MS-203
Interactive Guide Transcript:
Manage Role Groups in Exchange Online

Introduction

In this Interactive Guide, you will use the New Exchange Admin Center as well as Windows PowerShell to create a new Microsoft 365 management role group that will allow a service account to impersonate room resources without having the password.

What you will learn

After completing this lab, you will be able to:

- Create a new management scope using PowerShell
- Create a new Role Group using PowerShell
- Manage Role Group settings through the Exchange Online admin center

Task 1: Create a new management scope

When dealing with impersonation, it is best practice to create a management scope that limits access to a specified group of accounts. If you do not set a management scope, the role group will have access to all accounts in an organization. In this task we will create a new management scope with a Recipient restriction filter scoped to only mailboxes designated as a room resource type.

1. ☐ Type the following and hit Enter:
   ```
   Import-Module ExchangeOnlineManagement
   ```
2. ☐ Type the following and hit Enter:
   ```
   Connect-ExchangeOnline
   ```
3. ☐ Authenticate with your administrator credentials
   - Type admin@contoso.com and hit enter or select Next
   - Type Password and hit enter or select Next
4. ☐ To determine which mailboxes are designated as room resources, type the following and hit enter:
   ```
   Get-Mailbox | Where-Object {$_.ResourceType -eq "room"}
   ```
5. ☐ To create the new management scope, type the following and hit enter:
   ```
   New-ManagementScope "Room Resources" -RecipientRestrictionFilter
   "ResourceType -eq 'Room'"
   ```

6. ☐ To confirm the management scope was created successfully, type the following and hit enter:
```
Get-ManagementScope "Room Resources" | FL
```

Task 2: Create a new Role Group

A management role group is a universal security group used in the Role Based Access Control (RBAC) permissions model for Exchange Online. A management role group simplifies the assignment of management roles to a group of users. All members of a role group are assigned the same set of roles. After the role group is added, the members of the role group are granted the permissions provided by the roles assigned to the role group.

In this task, you are going to create a custom role group that will allow a service account to remotely access all room mailboxes within your organization. Then using the Exchange admin center, you will verify that the role was created successfully.

1. ☐ To create a new role group, type the following and hit enter:
```
New-RoleGroup -Name "Application Impersonation" -Roles
"ApplicationImpersonation","Mail Recipients","UserApplication" -Members
"ServiceAccount" -CustomRecipientWriteScope "Room Resources"
```
2. ☐ Select the Edge icon in the Windows taskbar to switch to the Microsoft 365 admin center in Microsoft Edge
3. ☐ Select Exchange in the left-hand navigation pane to open the Exchange admin center in a new tab.
4. ☐ In the Exchange admin center tab, in the left-hand navigation pane select Roles.
5. ☐ In the expanded group select admin roles.
6. ☐ In Admin roles window that is displayed, select the Role group you created at the beginning of this task.
7. ☐ In the Application Impersonation pane that appears, verify that the Write scope is set to "Room Resources" and then select the Assigned tab.
8. ☐ In the Assigned window, verify that the user "Service Account" has been assigned to the role and then select the permissions tab.
9. ☐ In the Permissions window, scroll down to verify that "ApplicationImpersonation" has been checked.