Academy Microsoft Exchange 2010 – Module 4

Ou comment réaliser en laboratoire sa migration de Exchange 2003 vers Exchange 2010 et en tester quelques nouvelles fonctionnalités.

Sommaire

[MODULE 4 : Délégation des accès avec Exchange 2010 2](#_Toc259488692)

[Principe de fonctionnement des Role Based Access Control (RBAC) 2](#_Toc259488693)

[Création d'un groupe de rôle personnalisé 4](#_Toc259488694)

[Création d'une étendue 4](#_Toc259488695)

[Ajout d'un nouveau rôle 4](#_Toc259488696)

[Affectation des entrées de rôles 5](#_Toc259488697)

[Création d'un nouveau groupe de rôle 6](#_Toc259488698)

[Conclusion 6](#_Toc259488699)

[Annexe 7](#_Toc259488700)

[Ressources complémentaires 7](#_Toc259488701)

[Rôles prédéfinis 7](#_Toc259488702)

# MODULE 4 : Délégation des accès avec Exchange 2010

Après avoir migré ou commencé à migré les boites aux lettres vers Exchange 2010, un administrateur souhaitera souvent déléguer certaines activités à des personnes soit mieux informées (par exemple, le département d'un individu) ou par des personnes habilitées à la faire (par exemple un avocat pour une recherche légale).

Dans les versions précédentes d'Exchange, donner ce genre d'accès avec uniquement les droits nécessaires s'avérait souvent très complexe voire impossible. Ce qui a amené bien souvent les administrateurs à effectuer une délégation d'administration complète de la messagerie en reposant sur un certain niveau de confiance dans les personnes ayant obtenu ce niveau de permission sous peine de se voir inondé de demandes.

Ces états sont souvent remontés lors des audits du système d'information des entreprises et l'une des conclusions de l'audit est de limiter les accès des collaborateurs d'une entreprise aux seuls autorisations nécessaires pour accomplir leur mission.

Exchange 2010 permet aux administrateurs de messagerie de répondre à ces besoins d'accès limités aux seuls besoins des métiers des entreprises ou d'un rôle. C'est ainsi que l'on parle de **RBAC – Role Based Access Control**.

## Principe de fonctionnement des Role Based Access Control (RBAC)

Le principe général de fonctionnement des RBAC est de ne donner à un rôle d'utilisateur (autre que l'administrateur) que les permissions nécessaires pour accomplir ce rôle.

Cela fonctionne sur le principe du

* **Où ?**
Avec le "où", on définit le périmètre de l'intervention d'un rôle à définir. Ce "où" peut être une liste personnalisée d'utilisateurs, la liste des utilisateurs d'une unité d'organisation (OU), les utilisateurs ayant leur boite aux lettres sur un serveur, etc …
* **Quoi ?**
C'est en quelque sorte le point central du RBAC et on définit ici le rôle que l'on souhaite manipuler. Ce rôle peut être un des rôles fournit par défaut ou un des rôles personnalisé. Nous verrons plus loin comment créer des rôles personnalisés.
Les rôles sont des conteneurs qui font en fait référence à des entrées de rôle. Ces entrées de rôle sont tout simplement des commandes associées à une série de paramètres autorisés. Par exemple, un set-user peut n'être autorisé que sur le paramètre "HomePhone".
* **Qui ?**
Quels sont les utilisateurs qui héritent de ce rôle, ou encore à quels individus on affecte ce rôle.

Ces trois points donnent une vision macroscopique de l'approche des RBAC. Il est important de bien noter une différence entre le rôle utilisé ici et le groupe de rôles utilisé ensuite qui est souvent appelé "rôle" par abus de langage.

Par exemple, le groupe de rôle "Recipient Management" (gestion des destinataires) est un groupe de rôles qui donne accès aux rôles unitaires suivants :

* Rôle des groupes de distribution
* Rôle des dossiers publics à extension messagerie
* Rôle de création du destinataire de messagerie
* Rôle des destinataires de message
* Rôle de suivi des messages
* Rôle de migration
* Déplacer le rôle des boîtes aux lettres
* Rôle des stratégies du destinataire

Dans la suite du document, nous ferons la distinction entre ces deux notions pour éviter les erreur de compréhension.

Ce principe d'affectation peut se schématiser comme suit :



Le point de démarrage étant le rôle à proprement parler.

Afin d'aider autant que possible les administrateurs de la messagerie Exchange 2010, l'équipe produit a créé 11 groupes de rôle par défaut qui devrait permettre de répondre aux besoins d'une très large majorité des entreprises. Ces groupes de rôles sont les suivants :

* Organization Management
* Public Folder Management
* Recipient Management
* View-Only Organization Management
* UM Management
* Help Desk
* Records Management
* Discovery Management
* Server Management
* Delegated Setup
* Hygiene Management

Je ne rentrerai pas dans le détail des prérogatives de chaque groupe de rôle, vous retrouverez ces informations sur le site Technet à l'adresse suivante : <http://technet.microsoft.com/fr-fr/library/dd351266.aspx>

Nous allons maintenant suivre pas à pas les étapes à suivre pour créer un groupe de rôle personnalisé.

## Création d'un groupe de rôle personnalisé

Dans le cadre de notre Exchange Academy, nous allons créer un groupe de rôle pour autoriser des personnes à gérer spécifiquement les directeurs de l'organisation.

### Création d'une étendue

La première étape de la procédure consiste à définir le périmètre d'application du rôle que nous allons créer ensuite. Ce périmètre peut être une OU, une requête sur l'annuaire Active Directory etc … Dans notre cas, nous allons créer une requête sur l'annuaire de l'entreprise.

New-ManagementScope –Name "Directeurs" –RecipientRestrictionFilter {memberofgroup –eq "cn=Directeurs,ou=Directions,dc=ucdemo,dc=fr"}

Note: Le conteneur "Directeurs" est à créer dans la console de gestion des utilisateurs et ordinateurs de Active Directory.

Nous venons de créer une étendue que nous allons utiliser ultérieurement dans la création du nouveau groupe de rôle, dans le schéma précédent, il s'agit du "**Ou ?**"

Cette étape est optionnelle, en effet, si nous ne spécifions aucun périmètre d'application du rôle, celui héritera du périmètre du rôle parent.

### Ajout d'un nouveau rôle

Nous allons maintenant définir le "**Quoi ?**" du schéma de présentation des groupes de rôle. Pour commencer, il faut créer le "Rôle" auquel nous allons affecter ensuite des entrées de rôle. Un rôle personnalisé dans Exchange 2010 doit nécessairement descendre d'un des rôles prédéfini. Il existe 65 rôles dit "builtin"; la liste de ces rôles est disponible en annexe de ce module.

Dans notre exemple, nous allons travailler sur une déclinaison du rôle "**MailRecipient**". Ce rôle par défaut est associé à la gestion des boites aux lettres, des utilisateurs de messagerie, des contacts, des listes de distribution (dynamiques ou non). Ce rôle a la particularité de ne pas permettre de créer d'objets nouveaux, seulement de modifier les objets existants.

Dans notre cas des directeurs, c'est souvent une bonne chose de séparer des personnes autorisées à créer les objets des personnes autorisées à les modifier. La première opération ayant plus d'impactant que la seconde.

Créons donc un nouveau rôle :

New-ManagementRole –Name "Gestion des directeurs" –Parent "Mail Recipients"

Cette cmdlet exécutée depuis une ligne de commande Powershell vient juste de créer un rôle de gestion personnalisé qui est identique au rôle prédéfinit "Mail Recipient".

Nous allons maintenant affecter des entrées de rôles à ce rôle, c’est-à-dire indiquer les opérations qui seront autorisées pour les personnes qui hériteront de ce rôle unitaire.

### Affectation des entrées de rôles

Comme par défaut la création d'un nouveau rôle hérite de toutes les entrées de rôle de son parent, en fonction de ce que vous souhaitez effectuer, il faut soit tout supprimer (sauf une entrée de rôle, le système ne vous laissera pas avoir un rôle vide) et ajouter des entrées une à une soit supprimer à l'unité les entrées de rôles que vous ne souhaitez pas voir affecté à ce rôle.

Dans notre cas, nous allons prendre la première option à savoir supprimer toutes les entrées de rôle sauf une. Pour cela, powershell va nous permettre de réaliser l'opération en une ligne de commande:

Get-ManagementRoleEntry "Gestion des directeurs\\*" | where {$\_.name –ne "Get-user"} | Remove-ManagementRoleEntry

La première partie de la ligne de commande liste toutes les entrées de rôles du rôle que nous avons créé à l'étape suivante.

La deuxième partie de la ligne de commande n'affiche que les entrées qui ne commencent pas par "Get-user", nous allons garder ces entrées pour créer notre rôle personnalisé.

La troisième partie de la ligne de commande supprimes les entrées de rôle que nous avons identifiées avec les deux premiers morceaux de la ligne de commande.

Il faut maintenant ajouter les entrées de rôle que nous souhaitons mettre à disposition de ce rôle. Pour cela, nous allons lancer la ligne suivante en powershell :

Add-ManagementRoleEntry "Gestion des directeurs\set-user" –Parameters FirstName,HomePhone,LastName,Notes,Office,MobilePhone, Department,Manager

Notre rôle a donc maintenant les entrées de rôle :

* Get-user avec tous les paramètres par défaut du rôle parent (mailrecipient)
* Set-user avec uniquement les paramètres FirstName,HomePhone,LastName,Notes,Office,MobilePhone,Department,Manager (ce sont les seuls paramètres autorisés à être modifiés pour une personne qui aura le rôle).

Il reste à définir le groupe de rôle pour permettre d'affecter ce rôle à des utilisateurs.

### Création d'un nouveau groupe de rôle

Le groupe de rôle est en fait un véritable groupe dans Active Directory qu'il est possible de voir avec la vue avancée de la console "Utilisateurs et Ordinateurs" de Active Directory auquel est attaché la série de permissions qui découlent des rôles unitaires qui sont associés à ce groupe de rôle.

La création du groupe de rôle va permettre d'associer l'étendue créée dans la première étape et le rôle que nous venons de créer. Il faut lancer la ligne de commande suivante :

New-RoleGroup –name "RG-Gestion des Directeurs" –Role "Gestion des Directeurs" –CustomRecipientWriteScope "Directeurs"

Le groupe de rôles "RG-Gestion des Directeurs" apparait maintenant dans l'ECP pour pouvoir affecter ce rôle à des utilisateurs de l'organisation.

Un utilisateur qui se voit affecter ce rôle peut donc :

* Lire les attributs de destinataires
* Modifier les attibuts comme le prénom, le nom, le numéro de téléphone personnel, le bureau, le téléphone mobile, le département et le responsable
* Uniquement pour les comptes placés dans l'OU "Directions\Directeurs"

Nous avons créé un rôle personnalisé au sein de notre organisation Exchange 2010.

## Conclusion

Exchange 2010 apporte un nouveau modèle de permissions basé sur des rôles. Cette approche est non seulement très granulaire tout en permettant de simplifier la gestion de la délégation des permissions dans une organisation.

La gestion des rôles et des groupes de rôles peut être personnalisé de façon intensive mais il est impératif d'avoir une vision claire du sujet et de ce que l'on veut obtenir comme résultat avant de se lancer dans cette approche sous peine de se perdre en complexité et obtenir l'inverse de l'effet escompté.

Il est globalement recommandé d'essayer de trouver le groupe de rôle approprié dans les groupes de rôles par défaut avant de commencer à regarder les groupes de rôle personnalisé.

Merci à Laurent Teruin pour les sources de l'exemple utilisé ici.

# Annexe

## Ressources complémentaires

Site technet sur les RBAC : <http://technet.microsoft.com/fr-fr/library/dd298183.aspx>
Et : <http://technet.microsoft.com/fr-fr/library/dd638186.aspx>

Présentation aux Techdays 2010 sur le sujet : <http://www.microsoft.com/france/vision/mstechdays10/Webcast.aspx?EID=450d555f-8ff6-49a0-baf0-051efd7a9ea6>

## Rôles prédéfinis

Liste des rôles prédéfinis (La liste est disponible à cette adresse : <http://technet.microsoft.com/fr-fr/library/dd298116.aspx>):

* ACTIVE DIRECTORY PERMISSIONS ROLE
* ADDRESS LISTS ROLE
* APPLICATIONIMPERSONATION ROLE
* AUDIT LOGS ROLE
* CMDLET EXTENSION AGENTS ROLE
* DATABASE AVAILABILITY GROUPS ROLE
* DATABASE COPIES ROLE
* DATABASES ROLE
* DISASTER RECOVERY ROLE
* DISTRIBUTION GROUPS ROLE
* EDGE SUBSCRIPTIONS ROLE
* E-MAIL ADDRESS POLICIES ROLE
* EXCHANGE CONNECTORS ROLE
* EXCHANGE SERVER CERTIFICATES ROLE
* EXCHANGE SERVERS ROLE
* EXCHANGE VIRTUAL DIRECTORIES ROLE
* FEDERATED SHARING ROLE
* INFORMATION RIGHTS MANAGEMENT ROLE
* JOURNALING ROLE
* LEGAL HOLD ROLE
* MAIL ENABLED PUBLIC FOLDERS ROLE
* MAIL RECIPIENT CREATION ROLE
* MAIL RECIPIENTS ROLE
* MAIL TIPS ROLE
* MAILBOX IMPORT EXPORT ROLE
* MAILBOX SEARCH ROLE
* MESSAGE TRACKING ROLE
* MIGRATION ROLE
* MONITORING ROLE
* MOVE MAILBOXES ROLE
* MYBASEOPTIONS ROLE
* MYCONTACTINFORMATION ROLE
* MYDIAGNOSTICS ROLE
* ACTIVE DIRECTORY PERMISSIONS ROLE
* ADDRESS LISTS ROLE
* APPLICATIONIMPERSONATION ROLE
* AUDIT LOGS ROLE
* CMDLET EXTENSION AGENTS ROLE
* DATABASE AVAILABILITY GROUPS ROLE
* DATABASE COPIES ROLE
* DATABASES ROLE
* DISASTER RECOVERY ROLE
* DISTRIBUTION GROUPS ROLE
* EDGE SUBSCRIPTIONS ROLE
* E-MAIL ADDRESS POLICIES ROLE
* EXCHANGE CONNECTORS ROLE
* EXCHANGE SERVER CERTIFICATES ROLE
* EXCHANGE SERVERS ROLE
* EXCHANGE VIRTUAL DIRECTORIES ROLE
* FEDERATED SHARING ROLE
* INFORMATION RIGHTS MANAGEMENT ROLE
* JOURNALING ROLE
* LEGAL HOLD ROLE
* MAIL ENABLED PUBLIC FOLDERS ROLE
* MAIL RECIPIENT CREATION ROLE
* MAIL RECIPIENTS ROLE
* MAIL TIPS ROLE
* MAILBOX IMPORT EXPORT ROLE
* MAILBOX SEARCH ROLE
* MESSAGE TRACKING ROLE
* MIGRATION ROLE
* MONITORING ROLE
* MOVE MAILBOXES ROLE
* MYBASEOPTIONS ROLE
* MYCONTACTINFORMATION ROLE
* MYDIAGNOSTICS ROLE