Cyber Shujaa

Cloud Security Specialist

Assignment 9: Lab - Role-Based Access Control

NAME: WELDON KIPKIRUI KENEI

CS NO: ADC-CSS02-25027

Introduction

In this lab scenario, we will demonstrate the capabilities of role-based access as a feature of Microsoft Entra ID's secure identity. We will outline every step taken to achieve these secure identities and access.

Table

Assignment 9: Lab - Role-Based Access Control **1**
Introduction **2**
Creating users and assigning them to groups **3**
Assign the Virtual Machine Contributor role to the Service Desk group. **4**
Conclusion **5**

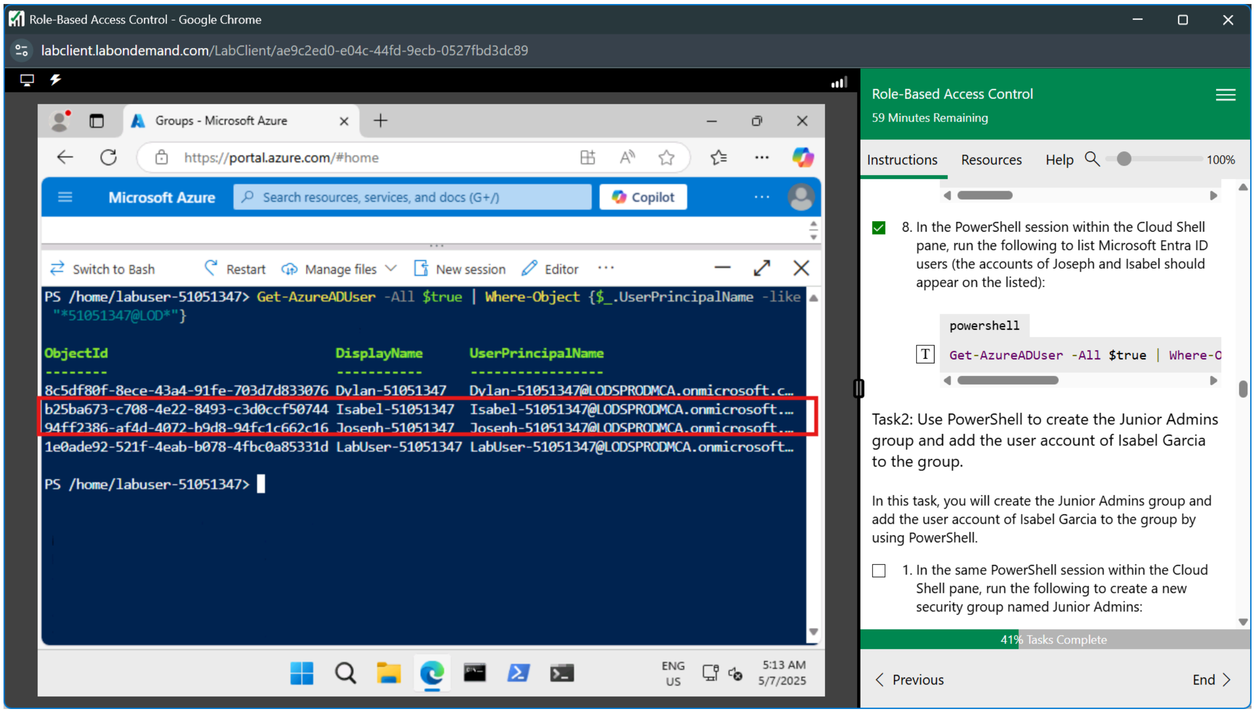
Creating users and assigning them to groups

Here, we will 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.

We can use the Cloud Shell and the Entra ID portal to create the user and group using `New-AzureADUser -DisplayName 'Isabel Garcia' -PasswordProfile $passwordProfile -UserPrincipalName "Isabel@$domainName" -AccountEnabled $true -MailNickName 'Isabel'`

” command. Using this command, `Get-AzureADUser -All $true | Where-Object {$_.UserPrincipalName -like "*51051347@LOD*"}`

We can list the users created under our domain. Also, some variables were created to make the command easier to write, for example, *$passwordProfile and $ domainName*



Role-Based Access Control - Google Chrome
labclient.labondemand.com/LabClient/ae9c2ed0-e04c-44fd-9ecb-0527fbd3dc89
Groups - Microsoft Azure
https://portal.azure.com/#home
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Switch to Bash
Restart
Manage files
New session
Editor

```
PS /home/labuser-51051347> Get-AzureADUser -All $true | Where-Object {$_.UserPrincipalName -like
 "*51051347@LOD*"}

ObjectId                             DisplayName      UserPrincipalName
--------                             -----------      -----------------
8c5df80f-8ece-43a4-91fe-703d7d833076 Dylan-51051347   Dylan-51051347@LODSPRODMCA.onmicrosoft.c…
b25ba673-c708-4e22-8493-c3d0ccf50744 Isabel-51051347  Isabel-51051347@LODSPRODMCA.onmicrosoft.…
94ff2386-af4d-4072-b9d8-94fc1c662c16 Joseph-51051347  Joseph-51051347@LODSPRODMCA.onmicrosoft.…
1e0ade92-521f-4eab-b078-4fbc0a85331d LabUser-51051347 LabUser-51051347@LODSPRODMCA.onmicrosoft…

PS /home/labuser-51051347>
```

☑ 8. 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

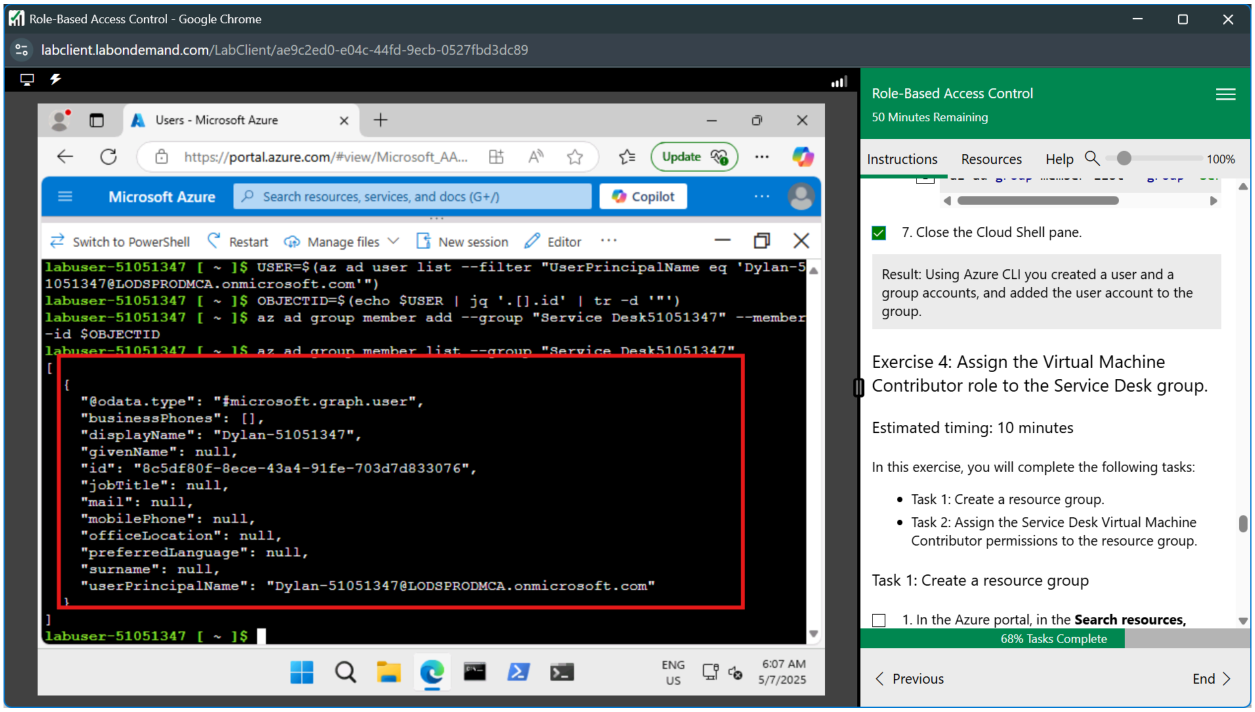
```
Get-AzureADUser -All $true | Where-O
```

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.

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

We can also use Azure CLI ‘bash' to create users and add them to a group. We created a service desk group and added a user, Dylan, to it. Ash is shown below;


Role-Based Access Control - Google Chrome
labclient.labondemand.com/LabClient/ae9c2ed0-e04c-44fd-9ecb-0527fbd3dc89
Users - Microsoft Azure
https://portal.azure.com/#view/Microsoft_AA...
Update
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Switch to PowerShell
Restart
Manage files
New session
Editor
ENG
US
6:07 AM
5/7/2025

```
labuser-51051347 [ ~ ]$ USER=$(az ad user list --filter "UserPrincipalName eq 'Dylan-5
1051347@LODSPRODMCA.onmicrosoft.com'")
labuser-51051347 [ ~ ]$ OBJECTID=$(echo $USER | jq '.[].id' | tr -d '"')
labuser-51051347 [ ~ ]$ az ad group member add --group "Service Desk51051347" --member
-id $OBJECTID
labuser-51051347 [ ~ ]$ az ad group member list --group "Service Desk51051347"
[
  {
    "@odata.type": "#microsoft.graph.user",
    "businessPhones": [],
    "displayName": "Dylan-51051347",
    "givenName": null,
    "id": "8c5df80f-8ece-43a4-91fe-703d7d833076",
    "jobTitle": null,
    "mail": null,
    "mobilePhone": null,
    "officeLocation": null,
    "preferredLanguage": null,
    "surname": null,
    "userPrincipalName": "Dylan-51051347@LODSPRODMCA.onmicrosoft.com"
  }
]
labuser-51051347 [ ~ ]$
```

Role-Based Access Control

50 Minutes Remaining

Instructions Resources Help 100%

☑ 7. 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.

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.

Task 1: Create a resource group

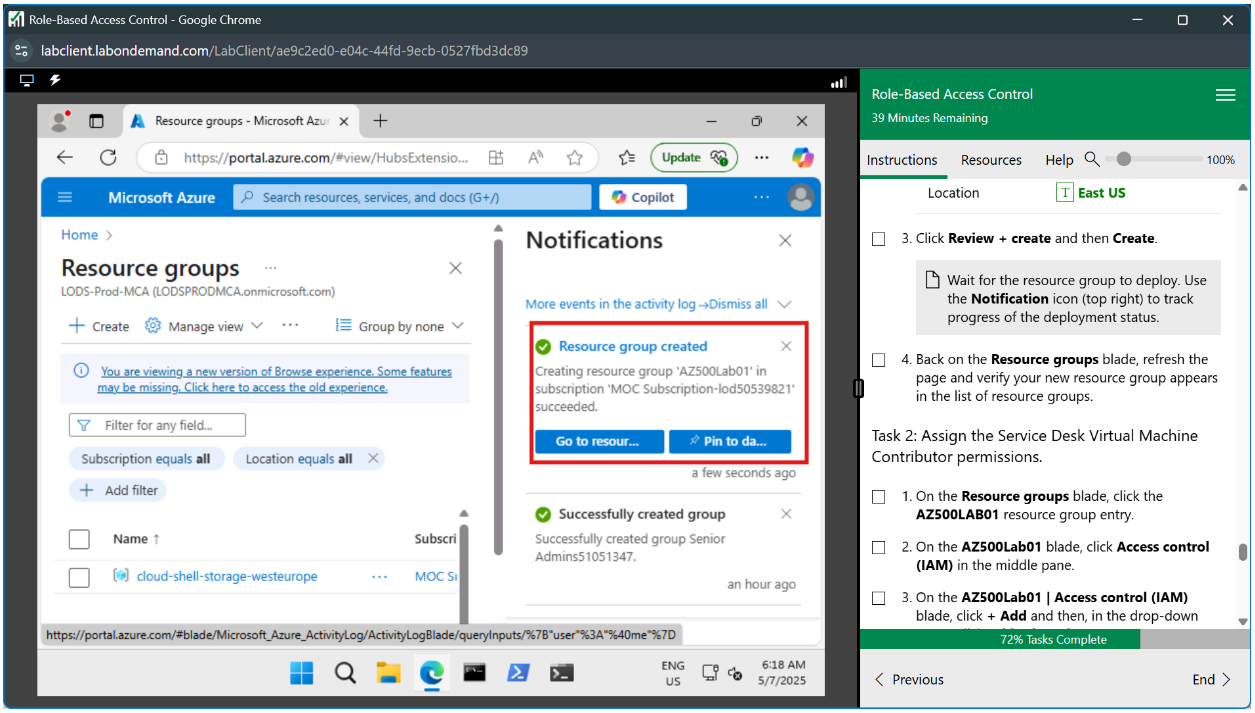
□ 1. In the Azure portal, in the **Search resources,**

68% Tasks Complete

< Previous End >

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

We first created a resource group as shown.


Role-Based Access Control - Google Chrome
labclient.labondemand.com/LabClient/ae9c2ed0-e04c-44fd-9ecb-0527fbd3dc89
Resource groups - Microsoft Azure
https://portal.azure.com/#view/HubsExtensio...
Update
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home >
+ Create
Manage view
Group by none
Filter for any field...
Subscription equals all
Location equals all
+ Add filter
Name ↑
Subscri
cloud-shell-storage-westeurope
MOC Si
More events in the activity log →Dismiss all
Go to resour...
Pin to da...
https://portal.azure.com/#blade/Microsoft_Azure_ActivityLog/ActivityLogBlade/queryInputs/%7B"user"%3A"%40me"%7D
ENG
US
6:18 AM
5/7/2025

Resource groups

LODS-Prod-MCA (LODSPRODMCA.onmicrosoft.com)

You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

Notifications

Resource group created

Creating resource group 'AZ500Lab01' in subscription 'MOC Subscription-lod50539821' succeeded.

a few seconds ago

Successfully created group

Successfully created group Senior Admins51051347.

an hour ago

Role-Based Access Control

39 Minutes Remaining

Instructions Resources Help 100%

Location **East US**

□ 3. 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.

□ 4. 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.

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

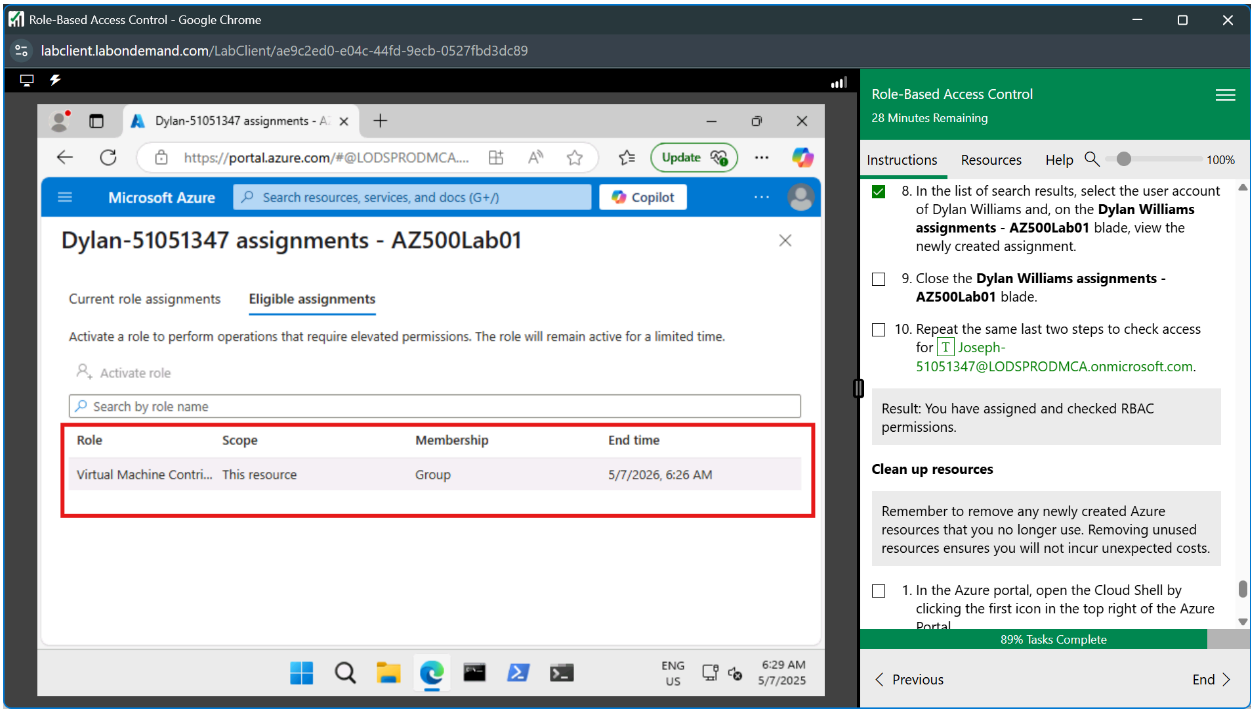
□ 2. On the **AZ500Lab01** blade, click **Access control (IAM)** in the middle pane.

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

72% Tasks Complete

< Previous End >

We then assigned the role to the service desk group. The user Dylan inherited the permission since he belongs to the assigned group.


Role-Based Access Control - Google Chrome
labclient.labondemand.com/LabClient/ae9c2ed0-e04c-44fd-9ecb-0527fbd3dc89
Dylan-51051347 assignments - A
https://portal.azure.com/#@LODSPRODMCA....
Update
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Current role assignments
Eligible assignments
Activate role
Search by role name
Role-Based Access Control
28 Minutes Remaining
Instructions
Resources
Help
100%
89% Tasks Complete
Previous
End
ENG
US
6:29 AM
5/7/2025

Dylan-51051347 assignments - AZ500Lab01

Activate a role to perform operations that require elevated permissions. The role will remain active for a limited time.

Role	Scope	Membership	End time
Virtual Machine Contri...	This resource	Group	5/7/2026, 6:26 AM

☑ 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 T Joseph-51051347@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.

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

Conclusion

To conclude, we have used Microsoft Entra ID to manage Identity by being able to create users, groups, and assign users to groups depending on their roles. As a best practice, we have assigned roles to groups that contain users who require the permissions accompanied in the roles to perform certain task for instance, the VM management role by the service desk group.