

Lab 2: Azure Identities

Student Name: Vivek Vashisht

Student ID: 000907246

Screenshots

- New Azure AD Tenant

Create a tenant - Microsoft Azure

portal.azure.com/#view/Microsoft_AAD_IAM/CreateDirectoryBlade/releaseCreateOperation~/false

Microsoft Azure

Search resources, services, and docs (G+)

Home > Default Directory | Overview > Manage tenants >

Create a tenant

Directory details

Configure your new directory

Organization name * ① VivekV's ORG ✓

Initial domain name * ① VVorganisation04 ✓
VVorganisation04.onmicrosoft.com

Location ① Canada ✓
Geographic location - United States

The location selected above will determine the geographic location where Azure AD B2C will store your Core Store data only. To determine where Microsoft will store or process your Azure AD B2C data, see [Azure AD B2C region availability and data residency](#).

Subscription

Choose the subscription to use for Azure AD B2C. [See pricing details](#)

Subscription * Azure subscription 1 ✓

Resource group * (New) 1stRG ✓
[Create new](#)

Resource group location * Canada Central ✓

Review + create

< Previous

Next: Review + create >

Manage tenants - Microsoft Az...

portal.azure.com/#view/Microsoft_AAD_IAM/DirectorySwitchBlade/subtitle/

VPN

Microsoft Azure

Search resources, services, and docs (G+)

Home > Default Directory | Overview >

Manage tenants

×

+ Create

↻ Refresh

≡ Columns

|

↔ Switch

🗑 Delete

⊖ Leave tenant

✓ Make default tenant

🕒 More information

|

💬 Got feedback?

Current tenant: Default Directory

🔍 Search tenants

+ Add filters

Showing 2 of 2 results

<input type="checkbox"/>	Organization name	↕	Domain name	↕	Tenant type	↕	Organization ID	↕	Favorite	↕
<input type="checkbox"/>	Default Directory (Default)		vivekvash1507gmail.onmicrosoft.com		Microsoft Entra ID		17c16687-3403-4510-9e65-5d5c202fbd22		★	
<input type="checkbox"/>	VivekV's ORG		VVorganisation04.onmicrosoft.com		Azure AD B2C		778de553-026c-4f25-8724-90533e3d6b60		★	

- PowerShell screen with successful creation of a user

- Users Created manually and from Csv file

Users - Microsoft Azure

portal.azure.com/?feature.msajls=true#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/~/_/AllUsers

VPN

Microsoft Azure

Search resources, services, and docs (G+)

Home > Default Directory | Users >

Users

×

Default Directory - Microsoft Entra ID

🔍 Search

«

+ New user

↓ Download users

📄 Bulk operations

↻ Refresh

⚙ Manage view

⌵

🗑 Delete

|

👤 Per-user MFA

|

💬 Got feedback?

All users

Azure Active Directory is now Microsoft Entra ID.

Audit logs

Sign-in logs

Diagnose and solve problems

Manage

Deleted users

Password reset

User settings

Bulk operation results

Troubleshooting + Support

New support request

10 users found

☐

Display name ↗

☐

User principal name ↕

☐

User type

☐

On-premises sy...

☐

Identities

☐

Company name

☐

Creation type

- CSV file used in the lab to create users with the UserCreateTemplate

```

UserCreateTemplate.csv
C:\Users\hp> OneDrive > Desktop > SEM 4 (FINAL) > Cloud Computing > Lab 2 > Modified UserCreateTemplate for the lab > UserCreateTemplate.csv
1 version:v1.0,,,,,,,,,,,,,
2 Name [displayName] Required,User name [userPrincipalName] Required,Initial password [passwordProfile] Required,Block sign in (Yes/No) [accountEnabled] Required,First
3 WHeisenberg,WHeisenberg@vivekvash1507gmail.onmicrosoft.com,ThisF1r3w@11,No,,,,,,,,,,,,,
4 NBohr,NBohr@vivekvash1507gmail.onmicrosoft.com,ThisF1r3w@11,No,,,,,,,,,,,,,
5 PDirac,PDirac@vivekvash1507gmail.onmicrosoft.com,ThisF1r3w@11,No,,,,,,,,,,,,,
6 PKim,PKim@vivekvash1507gmail.onmicrosoft.com,ThisF1r3w@11,No,,,,,,,,,,,,,
7 JLee,JLee@vivekvash1507gmail.onmicrosoft.com,ThisF1r3w@11,No,,,,,,,,,,,,,
8 CSmith,CSmith@vivekvash1507gmail.onmicrosoft.com,ThisF1r3w@11,No,,,,,,,,,,,,,
9

```

- PowerShell with User Commands in it for the Creation of users(i)

```

PS /home/vivek> New-AzureADUser -DisplayName "Rowan.Quartz" -PasswordProfile $PasswordProfile -UserPrincipalName "Rowan.Quartz@vivekvash1507gmail.onmicrosoft.com" -AccountEnabled $true -MailNickName "Rowan.Quartz"

ObjectID      DisplayName      UserPrincipalName
-----
ea9b3cba-8428-4523-9b7b-73853f365a19 Rowan.Quartz Rowan.Quartz@vivekvash1507gmail...

PS /home/vivek> New-AzureADUser -DisplayName "Finley.Starling" -PasswordProfile $PasswordProfile -UserPrincipalName "Finley.Starling@vivekvash1507gmail.onmicrosoft.com" -AccountEnabled $true -MailNickName "Finley.Starling"

ObjectID      DisplayName      UserPrincipalName
-----
8d0a1ee3-d3b3-462e-b370-019ee5ba009f Finley.Starling Finley.Starling@vivekvash1507...

PS /home/vivek> New-AzureADUser -DisplayName "Marlowe.Cedar" -PasswordProfile $PasswordProfile -UserPrincipalName "Marlowe.Cedar@vivekvash1507gmail.onmicrosoft.com" -AccountEnabled $true -MailNickName "Marlowe.Cedar"

ObjectID      DisplayName      UserPrincipalName
-----
4d9388c9-2dcb-4545-b499-d56865bd36e6 Marlowe.Cedar Marlowe.Cedar@vivekvash1507mai...

PS /home/vivek> New-AzureADUser -DisplayName "Tamsin.Frost" -PasswordProfile $PasswordProfile -UserPrincipalName "Tamsin.Frost@vivekvash1507gmail.onmicrosoft.com" -AccountEnabled $true -MailNickName "Tamsin.Frost"

ObjectID      DisplayName      UserPrincipalName
-----
2c385b08-7968-4ad7-9bed-b51d44a619e9 Tamsin.Frost Tamsin.Frost@vivekvash1507mail...

PS /home/vivek> New-AzureADUser -DisplayName "Ellis.Ocean" -PasswordProfile $PasswordProfile -UserPrincipalName "Ellis.Ocean@vivekvash1507gmail.onmicrosoft.com" -AccountEnabled $true -MailNickName "Ellis.Ocean"

ObjectID      DisplayName      UserPrincipalName
-----
1a178d39-b4a7-4de1-911d-002a20012ad7 Ellis.Ocean Ellis.Ocean@vivekvash1507mail.on...

```

- PowerShell with User Commands in it for the Creation of users(ii)

```

ObjectID                               DisplayName UserPrincipalName
-----
1a178d39-b4a7-4de1-911d-002a20012ad7 Ellis.Ocean Ellis.Ocean@vivekvash1507gmail.onm...

PS /home/vivek> New-AzureADUser -DisplayName "Brian.Sage" -PasswordProfile $PasswordProfile -UserPrincipalName "Brian.Sage@vivekvash1507gmail.onmicrosoft.com" -AccountEnabled $true -MailNickName "Brian.Sage"

ObjectID                               DisplayName UserPrincipalName
-----
d84c8583-22dc-4112-aded-b1c24e56c40f Brian.Sage Brian.Sage@vivekvash1507gmail.onm...

PS /home/vivek> New-AzureADUser -DisplayName "Quincy.Lumen" -PasswordProfile $PasswordProfile -UserPrincipalName "Quincy.Lumen@vivekvash1507gmail.onmicrosoft.com" -AccountEnabled $true -MailNickName "Quincy.Lumen"

ObjectID                               DisplayName UserPrincipalName
-----
96409005-307e-4014-a3b9-b9fa9ab4530 Quincy.Lumen Quincy.Lumen@vivekvash1507gmail...

PS /home/vivek> New-AzureADUser -DisplayName "Indigo.Vale" -PasswordProfile $PasswordProfile -UserPrincipalName "Indigo.Vale@vivekvash1507gmail.onmicrosoft.com" -AccountEnabled $true -MailNickName "Indigo.Vale"

ObjectID                               DisplayName UserPrincipalName
-----
bbd3651a-c006-43e4-b5dd-54ae5225e774 Indigo.Vale Indigo.Vale@vivekvash1507gmail.on...

PS /home/vivek> New-AzureADUser -DisplayName "Skye.Nebula" -PasswordProfile $PasswordProfile -UserPrincipalName "Skye.Nebula@vivekvash1507gmail.onmicrosoft.com" -AccountEnabled $true -MailNickName "Skye.Nebula"

ObjectID                               DisplayName UserPrincipalName
-----
edad664a-b240-41be-aebd-441786e354f2 Skye.Nebula Skye.Nebula@vivekvash1507gmail.on...

PS /home/vivek> New-AzureADUser -DisplayName "Arden.Flux" -PasswordProfile $PasswordProfile -UserPrincipalName "Arden.Flux@vivekvash1507gmail.onmicrosoft.com" -AccountEnabled $true -MailNickName "Arden.Flux"
  
```

- 10 users created Through PowerShell

Home > Default Directory | Users >

Users ...
Default Directory - Microsoft Entra ID

Search [] << + New user Download users Bulk operations Refresh Manage view Delete Per-user MFA Got feedback?

[Azure Active Directory is now Microsoft Entra ID.](#)

Search [] Add filter

11 users found

<input type="checkbox"/>	Display name ↑	User principal name ↑	User type	On-premises sy...	Identities	Company name	Creation type
<input type="checkbox"/>	Arden.Flux	Arden.Flux@vivekvash150...	Member	No	vivekvash1507gmail.onmicrosoft.c...		
<input type="checkbox"/>	Brian.Sage	Brian.Sage@vivekvash150...	Member	No	vivekvash1507gmail.onmicrosoft.c...		
<input type="checkbox"/>	Ellis.Ocean	Ellis.Ocean@vivekvash150...	Member	No	vivekvash1507gmail.onmicrosoft.c...		
<input type="checkbox"/>	Finley.Starling	Finley.Starling@vivekvash...	Member	No	vivekvash1507gmail.onmicrosoft.c...		
<input type="checkbox"/>	Indigo.Vale	Indigo.Vale@vivekvash150...	Member	No	vivekvash1507gmail.onmicrosoft.c...		
<input type="checkbox"/>	Marlowe.Cedar	Marlowe.Cedar@vivekvas...	Member	No	vivekvash1507gmail.onmicrosoft.c...		
<input type="checkbox"/>	Quincy.Lumen	Quincy.Lumen@vivekvash...	Member	No	vivekvash1507gmail.onmicrosoft.c...		
<input type="checkbox"/>	Rowan.Quartz	Rowan.Quartz@vivekvash...	Member	No	vivekvash1507gmail.onmicrosoft.c...		
<input type="checkbox"/>	Skye.Nebula	Skye.Nebula@vivekvash1...	Member	No	vivekvash1507gmail.onmicrosoft.c...		
<input type="checkbox"/>	Tamsin.Frost	Tamsin.Frost@vivekvash1...	Member	No	vivekvash1507gmail.onmicrosoft.c...		

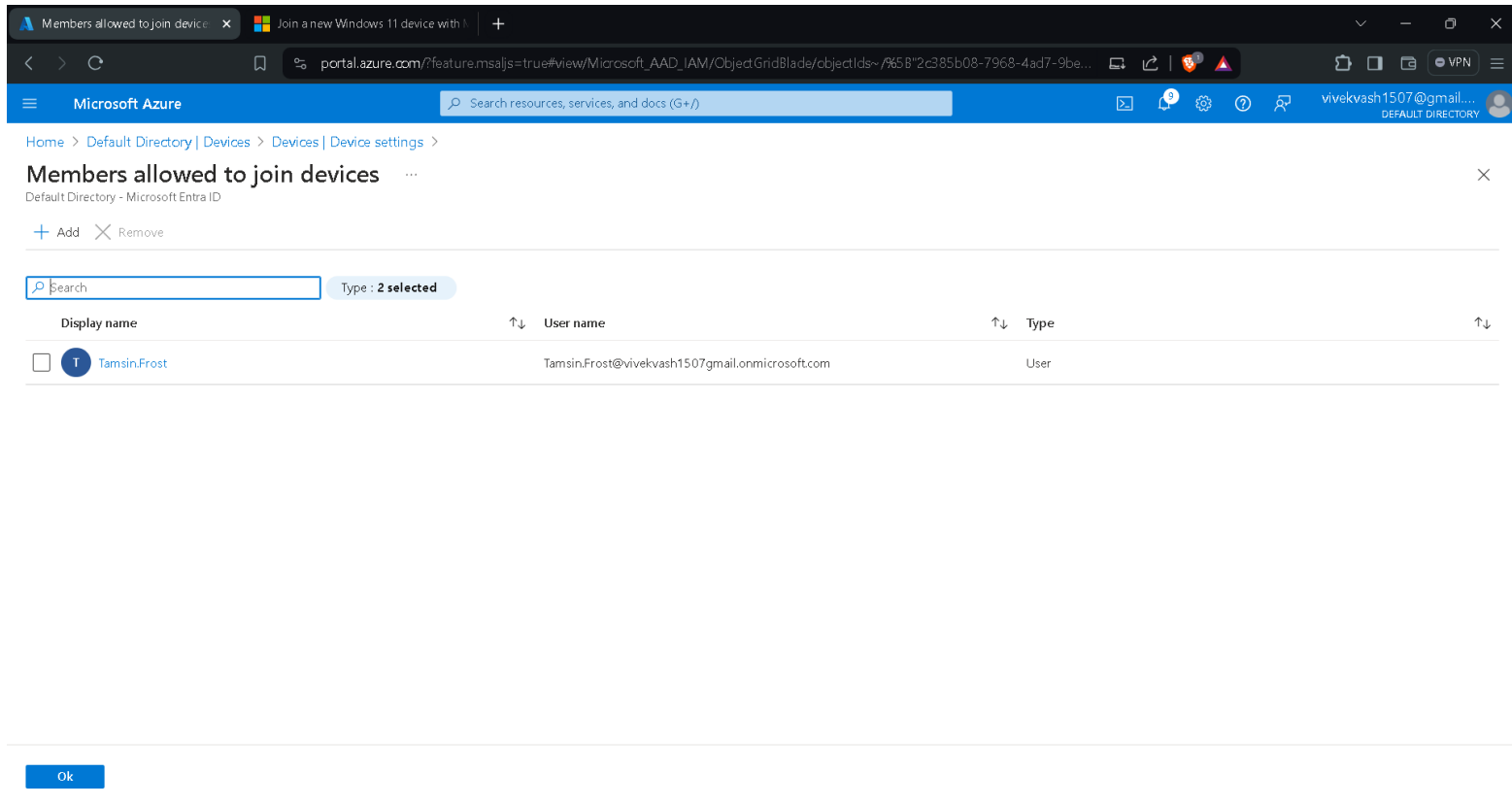
Switch to Bash Restart Manage files New session Editor Web preview Settings Help

```

ObjectID                               DisplayName UserPrincipalName
-----
  
```

- Windows 10/11 device added

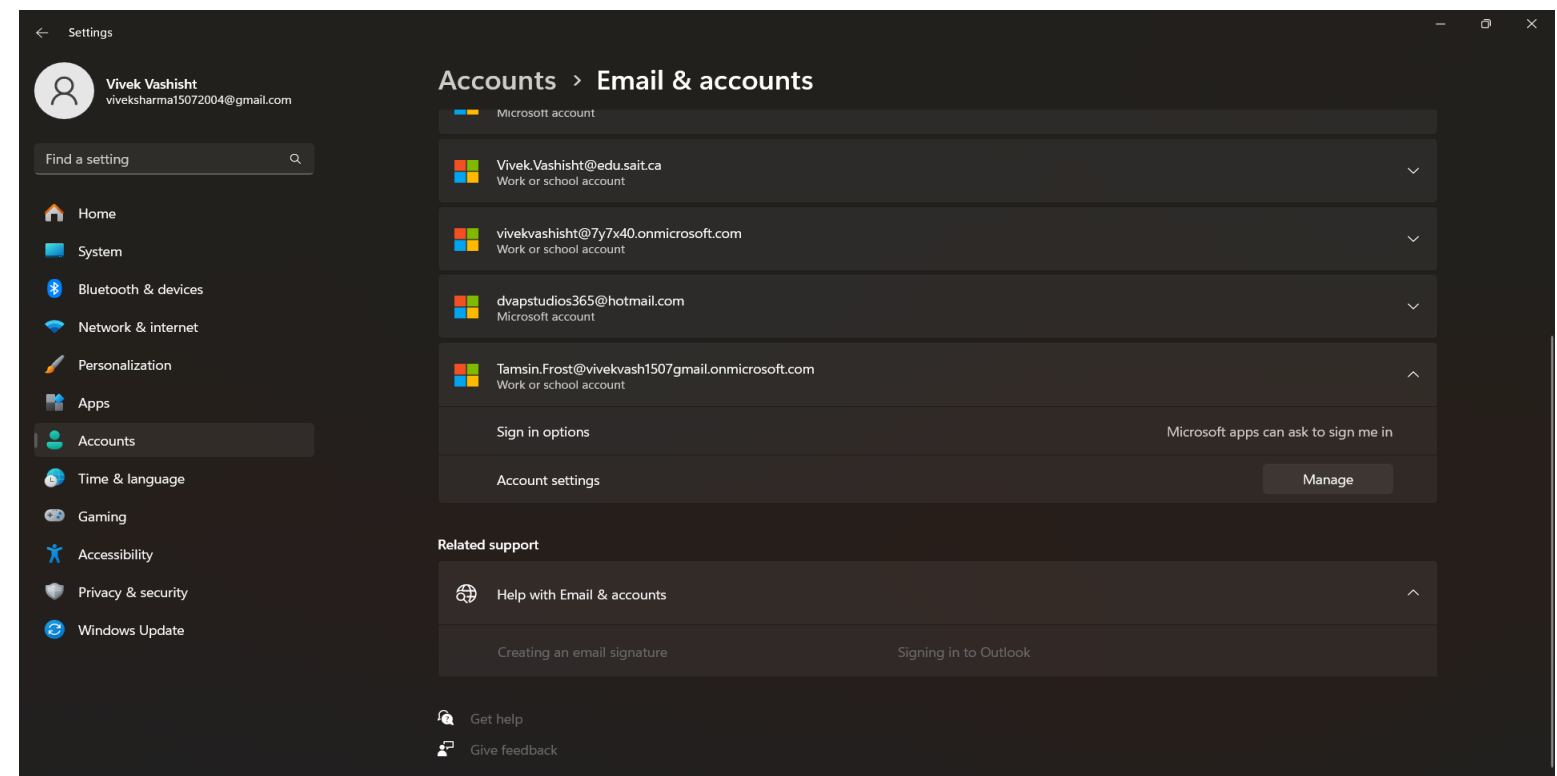
- Members/Users allowed to join devices



The screenshot shows the Microsoft Azure portal interface. The breadcrumb navigation is: Home > Default Directory | Devices > Devices | Device settings >. The page title is 'Members allowed to join devices' with a close button. Below the title is the text 'Default Directory - Microsoft Entra ID'. There are '+ Add' and 'X Remove' buttons. A search bar contains the text 'Search'. To the right of the search bar, it says 'Type: 2 selected'. Below this is a table with columns: 'Display name', 'User name', and 'Type'. The table contains two rows: one for 'Tamsin.Frost' and another for 'Tamsin.Frost@vivekvash1507gmail.onmicrosoft.com', both with the type 'User'. At the bottom of the page, there is an 'Ok' button.

Display name	User name	Type
Tamsin.Frost	Tamsin.Frost@vivekvash1507gmail.onmicrosoft.com	User

- Device Connected from the user Tamsin.Frost



The screenshot shows the Windows Settings app, specifically the 'Accounts > Email & accounts' page. The left sidebar shows the 'Accounts' section selected. The main content area displays a list of accounts. The first account is 'Microsoft account'. The second account is 'Vivek.Vashisht@edu.sait.ca' (Work or school account). The third account is 'vivekvashisht@7y7x40.onmicrosoft.com' (Work or school account). The fourth account is 'dvapstudios365@hotmail.com' (Microsoft account). The fifth account is 'Tamsin.Frost@vivekvash1507gmail.onmicrosoft.com' (Work or school account), which is expanded. Below the expanded account, there are two sections: 'Sign in options' and 'Account settings'. The 'Sign in options' section has a 'Manage' button. The 'Account settings' section has a 'Manage' button. At the bottom of the page, there is a 'Related support' section with links to 'Help with Email & accounts', 'Creating an email signature', and 'Signing in to Outlook'.

- User with Backup operator role on subscription

- Reader Role assignment on the User Group Tech Level II

Tech Level II assignments - 1stRG

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	Description	Scope	Group assignment	Condition
Reader	View all resources, but does not al...	This resource	--	None

Deny assignments (0)

- Ellis.Ocean user as Backup operator of Subscription(i)

Azure subscription 1 | Access control (IAM)

Check access Role assignments Roles Deny assignments Classic administrators

Number of role assignments for this subscription

4 4000

All Job function (1) Privileged (2)

Search by name or email

Type: All Role: All Scope: All scopes Group by: Role

Name	Type	Role	Scope	Condition
Owner (2)				
Vivek Vashisht vivekvash1507_gm...	User	Owner	This resource	Add
Vivek Vashisht vivekvash1507_gm...	User	Owner	This resource	Add
Backup Operator (1)				
Ellis.Ocean Ellis.Ocean@vivekv...	User	Backup Operator	This resource	None

- Ellis.Ocean user as Backup operator of Subscription(ii)

The screenshot shows the Azure portal interface for 'Ellis.Ocean assignments - Azure subscription 1'. The main content area is titled 'Current role assignments' and shows a table with one role assignment: 'Backup Operator' with the description 'Lets you manage backup services...' and scope 'This resource'. The left sidebar shows the 'Access control (IAM)' menu with options like Overview, Activity log, Tags, Diagnose and solve problems, Security, Events, Cost Management, Billing, and Settings.

- Custom role definition

- Custom RBAC Created Named VMAdmin

The screenshot shows the Azure portal interface for 'VMAdmin' custom role definition. The main content area is titled 'VMAdmin' and shows the 'Permissions' section with a table listing three permissions: 'Start Virtual Machine', 'Restart Virtual Machine', and 'Stop Virtual Machine'. The left sidebar shows the 'Access control (IAM)' menu with options like Overview, Activity log, Tags, Diagnose and solve problems, Security, Events, Cost Management, Billing, and Settings.

- Custom RBAC Created Named StoreAdmin(i)

Create a custom role - Microsoft

portal.azure.com/?feature.msajs=true#view/Microsoft_Azure_AD/CreateCustomRoleLandingBlade/roleId~/_null/scope/%2Fsubsc...

Microsoft Azure Upgrade

Search resources, services, and docs (G+/)

vivekvash1507@gmail...
DEFAULT DIRECTORY

Home > Azure subscription 1 | Access control (IAM) >

Create a custom role

BasicsPermissionsAssignable scopesJSONReview + create

+ Add permissions+ Exclude permissions

Click Add permissions to select the permissions you want to add to this custom role.
To add a wildcard (*) permission, you must manually add the permission on the JSON tab. [Learn more](#)

To exclude specific permissions from a wildcard permission, click Exclude permissions. [Learn more](#)

Permission	↑↓	Description	↑↓	Permission type	↑↓
Microsoft.Storage/storageAccounts/accountLocks/read	--			Action	
Microsoft.Storage/storageAccounts/fileServices/shares/...		Get file share		Action	
Microsoft.Storage/storageAccounts/fileServices/read		List file services		Action	
Microsoft.Storage/storageAccounts/blobServices/contai...		Returns list of containers		Action	
Microsoft.Storage/storageAccounts/delete		Deletes an existing storage account.		NotAction	

Definitions

Control plane
Actions specify the operations that a role is allowed to perform. NotActions specify the operations that are excluded from the allowed Actions (this is useful if a role has wildcards).

Data plane
DataActions specify the operations that a role is allowed to perform to the data within an object. NotDataActions specify the operations that are excluded from the allowed DataActions (this is useful if a role has wildcards).

Wildcards (*)
A wildcard (*) extends a permission to everything that matches the string you provide. To add a wildcard permission, use the JSON tab.

Review + createPreviousNext

Feedback

- Custom RBAC Created Named StoreAdmin(ii)

Create a custom role - Microsoft

portal.azure.com/?feature.msajs=true#view/Microsoft_Azure_AD/CreateCustomRoleLandingBlade/roleId~/_null/scope/%2Fsubsc...

Microsoft Azure Upgrade

Search resources, services, and docs (G+/)

vivekvash1507@gmail...
DEFAULT DIRECTORY

Home > Azure subscription 1 | Access control (IAM) >

Create a custom role

BasicsPermissionsAssignable scopesJSONReview + create

Basics

Role name

StoreAdmin

Role description

No role description provided

Permissions

Action	Microsoft.Storage/storageAccounts/accountLocks/read
Action	Microsoft.Storage/storageAccounts/fileServices/shares/read
Action	Microsoft.Storage/storageAccounts/fileServices/read
Action	Microsoft.Storage/storageAccounts/blobServices/containers/read
NotAction	Microsoft.Storage/storageAccounts/delete

Assignable Scopes

Scope

/subscriptions/ee9ea131-d6f1-4e0b-baee-b293615685ae

CreatePrevious

Feedback

- Custom RBAC Created Named StoreAdmin(iii)

The screenshot shows the Azure portal interface. On the left, the navigation pane is open, showing the 'Access control (IAM)' section. The main pane displays the 'StoreAdmin' custom role. The 'Permissions' tab is selected, showing a list of permissions under the 'Microsoft.Storage' namespace. The permissions are as follows:

Type	Permissions	Description
Read	--	--
Read	Get blob container	Returns a container
Read	List of blob containers	Returns list of containers
Read	List File Services	List file services
Read	Get file service properties	Get file service properties
Read	Get File Share	Get file share
Read	List File Shares	List file shares

- Management group created with Az CLI

- R&D Management Group Created(i)

The screenshot shows the Azure portal interface for 'Management groups'. The main pane displays a table of management groups and subscriptions. The table is as follows:

Name	Type	ID	Total subscriptions
Tenant Root Group	Management group	17c16687-3403-4510-9e65-5d5c202fbd22	1
Azure subscription 1	Subscription	ee9ea131-d6f1-4e0b-baee-b293615685ae	
R&D	Management group	ResearchandDevelopment	0

- R&D Management Group Created(ii)

The screenshot shows the Microsoft Azure portal interface for the 'R&D' Management Group. The breadcrumb navigation indicates the path: Home > Management groups > R&D. The left-hand navigation pane includes sections for Overview, Subscriptions, Resource Groups, Resources, Activity Log, Access control (IAM), Governance (Get started, Security, Policy, Deployments, Deployment stacks), and Cost Management (Cost analysis, Budgets). The main content area is titled 'Essentials' and displays the following details for the 'R&D' group:

- Name: R&D
- ID: ResearchandDevelopment
- Access Level: Owner
- Path: Tenant Root Group / R&D
- Parent management group: Tenant Root Group
- Child management groups: 0
- Total subscriptions: 0

Below the details, there is a search bar labeled 'Search by name or ID' and a message stating 'Showing 0 subscriptions in 1 groups'. A table with columns 'Name', 'Type', 'ID', and 'Total subscriptions' is present but empty. At the bottom, there is a large icon representing a management group and the text 'Empty Management Group'.

- Production Management Group Created Through CLI (i)

The screenshot shows a terminal window with the command to create a new management group in Azure:

```
vivek [ ~ ]$ az account management-group create --name 'Production'
```

The output of the command is a JSON object representing the newly created management group:

```
{
  "children": null,
  "details": {
    "managementGroupAncestors": null,
    "managementGroupAncestorsChain": null,
    "parent": {
      "displayName": "Tenant Root Group",
      "id": "/providers/Microsoft.Management/managementGroups/17c16687-3403-4510-9e65-5d5c202fbd22",
      "name": "17c16687-3403-4510-9e65-5d5c202fbd22"
    },
    "path": null,
    "updatedBy": "8ad0491b-df2f-4e46-a1cf-5e9bca459471",
    "updatedAt": "2024-05-22T06:26:12.276429+00:00",
    "version": 1
  },
  "displayName": "Production",
  "id": "/providers/Microsoft.Management/managementGroups/Production",
  "name": "Production",
  "tenantId": "17c16687-3403-4510-9e65-5d5c202fbd22",
  "type": "Microsoft.Management/managementGroups"
}
```

The terminal prompt returns to the user, indicating the command was successful.

- Production Management Group Created Through CLI(ii)

The screenshot displays the Microsoft Azure portal interface. The top navigation bar shows the 'Management groups' section. The main content area lists the following management groups and subscriptions:

Name	Type	ID	Total subscriptions
Tenant Root Group	Management group	17c16687-3403-4510-9e65-5d5c202fbd22	1
Azure subscription 1	Subscription	ee9ea131-d6f1-4e0b-baee-b293615685ae	
Production	Management group	Production	0
R&D	Management group	ResearchandDevelopment	0

Below the portal screenshot, a terminal window shows the execution of the following CLI command:

```
vivek [ ~ ]$ az account management-group create --name 'Production'
```

The output of the command is a JSON object:

```
{
  "children": null,
  "details": {
    "managementGroupAncestors": null,
    "managementGroupAncestorsChain": null,
    "parent": {
      "displayName": "Tenant Root Group",

```