Securing Identities

Lab: Implementing custom Role Based Access Control (RBAC) roles

Scenario

Adatum Corporation wants to implement custom RBAC roles to delegate permissions to start and stop (deallocate) Azure VMs.

Objectives

After completing this lab, you will be able to:

- Define a custom RBAC role
- Assign a custom RBAC role

Lab Setup

Estimated Time: 30 minutes

User Name: **Student**

Password: **Pa55w.rd**

Exercise 1: Define a custom RBAC role

The main tasks for this exercise are as follows:

1. Deploy an Azure VM by using an Azure Resource Manager template
2. Identify actions to delegate via RBAC
3. Create a custom RBAC role in an Azure AD tenant

Task 1: Deploy an Azure VM by using an Azure Resource Manager template

1. From the lab virtual machine, start Microsoft Edge and browse to the Azure portal at **http://portal.azure.com** and sign in by using the Microsoft account that has the Owner role in the target Azure subscription.
2. In the Azure portal, in the Microsoft Edge window, start a **PowerShell** session within the **Cloud Shell**.
3. If you are presented with the **You have no storage mounted** message, configure storage using the following settings:
    - Subsciption: the name of the target Azure subscription
    - Cloud Shell region: the name of the Azure region that is available in your subscription and which is closest to the lab location
    - Resource group: the name of a new resource group **az3000900-LabRG**
    - Storage account: a name of a new storage account
    - File share: a name of a new file share
4. From the Cloud Shell pane, create a resource groups by running (replace the `<Azure region>` placeholder with the name of the Azure region that is available in your subscription and which is closest to the lab location)

```
New-AzResourceGroup -Name az3000901-LabRG -Location <Azure region>
```

5. From the Cloud Shell pane, upload the Azure Resource Manager template **\allfiles\AZ-300T03\Module_04\azuredeploy09.json** into the home directory.
6. From the Cloud Shell pane, upload the parameter file **\allfiles\AZ-300T03\Module_04\azuredeploy09.parameters.json** into the home directory.
7. From the Cloud Shell pane, deploy an Azure VM hosting Ubuntu by running:

```
New-AzResourceGroupDeployment -ResourceGroupName az3000901-LabRG -
TemplateFile $home/azuredeploy09.json -TemplateParameterFile $home/
azuredeploy09.parameters.json
```

> Note: Do not wait for the deployment to complete but instead proceed to the next task.

1. In the Azure portal, close the Cloud Shell pane.

Task 2: Identify actions to delegate via RBAC

1. In the Azure portal, navigate to the **az3000901-LabRG** blade.
2. On the **az3000901-LabRG** blade, click **Access Control (IAM)**.
3. On the **az3000901-LabRG - Access Control (IAM)** blade, click **Roles**.
4. On the **Roles** blade, click **Owner**.
5. On the **Owner** blade, click **Permissions**.
6. On the **Permissions (preview)** blade, click **Microsoft Compute**.
7. On the **Microsoft Compute** blade, click **Virtual machines**.
8. On the **Virtual Machines** blade, review the list of management actions that can be delegated through RBAC. Note that they include the **Deallocate Virtual Machine** and **Start Virtual Machine** actions.

Task 3: Create a custom RBAC role in an Azure AD tenant

1. On the lab computer, open the file **\allfiles\AZ-300T03\Module_04\customRoleDefinition09.json** and review its content:

```
{
   "Name": "Virtual Machine Operator (Custom)",
   "Id": null,
   "IsCustom": true,
   "Description": "Allows to start and stop (deallocate) Azure VMs",
   "Actions": [
         "Microsoft.Compute/*/read",
         "Microsoft.Compute/virtualMachines/deallocate/action",
         "Microsoft.Compute/virtualMachines/start/action"
   ],
   "NotActions": [
   ],
   "AssignableScopes": [
         "/subscriptions/SUBSCRIPTION_ID"
   ]
```

```
}
```

2. In the Azure portal, in the Microsoft Edge window, start a **PowerShell** session within the **Cloud Shell**.
3. From the Cloud Shell pane, upload the Azure Resource Manager template **\allfiles\AZ-300T03\Module_04\customRoleDefinition09.json** into the home directory.
4. From the Cloud Shell pane, run the following to replace the **$SUBSCRIPTION_ID** placeholder with the ID value of the Azure subscription:

```
$subscription_id = (Get-AzContext).Subscription.id

(Get-Content -Path $HOME/customRoleDefinition09.json) -Replace
'SUBSCRIPTION_ID', "$subscription_id" | Set-Content -Path $HOME/
customRoleDefinition09.json
```

5. From the Cloud Shell pane, run the following to create the custom role definition:

```
New-AzRoleDefinition -InputFile $HOME/customRoleDefinition09.json
```

6. From the Cloud Shell pane, run the following to verify that the role was created successfully:

```
Get-AzRoleDefinition -Name 'Virtual Machine Operator (Custom)'
```

7. Close the Cloud Shell pane.

> Result: After you completed this exercise, you have defined a custom RBAC role

Exercise 2: Assign and test a custom RBAC role

The main tasks for this exercise are as follows:

1. Create an Azure AD user
2. Create an RBAC role assignment
3. Test the RBAC role assignment

Task 1: Create an Azure AD user

1. In the Azure portal, in the Microsoft Edge window, start a **PowerShell** session within the **Cloud Shell**.
2. From the Cloud Shell pane, run the following to explicitly authenticate to the target Azure AD tenant:

```
Connect-AzureAD
```

3. From the Cloud Shell pane, run the following to identify the Azure AD DNS domain name:

```
$domainName = ((Get-AzureAdTenantDetail).VerifiedDomains)[0].Name
```

4. From the Cloud Shell pane, run the following to create a new Azure AD user:

```
$passwordProfile = New-Object -TypeName
Microsoft.Open.AzureAD.Model.PasswordProfile

$passwordProfile.Password = 'Pa55w.rd1234'

$passwordProfile.ForceChangePasswordNextLogin = $false

New-AzureADUser -AccountEnabled $true -DisplayName 'lab user0901' -
PasswordProfile $passwordProfile -MailNickName 'labuser0901' -
UserPrincipalName "labuser0901@$domainName"
```

5. From the Cloud Shell pane, run the following to identify the user principal name of the newly created Azure AD

user:

```
(Get-AzureADUser -Filter "MailNickName eq 'labuser0901'").UserPrincipalName
```

6. Close the Cloud Shell pane.

Task 2: Create an RBAC role assignment

1. In the Azure portal, navigate to the **az3000901-LabRG** blade.
2. On the **az3000901-LabRG** blade, click **Access Control (IAM)**.
3. On the **az3000901-LabRG - Access Control (IAM)** blade, click **+ Add** and select the **Add role assignment** option.
4. On the **Add role assignment** blade, specify the following settings and click **Save**:
   - Role: **Virtual Machine Operator (Custom)**
   - Assign access to: **Azure AD user, group, or service principal**
   - Select: **lab user0901**

Task 3: Test the RBAC role assignment

1. Start a new in-private Microsoft Edge window, browse to the Azure portal at **http://portal.azure.com** and sign in by using the newly created user account:
   - Username: the user principal name you identified in the first task of this exercise
   - Password: **Pa55w.rd1234**
2. In the Azure portal, navigate to the **Resource groups** blade. Note that you are not able to see any resource groups.
3. In the Azure portal, navigate to the **All resources** blade. Note that you are able to see only the **az3000901-vm** and its managed disk.
4. In the Azure portal, navigate to the **az3000901-vm** blade. Try restarting the virtual machine. Review the error message in the notification area and note that this action failed because the current user is not authorized to carry it out.
5. Stop the virtual machine and verify that the action completed successfully.

> Result: After you completed this exercise, you have assigned and tested a custom RBAC role

Exercise 3: Remove lab resources

Task 1: Open Cloud Shell

1. At the top of the portal, click the **Cloud Shell** icon to open the Cloud Shell pane.
2. If needed, switch to the Bash shell session by using the drop down list in the upper left corner of the Cloud Shell pane.
3. At the **Cloud Shell** command prompt, type in the following command and press **Enter** to list all resource groups you created in this lab:

```
az group list --query "[?starts_with(name,'az30009')]".name --output tsv
```

4. Verify that the output contains only the resource groups you created in this lab. These groups will be deleted in the next task.

Task 2: Delete resource groups

1. At the **Cloud Shell** command prompt, type in the following command and press **Enter** to delete the resource groups you created in this lab

```
az group list --query "[?starts_with(name,'az30009')]".name --output tsv |
xargs -L1 bash -c 'az group delete --name $0 --no-wait --yes'
```

2. Close the **Cloud Shell** prompt at the bottom of the portal.

> Result: In this exercise, you removed the resources used in this lab.