

# **Microsoft ADC Cybersecurity Skilling Program**

## **Week 5 Lab Assignment**

**Student Name:** Vincent Onchieku Collins

**Student ID:** ADC-CSS02-25052

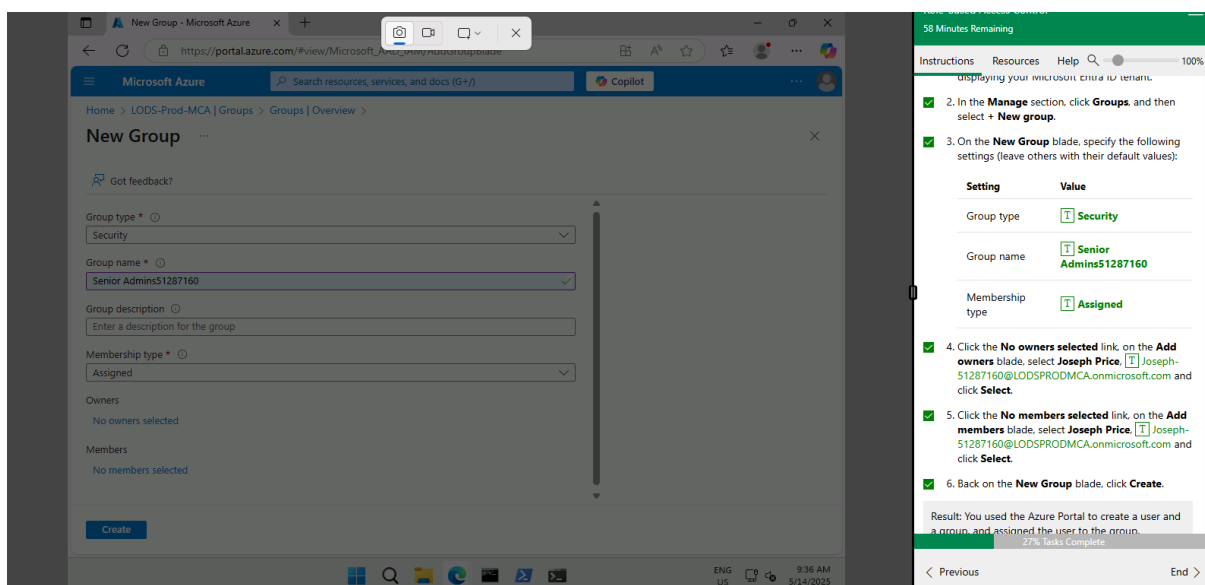
## Introduction

In this lab, I completed several exercises focused on role-based access control (RBAC) in Azure. The labs you need to complete will include:

1. Create a Senior Admins group containing the user account of Joseph Price as its member.
2. Create a Junior Admins group containing the user account of Isabel Garcia as its member.
3. Create a Service Desk group containing the user account of Dylan Williams as its member.
4. Assign the Virtual Machine Contributor role to the Service Desk group.

### Exercise 1: Create the Senior Admins group with the user account Joseph Price as its member.

The first exercise involved creating a Senior Admins group and adding a user account for Joseph Price. I began by logging into the Azure portal and creating a user account for Joseph. Once the user was created, I proceeded to create a security group called "Senior Admins" and assigned Joseph Price as both the owner and member of the group. This step demonstrated how to create user accounts and assign them to specific groups in the Azure portal.



Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Add owners

Try changing or adding filters if you don't see what you're looking for.

Search

Joseph-51

2 results found

All

Users

Enterprise applications

	Name	Type	Details
<input checked="" type="checkbox"/>	Joseph-51287160	User	Joseph-51287160@LODSPRODMCA.onmicrosoft.com
<input type="checkbox"/>	Joseph-51284815	User	Joseph-51284815@LODSPRODMCA.onmicrosoft.com

Select

Command Prompt

Role-based Access Control

1 Hr 3 Min Remaining

InstructionsResourcesHelp100%

Membership type

Assigned

4. Click the **No owners selected** link, on the **Add owners** blade, select **Joseph Price**, **Joseph-51287160@LODSPRODMCA.onmicrosoft.com** and click **Select**.

5. Click the **No members selected** link, on the **Add members** blade, select **Joseph Price**, **Joseph-51287160@LODSPRODMCA.onmicrosoft.com** and click **Select**.

6. Back on the **New Group** blade, click **Create**.

Result: You used the Azure Portal to create a user and a group, and assigned the user to the group.

Exercise 2: Create a Junior Admins group containing the user account of Isabel Garcia as its member.

Estimated timing: 10 minutes

In this exercise, you will complete the following tasks:

- Task 1: Use PowerShell to create a user account for Isabel Garcia.

27% Tasks Complete

Previous

End

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Add members

Try changing or adding filters if you don't see what you're looking for.

Search

Joseph-51

2 results found

All

Users

Groups

Devices

Enterprise applications

	Name	Type	Details
<input checked="" type="checkbox"/>	Joseph-51287160	User	Joseph-51287160@LODSPRODMCA.onmicrosoft.com
<input type="checkbox"/>	Joseph-51284815	User	Joseph-51284815@LODSPRODMCA.onmicrosoft.com

Select

Role-based Access Control

1 Hr 1 Min Remaining

InstructionsResourcesHelp100%

1. In the Azure portal, navigate back to the blade displaying your Microsoft Entra ID tenant.

2. In the **Manage** section, click **Groups**, and then select **+ New group**.

3. On the **New Group** blade, specify the following settings (leave others with their default values):

Setting	Value
Group type	Security
Group name	Senior Admins51287160
Membership type	Assigned

4. Click the **No owners selected** link, on the **Add owners** blade, select **Joseph Price**, **Joseph-51287160@LODSPRODMCA.onmicrosoft.com** and click **Select**.

5. Click the **No members selected** link, on the **Add members** blade, select **Joseph Price**, **Joseph-51287160@LODSPRODMCA.onmicrosoft.com** and click **Select**.

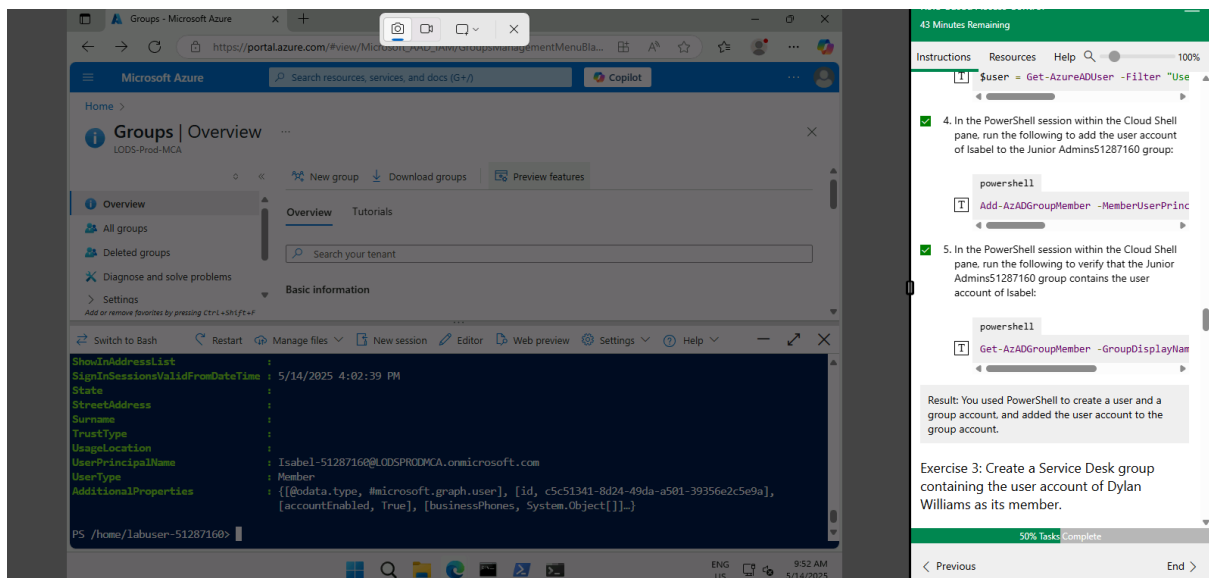
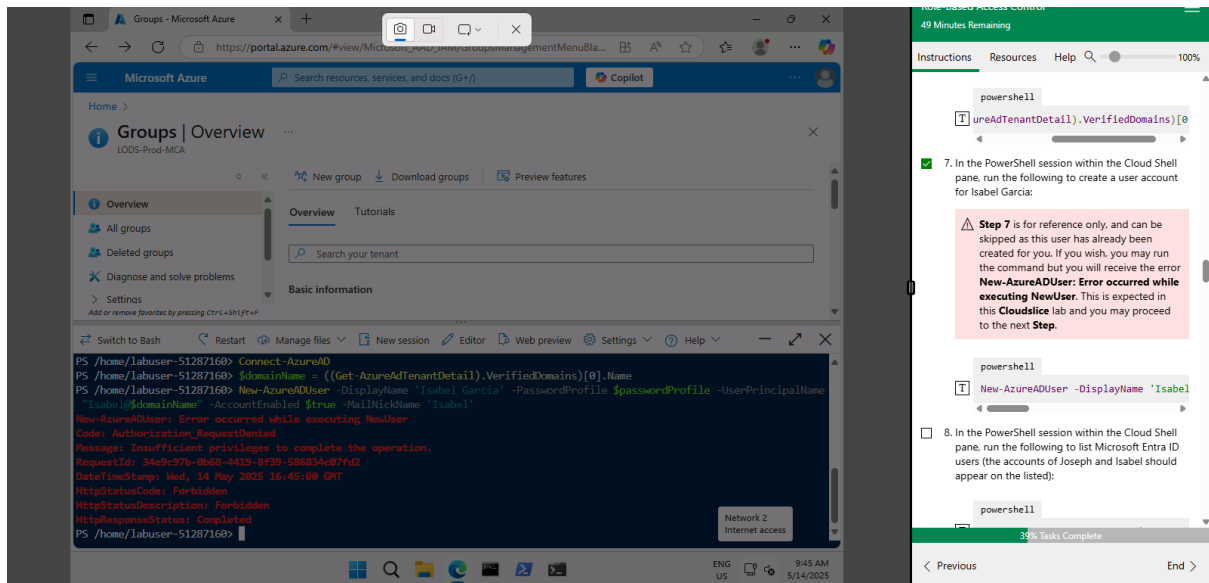
6. Back on the **New Group** blade, click **Create**.

27% Tasks Complete

Previous

End

The second exercise required me to use PowerShell to create a Junior Admins group containing the user account of Isabel Garcia. I first created a password profile for Isabel and connected to Microsoft Entra ID using PowerShell. After successfully creating the user account for Isabel, I used PowerShell commands to create a new security group named "Junior Admins" and added Isabel Garcia to the group. This exercise highlighted how to use PowerShell for user and group management, as well as adding users to security groups.



### Exercise 3: Create a Service Desk group containing the user account of Dylan Williams as its member.

For the third exercise, I used Azure CLI to create a Service Desk group containing the user account of Dylan Williams. I first created a user account for Dylan using Azure CLI, and then created a new security group called "Service Desk" using CLI commands. After creating the group, I added Dylan Williams to the Service Desk group. This exercise focused on leveraging Azure CLI for user and group management tasks.

The screenshot shows the Microsoft Azure portal interface on the left and a Cloud Shell session on the right. The Azure portal displays the 'Groups | Overview' page for the 'LODS-Prod-MCA' tenant. The Cloud Shell session shows the following commands and output:

```
cli
az ad user create --display-name "Dylan Williams" --password "Pa55w.rd1234" --user-principal-name Dylan@DOMAINNAME
cli
az ad user list --output table | grep S1287160
```

The output of the second command shows a table of user accounts, including Dylan Williams.

Task 2: Use Azure CLI to create the Service Desk group and add the user account of Dylan to the group.

In this task, you will create the Service Desk group and assign Dylan to the group.

1. In the same Bash session within the Cloud Shell pane, run the following to create a new security group named Service Desk.

The screenshot shows the Microsoft Azure portal interface on the left and a Cloud Shell session on the right. The Azure portal displays the 'Groups | Overview' page for the 'LODS-Prod-MCA' tenant. The Cloud Shell session shows the following commands and output:

```
cli
az ad group member list --group "Service Desk51291782"
```

The output of the command shows a table of group members, including Dylan Williams.

Exercise 4: Assign the Virtual Machine Contributor role to the Service Desk group.

Estimated timing: 10 minutes

In this exercise, you will complete the following tasks:

- Task 1: Create a resource group.
- Task 2: Assign the Service Desk Virtual Machine Contributor permissions to the resource group.

## Exercise 4: Assign the Virtual Machine Contributor role to the Service Desk group.

The final exercise involved assigning the Virtual Machine Contributor role to the Service Desk group. I first created a resource group named "AZ500Lab01" in the Azure portal. Once the resource group was created, I assigned the Virtual Machine Contributor role to the Service Desk group, granting them the necessary permissions to manage virtual machines within the resource group. This exercise demonstrated how to assign roles to groups in Azure, ensuring that users in the Service Desk group have the appropriate permissions for managing virtual machines.

The screenshot shows the Azure portal interface for creating a new resource group. The main pane displays the 'Create a resource group' form with the following details:

- Subscription: MOC Subscription-Iod5080608
- Resource group name: AZ500Lab01
- Region: (US) East US

The 'Review + create' button is visible at the bottom. On the right side, a task list is displayed under the heading '21 Minutes Remaining'.

**Task 2: Assign the Service Desk Virtual Machine Contributor permissions.**

1. On the **Resource groups** blade, refresh the page and verify your new resource group appears in the list of resource groups.
2. On the **AZ500Lab01** blade, click **Access control (IAM)** in the middle pane.
3. On the **AZ500Lab01 | Access control (IAM)** blade, click **+ Add** and then, in the drop-down menu, click **Add role assignment**.
4. On the **Add role assignment** blade, specify the following settings and click **Next** after each step:

74% Tasks Complete

The screenshot shows the Azure portal interface for adding a role assignment. The main pane displays the 'Add role assignment' form with the following details:

- Role: Virtual Machine Contributor
- Scope: /subscriptions/191502ca-fcd3-4ed2-bf58-78d41e4b6d73/resourceGroups/AZ500Lab01
- Members: Service Desk51291782
- Description: No description
- Assignment type: Active
- Assignment duration: Permanent

The 'Review + assign' button is visible at the bottom. On the right side, a task list is displayed under the heading '15 Minutes Remaining'.

**Task 2: Assign the Service Desk Virtual Machine Contributor permissions.**

5. Click **Review + assign** twice to create the role assignment.
6. From the **Access control (IAM)** blade, select **Check access**.
7. On the **AZ500Lab01 | Access control (IAM)** blade, on the **Check access** tab, in the **Search by name or email address** text box, check access for **[Dylan-51291782@LODSPRODMCA.onmicrosoft.com]**.
8. In the list of search results, select the user account of Dylan Williams and, on the **Dylan Williams assignments - AZ500Lab01** blade, view the newly created assignment.
9. Close the **Dylan Williams assignments - AZ500Lab01** blade.
10. Repeat the same last two steps to check access for **[Joseph-51291782@LODSPRODMCA.onmicrosoft.com]**.

Result: You have assigned and checked RBAC permissions.

84% Tasks Complete

The screenshot displays the Microsoft Azure portal interface. The main content area shows the 'Dylan-51291782 assignments - AZ500Lab01' page. The left sidebar contains navigation links for 'Home', 'Resource group', 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Resource visualizer', 'Events', 'Settings', 'Cost Management', 'Monitoring', 'Automation', and 'Help'. The main content area is divided into 'Current role assignments' and 'Eligible assignments'. The 'Current role assignments' section shows a table with columns: Role, Description, Scope, Group assignment, and Condition. The table lists two roles: 'LOD Reader' and 'Virtual Machine Contrib'. The 'Eligible assignments' section shows a search bar and a list of deny assignments. The right sidebar contains a checklist of steps for creating and checking role assignments, with a progress bar indicating 91% completion.

Role	Description	Scope	Group assignment	Condition
LOD Reader	View all resources, but does not ...	Subscription (inherited)	--	None
Virtual Machine Contrib	Lets you manage virtual machine...	This resource	Service Desk51291782	None

## Conclusion

The Week 5 lab assignment allows you to practice the core concepts of RBAC by guiding you through the creation of users and groups, followed by role assignment across different Azure interfaces—Azure portal, PowerShell, and Azure CLI. This hands-on experience is crucial for understanding how access management works in Azure and how to apply security principles effectively. By completing this lab, you will gain practical skills in managing user permissions and roles in a cloud environment.