Microsoft ADC Cybersecurity Skilling Program

Week 5 Lab Assignment

Student Name: Vincent Onchieku Collins

Student ID: ADC-CSS02-25052

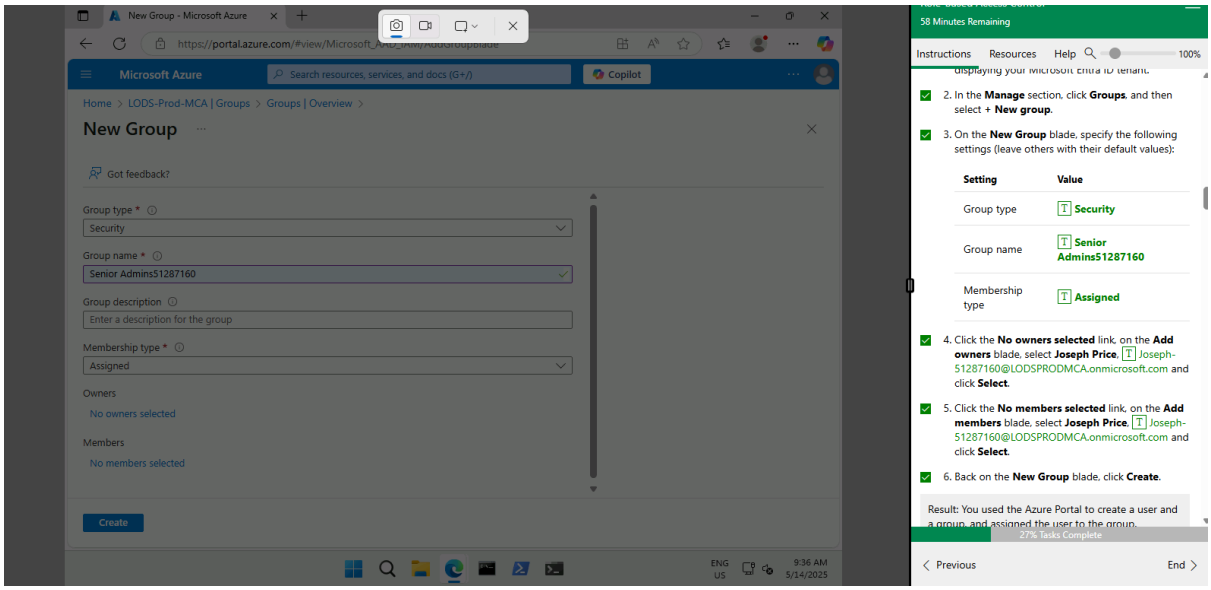
Introduction

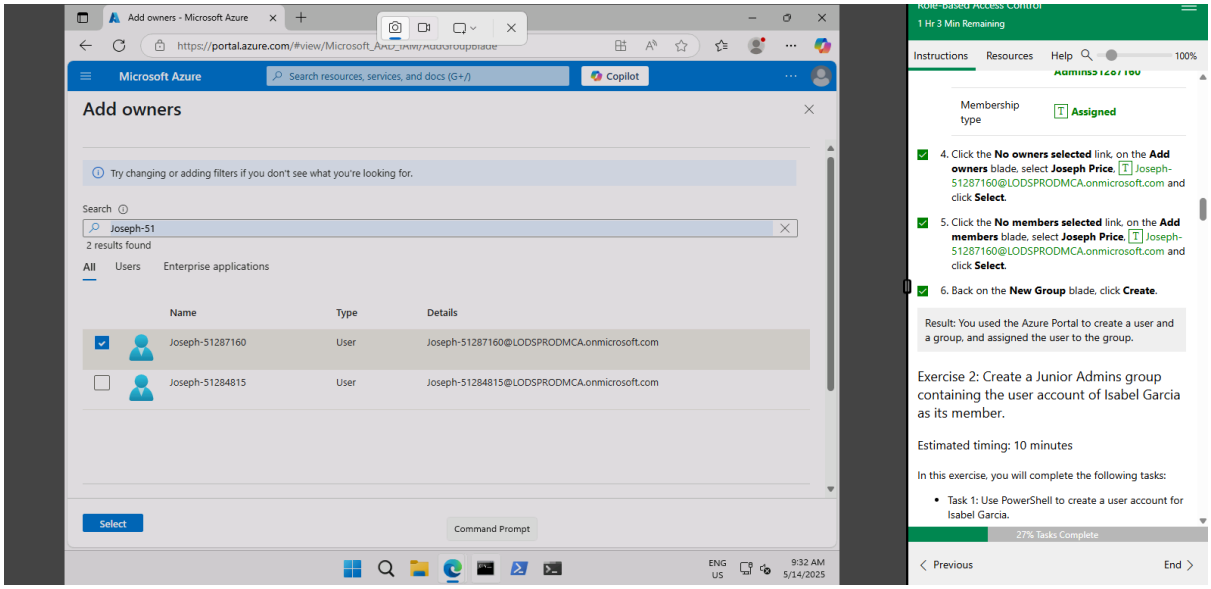
In this lab, I completed several exercises focused on role-based access control (RBAC) in Azure. The labs you need to complete will include:

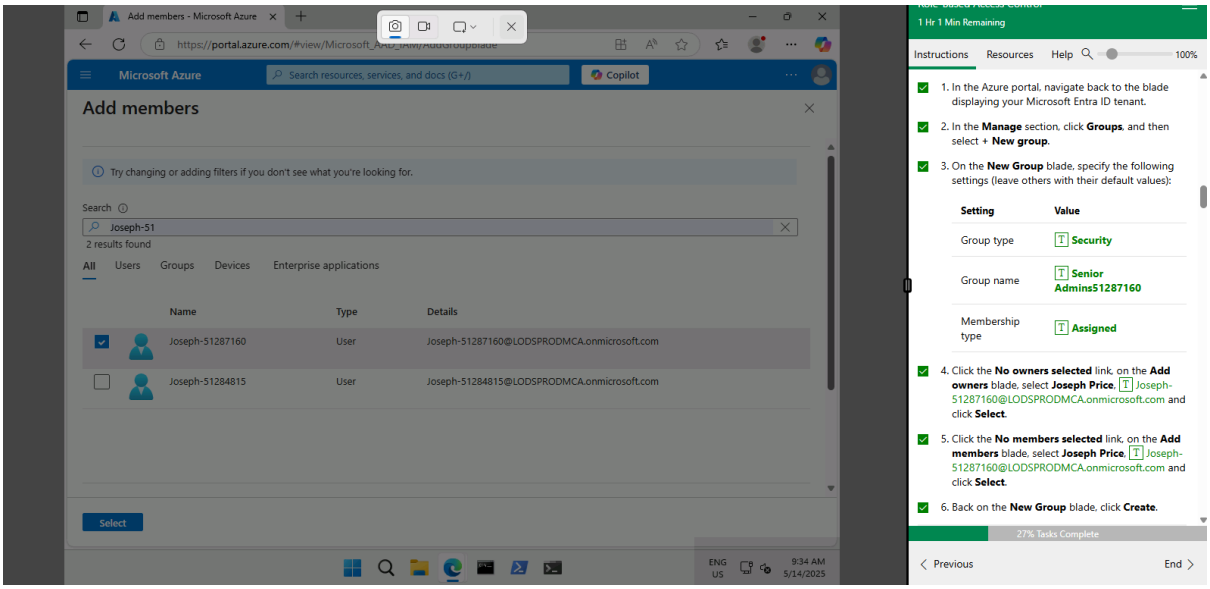
1. Create a Senior Admins group containing the user account of Joseph Price as its member.
2. Create a Junior Admins group containing the user account of Isabel Garcia as its member.
3. Create a Service Desk group containing the user account of Dylan Williams as its member.
4. Assign the Virtual Machine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

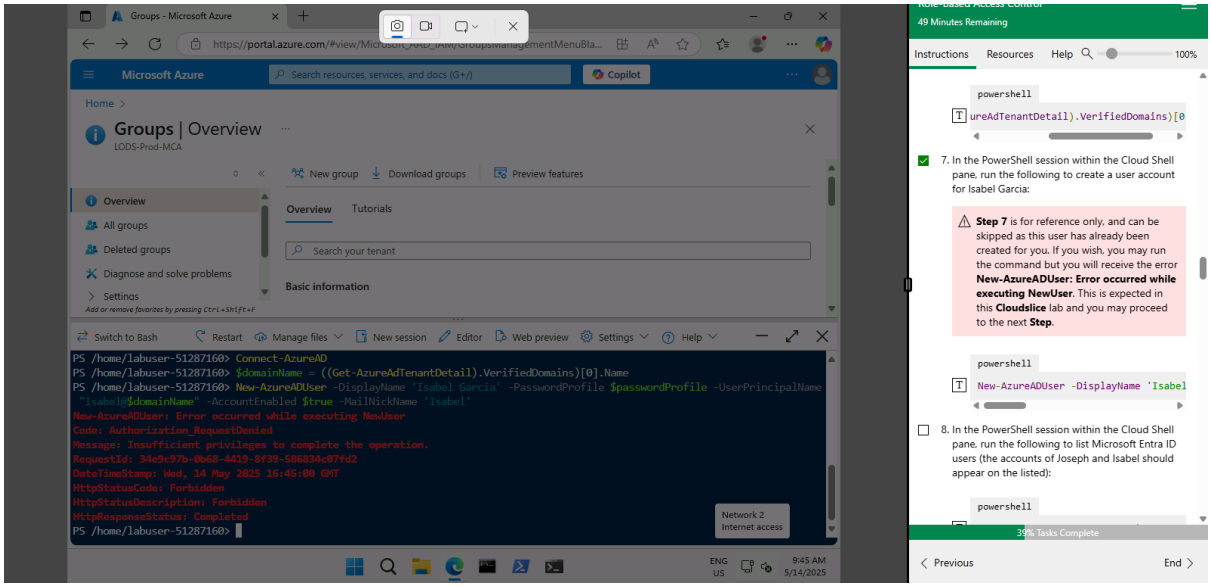


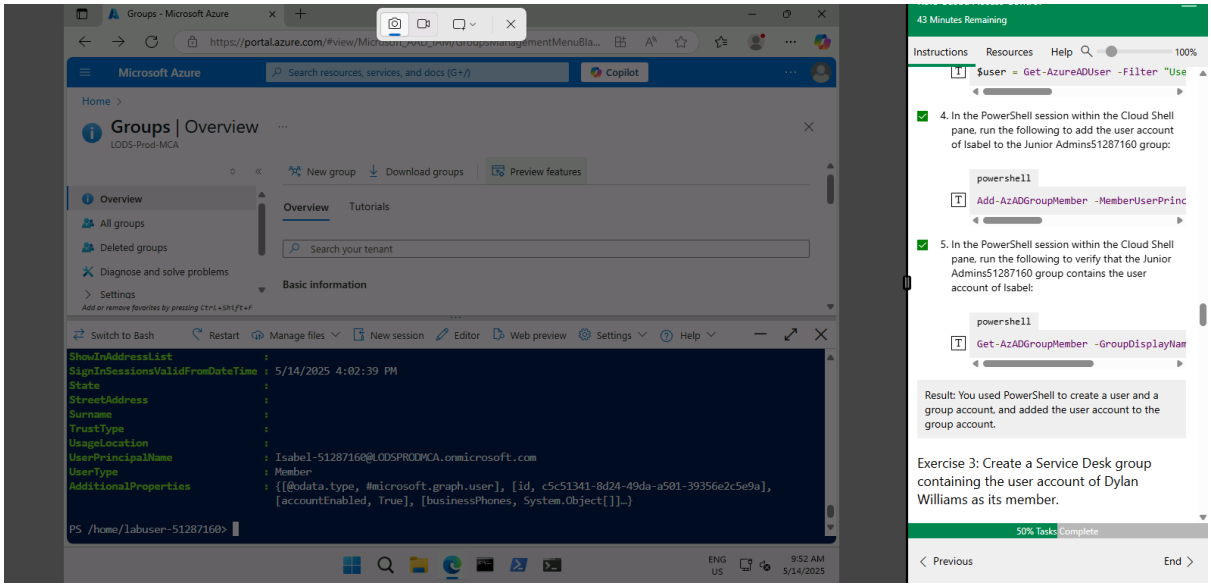

Add owners - Microsoft Azure
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Add owners
Try changing or adding filters if you don't see what you're looking for.
Search
Joseph-51
2 results found
All
Users
Enterprise applications
Name
Type
Details
Joseph-51287160
User
Joseph-51287160@LODSPRODMCA.onmicrosoft.com
Joseph-51284815
User
Joseph-51284815@LODSPRODMCA.onmicrosoft.com
Select
Command Prompt
1 Hr 3 Min Remaining
Instructions
Resources
Help
100%
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


Add members - Microsoft Azure
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
Joseph-51287160
User
Joseph-51287160@LODSPRODMCA.onmicrosoft.com
Joseph-51284815
User
Joseph-51284815@LODSPRODMCA.onmicrosoft.com
Select
1 Hr 1 Min Remaining
Instructions
Resources
Help
100%
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

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

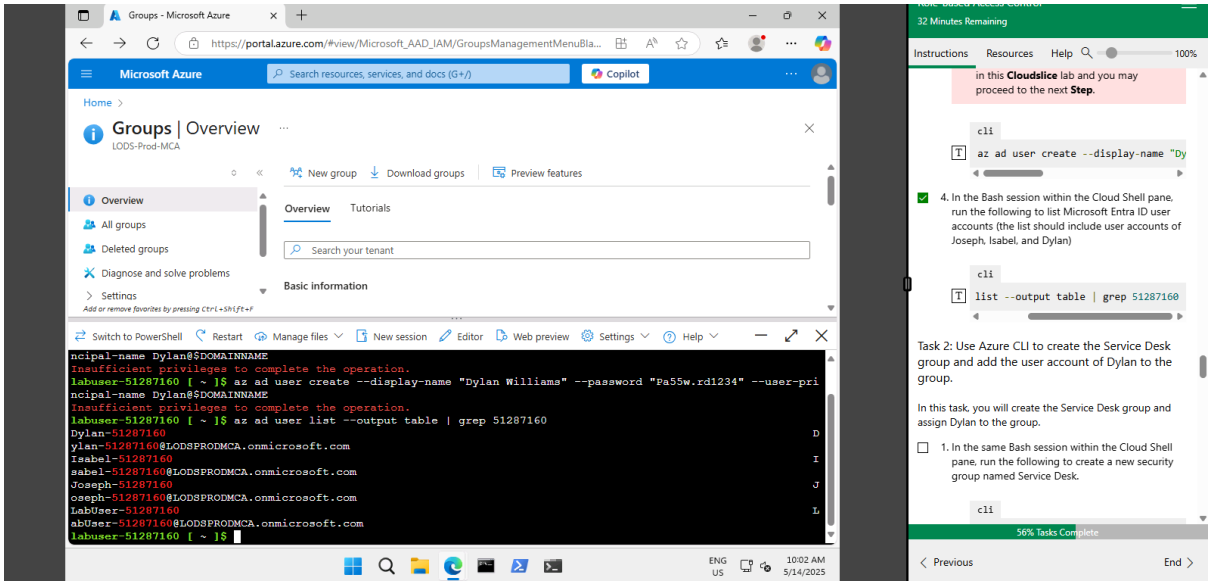
The second exercise required me to use PowerShell to create a Junior Admins group containing the user account of Isabel Garcia. I first created a password profile for Isabel and connected to Microsoft Entra ID using PowerShell. After successfully creating the user account for Isabel, I used PowerShell 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.

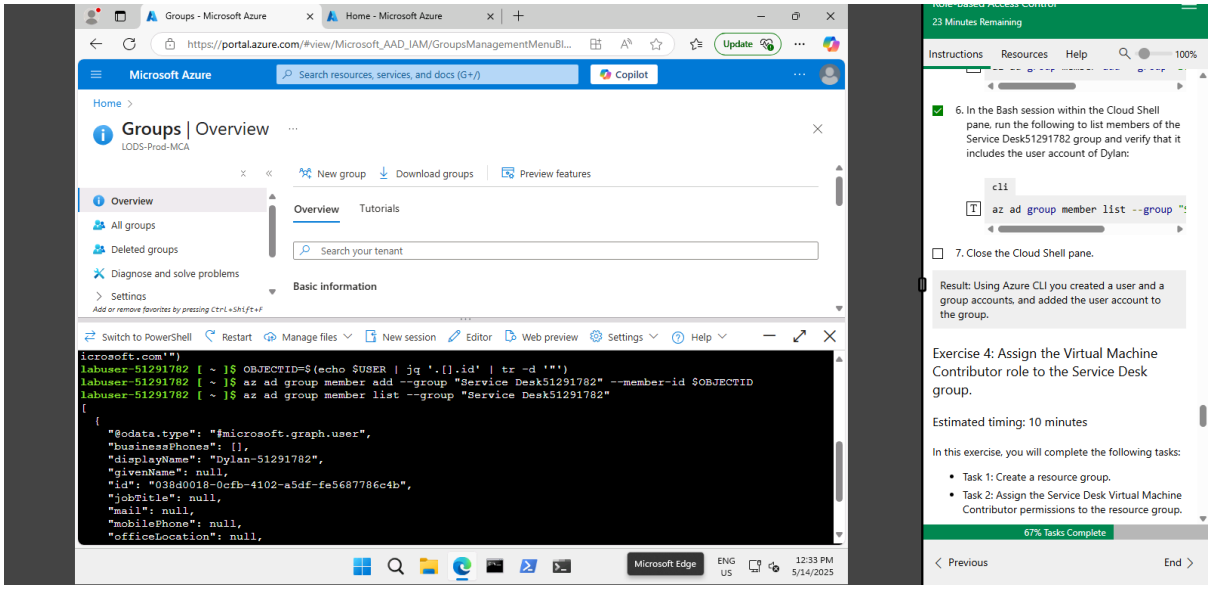




Exercise 3: Create a Service Desk group containing the user account of Dylan Williams as its member.

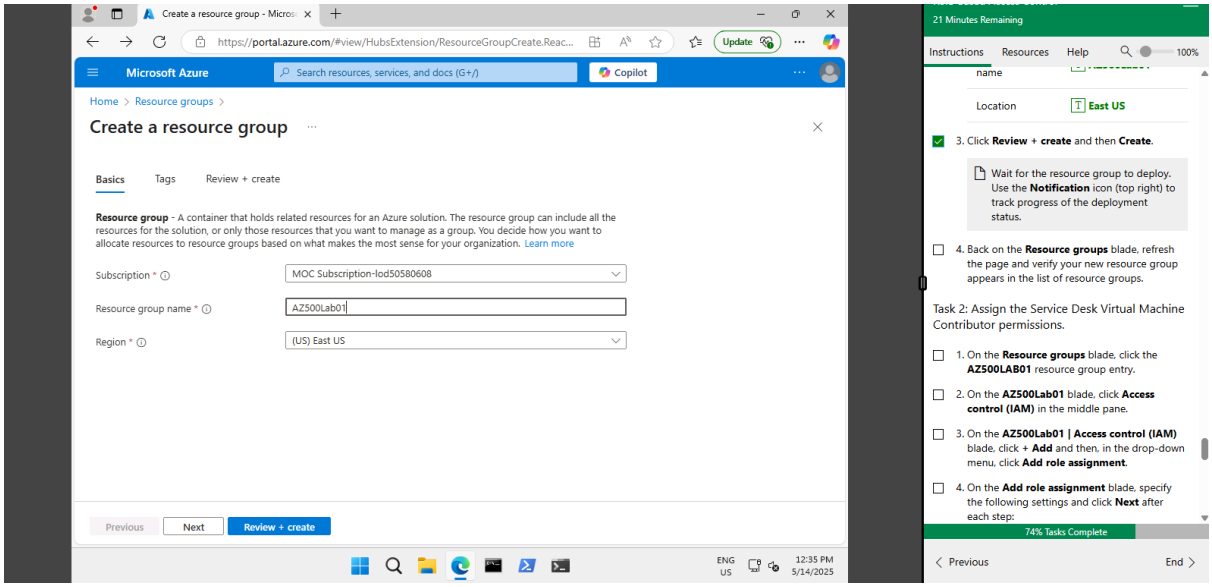
For the third exercise, I used Azure CLI to create a Service Desk group containing the user account of Dylan Williams. I first created a user account for Dylan using Azure CLI, and then created a new security group called "Service Desk" using CLI commands. After creating the group, I added Dylan Williams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

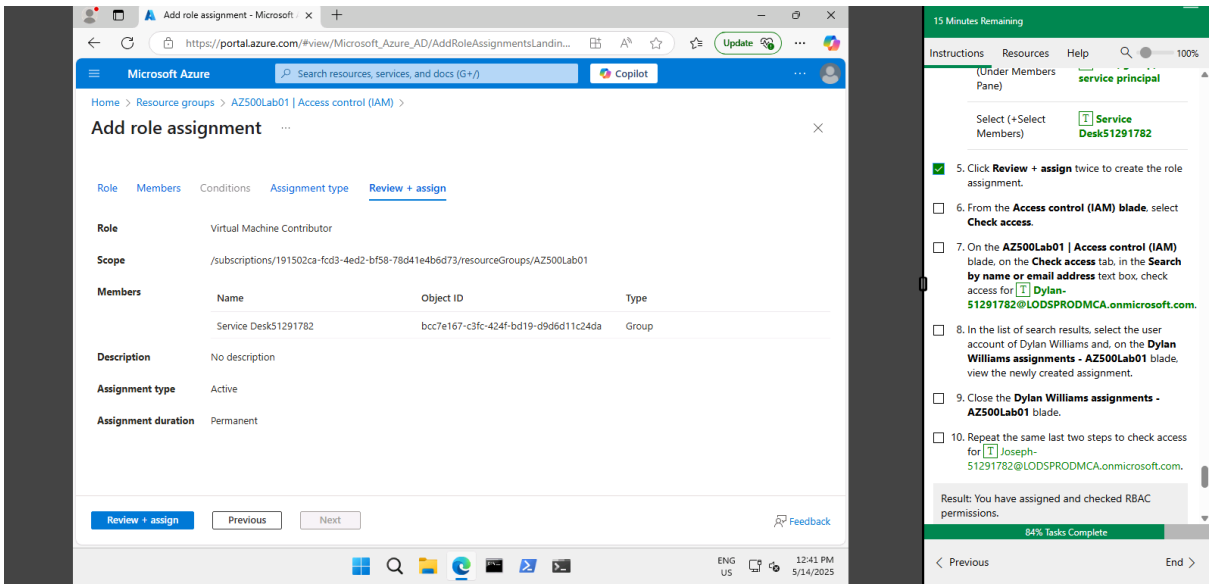


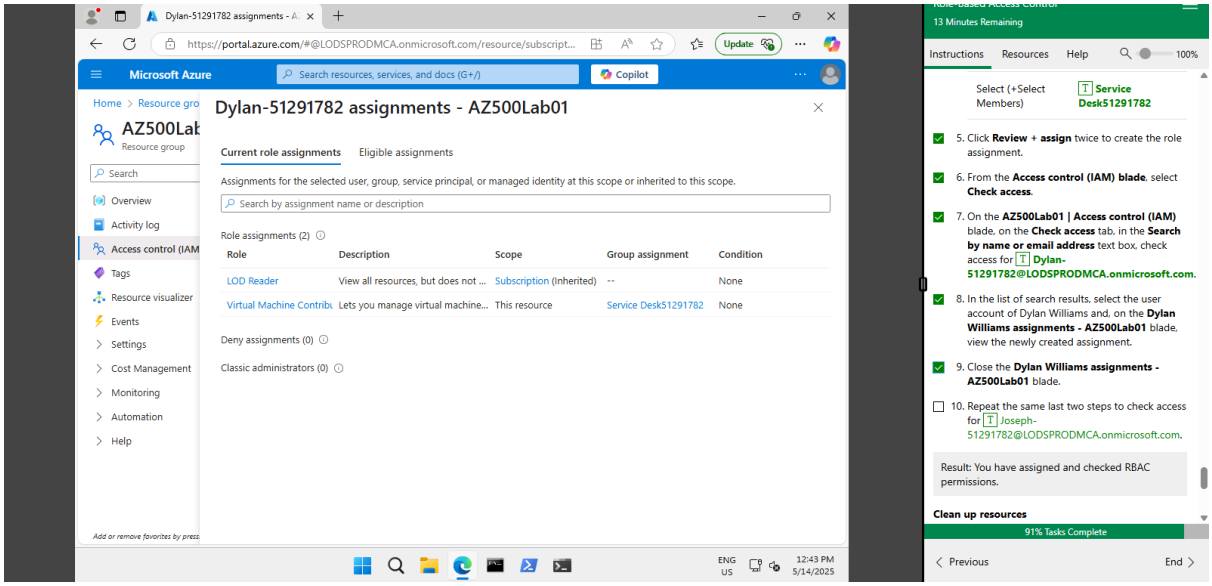


Exercise 4: Assign the Virtual Machine Contributor role to the Service Desk group.

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.







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.