

**Fatma Omar Salim**

**Cloud Security Project 1**

**CyberSafe Foundation: CyberGirls 2.0**

**Demonstrating how to assign Role-Based Access Control in Azure**

**Objectives**

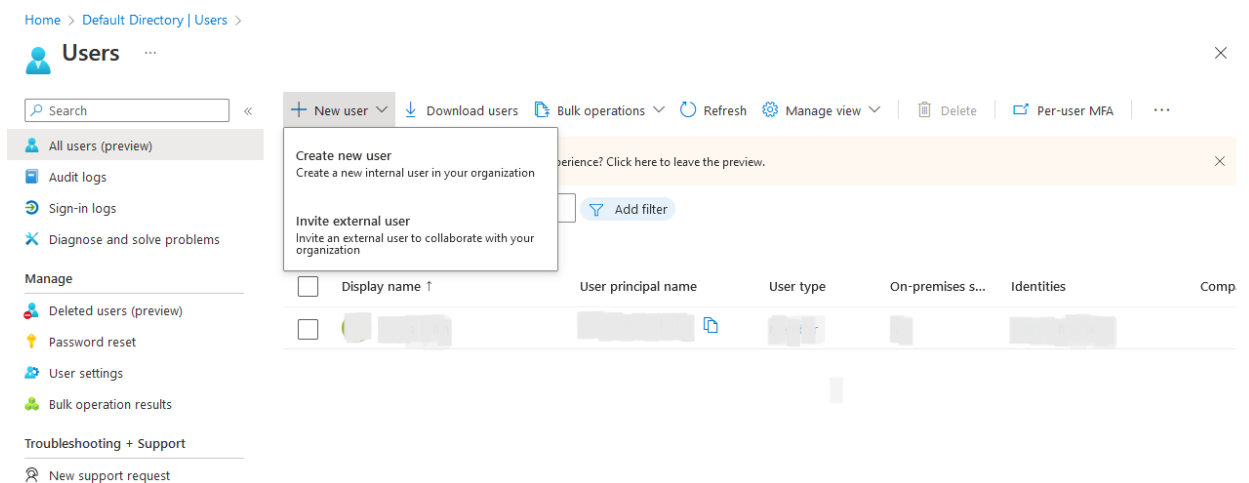
1. Create a Senior Admins group with Joseph Price as its member using the Azure Portal.
2. Create a Junior Admins group with Isabel Garcia as its member using Powershell.
3. Create a Service Desk group with Dylan Williams as its member using Azure CLI ( Command Line).
4. Assign the Virtual Machine Contributor role to the Service Desk group.

**Objective 1a : Creating the Senior Admins Group with the user Joseph as it member**

1. Sign into the Azure Portal via <https://portal.azure.com/>
2. In the **Search** tab, type **Azure Active Directory** and press **Enter**.



3. On the **Overview** blade of the Azure Active Directory under the **Manage** section, select **Users** and then select **+ New user** to add a new user.



4. Enter the user's details and click on Create. You will have to provide to the user his username and password and thus, you will have to note down his auto generated password which he will be using while signing in.

[Home](#) > [Default Directory | Users](#) > [Users](#) >

## New user

Default Directory

[Got feedback?](#)


### Select template

☒ **Create user**  
Create a new user in your organization.

☐ **Invite user**  
Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.  
[Help me decide](#)

### Identity

User name \* ⓘ

Joseph ✓@fatmasalimriarauniversity...   
The domain name I need isn't shown here

Name \* ⓘJoseph Price ✓

First nameJoseph ✓

Last namePrice ✓

### Password

☒ Auto-generate password

☐ Let me create the password

Initial password

\*\*\*\*\*

☐ Show Password

### Groups and roles

Groups0 groups selected

RolesUser

### Settings

Block sign in

YesNo

Usage location

▼

### Job info

Job title

Department

Create

Create

5. Refresh the web page and the new user created will appear on the users dashboard.

Home > **Users** ...

Search

+ New user Download users Bulk operations Refresh Manage view Delete Per-user MFA

All users (preview)

Audit logs

Sign-in logs

Diagnose and solve problems

Manage

Deleted users (preview)

Password reset

User settings

Bulk operation results

Troubleshooting + Support

New support request

Want to switch back to the legacy users list experience? Click here to leave the preview.

Search Add filter

2 users found

<input type="checkbox"/>	Display name ↑	User principal name	User type	On-premises s...	Identities	Comp
<input type="checkbox"/>	FS Fatma Salim		Member	No	MicrosoftAccount	
<input type="checkbox"/>	JP Joseph Price		Member	No		

## Objective 1b: Creating a Senior Admins Group and adding Joseph Price to it.

1. In the **Manage** section of the ADD, click on **Groups** and then select **+ New group**.

Home > Default Directory | Groups >

**Groups | All groups** ...

Default Directory - Azure Active Directory

All groups

Deleted groups

Diagnose and solve problems

Settings

General

Expiration

Naming policy

Activity

Privileged access groups (Preview)

Access reviews

Audit logs

Bulk operation results

Troubleshooting + Support

New support request

+ New group Download groups Refresh Manage view Delete Got feedback?

Search Add filter

Search mode Contains

0 groups found

<input type="checkbox"/>	Name ↑	Object Id	Group type	Membership t
No results.				

2. Enter the group details and click on **Create**. Before you create, make sure you add Joseph Price as both owner and a member of the group.

## New Group ...



Got feedback?

Group type \* ⓘ

Security

Group name \* ⓘ

Senior Admins

Group description ⓘ

Enter a description for the group

Membership type ⓘ

Assigned

Owners

1 owner selected

Members

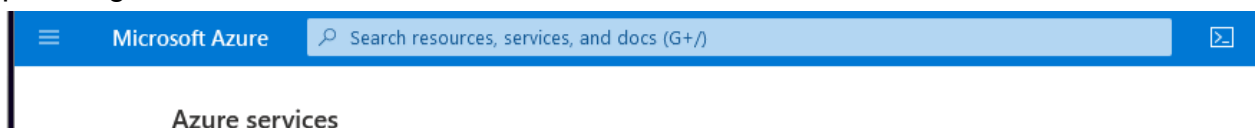
1 member selected

Create

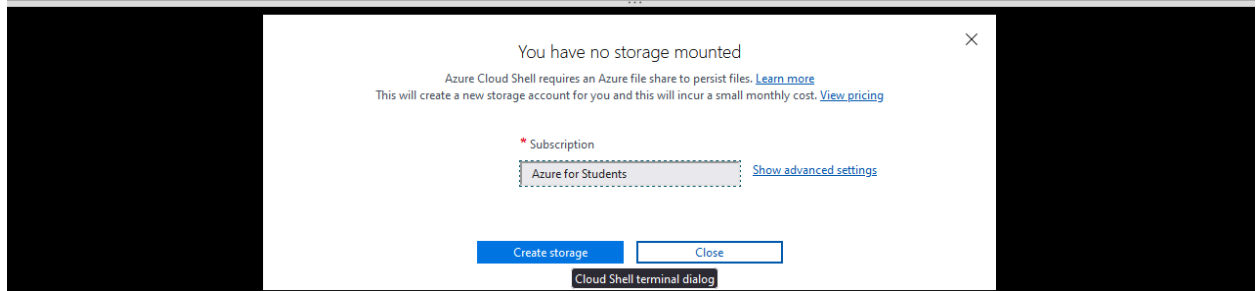
Create

### Objective 2a : Creating the Junior Admins group with Isabel Garcia as its member using Powershell.

1. Open the Cloud Shell by clicking the first icon in the top right corner of the Azure portal right after the Search Tab.



2. The Azure Cloud Shell will pop up on the bottom of the screen. Click on **Powershell** and **create storage**.



3. The first code creates a password profile object.  
`$passwordProfile = New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile`
4. The second code runs a set of values of the password within the profile object.  
`$passwordProfile.Password = "Pa55w.rd1234"`
5. The third code connects to Azure Active Directory.  
`Connect-AzureAD`
6. The fourth code identifies the name of the Azure AD tenant.  
`$domainName = ((Get-AzureAdTenantDetail).VerifiedDomains)[0].Name`
7. The fifth code creates a user account for Isabel Garcia.  
`New-AzureADUser -DisplayName 'Isabel Garcia' -PasswordProfile $passwordProfile -UserPrincipalName "Isabel@$domainName" -AccountEnabled $true -MailNickName 'Isabel'`
8. The last code lists Azure AD users showing both Joseph's and Isabel's.  
`Get-AzureADUser`

```
PowerShell ▾ ? ⚙️ 📄 {} 🔍
```

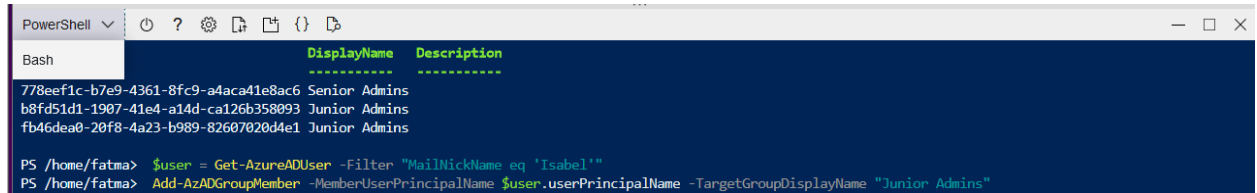
```
Requesting a Cloud Shell.Succeeded.  
Connecting terminal...  
  
Welcome to Azure Cloud Shell  
  
Type "az" to use Azure CLI  
Type "help" to learn about Cloud Shell  
  
MOTD: Switch to Bash from PowerShell: bash  
  
VERBOSE: Authenticating to Azure ...  
VERBOSE: Building your Azure drive ...  
PS /home/fatma> $passwordProfile = New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile  
PS /home/fatma> $passwordProfile.Password = "Pa5$w.rd1234"  
PS /home/fatma> Connect-AzureAD  
PS /home/fatma> $domainName = ((Get-AzureADTenantDetail).VerifiedDomains)[0].Name  
PS /home/fatma> New-AzureADUser -DisplayName 'Isabel Garcia' -PasswordProfile $passwordProfile -UserPrincipalName "Isabel@$domainName" -AccountEnabled $true  
ountEnabled $true New-AzureADUser -DisplayName 'Isabel Garcia' -PasswordProfile $passwordProfile -UserPrincipalName "Isabel@$domainName" -AccountEnabled $true  
ountEnabled $t New-AzureADUser -DisplayName 'Isabel Garcia' -PasswordProfile $passwordProfile -UserPrincipalName "Isabel@$domainName" -AccountEnabled $true  
ountEnabled $tru New-AzureADUser -DisplayName 'Isabel Garcia' -PasswordProfile $passwordProfile -UserPrincipalName "Isabel@$domainName" -AccountEnabled $true  
ountEnabled $str New-AzureADUser -DisplayName 'Isabel Garcia' -PasswordProfile $passwordProfile -UserPrincipalName "Isabel@$domainName" -AccountEnabled $true  
ountEnabled $str New-AzureADUser -DisplayName 'Isabel Garcia' -PasswordProfile $passwordProfile -UserPrincipalName "Isabel@$domainName" -AccountEnabled $true  
ountEnabled $str New-AzureADUser -DisplayName 'Isabel Garcia' -PasswordProfile $passwordProfile -UserPrincipalName "Isabel@$domainName" -AccountEnabled $true  
ountEnabled $st New-AzureADUser -DisplayName 'Isabel Garcia' -PasswordProfile $passwordProfile -UserPrincipalName "Isabel@$domainName" -AccountEnabled $true  
ountEnabled $true -MailNickName 'Isabel'  
  
-----  
ObjectID DisplayName UserPrincipalName UserType  
-----  
812bc9f5-fcb0-4a09-a315-3c652d82a3ae Isabel Garcia Isabel@fatmasalimriarauniversityac.onmicrosoft.com Member  
  
PS /home/fatma> Get-AzureADUser  
  
-----  
ObjectID DisplayName UserPrincipalName UserType  
-----  
6bcd24a9-d54d-4fa7-afaa-3dfc27374cdb Fatma Salim fatma.salim_riarauniversity.ac.ke#EXT#@fatmasalimriarauniversityac.onmicrosoft.com Member  
812bc9f5-fcb0-4a09-a315-3c652d82a3ae Isabel Garcia Isabel@fatmasalimriarauniversityac.onmicrosoft.com Member  
f539dd82-ce2c-4624-bb13-de6895487d66 Joseph Price Joseph@fatmasalimriarauniversityac.onmicrosoft.com Member  
  
PS /home/fatma>
```

## Objective 2b: Creating The Junior Admins group and adding Isabel Garcia to it using Powershell.

1. The first code creates a new security group named Junior Admin.  
New-AzureADGroup -DisplayName 'Junior Admins' -MailEnabled \$false  
-SecurityEnabled \$true -MailNickName JuniorAdmins
2. The second code lists the groups in your Azure AD tenant.  
Get-AzureADGroup
3. The third code obtains a reference to the user account of Isabel Garcia.  
\$user = Get-AzureADUser -Filter "MailNickName eq 'Isabel'"
4. The fourth code adds the user account of Isabel to the Junior Admins group.  
Add-AzADGroupMember -MemberUserPrincipalName \$user.userPrincipalName  
-TargetGroupDisplayName "Junior Admins"
5. The last code verifies that the Junior Admins group contains the user account of Isabel.

## Objective 3a : Creating a Service Desk group and adding Dylan Williams to it using Azure CLI.

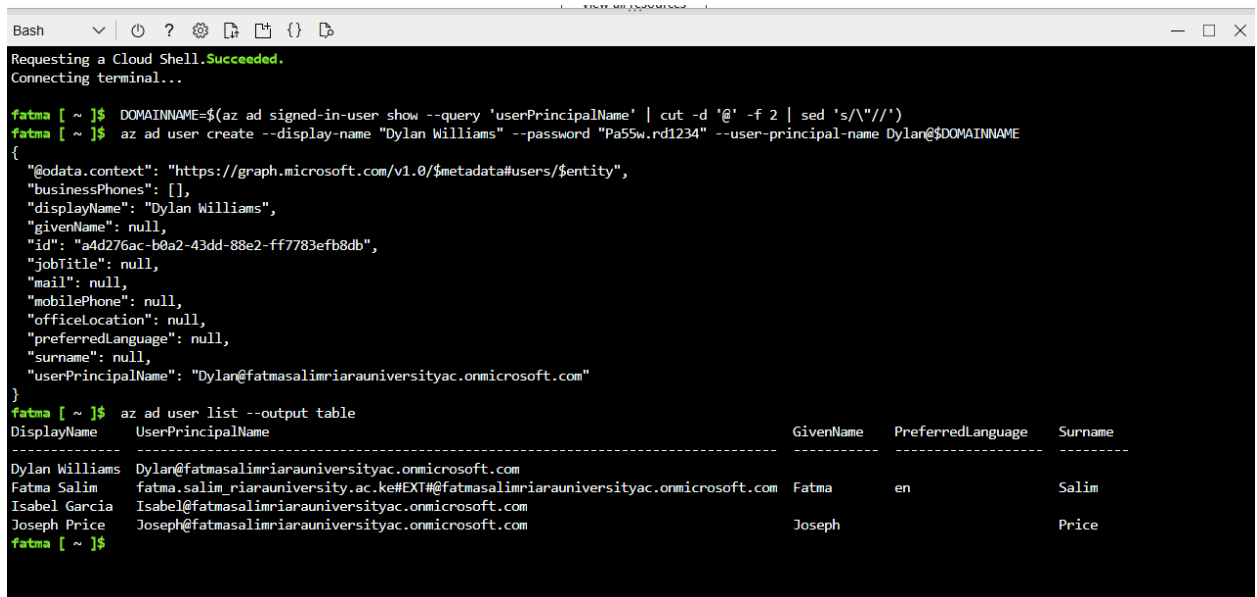
1. On the top of the Powershell tab, click on it and switch to Bash.



```
PowerShell
Bash
    DisplayName      Description
    -----
778eef1c-b7e9-4361-8fc9-a4aca41e8ac6 Senior Admins
b8fd51d1-1907-41e4-a14d-ca126b358093 Junior Admins
fb46dea0-20f8-4a23-b989-826070204e1 Junior Admins

PS /home/fatma> $user = Get-AzureADUser -Filter "MailNickName eq 'Isabel'"
PS /home/fatma> Add-AzADGroupMember -MemberUserPrincipalName $user.userPrincipalName -TargetGroupDisplayName "Junior Admins"
```

2. Run the following code to identify the name of your Azure AD Tenant.  
DOMAINNAME=\$(az ad signed-in-user show --query 'userPrincipalName' | cut -d '@' -f 2 | sed 's/\//')
3. Run the following to create a Dylan William's user.  
az ad user create --display-name "Dylan Williams" --password "Pa55w.rd1234" --user-principal-name Dylan@\$DOMAINNAME
4. Run the following code to list Azure AD user accounts.  
az ad user list --output table



```
Bash
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

fatma [ ~ ]$ DOMAINNAME=$(az ad signed-in-user show --query 'userPrincipalName' | cut -d '@' -f 2 | sed 's/\//')
fatma [ ~ ]$ az ad user create --display-name "Dylan Williams" --password "Pa55w.rd1234" --user-principal-name Dylan@$DOMAINNAME
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users/$entity",
  "businessPhones": [],
  "displayName": "Dylan Williams",
  "givenName": null,
  "id": "a4d276ac-b0a2-43dd-88e2-ff7783efb8db",
  "jobTitle": null,
  "mail": null,
  "mobilePhone": null,
  "officeLocation": null,
  "preferredLanguage": null,
  "surname": null,
  "userPrincipalName": "Dylan@fatmasalimriarauniversityac.onmicrosoft.com"
}
fatma [ ~ ]$ az ad user list --output table
DisplayName      UserPrincipalName
-----
Dylan Williams  Dylan@fatmasalimriarauniversityac.onmicrosoft.com
Fatma Salim     fatma.salim_riarauniversity.ac.ke#EXT#@fatmasalimriarauniversityac.onmicrosoft.com
Isabel Garcia   Isabel@fatmasalimriarauniversityac.onmicrosoft.com
Joseph Price    Joseph@fatmasalimriarauniversityac.onmicrosoft.com

fatma [ ~ ]$
```

DisplayName	UserPrincipalName	GivenName	PreferredLanguage	Surname
Dylan Williams	Dylan@fatmasalimriarauniversityac.onmicrosoft.com			
Fatma Salim	fatma.salim_riarauniversity.ac.ke#EXT#@fatmasalimriarauniversityac.onmicrosoft.com	Fatma	en	Salim
Isabel Garcia	Isabel@fatmasalimriarauniversityac.onmicrosoft.com			
Joseph Price	Joseph@fatmasalimriarauniversityac.onmicrosoft.com	Joseph		Price

## Objective 3b : Creating the Service Desk group and adding Dylan to it.

1. Run the following code to create a new security group named Service Desk.

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

2. Run the following code to list the Azure AD groups.  
az ad group list -o table
3. Run the following to obtain a reference to the user account of Dylan Williams  
USER=\$(az ad user list --filter "displayname eq 'Dylan Williams'")
4. Run the following code to obtain the objectId property of the user account of Dylan Williams.  
OBJECTID=\$(echo \$USER | jq '.[].id' | tr -d '"')
5. Run the following code to add the user account of Dylan to the Service Desk group.  
az ad group member add --group "Service Desk" --member-id \$OBJECTID
6. Run the following codes to list members of the Service Desk group.  
az ad group member list --group "Service Desk"

```
Bash
"proxyAddresses": [],
"renewedDateTime": "2022-09-15T19:07:40Z",
"resourceBehaviorOptions": [],
"resourceProvisioningOptions": [],
"securityEnabled": true,
"securityIdentifier": "S-1-12-1-461909565-1274687906-2365489291-441859219",
"theme": null,
"visibility": null
}
fatma [ ~ ]$ az ad group list -o table
CreatedDateTime  DisplayName  MailEnabled  MailNickname  RenewedDateTime  SecurityEnabled  SecurityIdentifier
-----
2022-09-15T19:07:40Z  Service Desk  False  ServiceDesk  2022-09-15T19:07:40Z  True  S-1-12-1-461909565-1274687906-2365489291-441859219
2022-09-15T17:57:02Z  Senior Admins  False  95c3b215-9  2022-09-15T17:57:02Z  True  S-1-12-1-2005856028-1130477545-2896480655-3330940580
2022-09-15T18:41:19Z  Junior Admins  False  JuniorAdmins  2022-09-15T18:41:19Z  True  S-1-12-1-3103609297-1105467655-315248033-2474653035
2022-09-15T18:47:57Z  Junior Admins  False  JuniorAdmins  2022-09-15T18:47:57Z  True  S-1-12-1-4215725728-1243816184-1619167673-3788775536
fatma [ ~ ]$ USER=$(az ad user list --filter "displayname eq 'Dylan Williams'")
fatma [ ~ ]$ OBJECTID=$(echo $USER | jq '.[].id' | tr -d '"')
fatma [ ~ ]$ az ad group member add --group "Service Desk" --member-id $OBJECTID
fatma [ ~ ]$ az ad group member list --group "Service Desk"
[
  {
    "@odata.type": "#microsoft.graph.user",
    "businessPhones": [],
    "displayName": "Dylan Williams",
    "givenName": null,
    "id": "a4d276ac-b0a2-43dd-88e2-ff7783efb8db",
    "jobTitle": null,
    "mail": null,
    "mobilePhone": null,
    "officeLocation": null,
    "preferredLanguage": null,
    "surname": null,
    "userPrincipalName": "Dylan@fatmasalimriarauniversityac.onmicrosoft.com"
  }
]
fatma [ ~ ]$
```



## Objective 4 : Assigning the Virtual Machine Contributor role to the Service Desk group.

1. In the **Search** tab, type **Resource groups** and press **Enter**.



2. Click + **Create**, enter group details and **review** and **create**.

A screenshot of the "Create a resource group" form in the Microsoft Azure portal. The form is titled "Create a resource group" and has a close button (X) in the top right corner. It has three tabs: "Basics", "Tags", and "Review + create". The "Basics" tab is selected. Below the tabs is a description of a resource group: "Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)". Below the description are two sections: "Project details" and "Resource details". The "Project details" section has two fields: "Subscription" (a dropdown menu with "Azure for Students" selected) and "Resource group" (a text input field with "AZ500IAB01" entered and a green checkmark icon). The "Resource details" section has one field: "Region" (a dropdown menu with "(US) East US" selected). At the bottom of the form is a "Review + create" button. Below this button are three buttons: "Review + create", "< Previous", and "Next : Tags >".

3. Click on the **AZ500IAB01** resource group entry.

- On the **AZ500IAB01** blade pane, click the **Access Control (IAM)** in the middle pane.

The screenshot displays the Azure portal interface. On the left, the 'Resource groups' blade is active, showing a list of resource groups under the 'Default Directory (fatmasalimriarauniversityac.on...)'. The resource group 'AZ500IAB01' is selected and highlighted. To the right, the 'AZ500IAB01' blade is open, showing a search bar and a list of menu items. The 'Access control (IAM)' item is highlighted in the middle pane. Below the menu items, there is a 'Settings' section with links to 'Deployments', 'Security', 'Policies', and 'Properties'.

Home > Resource groups >

## Resource groups

Default Directory (fatmasalimriarauniversityac.on...)

+ Create ⚙️ Manage view ▾ ⋮

Filter for any field...

Name ↑↓

- AZ500IAB01 ...
- cloud-shell-storage-west europe ...

**AZ500IAB01** ⚙️ ☆

Resource group

Search

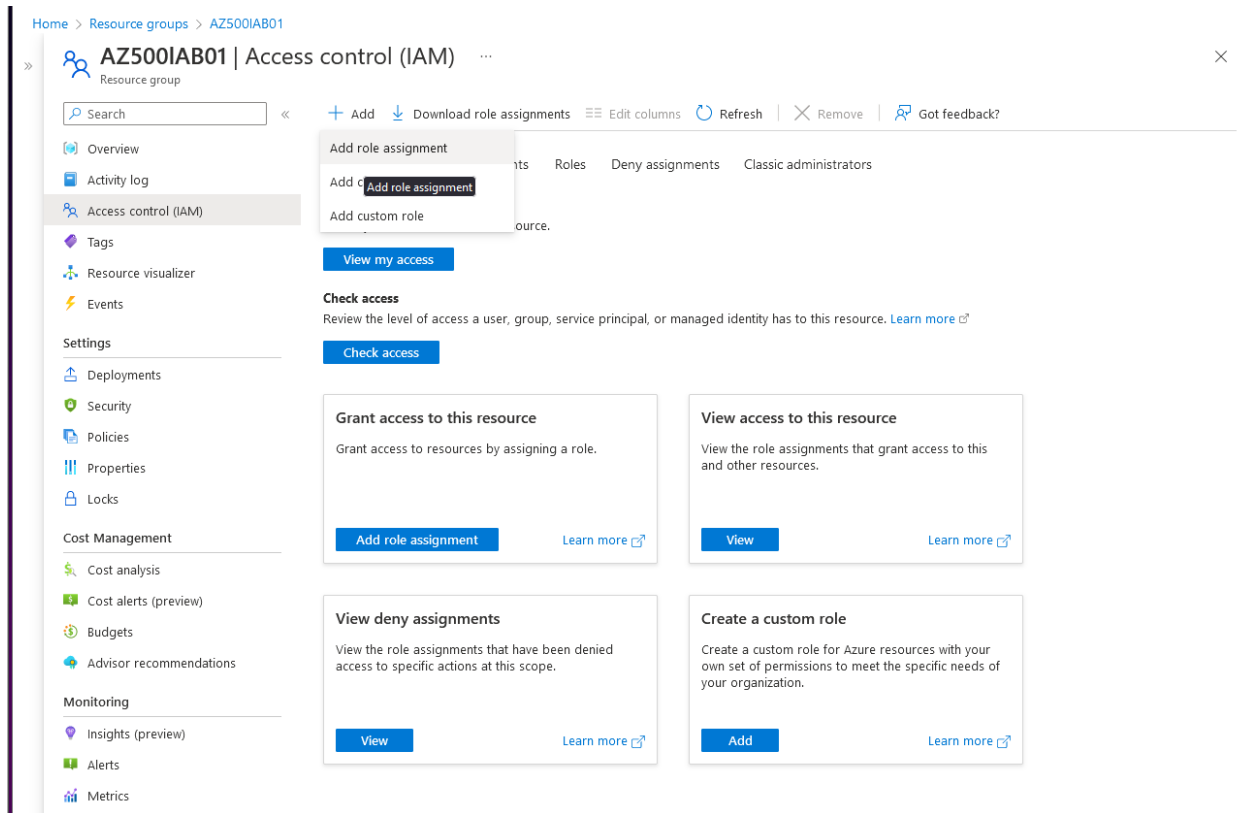
Overview

- Activity log
- Access control (IAM)**
- Tags
- Resource visualizer
- Events

Settings

- Deployments
- Security
- Policies
- Properties


- Click **+Add** and then, in the drop down menu, click on **Add role assignment**.



6. Add details as follows: type in the role search tab, '**Virtual Machine Contributor**', assign access to '**User, group, or service principal**' and add Service Desk as a member and click on **Review + assign** twice to assign the role.

Home > Resource groups > AZ500IAB01 | Access control (IAM) >

## Add role assignment ...

 Got feedback?


---

[Role](#) [Members](#) [Review + assign](#)

**Selected role** Virtual Machine Contributor

**Assign access to** ☒ User, group, or service principal  
☐ Managed identity

**Members** [+ Select members](#)

Name	Object ID	Type	
Service Desk	1b882e3d-31a2-4bfa-8b80-fe8c933c561a	Group	

**Description**

Optional

[Review + assign](#) [Previous](#) [Next](#)

<https://portal.azure.com/#>

- From the **Access Control** blade, select **Role assignments**.
- On the **AZ500IAB01 | Access Control (IAM)** blade, on the **Check access** tab, search tab, type **Dylan Williams**.

