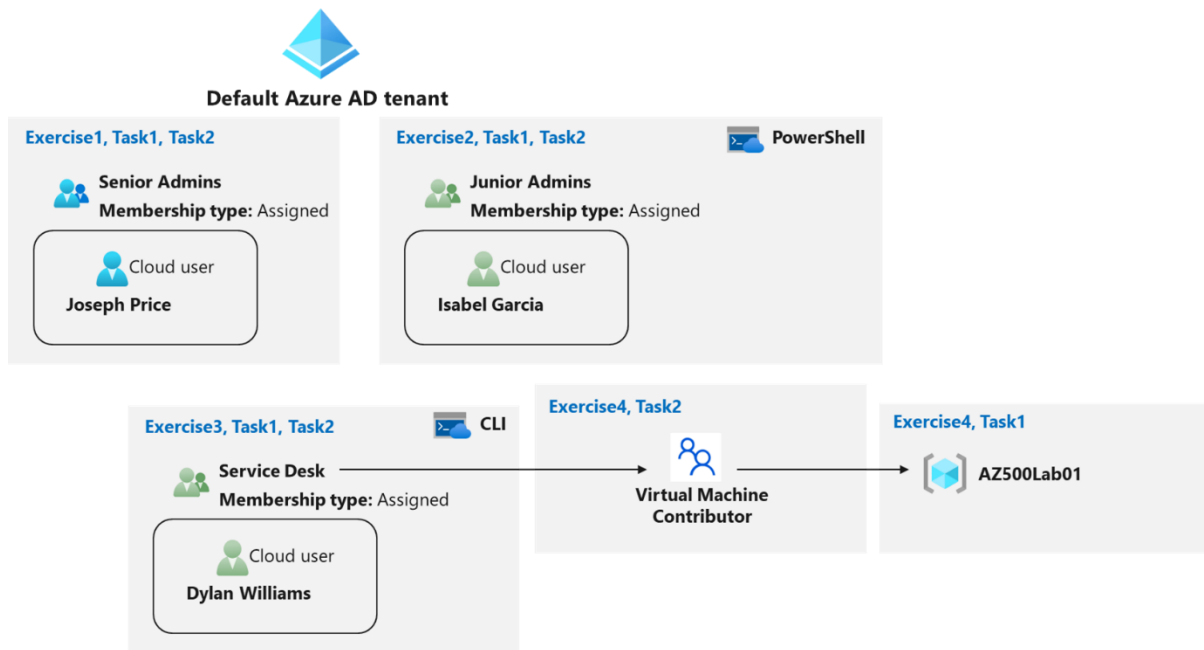


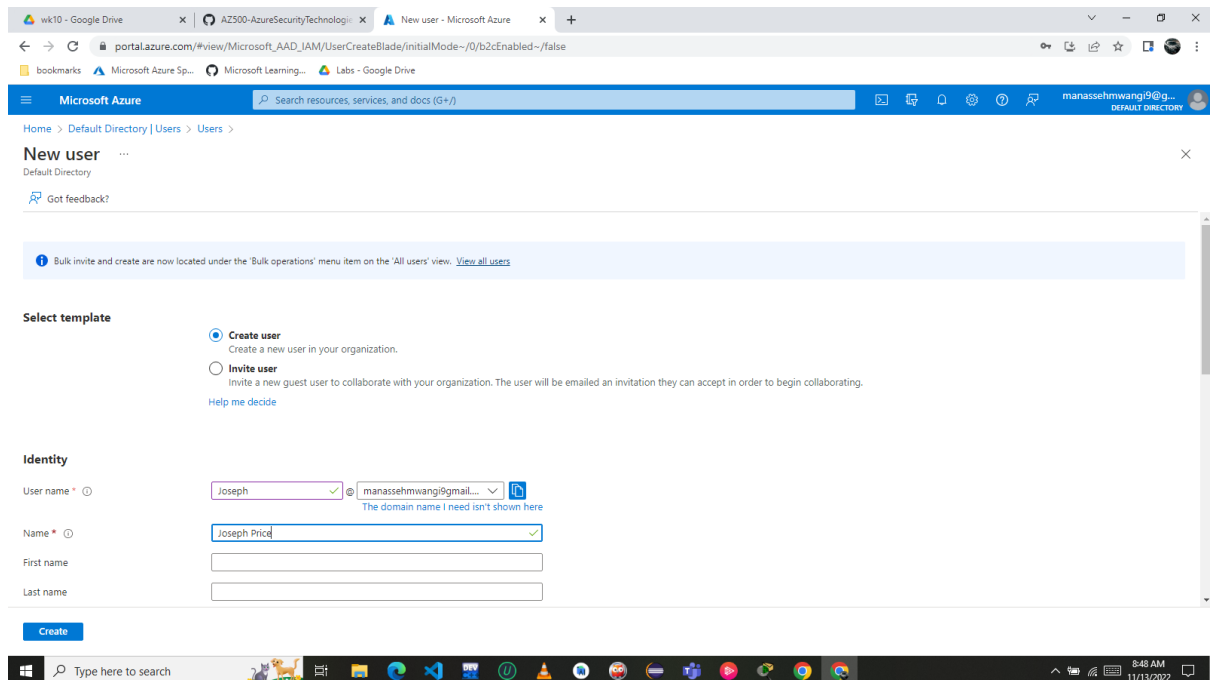
Lab 01: Role-Based Access Control

Architecture diagram



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

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



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

In this task, you will create the *Senior Admins* group, add the user account of Joseph Price to the group, and configure it as the group owner.

Microsoft Azure

Home > Default Directory | Groups > Groups | All groups >

New Group

Got feedback?

Group type *

Group name *

Group description

Azure AD roles can be assigned to the group ☐ Yes ☐ No

Membership type *

Owners
1 owner selected

Members
1 member selected

Create

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

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

Azure services

Create a resource Azure Active Directory Management groups Resource groups Virtual machines Application gateways Virtual networks Load balancers Route tables More services

PowerShell

```
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/manasseh> $passwordProfile = New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile
PS /home/manasseh> $passwordProfile.Password = "Pa5$w.rd1234"
PS /home/manasseh> Connect-AzureAD
PS /home/manasseh> $domainName = ((Get-AzureADTenantDetail).VerifiedDomains)[0].Name
PS /home/manasseh> New-AzureADUser -DisplayName 'Isabel Garcia' -PasswordProfile $passwordProfile -UserPrincipalName 'Isabel@domainName' -AccountEnabled $true -MailNickName 'Isabel'

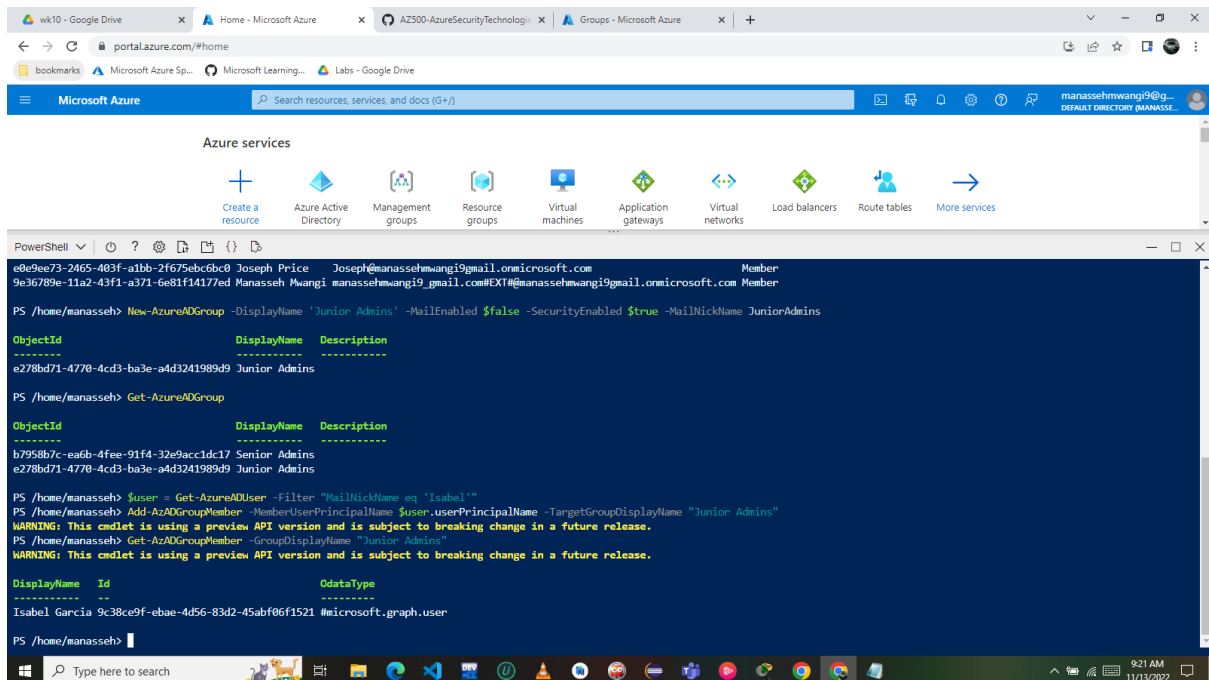
ObjectID          DisplayName      UserPrincipalName      UserType
-----
9c38ce9f-ebae-4d56-83d2-45abf06f1521 Isabel Garcia Isabel@manassehwwangi9mail.onmicrosoft.com Member

PS /home/manasseh> Get-AzureADUser

ObjectID          DisplayName      UserPrincipalName      UserType
-----
9c38ce9f-ebae-4d56-83d2-45abf06f1521 Isabel Garcia Isabel@manassehwwangi9mail.onmicrosoft.com Member
e0e9ee73-2465-483f-a1bb-2f675ebc6bc0 Joseph Price Joseph@manassehwwangi9mail.onmicrosoft.com Member
9e36789e-11a2-43f1-a371-6e81f14177ed Manasseh Mwangi manassehwwangi9_gmail.com#EXT#@manassehwwangi9mail.onmicrosoft.com Member

PS /home/manasseh>
```

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



```
PS /home/manasseh> New-AzureADGroup -DisplayName 'Junior Admins' -MailEnabled $false -SecurityEnabled $true -MailNickName JuniorAdmins

ObjectID      DisplayName  Description
-----
e278bd71-4770-4cd3-ba3e-a4d3241989d9 Junior Admins

PS /home/manasseh> Get-AzureADGroup

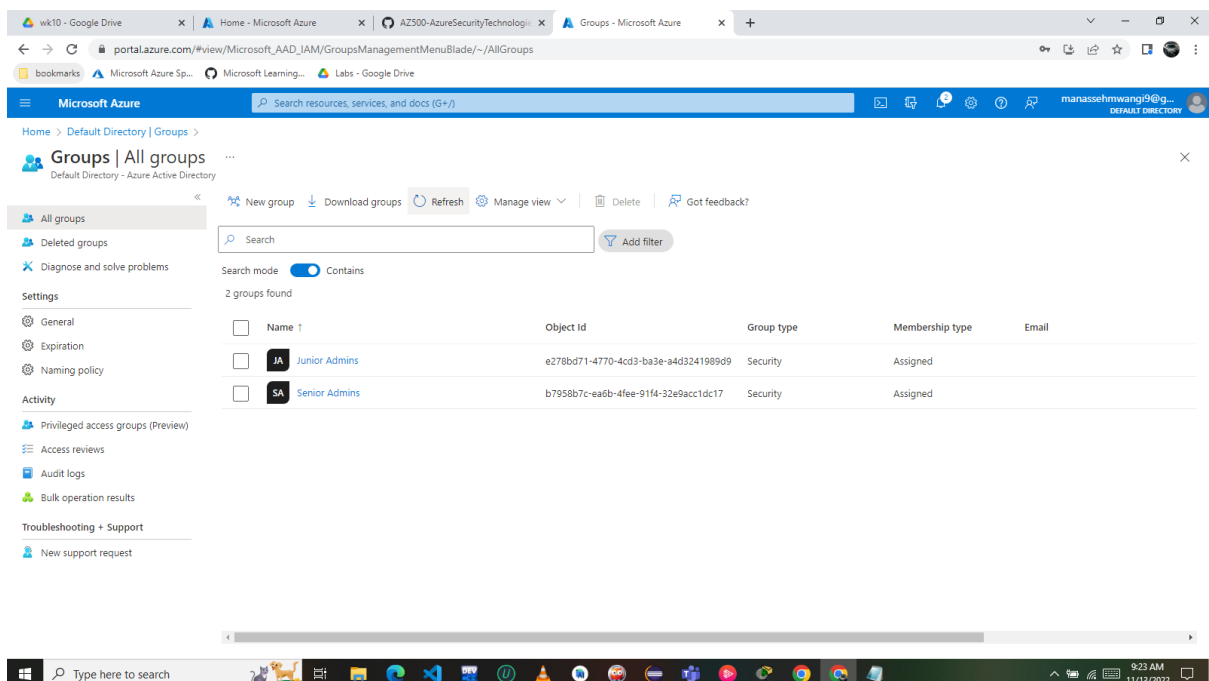
ObjectID      DisplayName  Description
-----
b7958b7c-ea6b-4fee-91f4-32e9acc1dc17 Senior Admins
e278bd71-4770-4cd3-ba3e-a4d3241989d9 Junior Admins

PS /home/manasseh> $user = Get-AzureADUser -Filter "MailNickName eq 'Isabel'"
PS /home/manasseh> Add-AzureADGroupMember -MemberUserPrincipalName $user.userPrincipalName -TargetGroupDisplayName "Junior Admins"
WARNING: This cmdlet is using a preview API version and is subject to breaking change in a future release.
PS /home/manasseh> Get-AzureADGroupMember -GroupDisplayName "Junior Admins"
WARNING: This cmdlet is using a preview API version and is subject to breaking change in a future release.

DisplayName  Id                                     OdataType
-----
Isabel Garcia 9c38ce9f-ebae-4d56-83d2-45abf06f1521 #microsoft.graph.user

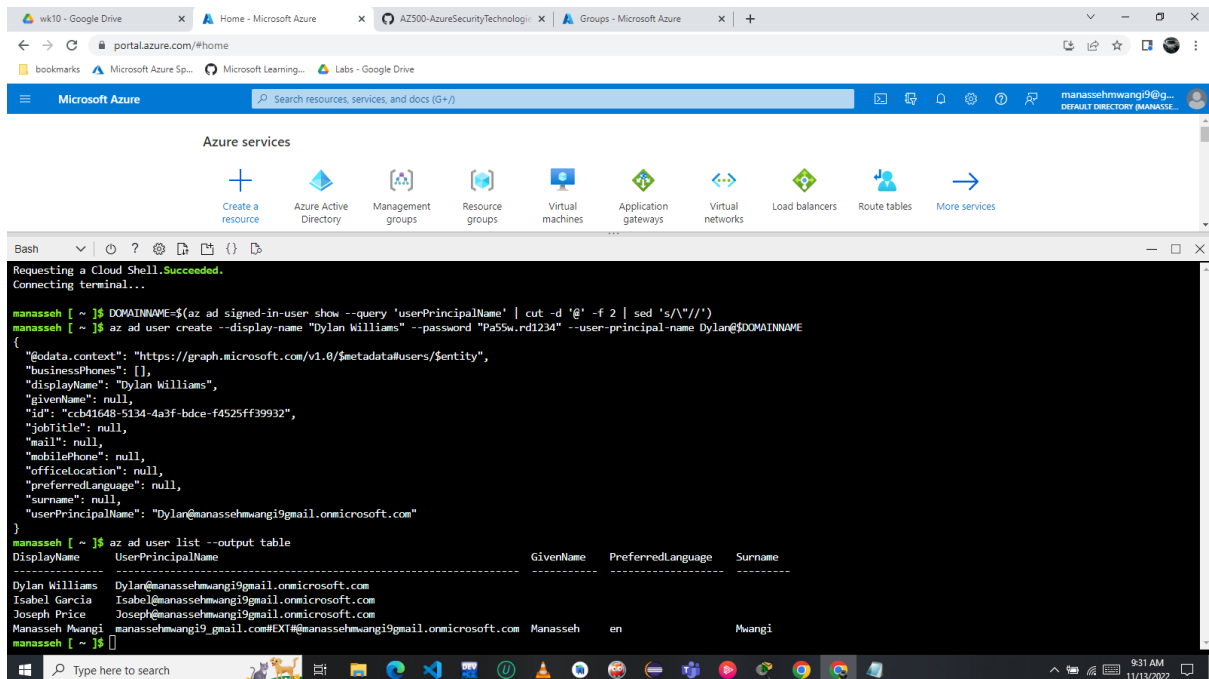
PS /home/manasseh>
```

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.

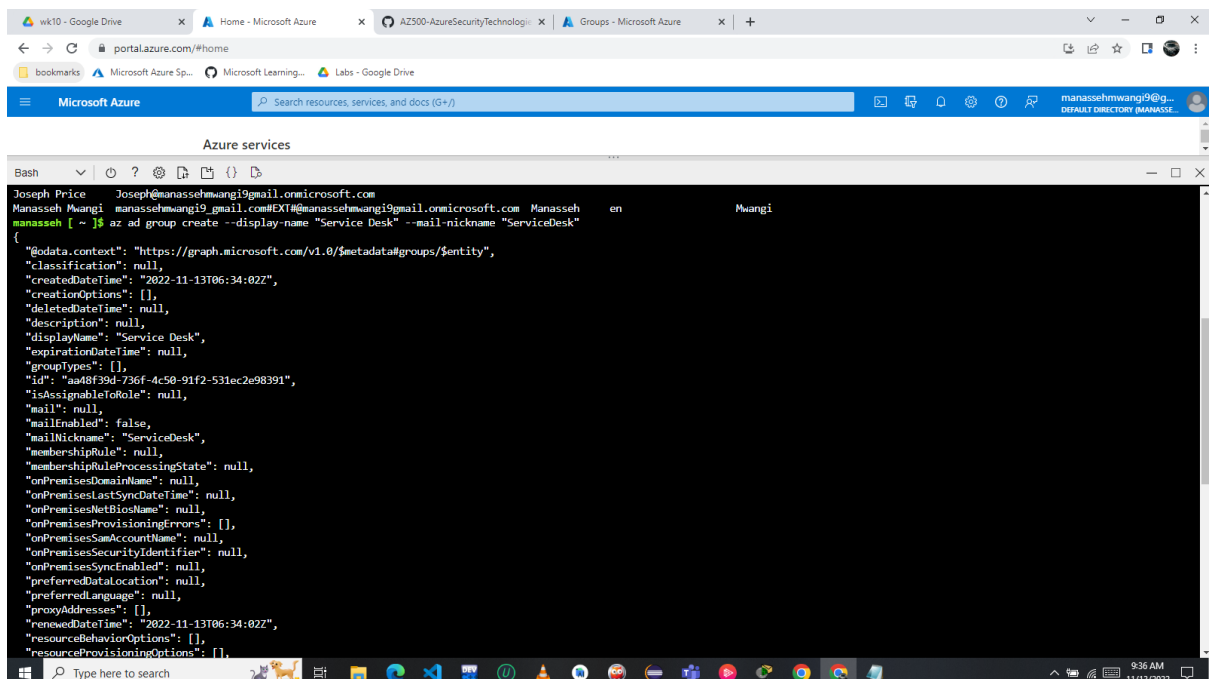
Task 1: Use Azure CLI to create a user account for Dylan Williams.



The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with the Microsoft Azure logo and a search bar. Below the navigation bar, there's a section for "Azure services" with various icons for different services. In the center, there's a terminal window titled "Bash" with the following commands and output:

```
manasseh [ ~ ]$ 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": "ccb41648-5134-4a3f-bdce-f4525ff39932",
  "jobTitle": null,
  "mail": null,
  "mobilePhone": null,
  "officeLocation": null,
  "preferredLanguage": null,
  "surname": null,
  "userPrincipalName": "Dylan@manassehwmangi9gmail.onmicrosoft.com"
}
manasseh [ ~ ]$ az ad user list --output table
DisplayName      UserPrincipalName      GivenName  PreferredLanguage  Surname
-----
Dylan Williams   Dylan@manassehwmangi9gmail.onmicrosoft.com
Isabel Garcia    Isabel@manassehwmangi9gmail.onmicrosoft.com
Joseph Price     Joseph@manassehwmangi9gmail.onmicrosoft.com
Manasseh Mwangi  manassehwmangi9_gmail.com#EXT#@manassehwmangi9gmail.onmicrosoft.com  Manasseh   en                Mwangi
```

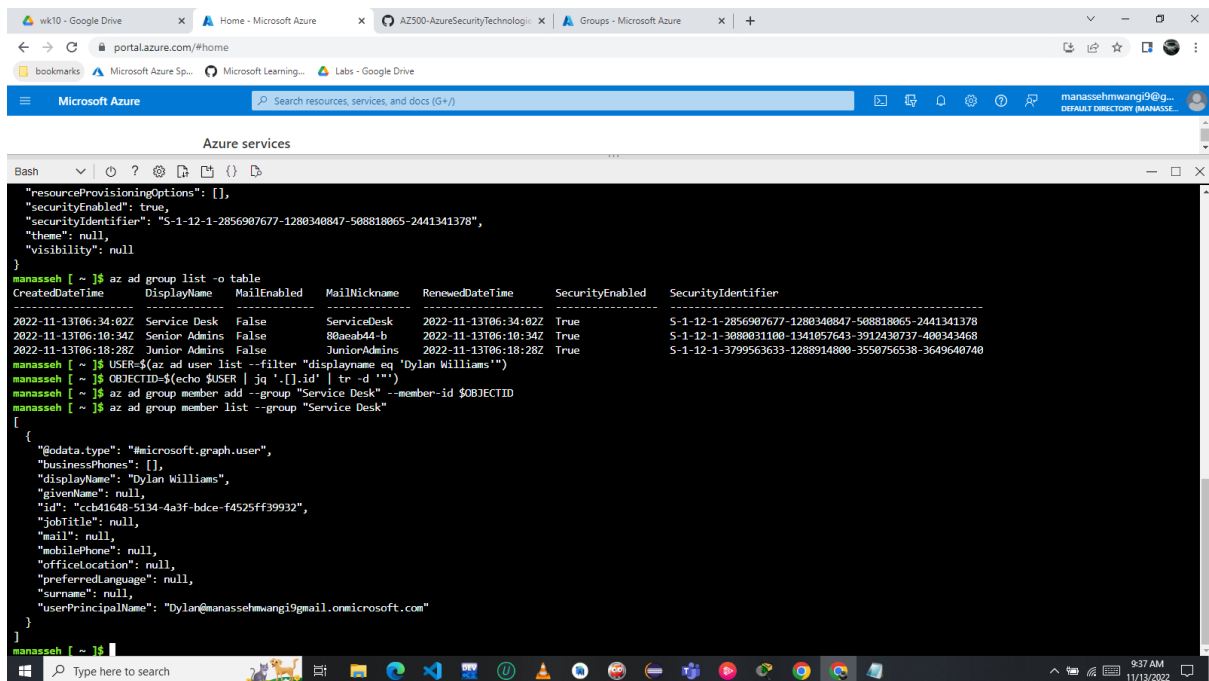
Task 2: Use Azure CLI to create the Service Desk group and add the user account of Dylan to the group.



The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with the Microsoft Azure logo and a search bar. Below the navigation bar, there's a section for "Azure services" with various icons for different services. In the center, there's a terminal window titled "Bash" with the following commands and output:

```
manasseh [ ~ ]$ az ad group create --display-name "Service Desk" --mail-nickname "ServiceDesk"
{
  "odata.context": "https://graph.microsoft.com/v1.0/$metadata#groups/$entity",
  "classification": null,
  "createdDateTime": "2022-11-13T06:34:02Z",
  "creationOptions": [],
  "deletedDateTime": null,
  "description": null,
  "displayName": "Service Desk",
  "expirationDateTime": null,
  "groupTypes": [],
  "id": "aa48f39d-736f-4c50-91f2-531ec2e98391",
  "isAssignableToRole": null,
  "mail": null,
  "mailEnabled": false,
  "mailNickname": "ServiceDesk",
  "membershipRule": null,
  "membershipRuleProcessingState": null,
  "onPremisesDomainName": null,
  "onPremisesLastSyncDateTime": null,
  "onPremisesNetBiosName": null,
  "onPremisesProvisioningErrors": [],
  "onPremisesSecurityIdentifier": null,
  "onPremisesSyncEnabled": null,
  "preferredDataLocation": null,
  "preferredLanguage": null,
  "proxyAddresses": [],
  "renewedDateTime": "2022-11-13T06:34:02Z",
  "resourceBehaviorOptions": [],
  "resourceProvisioningOptions": []
}
```

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

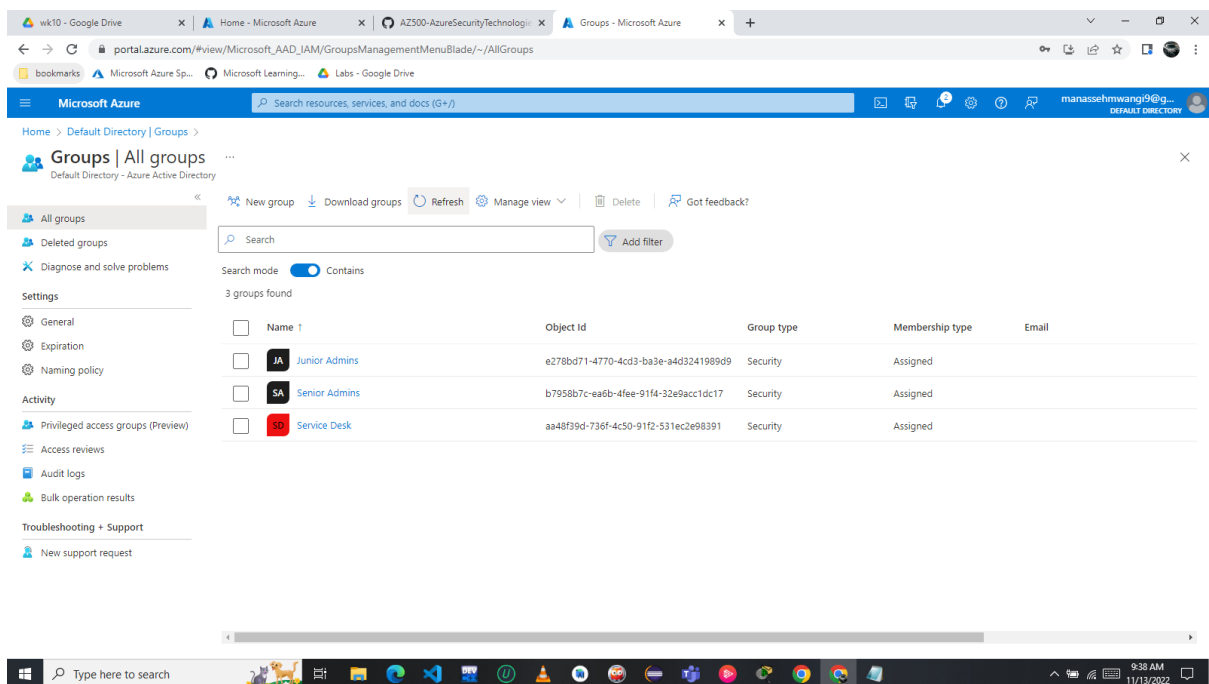


```
manasseh [ ~ ]$ az ad group list -o table
manasseh [ ~ ]$ az ad user list --filter "displayname eq 'Dylan Williams'"
manasseh [ ~ ]$ az ad group member add --group "Service Desk" --member-id $OBJECTID
manasseh [ ~ ]$ az ad group member list --group "Service Desk"
```

CreatedDateTime	DisplayName	MailEnabled	MailNickname	RenewedDateTime	SecurityEnabled	SecurityIdentifier
2022-11-13T06:34:02Z	Service Desk	False	ServiceDesk	2022-11-13T06:34:02Z	True	5-1-12-1-2856907677-1280340847-508818065-2441341378
2022-11-13T06:10:24Z	Senior Admins	False	8baeab4-b	2022-11-13T06:10:24Z	True	5-1-12-1-3080031100-1341057643-3912430737-400343468
2022-11-13T06:18:28Z	Junior Admins	False	JuniorAdmins	2022-11-13T06:18:28Z	True	5-1-12-1-3799563633-1288914800-3550756538-3649640740

```
{
  "odata.type": "#microsoft.graph.user",
  "businessPhones": [],
  "displayName": "Dylan Williams",
  "givenName": null,
  "id": "c6b41648-5134-4a3f-bdce-f4525ff39932",
  "jobTitle": null,
  "mail": null,
  "mobilePhone": null,
  "officeLocation": null,
  "preferredLanguage": null,
  "surname": null,
  "userPrincipalName": "Dylan@manassehwmw9@gmail.onmicrosoft.com"
}
```

When one checks the list all groups, the service desk group containing Dylan Williams was created using a bash script in the command line



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

Task 1: Create a resource group

Microsoft Azure

Home > Resource groups >

Create a resource group

Basics Tags Review + create

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](#)

Project details

Subscription * Azure Pass - Sponsorship

Resource group * AZ500Lab01

Resource details

Region * (US) East US

Review + create < Previous Next: Tags >

Wait for the resource group to deploy.

Microsoft Azure

Home >

Resource groups

Default Directory (manassehwmwang@gmail.com@microsoft.com)

+ Create Manage view Refresh Export to CSV Open query Assign tags

Filter for any field... Subscription equals all Location equals all Add filter

0 Unsecure resources 0 Recommendations No grouping List view

Name	Subscription	Location
AZ500Lab01	Azure Pass - Sponsorship	East US
cloud-shell-storage-westurope	Azure Pass - Sponsorship	West Europe

< Previous Page 1 of 1 Next > Showing 1 to 2 of 2 records. Give feedback

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

On the **Add role assignment** blade, specify the following settings

Virtual Machine Contributor

Got feedback?

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

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Virtual Machine Contributor Type: All Category: All

Showing 5 of 373 roles

Name	Description	Type	Category	Details
Classic Virtual Machine Contributor	Lets you manage classic virtual machines, but not access to them, and not the virtual network or storage account they're connected to.	BuiltInRole	Compute	View
Desktop Virtualization Power On Contributor	This role is in preview and subject to change. Provide permission to the Azure Virtual Desktop Resource Provider to start virtual machines.	BuiltInRole	None	View
Desktop Virtualization Power On Off Contributor	This role is in preview and subject to change. Provide permission to the Azure Virtual Desktop Resource Provider to start and stop virtual machines.	BuiltInRole	None	View
Desktop Virtualization Virtual Machine Contributor	This role is in preview and subject to change. Provide permission to the Azure Virtual Desktop Resource Provider to create, delete, and manage virtual machines.	BuiltInRole	None	View
Virtual Machine Contributor	Lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.	BuiltInRole	Compute	View

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

User, group, or service principal

Service Desk

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	aa48f9d-736f-4c50-91f2-531ec2e98391	Group

Description Optional

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

You have assigned RBAC permissions.

Resource groups > AZ500Lab01

AZ500Lab01 | Access control (IAM)

Number of role assignments for this subscription: 1

Search by name or email: [Type: All] [Role: All] [Scope: All scopes] [Group by: Role]

Name	Type	Role	Scope	Condition
<input type="checkbox"/> User Access Administrator	User	User Access Administrator	Root (Inherited)	None
<input type="checkbox"/> Virtual Machine Contributor	Group	Virtual Machine Contributor	This resource	None

select the user account of Dylan Williams and check RBAC permissions.

Resource groups > AZ500Lab01

Dylan Williams assignments - AZ500Lab01

Current role assignments

Assignments for the selected user, group, service principal, or managed identity at this scope or inherited to this scope.

Search by assignment name or description

Role	Description	Scope	Group assignment	Condition
<input type="checkbox"/> Virtual Machine Contributor	Lets you manage virtual machine...	This resource	Service Desk	None

select the user account of Joseph Price and check RBAC permissions.

Joseph Price assignments - AZ500Lab01

Current role assignments | Eligible assignments

Assignments for the selected user, group, service principal, or managed identity at this scope or inherited to this scope.

Search by assignment name or description

Role assignments (0)

Deny assignments (0)

Classic administrators (0)

My access

View my level of access to resources

Check access

Grant access to this resource

Add role assignment

View deny assignment

View the role assignment access to specific actions

Clean up resources

Azure services

Create a resource

Azure Active Directory

Management groups

Resource groups

Virtual machines

Application gateways

Virtual networks

Load balancers

Route tables

More services

Resources

Recent

Favorite

Name

Type

Last Viewed

PowerShell

Requesting a Cloud Shell.Succeeded.

Connecting terminal...

MOTD: Customize your experience: save your profile to \$HOME/.config/PowerShell

VERBOSE: Authenticating to Azure ...

VERBOSE: Building your Azure drive ...

PS /home/manasseh> Remove-AzResourceGroup -Name "AZ500LAB01" -Force -AsJob

Id	Name	PSJobTypeName	State	HasMoreData	Location	Command
2	Long Running O...	AzureLongRunni...	Running	True	localhost	Remove-AzResourceGroup

PS /home/manasseh>