Module 10 - Lab 1: Managing Azure Role-Based Access Control

Scenario

Adatum Corporation wants to test delegation of Azure management by using Role-Based Access Control

After completing this lab, you will be able to:

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

Exercise 1: Define a custom RBAC role

The main tasks for this exercise are as follows:

1. Identify actions to delegate via RBAC
2. Create a custom RBAC role in an Azure AD tenant

Task 1: Identify actions to delegate via RBAC

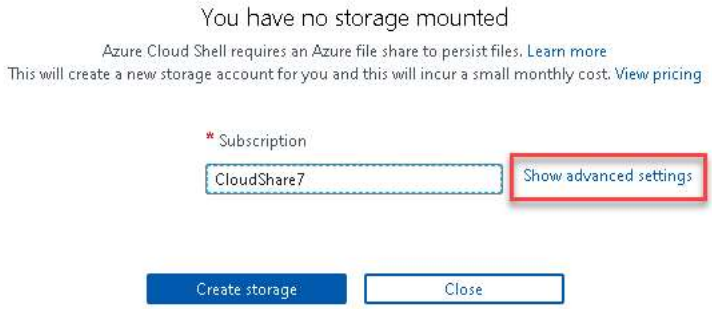
- [ ] 1. Navigate to portal.azure.com and sign in using email sheikhnasirTMGFA@gdcs4.com and password mEscx3ac4uTwEdlq.
- [ ] 2. In the Azure portal, navigate to the **az30311a-OQWFC7TGAW** blade.
- [ ] 3. On the **az30311a-OQWFC7TGAW** blade, select **Access Control (IAM)**.
- [ ] 4. On the **az30311a-OQWFC7TGAW - Access Control (IAM)** blade, select **Roles**.
- [ ] 5. On the **Roles** blade, select **View** Next to **Owner**.
- [ ] 6. On the **Owner** blade, select **Permissions**.
- [ ] 7. On the **Permissions (preview)** blade, select **Microsoft Compute**.
- [ ] 8. On the **Microsoft Compute** blade, select **Virtual machines**.
- [ ] 9. On the **Virtual Machines** blade, review the list of management actions that have been delegated to you as part of the lab provisioning.

Task 2: Create a custom RBAC role in an Azure AD tenant

- [ ] 1. On the lab computer, open Notepad and paste the following JSON file.

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

- [ ] 2. Save the file as roledefinition30310.json ensuring you select **All Files (.)** from the **Save as type** drop down menu.
- [ ] 3. Exit **Notepad**.
- [ ] 4. On the lab computer, in the browser window displaying the Azure portal, start a **PowerShell** session within the **Cloud Shell**.
- [ ] 5. Click **Show advanced settings**.



- [ ] 6. Select the **East US** region. Select **Use existing** Resource group and select the pre-provisioned resource group for the lab.

- [ ] 7. Enter a name for the storage account (this must be unique) and type **clouldshell** as the name of the File share then click **Create Storage.**

Your Cloud Shell will now launch.

- [ ] 8. From the Cloud Shell pane, upload the Azure Resource Manager template **roledefinition30310.json** into the home directory.
- [ ] 9. 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 $HOME/roledefinition30310.json) -Replace 'SUBSCRIPTION_ID', "$subscription_id" | Set-Content -Path $HOME/roledefinit
```

- [ ] 10. From the Cloud Shell pane, run the following to verify that the SUBSCRIPTION_ID placeholder was replaced with the ID value of the Azure subscription:

```
Get-Content -Path $HOME/roledefinition30310.json
```

- [ ] 11. From the Cloud Shell pane, run the following to create the custom role definition:

```
New-AzRoleDefinition -InputFile $HOME/roledefinition30310.json
```

> ⚠ **Note:** The command above will fail due to permissions. This is a limitation of the Cloud Share platform and is expected.

Exercise 2: Assign and test a RBAC role

The main tasks for this exercise are as follows:

1. Create an RBAC role assignment
2. Test the RBAC role assignment

Task 1: Create an RBAC role assignment

- [ ] 1. In the Azure portal, navigate to the **az30311a-OQWFC7TGAW** blade.
- [ ] 2. On the **az30311a-OQWFC7TGAW** blade, select **Access Control (IAM)**.
- [ ] 3. On the **az30311a-OQWFC7TGAW - Access Control (IAM)** blade, select **+ Add** and select the **Add role assignment** option.
- [ ] 4. On the **Add role assignment** blade, specify the following settings (leave others with their existing values) and select **Save**:

Setting	Value
Role	**Virtual Machine Contributor**
Assign access to	**Azure AD user, group, or service principal**
Select	**your second user on the Home tab of the lab environment**

Task 2: Test the RBAC role assignment

- [ ] 1. From the lab computer, start a new in-private web browser session, navigate to the Azure portal, **https://portal.azure.com** and sign in by using the **your second user on the Home tab of the lab environment**.
- [ ] 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 **az30310a-vm0** and its managed disk.

> ⚠ **Note**: It may take some time for the new role to apply. Log out and back into the Azure Portal if necessary.

- [ ] 4. Restart the virtual machine and verify that the action completed successfully.
- [ ] 5. Close the in-private web browser session.
