



Exchange 2010: Role Based Access Control (RBAC) Deep Dive



Mike Pfeiffer
Systems Instructor
Interface Technical Training

What is RBAC?

- Simplified access control administration
- Admins don't deal with ACLs in AD or Exchange
- Permissions are focused on tasks, not objects
- Granular Delegation of Rights
- Self-Service management



How RBAC Works

Role Based Access Control (RBAC)

Role Assignment – The link that holds together the Who, What, and Where.

Role (What) – Defines what can be done by a set of cmdlets and parameters that can be run.

Add/Del/Mod
Users



**Role
(What)**

Boston
Users



**Scope
(Where)**

Scope (Where) Defines the objects in AD that the Role can act on.
For example, the Boston Users OU

Role Group (Who) A security group that defines Who gets a specific scope applied to them. For example, the Boston Exchange Admins



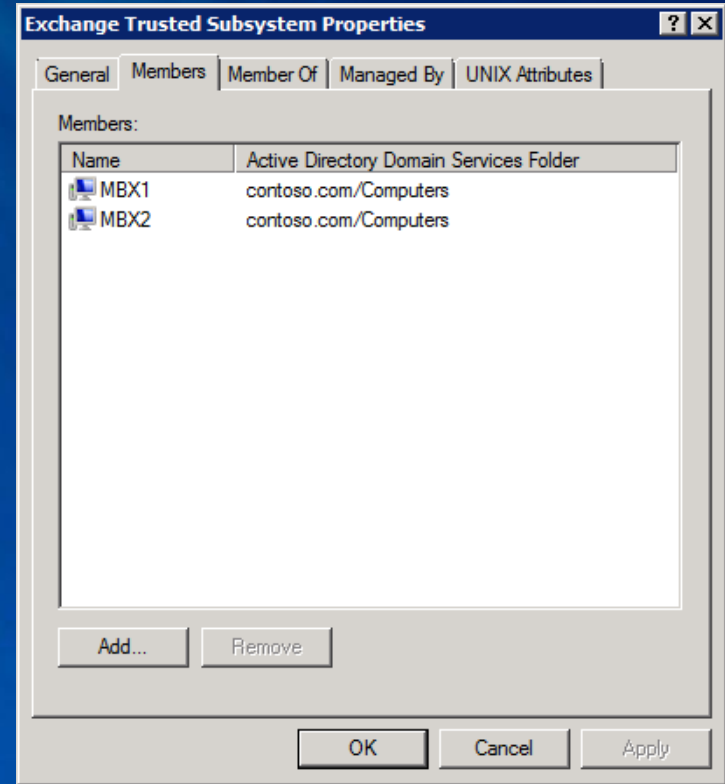
**Role Group
(Who)**

Boston Exchange
Admins

**Role
Assignment**

How RBAC Works

- Tasks are carried out by cmdlets through Remote Powershell
- Tasks run under the security context of the Exchange servers
- Exchange servers have rights in Active Directory



How RBAC Works

- Scope (Where):
Defines objects a role can act on
- Role (What):
Set of cmdlets and parameters
- Role Group (Who):
Active Directory Security Group
- Role Assignment (Glue):
Links the Who, What,
and Where

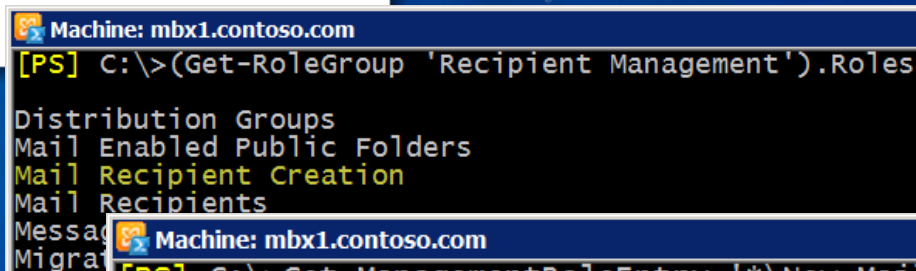


How RBAC Works

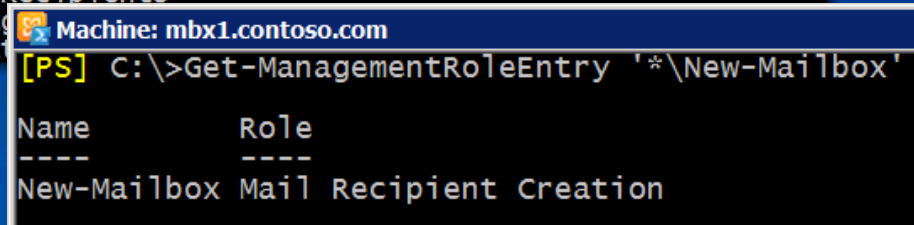
Scope (Where)



Role (What)



Role Group (Who)



The Where

- Management Scope Defines the “Where”
- Default Scope is Inherited
- Recipients
 - Recipient Root
 - Recipient Filter
- Servers
 - Server List
 - Server Filter
- Databases
 - Database List
 - Database Filter

```
New-ManagementScope -Name Employees`  
-RecipientRoot contoso.com/Employees`  
-RecipientRestrictionFilter {  
  RecipientType -eq 'UserMailbox' -or  
  RecipientType -eq 'MailUser' -or  
  RecipientType -eq 'MailContact'  
}
```

```
New-ManagementScope -Name 'Phoenix Servers'`  
-ServerList 'PHX-EX01', 'PHX-EX02', 'PHX-EX03'
```

```
New-ManagementScope -Name 'Phoenix Databases'`  
-DatabaseRestrictionFilter {Name -Like 'PHX*'}
```

The What

- Management Roles Defines the “What”
- Get-ManagementRole
- Get-ManagementRoleEntry
- Defines:
 - Cmdlets
 - Parameters

```
Machine: mbx1.contoso.com
[PS] C:\>Get-ManagementRole

Name                                     RoleType
----                                     -
Recipient Policies                      RecipientPolicies
Active Directory                         ActiveDirectory
Address Lists                            AddressLists
Audit Logs                               AuditLogs
Cmdlet Extensions                        CmdletExtensions

Machine: mbx1.contoso.com
[PS] C:\>Get-ManagementRoleEntry 'Exchange Servers\*'

Name                                     Role
----                                     -
Write-AdminAuditLog                     Exchange Servers
Update-OfflineAddressBook                Exchange Servers
Set-UmServer                             Exchange Servers
Set-TransportServer                      Exchange Servers
```


The Who

- Role Groups
- Active Directory Security Groups
- User Accounts

```
Machine: mbx1.contoso.com
[PS] C:\>Get-RoleGroup 'Organization Management' |
>> Get-RoleGroupMember
>>

Name                               RecipientType
----                               -
Administrator                       UserMailbox
```

```
Machine: mbx1.contoso.com
[PS] C:\>New-RoleGroup -Name 'Phoenix Admins' -Members wjordan,JCarrillo

Name                AssignedRoles      RoleAssignments      ManagedBy
----                -
Phoenix Admins      {}                  {}                    {contoso.com/M...
```

The Glue

- Management Role Assignments
- Define:
 - Scope
 - Role
 - Group or User
- Everything gets stuck together using a Role Assignment

```
Machine: mbx1.contoso.com
[PS] C:\>New-ManagementRoleAssignment
>> -Role 'Mailbox Import Export'
>> -SecurityGroup 'Phoenix Admins'
>>
```

```
Machine: mbx1.contoso.com
[PS] C:\>New-ManagementRoleAssignment
>> -Role 'Mailbox Import Export'
>> -User administrator
>>
```

Demo – RBAC for Administrators

○ Scenario

- Support personnel should be able to create Exchange recipients in the Sales OU in AD
- Support personnel should not be able to create Exchange recipients in any other OU in AD
- Support personnel should not be able to remove recipients in the Sales OU, or any other OU in AD

RBAC for End-Users

- Role Assignment Policies
- Set Per Mailbox using the RoleAssignmentPolicy attribute
- One Created by Default

```
Machine: mbx1.contoso.com
[PS] C:\>Get-RoleAssignmentPolicy | select name
Name
----
Default Role Assignment Policy
```

```
Machine: mbx1.contoso.com
[PS] C:\>(Get-RoleAssignmentPolicy).AssignedRoles
MyDistributionGroupMembership
MyBaseOptions
MyContactInformation
MyTextMessaging
MyVoiceMail
```

Demo – RBAC for End-Users





- Scenario


- End-Users can currently modify their Work, Fax, Mobile, and Home Phone numbers in ECP
- End-Users should be only be allowed to modify their Home Phone number in ECP

Distribution Group Management

- MyDistributionGroups Role
- Not Assigned by Default
- Allows End-Users to manage membership of DG's they own
- Allows End-Users to add DG's



Public Groups I Own


 New... |  Details |  | 



Display Name	E-Mail Address
Marketing	Marketing@contoso.com
Sales	Sales@contoso.com

Managed by:

 Add... 

Display Name	Organizational Unit
 Administrator	contoso.com/Users

Demo – RBAC for End-Users

- Scenario

- End-Users need to manage the membership of DG's they own
- End-Users should not be able to add or remove DG's

Troubleshooting RBAC

- Get-ManagementRoleAssignment
 - GetEffectiveUsers
 - WritableRecipient, WritableServer, WriteableDatabase
- Get-ManagementRoleEntry
 - Supports Wildcards
- Get-ManagementRole
 - Cmdlet
 - CmdletParameters

```
Get-ManagementRoleAssignment
-WritableRecipient djones
-GetEffectiveUsers |
  Where-Object{
    $_.EffectiveUserName -eq 'sysadmin'
  }
```

```
Machine: mbx1.contoso.com
[PS] C:\>Get-ManagementRole -CmdletParameters Phone

Name                               RoleType
----                               -
Mail Recipient Creation            MailRecipientCreation
Mail Recipients                    MailRecipients
Monitoring                         Monitoring
```


Thank You!

- Blog: www.mikepfeiffer.net
- E-Mail: mike.pfeiffer@interfacett.com
- Twitter: [@mike_pfeiffer](https://twitter.com/mike_pfeiffer)