit notre serveur source :



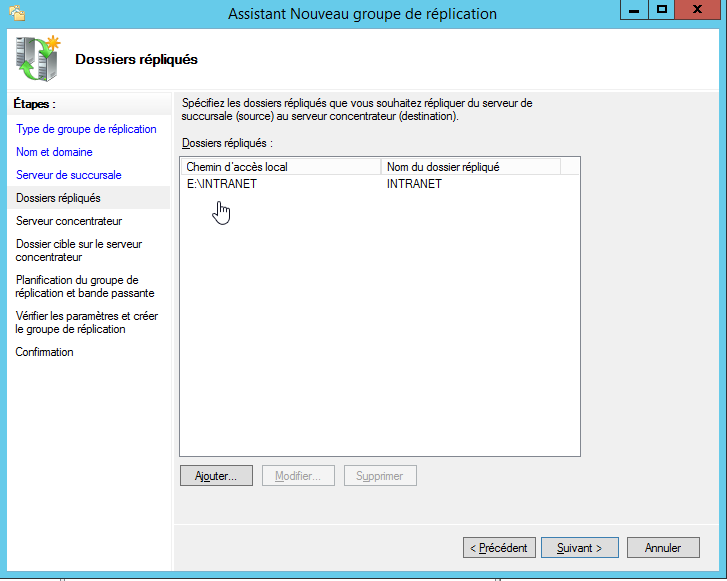




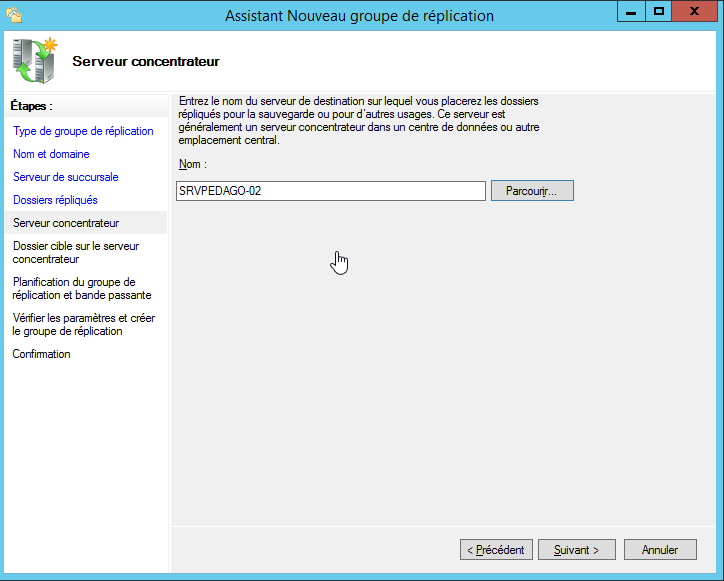




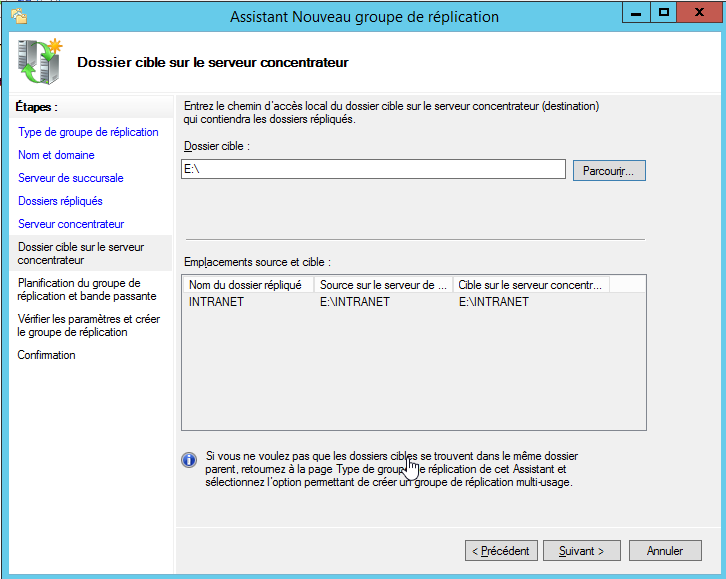
On sélectionne le dossier INTRANET



Le serveur de destination (SRVPEDAGO-02)

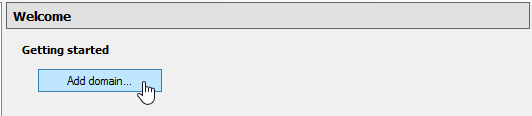


On choisit le disque E:\DATAS

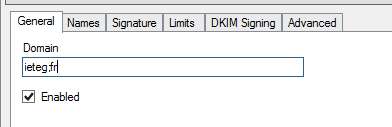


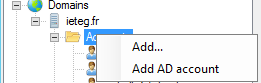
Puis on fait suivant, jusqu’à la fin où une vérification à lieu et tout est OK.

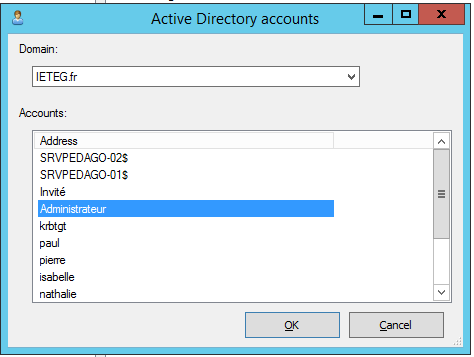
# SERVEUR MAIL : HMAILER



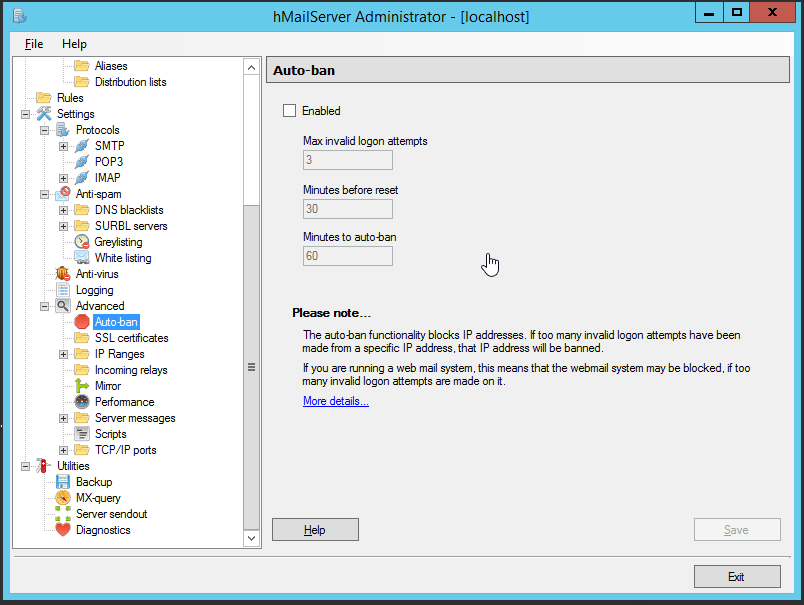
Dans le menu « Welcome », ajouter un domaine : « ieteg.fr



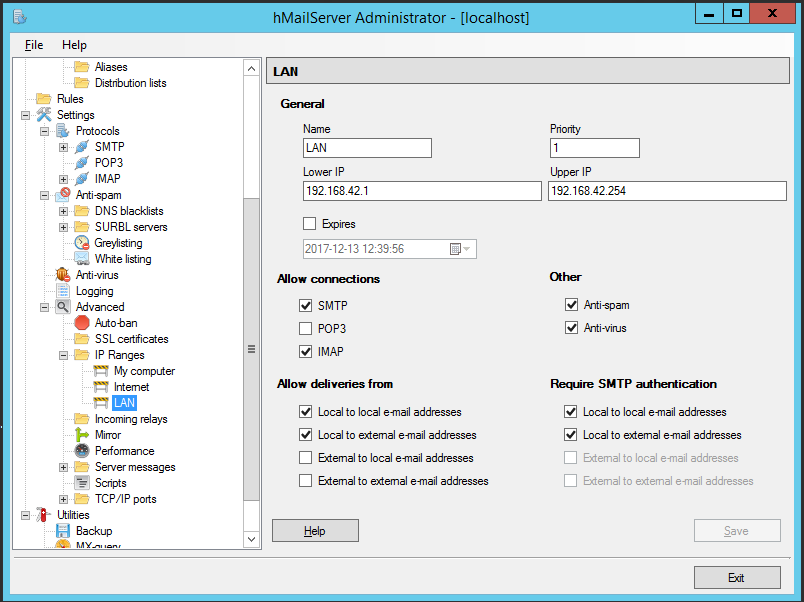
Puis, dans « account », choisir « Add AD account »



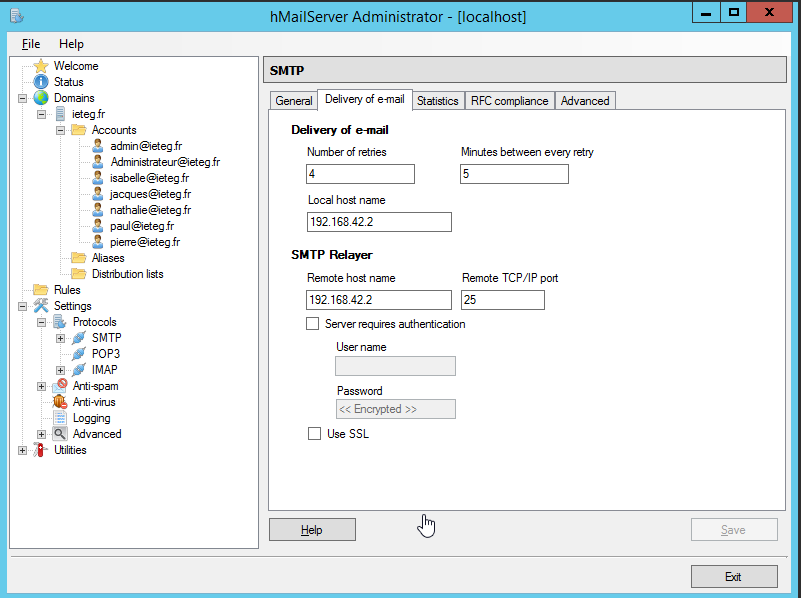
Prendre le compte administrateur.



Il faut désactiver l’Auto-ban dans le menu « Advanced »



Configurer le LAN dans « Advanced » 🡪 « IP Ranges »



Ainsi que les paramètres du serveur SMTP. On indique donc l’adresse IP du serveur qui délivrera les mail.

