Installation et configuration de Exchange 2010

par Michaël Todorovic (Autres articles) (Blog)

Date de publication : 12 août 2010

Dernière mise à jour : 10 janvier 2011

Exchange est un serveur de messagerie collaborative (emails, gestion de calendrier, planification de réunions, carnet d'adresses centralisé, répondeur téléphonique). Dans cet article, je vais expliquer comment installer une architecture Exchange 2010 simple et comment la configurer pour qu'elle accomplisse sa fonction de serveur de messagerie.

Je vous invite à poser vos questions ou commenter cet article afin de l'améliorer :

I - Introduction

Exchange est un produit qui a commencé sa carrière en 1996. À l'époque, Active Directory n'existait pas. Depuis l'apparition d'Active Directory en 1999, Exchange se base dessus. Les versions avant Exchange 2000 embarquaient donc leur propre annuaire pour gérer les utilisateurs. Aujourd'hui, nous sommes à la version 2010. Cette version apporte de nombreux changements par rapport à la version 2007, notamment sur la partie haute disponibilité et les besoins matériels (revus à la "baisse"). Je ne vais pas présenter ces nouveautés en tant que telles. De nombreux webcasts sont disponibles sur le site de Microsoft pour découvrir les nouveautés entre Exchange 2007 et 2010. Dans ce tutoriel, je vais présenter les différents composants et technologies d'Exchange puis je commencerai par créer une architecture simple. Ensuite, nous verrons comment implémenter cette architecture. Nous n'allons pas voir les services de messagerie unifiée qui feront l'objet d'un autre article ni la mise en place d'une architecture en haute disponibilité.

II - Les différents composants d'Exchange

II-A - Les rôles

Depuis Exchange 2007, nous avons quatre rôles qui réalisent chacun une partie des fonctions d'Exchange. Cela permet une meilleure granularité pour le dimensionnement de votre architecture. Par exemple, si vous avez besoin de plus de puissance pour une fonction d'Exchange, il vous suffira d'isoler le rôle sur un ou plusieurs serveurs. À l'inverse, il sera possible de colocaliser différents rôles. Voyons quels sont ces rôles.

II-A-1 - Rôle CAS : Client Access Server ou rôle d'accès client

Comme son nom l'indique, ce rôle va servir aux clients pour accéder à leur compte Exchange. Cela comprend les accès Outlook, Outlook Web App, Outlook AnyWhere et ActiveSync. C'est ici que les clients vont se connecter.

II-A-2 - Rôle Mailbox : boîtes aux lettres

Ce rôle héberge les boîtes aux lettres de chaque utilisateur, matériel ou salle de l'organisation Exchange. Il héberge également les carnets d'adresses et permet la planification de réunions et des ressources associées.

II-A-3 - Rôle Transport Hub : routage des messages

Ce rôle gère le routage et la remise des messages dans l'organisation Exchange. Il gère également la transmission de messages hors de l'organisation. Il peut également filtrer les messages ou appliquer des règles de routage configurées par l'administrateur. Ce rôle peut également journaliser les messages pour se conformer aux réglementations en vigueur.

II-A-4 - Rôle Edge : passerelle email

Ce rôle est indépendant d'Active Directory et est généralement placé en DMZ. Il s'agit d'une passerelle email qui peut accepter les emails provenant d'Internet ou de serveurs d'organisations externes clairement identifiés. Ce serveur va pouvoir procéder à un scan antispam et antivirus grâce à *Forefront Protection for Exchange*. Les emails entrants ayant passé l'hygiène de messagerie seront routés vers les serveurs Transport Hub de l'organisation. Ce rôle ne peut pas être colocalisé avec d'autres rôles d'Exchange.

II-A-5 - Rôle UM : Unified Messaging ou messagerie unifiée

Depuis Exchange 2007 SP1, un cinquième rôle a été ajouté : la messagerie unifiée. Ce rôle permet la réception des messages vocaux et fax dans la boîte aux lettres de l'utilisateur. Il permet également la consultation d'Exchange

depuis un téléphone : vous pouvez ainsi écouter vos messages vocaux, emails et réunions. Vous pouvez également créer des messages ou contacter directement des personnes grâce à la consultation de votre carnet d'adresses. Le serveur vocal est capable de reconnaitre la voix (sans nécessiter de configuration préalable) ou alors de fonctionner en DTMF (touches numériques de votre téléphone).

II-B - Les noms des différentes technologies d'Exchange

II-B-1 - Autodiscover

Il s'agit d'un service Web qui existe depuis Exchange 2007. Les clients Outlook savent utiliser ce service depuis la version 2007. Autodiscover permet de découvrir automatiquement les paramètres du serveur Exchange à partir de l'adresse email de l'utilisateur (à condition d'avoir son login et son mot de passe). Le client prend le domaine email de l'utilisateur, y préfixe Autodiscover et forme ainsi un domaine sur lequel Autodiscover doit être hébergé. Par exemple, si l'utilisateur entre l'adresse email utilisateur@mondomaine.fr, le client va aller interroger Autodiscover.mondomaine.fr. Ce service est accessible via HTTPS uniquement.

II-B-2 - Outlook Web App

Avant Exchange 2010, cela s'appelait *Outlook Web Access*. Il s'agit d'une application Web qui permet l'accès à son compte Exchange depuis un simple navigateur. Outlook Web App est compatible avec la plupart des navigateurs du marché (autres que Microsoft). OWA permet d'accéder à la plupart des fonctions d'Outlook. L'interface est quasiment identique. Vous pourrez ainsi consulter et rédiger des emails, gérer votre agenda, vos contacts, vos messages vocaux, etc.

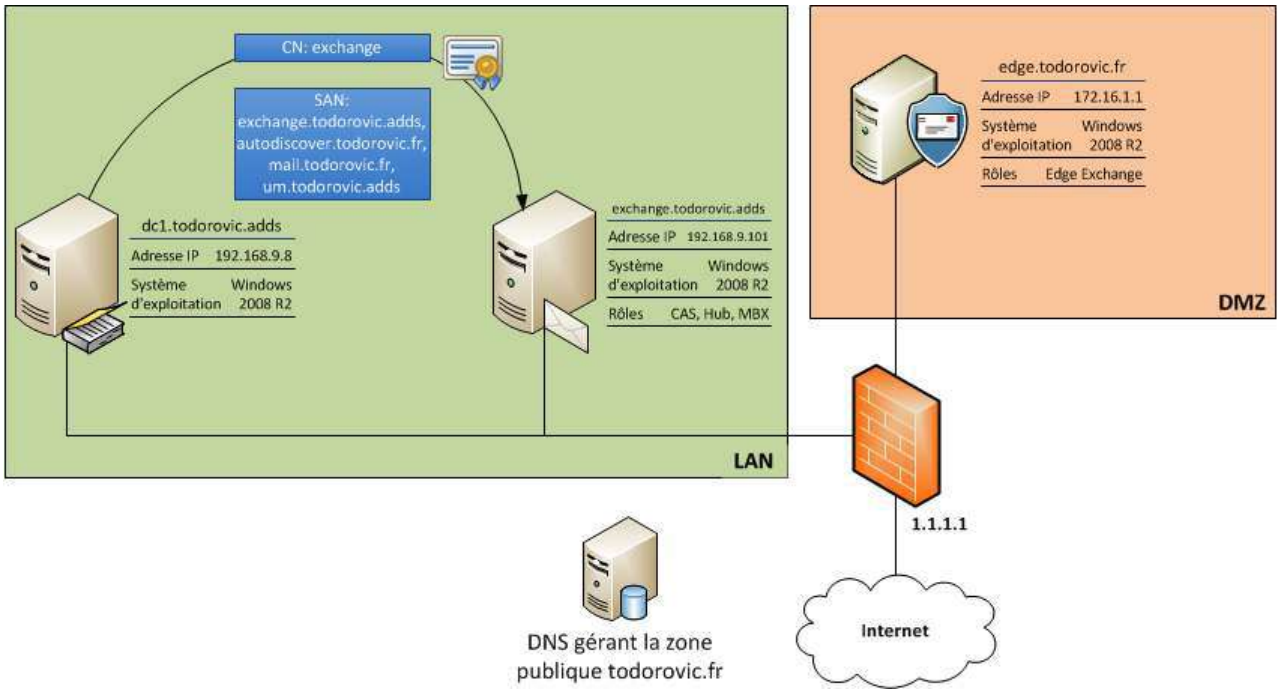
II-B-3 - Outlook Anywhere

Il s'agit encore une fois d'un service Web disponible par HTTPS.

III - Architecture

Je vais mettre en place une architecture simple. Je vais dans un premier temps configurer un serveur Exchange avec les rôles CAS, Hub et Mailbox colocalisés. Ensuite, j'ajouterai un serveur Edge pour gérer l'hygiène des messages et enfin je finirai par installer le rôle UM en collaboration avec **Office Communications Server**. Cette partie UM fera l'objet d'un autre article. Voici les besoins auxquels l'architecture devra répondre :

- envoi d'emails sur Internet ;
- réception d'emails ayant passé une hygiène de messagerie (antispam, antivirus) ;
- accès OWA depuis Internet et depuis le réseau interne avec la même adresse ;
- accès Outlook Anywhere ;
- Autodiscover.



Architecture répondant aux besoins

Tous les rôles d'Exchange sont supportés en environnement virtualisé à l'exception de l'UM. Dans le cadre d'une maquette, il est possible de virtualiser l'UM dans une certaine limite de performance.

Le serveur Exchange doit avoir une configuration IP fixe et faire partie du domaine Active Directory. Avant de procéder à l'installation d'Exchange, je conseille de mettre totalement à jour votre serveur.

Le serveur Exchange (exchange.todorovic.adds) possède les rôles CAS, Hub et Mailbox (MBX). Ce serveur devra posséder un certificat signé par une autorité de certification afin de ne pas avoir de problème de validation de certificat lors des accès client. L'autorité que j'utilise a été installée avec mon tutoriel **Configuration d'une infrastructure à clés publiques à 2 niveaux sous Windows 2008 (R2)**. Le certificat portera le nom NetBios du serveur à savoir "exchange" (sinon pas de validation de certificat lors de l'Autodiscover) et aura quatre noms alternatifs (SAN) : exchange.todorovic.adds (FQDN du serveur), mail.todorovic.fr (pour l'accès OWA, Outlook Anywhere et éventuellement Active Sync), Autodiscover.todorovic.fr (pour le service Autodiscover) et um.todorovic.adds (pour la messagerie unifiée si vous souhaitez l'activer plus tard : cela vous évitera de créer un nouveau certificat). Si vous voulez prendre en charge plusieurs domaines sur votre serveur Exchange, vous devrez ajouter ces domaines aux noms alternatifs de votre certificat.

Il faudra créer des alias dans le DNS pour que les noms alternatifs du serveur Exchange pointent sur celui-ci. Je vais utiliser encore une fois le principe du split-DNS pour simplifier la vie aux utilisateurs et aux administrateurs (même si cela requiert une petite gymnastique). Voici pourquoi j'utilise ce principe : **Nom de domaine privé/public ?** suivi de l'explication du split-DNS.

En DMZ, je vais placer un autre serveur Exchange qui ne sera pas dans Active Directory. Ce serveur aura le rôle Edge et assurera l'hygiène des messages. Ce serveur devra avoir un nom public pour fonctionner correctement. L'installation de ce serveur Edge sera traitée dans un prochain article.

Cette architecture est loin d'être complexe puisqu'il n'y a qu'un seul serveur. Elle permettra cependant de comprendre les bases d'Exchange. Cette partie architecture demande des précisions sur les licences. C'est en effet un point généralement mal compris.

IV - Un petit point sur les licences

IV-A - Côté serveur : licences Exchange

Les licences Exchange sont simples : il faut une licence par instance d'Exchange. Cela veut dire que si vous avez deux serveurs Exchange, il vous faudra deux licences. Le serveur Edge compte pour un serveur Exchange et est donc soumis au même principe.

Il existe deux éditions du serveur Exchange : Standard et Entreprise. La principale différence se fait sur le nombre de bases de données que le serveur peut posséder. Une édition standard peut gérer jusqu'à cinq bases de données alors que l'édition entreprise peut gérer jusqu'à 100 bases de données.

Introduction au modèle de licences pour Exchange Server 2010 : Fonctionnalités d'Exchange Server 2010 par type de licences.

IV-B - Côté client : CAL Exchange

Ce sont ces licences qui portent souvent à confusion. Il existe deux types de CAL : Standard et Entreprise. Si vous voulez accéder aux fonctions standard d'Exchange, il vous faudra une CAL standard. Si vous souhaitez accéder aux fonctions avancées d'Exchange, il vous faudra une CAL standard et une CAL entreprise : la standard donne accès à l'entreprise. Ces CAL n'ont rien à voir avec l'édition de votre architecture Exchange puisque la seule différence sur ces éditions est le nombre de bases gérées. Vous pourrez donc installer une édition standard et utiliser des CAL entreprise et inversement.

Pour savoir de quel type de CAL vous avez besoin, consultez la page ***Introduction au modèle de licences pour Exchange Server 2010 : Exchange 2010 Client Access Licenses (CAL).***

Pour chaque CAL Exchange, il vous faudra une CAL Windows Server. Si vous souhaitez utiliser la gestion des droits via ADRMS, il vous faudra une CAL RMS. Si vous utilisez Active Directory et un Windows client, vous avez déjà dû acheter les CAL Windows Server : il ne faut pas racheter à nouveau des CAL Windows Server puisque vous les possédez déjà.

IV-C - Connecteur externe Exchange

Ce connecteur permet un nombre illimité de clients externes tels que des partenaires, les fournisseurs ou des clients.

V - Installation

V-A - Les prérequis

Exchange Server a besoin d'Active Directory (au minimum sur Windows Server 2003) pour fonctionner. Active Directory va servir à stocker différentes données et également les comptes utilisateurs activés pour la messagerie.

Plusieurs rôles et fonctionnalités sont requis pour l'installation d'Exchange. Exchange est fourni avec plusieurs fichiers de configuration selon les rôles à installer. Ces fichiers, au format XML, se trouvent dans le répertoire Scripts du DVD. Pour installer les prérequis d'une installation typique d'Exchange, lancez :

```
ServerManagerCmd -ip E:\Scripts\Exchange-Typical.xml
```

Vous pouvez également installer ces prérequis avec PowerShell :

```
Import-Module ServerManager
Add-WindowsFeature NET-Framework,NET-HTTP-Activation,Web-Server,Web-ISAPI-Ext,Web-Basic-Auth,Web-Digest-Auth,Web-Windows-Auth,Web-Dyn-Compression,Web-Metabase,Web-Net-Ext,Web-Lgcy-Mgmt-Console,WAS-Process-Model,RSAT-ADDS,RSAT-Clustering,RSAT-Web-Server,RPC-Over-HTTP-proxy
```

- NET-Framework : Fonctionnalités du .NET Framework 3.5.1 ;
- NET-HTTP-Activation : Activation HTTP ;
- Web-Server : Serveur Web (IIS) ;
- Web-ISAPI-Ext : Extensions ISAPI ;
- Web-Basic-Auth : Authentification de base ;
- Web-Digest-Auth : Authentification Digest ;
- Web-Windows-Auth : Authentification Windows ;
- Web-Dyn-Compression : Compression de contenu dynamique ;
- Web-Metabase : Compatibilité avec la métabase de données ;
- Web-Net-Ext : Extensibilité .NET ;
- Web-Lgcy-Mgmt-Console : Outils de gestion IIS 6 ;
- WAS-Process-Model : Modèle de processus ;
- RSAT-ADDS : Outils AD DS ;
- RSAT-Clustering : Outils de clustering avec basculement ;
- RSAT-Web-Server : Outils du serveur Web (IIS) ;
- RPC-Over-HTTP-proxy : Proxy RPC sur HTTP.

Vous devrez ensuite changer le mode de démarrage du service de partage de ports net.tcp pour le passer en automatique. Vous pouvez passer par la MMC services ou passer en PowerShell :

```
Set-Service NetTcpPortSharing -StartupType Automatic
```

Enfin, il vous faudra installer le Filter Pack d'Office 2007 64 bits disponible **ici (FilterPackx64.exe)**. Ce pack est utilisé pour l'indexation et le scan des fichiers Office. Si vous le souhaitez, il est possible d'installer le Microsoft Office 2010 Filter Packs 64 bits disponible **ici (FilterPack64bit.exe)**. Vous pouvez également ajouter d'autres iFilters comme l'**Adobe PDF iFilter**.

Vous pouvez maintenant commencer à préparer l'Active Directory pour ensuite installer Exchange.

V-B - Préparation de l'Active Directory

La préparation de votre Active Directory se déroule en trois étapes. La première consiste à préparer le schéma Active Directory. Assurez-vous d'avoir un compte ayant les permissions adéquates. Afin de voir si la préparation s'effectue correctement, ouvrez une invite de commande et allez sur le DVD Exchange puis exécutez :

```
Setup /PrepareSchema
```

Si vous avez plusieurs contrôleurs de domaine, attendez la réplication ou forcez-la. Vous pourrez ensuite préparer votre forêt. Vous devrez préciser le nom de votre organisation. Cela correspond au nom court de votre forêt (sans TLD).

```
Setup /PrepareAD /OrganizationName:todorovic
```

Encore une fois, attendez la réplication ou forcez-la si vous avez plusieurs contrôleurs de domaine. Enfin, vous pourrez préparer votre domaine.

```
Setup /PrepareDomain
```

Si vous avez plusieurs domaines d'une même forêt que vous souhaitez préparer, vous pourrez exécuter :

```
Setup /PrepareAllDomains
```

Attendez à nouveau la réplication ou forcez-la. Vous pourrez ensuite commencer à installer votre serveur Exchange.

V-C - Déploiement

Commencez par lancer l'installation. Sur Windows 2008 R2, Windows Installer 4.5 est installé par défaut et si vous avez suivi l'installation des prérequis, .NET 3.5 SP1 devrait déjà être installé. On commence donc à l'étape 3 !

Lancement du setup

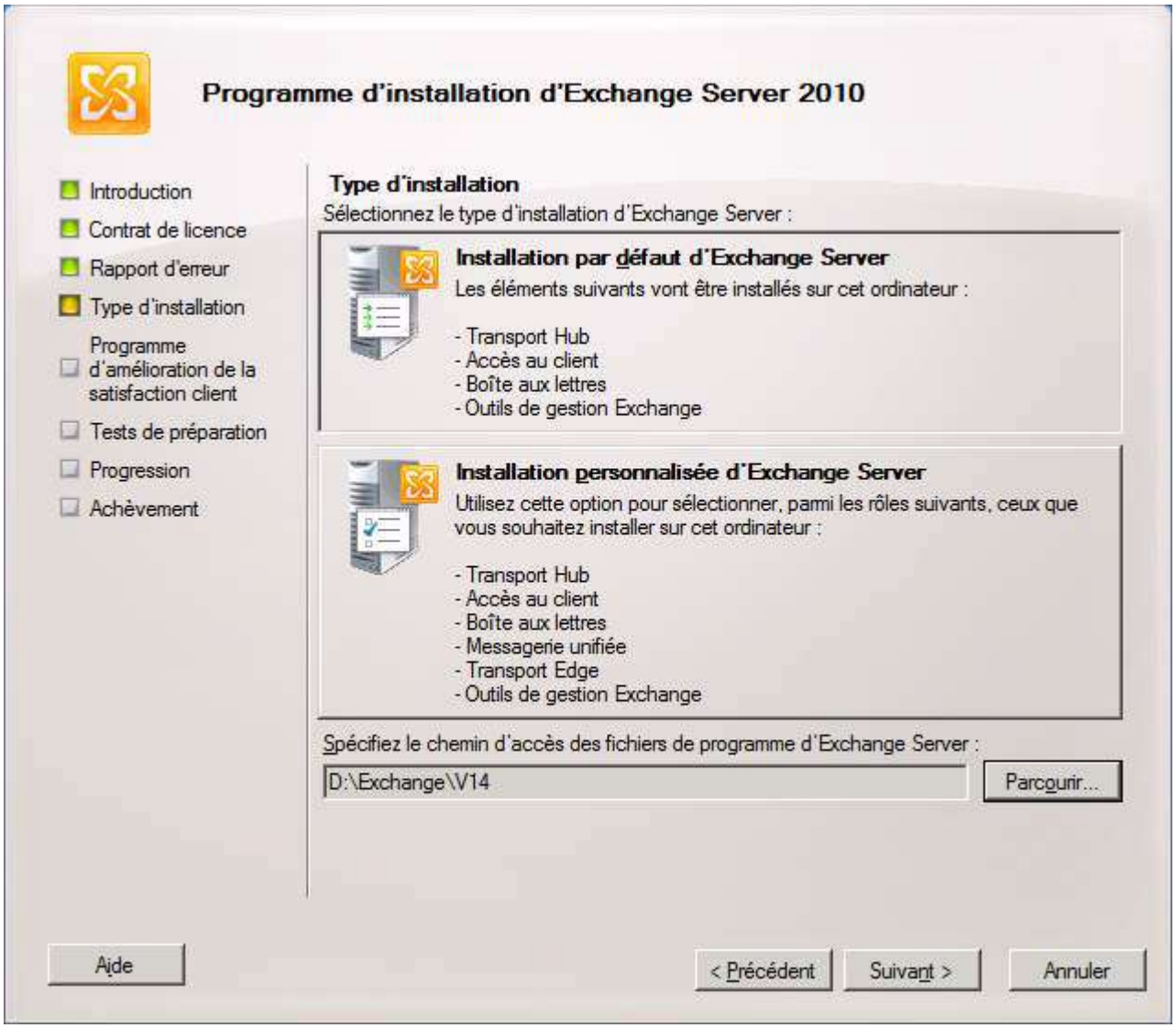
Le DVD embarque plusieurs langues : à moins que votre langue ne soit pas sur le DVD, vous pourrez cliquer sur *Etape 3 : Choisir l'option de langue d'Exchange, Installer uniquement les langues à partir du DVD*.

Sélection des sources de langage

Commencez l'assistant d'installation en cliquant sur *Etape 4 : Installer Microsoft Exchange*.

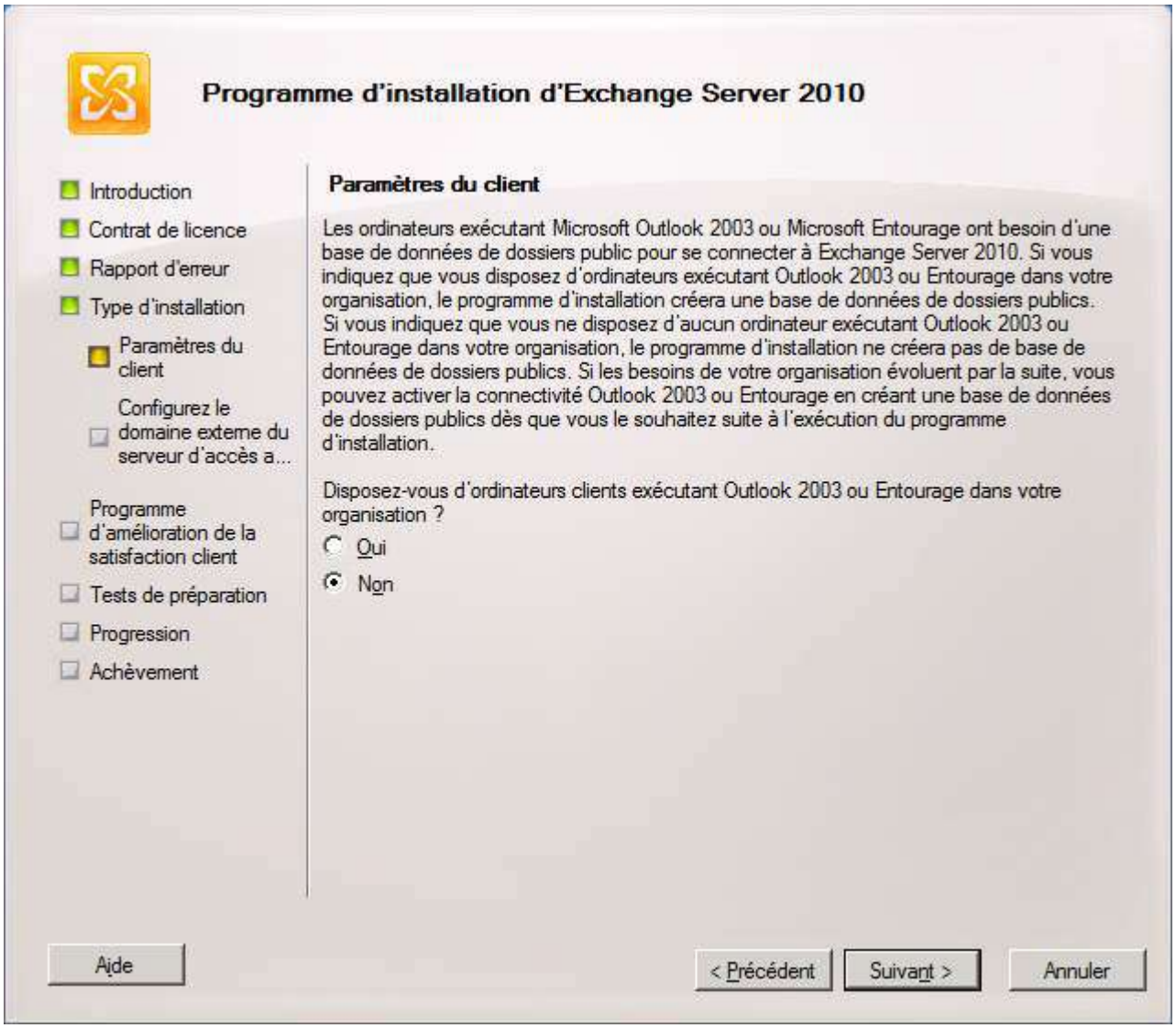
Installation

Après avoir passé l'introduction, accepté le contrat de licence et choisi votre mode de rapport d'erreur, vous aurez le choix entre une installation typique ou personnalisée. L'installation personnalisée vous permet d'installer les rôles dont vous avez besoin alors que l'installation typique installera les rôles CAS, Hub et Mailbox ainsi que les outils de gestion Exchange. Je vais procéder à l'installation typique. Comme d'habitude, choisissez d'installer le produit sur un disque non système.



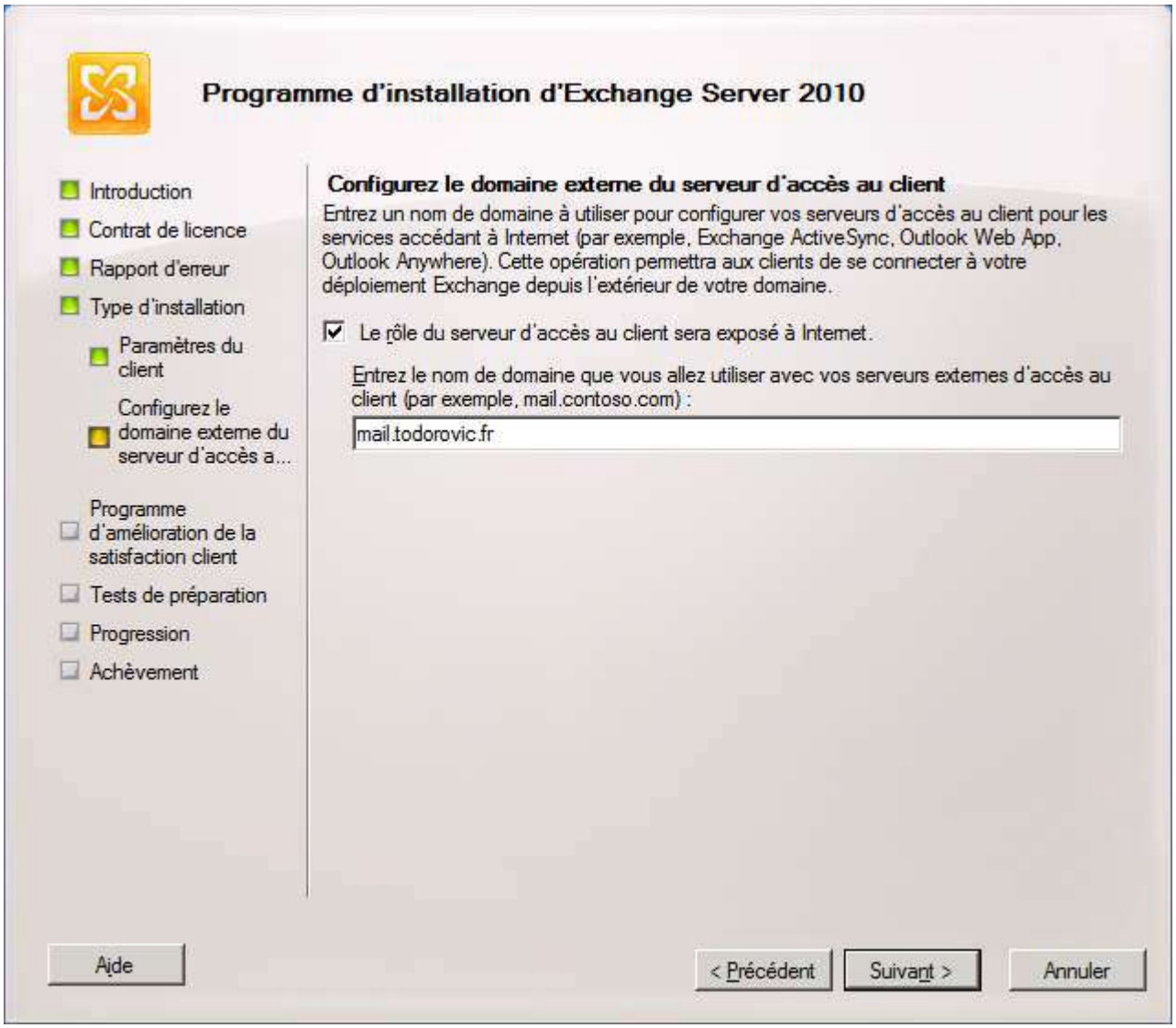
Sélection du type d'installation

L'assistant vous demande ensuite si votre réseau contient des clients Outlook 2003 ou Entourage (Mac OS). Cela permet d'assurer une compatibilité pour ces clients anciens. Je n'ai pas ces clients donc je fais le choix correspondant.



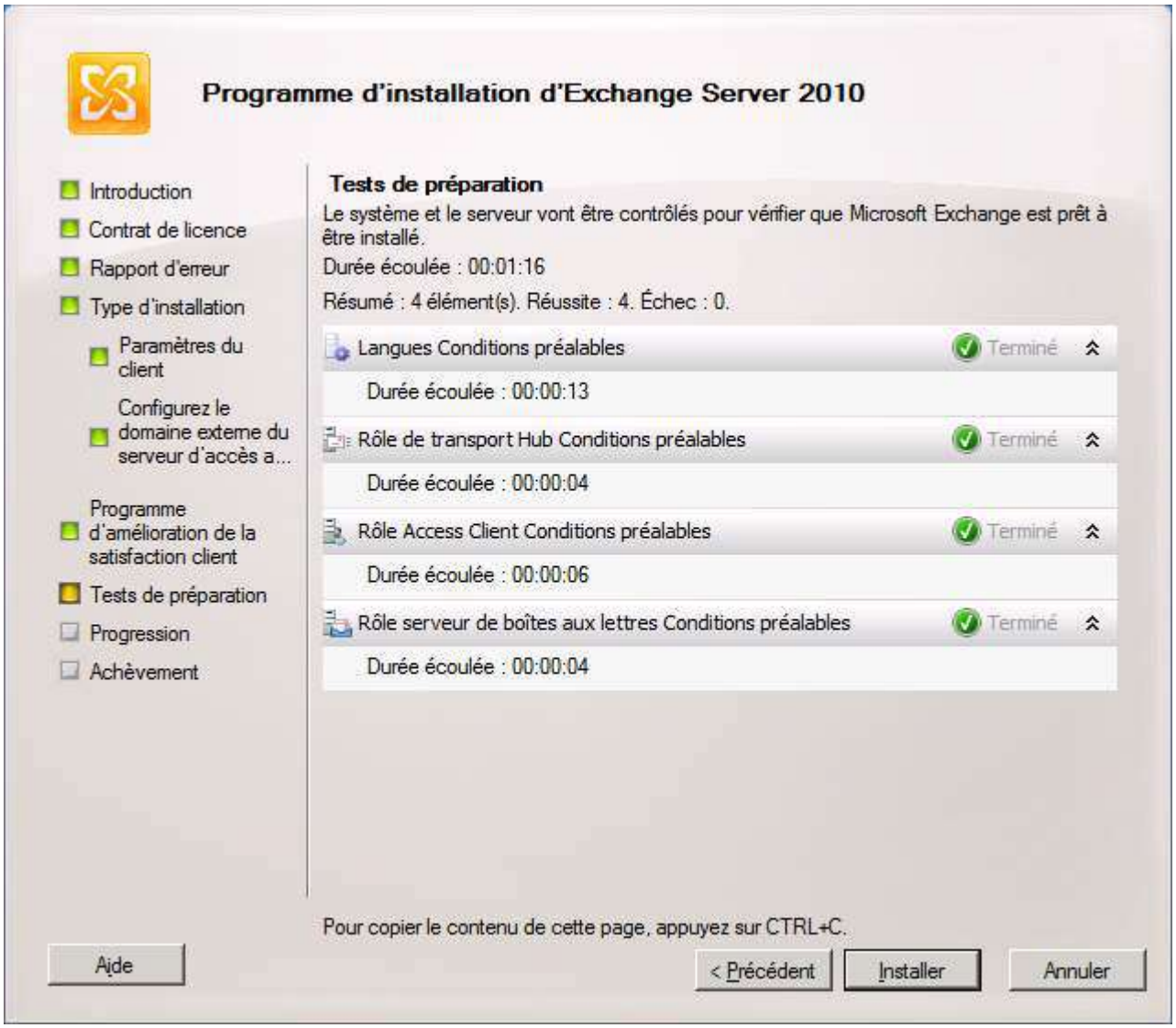
Clients anciens ou Mac ?

Si vous souhaitez rendre votre rôle d'accès client disponible depuis Internet pour OWA, Outlook Anywhere ou Active Sync, vous devrez indiquer le nom externe qu'aura votre serveur.



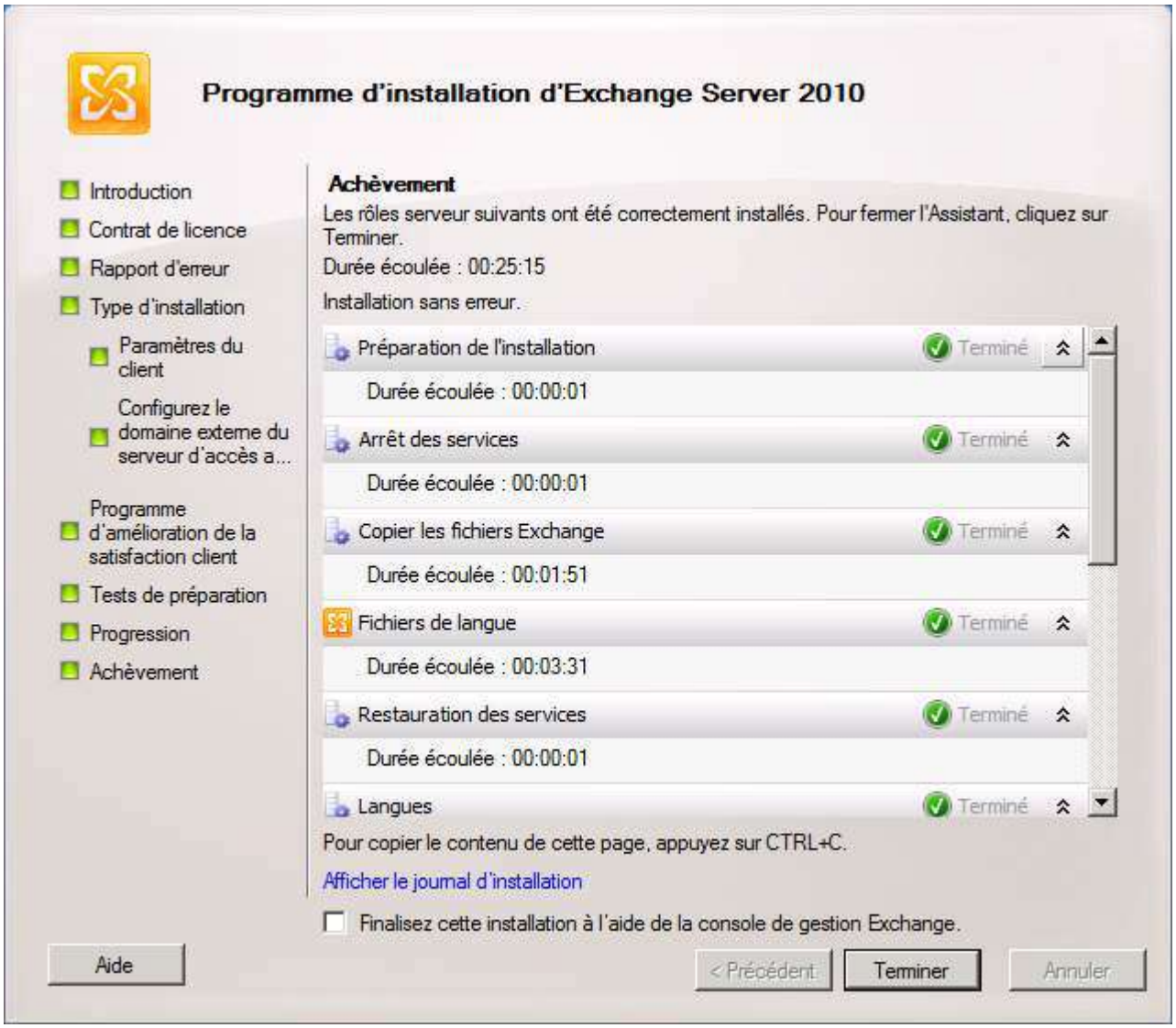
Exposition du rôle d'accès client sur Internet

Avant de lancer l'installation, Exchange procède à quelques tests afin de s'affranchir d'éventuels problèmes lors de l'installation. Si les tests sont effectués avec succès, vous ne devriez pas avoir de problème lors de l'installation.



Tests de préparation à l'installation

Une fois les tests effectués, vous pouvez lancer l'installation. Elle peut durer plus ou moins longtemps selon votre serveur et les rôles à installer. Dans mon cas, Exchange a mis 25 minutes à s'installer : je rédige cet article sur un portable. Il n'est donc pas adapté aux besoins d'Exchange. Sur un serveur dimensionné correctement, l'installation sera plus rapide.



Installation terminée

Ne lancez pas la console de gestion d'Exchange immédiatement : il est préférable de mettre à jour dès maintenant votre serveur Exchange via Microsoft Update.

VI - Configuration

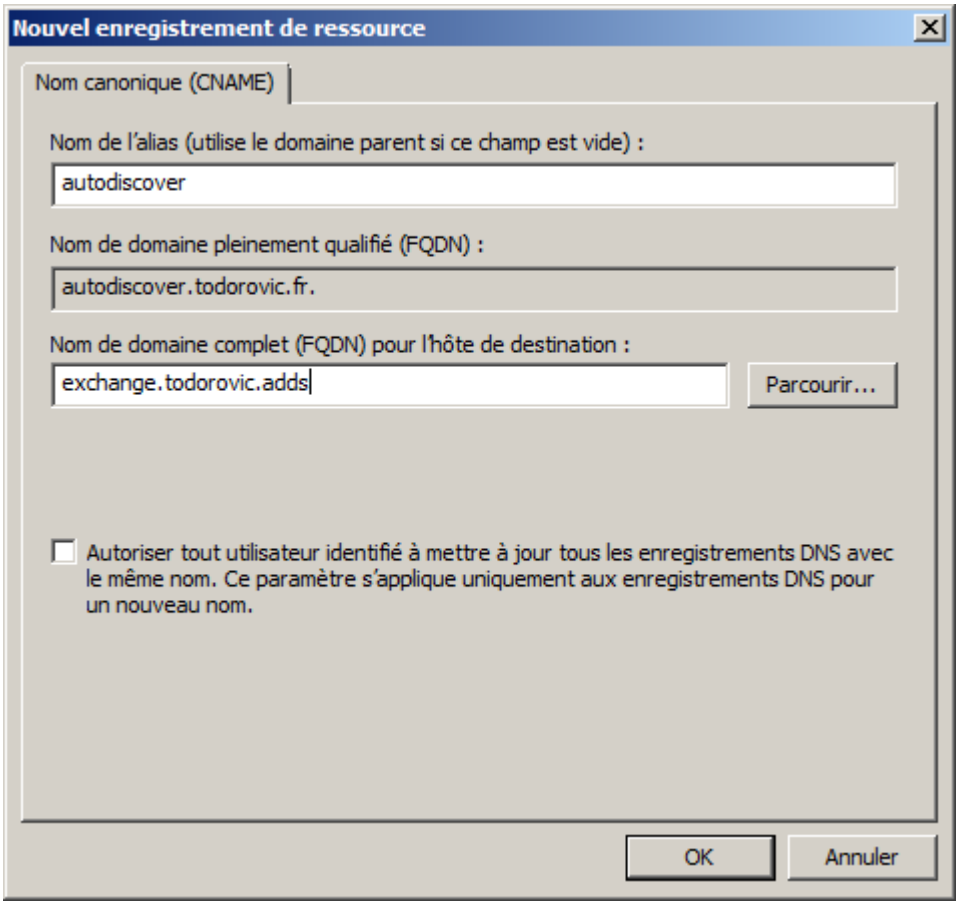
Depuis Exchange 2007, les serveurs sont intégralement administrables via Powershell. Le mode graphique de l'administration d'Exchange pilote en fait les cmdlets Powershell. Il est donc possible d'associer une commande Powershell à chaque action en mode graphique. L'inverse n'est cependant pas vrai : certaines choses ne sont faisables qu'en Powershell.

VI-A - DNS

Afin de rendre possible l'accès à votre serveur avec d'autres noms que le nom de machine, il est nécessaire d'ajouter des alias dans votre DNS (celui installé sur votre Active Directory par exemple). Le but est également de proposer une seule adresse d'accès à vos utilisateurs, qu'ils soient dans l'entreprise ou à l'extérieur. Il est en effet préférable de retenir que l'accès webmail est sur https://mail.monentreprise.fr quelque soit l'endroit où l'on est, que de retenir https://exchange.domainead.adds pour l'accès interne et https://mail.monentreprise.fr pour les accès externes.

VI-A-1 - Autodiscover

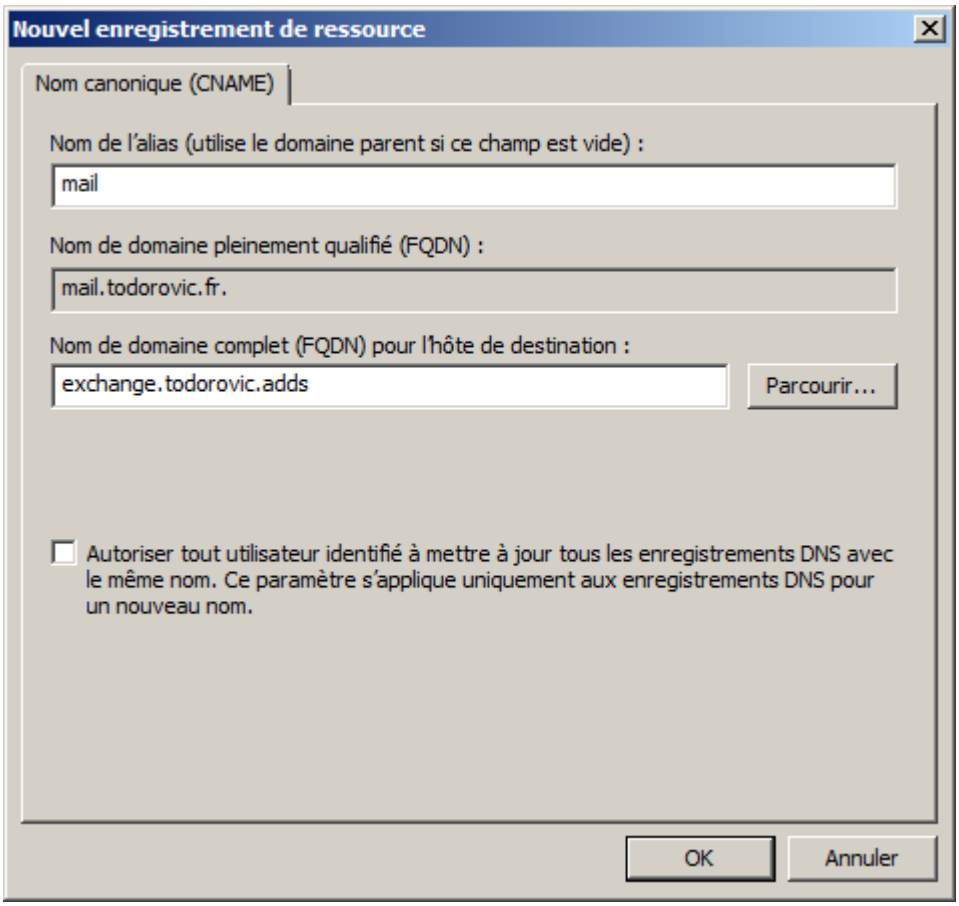
Si vous souhaitez utiliser Autodiscover, il suffit de créer un alias Autodiscover pointant sur votre serveur CAS. Dans la console de gestion de votre DNS interne, créez un enregistrement CNAME dans la zone publique (à usage privé). Ici, je fais pointer Autodiscover.todorovic.fr vers exchange.todorovic.adds : seuls les clients étant dans le réseau de l'entreprise pourront accéder à cet alias.



Création de l'alias Autodiscover interne

VI-A-2 - OWA, Outlook Anywhere

Par défaut, les accès OWA et Outlook Anywhere sont communs en termes de nom de serveur. Dans l'architecture que je propose, OWA et Outlook Anywhere sont accessibles via mail.todorovic.fr. On va donc créer l'alias pour les utilisateurs à l'intérieur de l'entreprise.



Création de l'alias pour les accès OWA et Autodiscover

Si vous souhaitez donner l'accès OWA via un autre nom que l'accès Outlook Anywhere, pensez à inclure ce nouveau nom alternatif dans le certificat que l'on va créer un peu plus loin.

VI-A-3 - Enregistrement MX

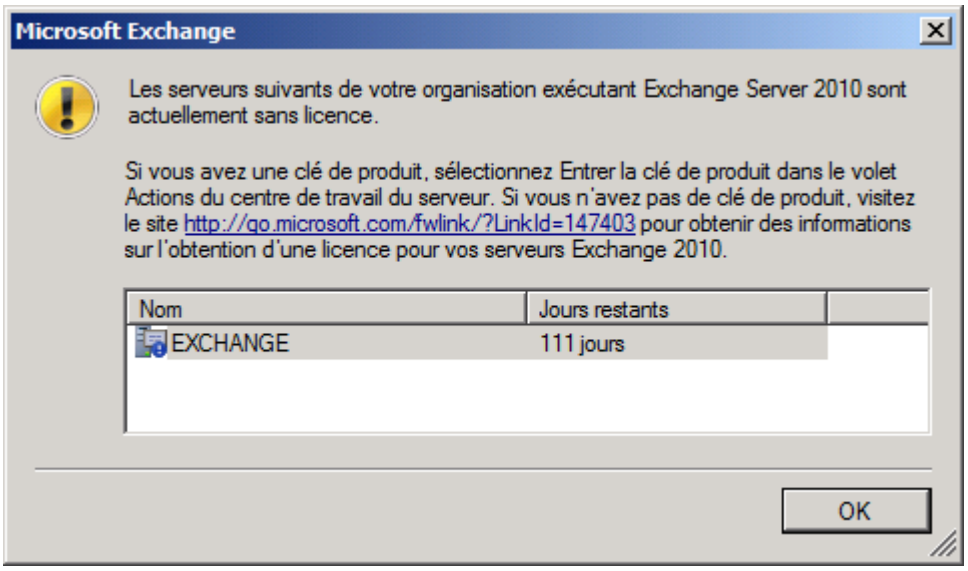
L'enregistrement MX va permettre aux autres serveurs email d'Internet de trouver votre serveur SMTP. Dans votre DNS public, il faudra créer un enregistrement A qui désignera votre serveur SMTP. Le choix du nom est libre. Vous devrez indiquer dans cet enregistrement A l'IP publique pour accéder à votre serveur.

Vous devrez ensuite créer un enregistrement MX. Cet enregistrement (nommé généralement mx.monentreprise.fr ou mail.monentreprise.fr) est en fait un pointeur vers vos serveurs SMTP. Vous devrez donc indiquer le nom de votre serveur SMTP (créé précédemment avec l'enregistrement A) et le poids (ou priorité) de cet enregistrement.

La pondération de l'enregistrement permet d'avoir des serveurs de backup si toutefois votre serveur STMP devient indisponible. Plus le poids d'un enregistrement est faible, plus cet enregistrement aura de "valeur". Les serveurs SMTP essaieront de contacter les serveurs de poids faible avant les serveurs de poids fort. Pensez donc à correctement indiquer vos poids dans votre DNS. Ne donnez pas un poids trop faible (afin de pouvoir mettre des serveurs plus prioritaires) ni trop fort (pour pouvoir mettre des serveurs de backup).

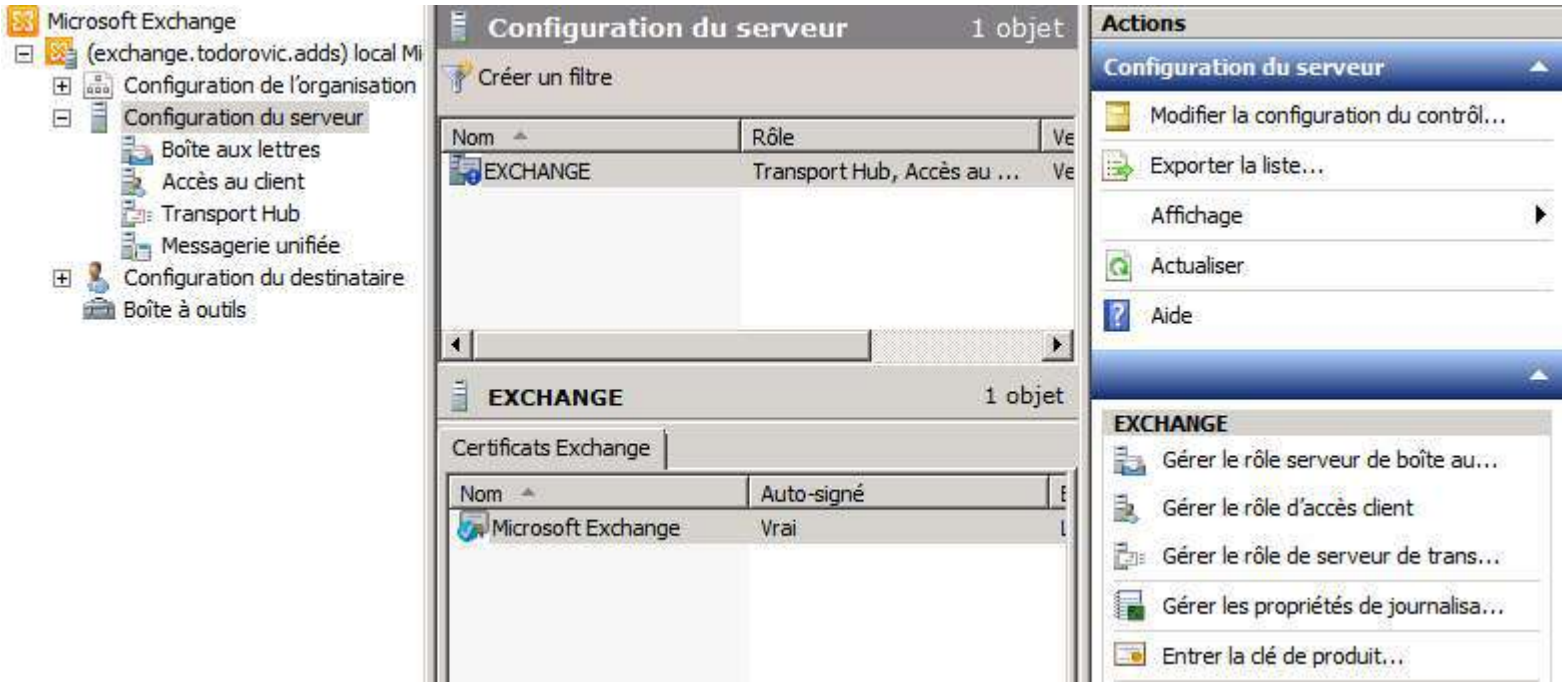
VI-B - Passage en mode avec licence

Lors de l'installation, l'assistant ne demande pas la clé Exchange. Vous devez l'entrer manuellement après l'installation du serveur. Si vous ne le faites pas, vous serez alors en mode d'évaluation de 120 jours (toutes les fonctionnalités sont accessibles durant ce temps).



Avertissement sur le mode de licence

Pour entrer votre clé de licence, vous avez deux moyens : en mode graphique ou en Powershell. En mode graphique, ouvrez *(nom_serveur) local Microsoft Exchange, Configuration serveur*. Dans le panneau de droite, cliquez sur *Entrer la clé de produit*.



Entrer la clé de produit en mode graphique

L'autre méthode est de passer par Powershell. Ouvrez **Exchange Management Shell (EMS)** puis exécutez :

```
Set-ExchangeServer -Identity exchange.todorovic.adds -ProductKey XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

Votre clé va alors être validée et vous serez prévenu qu'il faut redémarrer le service *Banque d'informations* d'Exchange pour prendre en compte ce changement. Il faudra en effet redémarrer ce service si votre serveur héberge le rôle Mailbox, ce qui est le cas dans cet article.

```
[PS] C:\Users\administrateur.TODOROVIC\Desktop>Set-ExchangeServer -Identity exch
ange.todorovic.adds -ProductKey [redacted]
AVERTISSEMENT : Clé de produit validée et ID de produit créé. Ce changement ne
prendra effet qu'après redémarrage du service de banques d'informations.
```

Licence entrée via Powershell

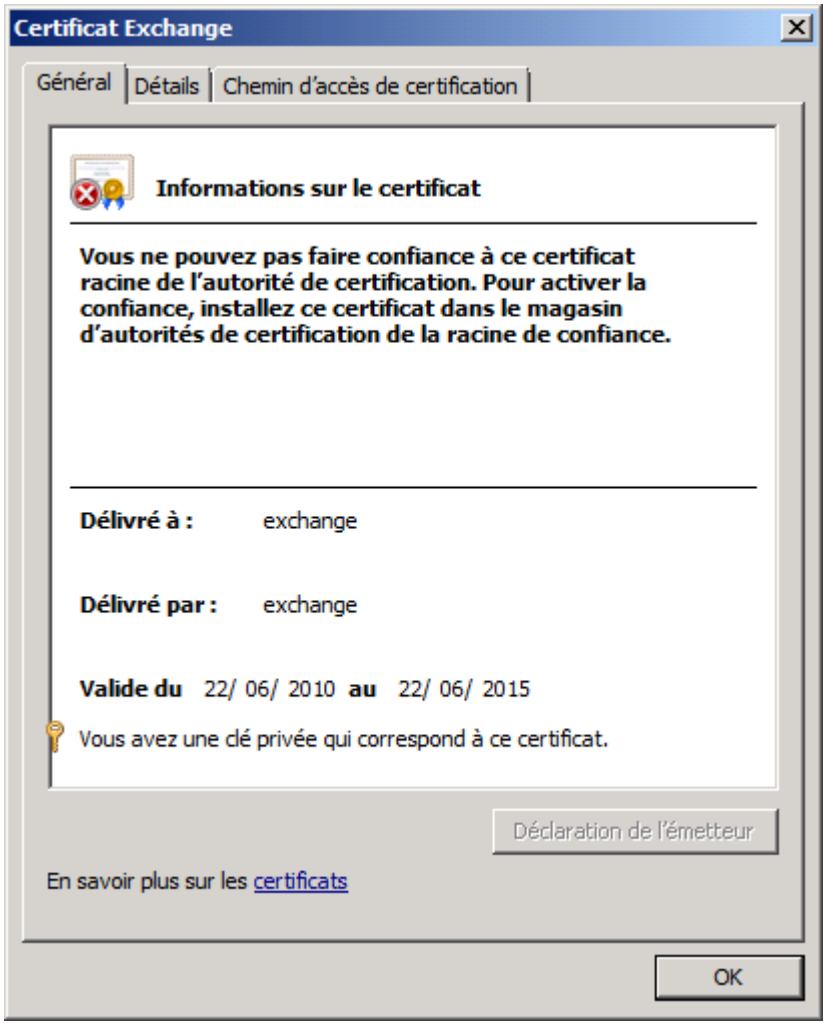
Pour redémarrer le service banque d'informations, vous pouvez redémarrer le service via la MMC ou en Powershell.

```
Restart-Service msexchangeis
```

Votre serveur est maintenant avec une licence valide et active.

VI-C - Création et assignation du certificat

Par défaut, Exchange se crée un certificat auto-signé qu'il assigne aux différents services. Le problème de ce genre de certificat est qu'on ne peut pas lui faire confiance. Par exemple, si mon serveur vous dit qu'il s'est auto-proclamé www.votrebanque.fr (alors qu'en réalité c'est www.voleur-de-compte-bancaire.fr), allez-vous lui faire confiance ? J'espère pour vous que non. Le certificat étant auto-signé, il est réputé comme n'étant pas de confiance : vous aurez alors constamment des erreurs de validation SSL lors des différents accès au serveur.



Certificat auto-signé

C'est pour cela que l'on va créer un certificat signé par notre autorité de certification interne (ou une autorité tierce de confiance). Nos collaborateurs font confiance à notre autorité de certification interne (distribution du certificat racine par GPO), ils n'auront donc pas de problème de validation. Voyons comment faire.

La génération du certificat signé peut se faire de différentes manières. Pour ma part, j'utilise la ligne de commande et certreq. Cette méthode a l'avantage de fonctionner avec des PKI sous Windows 2003, 2008 et 2008 R2. Vous trouverez plus d'informations sur cette méthode sur mon blog : **Comment générer un certificat en ligne de commande ?**.

Je vais utiliser un fichier texte nommé exchange.todorovic.adds.inf dont le contenu est ci-dessous. Le nom commun du certificat est le nom complet du serveur à savoir exchange.todorovic.adds. Les noms alternatifs (SAN) sont exchange.todorovic.adds(=FQDN du serveur), Autodiscover.todorovic.fr, mail.todorovic.fr et um.todorovic.adds. Il est important de noter que tout ceci est réalisé sur le compte de l'ordinateur (MachineKeySet=TRUE).

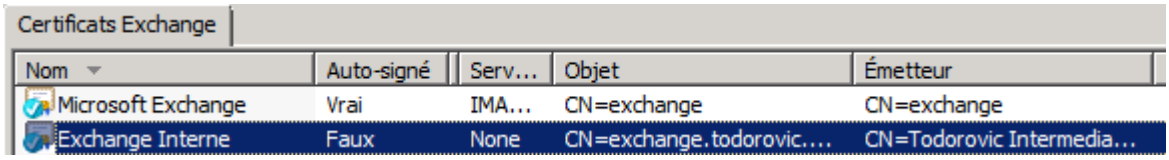
```
[Version]
Signature="$Windows NT$"

[NewRequest]
FriendlyName="Exchange Interne"
Subject="CN=exchange.todorovic.adds"
KeyLength=1024
Exportable=FALSE
MachineKeySet=TRUE
PrivateKeyArchive=FALSE
KeyUsage=0xa0

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1
OID=1.3.6.1.5.5.7.3.2

[RequestAttributes]
CertificateTemplate=WebServer
SAN="dns=exchange.todorovic.adds&dns=Autodiscover.todorovic.fr&dns=mail.todorovic.fr&dns=um.todorovic.adds"
```

Pourquoi répéter le nom du serveur Exchange ? Il est obligatoire d'avoir un nom de certificat. Nous utilisons les extensions SAN, cela change le comportement de la lecture du certificat. Dès que vous ajoutez l'attribut SAN à un certificat, son nom commun est ignoré. Il est donc nécessaire de dupliquer le nom complet du serveur Exchange sinon lors de l'Autodiscover sur Outlook, vous serez averti que le nom présenté est différent du nom du certificat alors que le nom est correct.

En ligne de commande, exécutez :

```
certreq -new exchange.todorovic.adds.inf exchange.todorovic.adds.req
certreq -submit exchange.todorovic.adds.req exchange.todorovic.adds.crt
certreq -accept exchange.todorovic.adds.crt
```

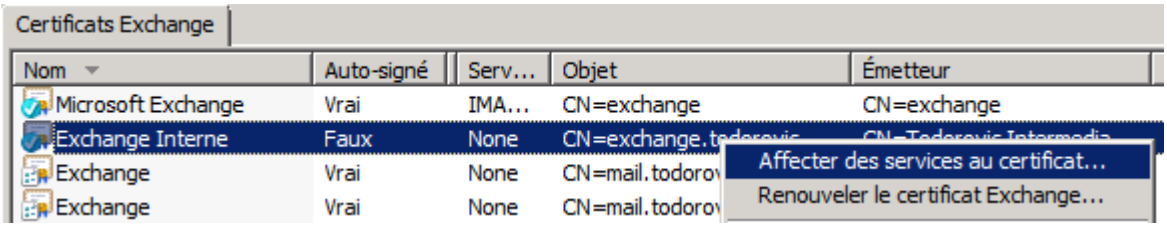
La première ligne crée une nouvelle clé privée et la demande de certificat associée. La deuxième ligne soumet le certificat à l'autorité de certification connue et enregistre le certificat. La dernière associe le certificat à la clé privée dans le magasin personnel de l'ordinateur. Si vous allez dans la configuration serveur (là où on peut entrer la clé produit), vous trouverez alors un nouveau certificat non auto-signé.



Certificat signé par l'autorité de certification interne

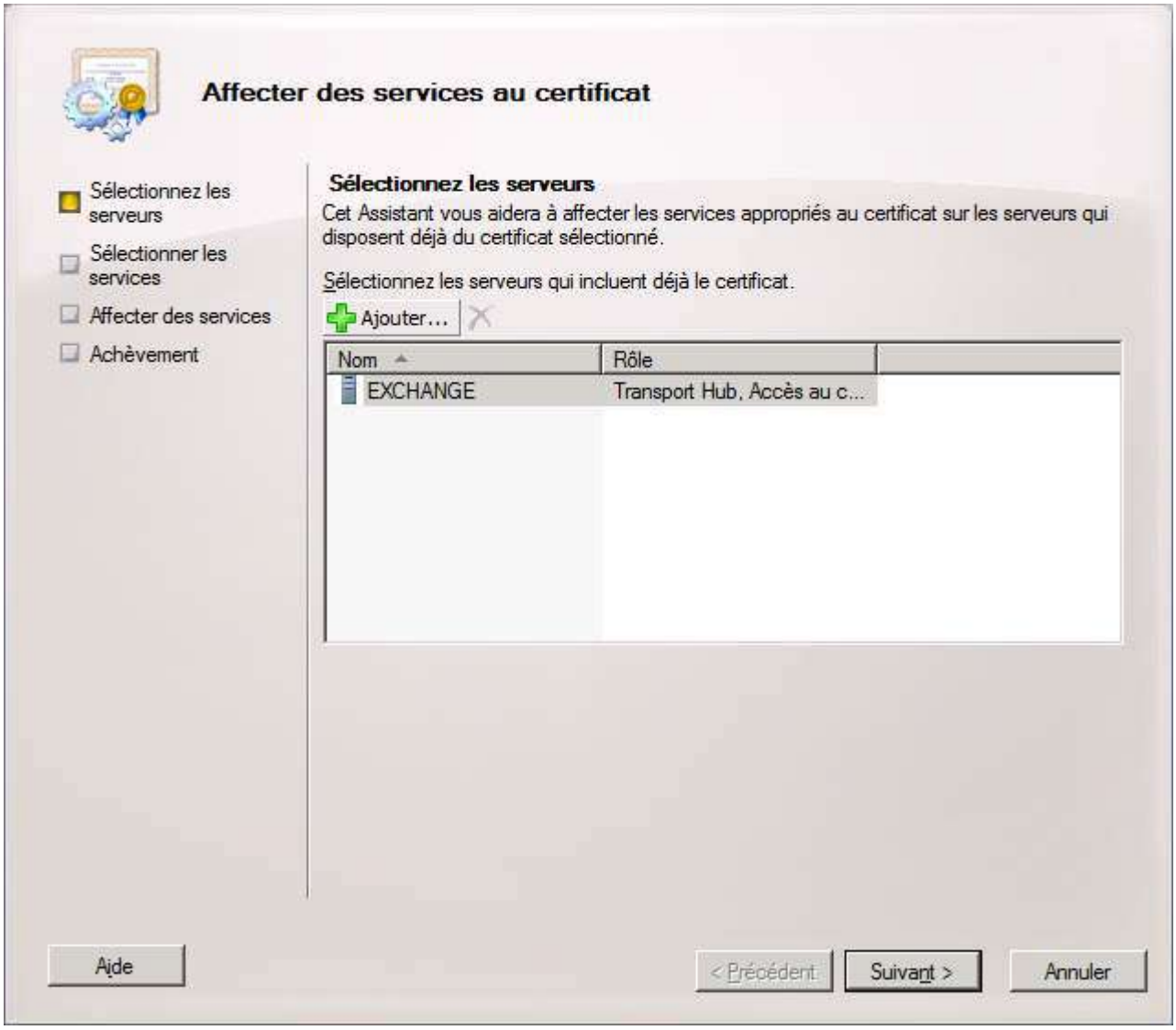
Il ne reste plus qu'à assigner le certificat aux services Exchange. Vous pouvez le faire en mode graphique ou Powershell.

Dans la configuration serveur, faites un clic droit sur le certificat que vous venez de créer puis *Affecter des services au certificat*.



Affectation des services au certificat

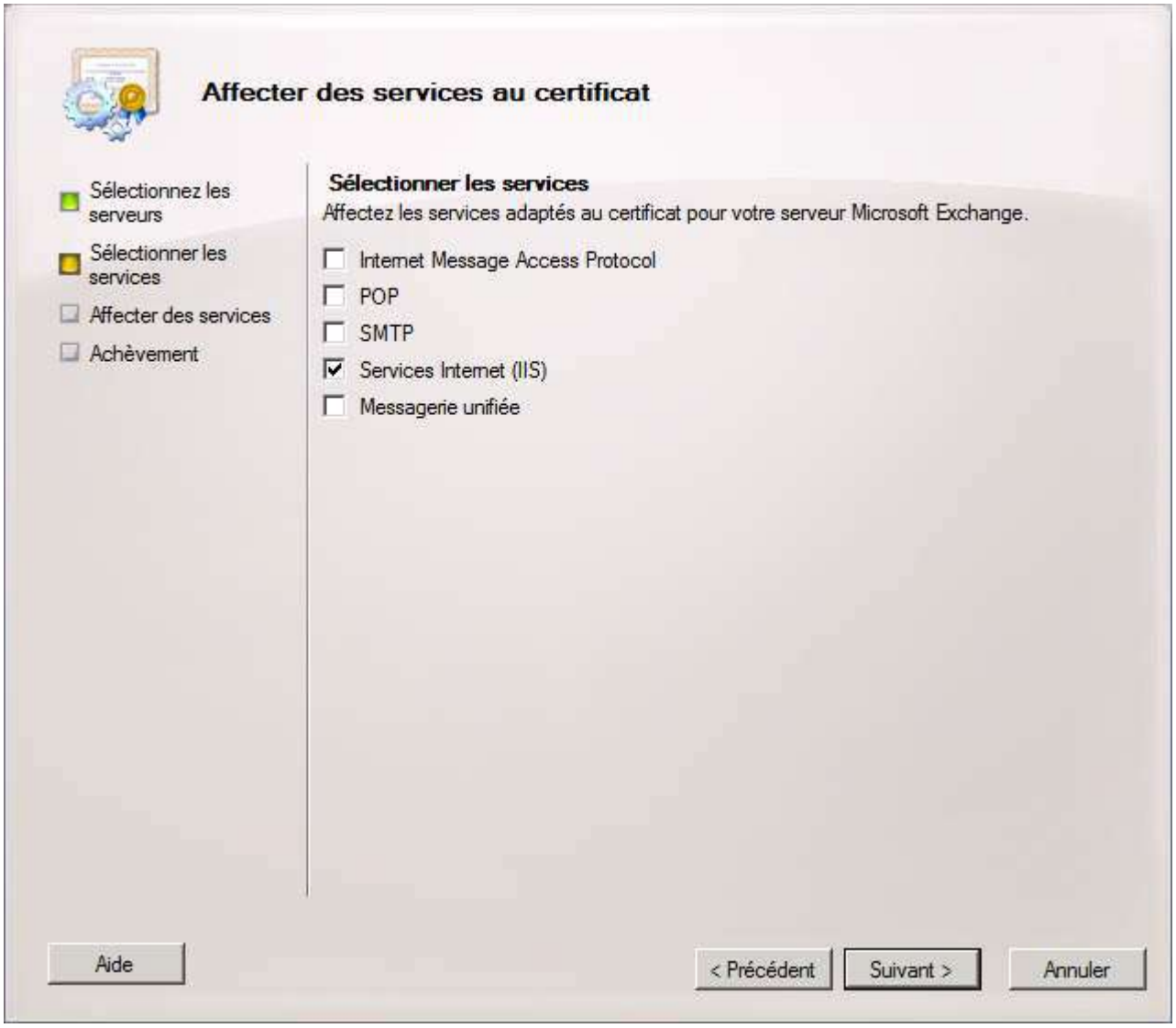
Pour commencer, vous devrez sélectionner le ou les serveurs auxquels vous souhaitez attribuer les certificats.



Sélection du serveur

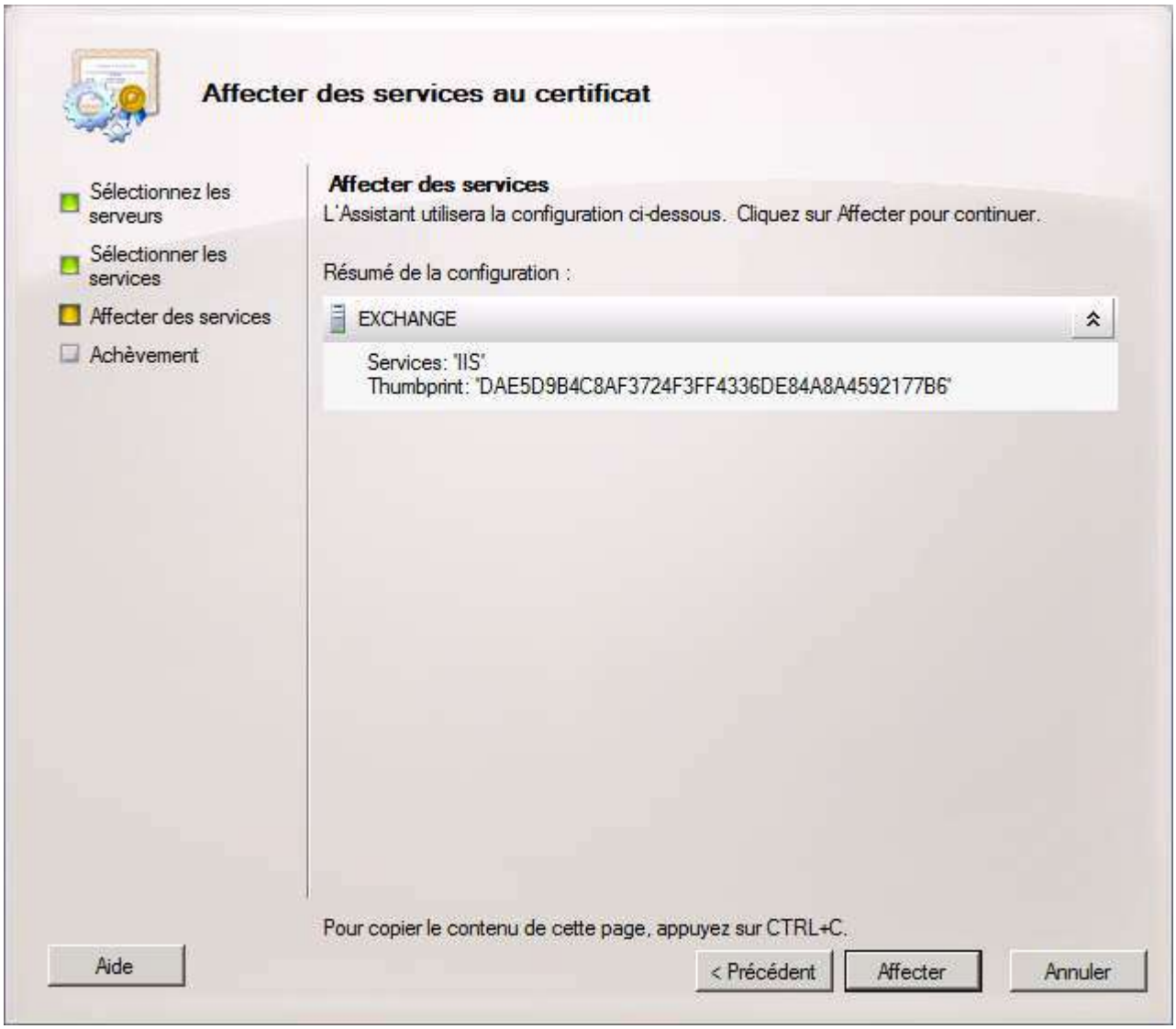
Vous devrez ensuite sélectionner les services que vous souhaitez sécuriser avec ce certificat. Je ne souhaite pas utiliser IMAP ni POP donc je ne vais pas les sélectionner. Je ne vais pas sécuriser SMTP mais cela est possible, notamment si vous avez des partenaires ou clients (au sens commercial et non réseau) qui vous envoient des

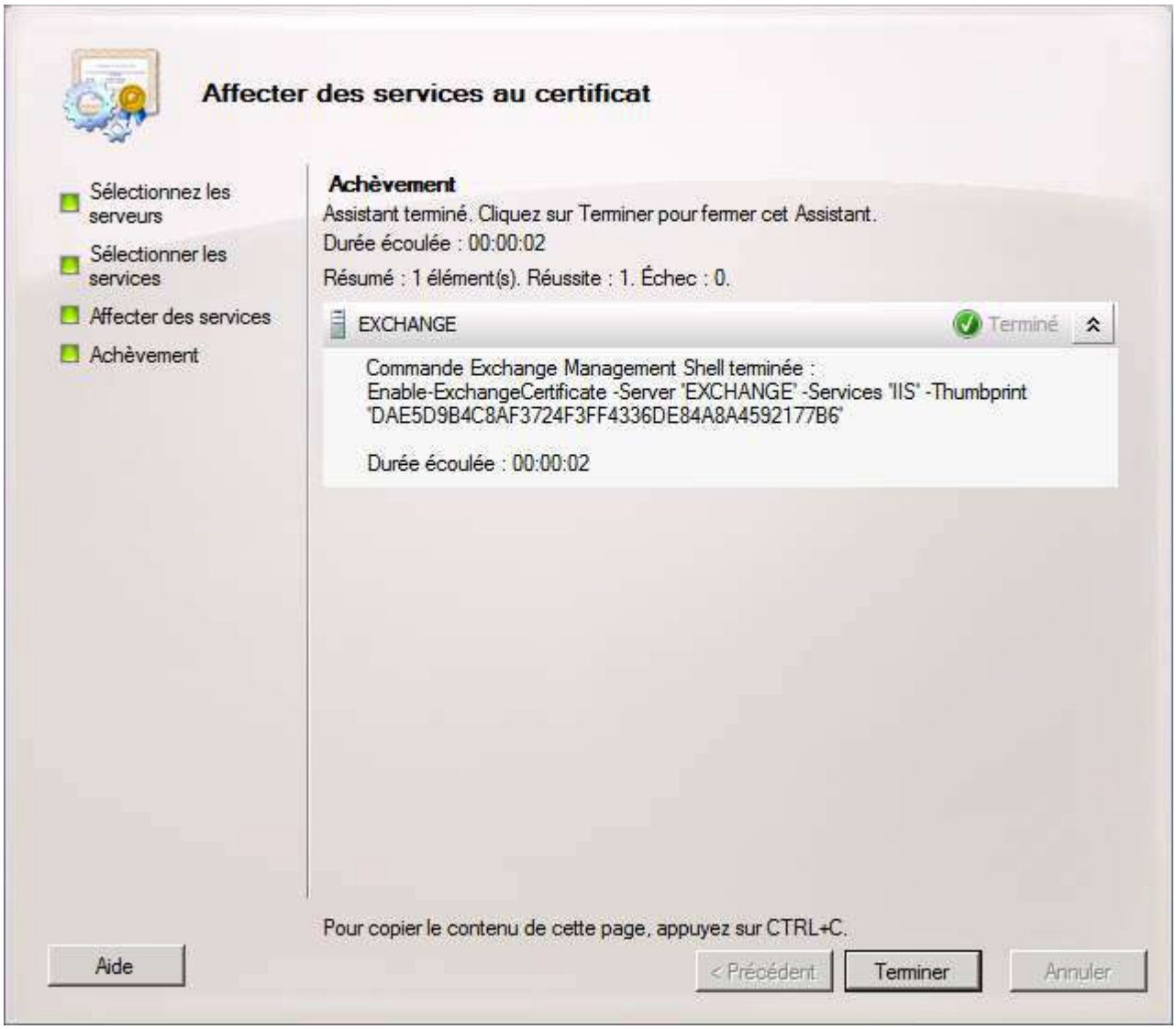
documents confidentiels. Je sélectionne IIS qui gère Autodiscover, OWA et Outlook Anywhere dans une certaine limite. Le rôle de messagerie unifiée n'étant pas installé, il est inutile d'y assigner le certificat.



Sélection des services sécurisés

Un bref résumé sera affiché. Cliquez sur *Affecter* pour finir l'affectation.





Assignation finie

Comme vous pouvez le voir, la commande Powershell est ici montrée. Pour assigner les services au certificat en Powershell, vous devrez d'abord récupérer l'empreinte numérique du certificat. Cela est possible grâce à Powershell.

```
Get-ExchangeCertificate | fl Thumbprint,FriendlyName,Subject
Enable-ExchangeCertificate -Server "Exchange" -Services "IIS" -Thumbprint
 "DAE5D9B4C8AF3724F3FF4336DE84A8A4592177B6"
```

La première ligne va vous permettre d'afficher les certificats valides pour Exchange et également d'identifier votre certificat. Ce qui nous intéresse est l'empreinte numérique (Thumbprint). C'est grâce à cela que le certificat est identifié de manière unique.

```
[PS] C:\users\administrateur.TODOROVIC\Documents>Get-ExchangeCertificate | fl th
umbprint,friendlyname,subject


Thumbprint   : DAE5D9B4C8AF3724F3FF4336DE84A8A4592177B6
FriendlyName : Exchange Interne
Subject      : CN=exchange.todorovic.adds

Thumbprint   : 21BF439EDD9245D44A8E920DE17F9F2B3168475A
FriendlyName : Exchange
Subject      : CN=mail.todorovic.fr
```

Get-ExchangeCertificate

La deuxième ligne assigne le service IIS du serveur nommé Exchange au certificat dont le thumbprint correspond à celui entré. Les différents services sont dans la liste ci-dessous. Si vous souhaitez assigner plusieurs services au certificat, vous devrez les séparer par des virgules (-Services "IIS,UM").

- IMAP
- POP
- IIS
- SMTP
- UM

Si vous changez les services assignés à un certificat, vous devrez redémarrer ces services. Dans le cas présent, il faudra redémarrer IIS.

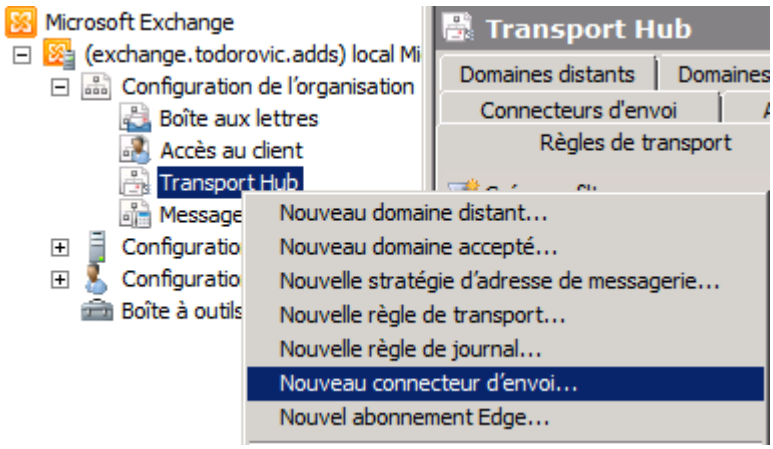
VI-D - Envoi/réception d'emails : sans serveur Edge

Par défaut, Exchange ne va pas permettre l'envoi/réception d'emails sur Internet. Voyons comment configurer le serveur pour changer ce comportement.

VI-D-1 - Connecteur d'envoi

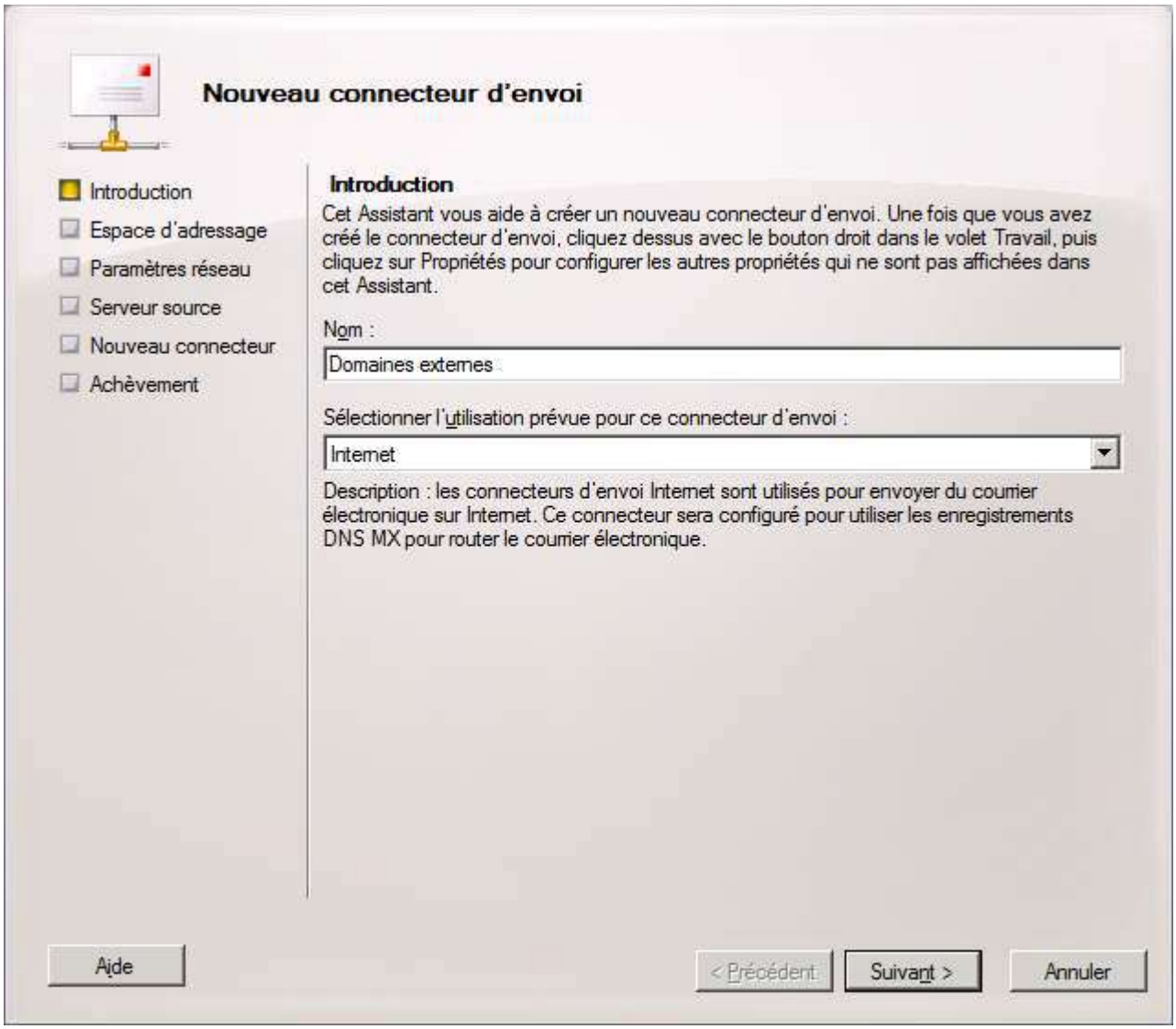
La création d'un connecteur d'envoi va permettre d'envoyer des emails vers une destination donnée. Sans ce connecteur, l'envoi d'emails à destination d'Internet sera indisponible. Voyons comment créer ce connecteur.

Ce connecteur se configure dans le rôle Transport Hub de l'organisation. Ouvrez le rôle dans l'organisation Exchange. Faites un clic droit puis cliquez sur *Nouveau connecteur d'envoi*.



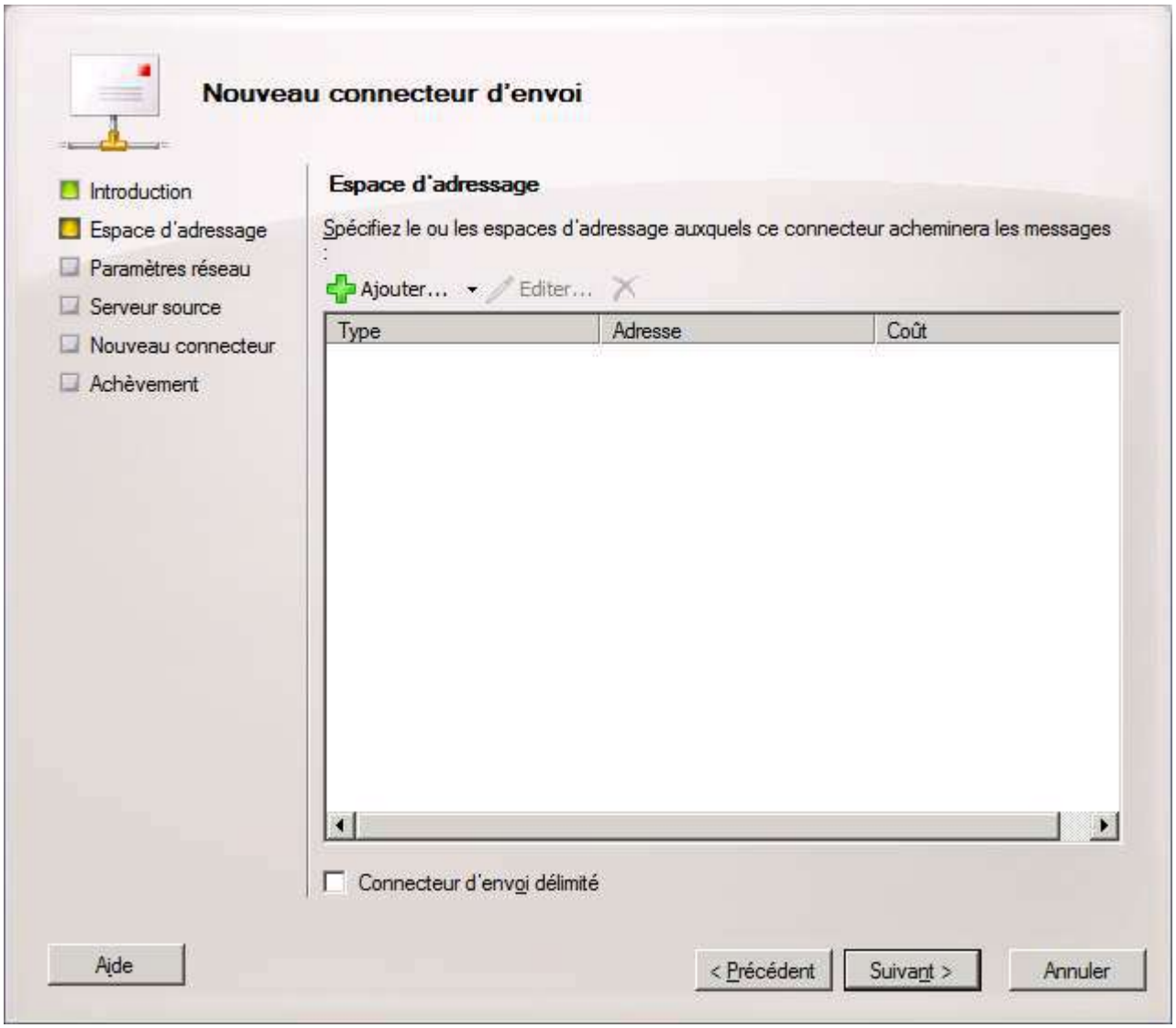
Ouverture de l'assistant

La première étape va consister à nommer votre connecteur et à indiquer le type d'usage (personnalisé, interne, Internet, partenaire). Ce connecteur est destiné à envoyer des emails sur Internet, il faut donc choisir le type correspondant.



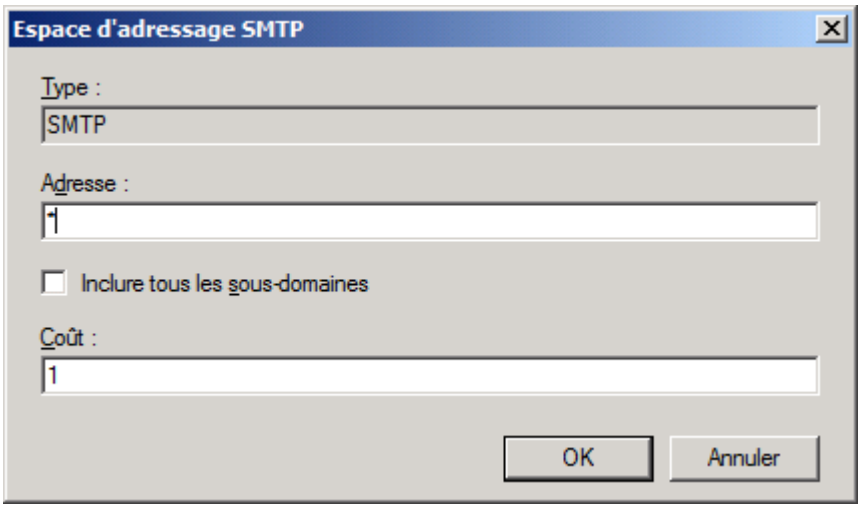
Nommage du connecteur d'envoi

Il faudra ensuite définir l'espace d'adressage du connecteur : il s'agit des domaines vers lesquels le connecteur pourra envoyer des emails. Grâce à cela, vous pourrez forcer l'envoi de messages à destination d'un domaine particulier vers un serveur particulier. Ici, le connecteur sera général : il sera possible d'envoyer des emails à tous les domaines. Cliquez sur *Ajouter*.



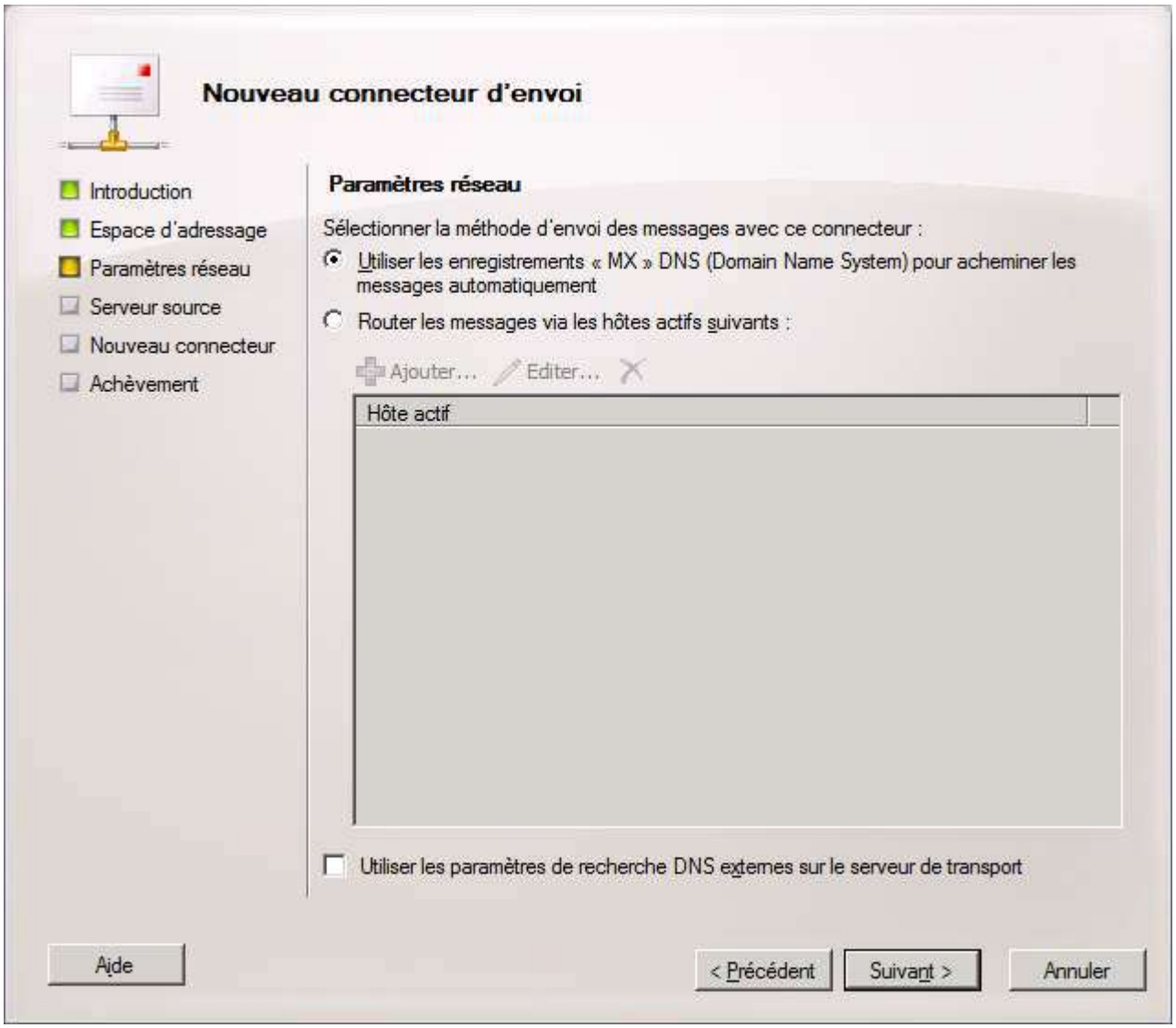
Définition de l'espace d'adressage

Dans "Adresse", vous pourrez préciser un domaine ou un wildcard (tous les domaines). Si vous définissez un domaine (entreprise.fr), il sera possible d'autoriser ou non les envois à destination des sous-domaines. Enfin, vous pourrez définir un coût. Cela sera utile lors de la détermination du routage du message si vous souhaitez créer plusieurs connecteurs d'envoi.



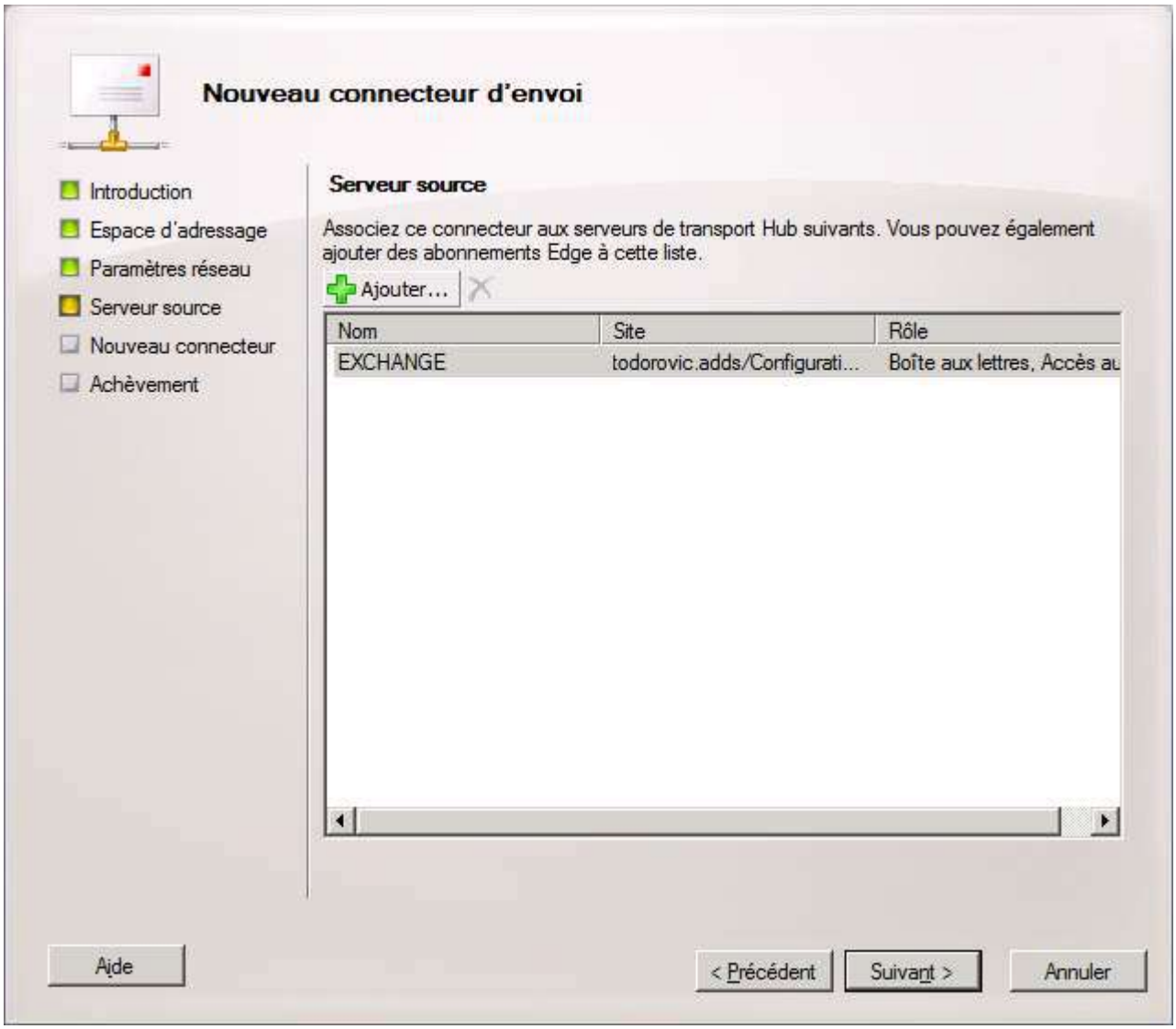
Configuration de l'espace d'adressage

Vous devrez ensuite indiquer si vous souhaitez utiliser les enregistrements MX des domaines pour envoyer les emails automatiquement ou si vous souhaitez faire passer les messages par un hôte particulier (hygiène de messagerie par exemple). Nous sommes dans une configuration sans serveur d'hygiène donc il faut choisir l'utilisation des enregistrements MX des DNS.



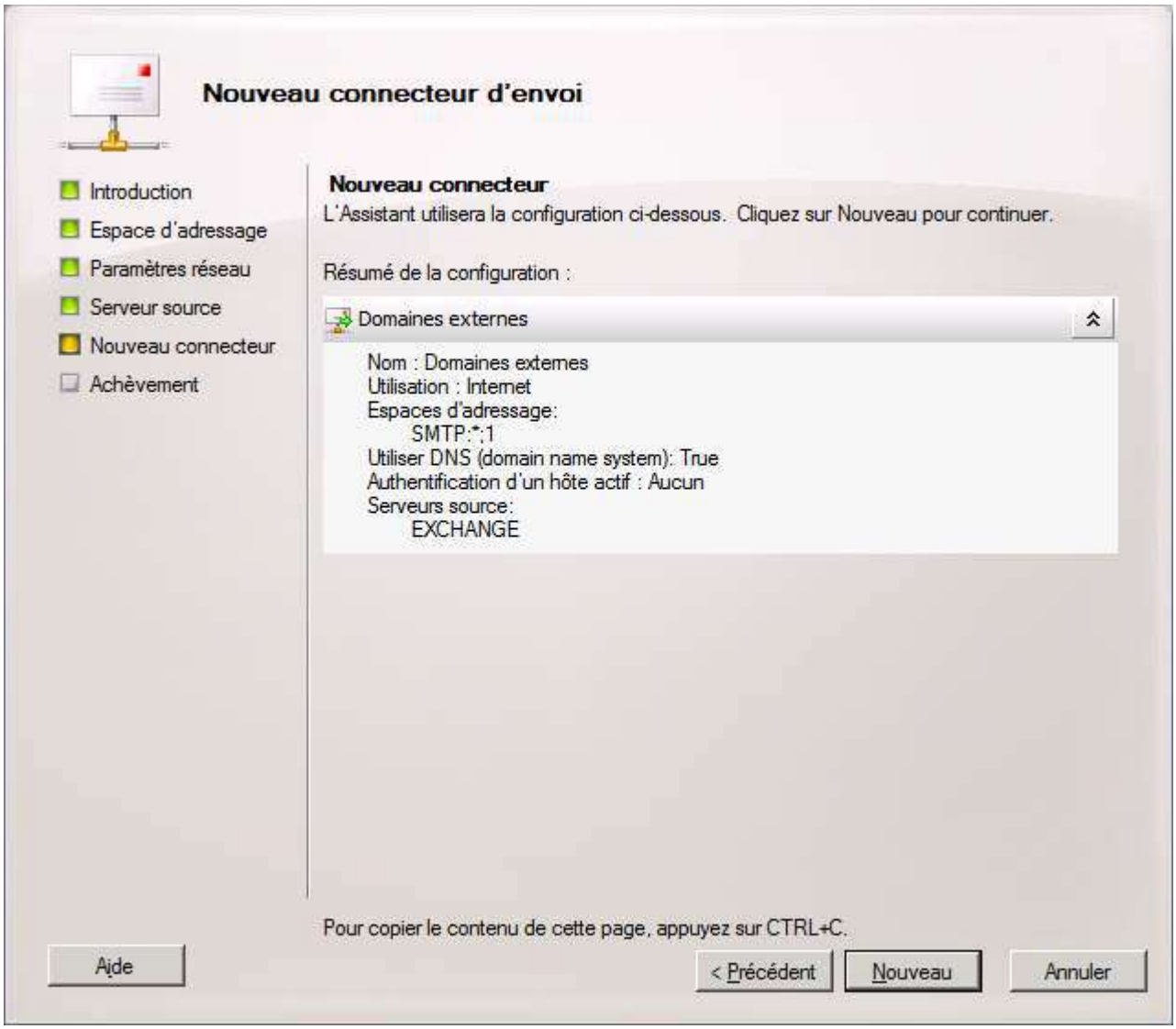
Utilisation des enregistrements MX

Puisque le connecteur d'envoi est géré au niveau de l'organisation, vous devrez sélectionner quels serveurs Transport Hub utiliseront ce connecteur.



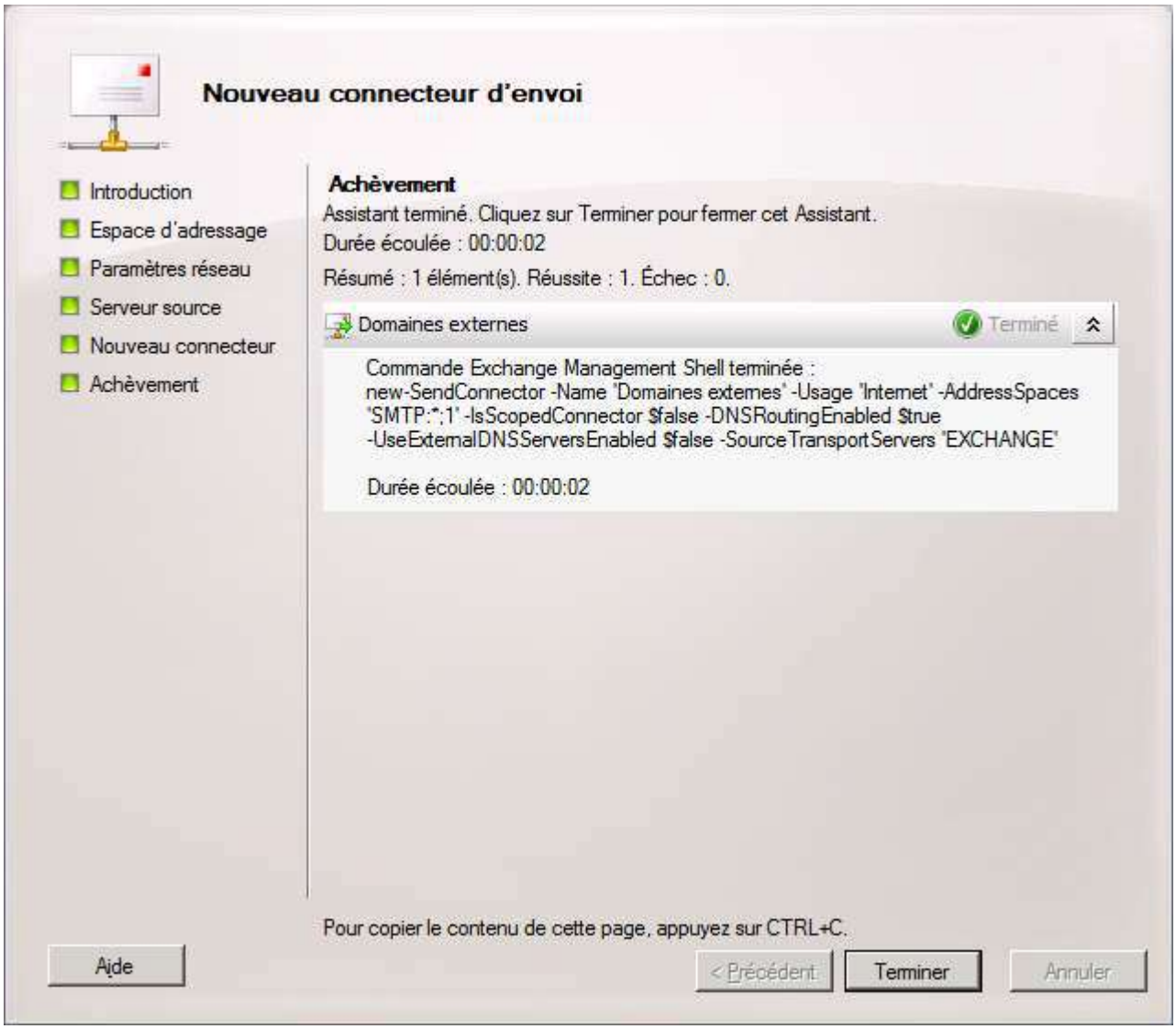
Attribution du connecteur aux serveurs de l'organisation

Un résumé sera affiché, cliquez sur *Suivant* pour créer le connecteur.



Résumé de la configuration du connecteur

Il sera possible de créer ce connecteur via EMS. La commande est indiquée ci-dessous.

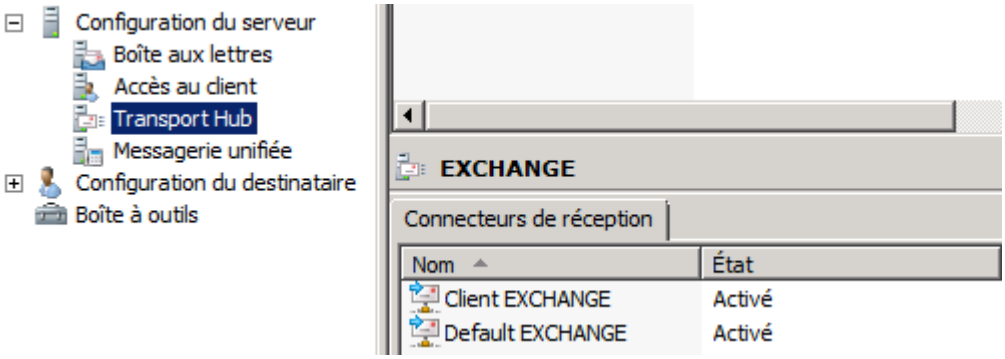


Connecteur créé

Vous pouvez maintenant envoyer des emails à destination d'Internet.

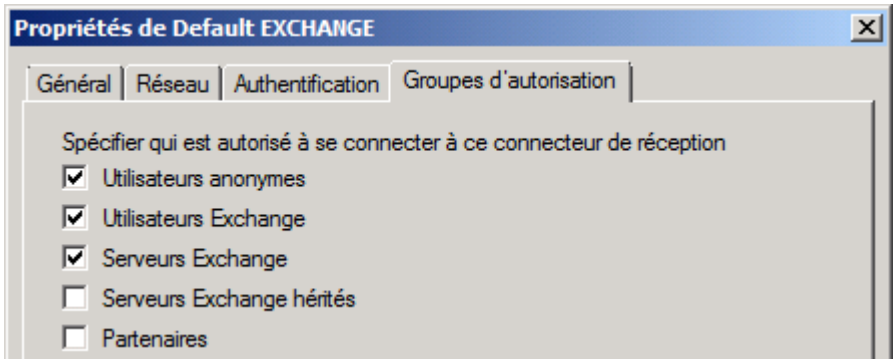
VI-D-2 - Connecteur de réception

Contrairement au connecteur d'envoi, les connecteurs de réception sont gérés par serveur. Par défaut, il existe deux connecteurs de réception.



Connecteurs de réception par défaut

Le premier connecteur "Client EXCHANGE" permet les communications SMTPS (TCP 587) uniquement pour les utilisateurs Exchange. Le second connecteur "Default EXCHANGE" permet les communications SMTP (TCP 25) pour les utilisateurs et serveurs Exchange. Afin de permettre aux serveurs SMTP externes d'envoyer des emails à notre serveur Exchange, il va falloir modifier les autorisations du connecteur Exchange. Ouvrez les propriétés du connecteur "Default Exchange", allez dans **Groupes d'autorisation** puis cochez **Utilisateurs anonymes**. J'ai décoché **Serveurs Exchange hérités** : il s'agit des serveurs dits "legacy", autrement dit des serveurs Exchange anciens (2003).



Modification du connecteur de réception

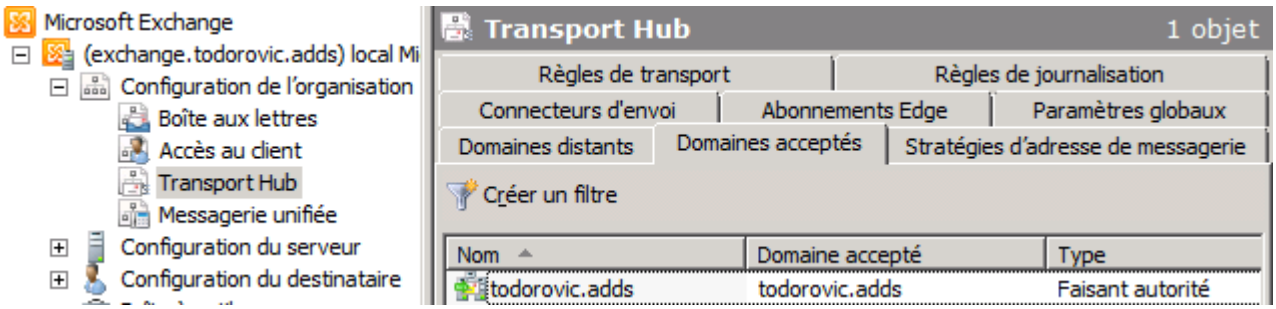
Voici la commande Powershell équivalente :

```
Set-ReceiveConnector -PermissionGroups 'AnonymousUsers, ExchangeUsers, ExchangeServers' -Identity
 'EXCHANGE\Default EXCHANGE'
```

VI-E - Création des règles de génération d'adresses email

Pour commencer, il faut ajouter un nouveau domaine accepté par le serveur Exchange. Pour cela, il faut aller dans la configuration de l'organisation pour régler les paramètres du serveur de transport. Allez dans l'onglet **Domaines acceptés**.

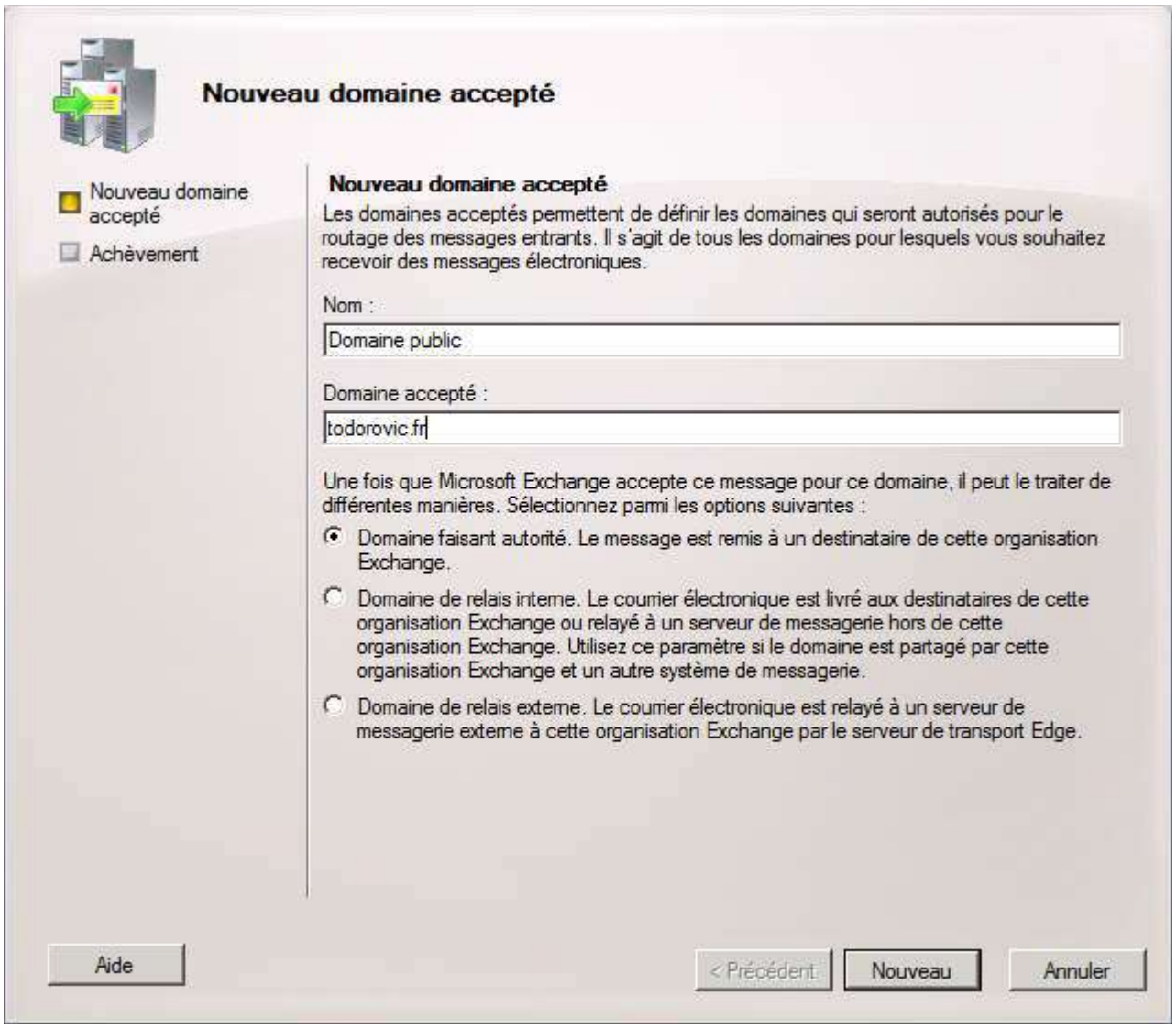
Comme vous pouvez le constater, il y a déjà un domaine correspondant à votre domaine AD. Si vous êtes dans une configuration avec un domaine privé, l'ajout du nouveau domaine est obligatoire pour que votre serveur Exchange puisse communiquer avec l'extérieur.



Domaines acceptés

Faites un clic droit en dessous du domaine par défaut puis *Nouveau domaine accepté*. Donnez un nom à ce nouveau domaine puis indiquez le nom de domaine que l'organisation Exchange va accepter. Vous devrez également choisir le type de domaine (faisant autorité, relais interne ou relais externe). Par défaut, choisissez le domaine faisant autorité. Les domaines relais correspondent à des configurations particulières de votre messagerie.

Enfin cliquez sur *Nouveau*.



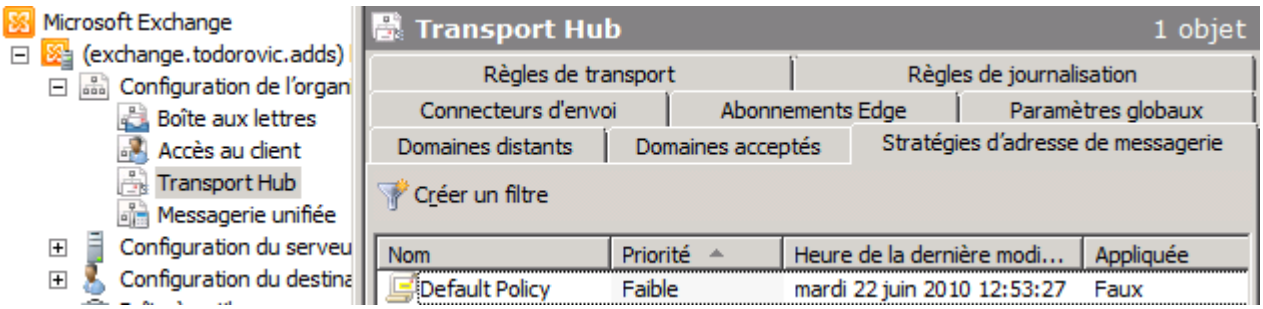
Création d'un nouveau domaine accepté

Ensuite, la création du nouveau domaine accepté aura lieu. Vous aurez alors l'équivalent en Powershell.

Création effectuée avec succès

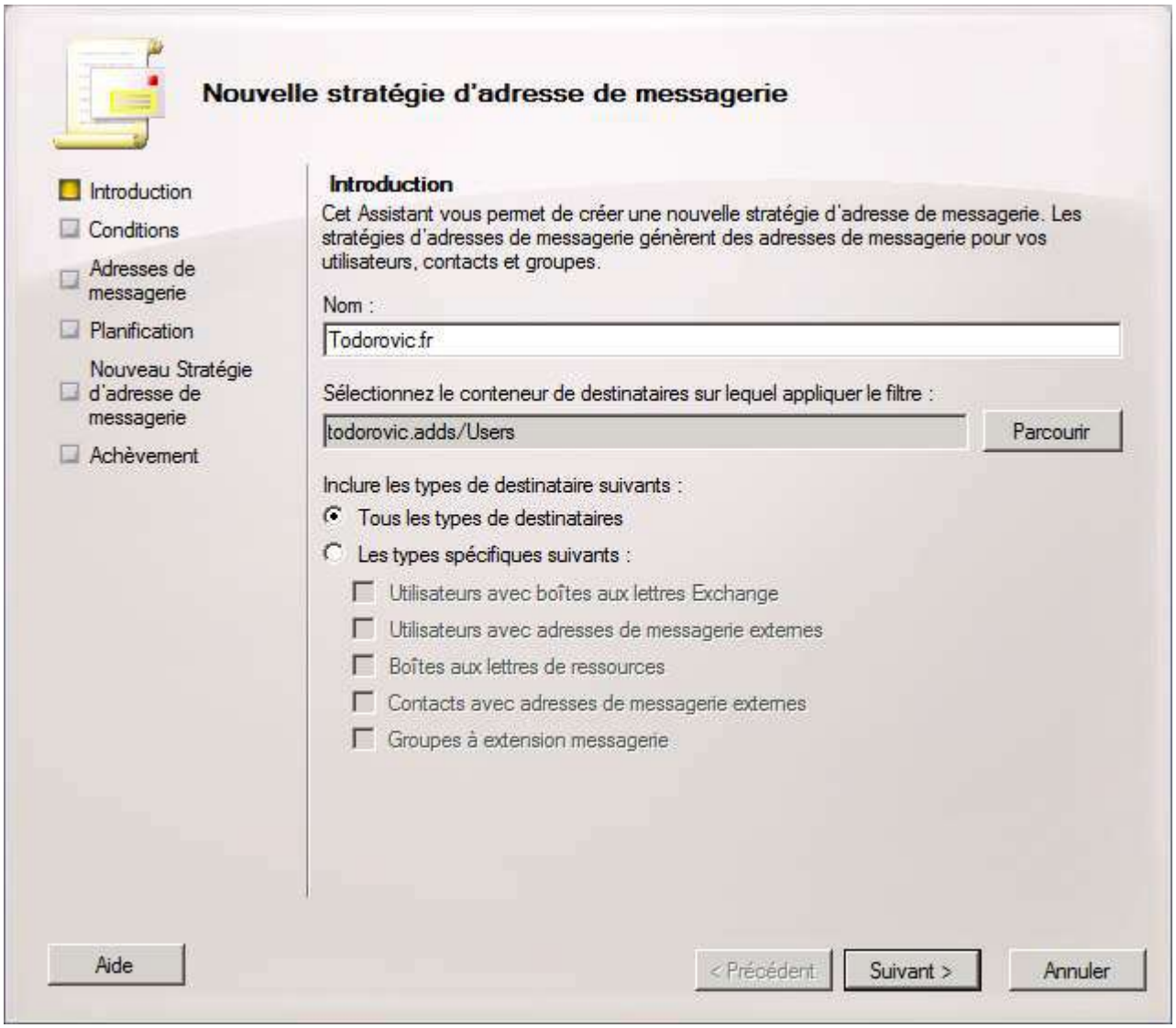
Il est maintenant possible de créer les règles de construction d'adresses email à partir des informations stockées dans Active Directory. Pour cela, allez dans les **Stratégies d'adresse de messagerie** dans le Transport Hub au niveau de l'organisation. Il existe une règle par défaut : les adresses de messagerie sont créées avec le domaine par défaut (todorovic.adds dans mon cas). Cette règle n'est pas appliquée à l'exception du compte ayant installé Exchange. Il n'est plus possible de modifier cette règle depuis Exchange 2010. Il faut donc en créer une nouvelle.

Pour cela, faites un clic droit en dessous de la règle par défaut puis *Nouvelle stratégie d'adresse de messagerie*.



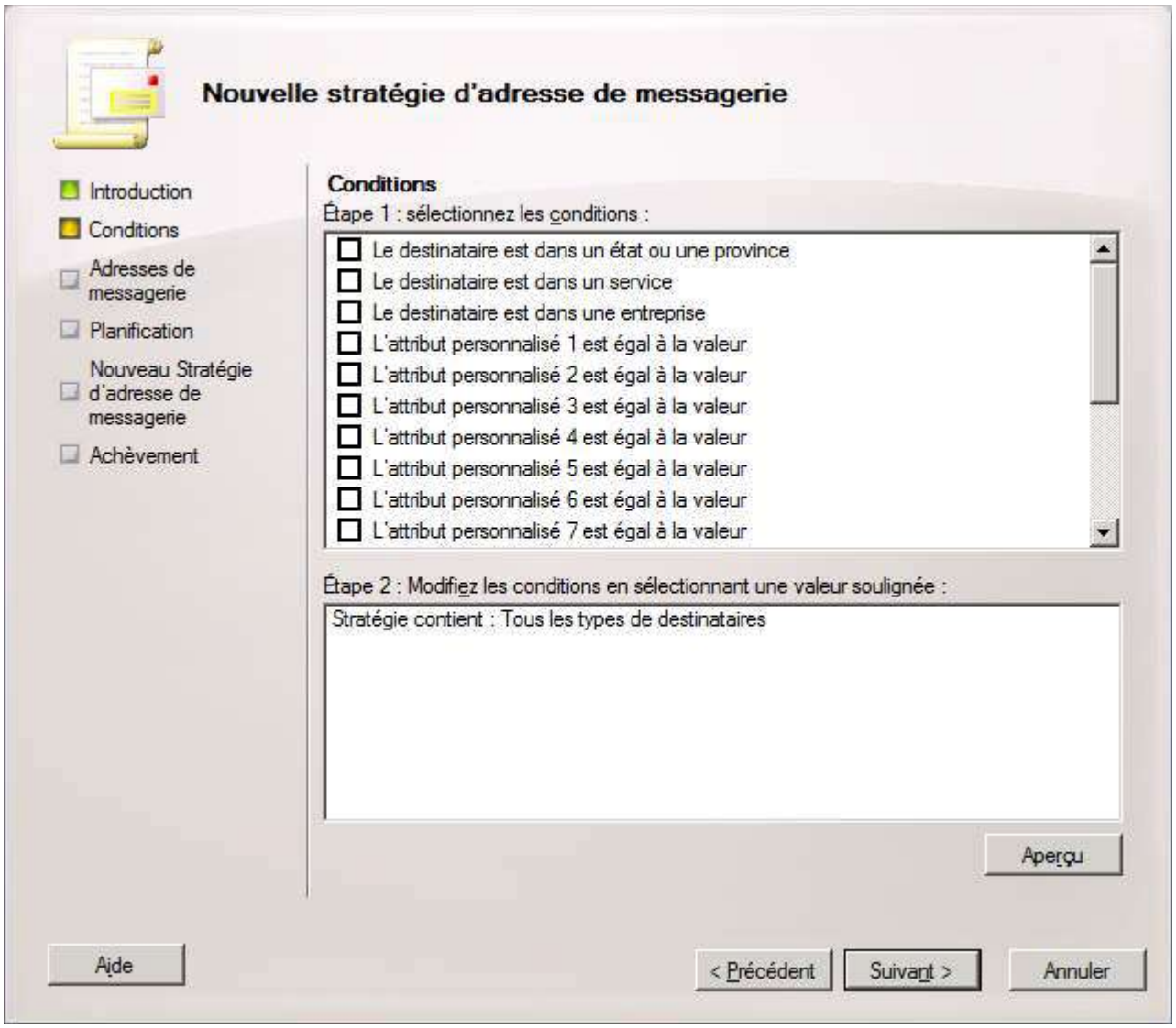
Stratégies d'adresse de messagerie

Nommez votre nouvelle règle puis indiquez le conteneur (unité d'organisation) d'utilisateurs sur lequel la règle sera appliquée. Ensuite indiquez sur quels types d'objets sera appliquée la règle. Pour simplifier l'administration et n'ayant qu'un seul domaine à héberger, je peux choisir tous les types d'objets.



Création de la nouvelle stratégie

Vous pourrez ensuite préciser des conditions d'application de votre nouvelle stratégie. Ces règles sont basées sur les attributs des objets. Vous ne pouvez pas accéder à tous les attributs depuis le mode graphique. Vous pouvez en revanche définir des attributs personnalisés. Ces attributs sont numérotés, vous devrez donc documenter ces attributs afin de savoir à quoi ils correspondent.

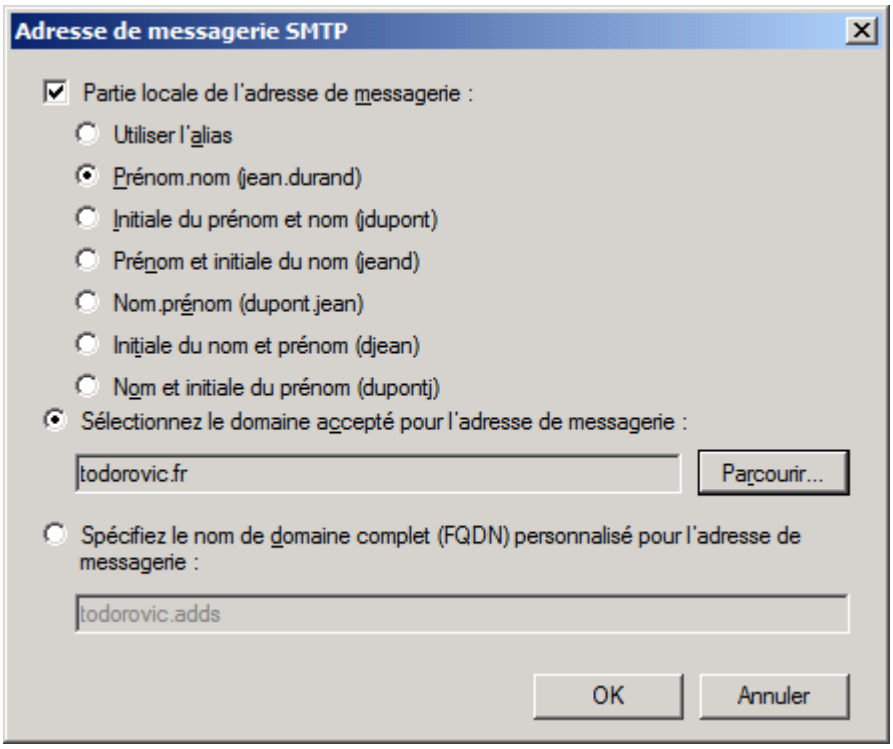


Conditions d'application de la stratégie

Vous devrez ensuite indiquer les règles de création d'adresses email. Il est possible de créer plusieurs adresses pour un compte en créant plusieurs règles. Cliquez sur *Ajouter*.

Politiques d'adresses de messagerie

Définissez la règle comme bon vous semble. Des exemples sont là pour vous aider à voir ce que la règle donnera comme adresse.

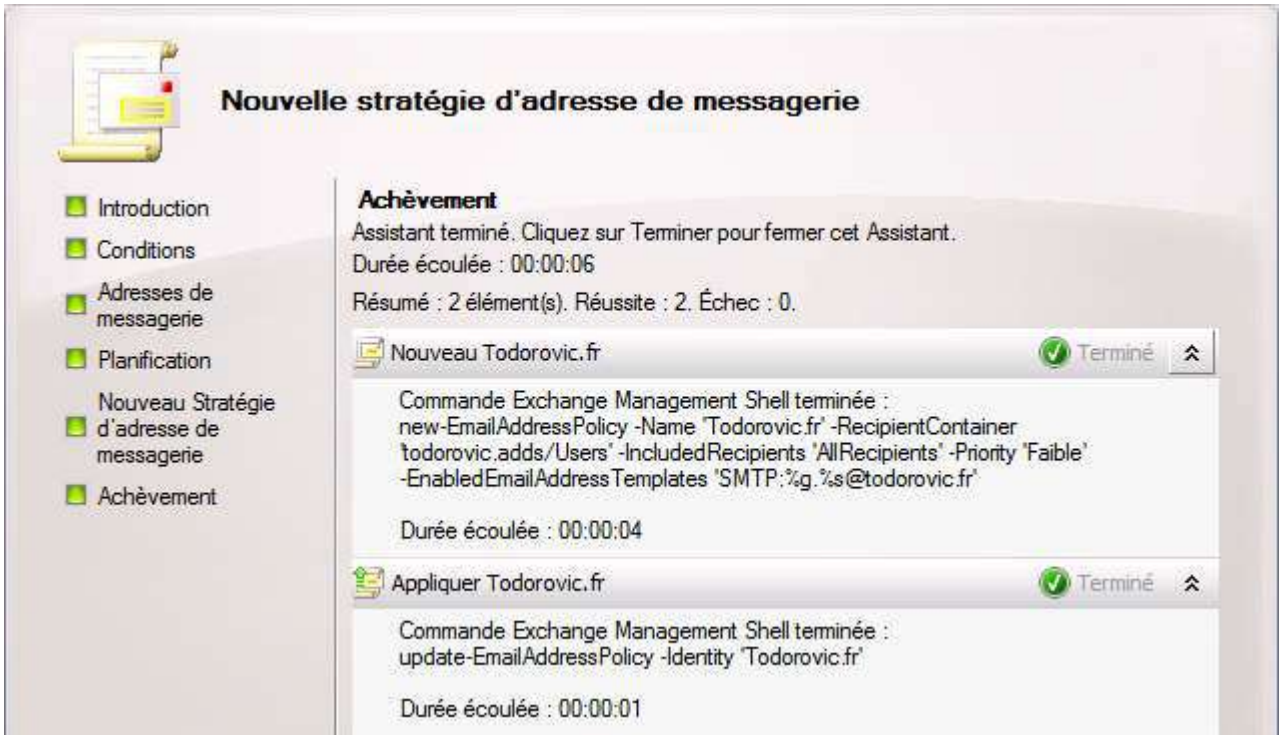


Configuration de la règle de création d'adresse de messagerie

Une fois que vous avez créé les règles souhaitées, passez à la planification de l'application de la stratégie. Vous pourrez l'appliquer plus tard, immédiatement ou à un moment précis. Lorsqu'une règle est appliquée, elle sera également appliquée aux nouveaux comptes créés.

Planification de l'application de la stratégie

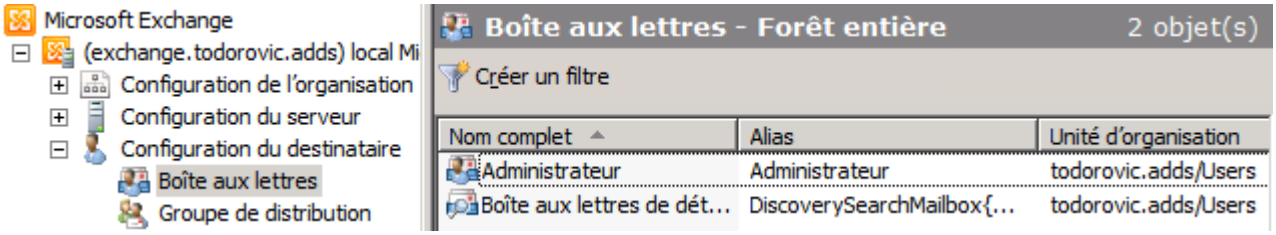
Après un résumé, vous finirez par créer la stratégie. Encore une fois, vous aurez l'équivalent Powershell indiqué.



Stratégie créée

VI-F - Création basique des comptes Exchange

Il existe plusieurs types de boîtes aux lettres Exchange. On distingue ainsi les boîtes aux lettres d'utilisateurs des boîtes aux lettres de ressources (salle ou matériel). Les boîtes de ressources permettent la réservation de ces dernières pour des réunions. La création des boîtes de ressources et utilisateurs se font de la même manière. Allez dans la **configuration du destinataire** puis **Boîte aux lettres**.

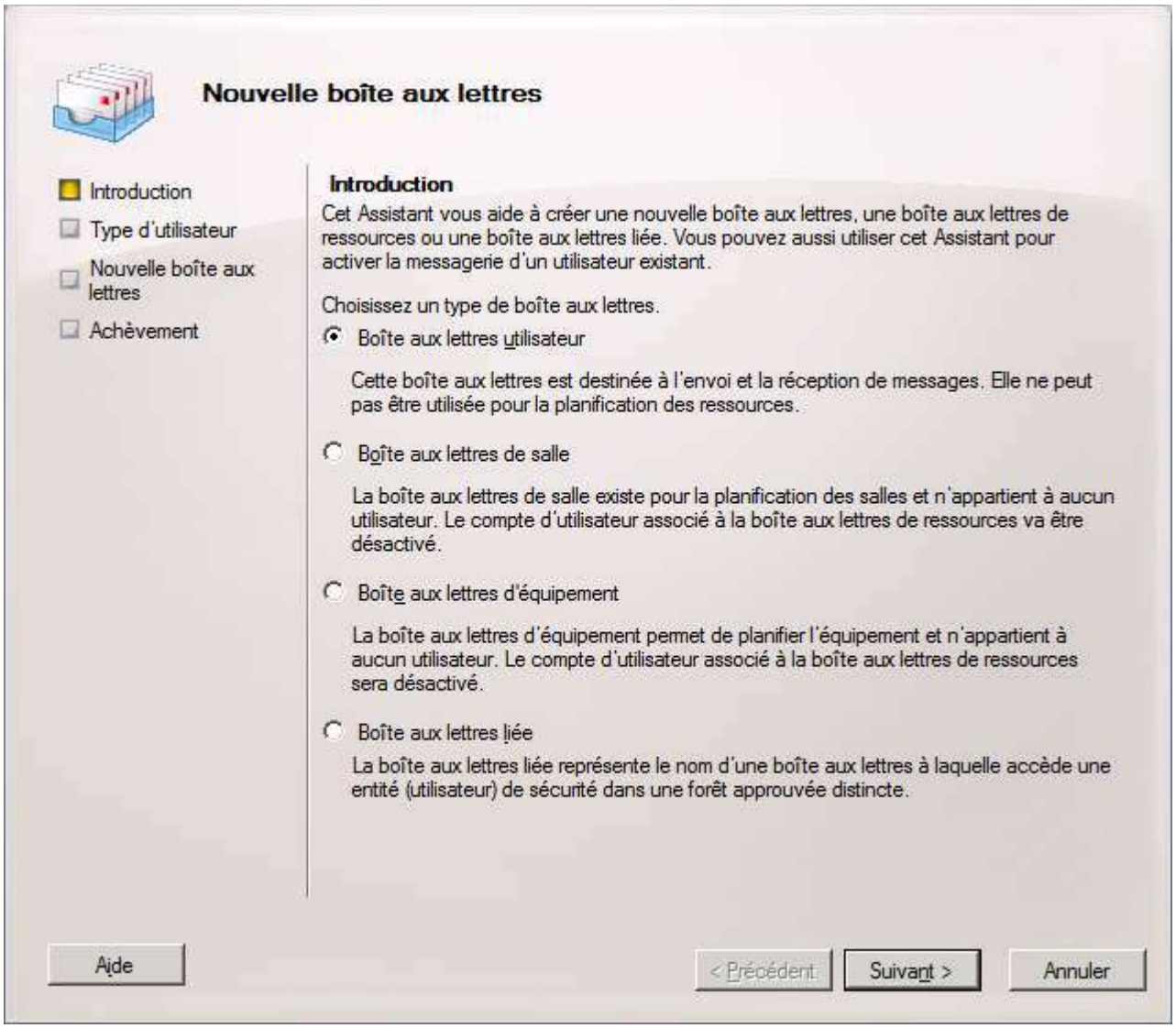


Boîtes aux lettres

VI-F-1 - Utilisateurs et ressources

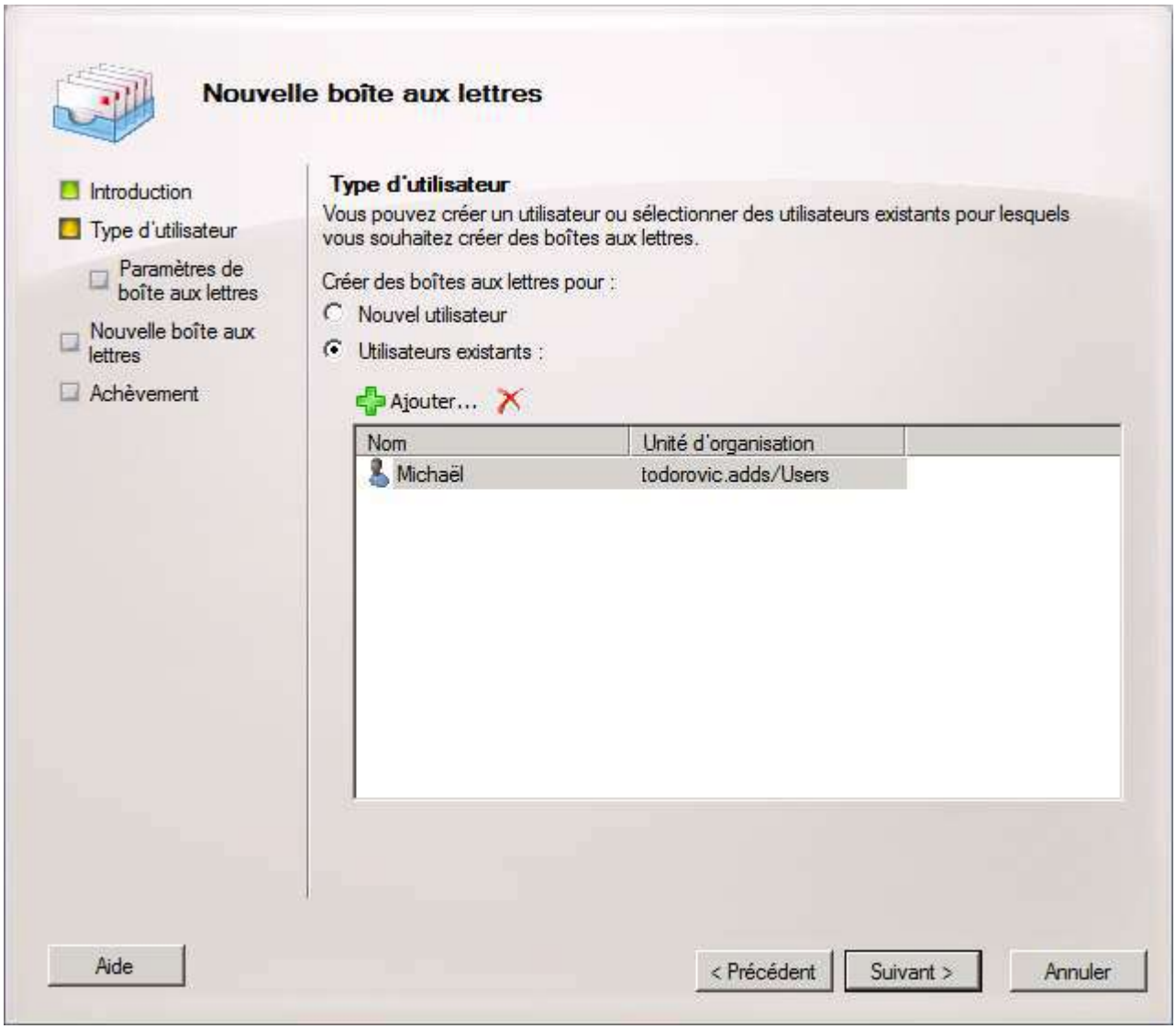
VI-F-1-a - Compte AD existant

Pour créer un nouvel utilisateur, faites un clic droit en dessous des boîtes déjà créées puis cliquez sur *Nouvelle boîte aux lettres*. Sélectionnez alors **Boîte aux lettres utilisateur**.



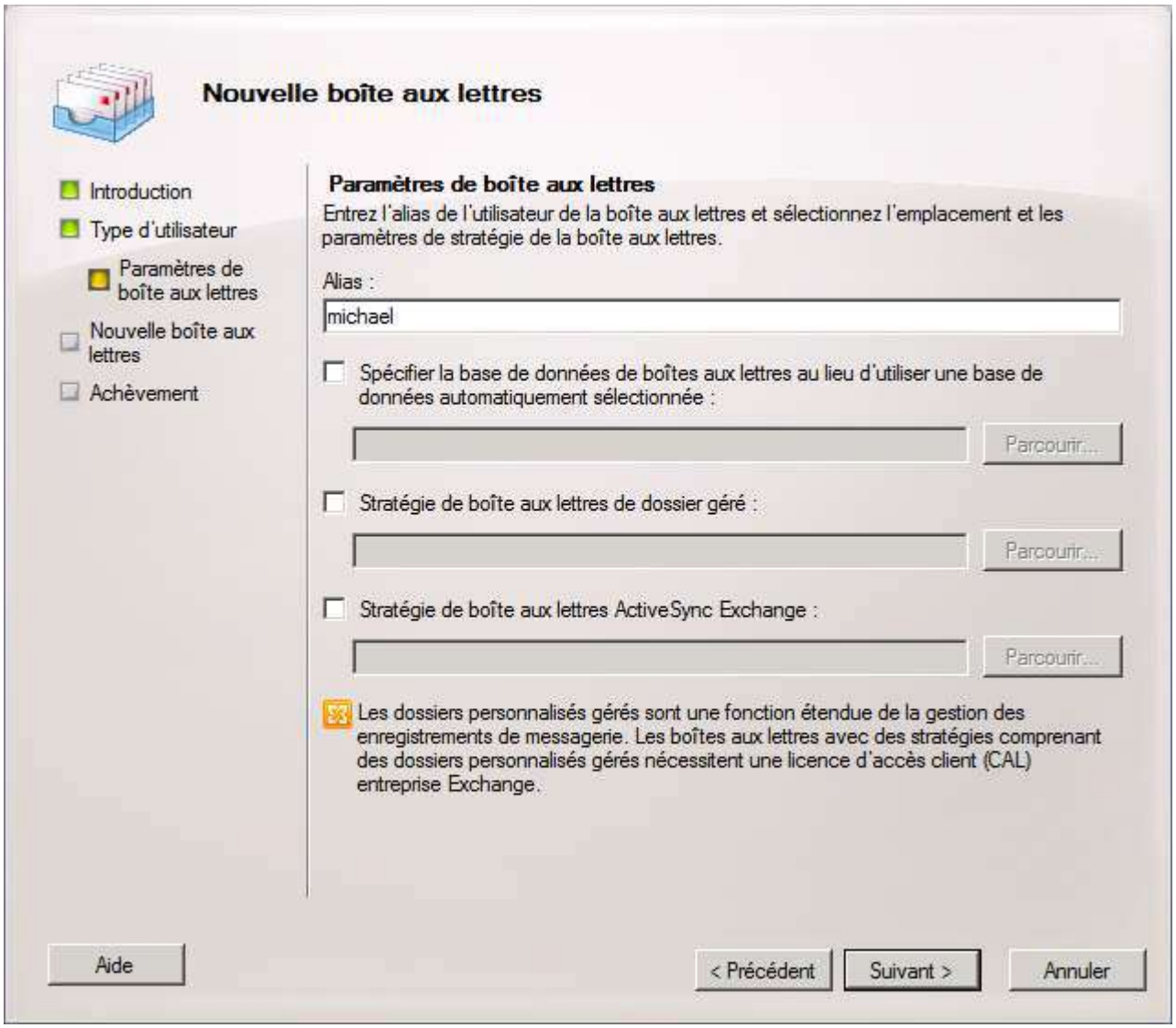
Création d'une nouvelle boîte aux lettres

La création de compte Exchange peut se faire de deux manières. Soit vous créez un nouvel utilisateur dans Active Directory et vous lui affectez immédiatement une boîte Exchange ou alors vous pouvez créer une boîte Exchange à un utilisateur déjà existant. Je vais créer une boîte à un utilisateur déjà existant. Sélectionnez **Utilisateurs existants** puis ajoutez les utilisateurs après les avoir sélectionnés dans Active Directory. L'assistant ne permet pas de lier une archive lors de la création de la boîte aux lettres. Il faudra procéder à cette étape plus tard si vous le souhaitez.



Sélection des utilisateurs

Vous devrez ensuite indiquer des paramètres de la boîte aux lettres. Dans une configuration basique, vous n'aurez qu'à indiquer l'alias de la boîte aux lettres. C'est ici que vous pourrez indiquer différentes stratégies à appliquer sur la boîte aux lettres ainsi que son emplacement dans les bases de données Exchange.



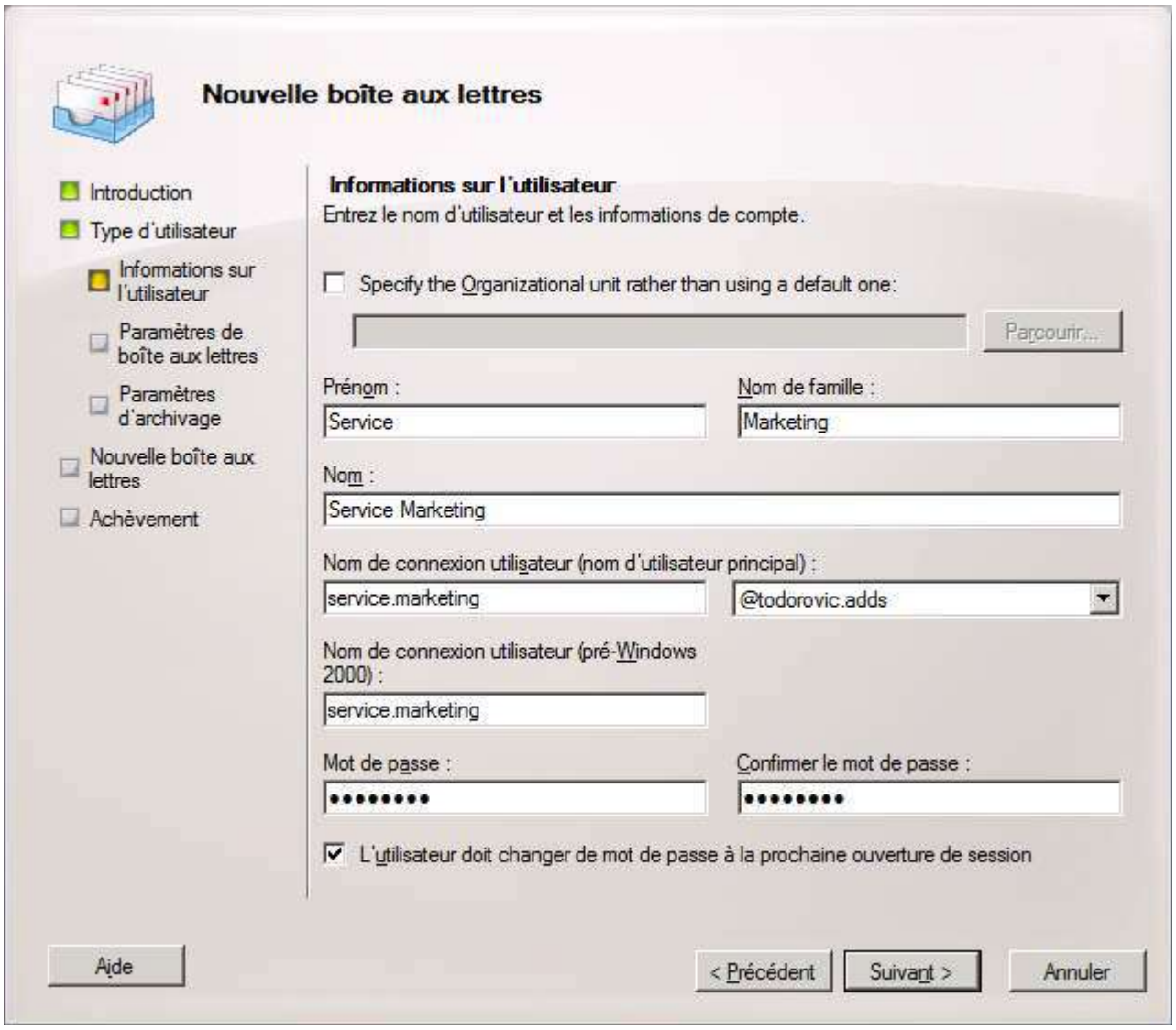
Paramètres de la boîte aux lettres

Vous pourrez procéder à la création des boîtes aux lettres après avoir validé le résumé de la création de boîtes. Comme toujours, l'équivalent en Powershell sera affiché.

Création des boîtes effectuée

VI-F-1-b - Création du compte AD

La création d'une boîte aux lettres sans avoir de compte AD se fait de la même manière que précédemment. Au lieu de choisir des utilisateurs existants, créez un nouvel utilisateur. Vous devrez indiquer les informations concernant votre utilisateur afin de le créer.

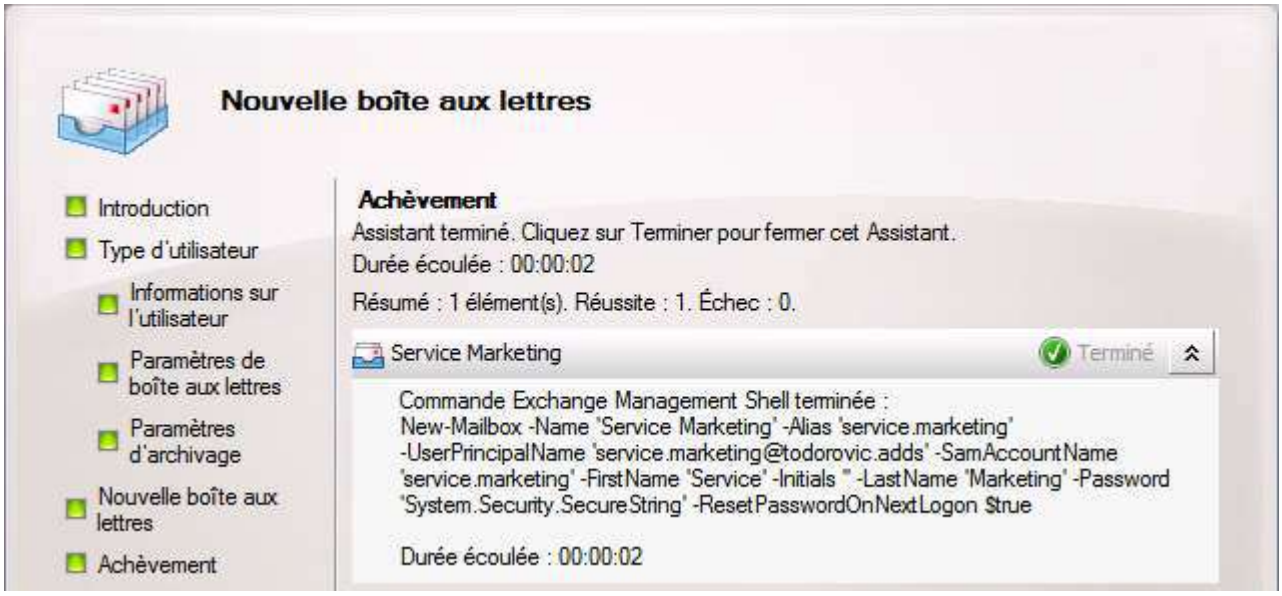


Création du nouvel utilisateur

Vous devrez ensuite préciser les paramètres de boîtes aux lettres. Contrairement à la création de boîtes avec un compte existant, vous pourrez associer une archive dès la création de la boîte aux lettres.

Activation de l'archivage

Après un résumé de la création à effectuer, celle-ci sera réalisée.

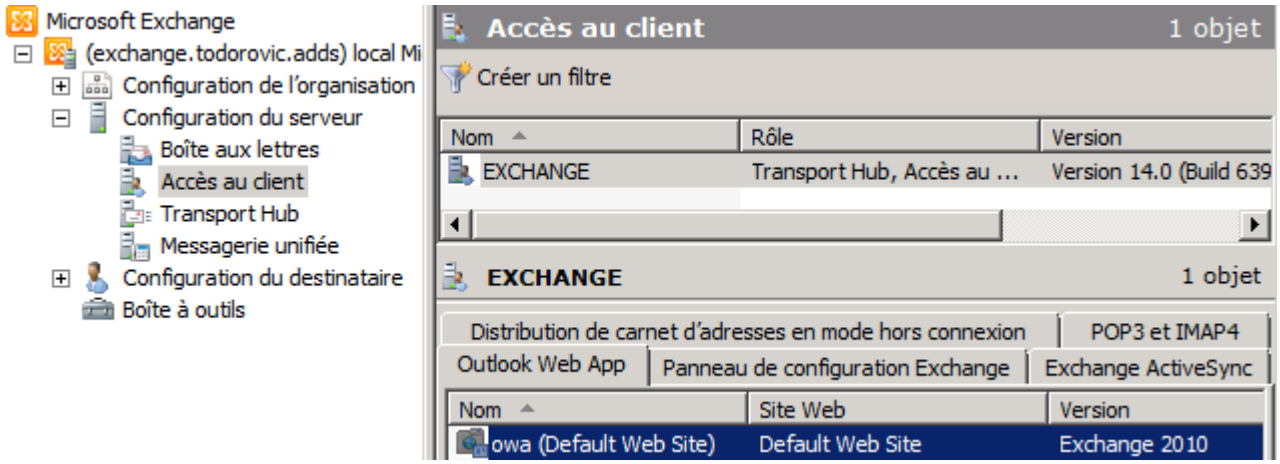


Création de l'utilisateur et de la boîte aux lettres

VI-G - Outlook Web App

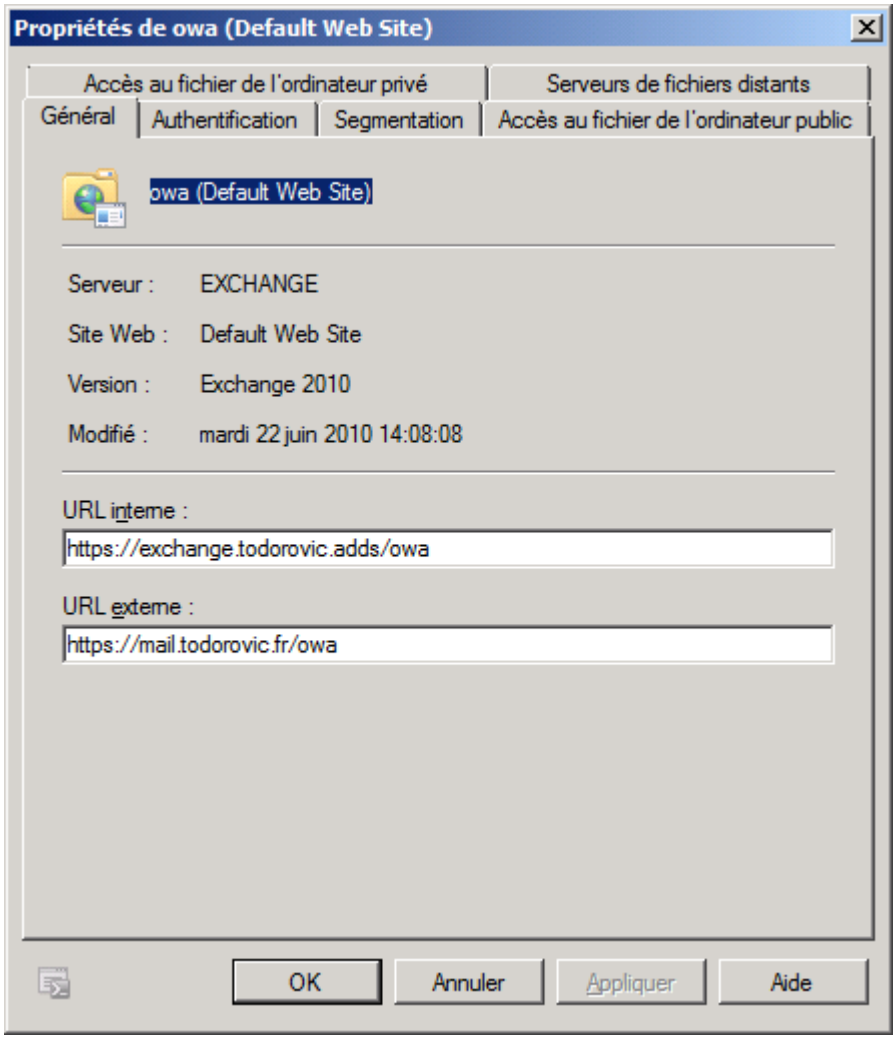
VI-G-1 - Authentification

Outlook Web App permet un accès Web à votre boîte Exchange. Depuis Exchange 2007, OWA se rapproche le plus possible du client lourd Outlook. Il est possible de configurer cet accès Web de manière poussée. Il faudra aller dans la configuration du serveur d'accès client.



Configuration d'OWA

Ouvrez les propriétés du site OWA "owa (Default Web Site).



Propriétés d'Outlook Web App

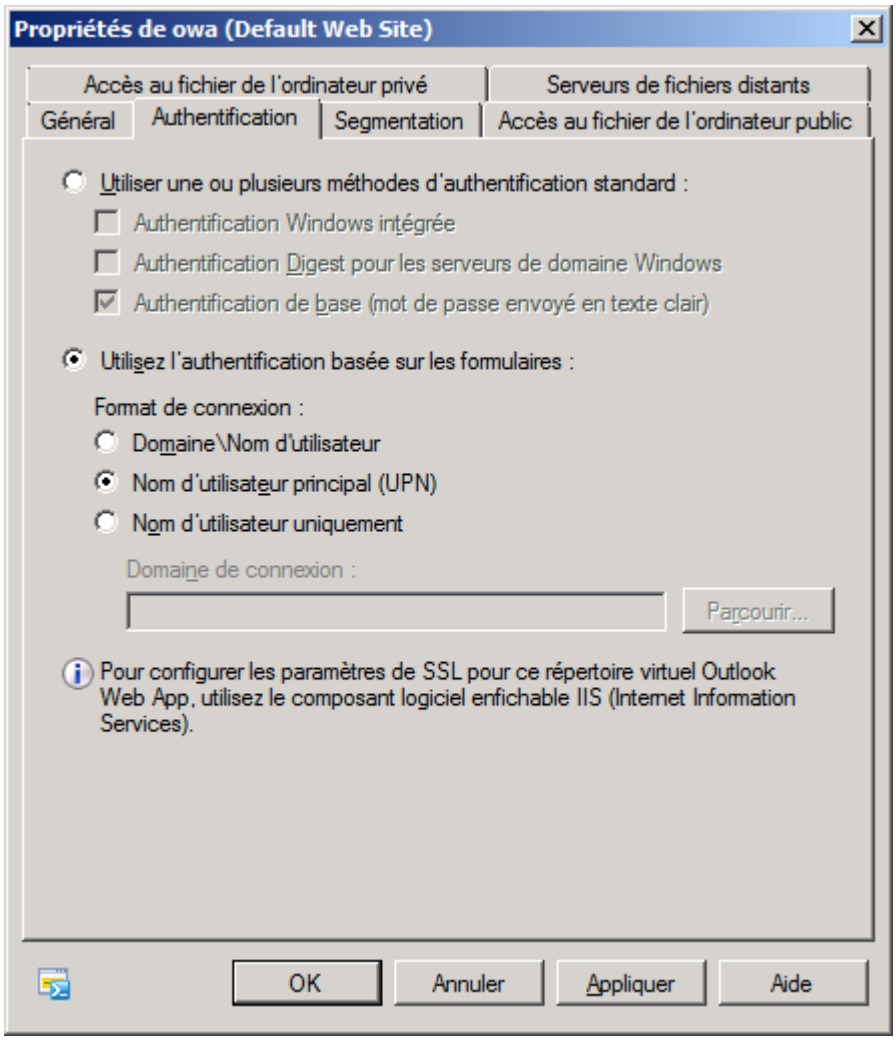
Vous pourrez modifier l'authentification d'OWA, activer ou non différentes fonctionnalités, gérer les accès aux fichiers et notamment le WebReady Document Viewing qui permet la visualisation des documents Office, Pdf, etc. en format html. En revanche, contrairement à ce que l'on pourrait croire, il n'est plus possible d'accéder à un serveur de fichiers depuis OWA. Il semblerait que la présence de la gestion de l'accès aux serveurs de fichiers soit un bug de la version finale d'Exchange.

Afin de simplifier notamment la vie de vos utilisateurs, vous pouvez changer le type d'authentification d'OWA. Par défaut, vous devrez vous connecter avec votre identifiant SAM (DOMAINE\utilisateur) sur un formulaire. Il est possible de se connecter avec son identifiant SAM, UPN ou utilisateur (en forçant un domaine précis). Vous pouvez également utiliser une authentification standard (intégrée Windows, Digest ou Basic). La méthode d'authentification doit être choisie selon plusieurs critères :

- source d'accès à OWA ; interne, externe ou interne/externe : si vous ne donnez accès à OWA qu'en interne, le meilleur choix sera sans doute l'authentification intégrée Windows (authentification par négociation NTLM ou Kerberos). La méthode Basic est déconseillée. Si vous souhaitez donner un accès externe avec un reverse-proxy simple, vous ne pourrez pas proposer l'authentification intégrée Windows (c'est techniquement possible mais demande un prérequis important : il faut que l'ordinateur accédant à OWA fasse partie de l'entreprise et se connecte régulièrement). Il faudra alors choisir une authentification par formulaire : le login par UPN permet de se connecter avec ce que l'on peut prendre pour une adresse email pour peu que votre domaine soit configuré comme il faut (suffixe UPN identique au suffixe email et politique de nommage des utilisateurs AD identique à celle des adresses email). Concrètement, cela signifie que si vous avez une adresse email prenom.nom@domaine.com, il faudra que vos utilisateurs AD soit nommés prenom.nom et que leur suffixe UPN soit domaine.com. Cela permet à vos utilisateurs de se connecter directement avec leur adresse email (du moins avec une adresse identique à leur adresse email), ils n'ont donc pas plusieurs logins à retenir (Windows, Exchange, etc.). Ils peuvent d'ailleurs se connecter avec leur adresse UPN sur votre domaine Active Directory et ils n'ont alors qu'un login à retenir. Personnellement, j'essaie de faire en sorte que l'adresse UPN soit le seul login à retenir, c'est bien plus simple pour tout le monde ;
- volonté de proposer un SSO : si vous souhaitez proposer une authentification unique à vos utilisateurs, il faudra activer l'authentification intégrée Windows ou Basic ;
- méthode de publication d'OWA sur Internet : reverse-proxy simple ou pré-authentifiant. Si vous mettez en place un reverse-proxy simple (qui ne fait aucune authentification), vous pourrez choisir l'authentification par formulaire ou standard (avec restrictions). Si vous mettez en place un reverse-proxy pré-authentifiant, vous ne pourrez pas choisir l'authentification par formulaire. C'est le reverse-proxy qui transmettra un ticket à OWA pour dire que l'utilisateur est authentifié. Vous devrez savoir comment votre reverse-proxy transmet l'information d'authentification (ticket Digest, Kerberos, etc.) afin de choisir la bonne méthode d'authentification dans OWA.

Pour changer la méthode d'authentification, allez dans les propriétés d'OWA, onglet **Authentification** puis choisissez votre méthode d'authentification.

Pour obtenir la commande PowerShell équivalente, cliquez sur la petite icône Powershell en bas de la fenêtre après avoir changé votre méthode d'authentification.



Authentification OWA

Tout changement de méthode d'authentification requiert un redémarrage de IIS. Exécutez la commande suivante :

```
iisreset /noforce
```

VI-G-2 - Autorisation : segmentation des fonctionnalités

Il existe deux niveaux d'autorisation dans OWA : par utilisateur ou par serveur. Au niveau utilisateur, vous pourrez activer ou non l'accès OWA mais vous pourrez surtout appliquer une stratégie à vos utilisateurs. Cette stratégie, à créer dans la **configuration de l'organisation, Accès client, Stratégies de boîte aux lettres de Outlook Web App**, vous permettra de gérer différents profils d'utilisateurs. Vous pourrez au choix activer ou désactiver les fonctionnalités suivantes :

- intégration Active Sync ;
- toutes les listes d'adresses : affichage de toutes les listes ou seulement des listes globales ;
- calendrier ;
- contact ;
- journal ;
- filtrage de courrier indésirable ;
- rappels et notifications ;
- notes ;
- client - Premium : accès à l'interface étendue d'OWA ;
- dossiers de recherche ;

- signature électronique ;
- vérificateur d'orthographe ;
- tâches ;
- sélection de thème ;
- intégration à la messagerie unifiée ;
- modification de mot de passe ;
- règles ;
- dossiers publics ;
- S/MIME ;
- récupération des éléments supprimés ;
- messagerie instantanée ;
- messages SMS.

Vous pourrez également modifier ces autorisations directement sur le compte utilisateur.

VI-H - Activation d'Outlook Anywhere

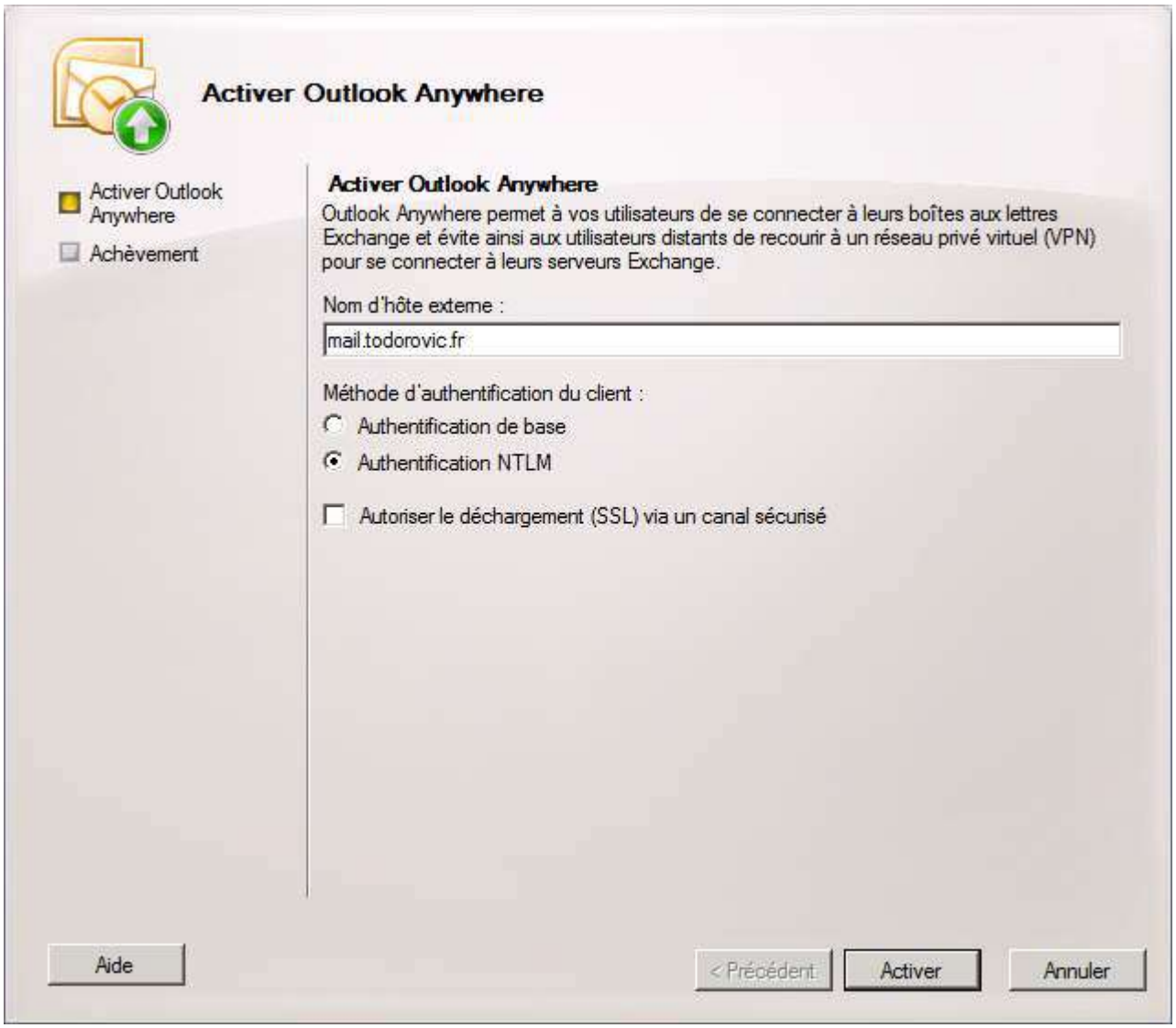
Outlook Anywhere permet la connexion de clients lourds venant d'Internet. Sa gestion se trouve donc dans le rôle d'accès client. Allez dans **Configuration du serveur, Accès client**. À droite, cliquez sur *Activer Outlook Anywhere*.

Activation d'Outlook Anywhere

Vous devrez ensuite indiquer le nom d'hôte externe ainsi que la méthode d'authentification. L'authentification de base est moins sécurisée que celle exploitant NTLM. Il est donc préférable d'utiliser la négociation NTLM.

Le déchargement SSL permet au serveur de ne plus chiffrer avec le processeur mais avec un coprocesseur dédié à cette fonction. Cette opération permet d'accélérer les chiffrements et déchiffrements SSL et par la même occasion de ne plus occuper le processeur du serveur. Ne disposant pas de ce matériel, je n'active pas cette fonction. Pour l'activer plus tard, vous devrez passer par Powershell.

Une fois la configuration effectuée, cliquez sur *Activer*.



Configuration d'Outlook Anywhere

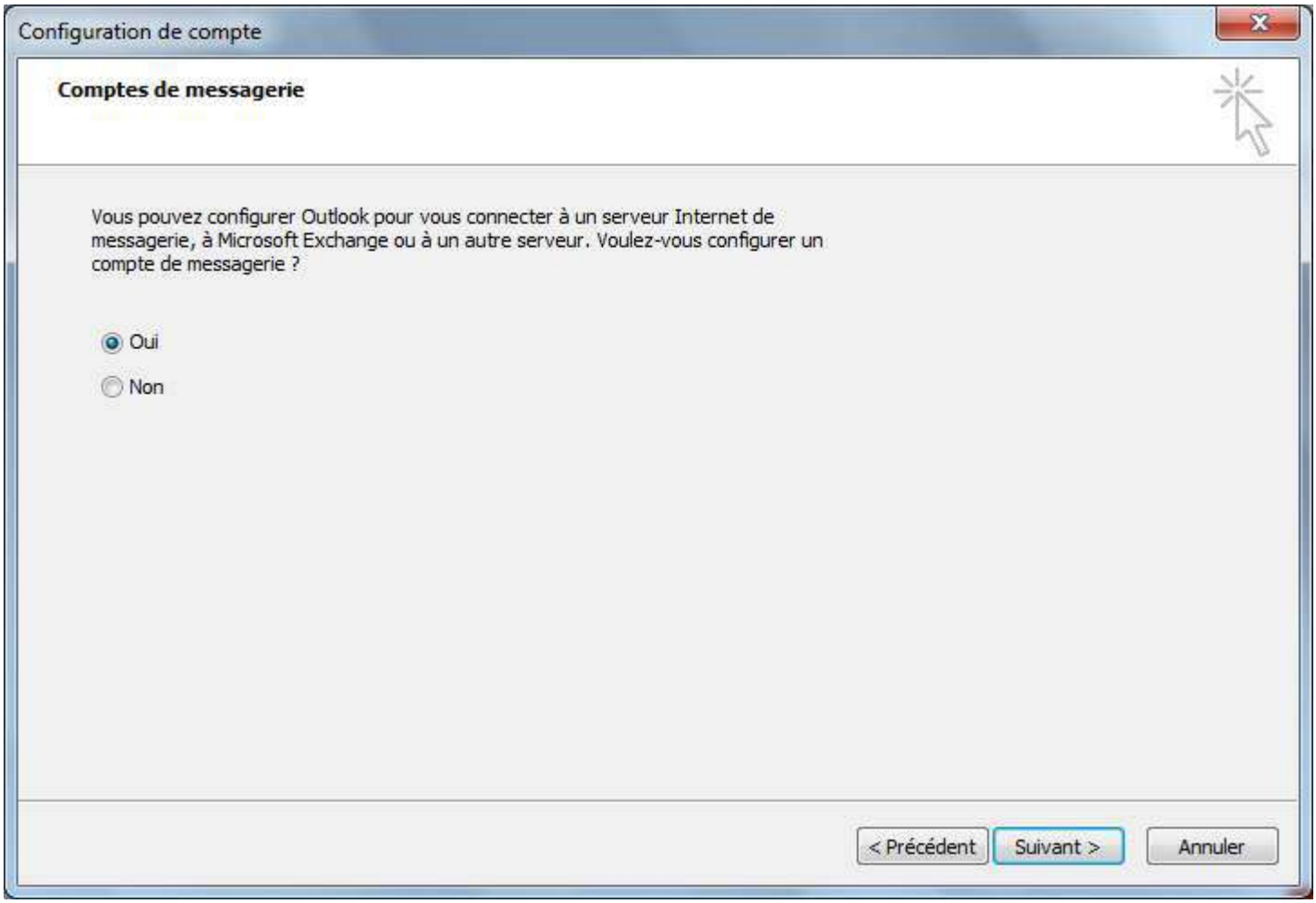
Outlook Anywhere sera activé environ 15 minutes après la fin de l'assistant. Contrôlez l'absence de messages d'erreur dans l'observateur d'événements.

Pour vous connecter via Outlook Anywhere, vous devrez avoir le service Autodiscover configuré correctement à l'extérieur de votre entreprise. En effet, Outlook demandera à Autodiscover les paramètres de connexion : Outlook passera alors uniquement en HTTPS sur Outlook Anywhere.

VII - Tests

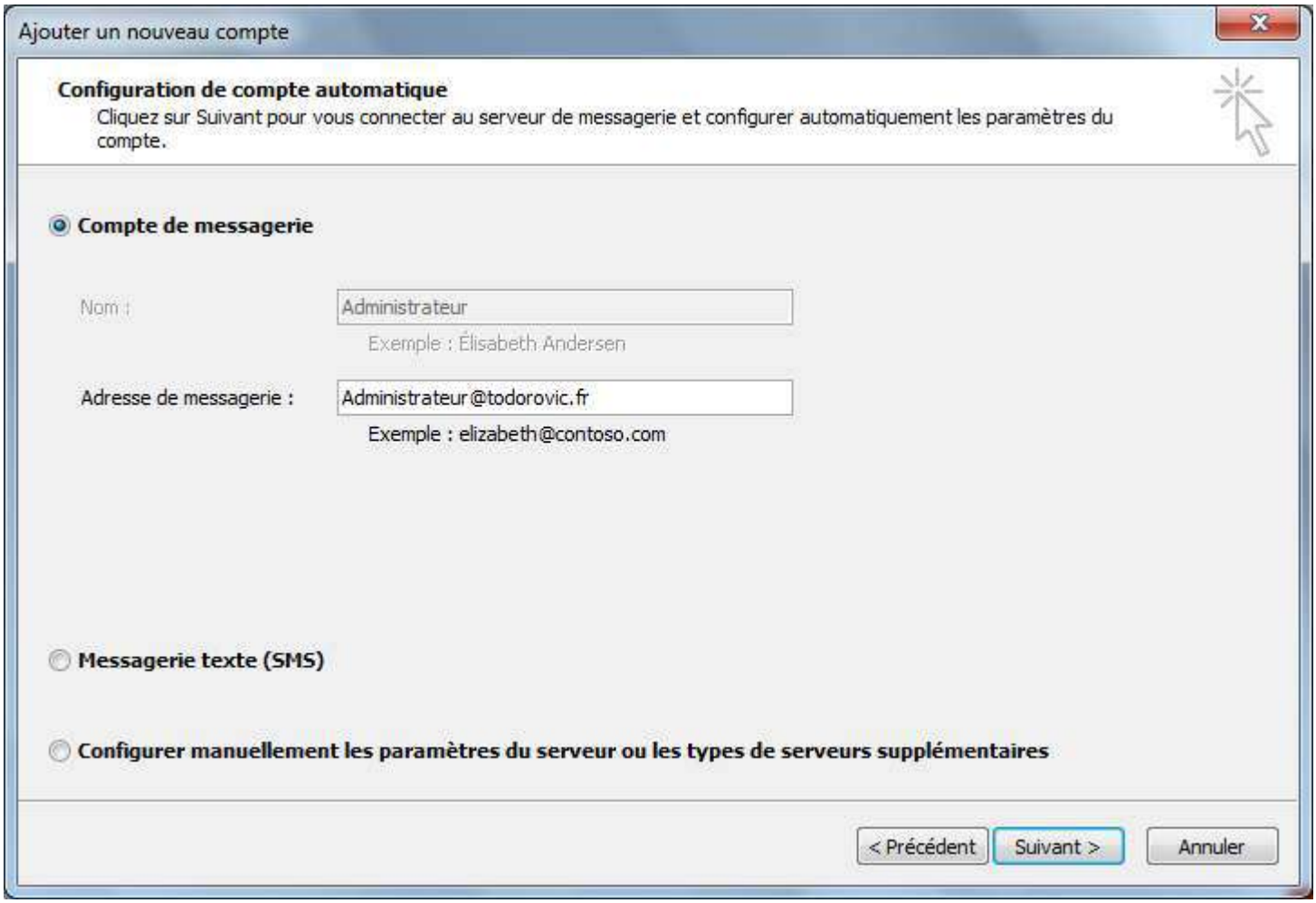
VII-A - Autodiscover interne

Ouvrez la session Windows d'un utilisateur activé sur Exchange avec Outlook non encore configuré. L'assistant de configuration va vous demander si vous souhaitez configurer un compte de messagerie. Il faut bien entendu dire oui.



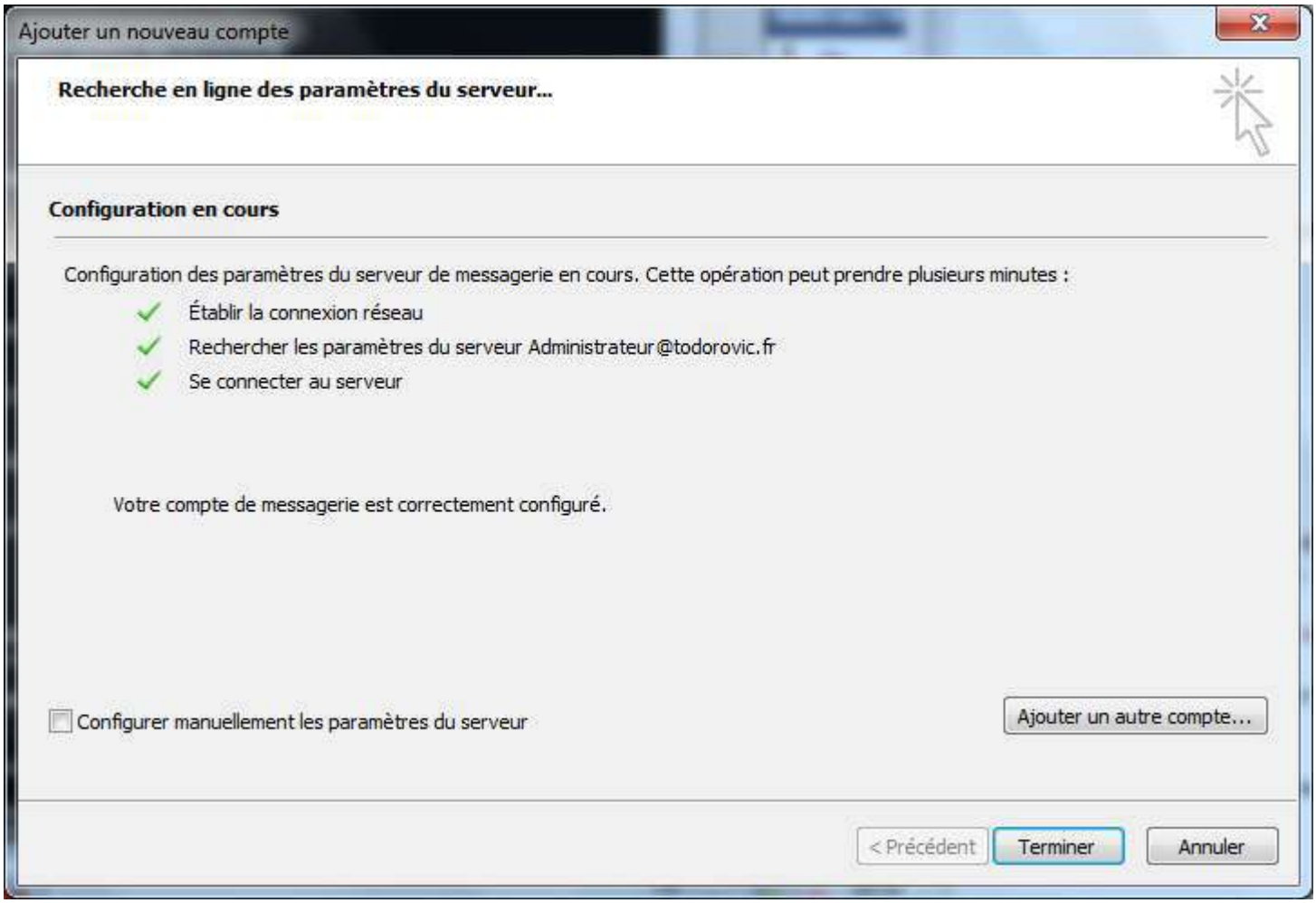
Connexion à un compte de messagerie ?

Ensuite, l'assistant va tenter de récupérer les informations d'adresse email de l'utilisateur à partir d'Active Directory. Le champ "Adresse de messagerie" devrait alors se remplir tout seul.



Adresse email récupérée

Lorsque vous cliquerez sur *Suivant*, Autodiscover se lancera pour détecter les paramètres du serveur Exchange. Si tout se passe bien, vous devriez rien avoir à faire et obtenir un compte configuré automatiquement.



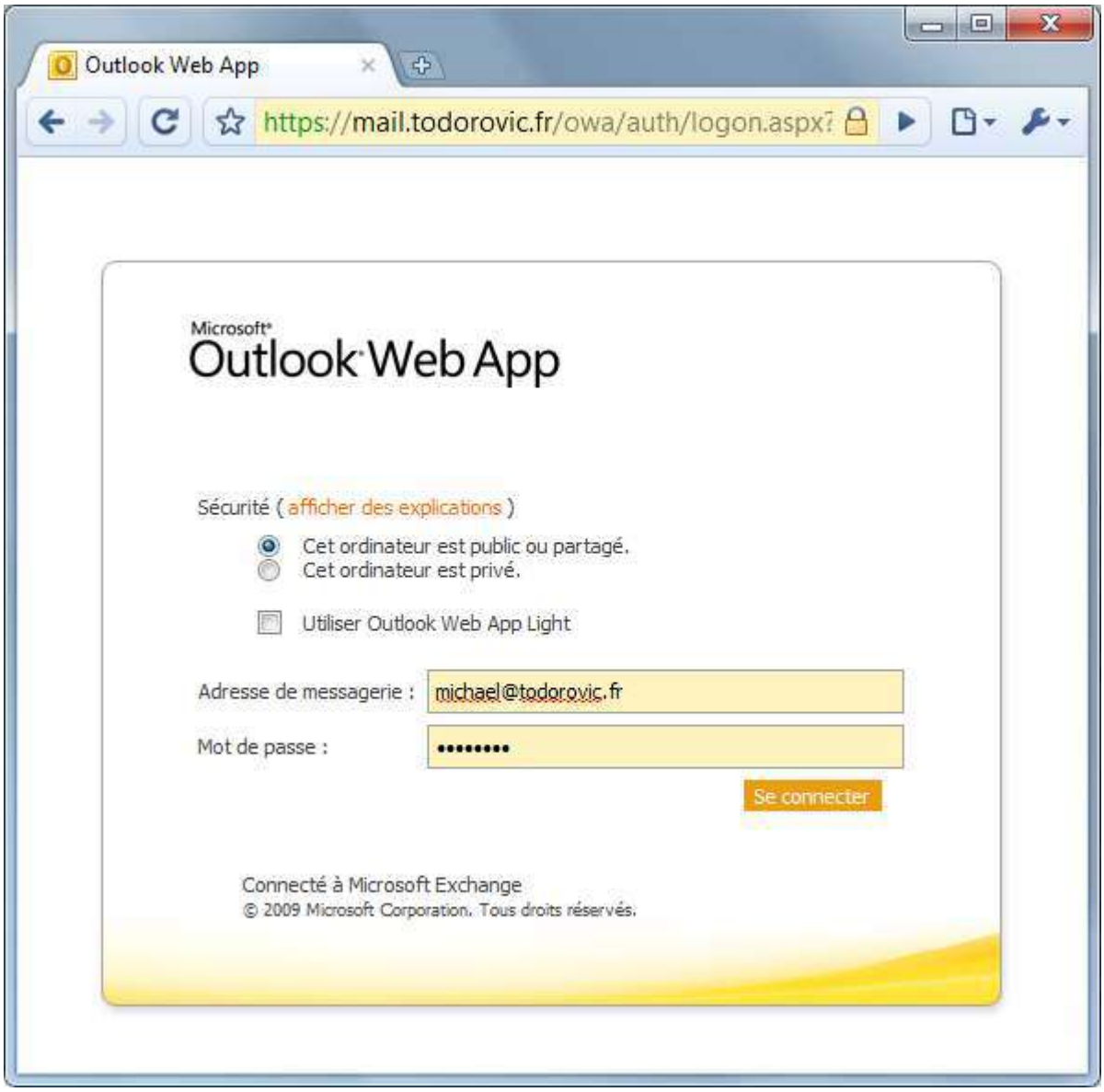
Compte Exchange configuré

VII-B - Outlook Web Access

Ouvrez un navigateur Web dans votre réseau interne puis accédez à votre serveur OWA (https://mail.todorovic.fr/owa). Dans ma maquette, j'utilise Internet Explorer et Chrome comme navigateurs. On sait déjà qu'Internet Explorer est parfaitement capable d'afficher OWA, je vais faire ce test avec Chrome.

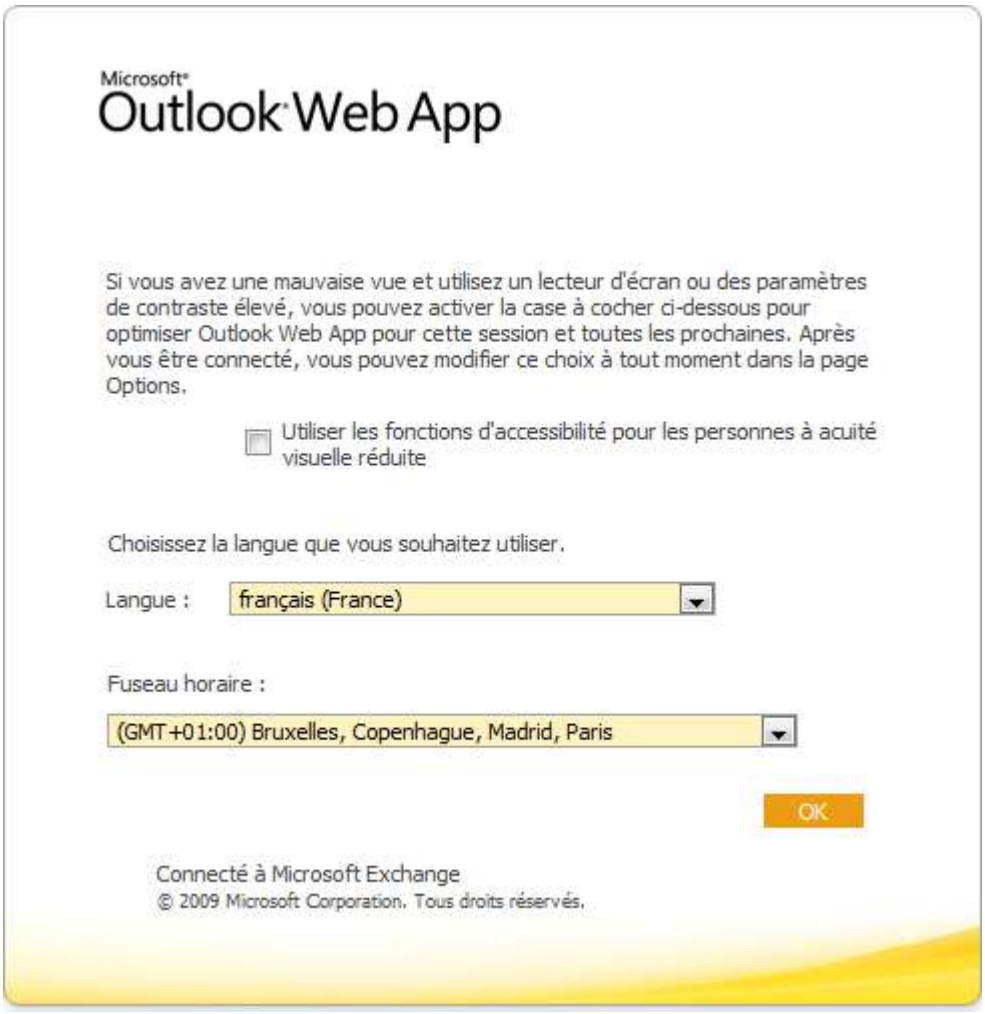
Sans faire de "troll", contrairement à Firefox, Chrome utilise les paramètres Windows : configuration d'Internet Explorer, magasins de certificats, etc. Cela veut dire qu'en déployant les certificats racines de vos autorités de certification via une GPO, Chrome exploitera ces certificats puisqu'ils sont dans le magasin de l'ordinateur : c'est pour cela que je n'ai pas d'erreur SSL. Firefox possédant ses propres magasins de certificats, il affichera une erreur SSL tant que vos autorités de certification ne seront pas dites de confiance dans Firefox.

Si vous avez configuré l'authentification par formulaire avec l'identifiant UPN, vous pourrez entrer l'adresse email de votre compte.



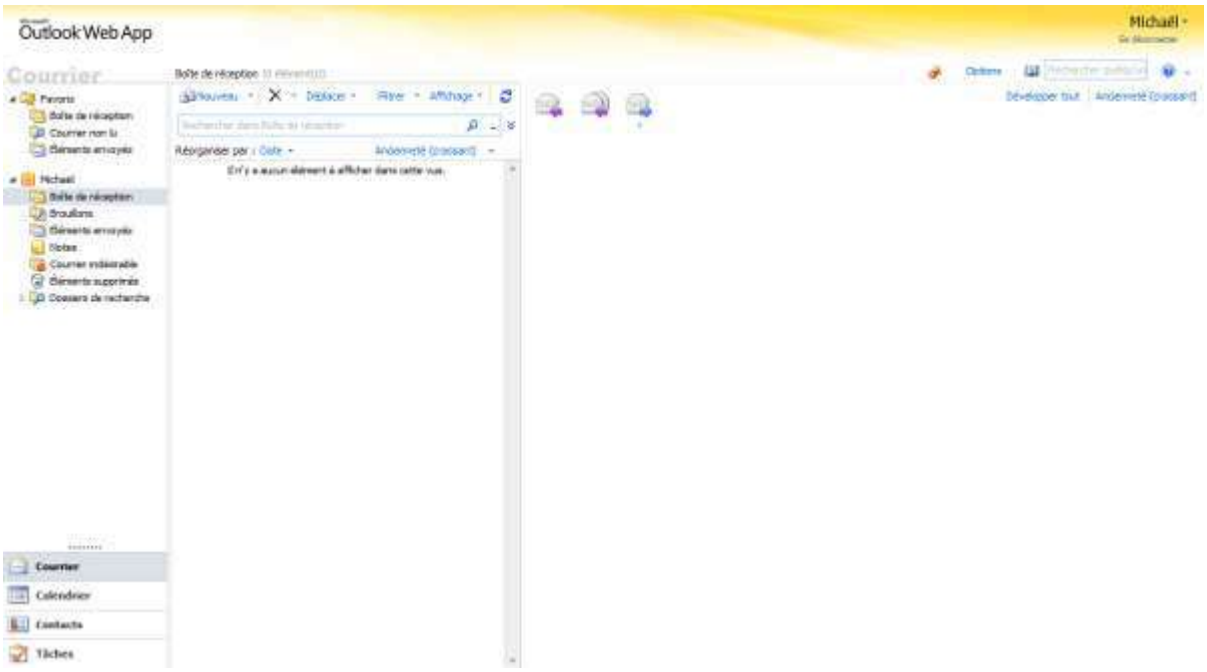
Connexion à Outlook Web App

Lors de votre premier accès à OWA, vous pourrez le configurer : langue, fuseau horaire et accessibilité.



Configuration sommaire lors de la première connexion

Vous pourrez ensuite utiliser OWA comme si vous étiez sous Outlook (ou presque).



Outlook Web App

VIII - Conclusion

Ce tutoriel vous aura permis, je l'espère, d'avoir une première approche sur Exchange 2010. Il s'agit d'un produit très complet et parfaitement intégré à Active Directory. La mise en place de ses fonctions collaboratives de base est absente puisque totalement intégrées. Le point le plus appréciable est sans doute Autodiscover : contrairement à d'autres solutions construites de toutes pièces (Postfix/Exim + solutions collaboratives), vous n'aurez plus à perdre de temps sur la configuration des clients lourds. Vous n'aurez pas non plus à perdre de temps à configurer un webmail puisqu'il est totalement intégré au serveur.

L'autre avantage énorme d'Exchange concerne la mobilité : Outlook Anywhere vous permet de passer à travers les firewalls puisqu'il utilise HTTPS. Certains diront : "oui et alors... ?" par exemple, il m'est déjà arrivé de me connecter à un Wi-Fi dans un hôtel (réalisé par une box d'un opérateur au nom d'agrume) qui par défaut bloque les SMTP autres que celui de l'opérateur : impossible donc d'envoyer des emails. Il est également possible d'aller dans d'autres endroits où la connexion est limitée aux ports 80 et 443 : il vous sera alors impossible d'utiliser SMTP, IMAP/POP. On a donc une solution quasi passe-partout.

Exchange est donc une solution très bien pensée et en avance par rapport à la concurrence sur beaucoup de points (oui, Exchange n'est pas parfait). Vous ne regretterez sans doute pas ce choix... à condition de correctement dimensionner votre infrastructure.

IX - Remerciements

Je tiens à remercier **jacques_jean** et **shawn12** pour leurs conseils et corrections.