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.

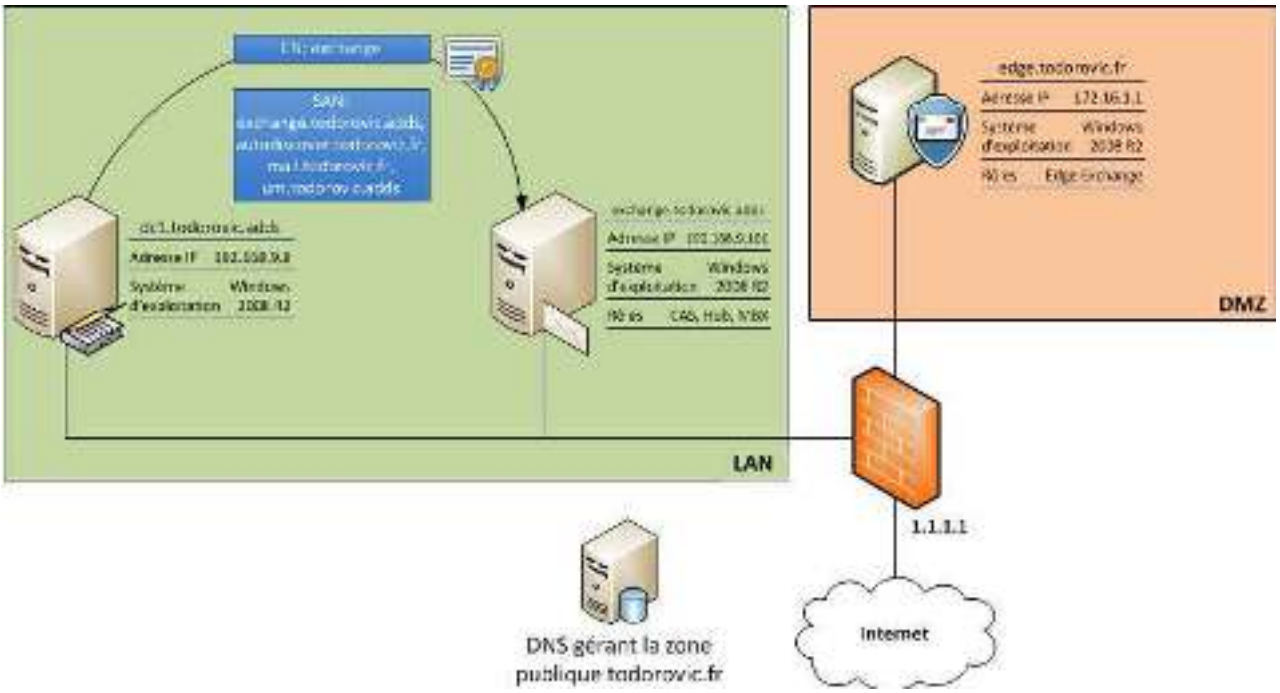
II-B-3 - Outlook Anywhere

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 :