NAME: BINYANYA DEBORAH NYATICHI

CS NO: ADC-CSS02-25051.

DESCRIPTION: Week 5: Secure Identity and Access

ASSIGNMENT: Assignment 9: Lab - Role-Based Access Control

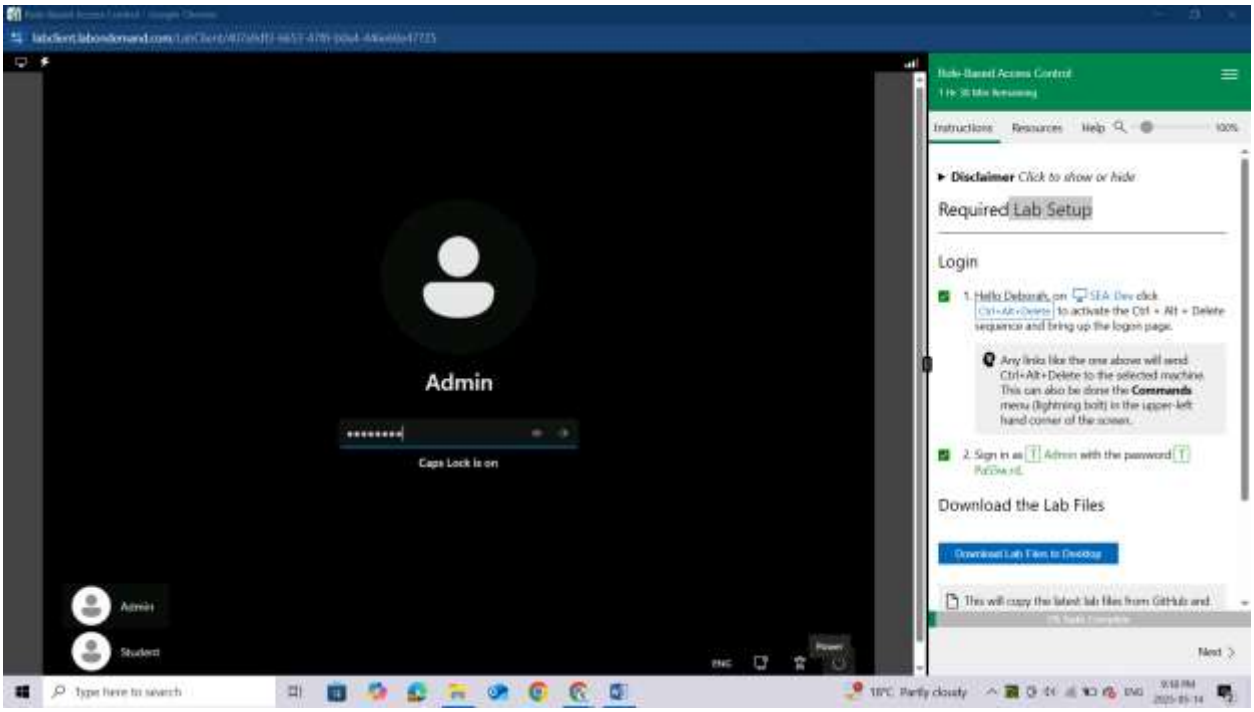
DATE: 14/05/2025

INTRODUCTION

In this lab, I will be working on implementing Role-Based Access Control (RBAC) in a cloud environment to enhance security and streamline user permissions. Specifically, I will create three separate security groups—Senior Admins, Junior Admins, and Service Desk—each containing a designated user: Joseph Price, Isabel Garcia, and Dylan Williams, respectively. After establishing the groups and assigning the correct users, I will apply the Virtual Machine Contributor role to the Service Desk group. This exercise aims to demonstrate how to manage access control effectively by granting the right level of permissions to users based on their roles within an organization.

ROLE-BASED ACCESS CONTROL

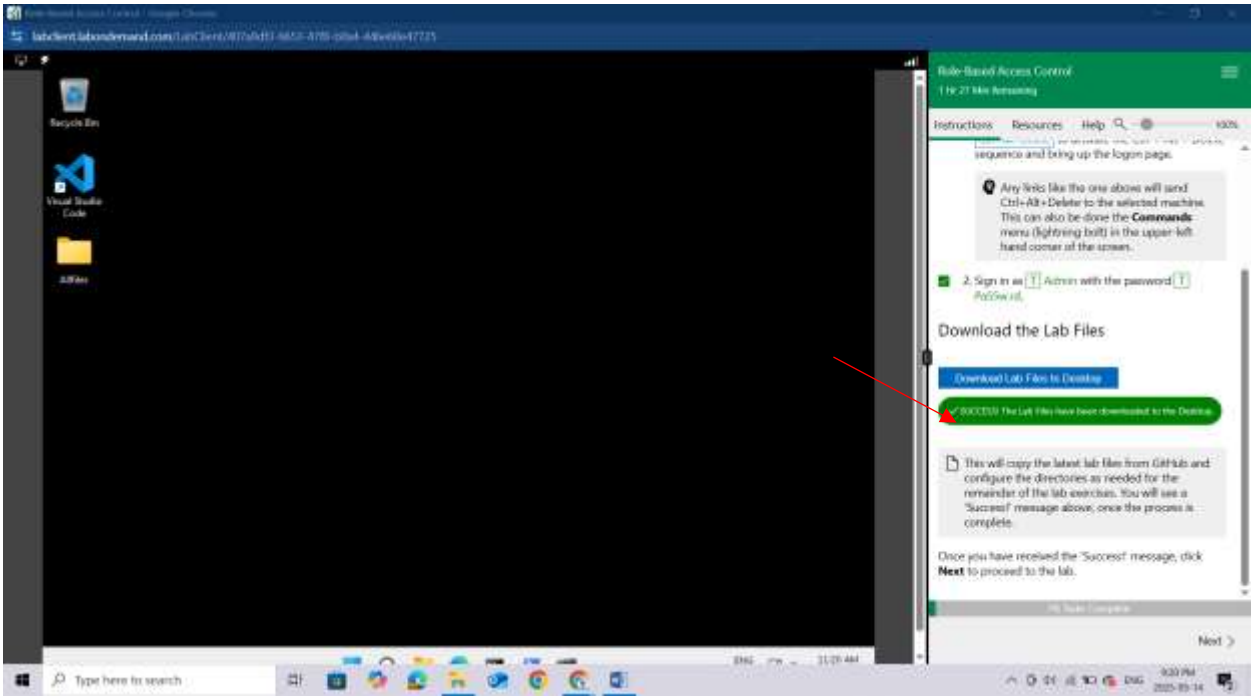
Lab Setup



Download the Lab Files

Download the files from the link provided in the lab setup

After successful download you will see a green bar of "***SUCCESS! The Lab Files have been downloaded to the Desktop.***"



Lab 01: Role-Based Access Control

Lab scenario

You have been asked to create a proof of concept showing how Azure users and groups are created. Also, how role-based access control is used to assign roles to groups. Specifically, you need to:

Create a Senior Admins group containing the user account of Joseph Price as its member.

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

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

Assign the Virtual Machine Contributor role to the Service Desk group.

Lab objectives

In this lab, you will complete the following exercises:

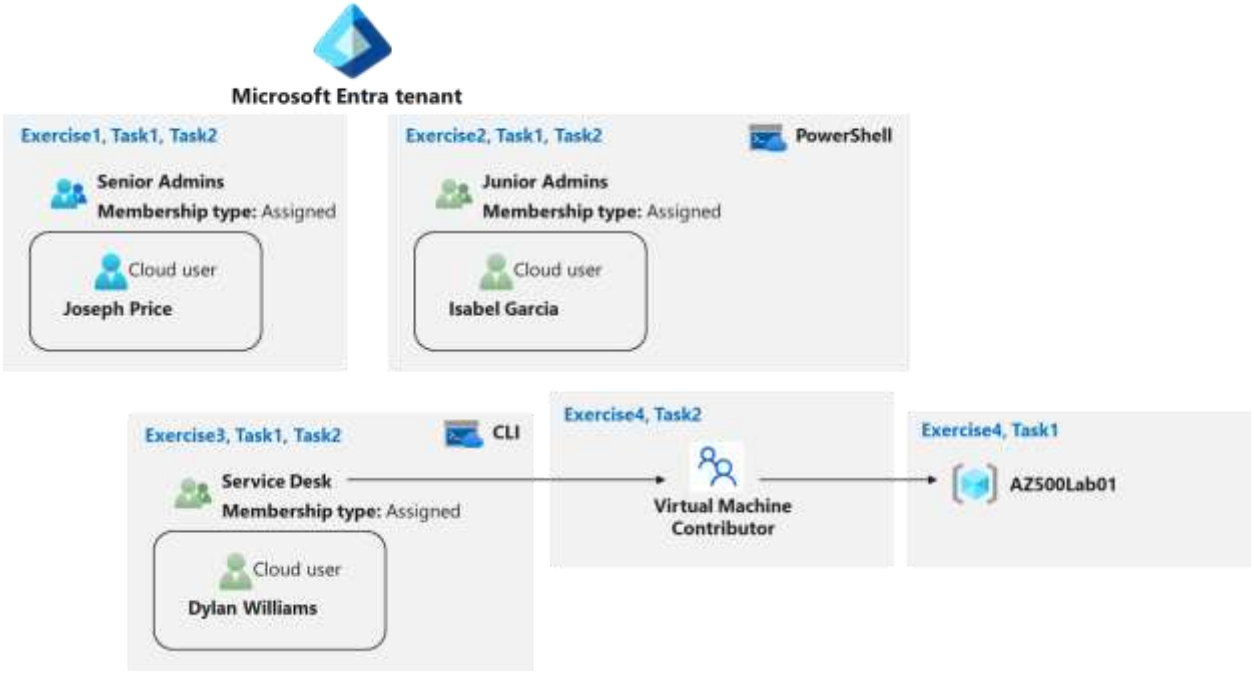
Exercise 1: Create the Senior Admins group with the user account Joseph Price as its member (the Azure portal).

Exercise 2: Create the Junior Admins group with the user account Isabel Garcia as its member (PowerShell).

Exercise 3: Create the Service Desk group with the user Dylan Williams as its member (Azure CLI).

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

Role-Based Access Control architecture diagram



Instructions

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

In this exercise, you will complete the following tasks:

Task 1: Use the Azure portal to create a user account for Joseph Price.

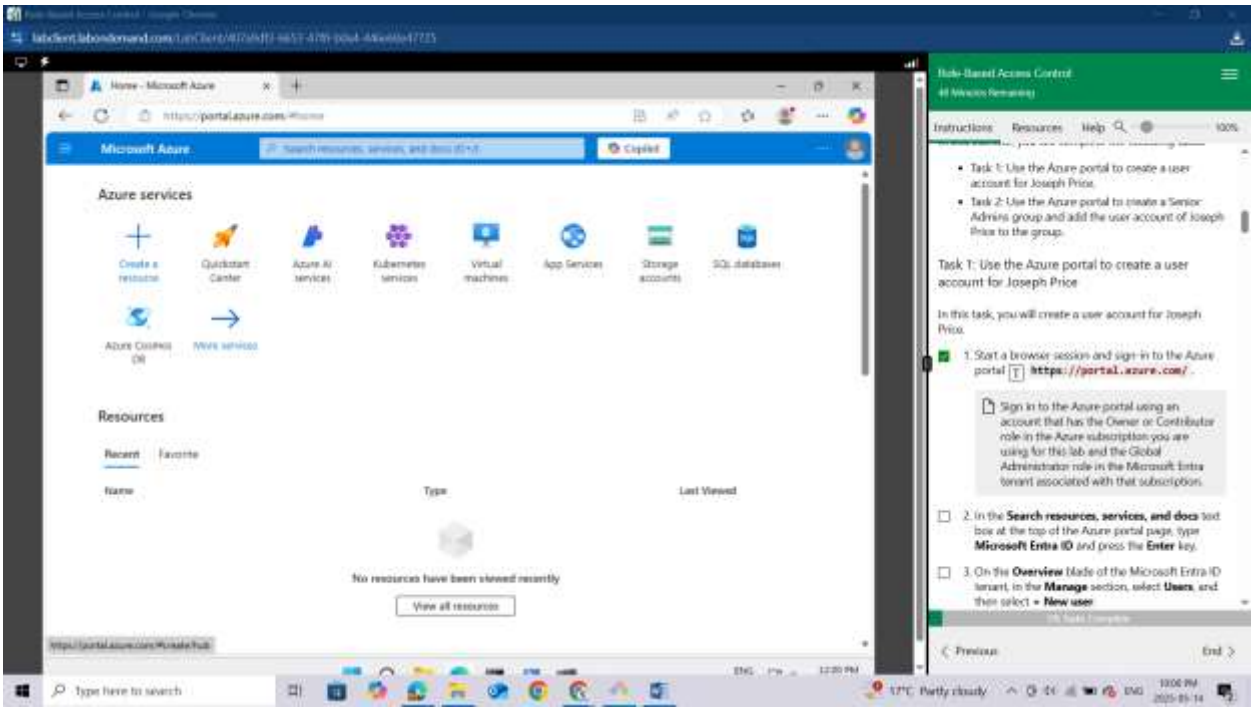
Task 2: Use the Azure portal to create a Senior Admins group and add the user account of Joseph Price to the group.

Task 1: Use the Azure portal to create a user account for Joseph Price

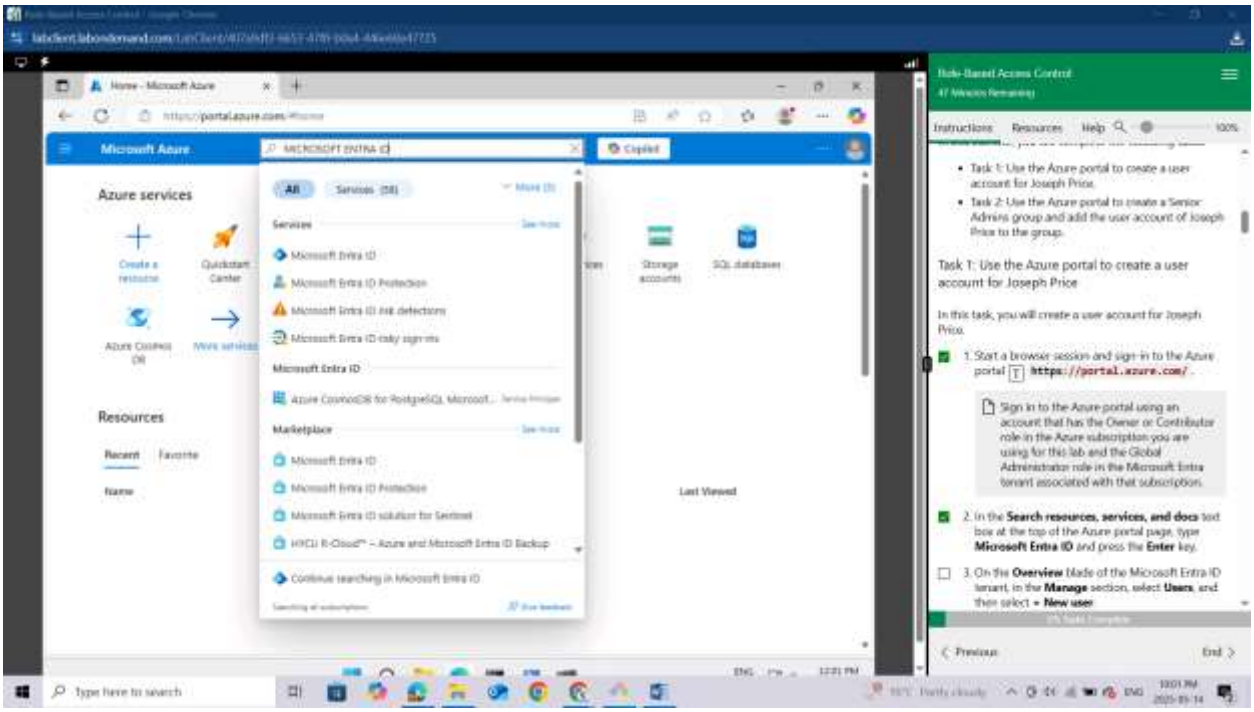
In this task, you will create a user account for Joseph Price.

Start a browser session and **sign-in** to the Azure portal https://portal.azure.com/.

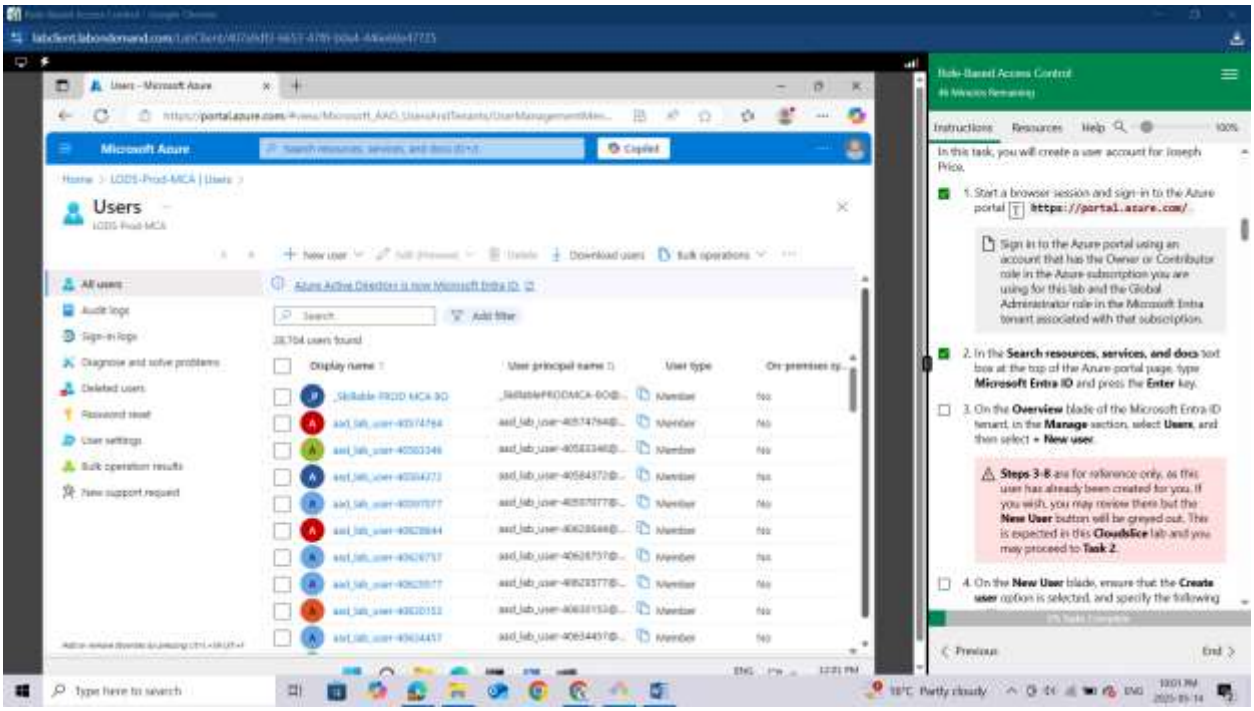
Sign in to the Azure portal using an account that has the Owner or Contributor role in the Azure subscription you are using for this lab and the Global Administrator role in the Microsoft Entra tenant associated with that subscription.



In the Search resources, services, and docs text box at the top of the Azure portal page, type **Microsoft Entra ID** and press the **Enter key.**



On the Overview blade of the Microsoft Entra ID tenant, in the **Manage** section, **select Users**, and then select **+ New user**.



Steps 3-8 are for reference only, as this user has already been created for you. If you wish, you may review them but the New User button will be greyed out. This is expected in this Cloudslice lab and you may proceed to Task 2.

On the New User blade, ensure that the Create user option is selected, and specify the following settings:

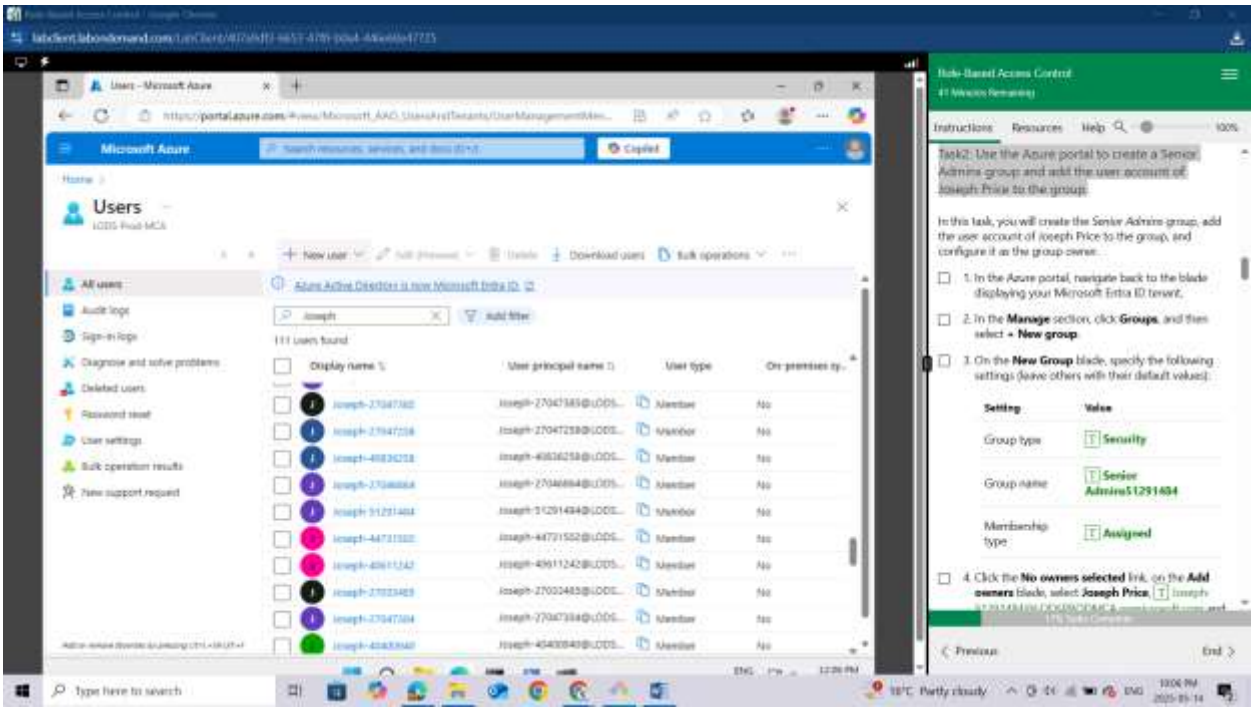
Setting	**Value**
User name	Joseph
Name	Joseph Price

Click on the copy icon next to the User name to copy the full user.

Ensure that the Auto-generate password is selected, select the Show password checkbox to identify the automatically generated password. You would need to provide this password, along with the user name to Joseph.

Click **Create**.

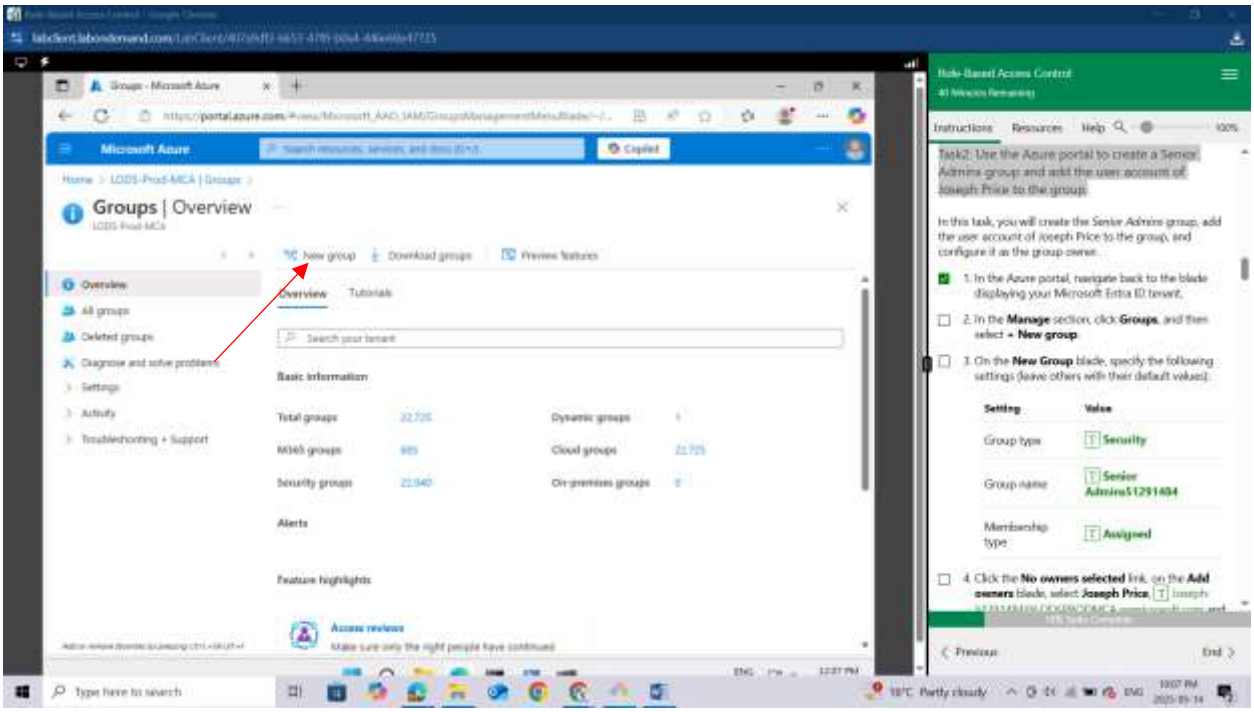
Refresh the **Users | All users** blade to verify the new user was created in your Microsoft Entra tenant.



Task2: Use the Azure portal to create a Senior Admins group and add the user account of Joseph Price to the group.

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

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



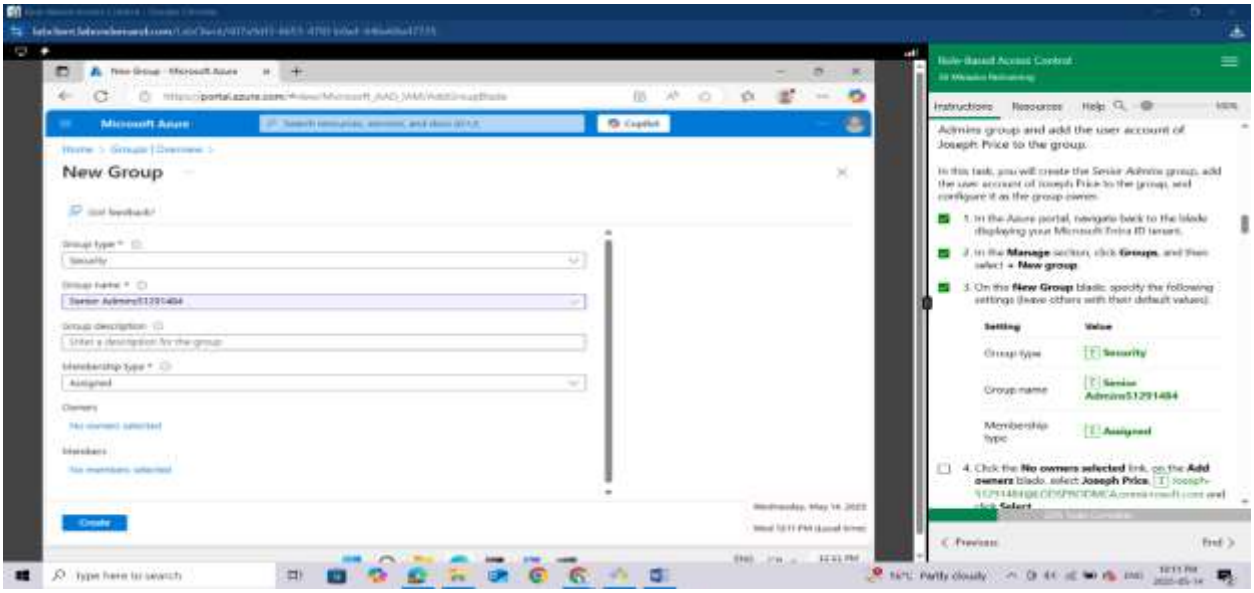
On the New Group blade, specify the following settings (leave others with their default values):

Setting Value

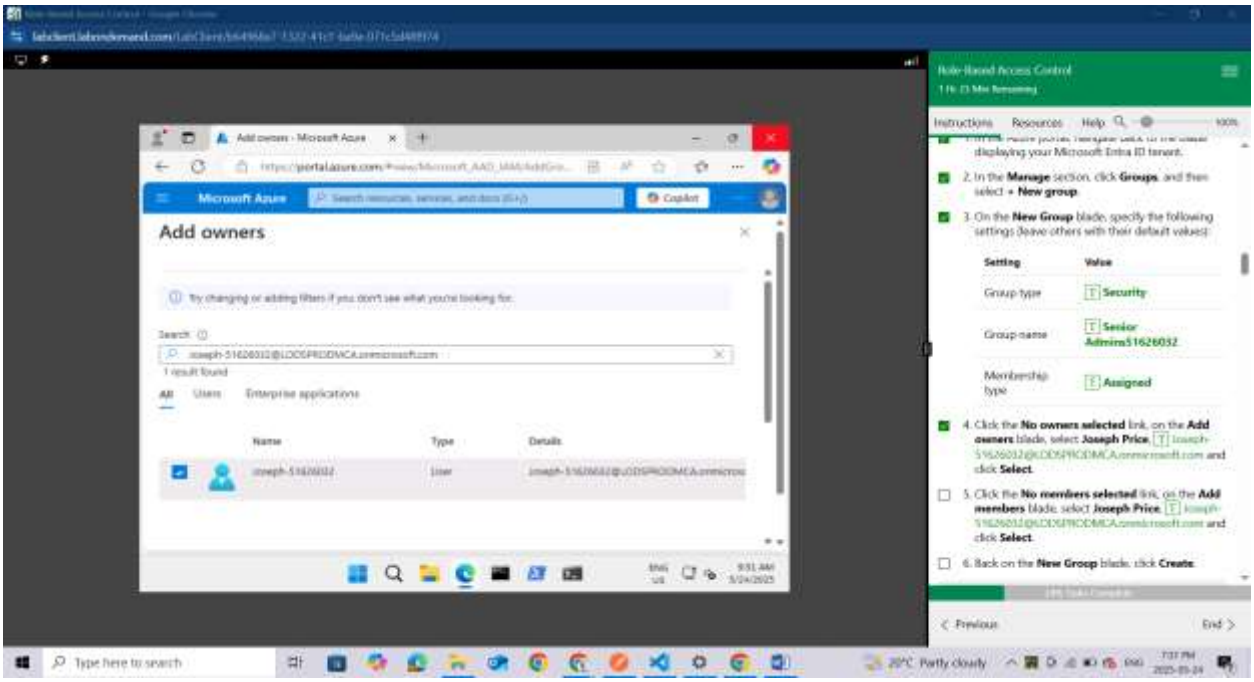
Group type Security

Group name Senior Admins51291484

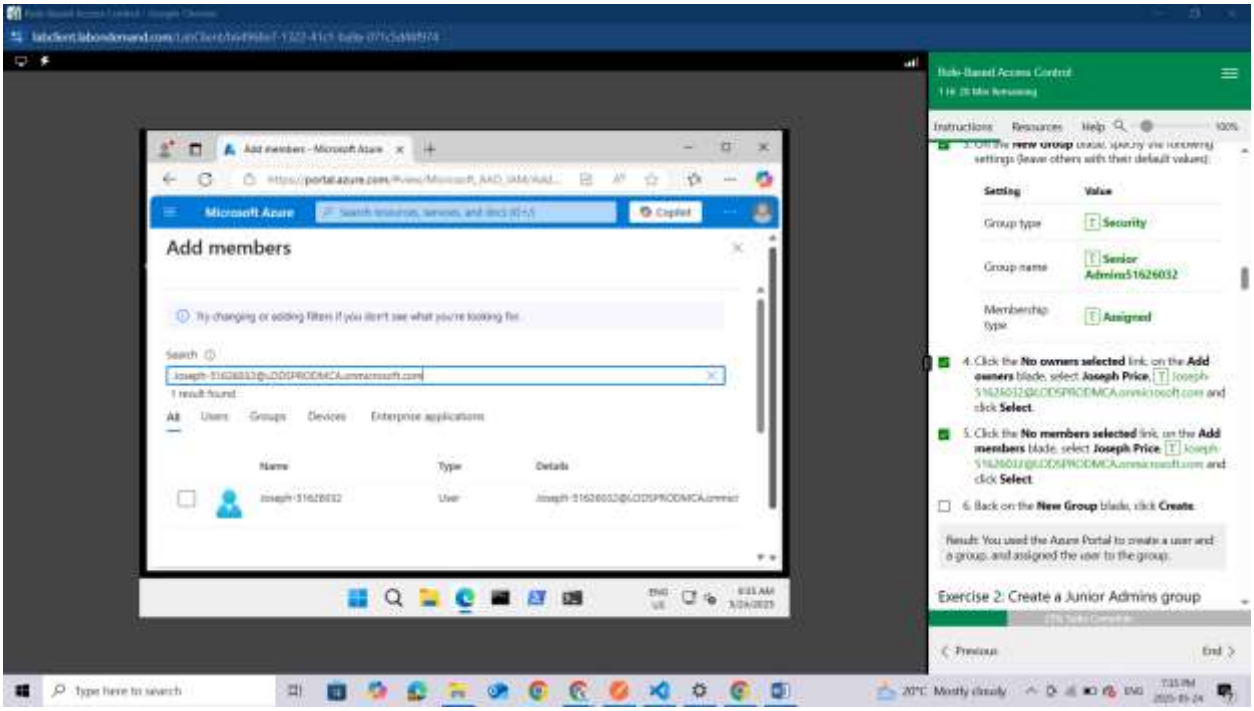
Membership type Assigned



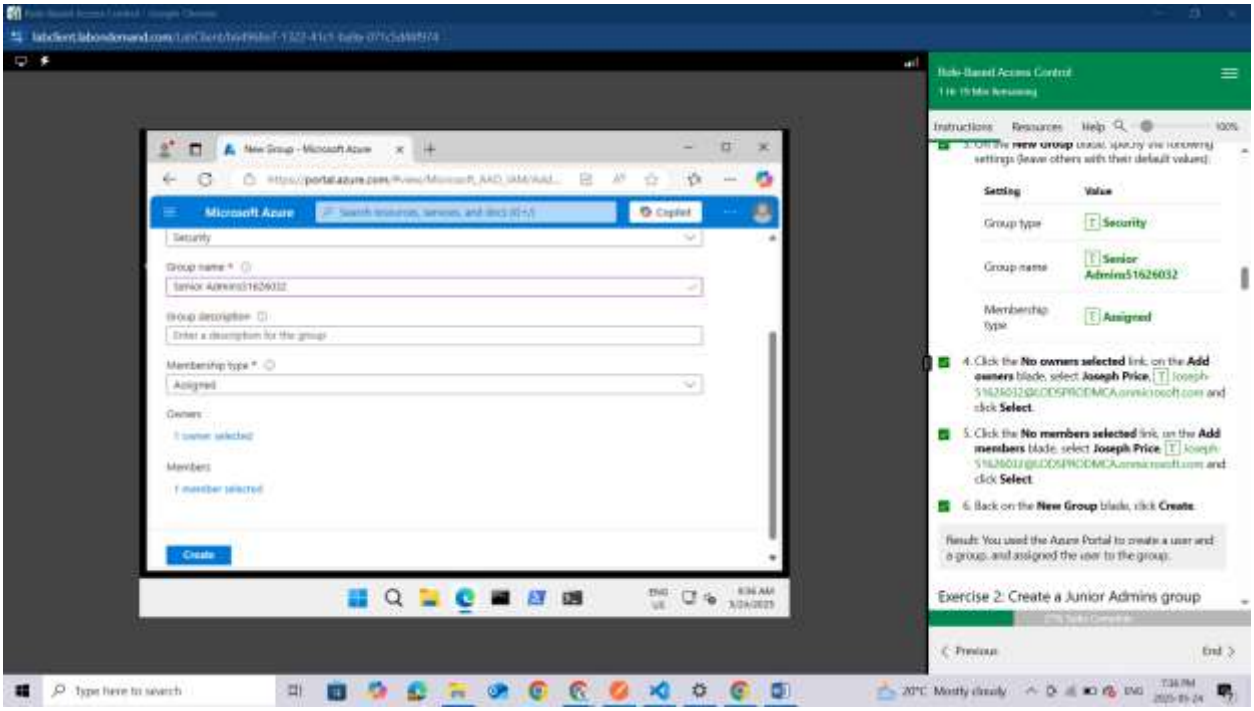
Click the **No owners selected link**, on the Add owners blade, select **Joseph Price, Joseph-51626032@LODSPRODMCA.onmicrosoft.com** and click **Select**.



Click the **No members selected link,** on the Add members blade, select **Joseph Price, Joseph-51626032@LODSPRODMCA.onmicrosoft.com** and click **Select**.



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.

In this exercise, you will complete the following tasks:

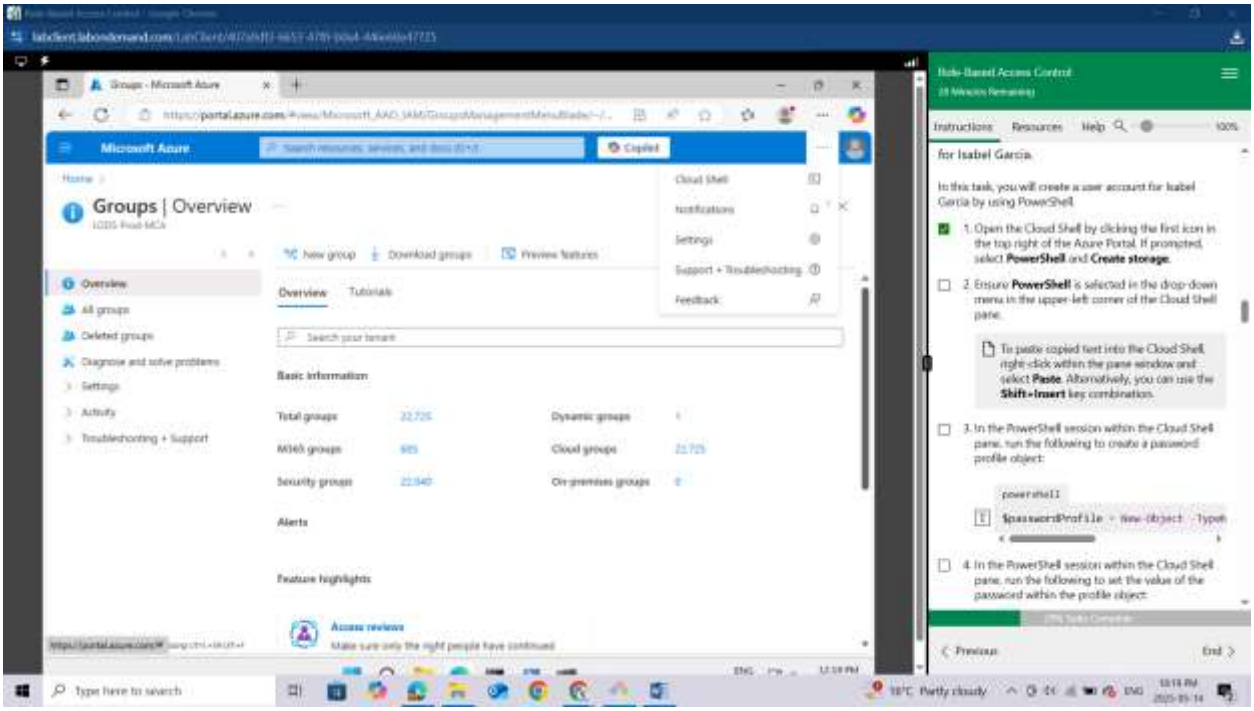
Task 1: Use PowerShell to create a user account for Isabel Garcia.

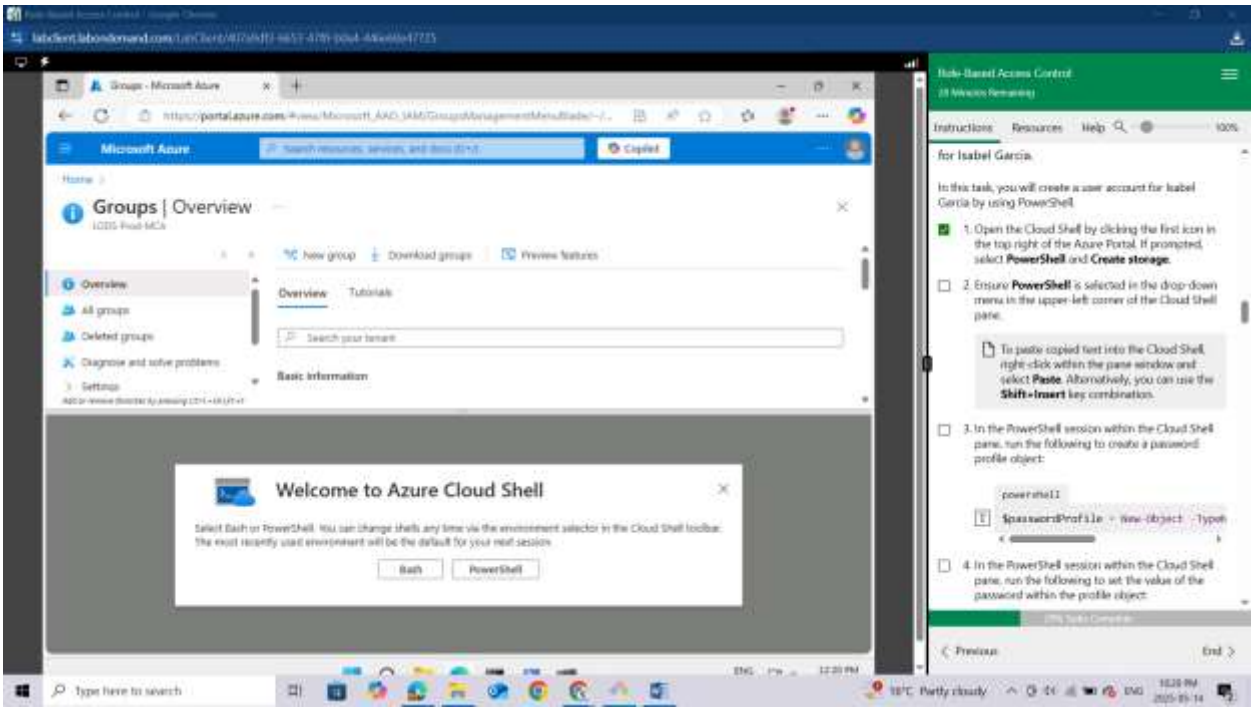
Task 2: Use PowerShell to create the Junior Admins group and add the user account of Isabel Garcia to the group.

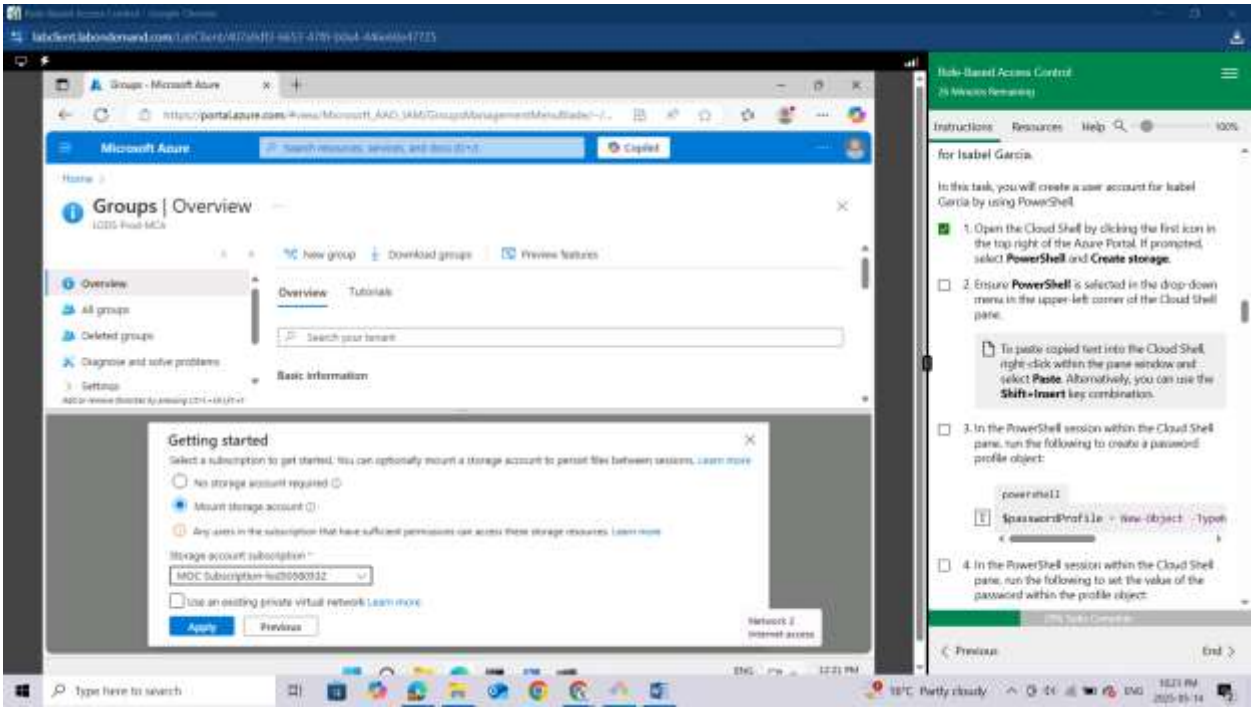
Task 1: Use PowerShell to create a user account for Isabel Garcia.

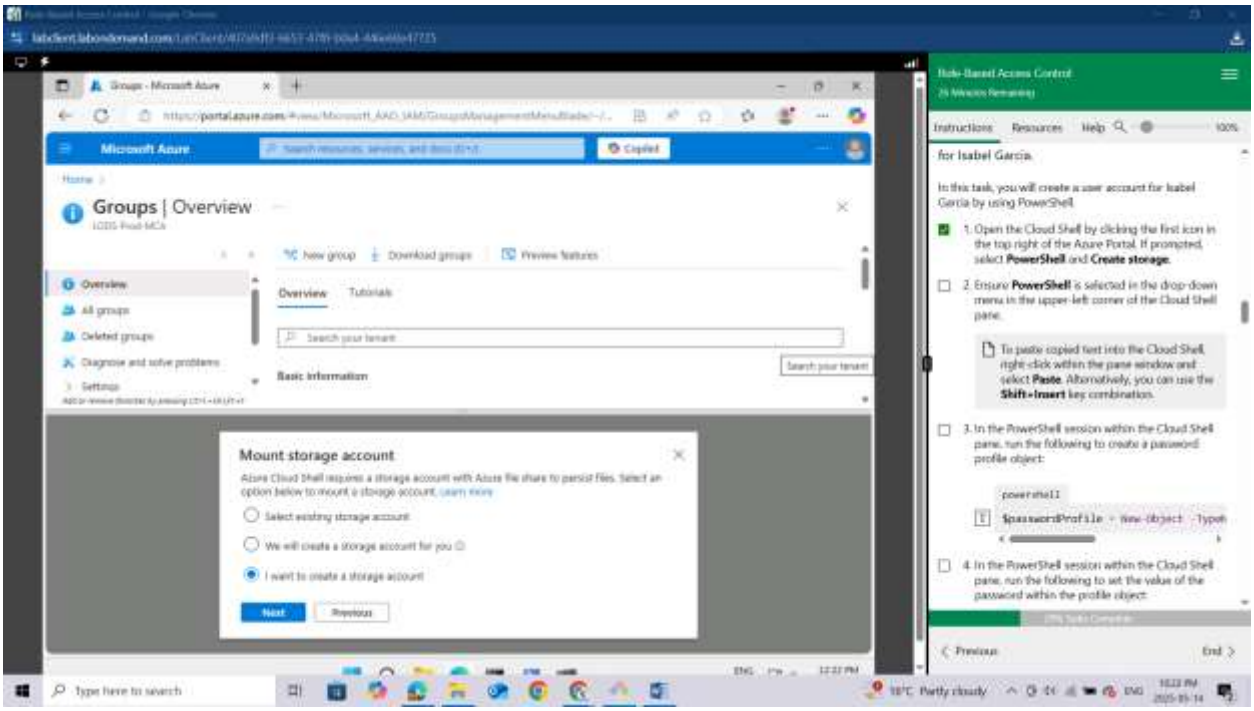
In this task, you will create a user account for Isabel Garcia by using PowerShell.

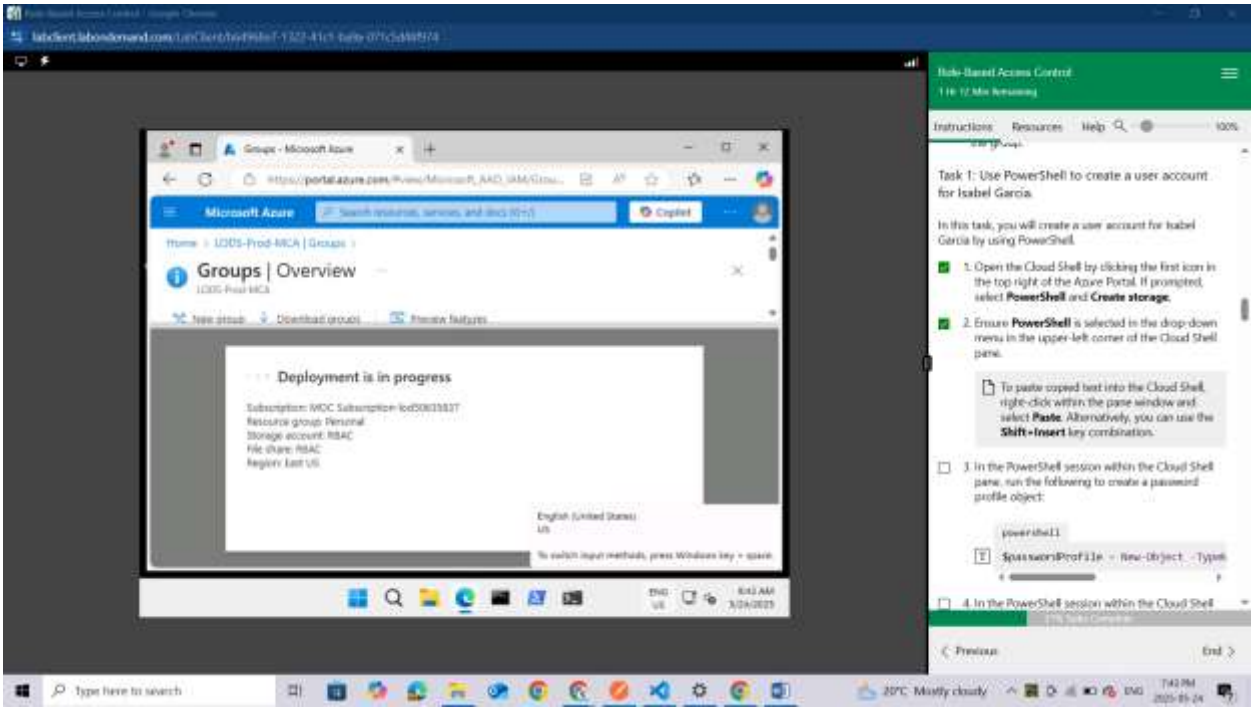
Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, select PowerShell and Create storage.

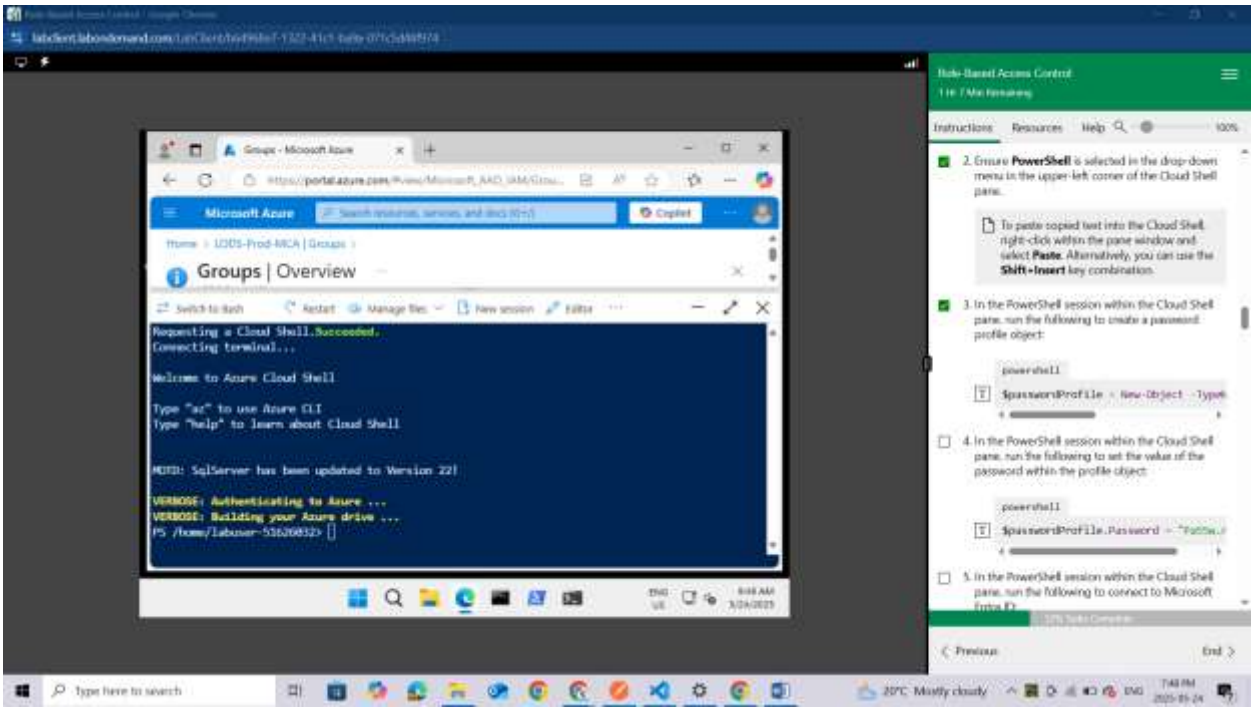



Groups | Overview
Welcome to Azure Cloud Shell
Bash
PowerShell
Role-Based Access Control
for Isabel Garcia.
In this task, you will create a user account for Isabel Garcia by using PowerShell.
1. Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, select PowerShell and Create storage.
2. Ensure PowerShell is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.
To paste copied text into the Cloud Shell, right-click within the pane window and select Paste. Alternatively, you can use the Shift+Insert key combination.
3. In the PowerShell session within the Cloud Shell pane, run the following to create a password profile object:
4. In the PowerShell session within the Cloud Shell pane, run the following to set the value of the password within the profile object:

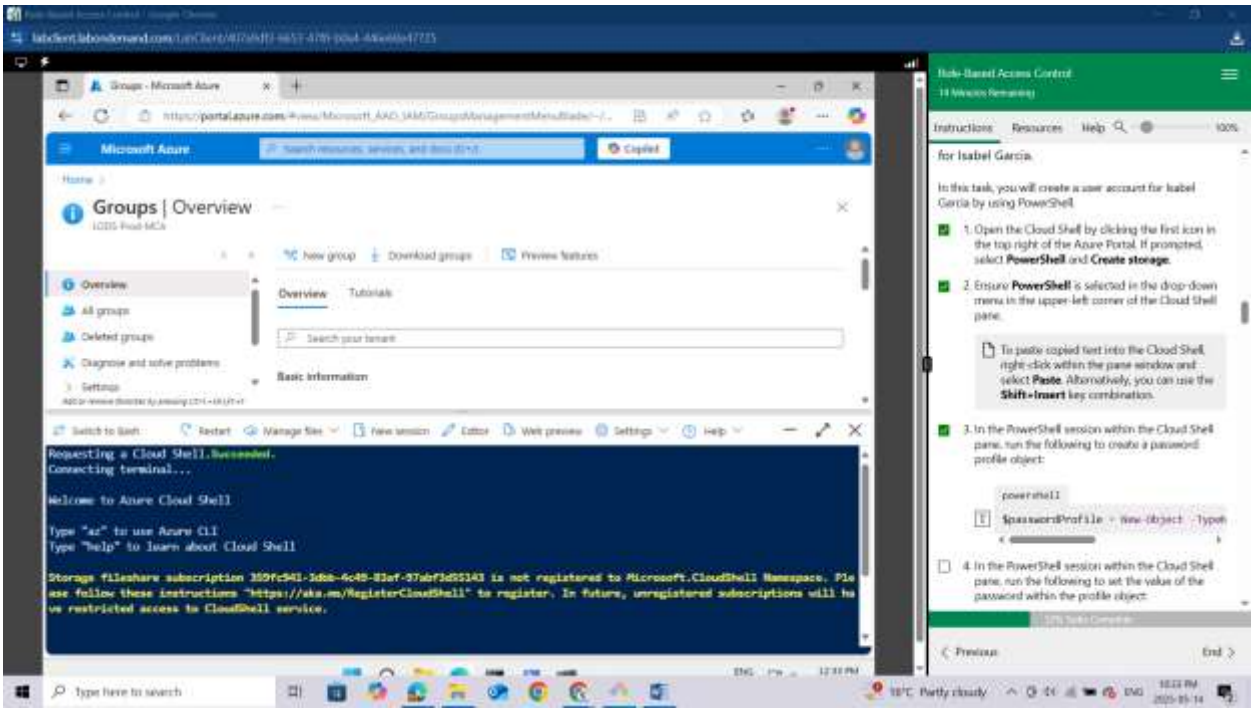

Groups | Overview
Getting started
Role-Based Access Control
for Isabel Garcia.
In this task, you will create a user account for Isabel Garcia by using PowerShell.
1. Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, select PowerShell and Create storage.
2. Ensure PowerShell is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.
To paste copied text into the Cloud Shell, right-click within the pane window and select Paste. Alternatively, you can use the Shift+Insert key combination.
3. In the PowerShell session within the Cloud Shell pane, run the following to create a password profile object:
4. In the PowerShell session within the Cloud Shell pane, run the following to set the value of the password within the profile object:


Groups | Overview
Mount storage account
Azure Cloud Shell requires a storage account with Azure file share to persist files. Select an option below to mount a storage account. Learn more
Select existing storage account
We will create a storage account for you
I want to create a storage account
Next
Previous
Role-Based Access Control
Instructions
Resources
Help
for Isabel Garcia.
In this task, you will create a user account for Isabel Garcia by using PowerShell.
1. Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, select PowerShell and Create storage.
2. Ensure PowerShell is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.
To paste copied text into the Cloud Shell, right-click within the pane window and select Paste. Alternatively, you can use the Shift+Insert key combination.
3. In the PowerShell session within the Cloud Shell pane, run the following to create a password profile object:
powershell
$passwordProfile = New-Object -TypeN
4. In the PowerShell session within the Cloud Shell pane, run the following to set the value of the password within the profile object:
Previous
End


Groups | Overview
Deployment is in progress
Role-Based Access Control
Instructions
Resources
Help
Task 1: Use PowerShell to create a user account for Isabel Garcia.
In this task, you will create a user account for Isabel Garcia by using PowerShell.
1. Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, select PowerShell and Create storage.
2. Ensure PowerShell is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.
To paste copied text into the Cloud Shell, right-click within the pane window and select Paste. Alternatively, you can use the Shift+Insert key combination.
3. In the PowerShell session within the Cloud Shell pane, run the following to create a password profile object:
powershell
$passwordProfile = New-Object -TypeN
4. In the PowerShell session within the Cloud Shell
Previous
End



Ensure PowerShell is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.



To paste copied text into the Cloud Shell, ***right-click*** *within the pane window and select* ***Paste****. Alternatively, you can use the* ***Shift+Insert*** *key combination.*

In the PowerShell session within the Cloud Shell pane, run the following to create a password profile object:

powershell

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

In the PowerShell session within the Cloud Shell pane, run the following to set the value of the password within the profile object:

powershell

$passwordProfile.Password = "Pa55w.rd1234"

In the PowerShell session within the Cloud Shell pane, run the following to connect to Microsoft Entra ID:

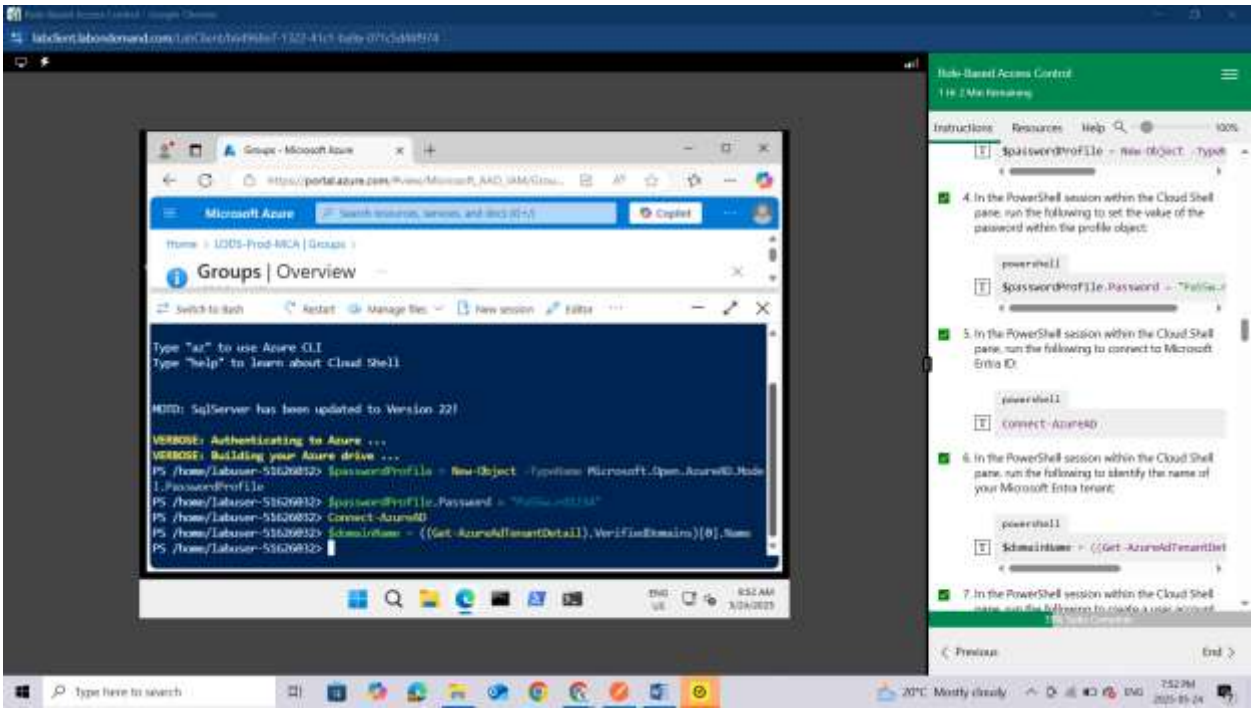
powershell

Connect-AzureAD

In the PowerShell session within the Cloud Shell pane, run the following to identify the name of your Microsoft Entra tenant:

powershell

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

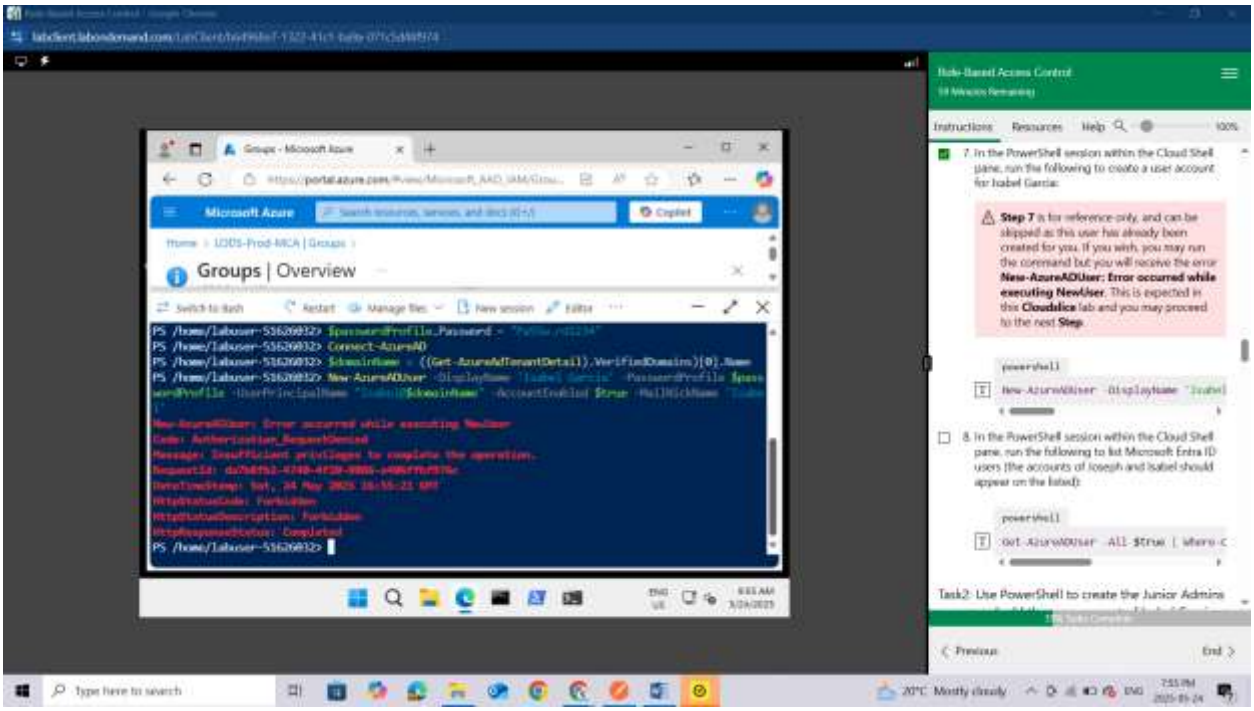


In the PowerShell session within the Cloud Shell pane, run the following to create a user account for Isabel Garcia:

Step 7 is for reference only, and can be skipped as this user has already been created for you. If you wish, you may run the command but you will receive the error New-AzureADUser: Error occurred while executing NewUser. This is expected in this Cloudslice lab and you may proceed to the next Step.

powershell

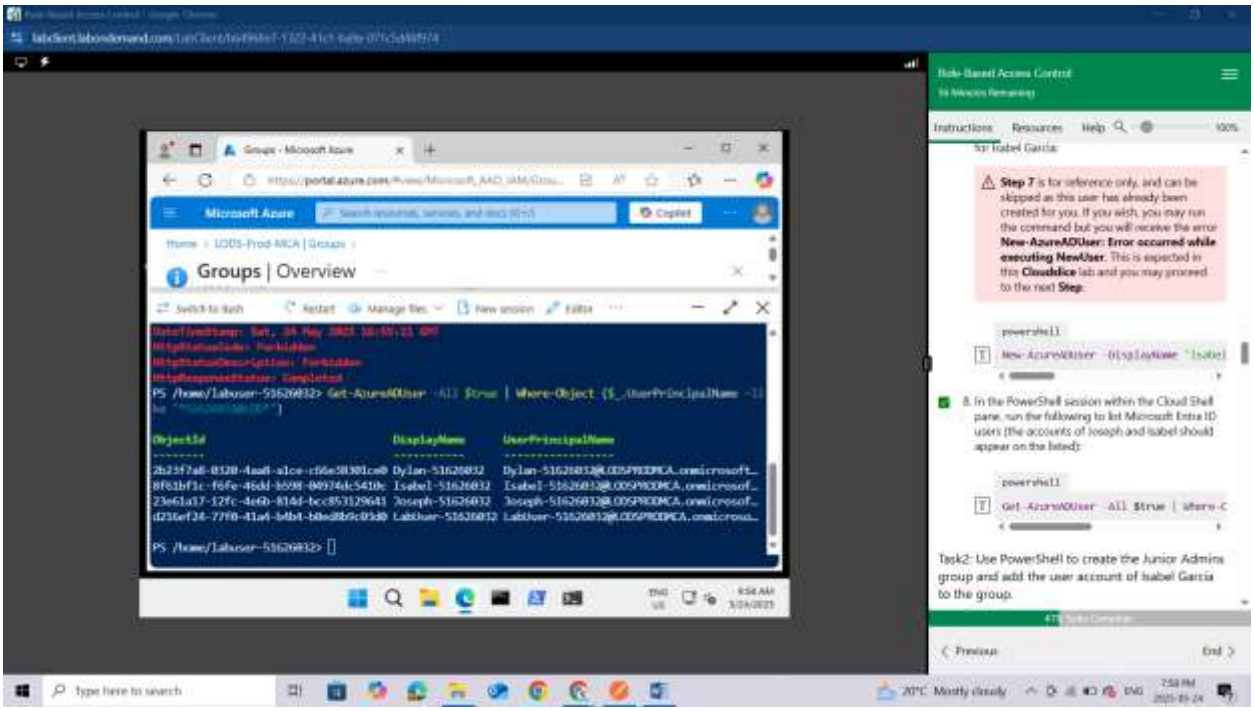
New-AzureADUser -DisplayName 'Isabel Garcia' -PasswordProfile $passwordProfile -UserPrincipalName "Isabel@$domainName" -AccountEnabled $true -MailNickName 'Isabel'



In the PowerShell session within the Cloud Shell pane, run the following to list Microsoft Entra ID users (the accounts of Joseph and Isabel should appear on the listed):

powershell

Get-AzureADUser -All $true | Where-Object {$_.UserPrincipalName -like "*51626032@LOD*"}



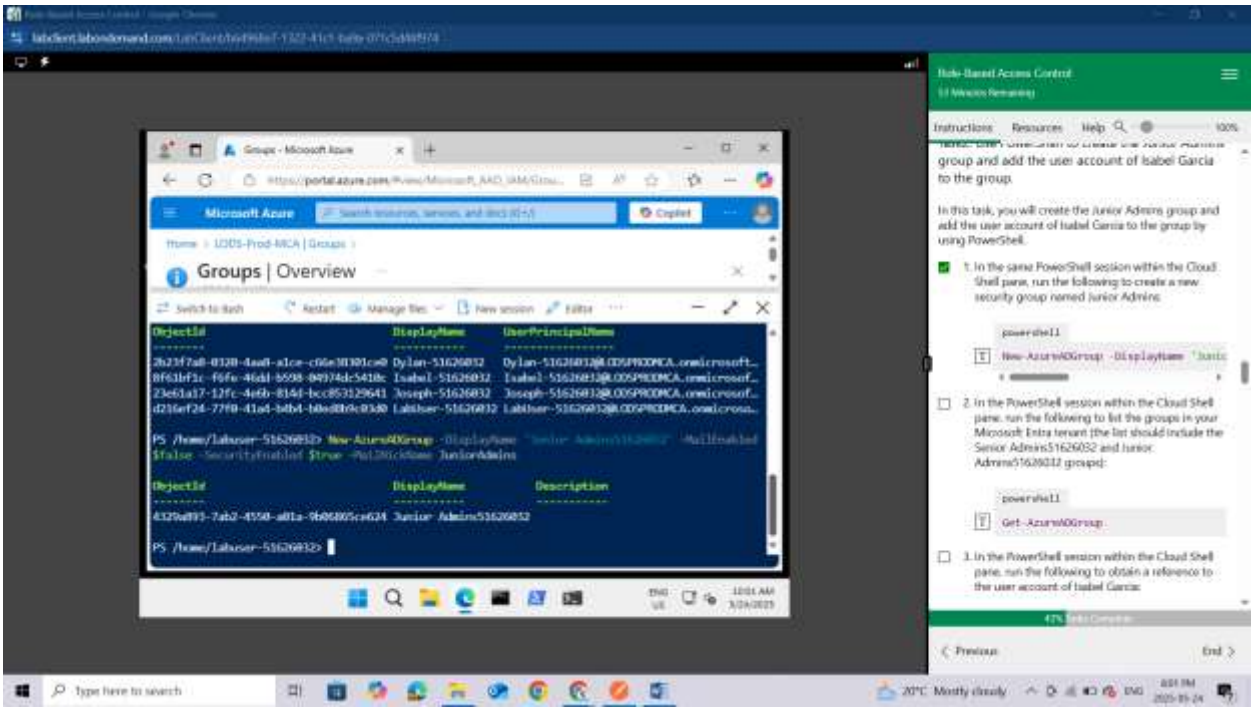
Task2: Use PowerShell to create the Junior Admins group and add the user account of Isabel Garcia to the group.

In this task, you will create the Junior Admins group and add the user account of Isabel Garcia to the group by using PowerShell.

In the same PowerShell session within the Cloud Shell pane, run the following to create a new security group named Junior Admins:

powershell

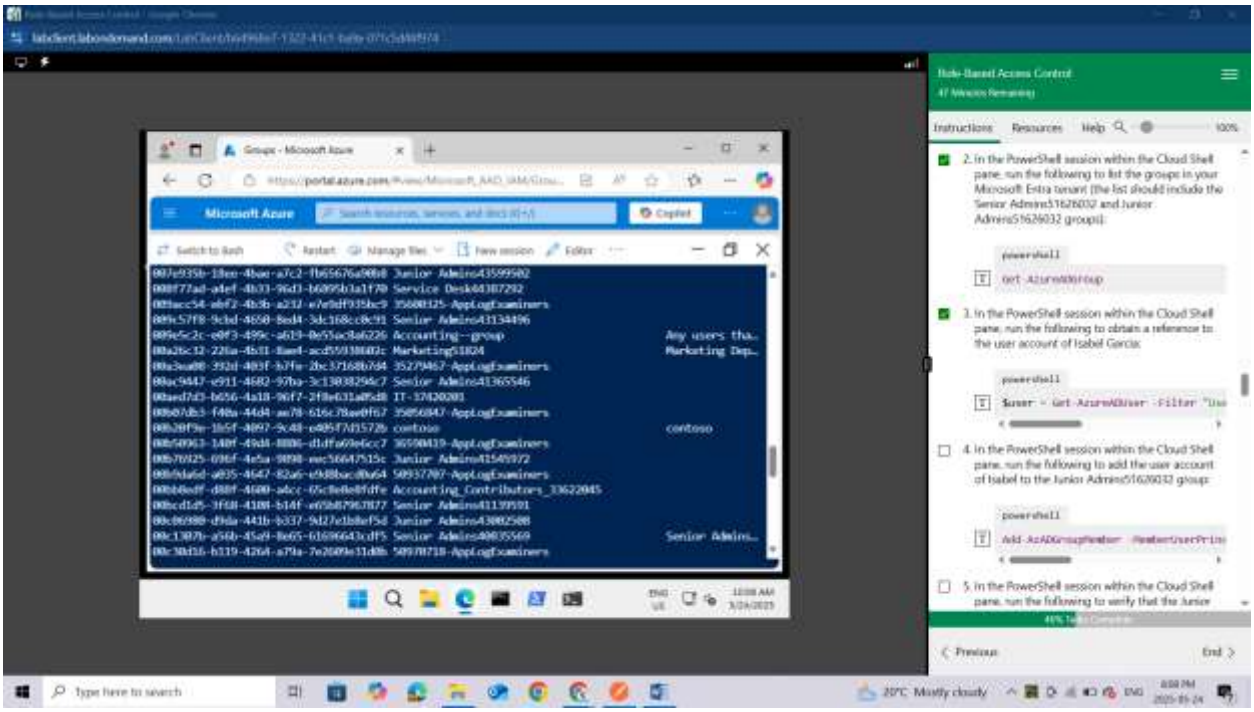
New-AzureADGroup -DisplayName 'Junior Admins51626032' -MailEnabled $false -SecurityEnabled $true -MailNickName JuniorAdmins



In the PowerShell session within the Cloud Shell pane, run the following to list the groups in your Microsoft Entra tenant (the list should include the Senior Admins51626032 and Junior Admins51626032 groups):

powershell

Get-AzureADGroup



In the PowerShell session within the Cloud Shell pane, run the following to obtain a reference to the user account of Isabel Garcia:

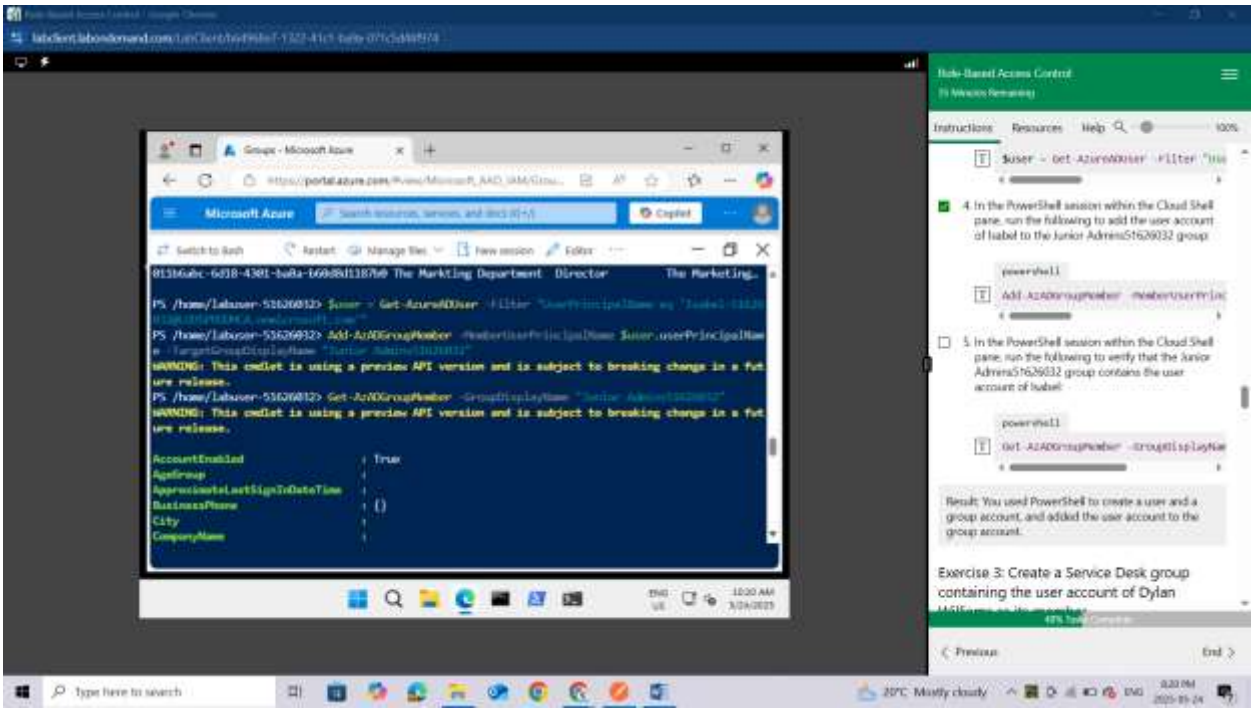
powershell

$user = Get-AzureADUser -Filter "UserPrincipalName eq 'Isabel-51626032@LODSPRODMCA.onmicrosoft.com'"

In the PowerShell session within the Cloud Shell pane, run the following to add the user account of Isabel to the Junior Admins51626032 group:

powershell

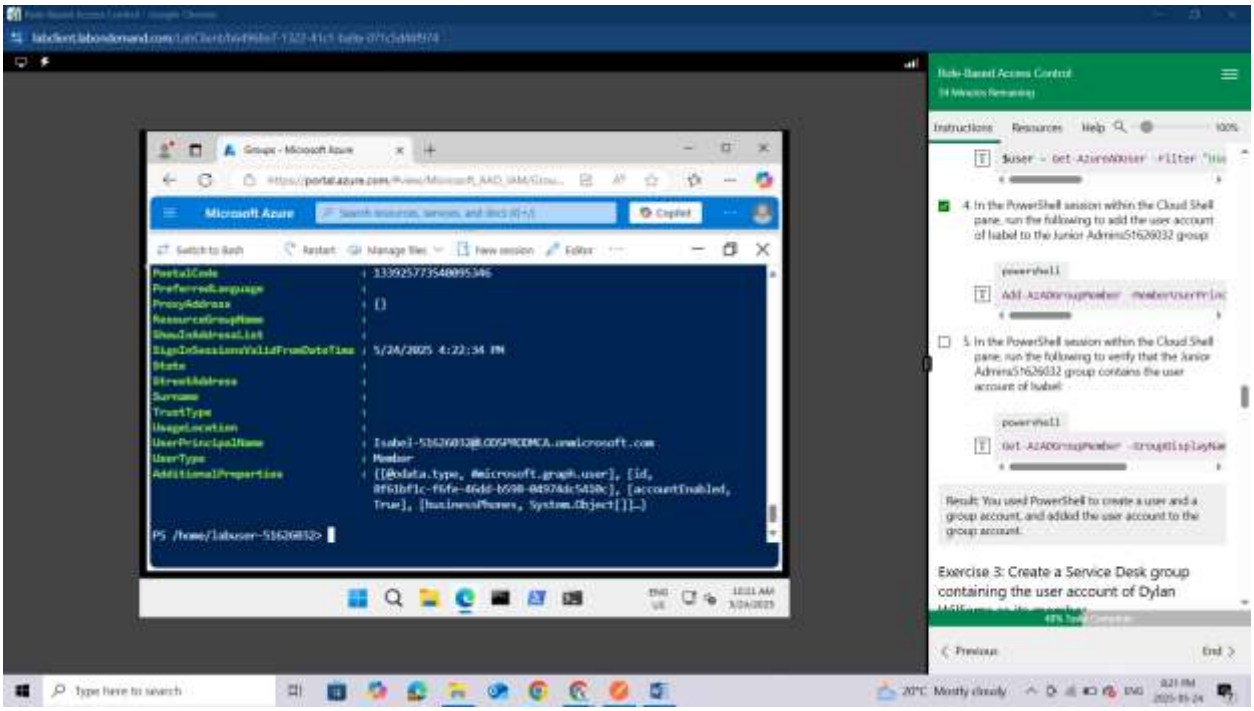
Add-AzADGroupMember -MemberUserPrincipalName $user.userPrincipalName -TargetGroupDisplayName "Junior Admins51626032"



In the PowerShell session within the Cloud Shell pane, run the following to verify that the Junior Admins51626032 group contains the user account of Isabel:

powershell

Get-AzADGroupMember -GroupDisplayName "Junior Admins51626032"



Result: You used PowerShell to create a user and a group account, and added the user account to the group account.

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

In this exercise, you will complete the following tasks:

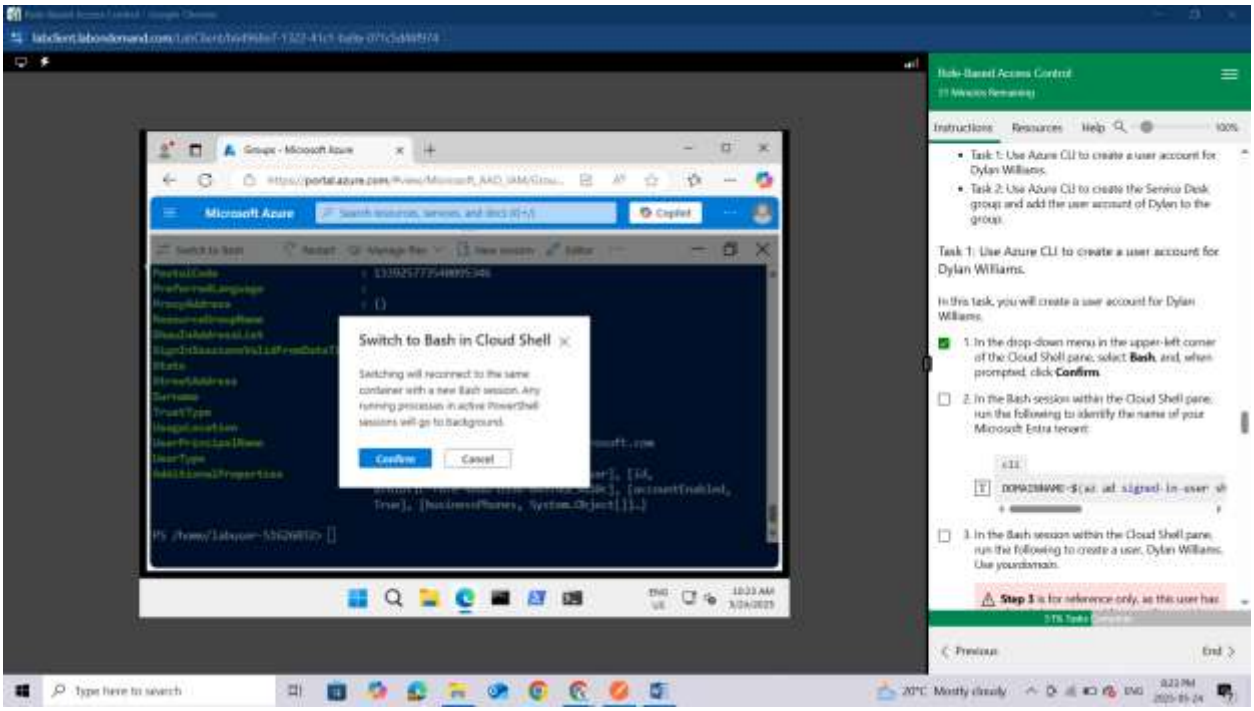
Task 1: Use Azure CLI to create a user account for Dylan Williams.

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

Task 1: Use Azure CLI to create a user account for Dylan Williams.

In this task, you will create a user account for Dylan Williams.

In the drop-down menu in the upper-left corner of the Cloud Shell pane, select **Bash**, and, when prompted, click **Confirm**.



In the Bash session within the Cloud Shell pane, run the following to identify the name of your Microsoft Entra tenant:

cli

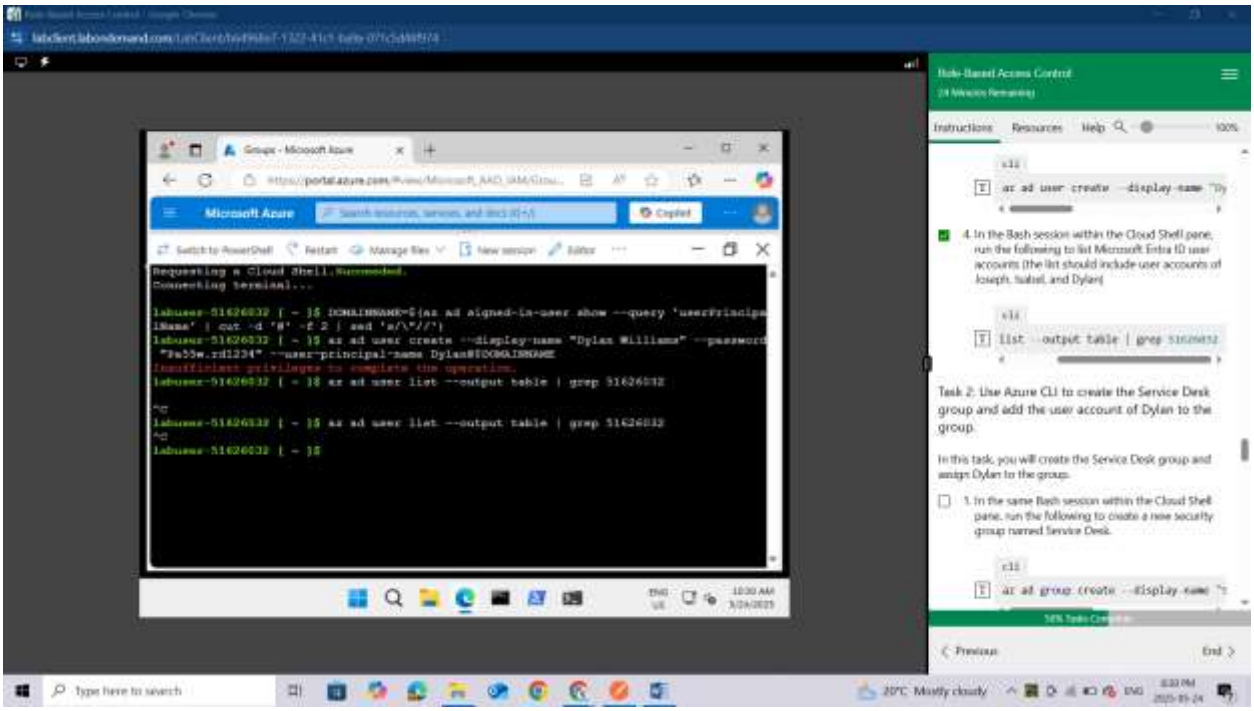
DOMAINNAME=$(az ad signed-in-user show --query 'userPrincipalName' | cut -d '@' -f 2 | sed 's/\"//')

In the Bash session within the Cloud Shell pane, run the following to create a user, Dylan Williams. Use yourdomain.

Step 3 is for reference only, as this user has already been created for you. If you wish, you may run the command but you will receive the error Insufficient privileges to complete the operation. This is expected in this Cloudslice lab and you may proceed to the next Step.

cli

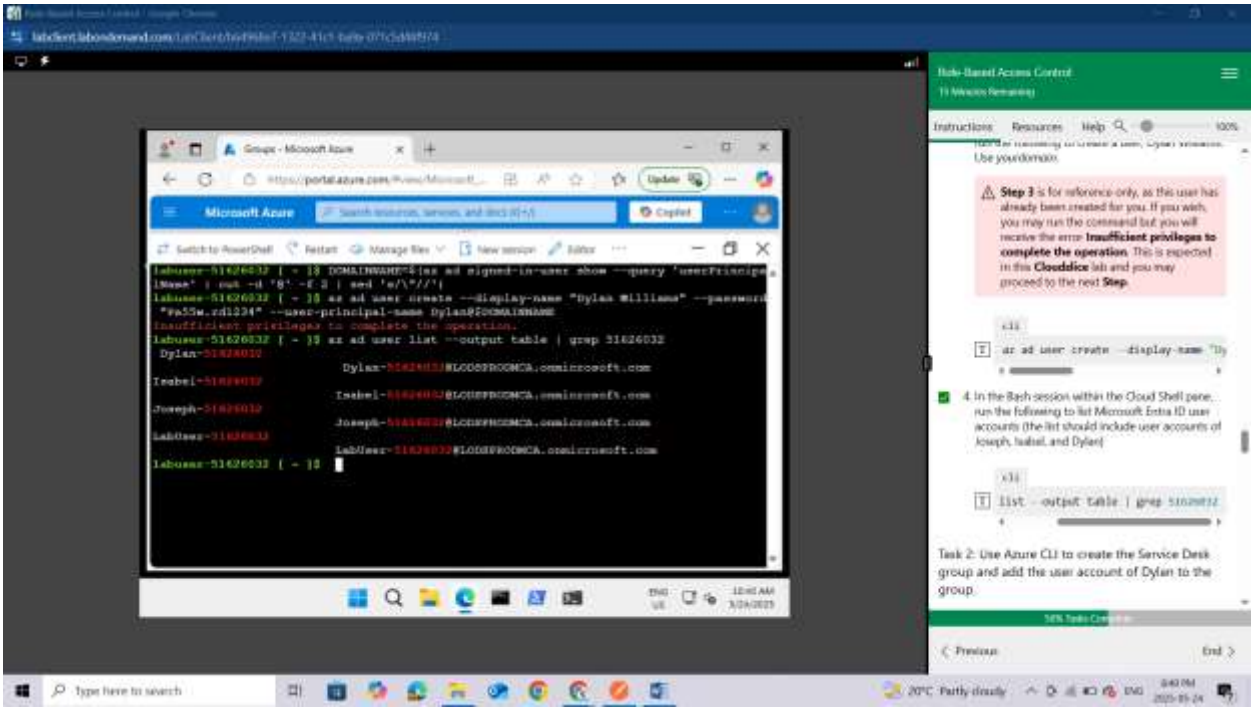
az ad user create --display-name "Dylan Williams" --password "Pa55w.rd1234" --user-principal-name Dylan@$DOMAINNAME



In the Bash session within the Cloud Shell pane, run the following to list Microsoft Entra ID user accounts (the list should include user accounts of Joseph, Isabel, and Dylan)

cli

az ad user list --output table | grep 51626032



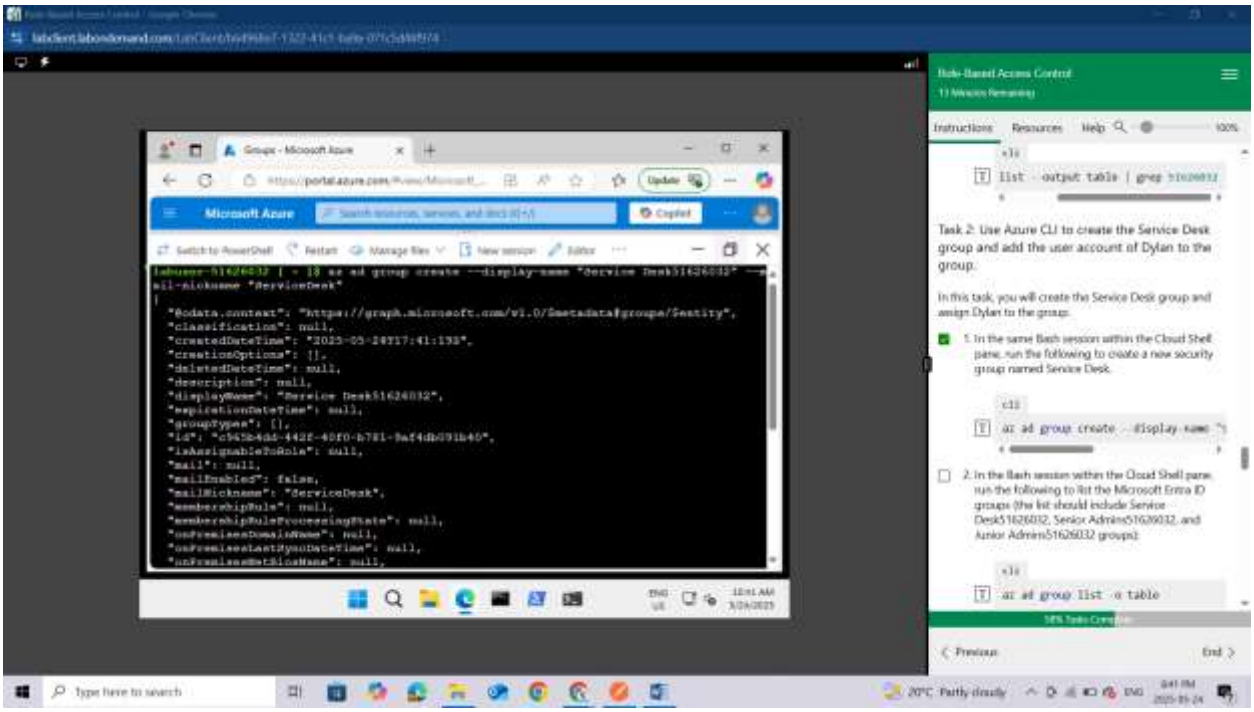
Task 2: Use Azure CLI to create the Service Desk group and add the user account of Dylan to the group.

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

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

cli

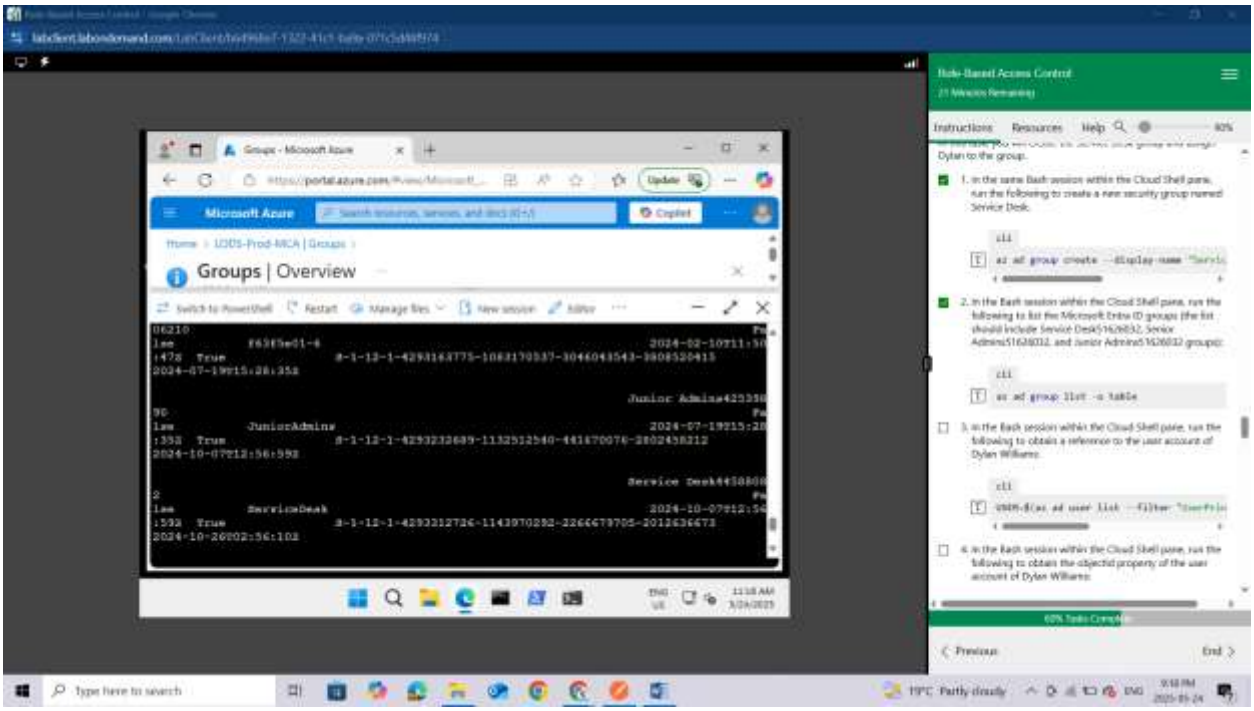
az ad group create --display-name "Service Desk51626032" --mail-nickname "ServiceDesk"



In the Bash session within the Cloud Shell pane, run the following to list the Microsoft Entra ID groups (the list should include Service Desk51626032, Senior Admins51626032, and Junior Admins51626032 groups):

cli

az ad group list -o table



In the Bash session within the Cloud Shell pane, run the following to obtain a reference to the user account of Dylan Williams:

cli

USER=$(az ad user list --filter "UserPrincipalName eq 'Dylan-51626032@LODSPRODMCA.onmicrosoft.com'")

In the Bash session within the Cloud Shell pane, run the following to obtain the objectId property of the user account of Dylan Williams:

cli

OBJECTID=$(echo $USER | jq '.[].id' | tr -d '"')

In the Bash session within the Cloud Shell pane, run the following to add the user account of Dylan to the Service Desk51626032 group:

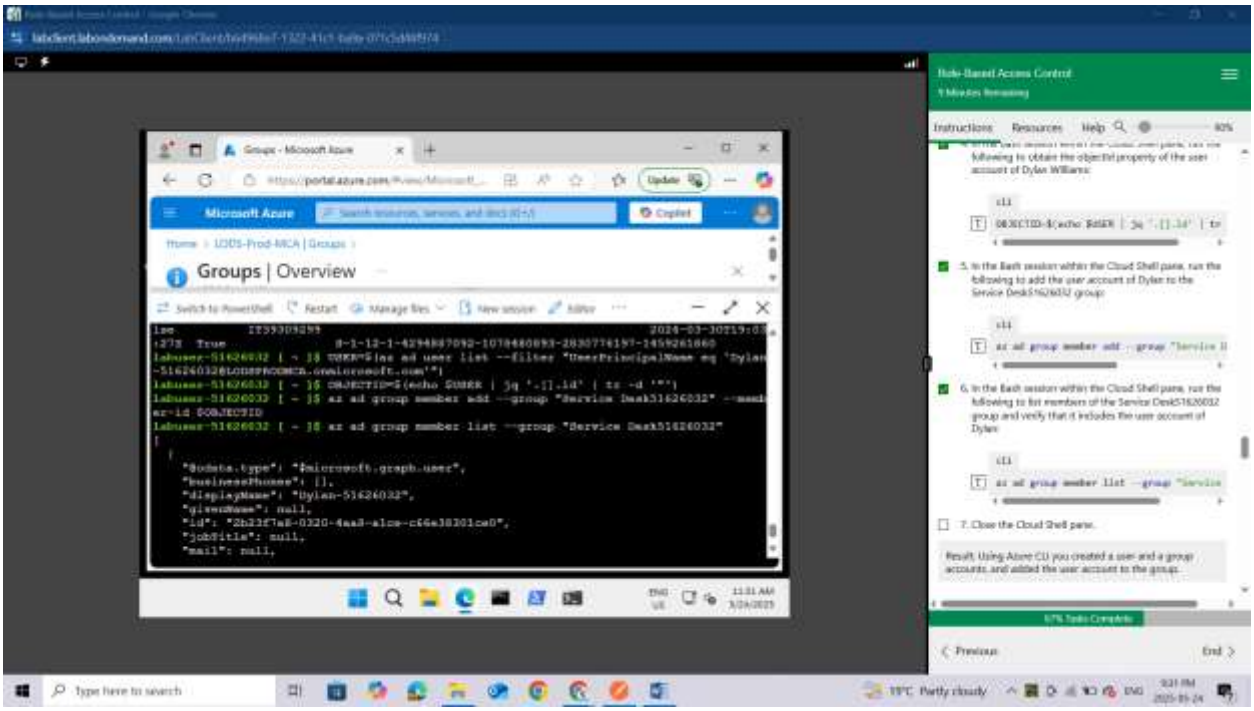
cli

az ad group member add --group "Service Desk51626032" --member-id $OBJECTID

In the Bash session within the Cloud Shell pane, run the following to list members of the Service Desk51626032 group and verify that it includes the user account of Dylan:

cli

az ad group member list --group "Service Desk51626032"



Close the Cloud Shell pane.

Result: Using Azure CLI you created a user and a group accounts, and added the user account to the group.

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

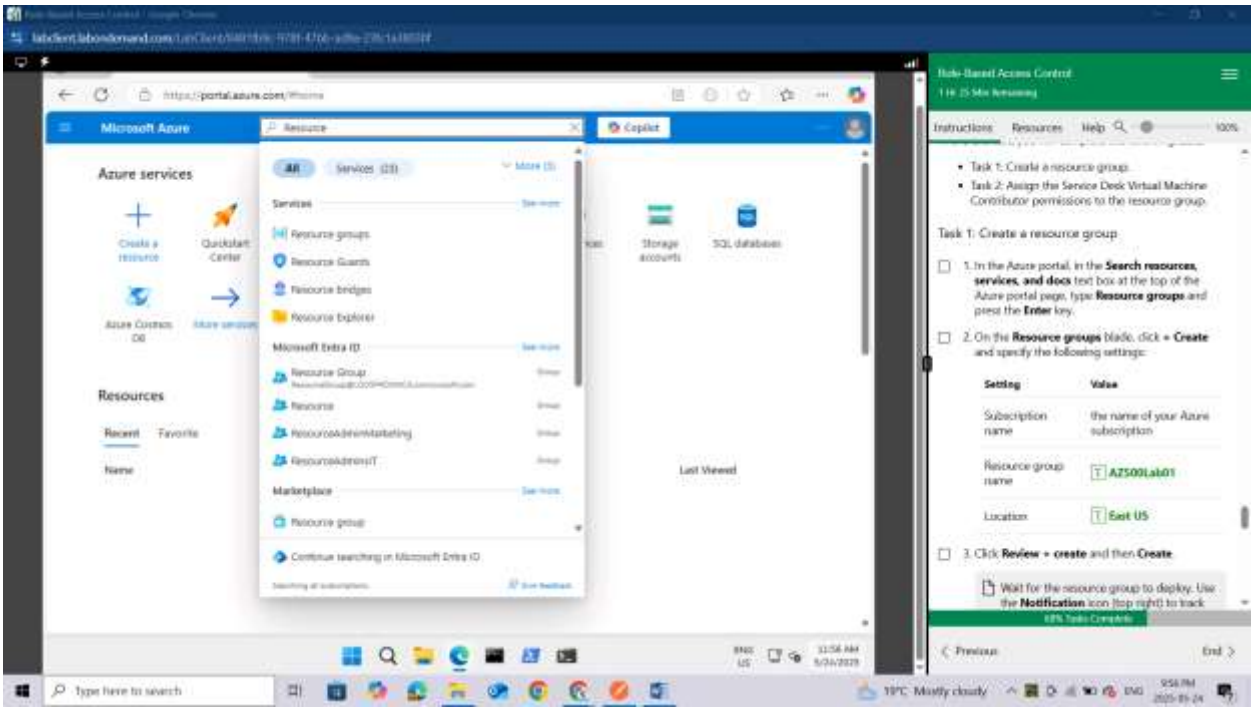
In this exercise, you will complete the following tasks:

Task 1: Create a resource group.

Task 2: Assign the Service Desk Virtual Machine Contributor permissions to the resource group.

Task 1: Create a resource group

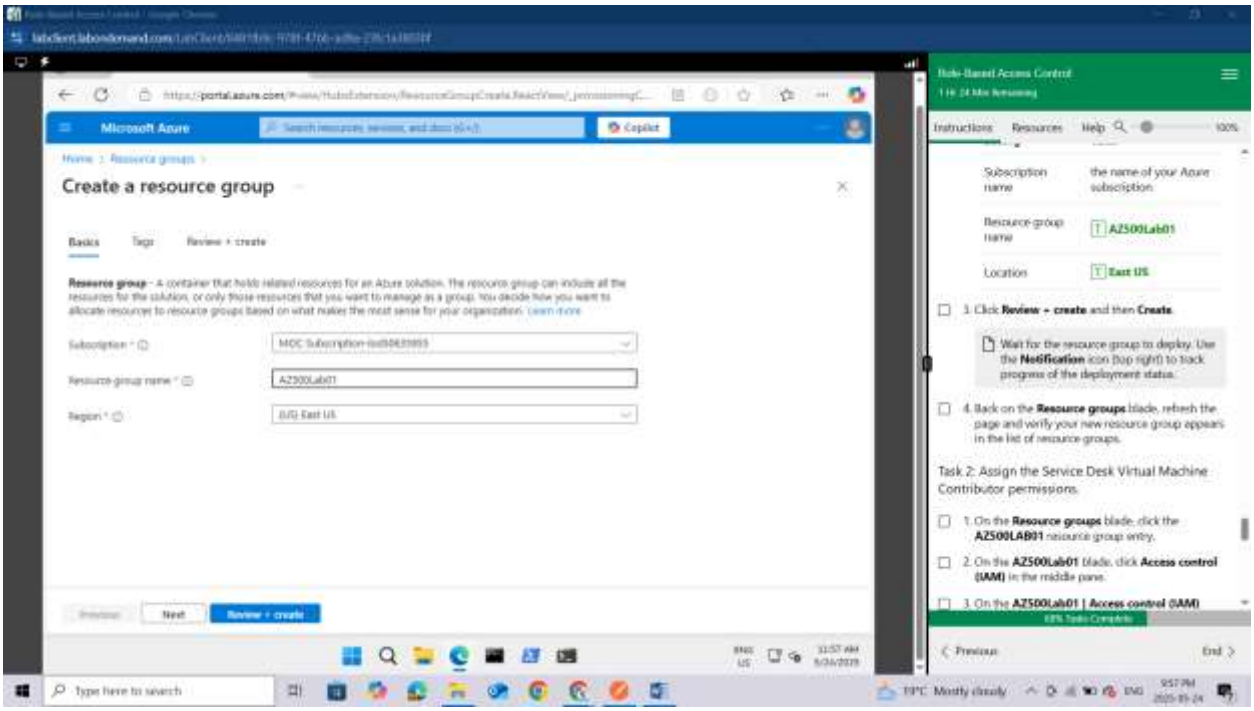
In the Azure portal, in the Search resources, services, and docs text box at the top of the Azure portal page, type **Resource groups** and press the **Enter** key.



On the Resource groups blade, click **+ Create** and specify the following settings:

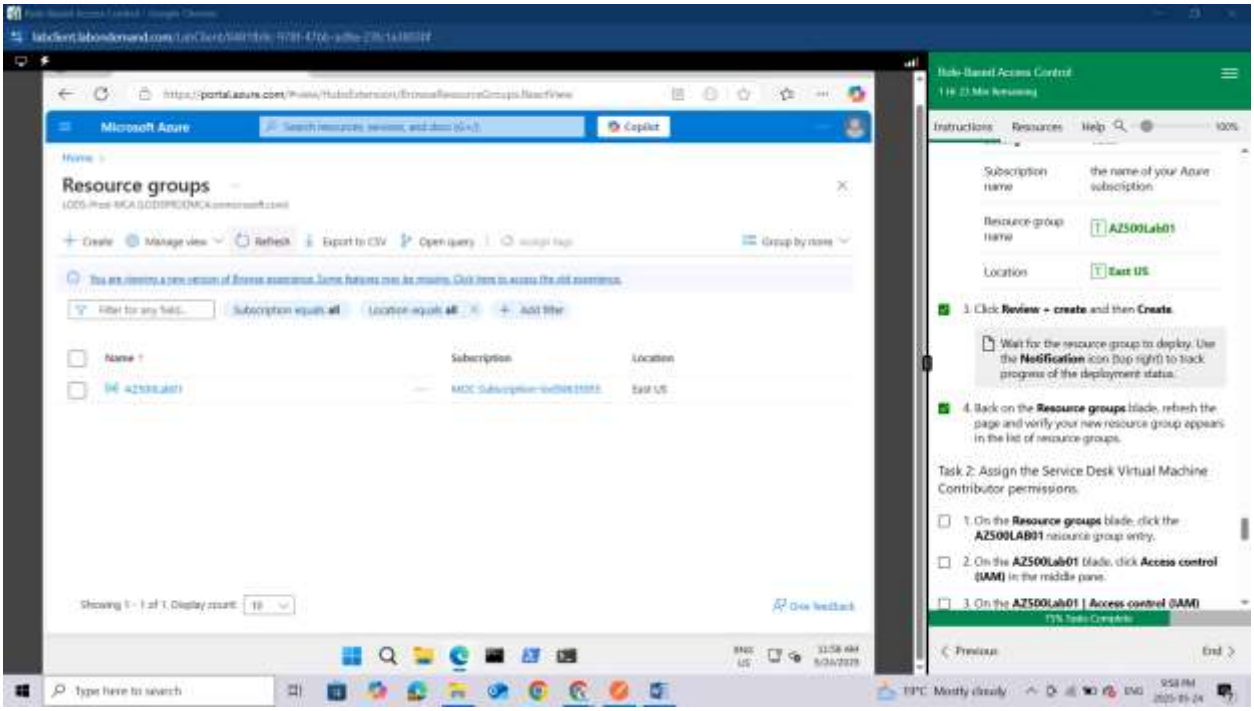
Setting	Value
Subscription name	the name of your Azure subscription
Resource group name	AZ500Lab01
Location	East US

Click **Review + create** and then **Create**.



Wait for the resource group to deploy. Use the Notification icon (top right) to track progress of the deployment status.

Back on the Resource groups blade, refresh the page and verify your new resource group appears in the list of resource groups.

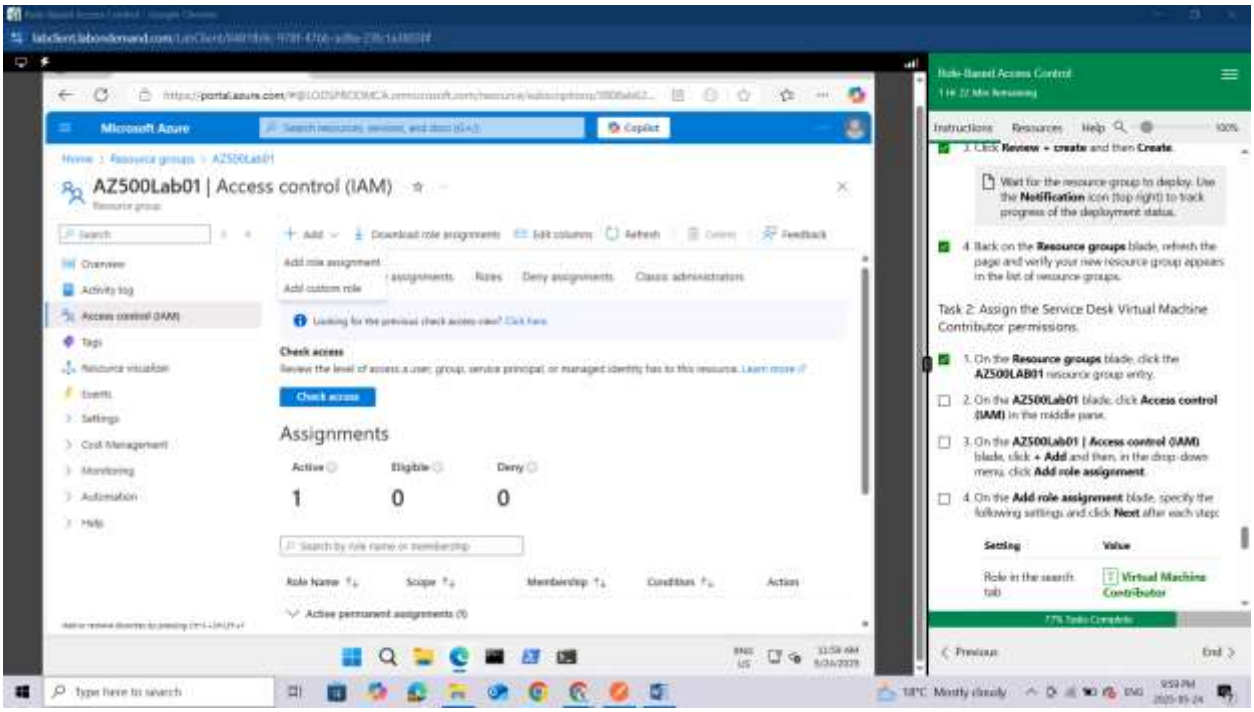


Task 2: Assign the Service Desk Virtual Machine Contributor permissions.

On the Resource groups blade, click the AZ500LAB01 resource group entry.

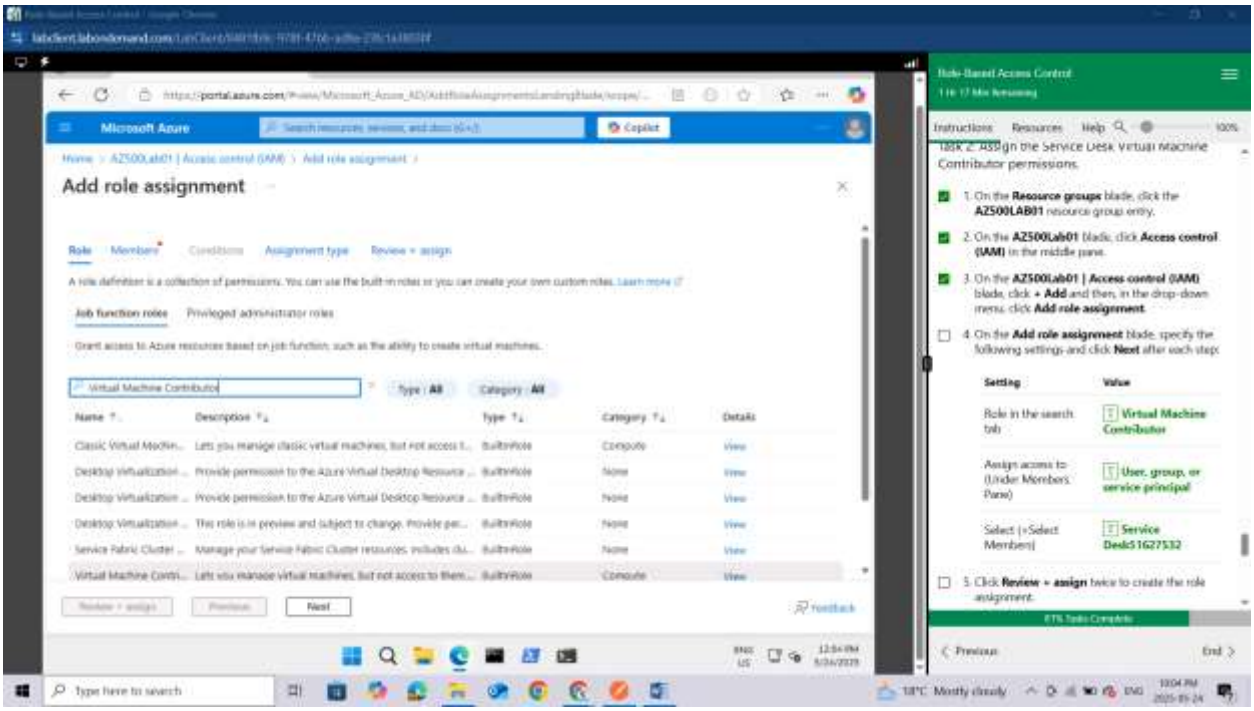
On the **AZ500Lab01** blade, click **Access control (IAM)** in the middle pane.

On the **AZ500Lab01 | Access control (IAM)** blade, click **+ Add** and then, in the drop-down menu, click **Add role assignment.**



On the **Add role assignment** blade, specify the following settings and click **Next** after each step:

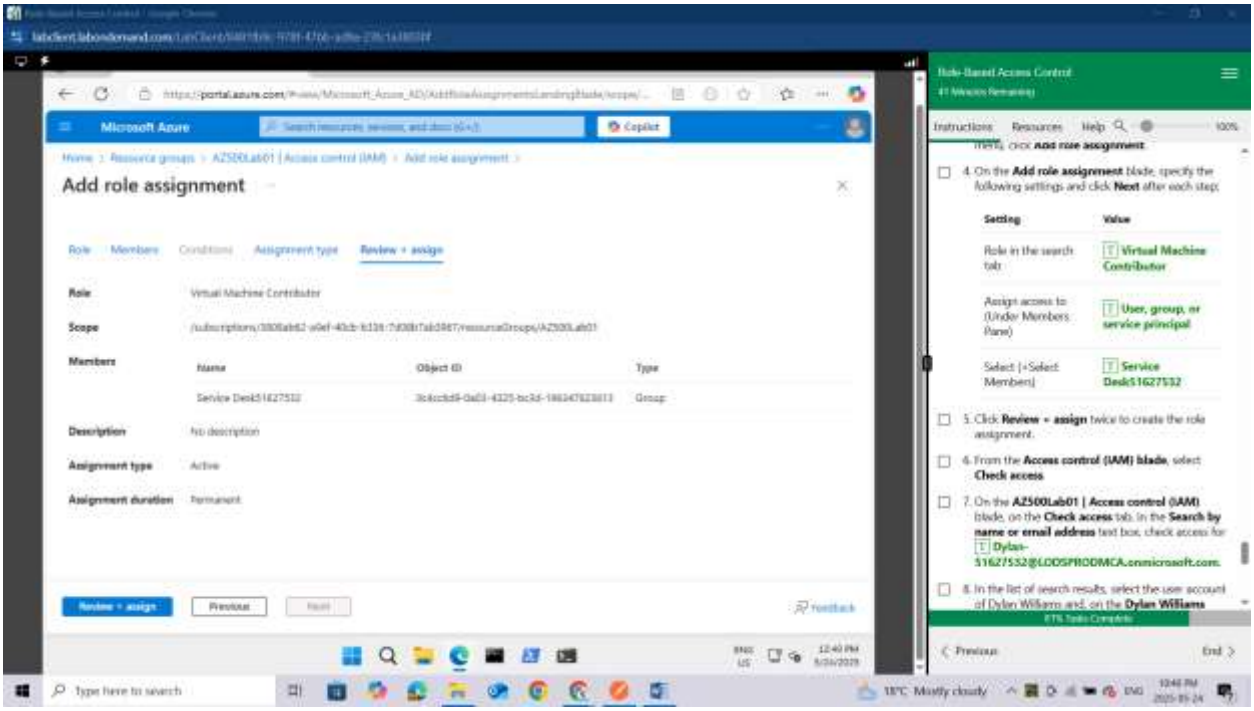
Setting	Value
Role in the search tab	Virtual Machine Contributor



Assign access to (Under Members Pane) User, group, or service principal

Select **(+Select Members**) Service Desk51626032

Click **Review + assign** twice to create the role assignment.

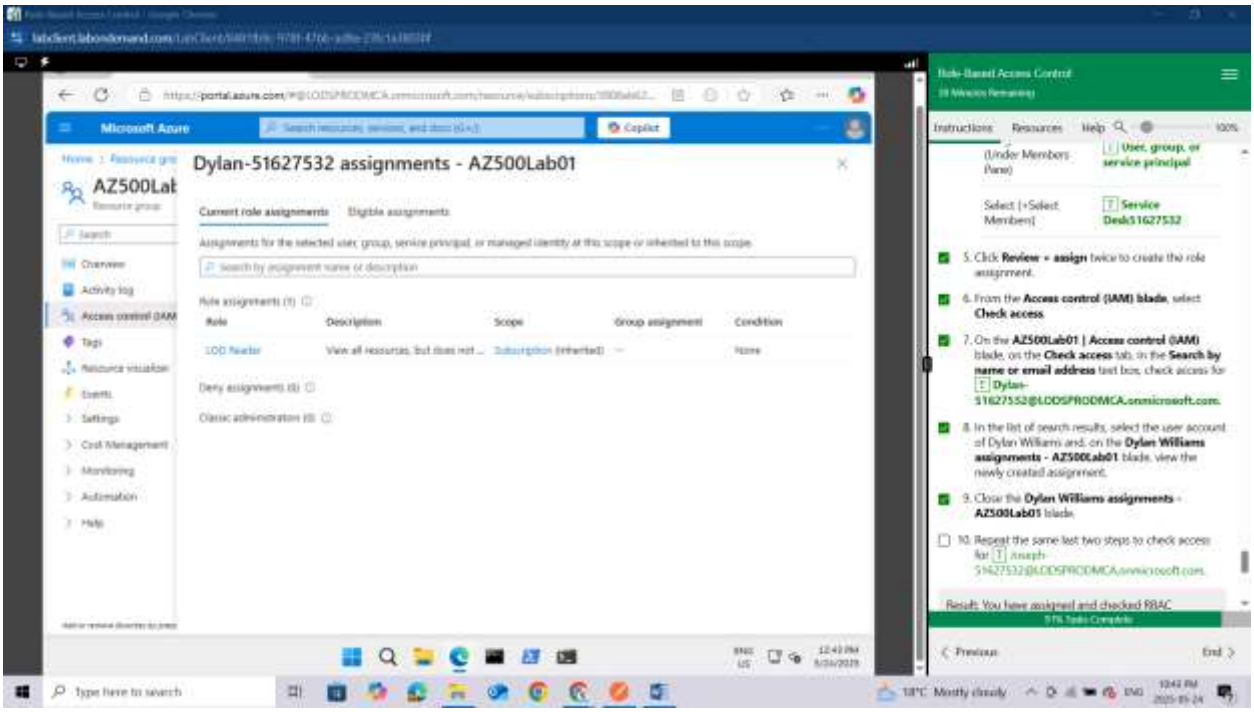


From the **Access control (IAM)** blade, select **Check access.**

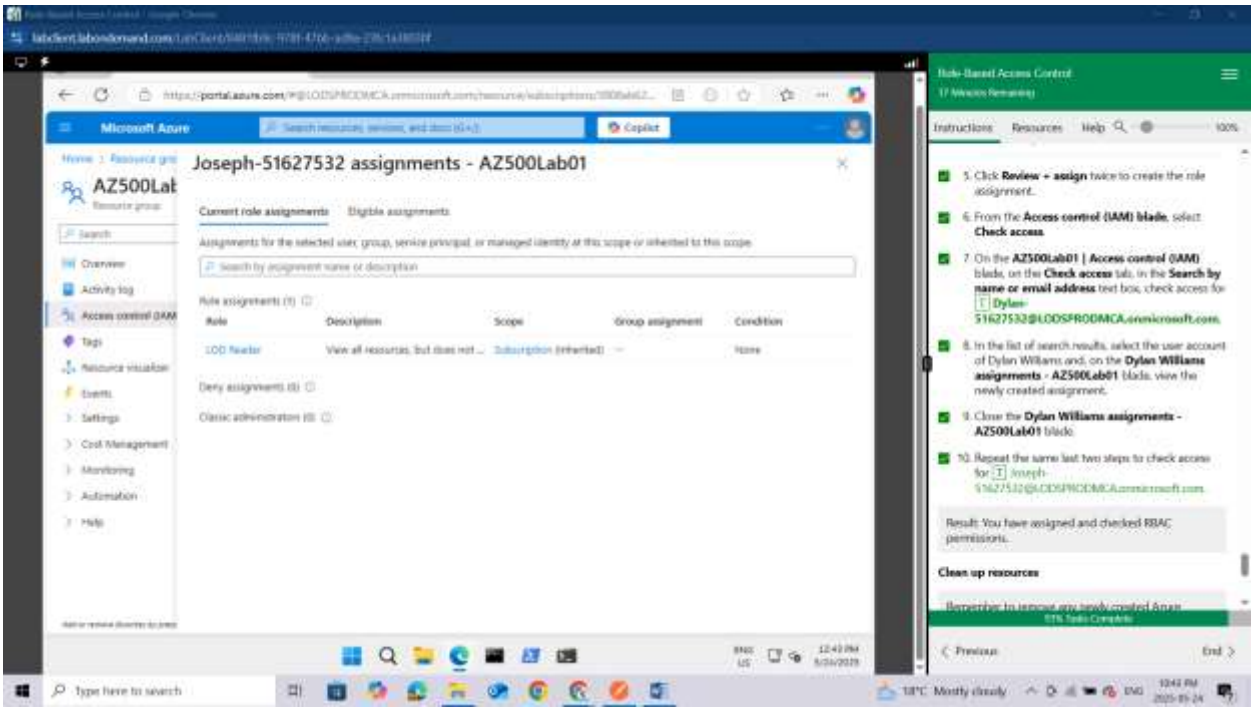
On the **AZ500Lab01 | Access control (IAM)** blade, on the **Check access** tab, in the Search by name or email address text box, check access for **Dylan-51626032@LODSPRODMCA.onmicrosoft.com**.

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.**

Close the **Dylan Williams assignments - AZ500Lab01** blade.



Repeat the same last two steps to check access for **Joseph-51626032@LODSPRODMCA.onmicrosoft.com.**



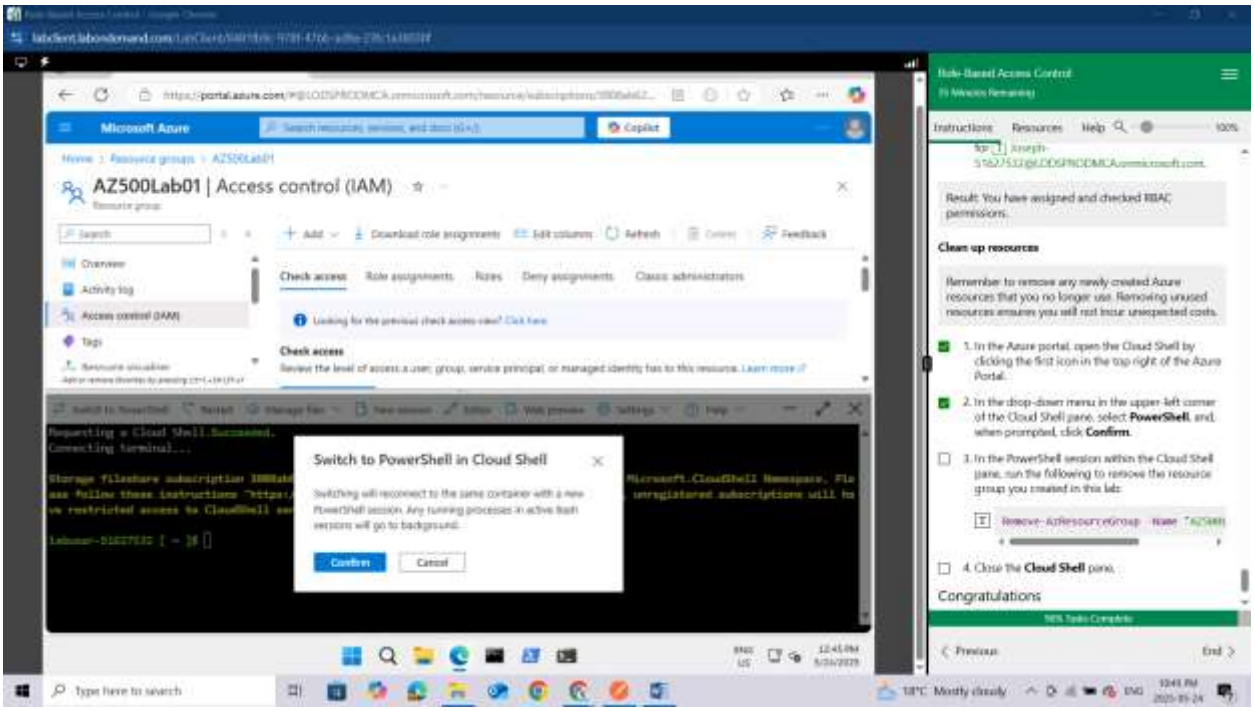
Result: You have assigned and checked RBAC permissions.

Clean up resources

Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs.

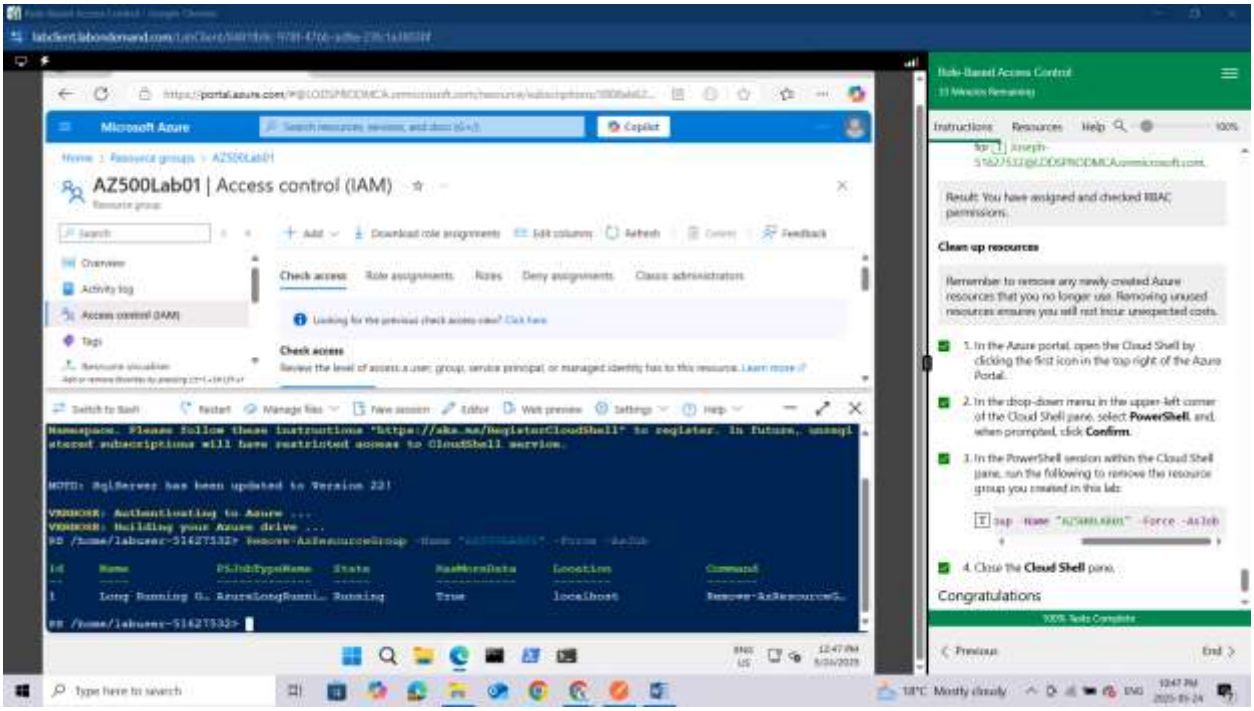
In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal.

In the drop-down menu in the upper-left corner of the Cloud Shell pane, select **PowerShell**, and, when prompted, click **Confirm**.



In the PowerShell session within the Cloud Shell pane, run the following to remove the resource group you created in this lab:

Remove-AzResourceGroup -Name "AZ500LAB01" -Force –AsJob



Close the Cloud Shell pane.

CONCLUSION

In this lab, I successfully implemented **Role-Based Access Control (RBAC)** in Microsoft Azure using the Learn on Demand platform. I created three security groups—*Senior Admins, Junior Admins, and Service Desk*—and correctly assigned user accounts to each group: ***Joseph Price to Senior Admins***, ***Isabel Garcia to Junior Admins***, and ***Dylan Williams to Service Desk***. To enforce least privilege access, I assigned the **Virtual Machine Contributor** role to the **Service Desk group**, enabling them to manage virtual machines without unnecessary permissions. This lab reinforced my understanding of Azure RBAC principles and how to apply them to control access and enhance security within an Azure environment.