# ****Académie Microsoft Exchange Server 2010****

|  |  |
| --- | --- |
| Damien Caro | MODULE 2 : Migration des boites aux lettres de Exchange 2003 à Exchange 2010 Article de [Damien Caro](http://blogs.technet.com/dcaro/), **Architecte Infrastructure sur les solutions de Communications Unifiées, Microsoft France**  **Sommaire de l'article :**  [Principe de coexistence de serveurs d'accès client (CAS)](#_Toc250983685)  [Mise en place des certificats sur le serveur CAS 2010](#_Toc250983686)  [Génération de la demande de certificat](#_Toc250983687)  [Obtention du certificat](#_Toc250983688)  [Import du certificat et affectation aux services](#_Toc250983689)  [Modification du certificat sur le serveur Frontal Exchange 2003](#_Toc250983690)  [Configuration des espaces de nom pour le serveur CAS Exchange 2010](#_Toc250983691)  [Basculement du point d'accès OWA](#_Toc250983692)  [Déplacement des boites aux lettres](#_Toc250983693)  [Conclusion et prochaines étapes](#_Toc250983694) |

Dans le module précédent, nous avons procédé à l'installation d'Exchange 2010. Cette étape a eu des conséquences au niveau de l'infrastructure de messagerie mais pour le moment il n'y a aucun impact au niveau des clients de messagerie. Cette deuxième étape, à savoir la migration des serveurs CAS est une opération qui va impacter les accès aux boites aux lettres.

A la fin de ce module, nous migrerons le contenu des boites aux lettres de notre infrastructure. Cette dernière étape est souvent la plus longue dans un projet de migration.

## Principe de coexistence de serveurs d'accès client (CAS)

Il est possible de faire coexister au sein de la même organisation des serveurs frontaux fonctionnant avec Exchange 2003 et des serveurs CAS avec Exchange 2010.

Dans le cas d'une petite migration, si la migration peut être effectuée en une seule fois au cours d'une plage d'indisponibilité des accès client, vous pouvez passer directement à l'étape suivante.

Si vous avez besoin de maintenir la continuité des accès clients, il est nécessaire d'avoir un serveur front-end OWA 2003 avec une authentification par formulaires pour permettre une authentification SSO entre les deux environnements (2010 et 2003).

Vue d'ensemble de la procédure de mise en place du mode de coexistence :

* Les deux générations de serveurs sont installées en parallèle dans l'organisation (ce qui a été réalisé dans le premier module).
* Association de noms DNS de type 'legacy' pour le serveur frontal Exchange 2003.
* Obtention d'un nouveau certificat sur le serveur CAS Exchange 2010 avec les noms d'hôtes utilisé pendant la phase de coexistence.
* Configuration des espaces de nom pour le serveur CAS Exchange 2010.
* Déplacement du serveur générant le carnet d'adresse en mode autonome (OAB).
* Modification du DNS pour pointer vers le nouveau serveur CAS Exchange 2010.
* Déplacement des boites aux lettres.

La première phase ayant été réalisée lors du premier module, nous allons pouvoir directement adresser la deuxième étape à savoir la demande de certificats.

Attention : Les étapes que nous décrivons ici dans le détail ne sont valables quand dans notre lab sans publication vers Internet. Dans le cas d'une publication à travers un reverse-proxy, les échanges entre le reverse-proxy et le serveur frontal (Exchange 2003) ou le CAS (Exchange 2010) se font en utilisant le nom FQDN interne de ces serveurs. Les changements au niveau des certificats se font au niveau du reverse-proxy sauf dans le cas où les clients interne accèdent à OWA en interne avec une entrée dans le DNS différente de celle publiée à l'extérieur.

Voici un schéma d'architecture des flux de communications dans l'état actuel des choses :  


## Mise en place des certificats sur le serveur CAS 2010

Dans notre infrastructure, le certificat qui va être associé au CAS Exchange 2010 doit pouvoir servir les noms d'hôte suivants :

* mail.ucdemo.fr
* autodiscover.ucdemo.fr
* legacy.ucdemo.fr

mail.ucdemo.fr : Permet de répondre aux requêtes des clients OWA en leur assurant une transition transparente tout en gardant les mêmes url d'accès.

autodiscover.ucdemo.fr : Permet de répondre aux client Outlook 2007 ou supérieur qui ont besoin de résoudre le nom autodiscover pour se configurer automatiquement.

legacy.ucdemo.fr : Ce nom est utilisé uniquement pendant la phase de coexistence. Le nom legacy étant en fait affecté au serveur Exchange 2003.

Pour atteindre ce but, nous allons suivre les étapes suivantes :

* Génération de la requête pour obtenir un certificat de la part d'une autorité de certification
* Obtention du certificat
* Import et affectation du certificat nouvellement obtenu

### Génération de la demande de certificat

Pour générer la demande à soumettre à l'autorité de certification, il est possible d'utiliser le cmdlet powershell d'Exchange 2010 ou l'interface graphique du nouvel assistant de gestion des certificats d'Exchange 2010.

#### Génération de la demande de certificat par cmdlet powershell :

Création du fichier de demande :

New-ExchangeCertificate

-GenerateRequest

-Path c:\certificates\request.req

-SubjectName “c=FR, o=ucdemo, cn=ac-exch-1.ucdemo.fr”

-DomainName mail.ucdemo.fr, autodiscover.ucdemo.fr, legacy.ucdemo.fr

-PrivateKeyExportable $true

Transmettez le fichier de requête à l'autorité de certification de votre choix. Dans notre lab, nous allons utiliser l'autorité de certification interne installée sur notre DC.

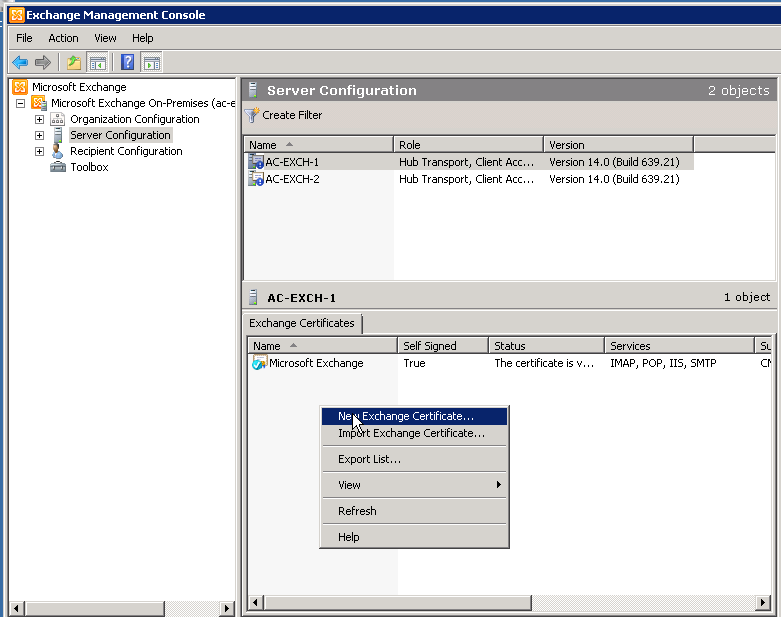
Utiliser le cmdlet Import-ExchangeCertificate pour importer le certificat obtenu en réponse à votre demande

Finalement activez le certificat en question par le cmdlet Enable-ExchangeCertificate pour l'associer à un ou plusieurs services de messsagerie.

#### Génération de la demande de certificat par l'assistant d'Exchange 2010:

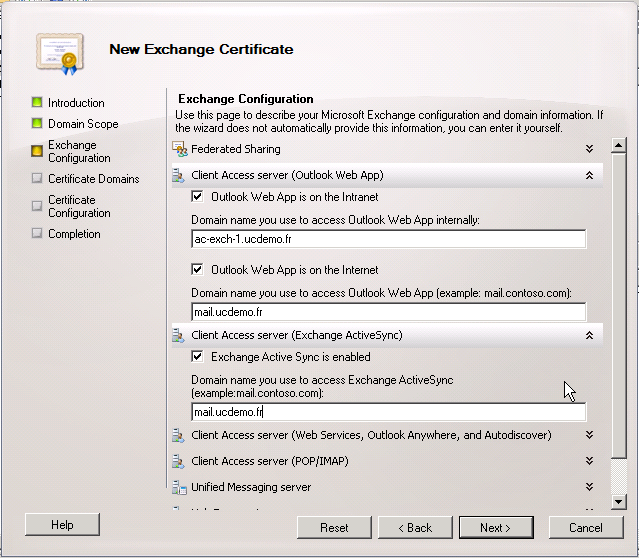
Une des nouveautés de Exchange 2010 est justement de fournir un assistant pour les demandes de certificats automatisant les tâches que nous venons de décrire ci-dessus.

L'assistant se lance depuis la l'Exchange Management Console : Il faut sélectionner le conteneur "Server Configuration" puis un clic droit dans le rectangle "Exchange Certificates".

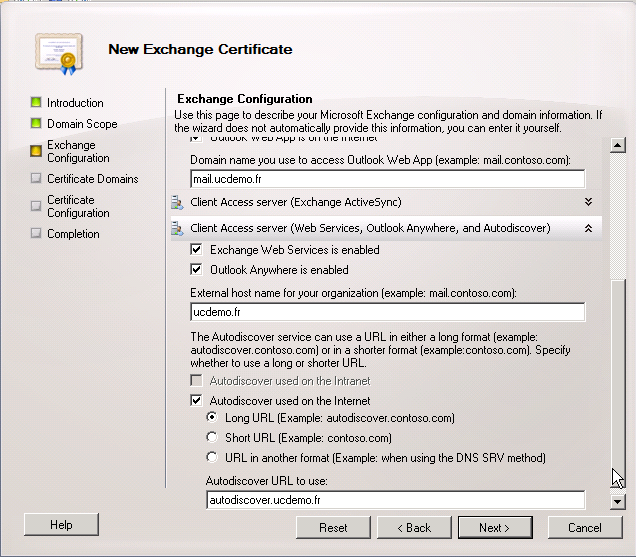


Ensuite, il faut saisir un nom d'affichage qui sert à identifier le certificat une fois qu'il est dans le magasin de certificats.

Après avoir passé le champ concernant l'usage de wildcard certificates, il reste à renseigner les informations concernant les différents accès clients que nous allons utiliser sur cette plateforme. Voici les informations à renseigner pour notre infrastructure de lab :

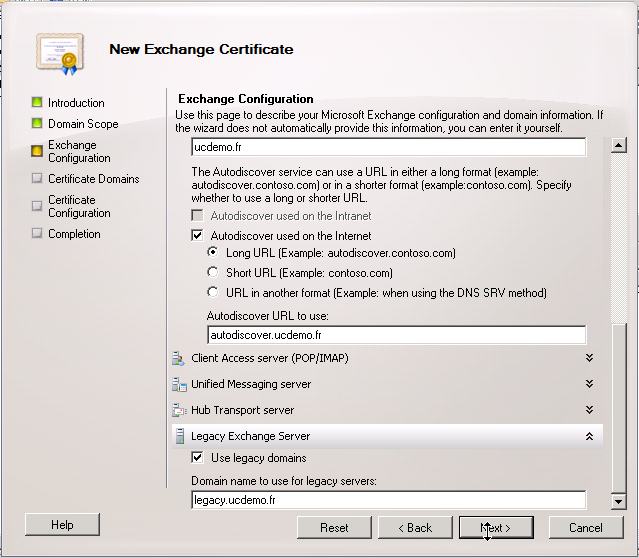


Le nom **mail.ucdemo.fr** est présent dans la demande de certificat pour pouvoir répondre aux requêtes qui tombent sur le serveur une fois que nous aurons modifié le DNS.



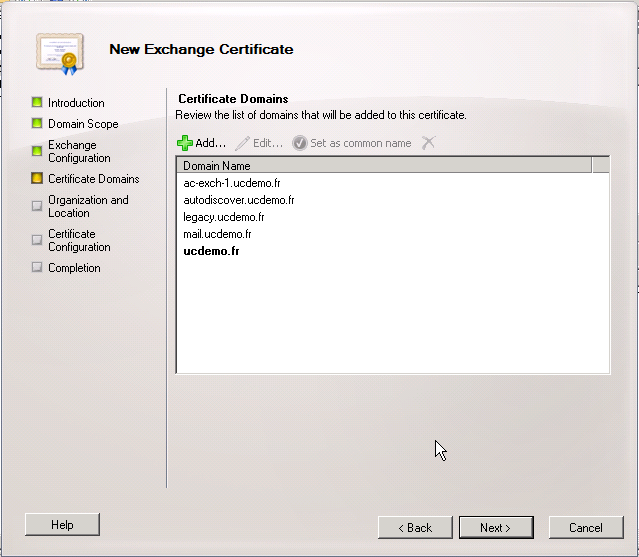
Vérifiez à l'étape précédente si les urls sont correctement renseignées. En particulier le champ utilisé pour l'autodiscover.

La dernière étape de cette page consiste à indiquer l'adresse des "legacy exchange servers" c’est-à-dire l'adresse utilisée pour la redirection vers Exchange 2003.

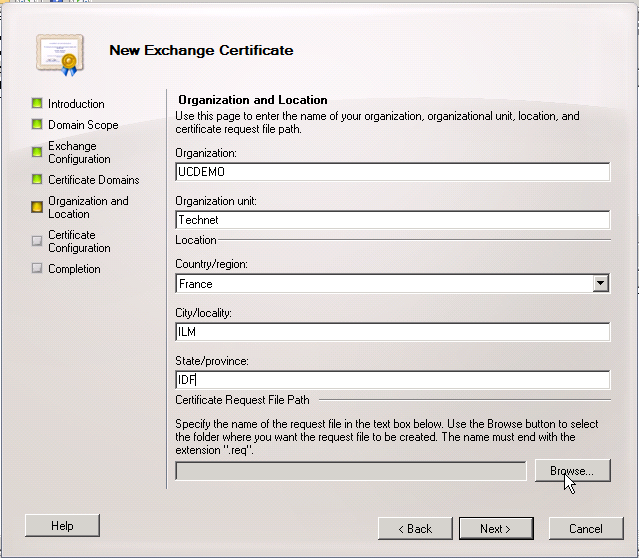


L'étape suivante consiste à vérifier que tous les noms alternatifs (ou SAN – Subject Alternate Names) ont bien étés pris en compte.

Vous avez aussi la possibilité de spécifier le common name que vous souhaitez utiliser parmi la liste des domaines ajoutés au certificat.



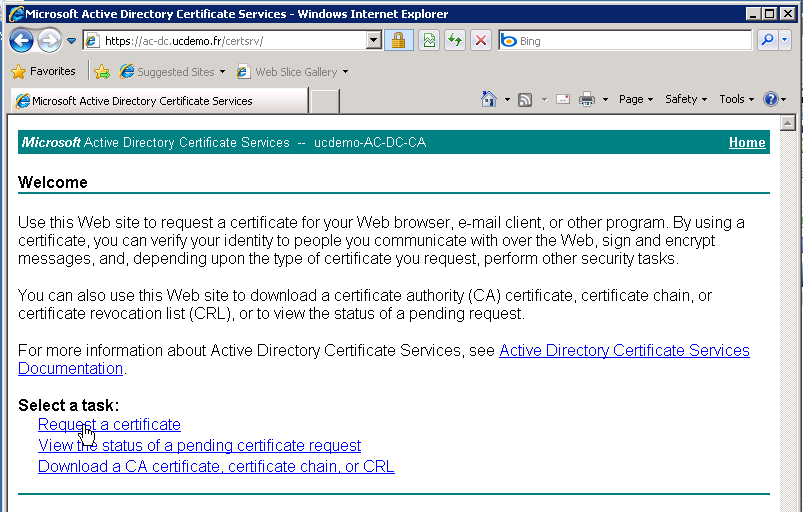
Après avoir renseigné les champs classiques pour la demande de certificat (organisation, nom, ville, …) il reste à enregistrer la demande de certificat dans un fichier pour le soumettre à notre autorité de certification.



### Obtention du certificat

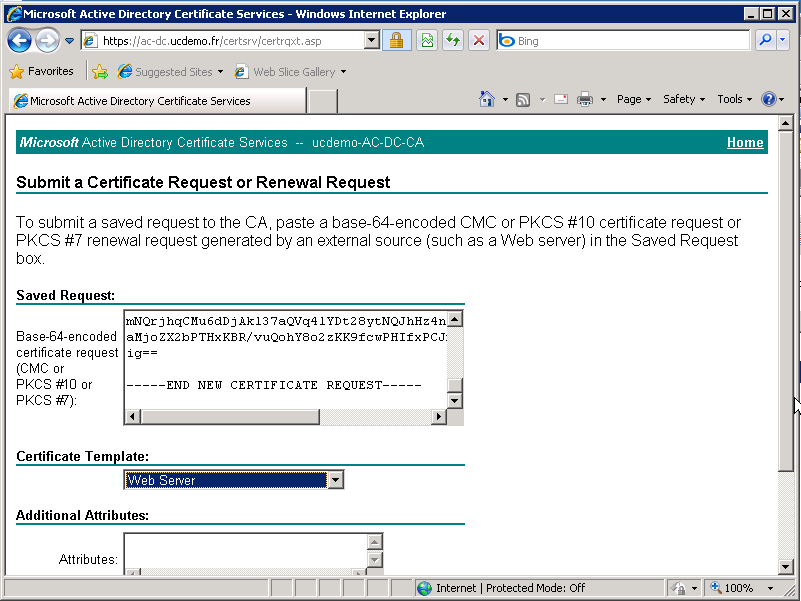
La soumission de la demande de certificat (le fichier .req que nous avons créé) dépend de chaque autorité de certification. Les prochaines étapes sont applicables dans notre lab pour une autorité de certification Microsoft.

Dans notre cas, nous allons sur l'interface web de l'autorité de certification pour demander un nouveau certificat :



Demandez à effectuer une demande avancée puis choisir l'option "**Submit a certificate request using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.**"

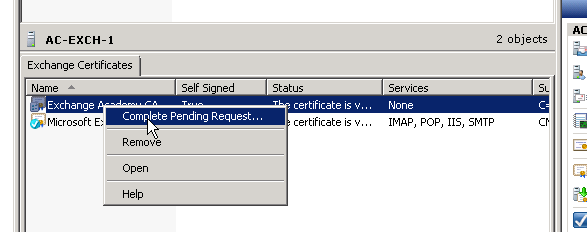
Copiez le contenu du fichier .req dans le champ texte prévu à cet effet et choisissez le modèle de certificat "**Web Server**" comme dans la capture d'écran suivante :



Sauvegardez le certificat ainsi obtenu. Il va être possible de l'importer dans Exchange 2010.

### Import du certificat et affectation aux services

Dans notre lab (qui, n'a pas de serveur proxy), l'importation du certificat se fait sur le serveur CAS depuis la console d'administration d'Exchange 2010 dans le mode "**complete pending request**" afin de pouvoir associer le certificat à la demande qui a été générée. De retour dans l'Exchange Management Console, il suffit de faire un clic droit sur la demande en cours :



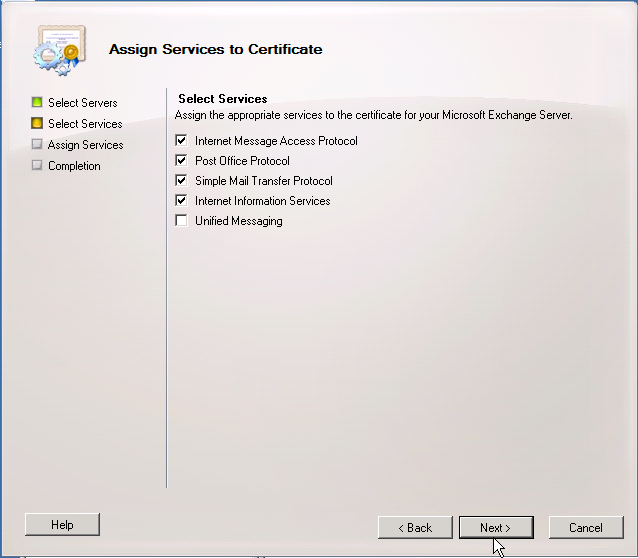
Pointez vers le certificat qui vient d'être téléchargé pour compléter l'importation du certificat.

La dernière étape consiste à **assigner** ce certificat à un ou plusieurs services. Il est possible de réaliser cette étape en ligne de commande Powershell ou de le faire depuis l'assistant avec les étapes suivantes.

Relancez l'assistant depuis la console d'administration d'Exchange 2010 et choisissez "**Assign Services to Certificate**" sur le certificat que vous venez d'importer.



Il suffit ensuite de choisir les services que l'on veut affecter à ce certificat. C’est-à-dire que l'on indique à chacun de ces services d'utiliser ce certificat pour les sécurisations des communications.



Attention : Il faut redémarrer les services Exchange utilisant ces certificats pour que l'opération soit prise en compte. Une méthode un peu plus radicale consiste à redémarrer le serveur.

Le serveur hébergeant le rôle d'accès client d'Exchange 2010 est maintenant configuré au niveau des certificats. Il reste à effectuer les étapes suivantes avant de procéder au déplacement des boites aux lettres à proprement parler.

Voici l'état des lieux après l'affectation du certificat sur le serveur Exchange 2010 :  


## Modification du certificat sur le serveur Frontal Exchange 2003

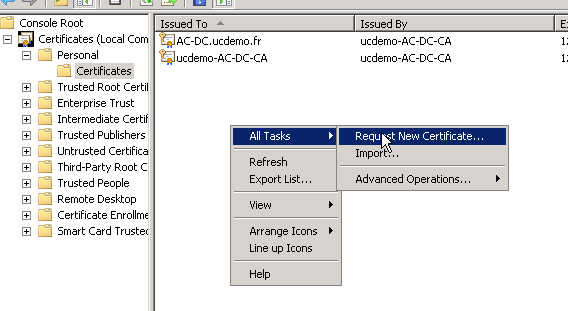
Cette étape n'est nécessaire que dans le cas où l'on accède aux serveurs frontaux depuis le réseau interne sans passer par un ou plusieurs reverse-proxy.

Le fonctionnement du CAS 2010 vis-à-vis des frontaux Exchange 2003 étant une opération de redirection sur l'adresse "legacy.ucdemo.fr" il est nécessaire que le canal SSL puisse s'établir sur ce nom sans erreur. Pour cela nous allons demander à notre autorité de certification un certificat avec les noms DNS suivants :

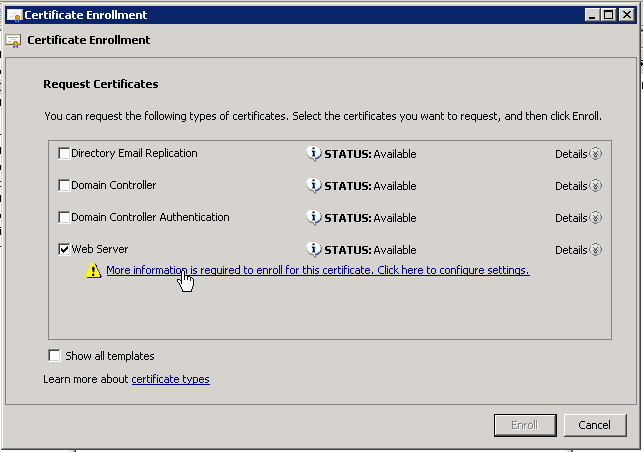
* ac-exch03-fe.ucdemo.fr : le serveur doit pouvoir chiffrer les communications à son nom.
* legacgy.ucdemo.fr : c'est le nom de redirection qui sera utilisé
* mail.ucdemo.fr : tant que la bascule n'a pas été faite, c'est toujours le serveur Exchange 2003 qui sert les requêtes client sur le nom dns mail.ucdemo.fr

Nous allons utiliser l'assistant inclus dans la MMC de gestion des certificats de Windows 2008 pour demander notre certificat. Voici les étapes à suivre :

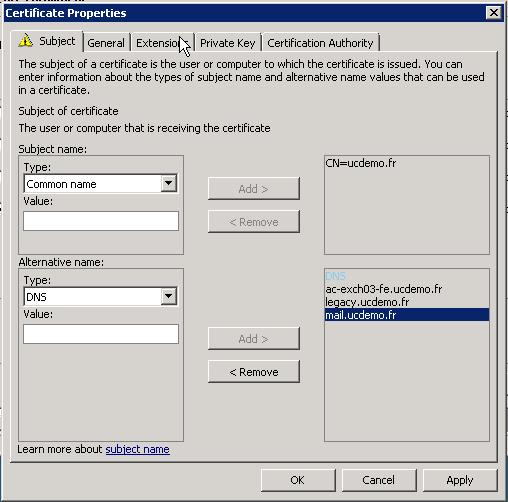
Demander un nouveau certificat par un clic droit dans la MMC (il est important d'avoir ouvert le magasin de l'ordinateur pour pouvoir demander un certificat d'ordinateur):



Cliquer sur "next" sur la page d'introduction de l'assistant et choisir le modèle "Web Server" :



Renseigner les SAN (Subject Alternate Names) comme suit pour notre lab :



Penser à aller dans l'onglet "Private Key" pour autoriser l'exportation de la clef privée :



Valider les étapes restante jusqu'à la fin de l'opération.

Le certificat est alors placé dans le magasin de certificats d'où il est possible de l'exporter et de l'importer à nouveau sur n'importe quel autre serveur, dans notre cas, le serveur Exchange 2003 frontal (AC-EXCH03-FE.ucdemo.fr).

Le serveur Exchange 2003 Frontal continue ainsi de servir les requêtes existantes et est prêt pour l'étape suivante.

## Configuration des espaces de nom pour le serveur CAS Exchange 2010

La configuration des espaces de nom ou *namespace*s consiste en pratique à indiquer au serveur CAS les URLs à utiliser en interne et en externe pour les différents types d'accès clients.

Cette étape touche les accès utilisant un mode web à la messagerie. Dans notre lab, le seul mode d'accès que nous n'avons pas activé est "Outlook Anywhere". Cependant si dans votre infrastructure vous aviez une configuration de ce type, il faudra le configurer en utilisant le cmdlet suivant :

Enable-OutlookAnywhere -Server:<CAS2010> -ExternalHostName:mail.ucdemo.fr -SSLOffloading $false

Nous allons donc configurer les URLs internes et externes pour chacun des types d'accès avec les commandes suivantes :

Set-OABVirtualDirectory AC-EXCH-1\OAB\* -ExternalURL https://mail.ucdemo.fr/OAB

Set-WebServicesVirtualDirectory AC-EXCH-1\EWS\* -ExternalURL https://mail.ucdemo.fr/ews/exchange.asmx

Set-ActiveSyncVirtualDirectory -Identity AC-EXCH-1\Microsoft-Server-ActiveSync -ExternalURL https://mail.ucdemo.fr

Set-OWAVirtualDirectory AC-EXCH-1\OWA\* -ExternalURL https://mail.ucdemo.fr/OWA

Set-ECPVirtualDirectory AC-EXCH-1\ECP\* -ExternalURL https://mail.ucdemo.fr/ECP

Une fois les URLs externes de positionnées pour tous les accès web à Exchange 2010, il reste à configurer l'URL à utiliser pour se connecter à Exchange 2003. Le principe est que le serveur CAS 2010 servira de tête de pont pour tous les accès client (aussi bien pour les boites aux lettres Exchange 2010 que pour les boites aux lettres Exchange 2003). Il fera ensuite une redirection vers l'URL qui va être indiquée dans celle ligne de commande pour les clients qui ont encore leurs boites aux lettres sur Exchange 2003.

Set-OWAVirtualDirectory <CAS2010>\OWA\* -Exchange2003URL https://legacy.contoso.com/exchange

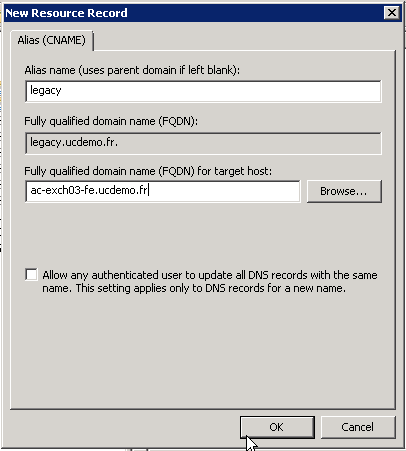
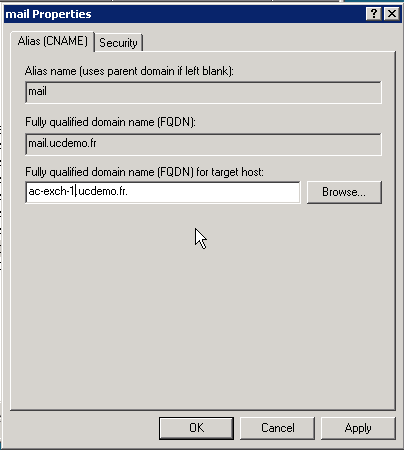
## Basculement du point d'accès OWA

Les étapes préparatoires sont maintenant terminées:

* Le serveur Exchange 2003 est prêt à recevoir des requêtes redirigées depuis le CAS 2010
* Le serveur CAS 2010 est configuré avec les espaces de noms à utiliser en interne comme en externe (si nous avions)
* Les certificats ont été enregistrés

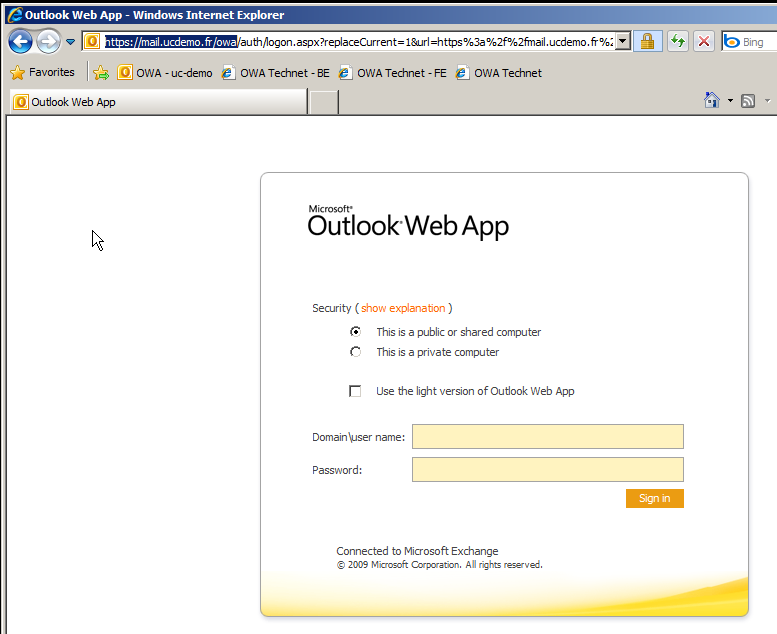
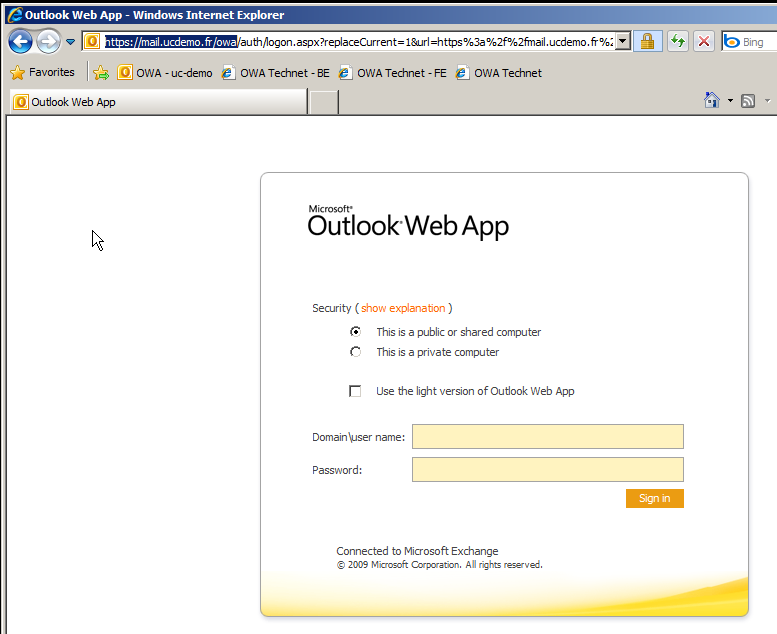
Il reste à faire pointer nos clients vers le CAS 2010.

Cela se fait par deux petites modifications dans le DNS:

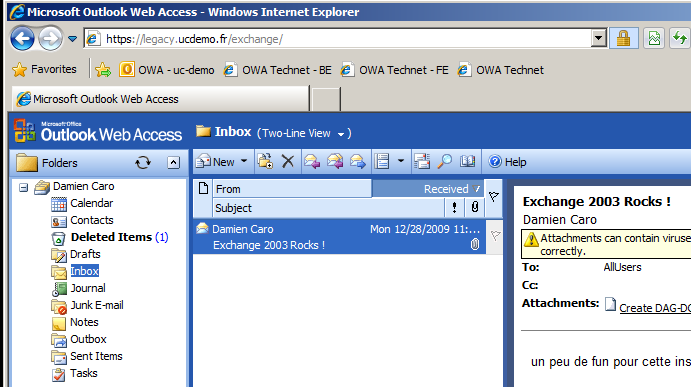
1. Ajouter un CNAME pour faire pointer **legacy.ucdemo.fr** vers **ac-exch03-fe.ucdemo.fr** :  
   
2. Modifier le CNAME existant pour faire pointer mail.ucdemo.fr vers ac-exch-1.ucdemo.fr :  
   

N'hésitez pas à faire un test, la page d'accueil est le formulaire OWA 2010 mais une fois l'authentification passée, vous aurez toujours votre boite aux lettres de test sous OWA 2003.

Voici la fenêtre de connexion basée sur des formulaires :



Et la connexion sur une boite aux lettres non migrée donne cette page :



Voici un schéma descriptif des flux de communication dans l'état actuel des choses:  


Il reste la dernière étape à savoir le déplacement des boites aux lettres vers Exchange 2010.

## Déplacement des boites aux lettres

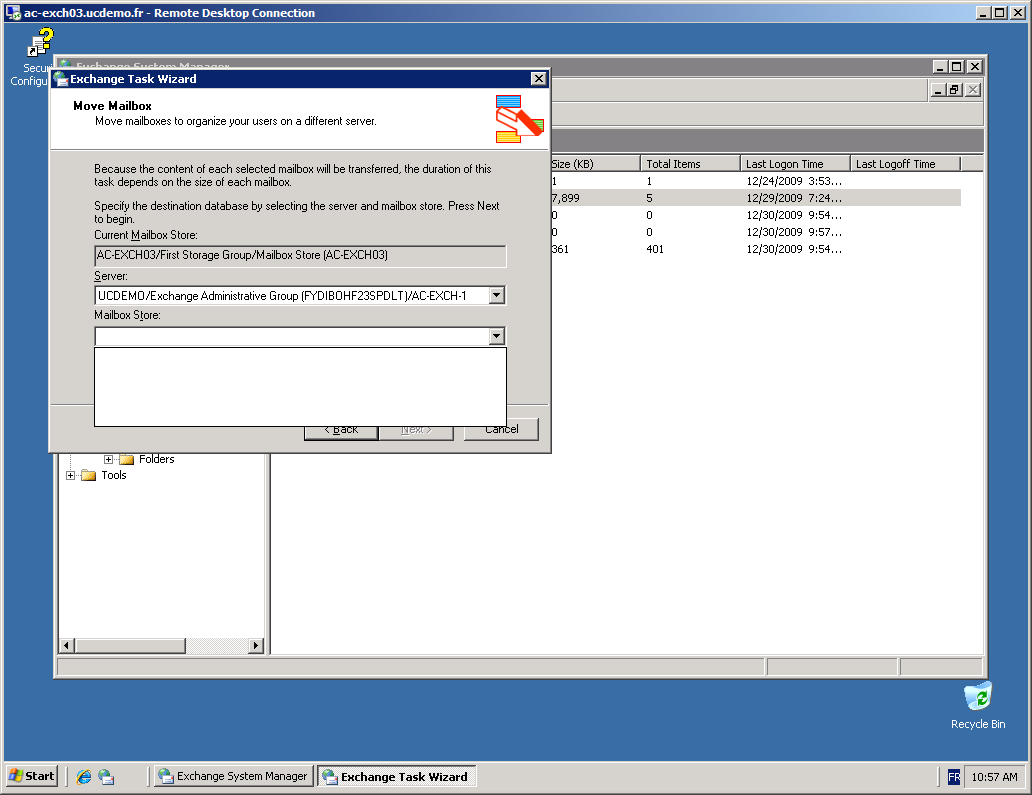
Pour déplacer une boite aux lettres, il faut juste spécifier la base de données de destination. Cette base de données de destination peut être sur le même serveur, sur un serveur différent, dans un autre domaine, dans un autre site Active Directory ou encore dans une autre forêt.

Le processus de migration des données des boites aux lettres est décrit en détail à cette adresse : <http://technet.microsoft.com/en-us/library/dd298174.aspx>

Dans notre cas, nous allons effectuer une migration des données de notre serveur dorsal Exchange 2003 vers notre serveur Exchange 2010 ayant le rôle de serveur de boites aux lettres.

Le serveur source tournant avec Exchange 2003 SP2, le déplacement de boites aux lettres s'effectuera en mode "offline". C’est-à-dire que les utilisateurs ne pourront pas accéder à leur boite aux lettres pendant le déplacement (Le déplacement online n'est possible que si le serveur source tourne avec Exchange 2007 SP2).

La demande de migration doit se faire depuis la ligne de commande d'administration de Exchange 2010 (Exchange Management Shell). Il n'est pas possible d'effectuer la demande de migration depuis le System Manager d'Exchange 2003, ce dernier ne voit pas les bases de données de destination :



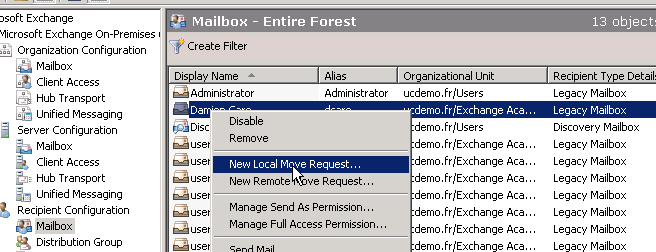
Nous allons donc procéder à la migration depuis Exchange 2010 depuis l'interface graphique pour une seule boite aux lettres et depuis Powershell pour une série de boites aux lettres:

#### Déplacement de boites aux lettre par interface graphique

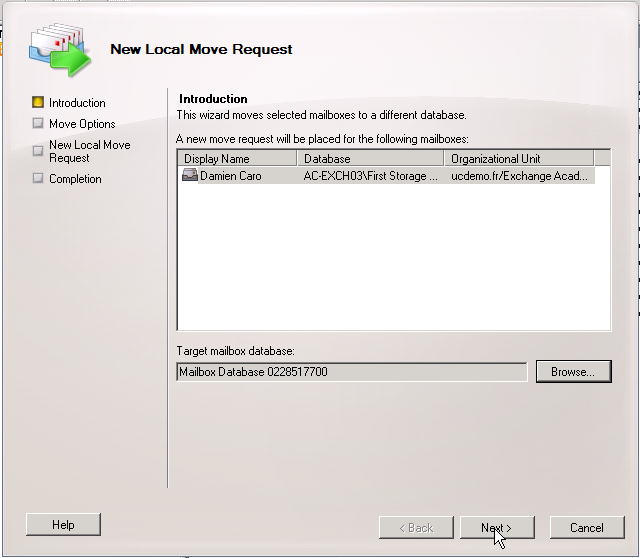
La demande de déplacement se fait depuis le conteneur "**Mailbox**" sous "**Recipient configuration**". Les boites aux lettres sur Exchange 2003 sont grisées, il est possible d'effectuer deux types de demandes de déplacement :

* Remote move request : Cette demande de déplacement est prévue pour un déplacement inter-organisation. Cette option est prévue principalement pour la gestion des cas où une partie de l'organisation est sur site et une autre partie de l'organisation est hébergée "dans les nuages".
* Local move request : Cette option est celle qui nous intéresse, il s'agit de réaliser un déplacement intra-organisation.

Choisissez la boite aux lettres à déplacer :



Renseignez les champs nécessaires aux déplacement de la boite aux lettres (en particulier la base de données de destination) :



Sélectionnez le comportement à adopter en cas d'incident sur la boite aux lettres (abandon total ou abandon seulement si un nombre d'erreur supérieur à une valeur personnalisable est rencontré).

A la fin de l'assistant, la boite aux lettres va apparaitre en couleur (indiquant un objet Exchange 2010) mais sera identifiée comme "User Mailbox" qu'une fois le déplacement terminé. L'état intermédiaire montrera ceci :



Une fois la migration terminée, voici ce qui apparait :

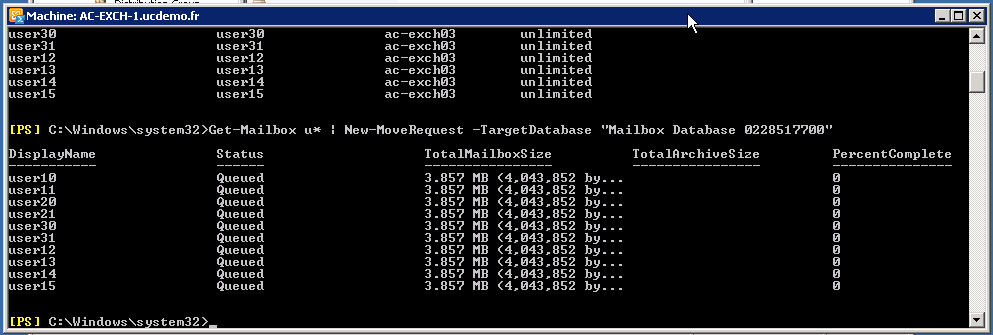


Cet état indique que la migration est terminée. L'utilisateur peut à ce moment se reconnecter à sa boite aux lettres.

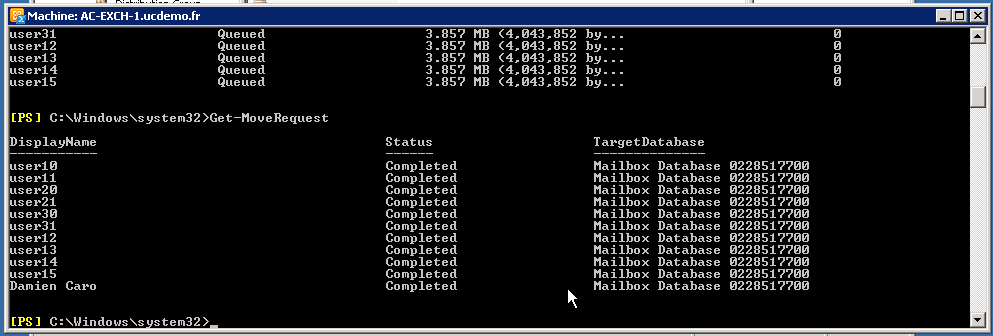
#### Déplacement de boites aux lettre par powershell

Si on a un grand nombre d'utilisateurs à migrer en bloc, je vous recommande de les migrer via powershell à travers le cmdlet **New-MoveRequest**.

Il est possible de donner à ce cmdlet une liste de boites aux lettres à migrer ou tout simplement de faire un filtre sur le cmdlet **Get-Mailbox**. Dans le cas de notre lab, nous avons utilisé cette option car elle permet de faire une sélection par exemple en se basant sur le début de l'alias de la boite aux lettres et de grouper tous ces utilisateurs sur une même base de données.

Dans notre lab, voici le retour du cmdlet powershell pour la migration des boites aux lettres d'exemple :  


Il est possible de suivre la procédure pendant qu'elle s'exécuter avec le cmdlet **Get-MoveRequest**. Voici un exemple de ce que retourne ce cmdlet :



Quand tous les états sont "Completed" cela veut dire que les migrations sont terminées.

## Conclusion et prochaines étapes

Au cours de ce module nous avons réalisé les étapes suivantes :

* Configuration du serveur d'accès client CAS d'Exchange 2010
* Re-paramétrage du serveur Frontal d'Exchange 2003
* Modification de la configuration DNS
* Déplacement des boites aux lettres vers Exchange 2010

Maintenant que nous avons déplacé les utilisateurs sur notre nouvelle infrastructure les prochaines étapes consistent à finir de déplacer les différents services d'Exchange 2003 vers Exchange 2010 avant de pouvoir supprimer ces serveurs de notre infrastructure. Nous réaliserons ces étapes dans le quatrième module.

Mais au préalable, dans le prochain module, nous allons ajouter la haute disponibilité à notre infrastructure Exchange 2010 en place. Dans le prochain module, nous allons créer un DAG et créer une réplique de la base de données de notre serveur AC-EXCH-1 sur AC-EXCH-2.