interface
TECH | IMMERSION

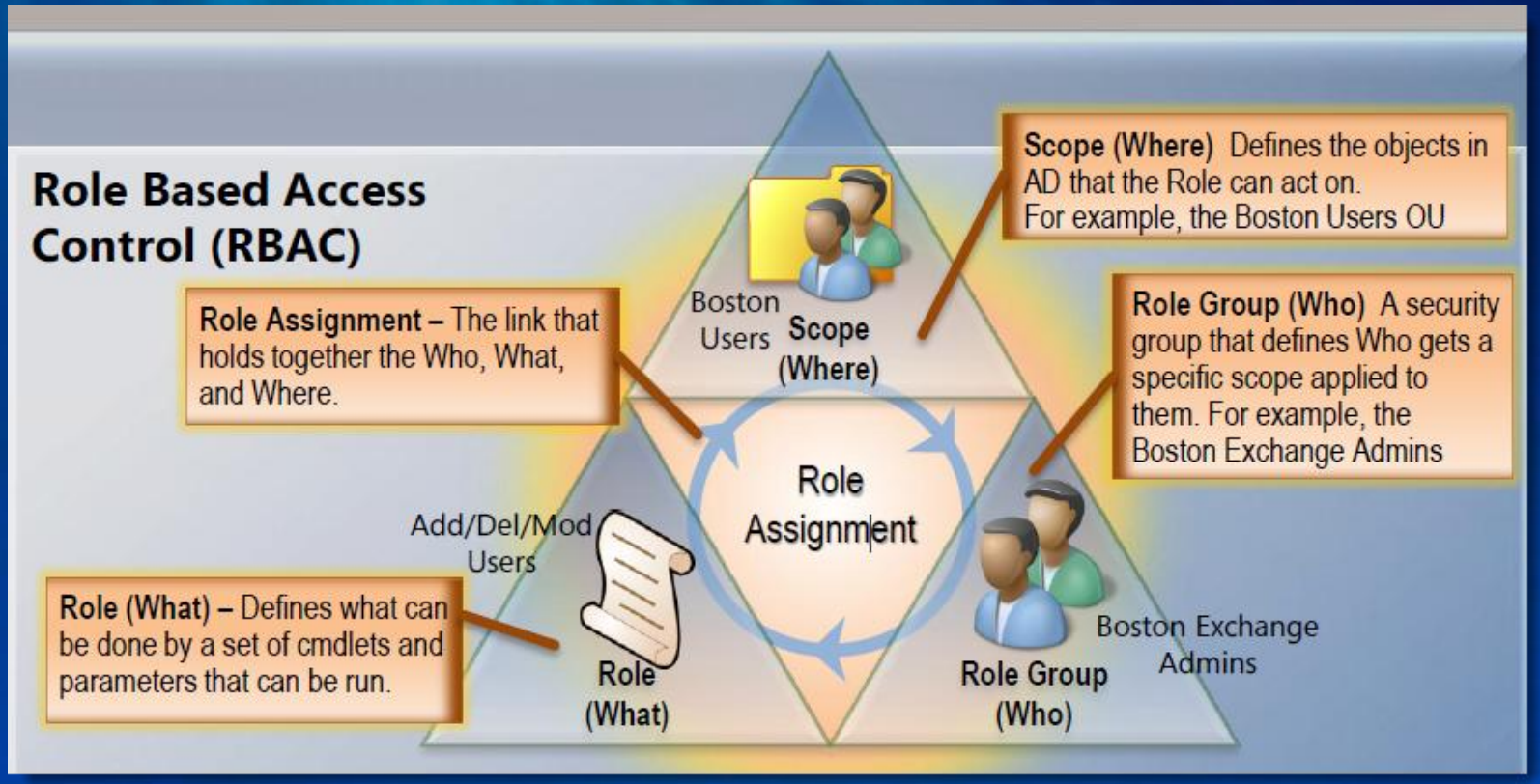
# Exchange 2010: Role Based Access Control (RBAC) Deep Dive

Mike Pfeiffer
Systems Instructor
Interface Technical Training

# What is RBAC?

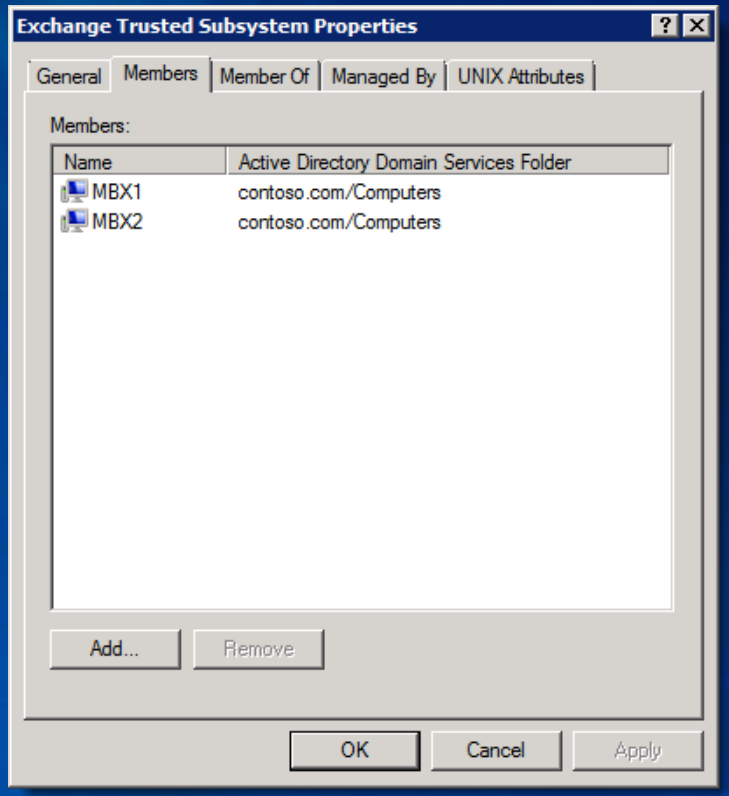
- Simplified access control administration
- Admins don’t deal with ACLs in AD or Exchange
- Permissions are focused on tasks, not objects
- Granular Delegation of Rights
- Self-Service management

# How RBAC Works



# 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



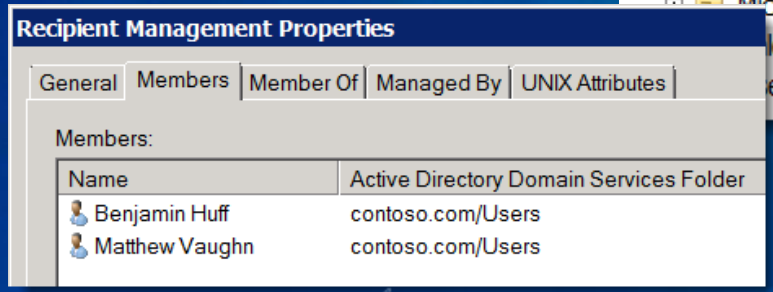
# How RBAC Works

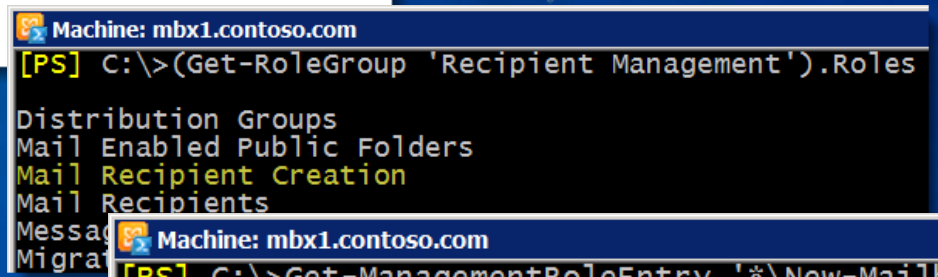
- Scope (Where):
  Defines objects a role can act on
- Role (What):
  Set of cmdlets and parameters
- Role Group (Who):
  Active Directory Security Group
- Role Assignment (Glue):
  Links the Who, What,
  and Where

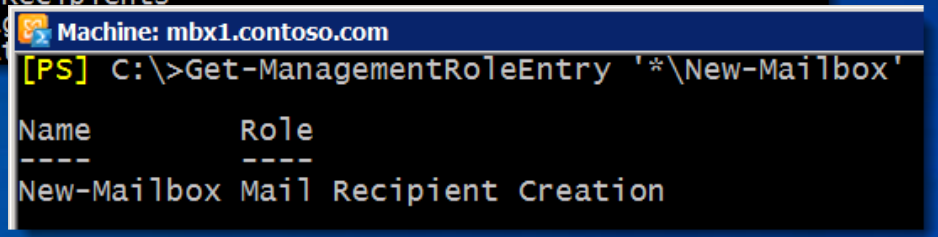
# How RBAC Works

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

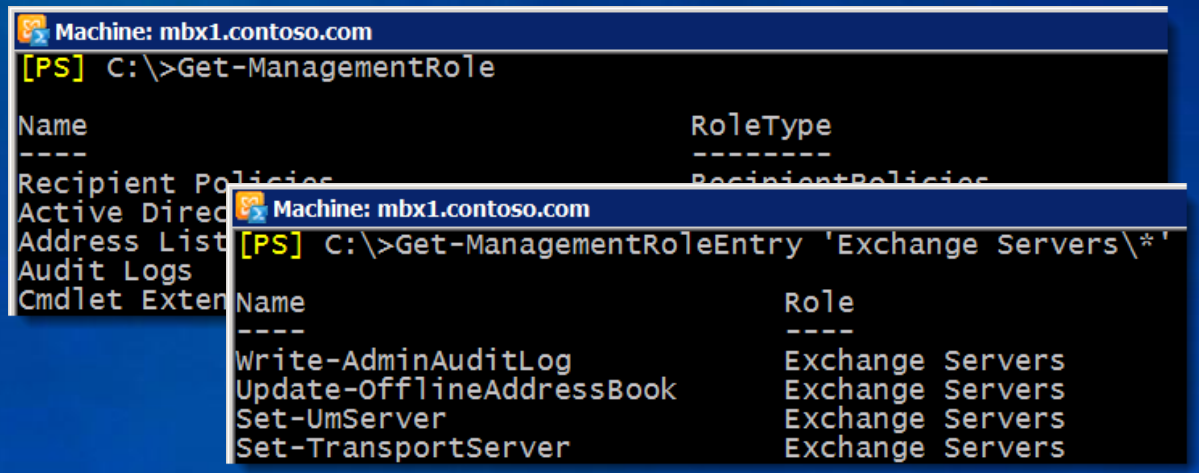
```
New-ManagementScope -Name Employees `
-RecipientRoot contoso.com/Employees `
-RecipientRestrictionFilter {
  RecipientType -eq 'UserMailbox' -or
  RecipientType -eq 'MailUser' -or
  RecipientType -eq 'MailContact'
}
```

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

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

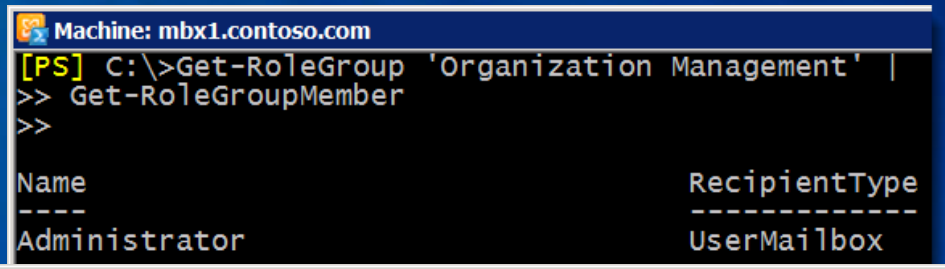
# The What

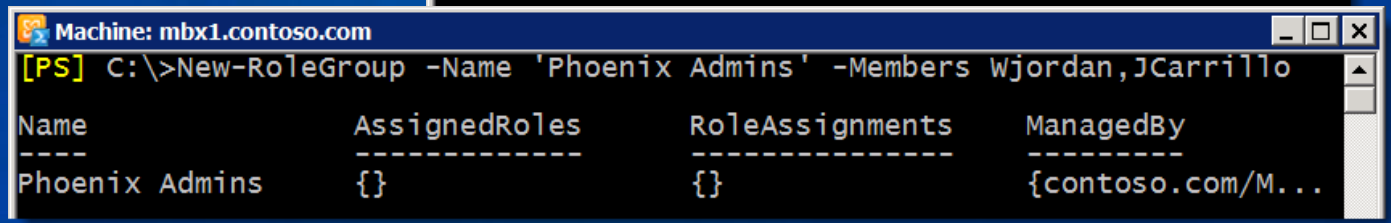
- Management Roles Defines the “What”
- Get-ManagementRole
- Get-ManagementRoleEntry
- Defines:
  - Cmdlets
  - Parameters



# The Who

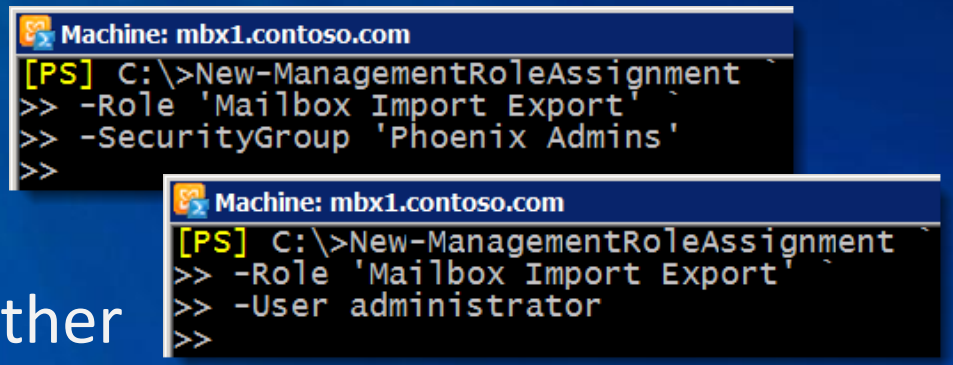
- Role Groups
- Active Directory Security Groups
- User Accounts



# The Glue

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

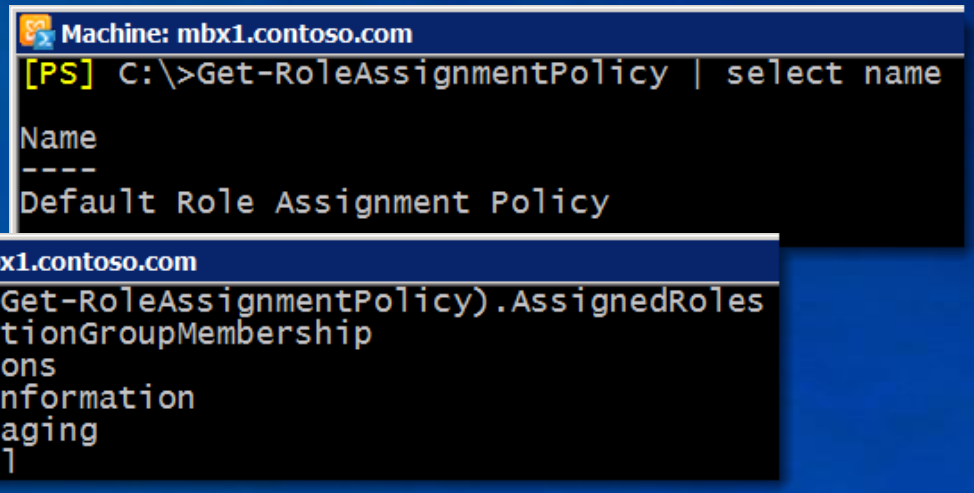


# Demo – RBAC for Administrators

- 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

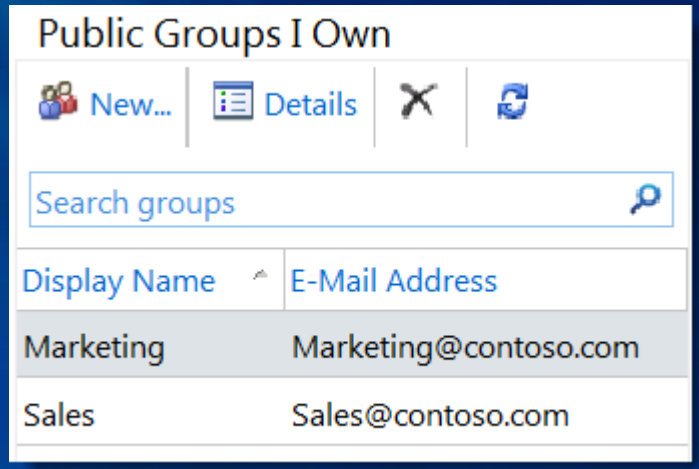


# Demo – RBAC for End-Users

- 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



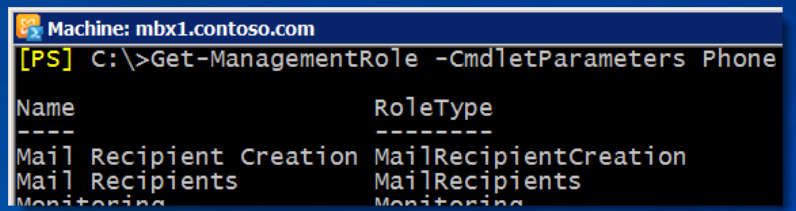
# Demo – RBAC for End-Users

- 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'
    }
```



# Thank You!

- Blog: www.mikepfeiffer.net
- E-Mail: mike.pfeiffer@interfacett.com
- Twitter: @mike_pfeiffer