

Windows Serveur 2012.

Présentation :

Windows Serveur 2012 est une nouvelle version de Windows Server qui apporte de nombreuses nouveautés qui permettent de rendre les serveurs plus évolutifs, virtualisables (Hyper-V) et favorise les évolutions vers les cloud.

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. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes,

Objectif :

Installer et configurer un autre Windows Serveur 2012 pour faire de la réplication Active Directory.

Pré requis :

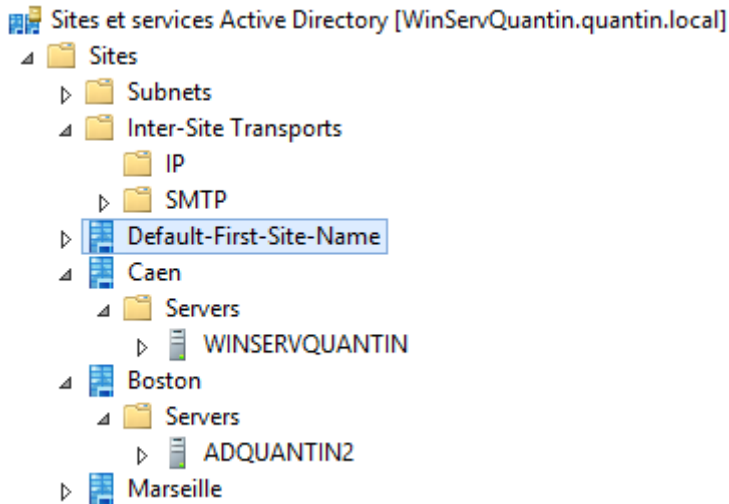
- Avoir une connexion internet
- Avoir deux IP fixe pour les Windows Serveurs.
- Ma machine s'appelle WinServQuantin et son @IP est 192.168.1.134/24
- Mon second AD s'appelle ADQuantin2 et son @IP est 192.168.1.135/24
- Le troisième (RODC) s'appelle ADQuantin3 et son @IP est 192.168.1.136/24
- Le nom de domaine est quantin.local

Sommaire :

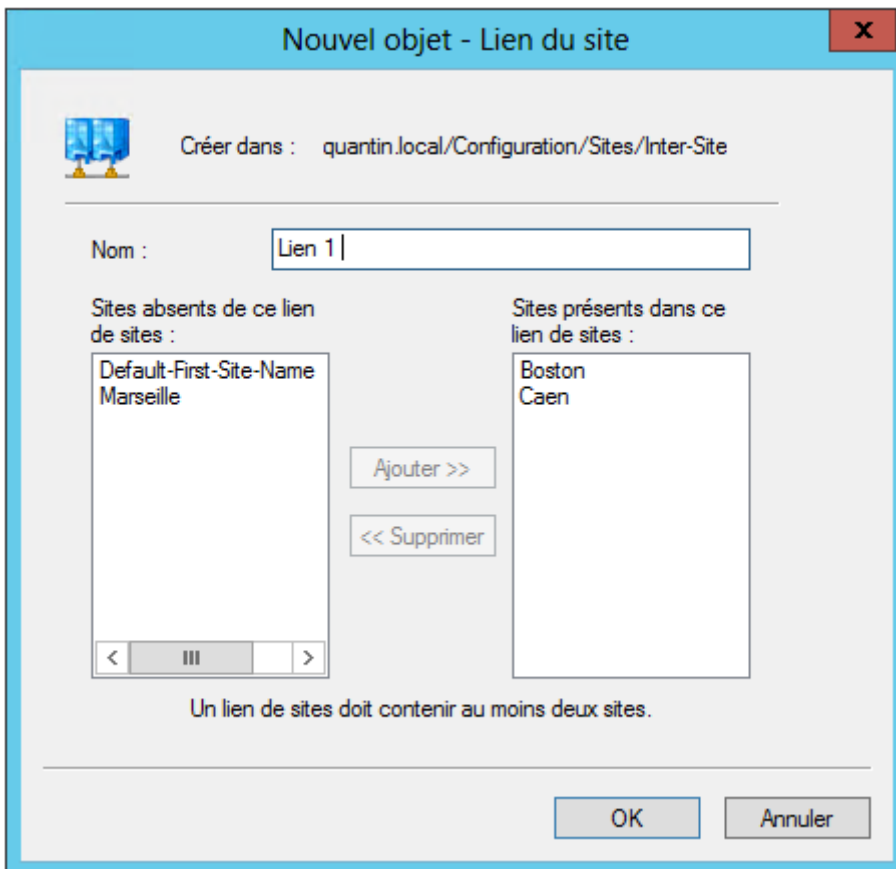
- I) Configuration des Sites
- II) Test de la réplication
- III) Configuration de la stratégie RODC

I) Configuration des sites

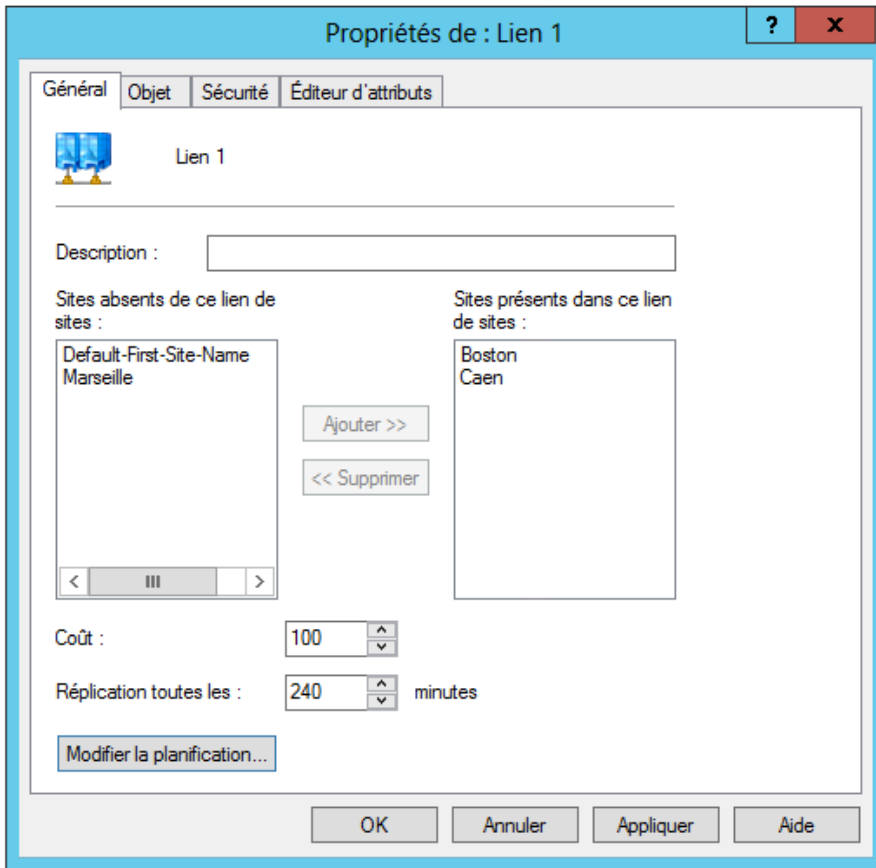
On va dans l'outil « Site et services Active Directory » afin de créer trois sites depuis le principal, Caen pour le principal, Boston pour le second et Marseille pour le RODC :



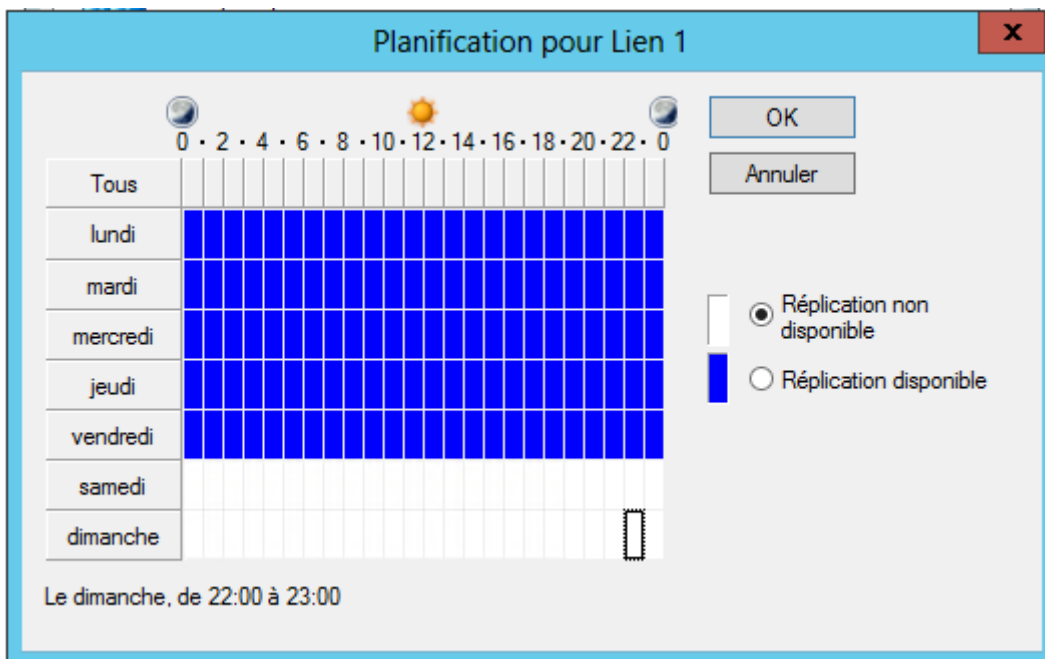
On crée un lien du site entre Caen et Boston :



On peut modifier le temps de réplication, ici 240 minutes :



Et on peut aussi modifier la planification horaire des réplifications :



II) Test sur la réplication

Via le Cmd :

repadmin /showrepl NomduServeur afficher les partenaires

```
C:\Users\Administrateur>repadmin /showrepl winServQuantin
Caen\WINSERUQUANTIN
Options DSA : IS_GC
Options de site : (none)
GUID de l'objet DSA : cc8e5efb-258a-4348-a122-6ea49574f547
ID de l'invocation DSA : cc8e5efb-258a-4348-a122-6ea49574f547

=== INSTANCES VOISINES ENTRANTES ===

DC=quantin,DC=local
  Boston\ADQUANTIN2 via RPC
    GUID de l'objet DSA : 52f7aff1-7592-41e4-840b-2185bdf05858
    La dernière tentative, le 2015-12-03 10:07:00, a réussi.

CN=Configuration,DC=quantin,DC=local
  Boston\ADQUANTIN2 via RPC
    GUID de l'objet DSA : 52f7aff1-7592-41e4-840b-2185bdf05858
    La dernière tentative, le 2015-12-03 10:07:00, a réussi.

CN=Schema,CN=Configuration,DC=quantin,DC=local
  Boston\ADQUANTIN2 via RPC
    GUID de l'objet DSA : 52f7aff1-7592-41e4-840b-2185bdf05858
    La dernière tentative, le 2015-12-03 10:06:59, a réussi.
```

repadmin /showconn NomduServeur afficher les connexions

```
C:\Users\Administrateur>repadmin /showconn winServQuantin
Nom unique de base : CN=Caen,CN=Sites,CN=Configuration,DC=quantin,DC=local
==== OBJETS DE CONNEXION DU VÉRIFICATEUR DE COHÉRENCE DES DONNÉES =====
Connexion --
  Nom de la connexion.. : ff355167-32bd-4ff6-b517-01159f352f7a
  Nom du serveur DNS... : WinServQuantin.quantin.local
  Nom unique du serveur : CN=NTDS Settings,CN=WINSERUQUANTIN,CN=Servers,CN=Caen,CN=Sites,CN=Configuration,DC=quantin,DC=local
  Source : Boston\ADQUANTIN2
  Aucun échec.
  Type de transport : IP
  Options : isGenerated overrideNotifyDefault
  Contexte de nom des réplicas : DC=ForestDnsZones,DC=quantin,DC=local
  Raison : IntersiteTopology
    Le lien du réplica a été ajouté.
  Contexte de nom des réplicas : DC=DomainDnsZones,DC=quantin,DC=local
  Raison : IntersiteTopology
    Le lien du réplica a été ajouté.
  Contexte de nom des réplicas : CN=Configuration,DC=quantin,DC=local
  Raison : IntersiteTopology
    Le lien du réplica a été ajouté.
  Contexte de nom des réplicas : DC=quantin,DC=local
  Raison : IntersiteTopology
    Le lien du réplica a été ajouté.
1 connexions trouvées.
```

repadmin /syncall NomduServeur /A /e forcer la réplication

```
C:\Users\Administrateur>repadmin /syncall WinServQuantin /A /e
Synchronisation de tous les contextes de nom détenus sur WinServQuantin.
Synchronisation de la partition : DC=ForestDnsZones,DC=quantin,DC=local
MESSAGE DE RAPPEL : La réplication suivante est en cours :
```

dcdiag /test :topology vérifier la topologie de réplication

```
C:\Users\Administrateur>dcdiag /test:topology
Diagnostic du serveur d'annuaire
Exécution de l'installation initiale :
  Tentative de recherche de serveur associé...
  Serveur associé : WinServQuantin
  * Forêt AD identifiée.
  Collecte des informations initiales terminée.
Exécution des tests initiaux nécessaires
  Test du serveur : Caen\WINSERUQUANTIN
  Démarrage du test : Connectivity
  ..... Le test Connectivity
  de WINSERUQUANTIN a réussi
Exécution des tests principaux
  Test du serveur : Caen\WINSERUQUANTIN
  Démarrage du test : Topology
  ..... Le test Topology
  de WINSERUQUANTIN a réussi

  Exécution de tests de partitions sur ForestDnsZones
  Exécution de tests de partitions sur DomainDnsZones
  Exécution de tests de partitions sur Schema
  Exécution de tests de partitions sur Configuration
  Exécution de tests de partitions sur quantin
  Exécution de tests d'entreprise sur quantin.local
```

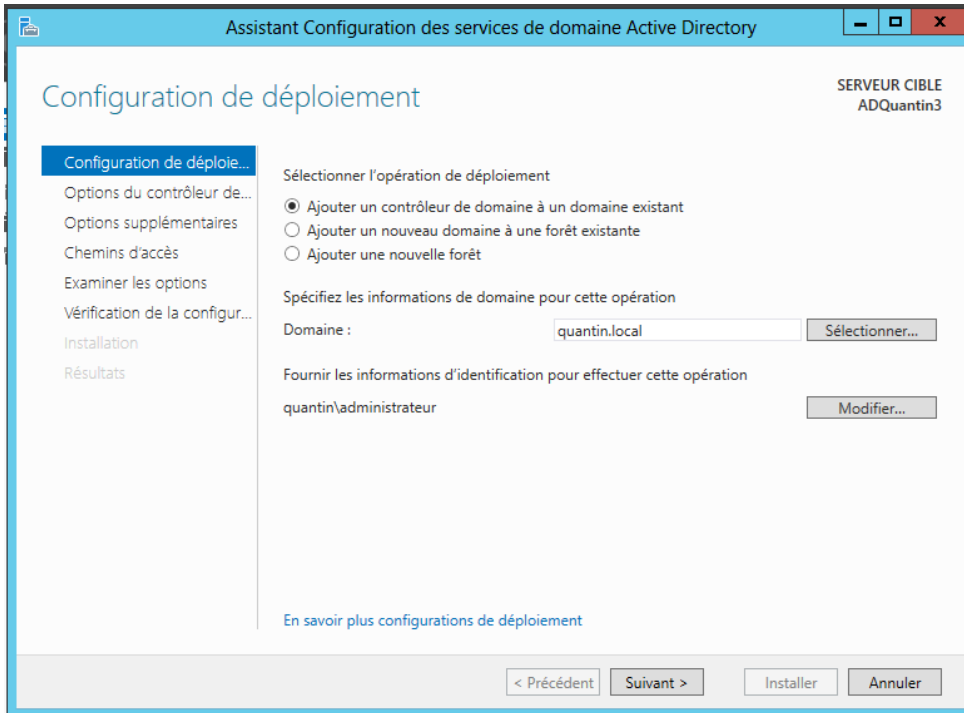
dcdiag /test :replications vérifier ponctualité du contrôleur

```
C:\Users\Administrateur>dcdiag /test:replications
Diagnostic du serveur d'annuaire
Exécution de l'installation initiale :
  Tentative de recherche de serveur associé...
  Serveur associé : WinServQuantin
  * Forêt AD identifiée.
  Collecte des informations initiales terminée.
Exécution des tests initiaux nécessaires
  Test du serveur : Caen\WINSERUQUANTIN
  Démarrage du test : Connectivity
  ..... Le test Connectivity
  de WINSERUQUANTIN a réussi
Exécution des tests principaux
  Test du serveur : Caen\WINSERUQUANTIN
  Démarrage du test : Replications
  ..... Le test Replications
  de WINSERUQUANTIN a réussi

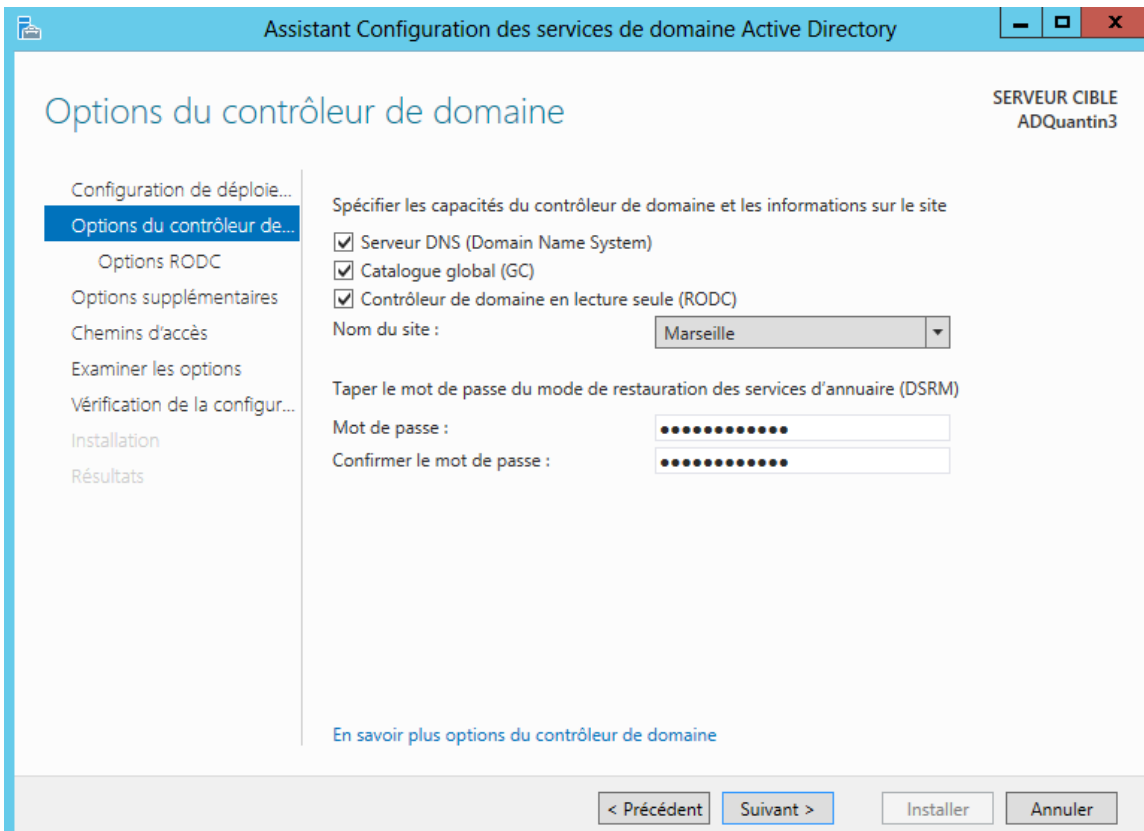
  Exécution de tests de partitions sur ForestDnsZones
  Exécution de tests de partitions sur DomainDnsZones
  Exécution de tests de partitions sur Schema
  Exécution de tests de partitions sur Configuration
  Exécution de tests de partitions sur quantin
  Exécution de tests d'entreprise sur quantin.local
```

III) Configuration de la stratégie RODC

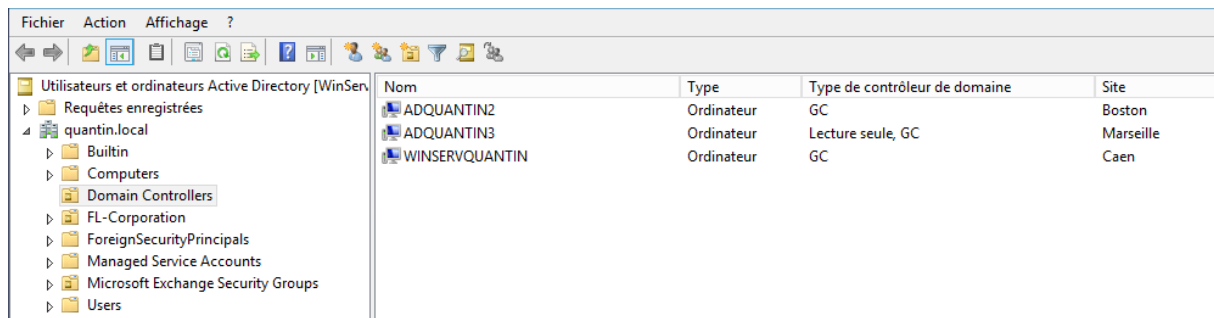
On installe le service ADDS sur ADQuantin3 :



Puis on choisit RODC :

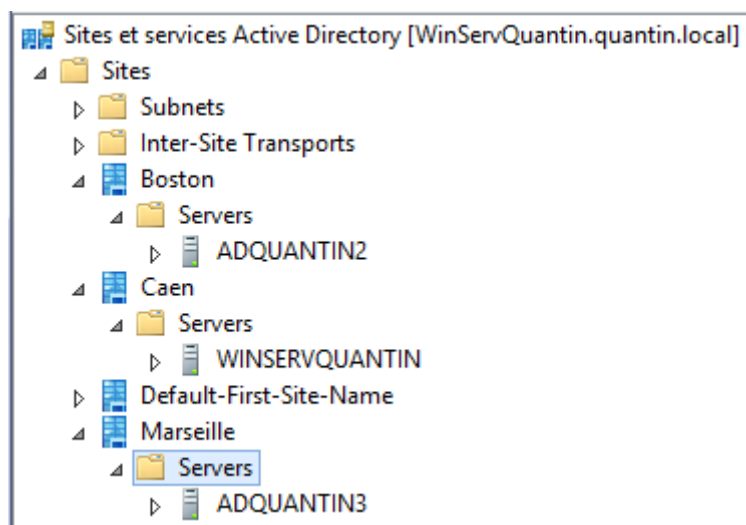


Dans utilisateurs et ordinateurs de l'AD, on voit bien l'ADQuantin3 qui est en lecture seule (RODC).

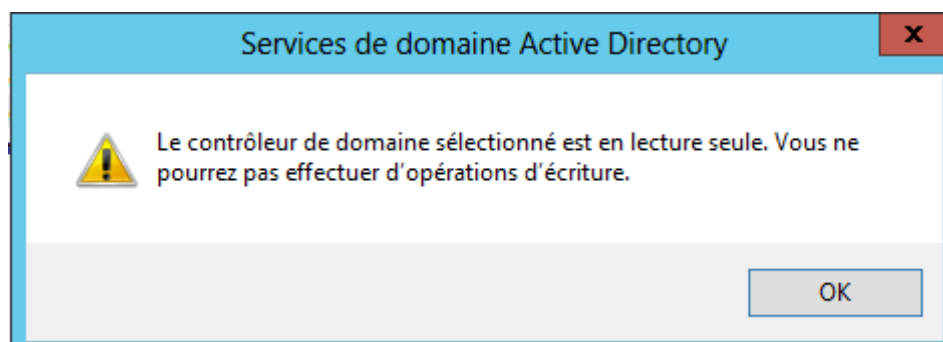


Nom	Type	Type de contrôleur de domaine	Site
ADQUANTIN2	Ordinateur	GC	Boston
ADQUANTIN3	Ordinateur	Lecture seule, GC	Marseille
WINSERVQUANTIN	Ordinateur	GC	Caen

Dans Sites, on voit la présence du Serveur RODC :



Vu que c'est en RODC, on a bien ce type de message d'erreur :



Enfin, on remarque que les enregistrements DNS se sont fait correctement :

Directe :

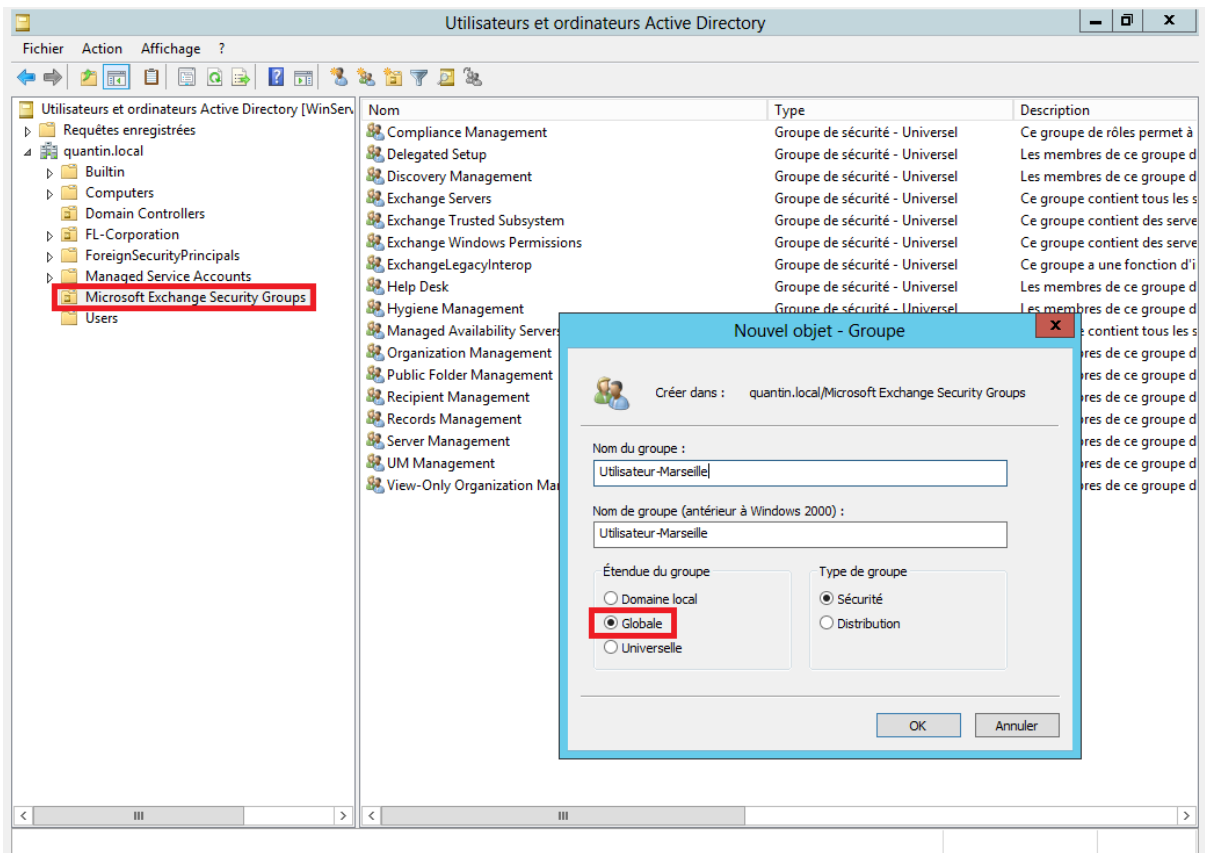
Nom	Type	Données	Horodateur
WINSERVQUANTIN			
Zones de recherche directes			
_msdcqs.quantin.local			
quantin.local			
Zones de recherche inversée			
Points d'approbation			
Redirecteurs conditionnels			
Journaux globaux			
_msdcqs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(identique au dossier parent)	Source de nom (SOA)	[119], winservquantin.qua...	statique
(identique au dossier parent)	Serveur de noms (NS)	winservquantin.quantin.lo...	statique
(identique au dossier parent)	Serveur de noms (NS)	adquantin2.quantin.local.	statique
(identique au dossier parent)	Hôte (A)	192.168.1.134	03/12/2015 09:00:00
(identique au dossier parent)	Hôte (A)	192.168.1.135	03/12/2015 09:00:00
ADQUANTIN2	Hôte (A)	192.168.1.135	statique
ADQUANTIN3	Hôte (A)	192.168.1.136	03/12/2015 10:00:00
Pc-PC	Hôte (A)	192.168.1.2	19/11/2015 08:00:00
winservquantin	Hôte (A)	192.168.1.134	statique

Inversé :

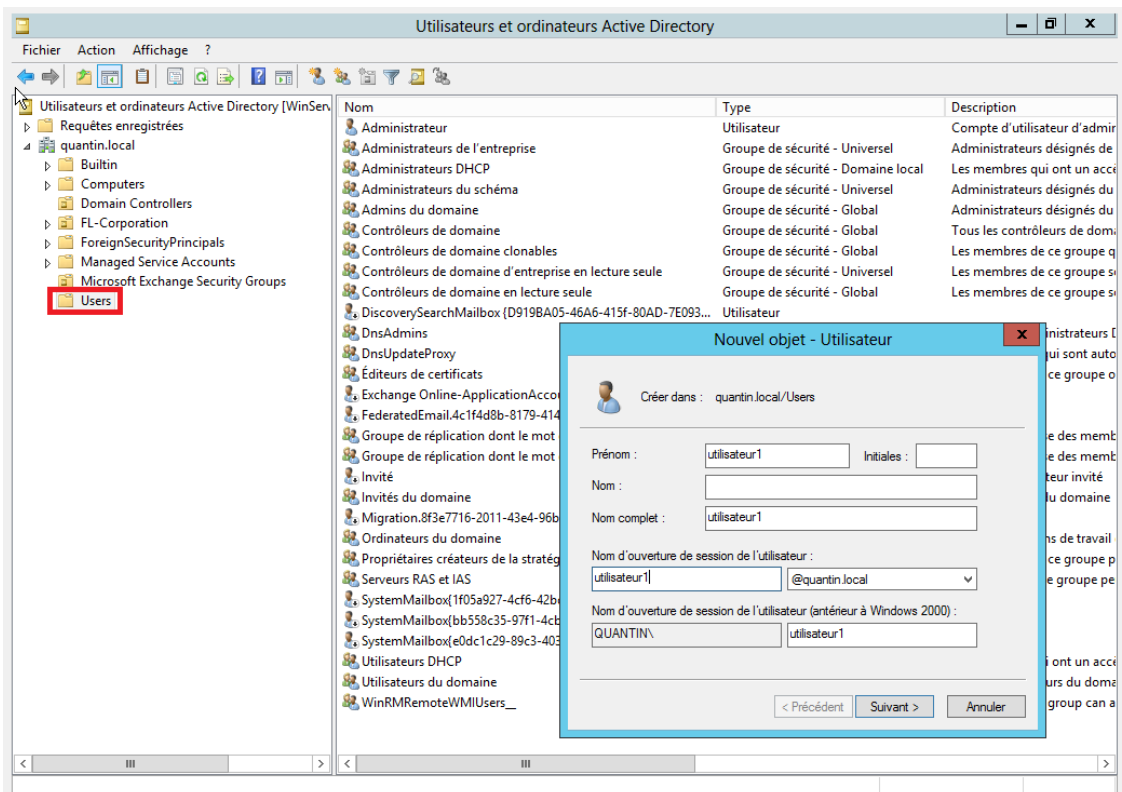
Nom	Type	Données	Horodateur
WINSERVQUANTIN			
Zones de recherche directes			
_msdcqs.quantin.local			
quantin.local			
Zones de recherche inversée			
1.168.192.in-addr.arpa			
Points d'approbation			
Redirecteurs conditionnels			
Journaux globaux			
(identique au dossier parent)	Source de nom (SOA)	[8], winservquantin.quanti...	statique
(identique au dossier parent)	Serveur de noms (NS)	adquantin2.quantin.local.	statique
(identique au dossier parent)	Serveur de noms (NS)	winservquantin.quantin.lo...	statique
192.168.1.134	Pointeur (PTR)	winservquantin.quantin.lo...	statique
192.168.1.135	Pointeur (PTR)	adquantin2.quantin.local.	03/12/2015 09:00:00
192.168.1.136	Pointeur (PTR)	adquantin3.quantin.local.	03/12/2015 10:00:00

IV) Mise en cache des mots de passe

On va créer des groupes de sécurité :



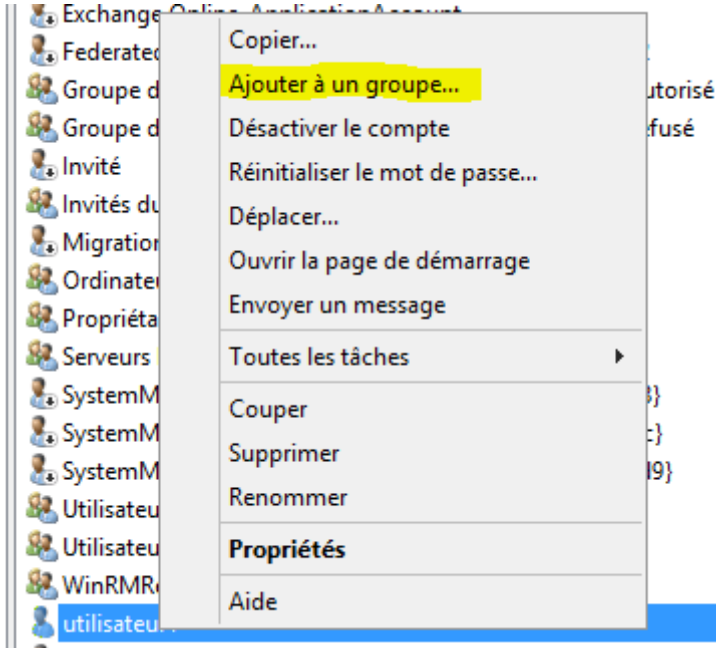
Puis, on va créer des utilisateurs (1 et 2) :



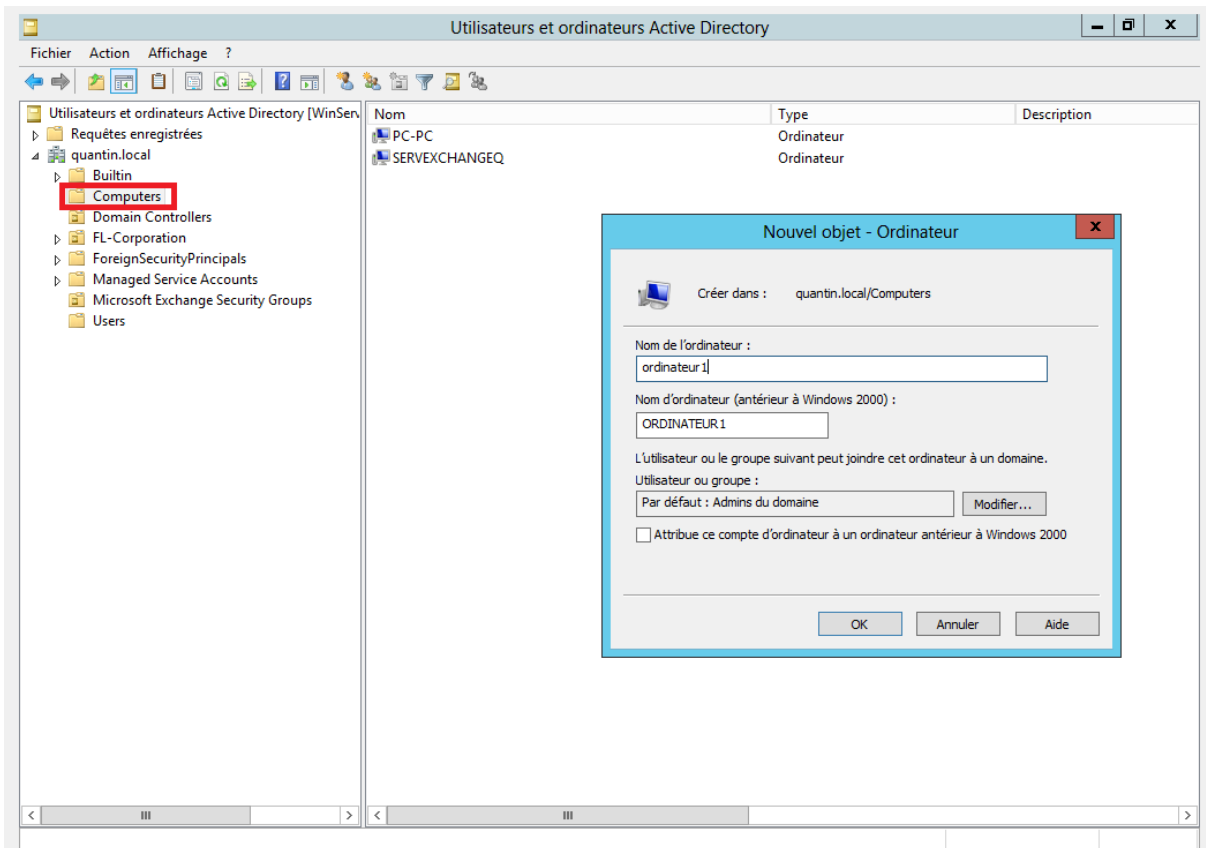
On a bien nos 2 utilisateurs :



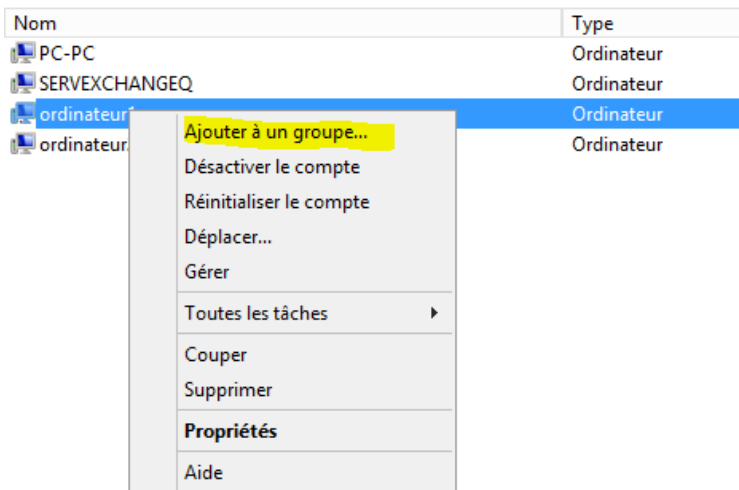
On l'ajoute au groupe Utilisateur-marseille :



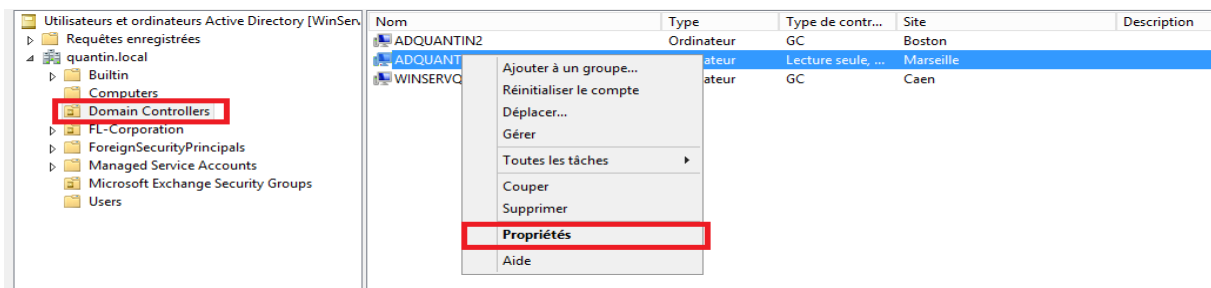
On créer deux ordinateurs :



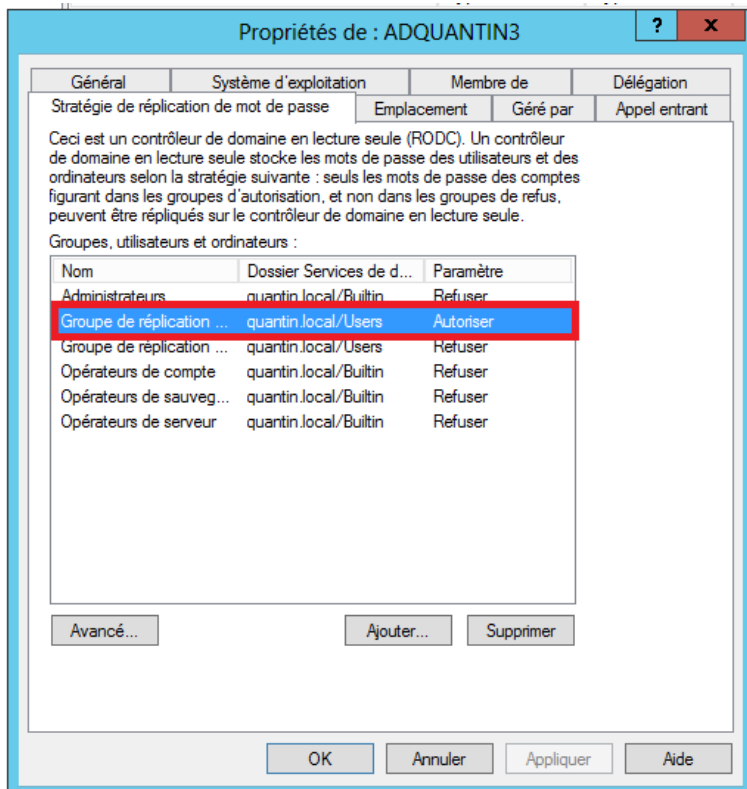
On ajoute les deux ordinateurs au groupe utilisateur-Marseille :



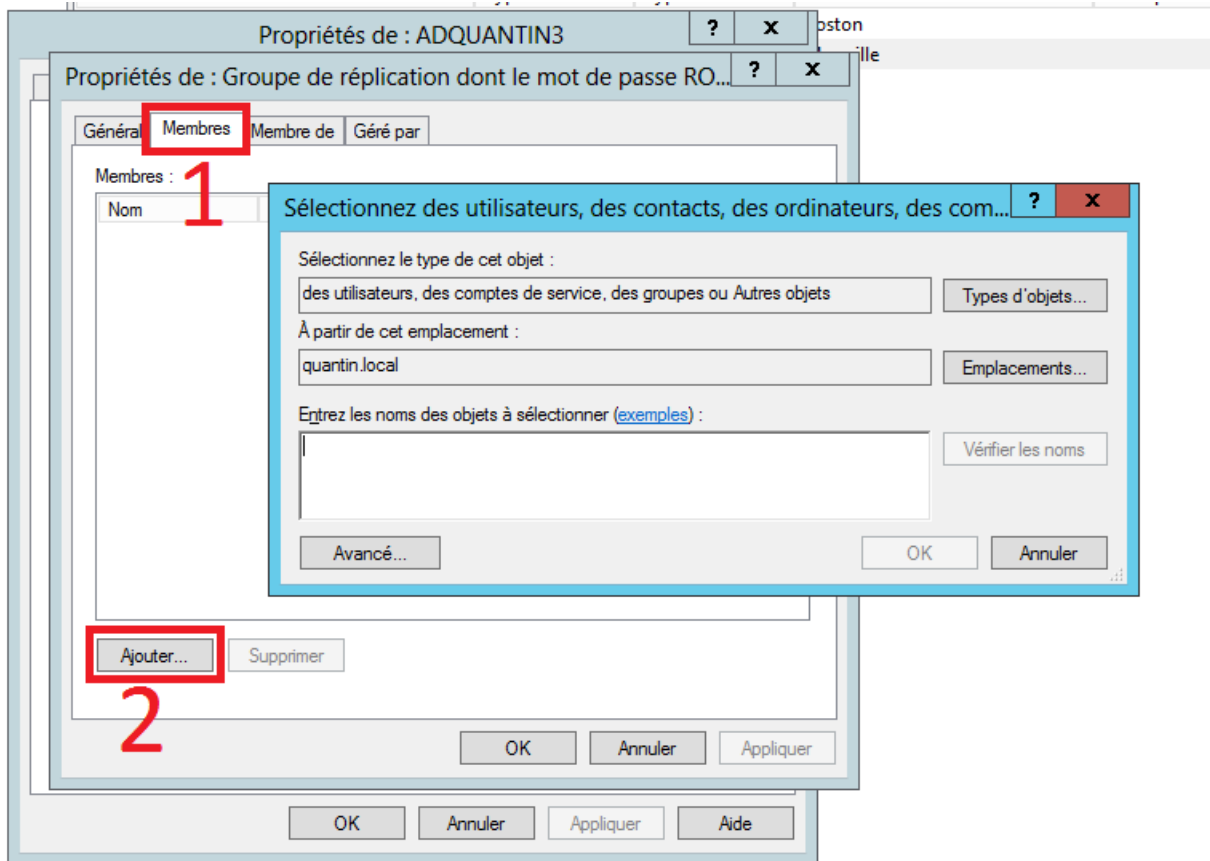
Maintenant, on édite les propriétés du RODC :



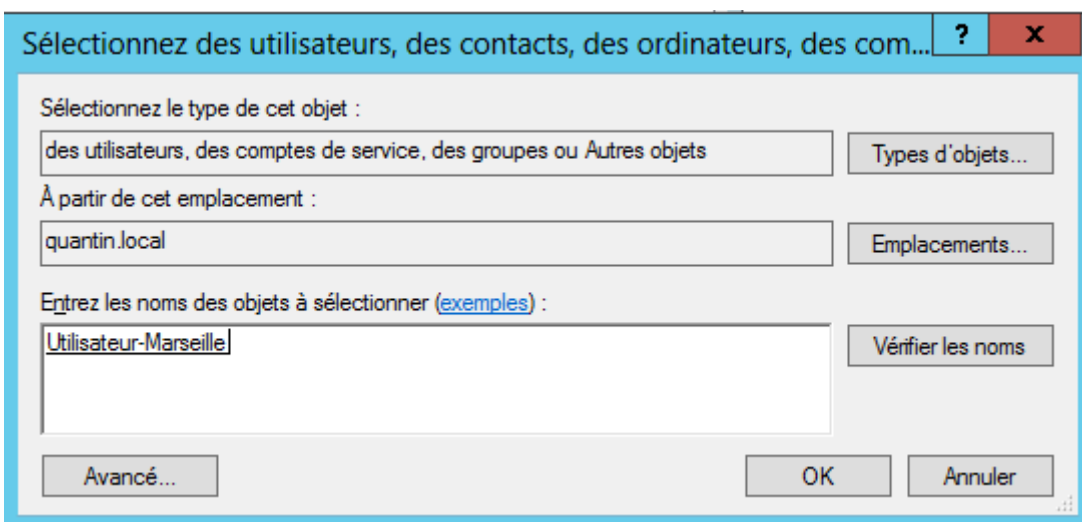
Puis, dans l'onglet Stratégie de réplcation de mot de passe, on double clic sur l'encadré en rouge :



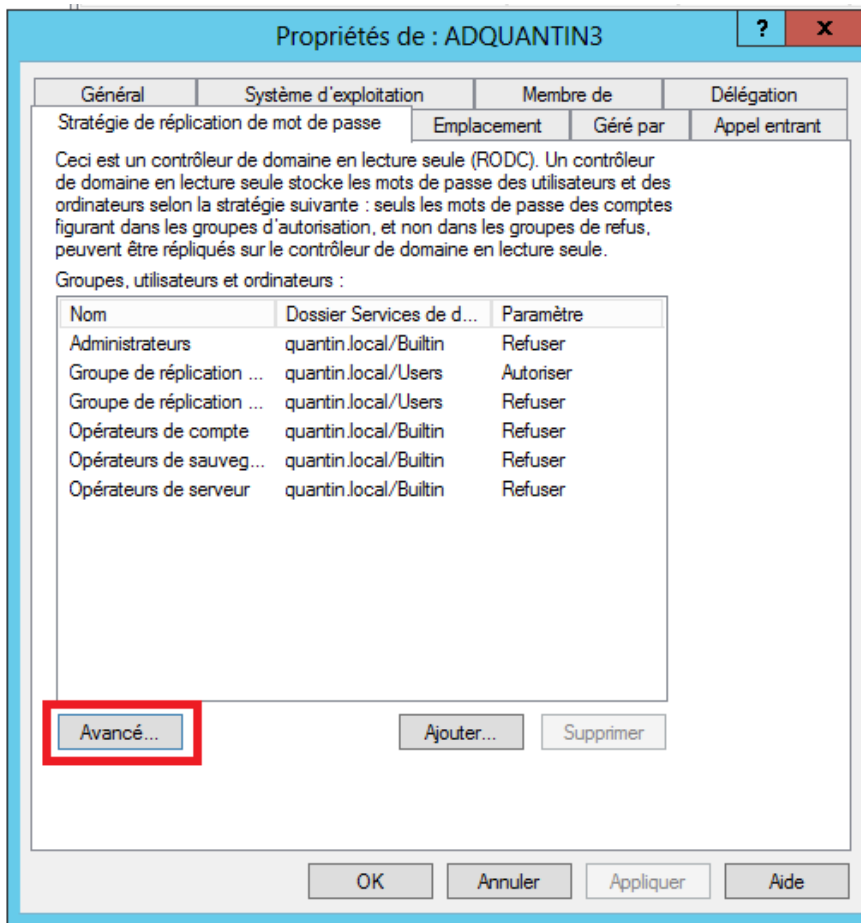
Onglet Membres puis Ajouter :



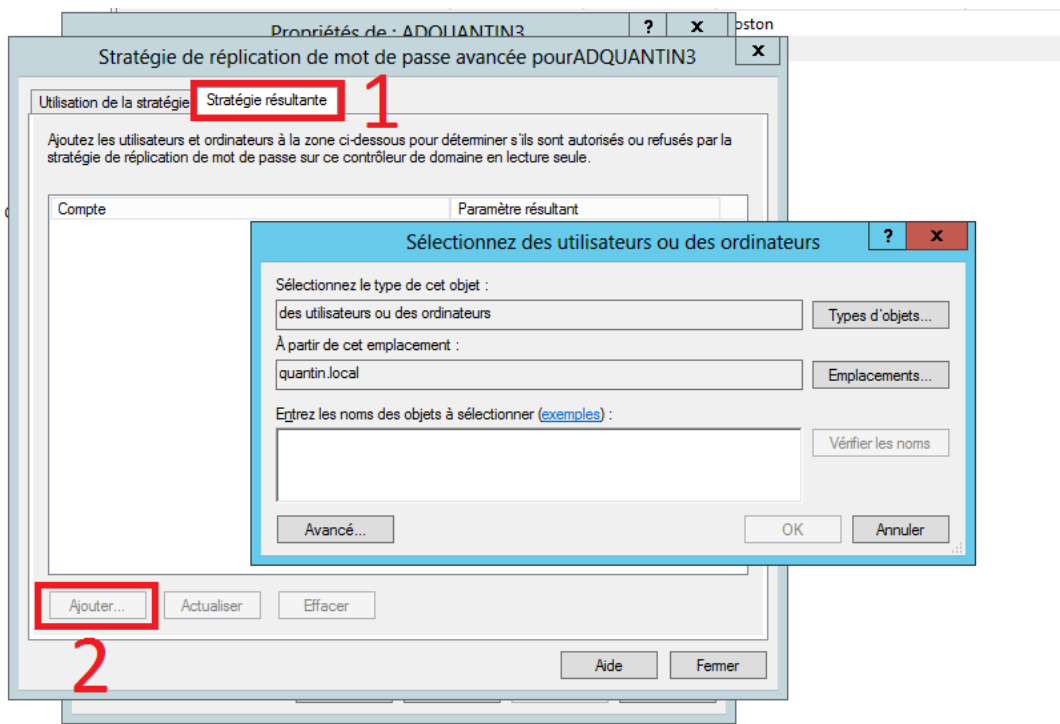
Puis, on met le groupe Utilisateur-Marseille (deux ok pour valider):



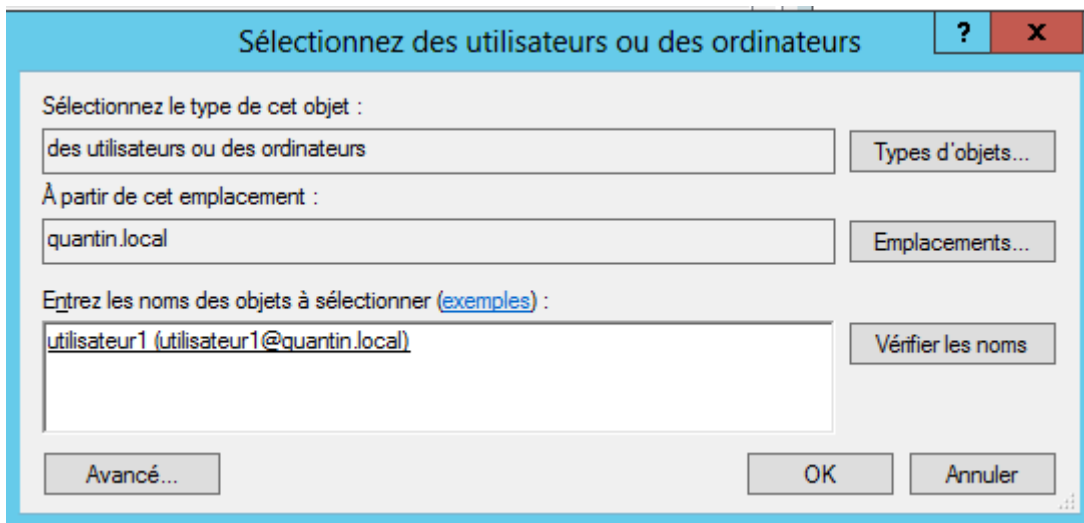
On va dans avancé maintenant :



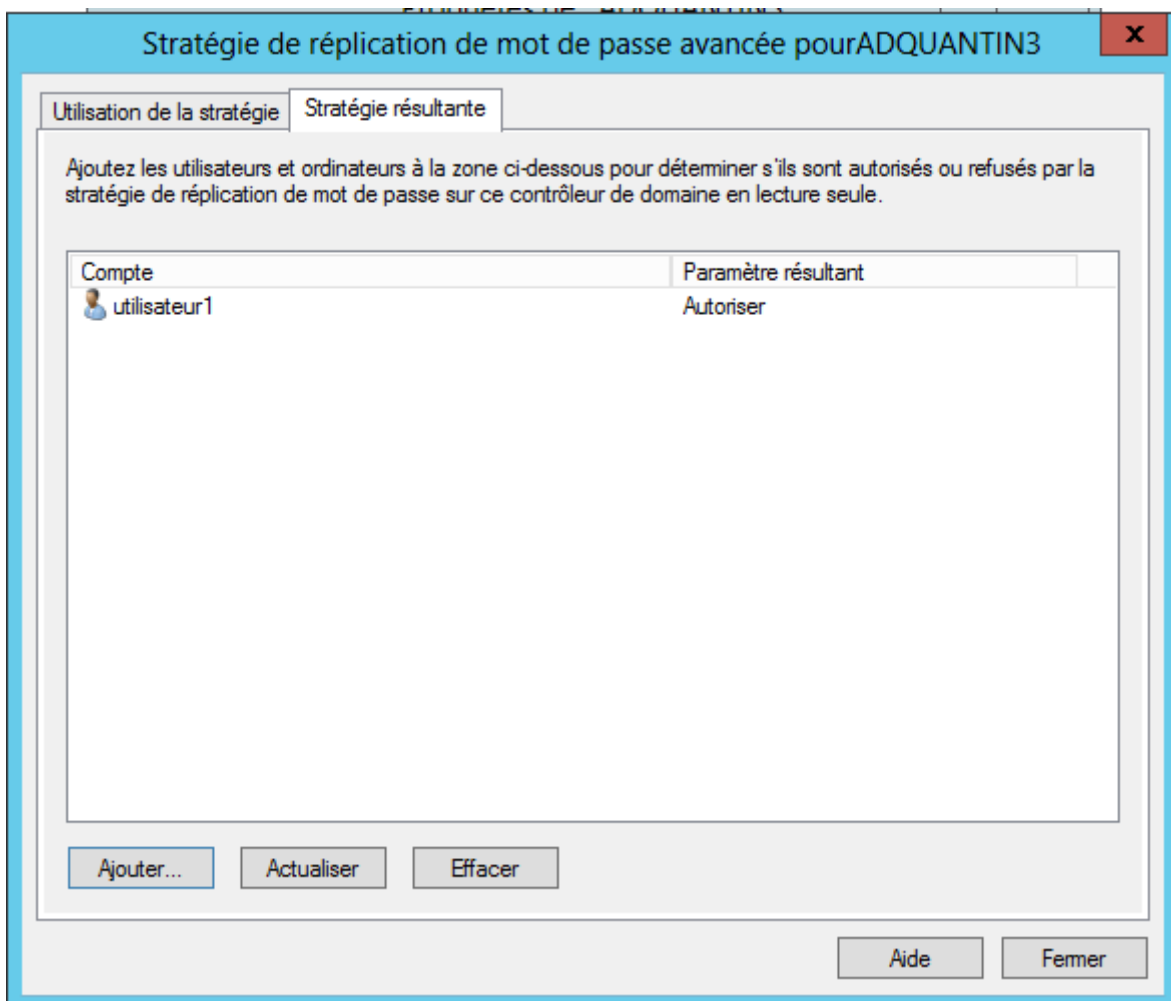
Puis dans l'onglet Stratégie résultante, ajouter :



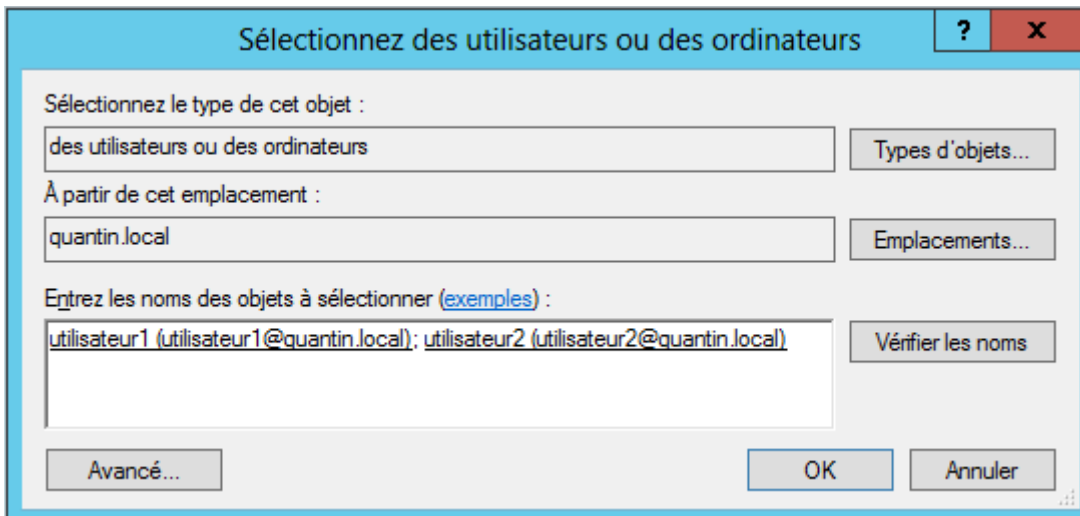
On ajoute l'utilisateur1 :



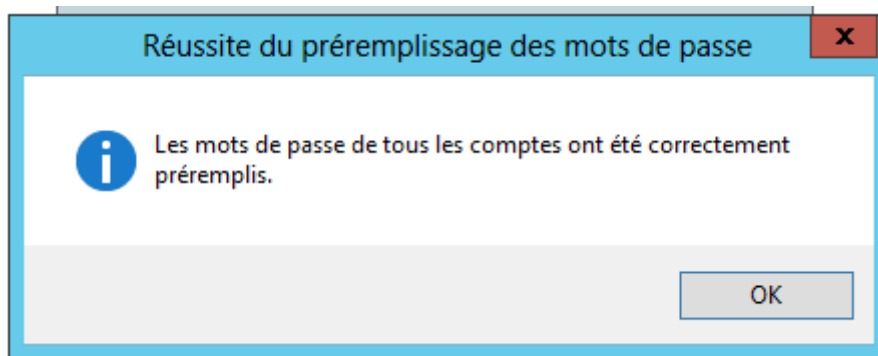
On voit que l'utilisateur1 est autorisé. Cela veut dire que le mot de passe du compte d'utilisateur sélectionné est autorisé à être mis en cache sur le serveur RODC:



Cliquez sur l'onglet Utilisation de la stratégie puis sur le bouton Préremplir les mots de passe. Ensuite, on ajoute deux utilisateurs :



Message d'information de réussite :



Faire de même pour les ordinateurs 1 et 2 puis vérifier :

