Nous allons installer sur deux serveurs Active Directory avec une réplication RODC sur un système d'exploitation dénommé Windows Serveur 2012 R2. Pour cela, il faudra mettre en place sur ce système les fonctionnalités Active Directory sur les deux machines et les relier.

## Sommaire

# 1 Installation du système Windows Serveur 2012 R2

Après avoir crée une clé bootable grâce à l'ISO de la version du système, insérer la clé et démarrer la machine ce même périphérique.

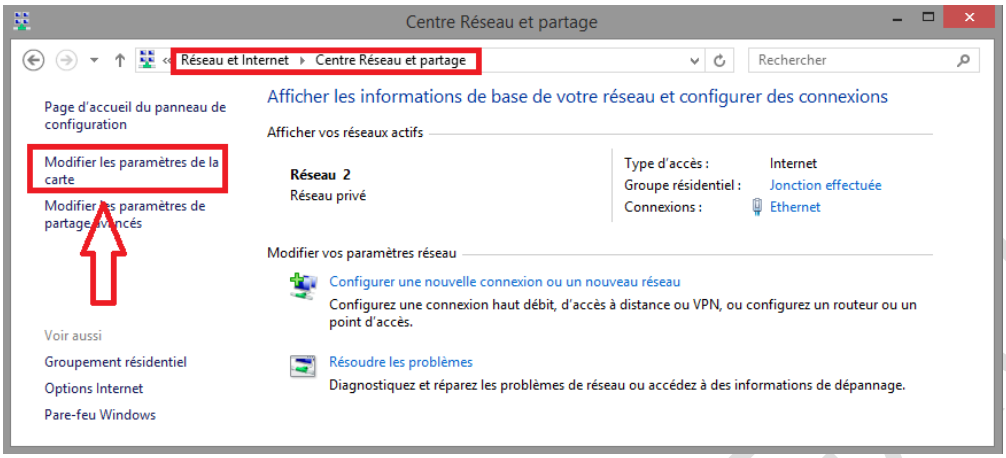

Il suffit de sélectionner les différents paramètres à chaque étape. Windows explique de façon simple la démarche à suivre.

# 2 Configurer le système

## 2.1 Configurer une IP statique

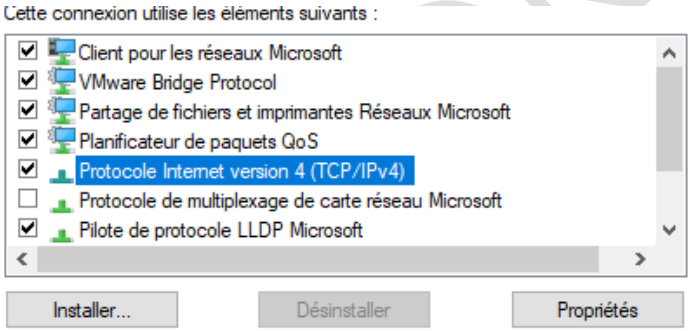
Avant d'installer des fonctionnalités à ce serveur, il faut lui mettre une IP statique. Pour cela, effectuer un clic droit sur l'icone de connexion et sélectionner ***centre de réseau et partage.***

Sélectionner ensuite ***modifier les paramètres de la carte.***

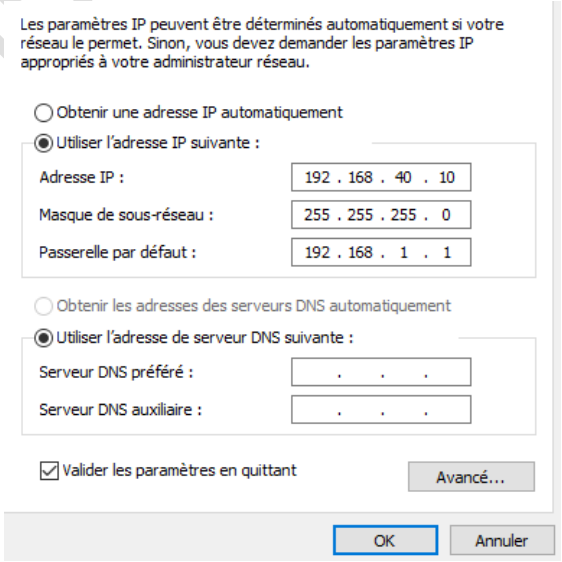



Effectuer un clic droit sur la carte réseau Ethernet et cliquer sur ***propriété.***

Sélectionner l'élément concernant l'***IPv4*** et faire ***propriétés***.




Entrer une ***IP disponible*** dans le réseau dans lequel sera connecté le serveur ainsi que son ***masque***, sa ***passerelle*** et son ***DNS***. ***Ne pas oublier de cocher la case de validation*** !

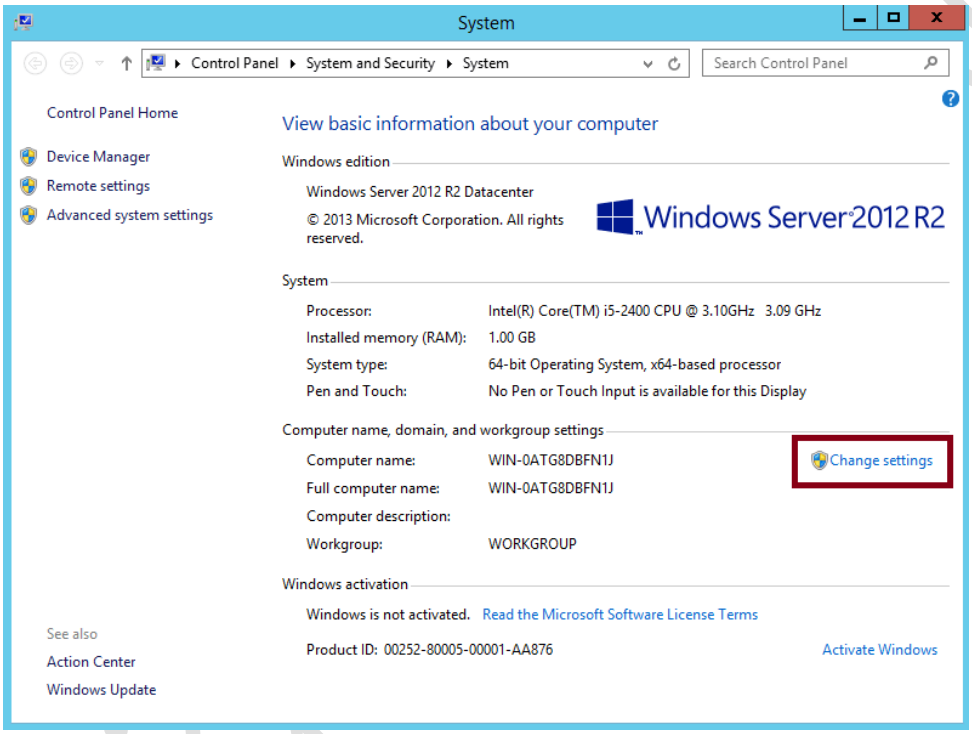


## 2.2 Renommer la machine

Le serveur possède actuellement un nom complexe. Pour le renommer, il suffit d'effectuer un clic droit sur le ***bouton démarrer***, puis sélectionner ***système***. Sur cette page, il est possible de changer le nom de la machine.

Ce nom ne peut pas comporter plus de 15 caractères ! Il est conseillé de la renommer de façon à connaitre sa fonction. *Exemple : WS2012R2-AD-DNS*.

Un redémarrage de la machine sera nécessaire pour appliquer les modifications.

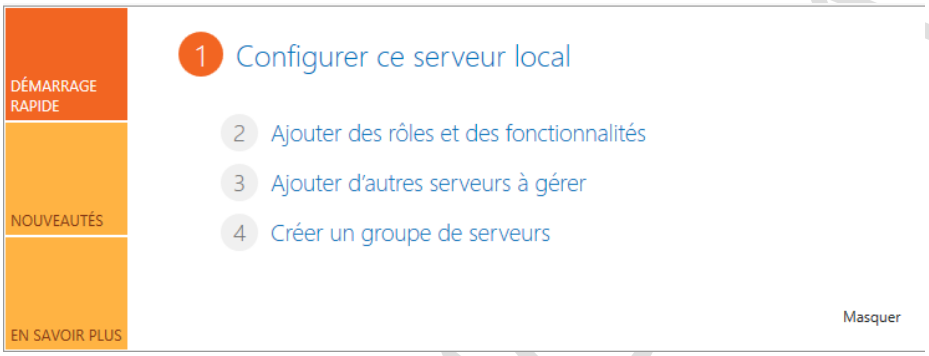


# 3 L'Active Directory

Active Directory (AD) est une fonctionnalité fournie par Microsoft ayant pour objectif fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows.

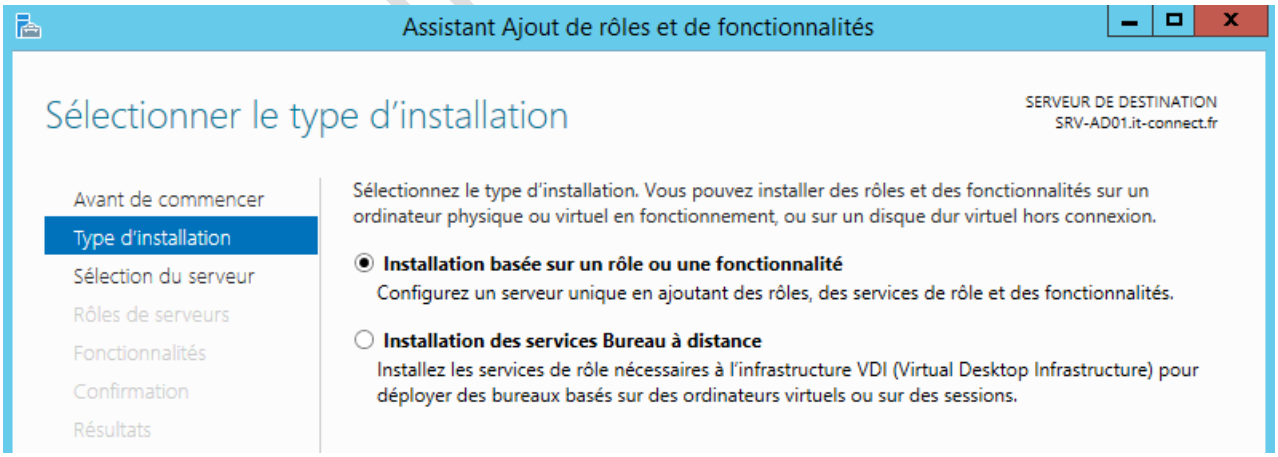
## 3.1 Installation de l'AD

Pour installer cette fonctionnalité, il faut aller dans le ***gestionnaire de serveur*** qui s'ouvre automatiquement au démarrage du système. Puis cliquer sur la rubrique ***Ajouter des rôles et des fonctionnalités***.



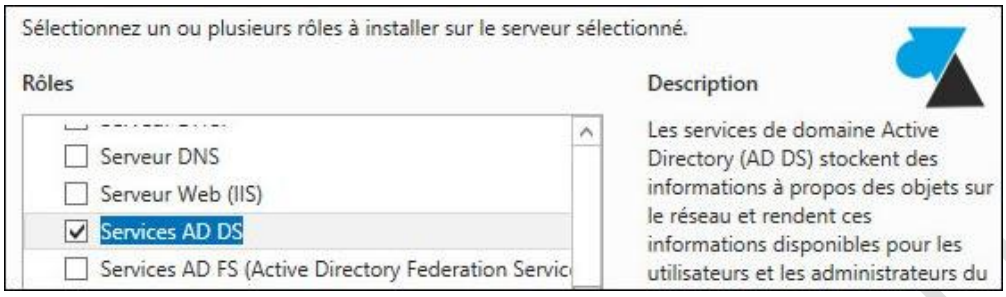

Une fenêtre d'assistance s'ouvre afin d'aider à l'installation des nouvelles fonctionnalités. Il faut suivre les différentes exigences de la rubrique ***Avant de commencer*** puis faire suivant.

Dans le type d'installation, sélectionner ***installation basée sur un rôle ou fonctionnalité.***




Dans ***Sélection du serveur***, sélectionner le serveur actuel.

Dans la rubrique **Rôle de serveurs**, cocher la case de **service AD DS**

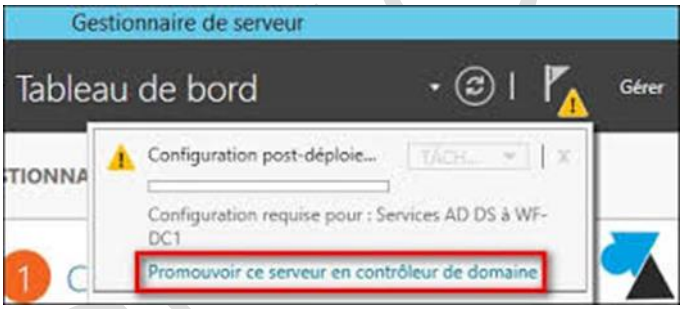



Pour la rubrique ***Fonctionnalités***, ne rien toucher et cliquer sur suivant.

L'assistant va vérifier si toutes les conditions sont réuni pour faire l'installation puis afficher le résultat. Il suffit de faire ***suivant*** et ***installer***.

## 3.2 Promouvoir l'AD

Une fois l'installation de l'AD effectué, il faut le promouvoir. C'est-à-dire de le configurer. Pour ce faire, aller sur le ***Gestionnaire de serveur*** et cliquer sur le ***drapeau*** en haut, puis sur ***promouvoir ce serveur en contrôleur de domaine***.




Cocher ***ajouter une nouvelle forêt*** et ***donner lui un nom*** puis faire suivant. Par exemple btssio1.lab.

Ensuite, mettre un ***mot de passe*** assez complexe puis faire suivant.

Pour les autres options, laisser comme c'est par défaut.

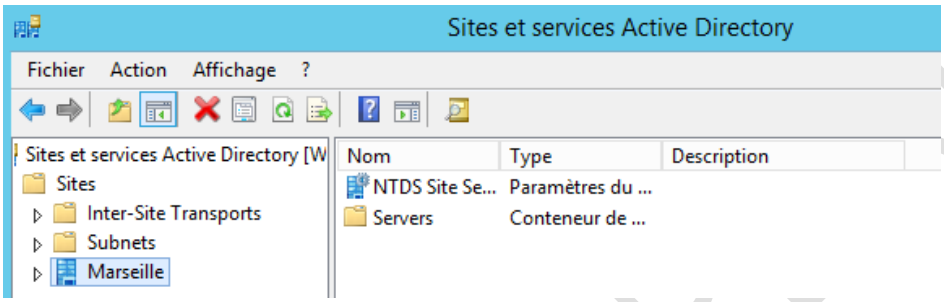
Effectuer les changements nécessaires comme indiquer dans la ***vérification***. Cette dernière étape indique les modifications à apporter de façon explicite.

## 3.3 Mettre en place d'un RODC

### 3.3.1 Mise en place de la première machine (AD1)

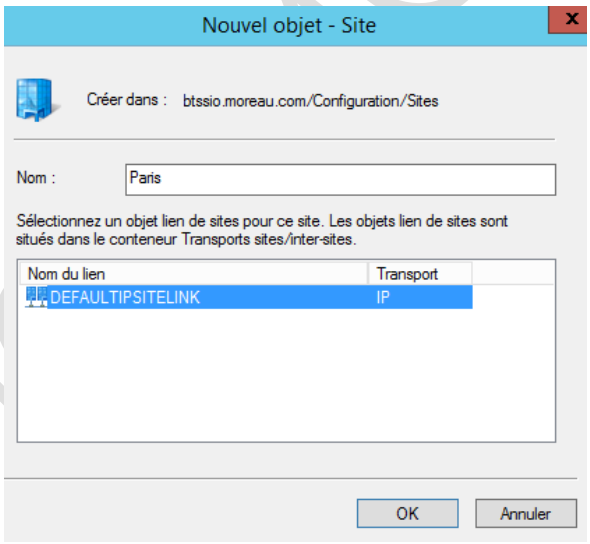
Ouvrir ***Sites et services Active Directory***.

Dérouler ***Sites*** puis faire un clic droit sur ***Default-First-Site-Name*** afin de le ***renommer***, en par exemple, Marseille.

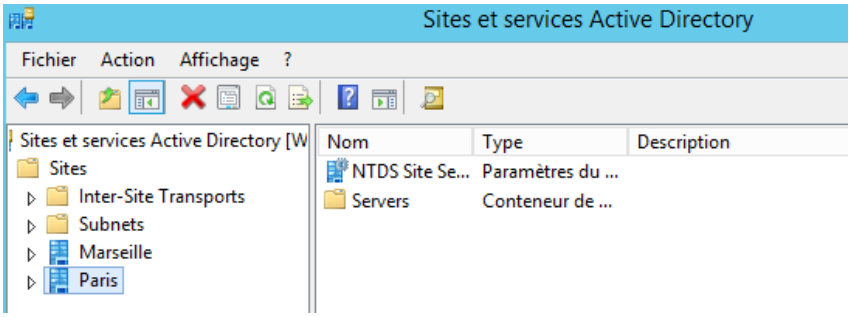



Faire un clic droit sur ***Sites*** puis sélectionner ***Nouveau*** et ***Sites***.

Saisir un ***nom*** dans le champ correspondant à cela puis cliquer sur ***DEFAULTIPSITELINK*** puis ***valider***.



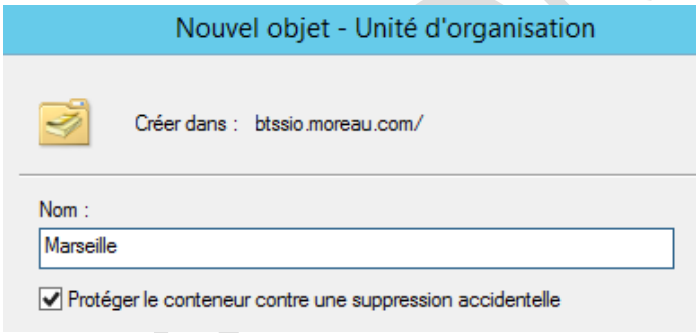

Voici ce qu'il faut obtenir :



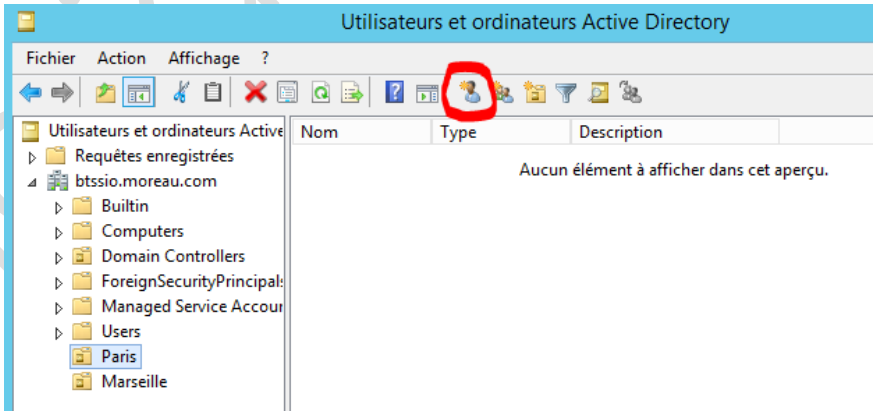

Démarrer la console dénommée ***Utilisateurs et ordinateurs Active Directory***, effectuer un clic droit sur le ***nom de la forêt*** (ici btssio.moreau.com) puis cliquer sur ***Nouveau – Unité d'organisation.***

Saisir dans le champ ***Nom***, le nom du ***nouveau site crée***, ici Paris.

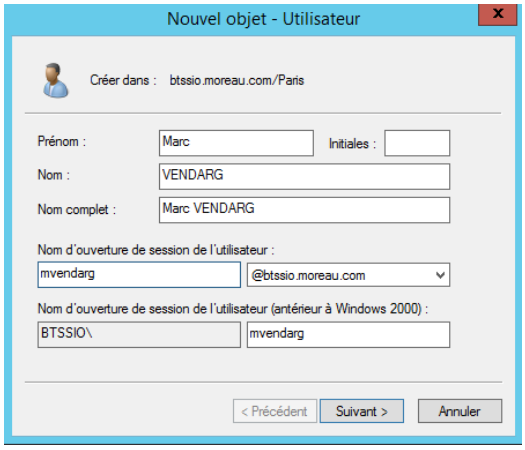
Faire la même étape pour le premier champ qui avait été renommé, ici Marseille.




Cliquer sur Paris, puis sur l'icone permettant de créer un nouvel utilisateur (Celui-ci se situe dans la barre d'outils).

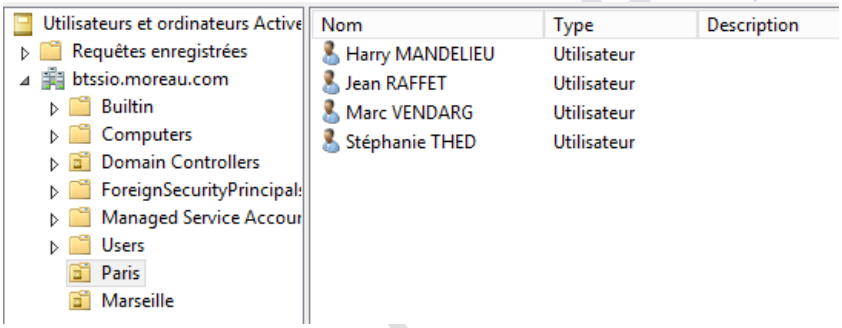



Il faut saisir un ***prénom***, un ***nom***, ainsi qu'un ***nom d'ouverture de session de l'utilisateur*** (un pseudo). Ici, cet utilisateur est Marc VENDARG. Puis faire ***suivant***.



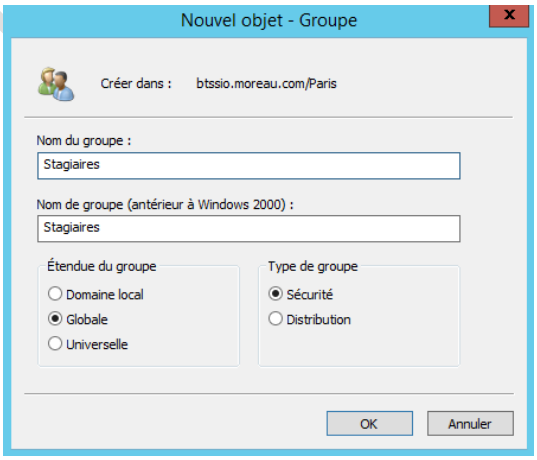

Dans l'onglet suivant, saisir le ***mot de passe de l'utilisateur*** crée avec les options souhaitées.

Créer autant d'utilisateur que souhaiter. Voici un exemple :



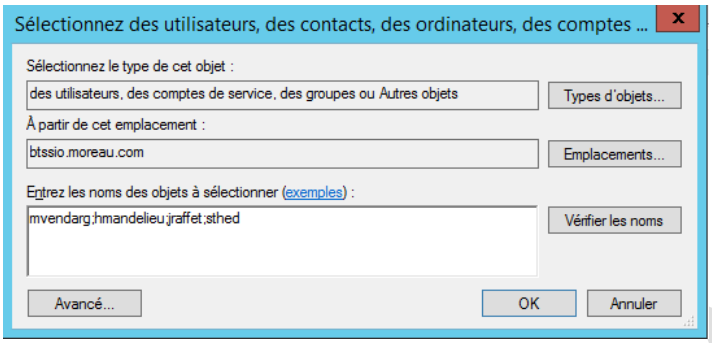

Cliquer à nouveau sur l'unité d'organisation qui possède les utilisateurs (ici Paris) puis sélectionner l'icone permettant de crée un groupe. 

Saisir le ***nom du groupe*** crée avec une étendue du groupe en ***globale*** et un type de groupe ***sécurité***. Puis valider.

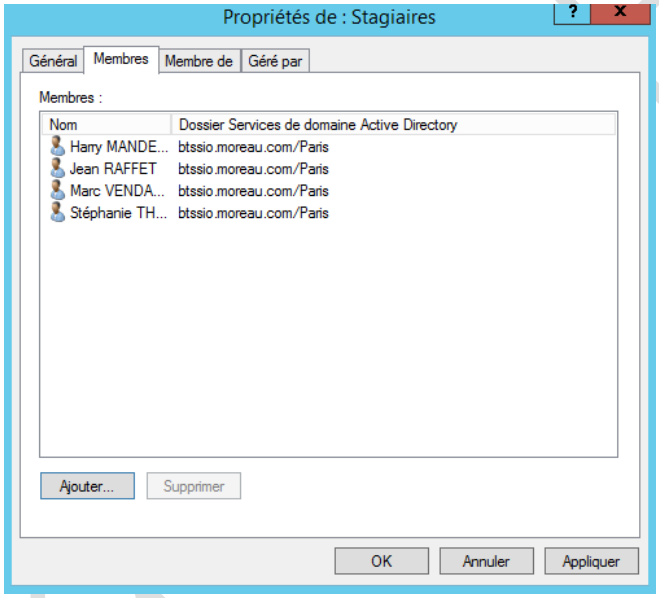



Faire un ***double clic*** sur le ***groupe crée***, puis aller dans ***l'onglet Membre***.

***Ajouter les membres*** de ce groupe grâce à leurs ***noms de session*** séparé par des ***point-virgule « ; ».*** Puis valider.



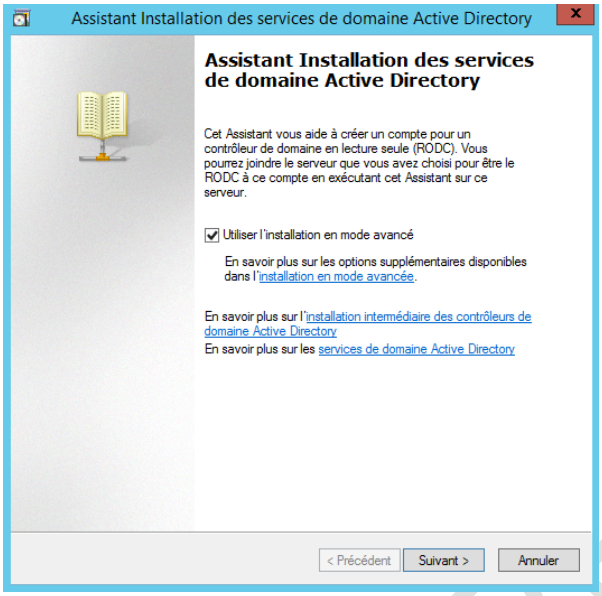

Voici le résultat :




Cliquer sur ***appliquer*** puis ***OK***.

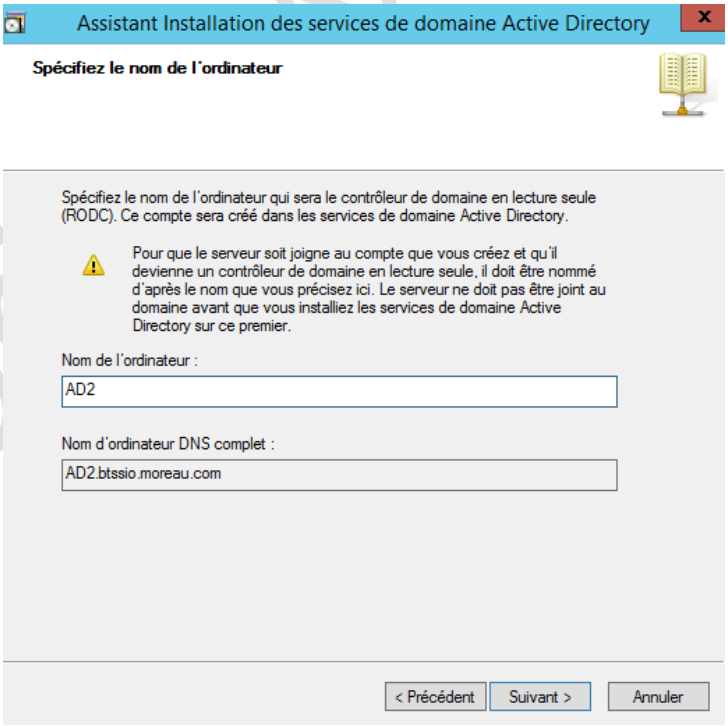
Faire un ***clic droit*** sur l'unité d'organisation ***Domains Controllers*** puis sélectionner ***Créer au préalable un compte de contrôleur de domaine en lecture seule***.

Cocher l'option ***Utiliser l'installation en mode avancé***, puis sur ***suivant***.

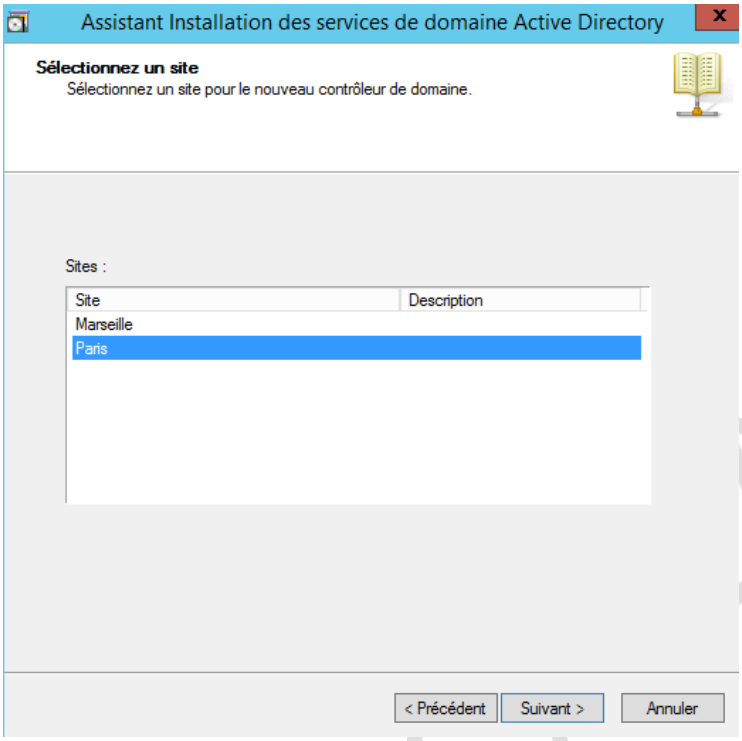



Dans la fenêtre suivante dénommée ***Information d'identification réseau***, laisser le choix par défaut et cliquer sur ***suivant***.

Dans la fenêtre ***Spécifiez le nom de l'ordinateur***, saisir le nom de la machine qui sera lier à la machine actuelle. Ici, AD2.

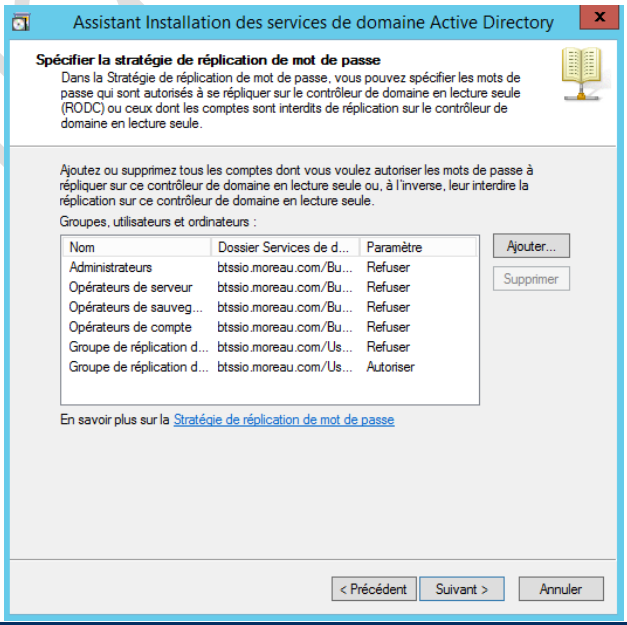



Sélectionner le site qui avait été crée précédemment, ici Paris et faire suivant.



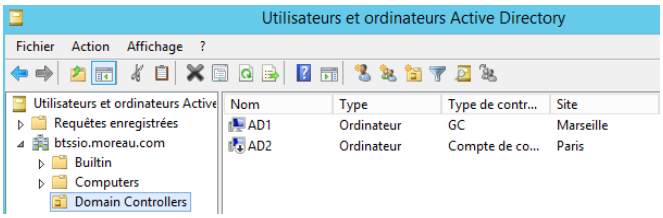

Dans la fenêtre ***Options supplémentaires pour le contrôleur de domaine***, laisser le choix par défaut et faire suivant.

La fenêtre ***Spécifier la stratégie de réplication de mot de passe*** permet d'indiquer comment sont ***mis en cache les mots de passe***. Par défaut, les mots de passe des comptes ayant des droits d'administration (Opérateur, Administrateur…), ne sont pas mis en cache. Cliquer sur ***suivant***.



Dans la fenêtre ***Délégation de l'installation et l'administration du RODC***, cliquer sur définir. Saisir un ***nom d'utilisateur***, ici mvendarg, puis sur ***vérifier les noms***.

Cliquer sur ***OK*** puis sur ***suivant***, enfin, ***lancer l'installation*** et cliquer sur ***terminer*** pour quitter l'assistant.




### 3.3.2 Mise en place de la second machine (AD2)

Penser à bien ***régler l'IP*** du ***DNS*** de la seconde machine vers la première. Ici, AD1 est 172.16.0.1 donc le DNS de AD2 est aussi 172.16.0.1. De plus, il faut aller dans les ***options avancées***, puis dans ***l'onglet DNS***, on ajoute le ***suffixe*** qui est le ***nom de domaine*** (la forêt). S'il y a un problème, mettre en ***premier*** DNS le ***127.0.0.1*** et en ***second***, ***l'IP de l'AD1***.

Sur cette machine renommée ici en AD2, ouvrir une session puis cliquer sur ***Ajouter des rôles et des fonctionnalités*** dans la fenêtre ***Gestionnaire de Serveur***.

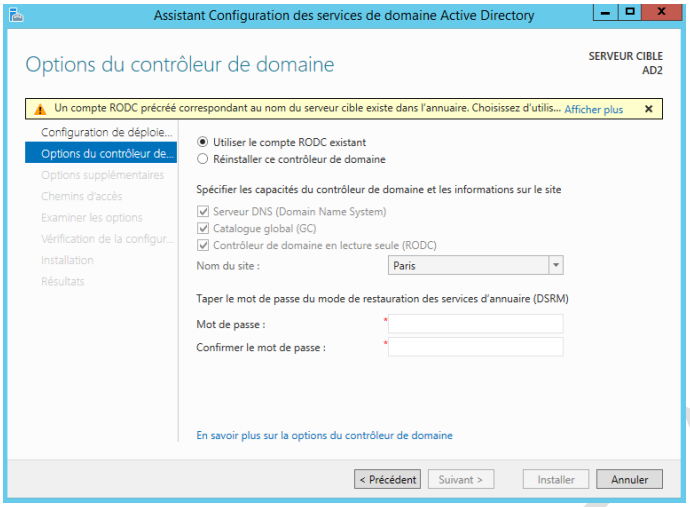
Installer les ***services AD DS*** comme sur la première machine.

Cliquer sur ***Promouvoir ce serveur en contrôleur de domaine***

L'assistant ce lance et cliquer sur sélectionner puis authentifier le nom de la forêt de la première machine \ l'utilisateur auparavant mis dans la fenêtre : ***Délégation de l'installation et l'administration du RODC***. Ici, cela donne btssio.moreau\mvendarg avec le mot de passe de l'utilisateur, ici Pa$$word.

Faire ***suivant***.

Dans ***Options du contrôleur de domaine***, crée un nouveau ***mot de passe*** dans ***Taper le mot de passe du mode de restauration des services d'annuaire (DSRM).***




Cliquer sur ***suivant.***

Au niveau des fenêtres ***Options supplémentaires***, ***Chemins d'accès*** et ***Examiner les options***, laisser les ***paramètres par défaut.***

Puis procéder à la promotion avec le bouton ***Installer***.

***Redémarrer la machine*** (ici AD2) en ouvrant la session en tant que ***nomdedomaine\utilisateur*** et son ***mot de passe*** associé (ici, btssio.moreau\mvendarg Pa$$word).

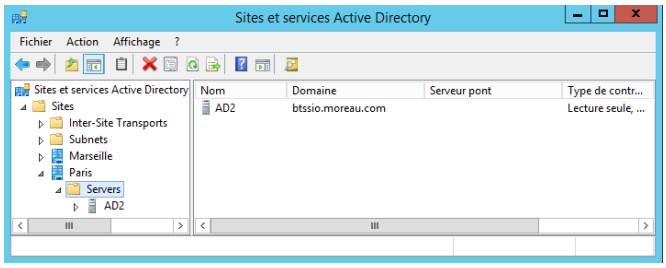
Le contrôleur de domaine est bien en lecture seule. Il est impossible de créer un utilisateur, un groupe… Les options sont maintenant grisées.

Par défaut, la fenêtre se connecte au contrôleur de domaine en mode lecture/écriture. Pour que la console se connecte au RODC, faire un clic droit sur le domaine est cliquer sur l'option ***Changer de contrôleur de domaine***.

Le serveur DNS est lui aussi en lecture seule.

### 3.3.3 De retour sur la première machine (AD1)

Sur la première machine (ici, AD1), lancer la console ***Sites et services Active Directory.*** Développer les nœuds ***sites***, la ***forêt créée*** (ici, Paris) puis ***Servers*** et ***vérifier*** la présence de la **seconde machine** (ici, AD2).



Lancer la console ***Utilisateurs et ordinateurs Active Directory*** sur la première machine (ici, AD1).

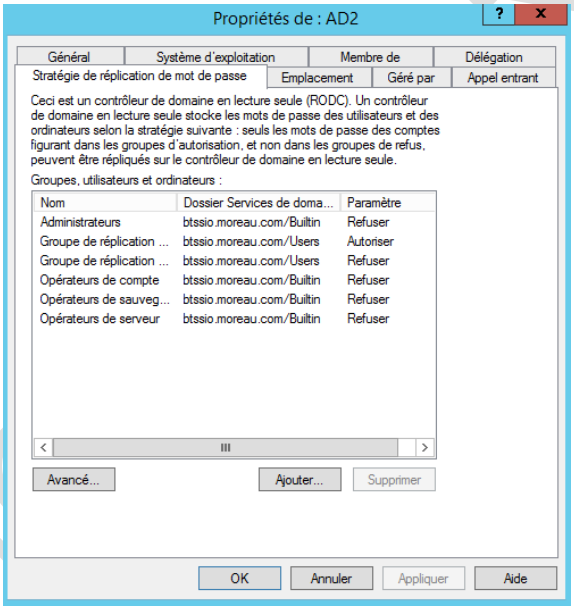
Développer les nœuds de la ***forêt*** (ici, btssio.moreau.com) puis le dossier ***Users.***

Ensuite, double cliquer sur ***Groupe de réplication dont le mot de passe RODC est autorisé*** puis cliquer sur l'onglet ***Membre.***

Cliquer sur ***Ajouter***, et saisir ***tous les utilisateurs*** séparés par des points-virgules « ; » (ici, jraffet;hmandelieu;sthed;mvendarg), puis cliquer sur ***Vérifier les noms.***

Puis valider.

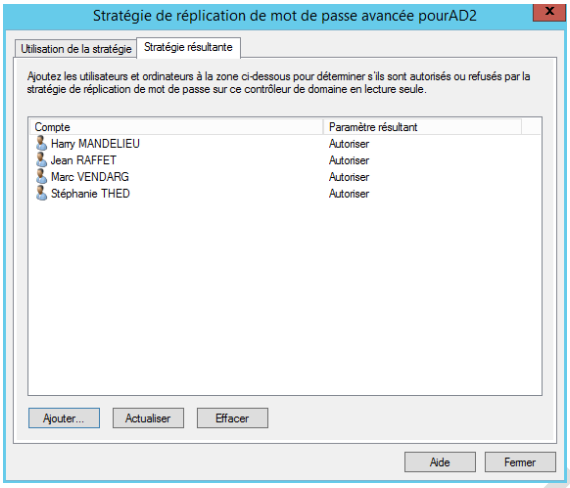
Sélectionner l'unité d'organisation ***Domain Controllers***, puis double cliquer sur le ***nom de la seconde machine*** (ici, AD2) et aller dans l'onglet ***Stratégie de réplication de mot de passe.***




Cliquer sur le bouton ***Avancé***, et ensuite sur ***Stratégie résultante***.

Cliquer sur ***Ajouter***, saisir ***tous les utilisateurs*** séparés par des points-virgules « ; » (ici, jraffet;hmandelieu;sthed;mvendarg), puis ***vérifier les noms***.

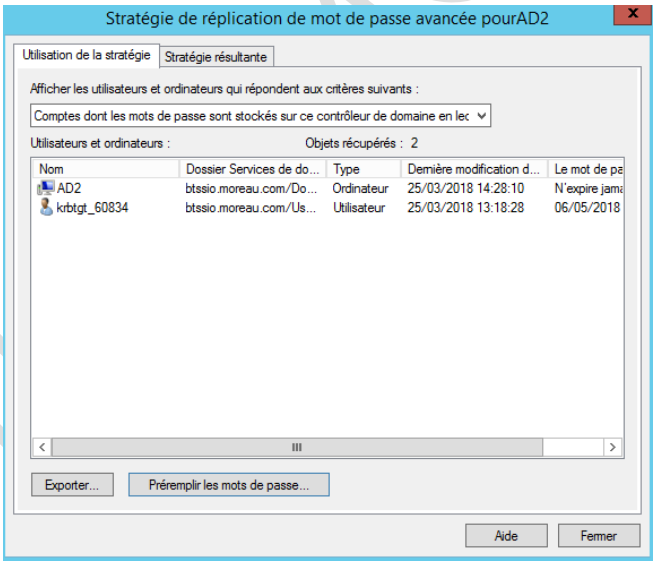
Enfin, cliquer sur ***OK***, le résultat ***Autoriser*** s'affiche.




Le mot de passe des comptes utilisateurs sera mis en cache lors de la prochaine réplication ou connexion utilisateur.

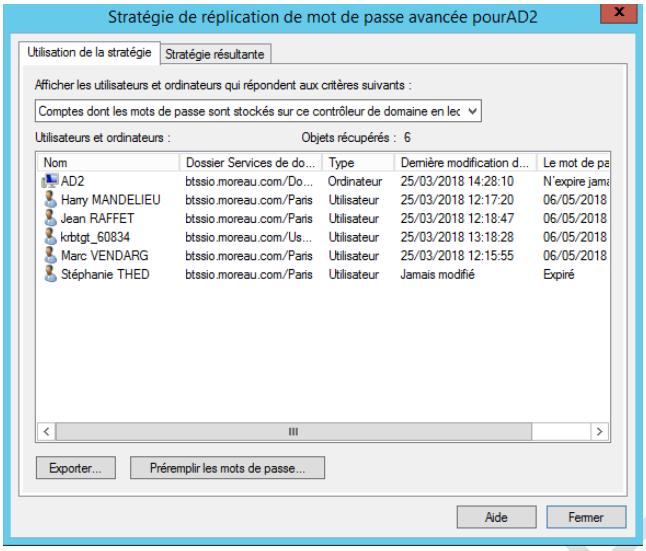
Dans certaines situations, il peut être utile de « forcer » cette mise en cache sans avoir à attendre la réplication ou la connexion utilisateur.

Sélectionner l'onglet Utilisation de la stratégie et cliquer sur Préremplir les mots de passe.




Saisir ***tous les utilisateurs*** séparés par des points-virgules « ; » (ici, jraffet;hmandelieu;sthed;mvendarg), puis ***vérifier les noms***.

Faire ***OK*** puis ***Oui*** dans la fenêtre qui s'affiche.




Le contrôleur de domaine en lecture seule peut désormais authentifier ces comptes mêmes si une coupure de la liaison avec le contrôleur de domaine en lecture/écriture a lieu.