

Get the best out of Live Sessions HOW?



Check your Internet Connection

Log in 10 mins before, and check your internet connection to avoid any network issues during the LIVE session.

Speak with the Instructor

By default, you will be on mute to avoid any background noise. However, if required you will be **unmuted by instructor**.



Clear Your Doubts

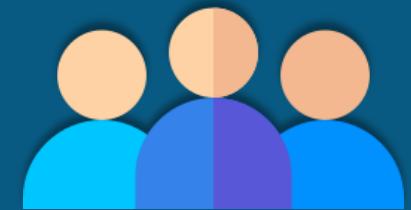


Feel free to clear your doubts. Use the “**Questions**” tab on your webinar tool to interact with the instructor at any point during the class.

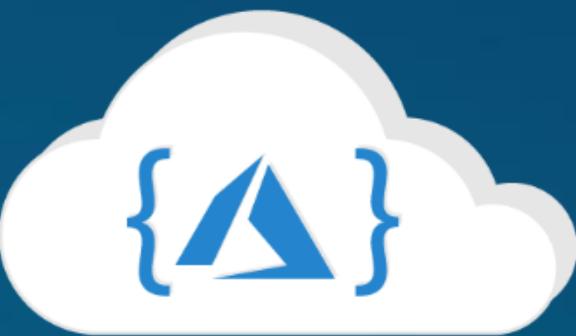


Let us know if you liked our content

Please share feedback after each class. It will help us to enhance your learning experience.



edureka!



Microsoft Azure Developer Associate (AZ-204)

COURSE OUTLINE

MODULE 08

Introduction to Azure IaaS Compute Solutions

Implementing Azure Batch Service and Disk Encryption

Designing and Developing Applications That Use Containers

Implementing Azure App Service Web Apps and Mobile Apps

Implementing Azure App Service API Apps and Azure Functions

Developing Solutions That Use Azure Table Storage and Cosmos DB

Developing Solutions That Use Relational Database and Azure Blob Storage

Implementing Authentication and Access Control in Azure

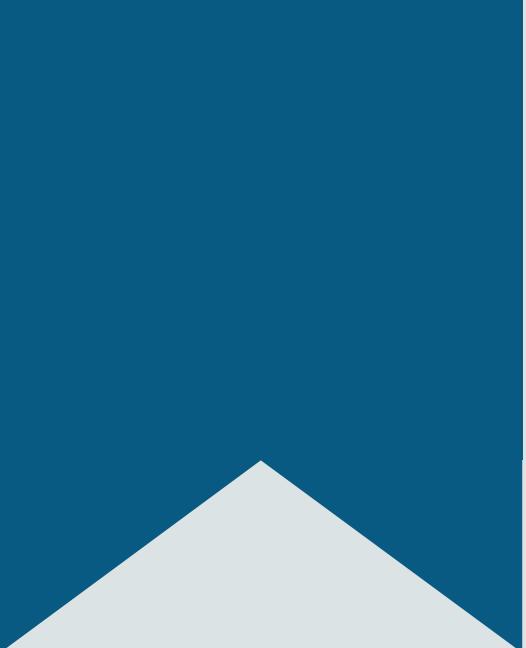
Implementing Secure Data Solutions and Integrate Caching & CDN

Instrument Monitoring, Logging and Scalability Of Apps & Services

Connecting to and Consuming Azure and Third-party Services

Developing Event-based and Message-based Solutions in Azure





Module 8 – Implementing Authentication and Access Control in Azure

Topics

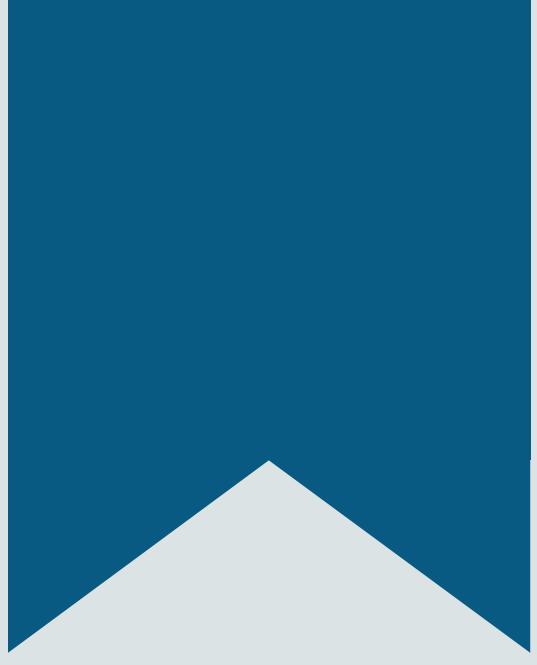
- Access Control
- Role-based access control (RBAC)
- Azure Active Directory (AD)
- Azure AD Licenses
- Multi-Factor Authentication (MFA)
- Manage Multiple Directories In Azure
- Azure AD Identity Management Capabilities
- Access Reviews In Azure
- Authentication In Azure Active Directory
- Claim-Based Architecture
- Azure AD – Authentication Frameworks
- Azure Managed Service Identity
- Implement OAuth 2.0 Authorization

Objectives

After completing this module, you should be able to:

- Understand the architecture of the Microsoft identity platform
- Implement OAuth2 authentication
- Implement managed identities for Azure resources
- Implement authentication by using certificates, forms-based authentication, or tokens
- Implement multi-factor authentication
- Learn how to use Claims-based and Role-based authorization in the development solutions





Access Control

Access Control

- Resource Manager enables access control to specific actions for your organization
- **Role-based access control (RBAC)** is integrated into the management platform and applies that access control to all services in your resource group
- There are two main concepts to understand when working with role-based access control:
 - **Activity logs** – for monitoring changes to role assignments and definitions
 - **Inherited policies** – for providing differing roles for different resources or resource groups
- **Role definitions** - Describe a set of permissions and can be used in many assignments
- **Role assignments** - Associate a definition with an identity (user or group) for a particular scope (subscription, resource group, or resource). The assignment is inherited by lower scopes



What Can RBAC Do?



Allow different users to manage different resources



Allow a DBA group to manage SQL databases in a subscription

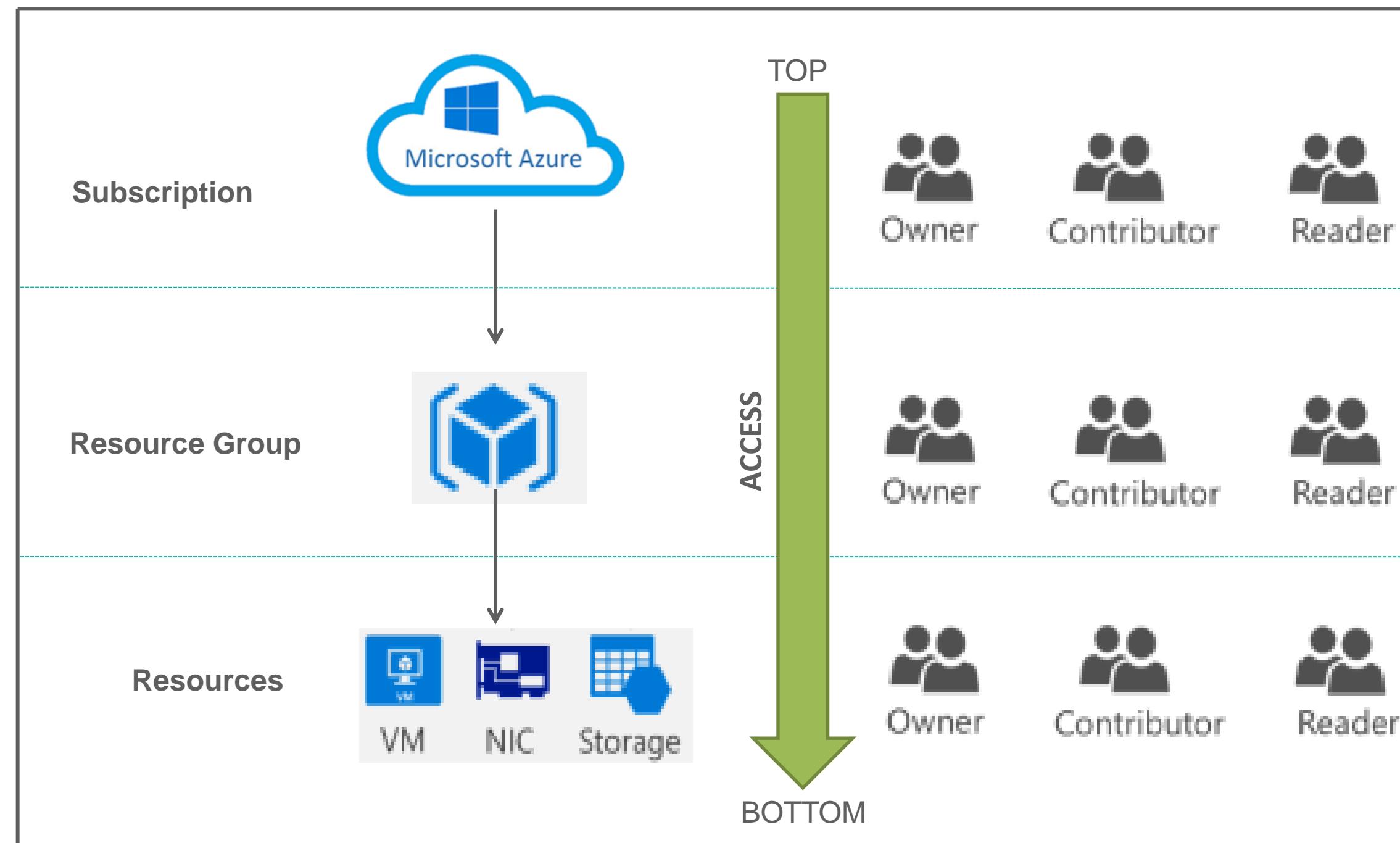


Allow a user to manage all resources in a resource group, such as virtual machines, websites, and storage



Allow an application to access all resources in a resource group

High-level Overview of RBAC



Note: Azure RBAC is inherited by the child once provided at the parent level.

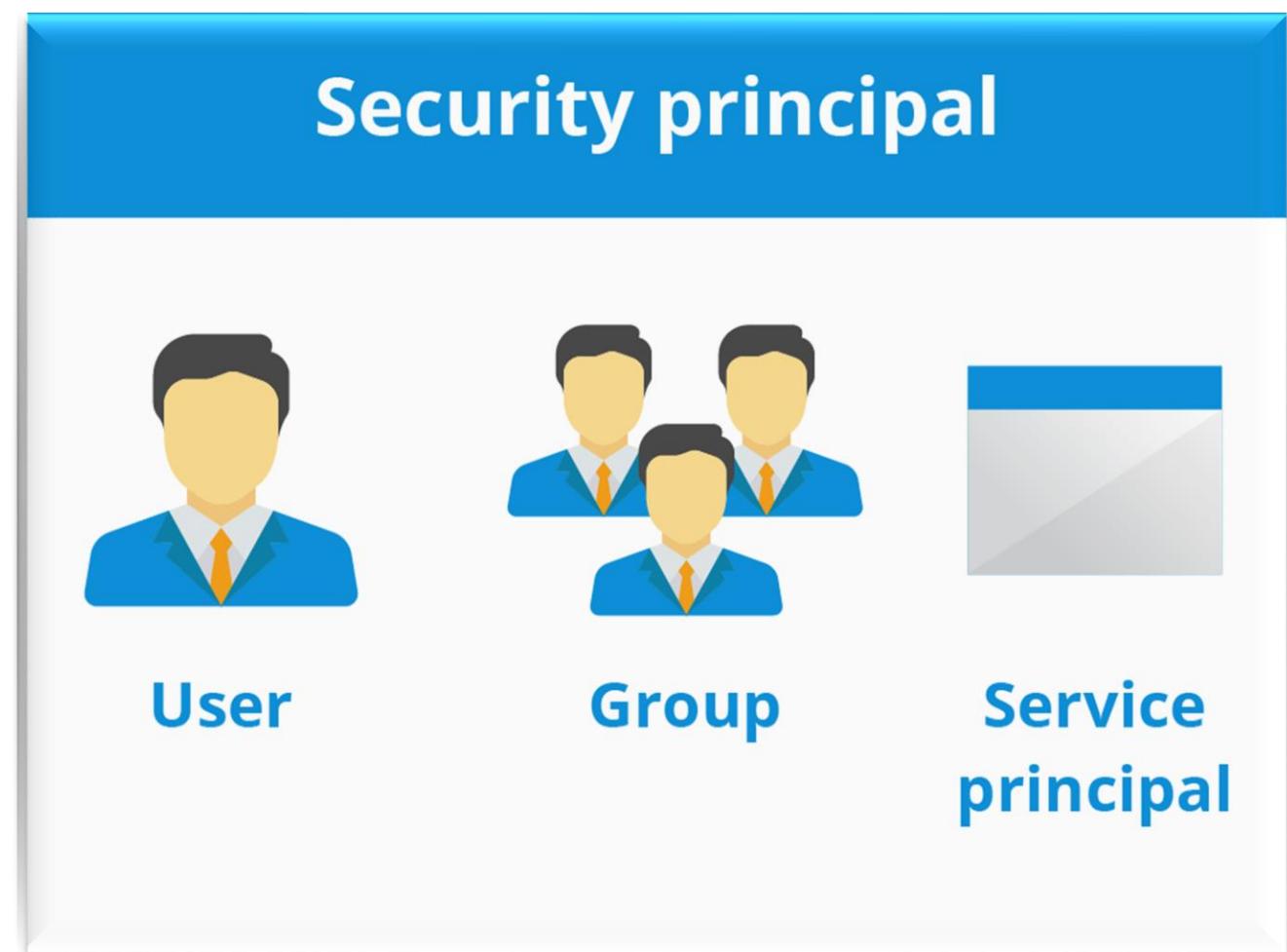
How Does RBAC Work?

- RBAC works by the practice of assigning the **Least Privilege** to help improve overall security
- RBAC controls access to resources using **Role Assignments**
- **Role Assignments** are used to enforce permissions for your organization
- A role assignment consists of three elements:
 - Security Principal
 - Role Definition
 - Scope



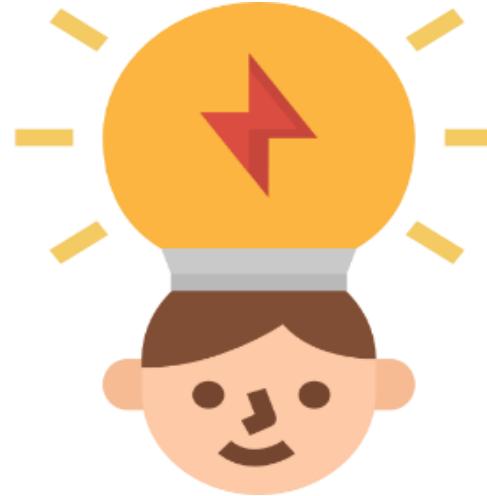
RBAC – Security Principal

- A **Security Principal** is an object that represents a user, group, or service principal that is requesting access to Azure resources
- **User** - An individual who has a profile in Azure Active Directory. Roles can be assigned to users in other tenants
- **Group** - A set of users created in Azure Active Directory. When you assign a role to a group, all users within that group have that role
- **Service Principal** - A security identity used by applications or services to access specific Azure resources. It functions as a user ID for an application



RBAC – Role Definition

- A **Role Definition** is a collection of permissions; it lists the operations that can be performed, such as read, write, and delete.
Azure includes several built-in_roles –



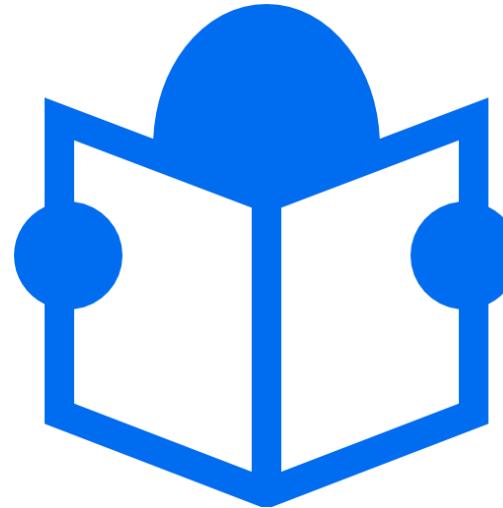
Contributor
Can create & manage all types of Azure resources but can't grant access to others



Owner
Has full access to all resources and delegates access to others



User Access Administrator Lets you manage user access to Azure resources



Reader
Can view existing Azure resources

RBAC – Other Platform Roles

Azure provides the other platform roles such as:

Network Contributor

Can manage all network resources, but not grant access to them

Storage Account Contributor

Can manage storage accounts, but not grant access to them

SQL Server Contributor

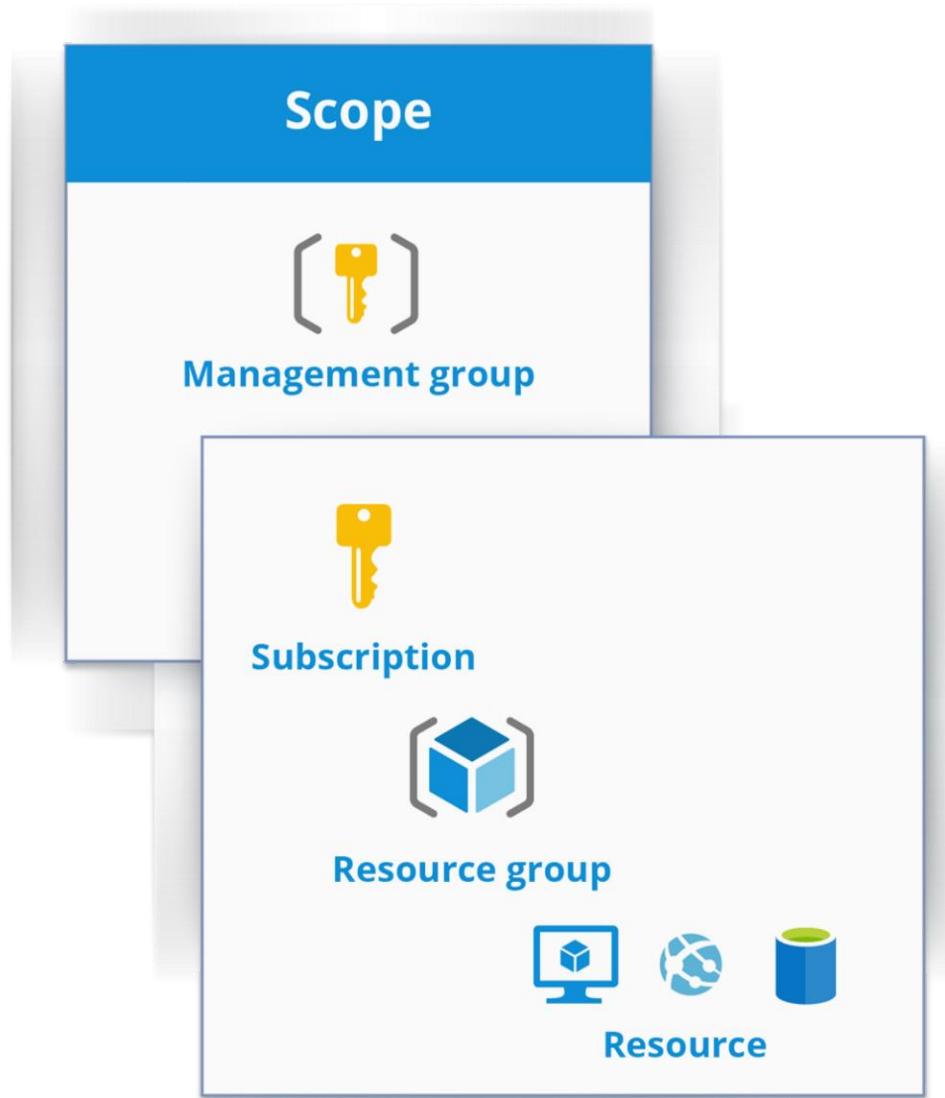
Can manage SQL servers and databases, but not their security related policies

Website Contributor

Can manage websites, but not the web plans to which they are connected

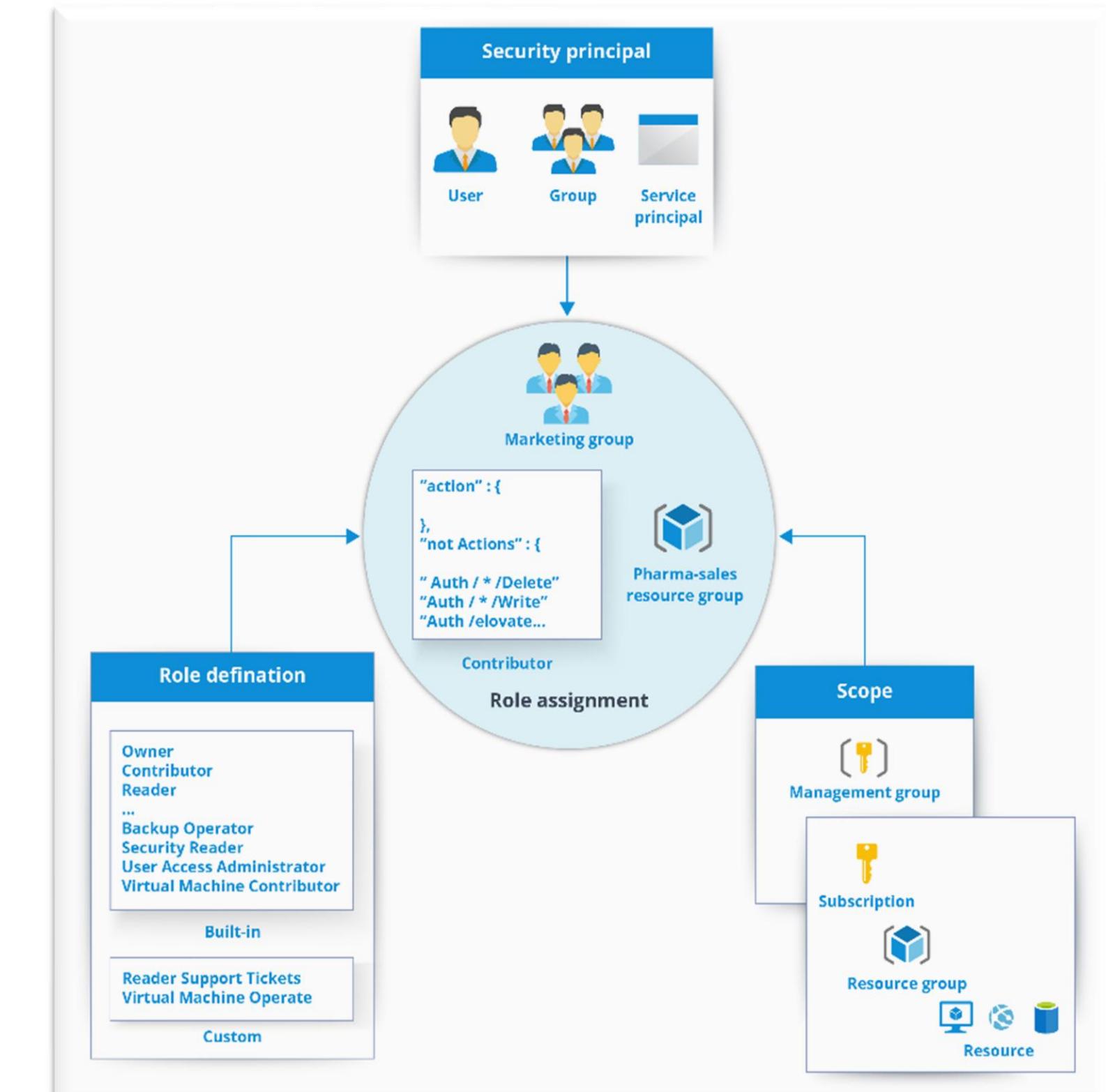
RBAC – Scope

- *Scope* is the boundary applied to the access
- When a role has been assigned, it's actions can be limited by defining a scope
- Scope can be specified at multiple levels: **subscription**, **resource group**, or **resource**
- Scopes are structured in a parent-child relationship where every child will have only one parent



RBAC – Role Assignment

- A **Role Assignment** is the process of binding a role definition to a user, group, or service principal at a particular scope for the purpose of granting access.
- Access is granted by creating a role assignment, and access is revoked by removing a role assignment.



Custom Roles in Azure AD

We can create custom roles and define the properties and rules for the roles according to our business requirements. Custom roles can be assigned at the directory level or at an app registration scope level. Once the custom role is created, it will be added in the Roles section of the page.

The screenshot shows the 'Roles and administrators' page in Azure Active Directory. A red box highlights the 'New custom role' button in the top right corner. Another red box highlights the 'Roles and administrators' link in the left sidebar. The main content area displays administrative roles with their descriptions:

ROLE	DESCRIPTION
Application administrator	Can create and manage all aspects of a Microsoft application.
Application developer	Can create application registrations and manage their settings.
Application Consent Administrator	Can manage basic aspects of application consent requests.

Custom Role Example

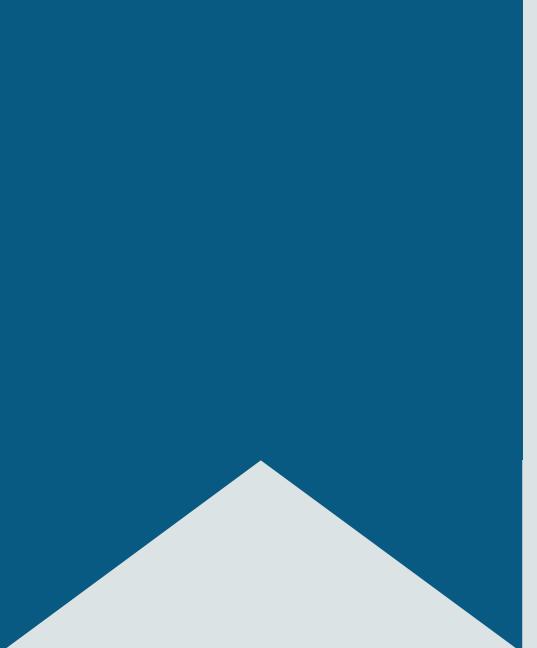
Below is the json template example used to define custom roles :

```
$role = Get-AzureRmRoleDefinition "Virtual Machine Contributor"  
$role.Id=$null  
$role.Name= "Custom Role- Virtual Machine Operator Demo01"  
$role.Description= "Can Monitor and Restart VMs"  
$role.actions.clear()  
$role.actions.Add("Microsoft.Storage/*/read")  
$role.actions.Add("Microsoft.Network/*/read")  
$role.actions.Add("Microsoft.Compute/*/read")  
$role.actions.Add("Microsoft.Compute/virtualMachines/start/action")  
$role.actions.Add("Microsoft.Compute/virtualMachines/restart/action")  
$role.actions.Add("Microsoft.Resources/Subscriptions/resourceGroups/read")  
$role.actions.Add("Microsoft.Insights/alertRules/*")  
$role.actions.Add("Microsoft.Support/*")  
$roleAssignableScopes.Clear()  
$role.AssignableScopes.Add("/subscriptions/9fbfa342-4255-485e-932f-6f05ad268486")  
New-AzureRmRoleDefinition -Role $role
```

CustomRoles.json

Below is the script to create a custom role using azure Powershell and above template:

```
New-AzureRmRoleDefinition -InputFile C:\Users\Admin\templates\CustomRoles.json
```



Managing Access for Resource Groups

RBAC – View Access

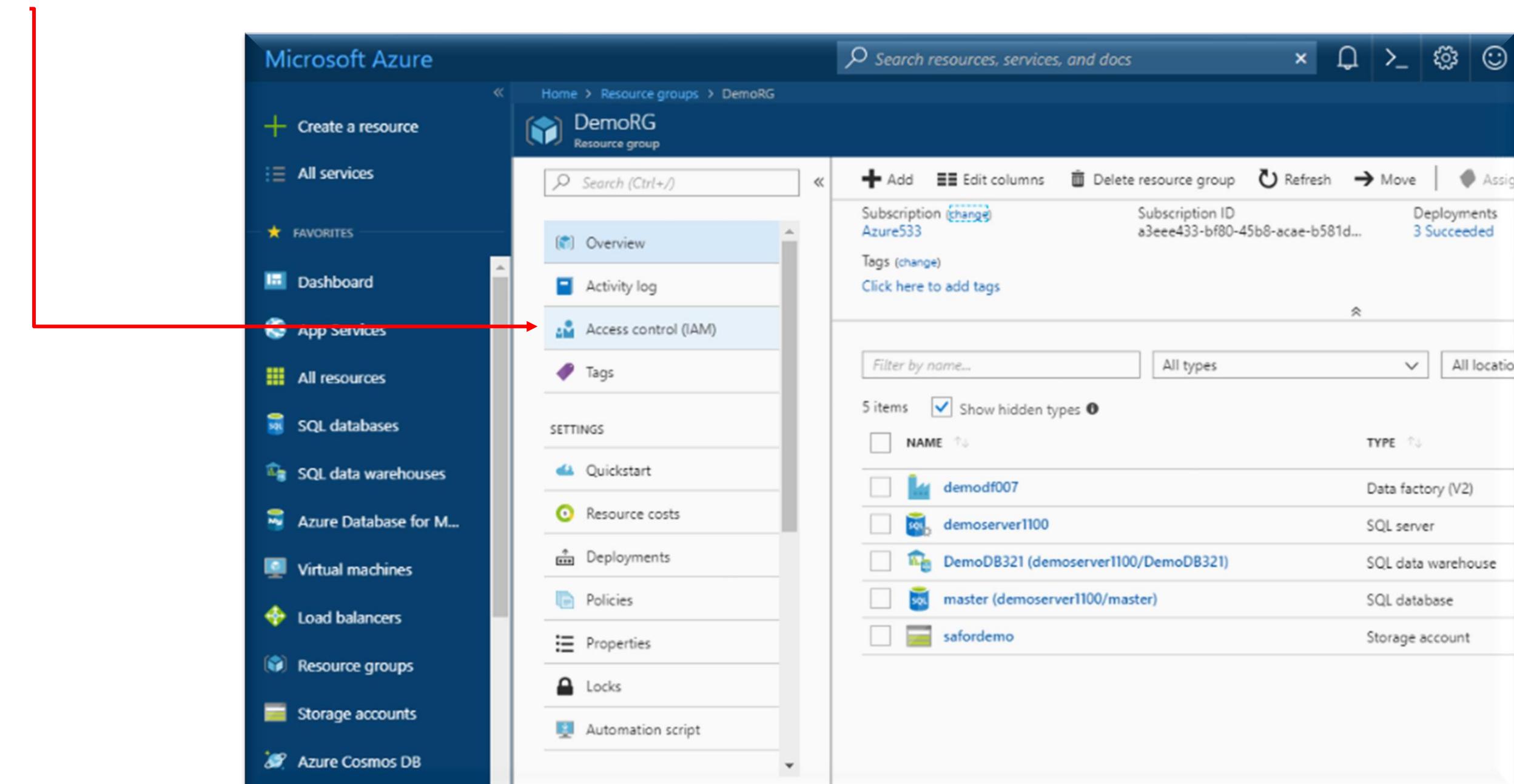
1. Select **Resource Groups** in the navigation bar on the left
2. Select the name of the resource group from the **Resource groups** blade

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation bar includes options like 'Create a resource', 'All services', 'FAVORITES' (with 'My dashboards' listed), 'SQL data warehouses', 'Azure Database for M...', 'Virtual machines', 'Load balancers', 'Resource groups' (which is selected and highlighted in blue), 'Storage accounts', 'Azure Cosmos DB', 'Virtual networks', and 'Azure Active Directory'. The main content area is titled 'Resource groups' and shows a list of 34 items. The list includes 'asgn11', 'asgn2', 'asgn3', 'asgn4', 'AzIoT', 'AzureBackupRG_japanwest_1', 'AzureBackupRG_southcentralus_1', 'AzureBackupRG_SouthIndia_1', and 'cloud-shell-storage-centralindia'. Each item has a checkbox next to it and is associated with the 'Azure533' subscription. The table has columns for 'NAME' and 'SUBSCRIPTION'.

NAME	SUBSCRIPTION
asgn11	Azure533
asgn2	Azure533
asgn3	Azure533
asgn4	Azure533
AzIoT	Azure533
AzureBackupRG_japanwest_1	Azure533
AzureBackupRG_southcentralus_1	Azure533
AzureBackupRG_SouthIndia_1	Azure533
cloud-shell-storage-centralindia	Azure533

RBAC – View Access (Cont.)

3. Select **Access control** from the left menu
4. The **Access control** blade lists all users, groups, and applications that have been granted access to the resource group



RBAC – Add Access

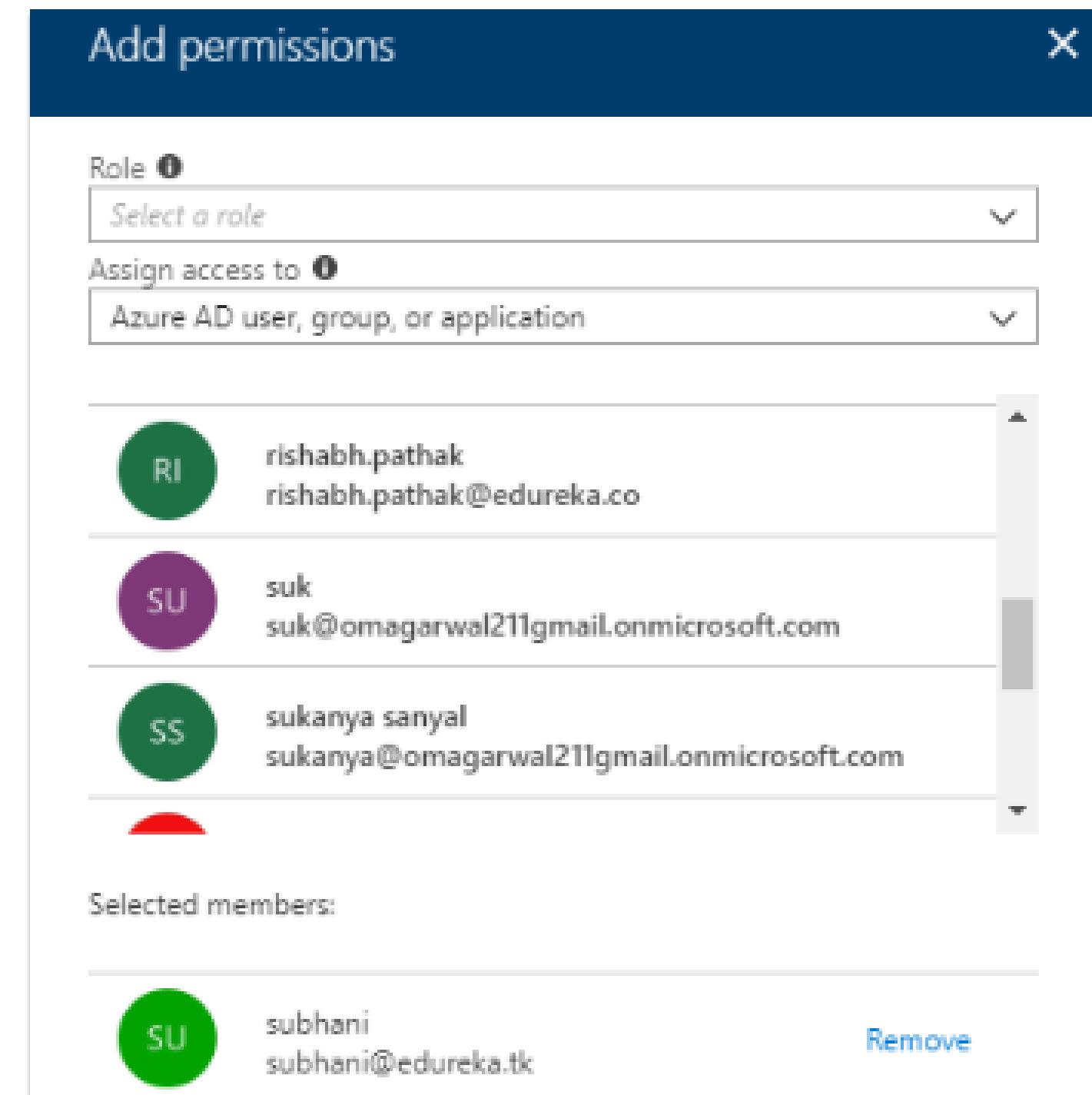
5. Access can be provided from within a resource, resource group, or subscription that is the scope of the role assignment
6. Select **Add** on the Access control blade and select a role that is to be assigned access

The screenshot shows the Azure portal's Access control (IAM) blade for a resource group named "asgn11". The "Access control (IAM)" tab is selected in the left sidebar. A red box highlights the "Add" button in the top navigation bar. The main area displays a table of current access assignments under the "CONTRIBUTOR" section. The table includes columns for NAME, TYPE, ROLE, and SCOPE. Four entries are listed:

NAME	TYPE	ROLE	SCOPE
azure-cli-2018-05-15-0...	App	Contributor	Subscription (Inherited)
EduSP	App	Contributor	Subscription (Inherited)
edusp1	App	Contributor	Subscription (Inherited)
Postman	App	Contributor	Subscription (Inherited)

RBAC – Add Access (Cont.)

7. Select the user, group, or application in your directory that is to be granted access
8. Select **OK** to create the assignment
9. After successfully adding a role assignment, it will appear on the **Users** blade



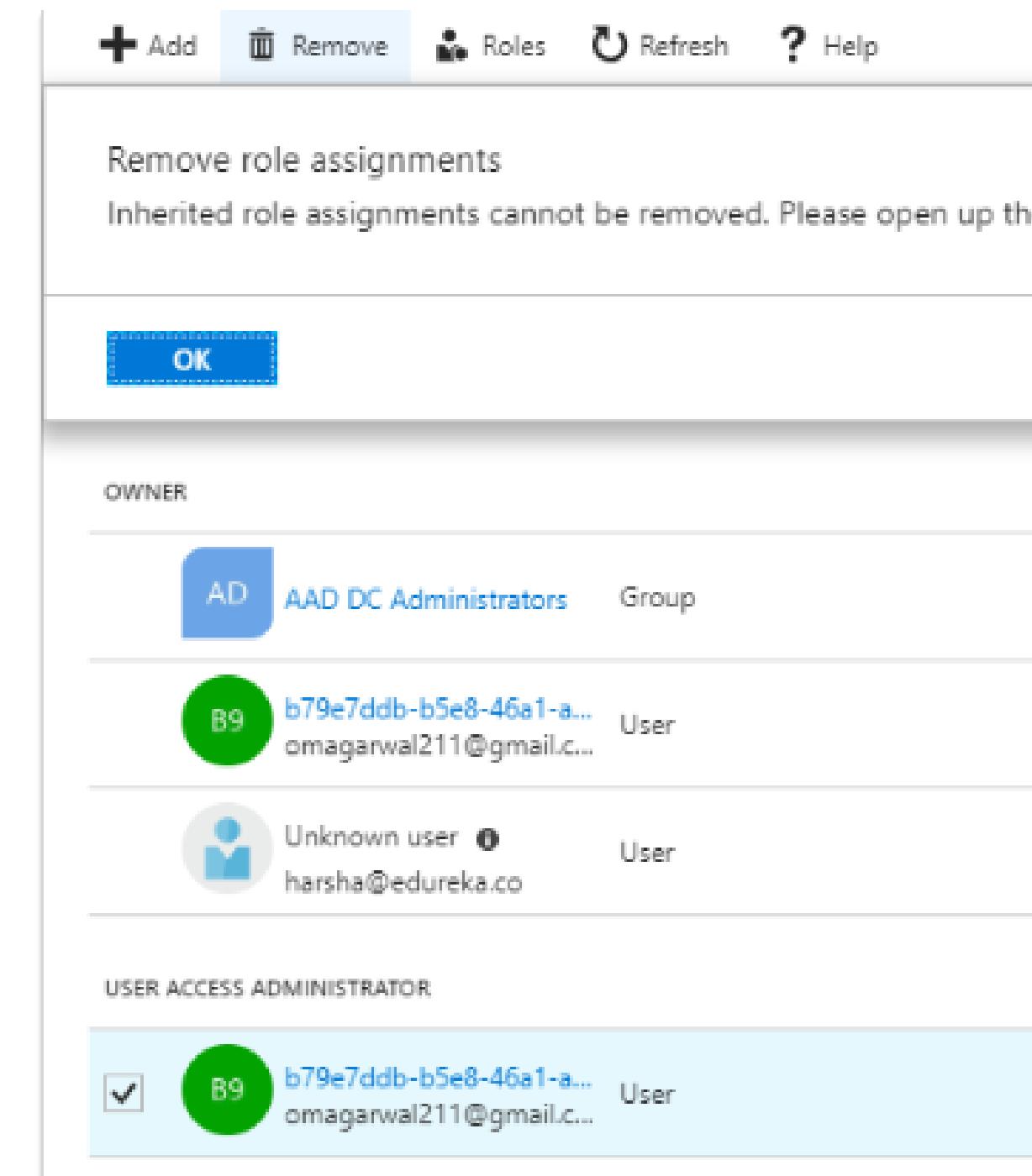
RBAC – Remove Access

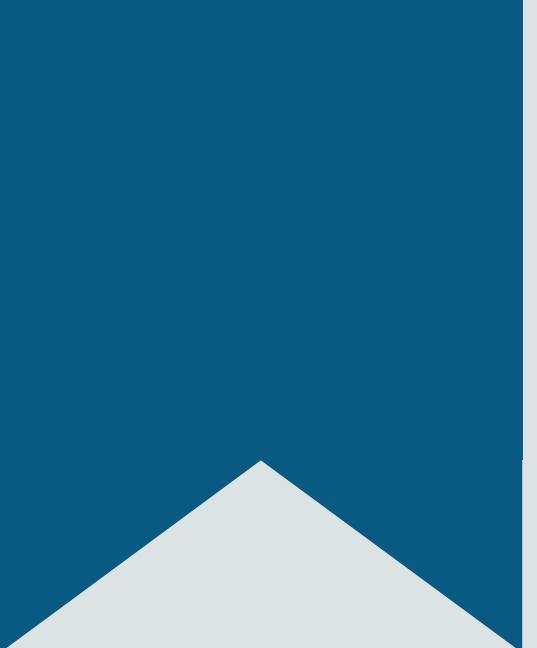
10. Hover your cursor over the name of the assignment that you want to remove. A check box appears next to the name.

11. Use the check boxes to select one or more role assignments.

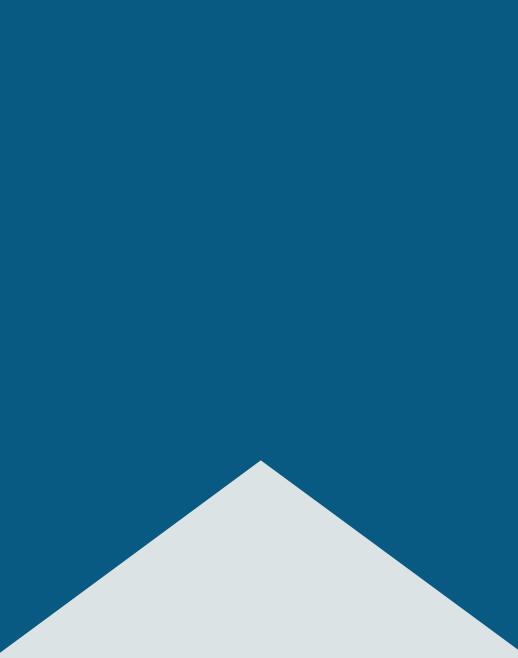
12. Select Remove.

13. Select Yes to confirm the removal.





Demo 1 – Implement Role Based Access Control

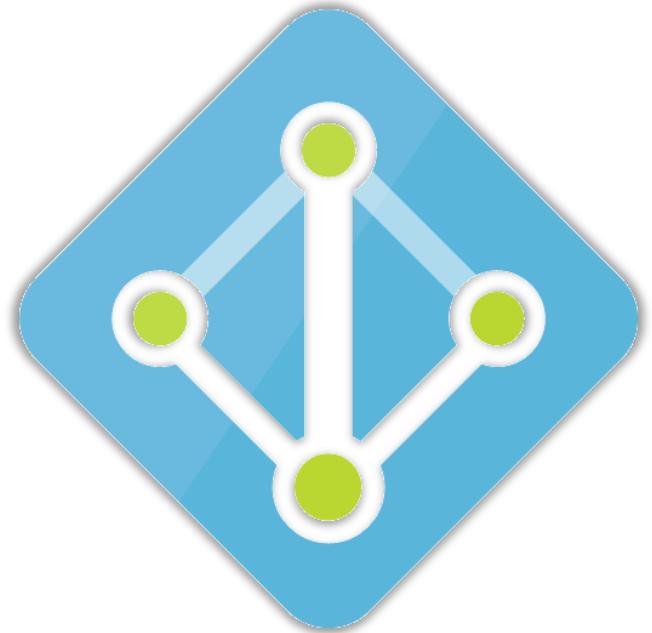


Azure Active Directory

Azure Active Directory (Azure AD)

Azure AD is Microsoft's multi-tenant, cloud-based directory and identity-management service that combines core directory services, application access management, and identity protection into a single solution

- If you already have an on-premises directory, it can be extended to the cloud using the directory integration capabilities of Azure AD
- Azure AD helps users to sign in and access external resources in Azure portal and many other SaaS applications
- It also allows internal access to apps on your corporate network and intranet, along with any cloud apps developed by your own organization



Azure Active Directory

Applications Of Azure AD



IT Administrators

- As an IT admin, you can use Azure AD to control access to your apps and your app resources, based on your business requirements
- Azure AD meets your access governance requirements by protecting user identities and credentials



Application Developers

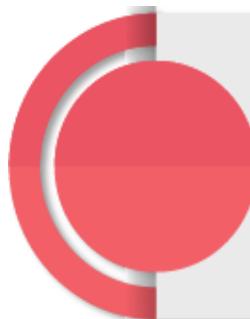
- As an app developer, Azure AD allows single sign-on (SSO) to your app to enable working with a user's pre-existing credentials
- Azure AD also provides APIs to help you build personalized app experiences leveraging existing organizational data



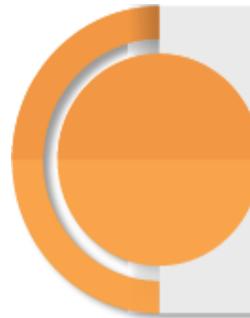
Microsoft Online Subscribers

- Each Microsoft 365, Office 365, Azure, and Dynamics CRM Online tenant is automatically an Azure AD tenant
- One can immediately start managing access to integrated cloud apps

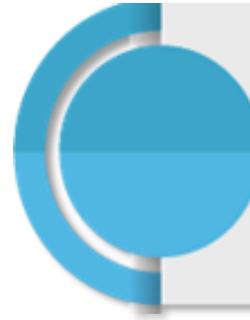
Azure AD Licenses



If you subscribe to any Microsoft Online business service, you automatically get Azure AD with access to all the free features



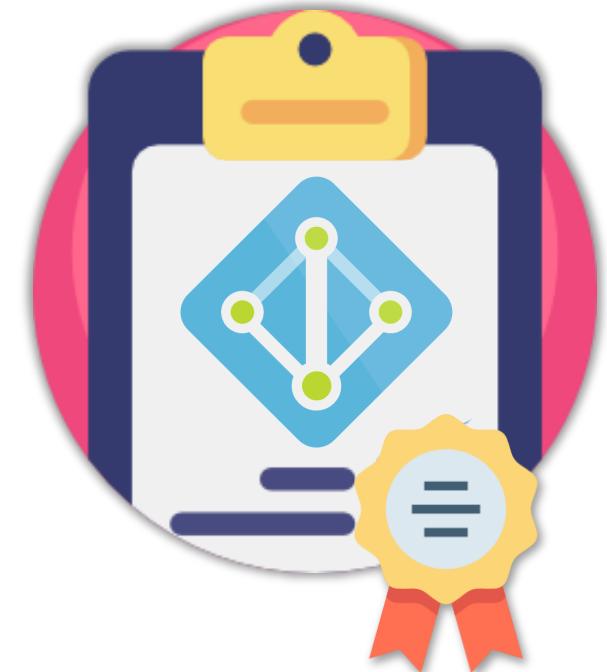
Azure AD paid licenses are built on top of your existing free directory, providing enhanced monitoring, security reporting, and secure access for your mobile workforce



To enhance your Azure AD implementation, you can add paid capabilities by upgrading from Azure Free AD to *Azure Active Directory Basic, Premium P1, or Premium P2* licenses



Pay-as-you-go feature licenses such as *Azure AD Business-to-Customer (B2C)* can help you provide identity and access management solutions for your customer-facing apps



Azure AD Licenses (Cont.)

Azure AD Free

Provides *user and group management, on-premises directory synchronization, and single sign-on* across Azure, Office 365, and many popular SaaS apps

Azure AD Premium P1

Along with the Free and Basic features, P1 also lets your *hybrid users access both on-premises and cloud resources, supports advanced administration, such as dynamic groups, and cloud write-back capabilities*

Azure AD Basic

Along with the Free features, Basic also provides *cloud-centric app access, group-based access management, self-service password reset for cloud apps, and Azure AD Application Proxy*

Azure AD Premium P2

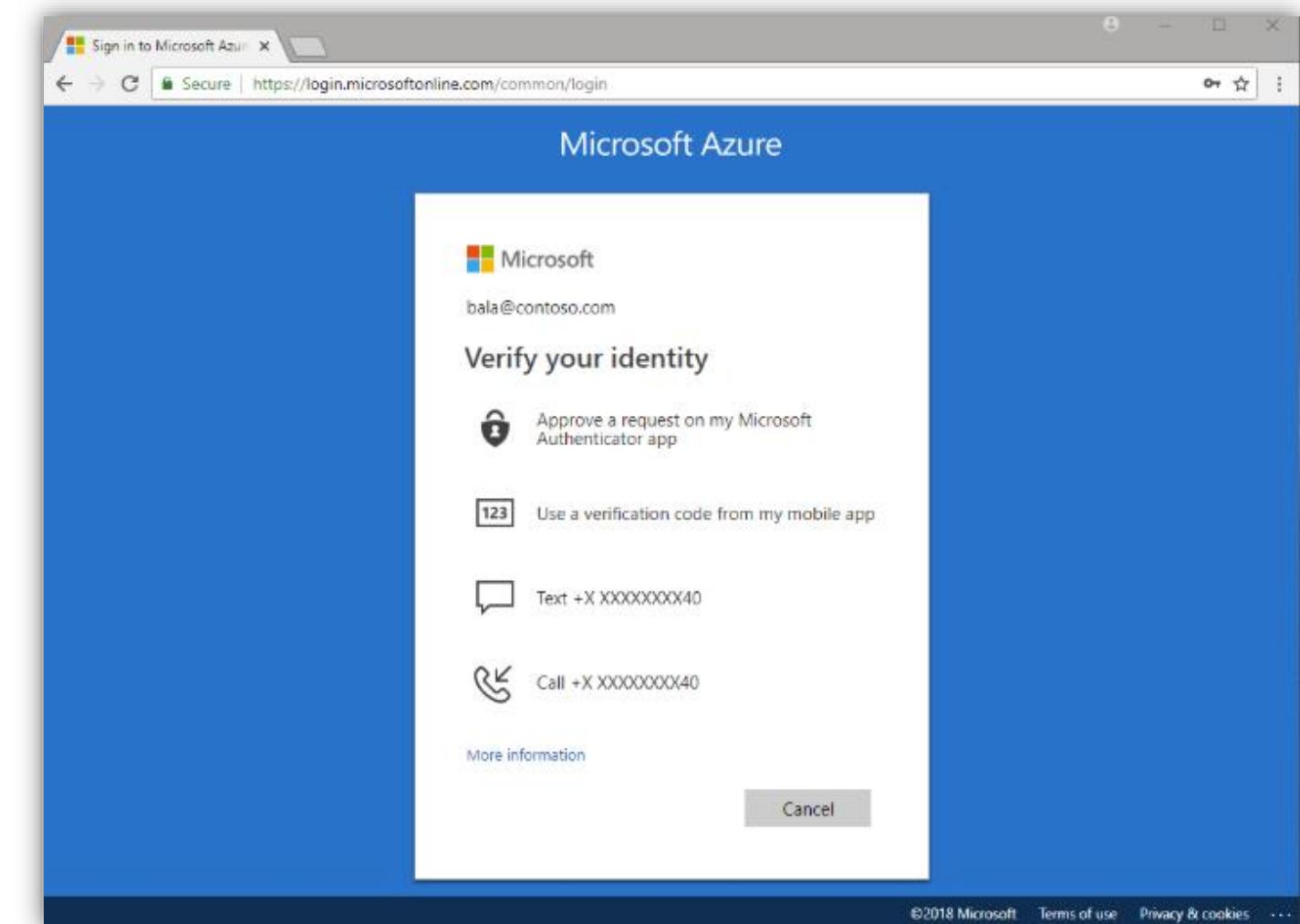
P2 also offers *Azure AD Identity Protection to provide risk-based conditional access to your apps, Privileged Identity Management to discover, restrict, and monitor admins and their access to resources*

Azure AD Authentication Methods

Authentication Methods

- Microsoft Azure AD includes features, like **Azure Multi-Factor Authentication (Azure MFA)** and **Azure AD self-service password reset (SSPR)**, to help administrators protect their organizations and users with additional authentication methods
- Azure MFA and Azure AD SSPR give admins control over configuration, policy, monitoring, and reporting using Azure AD and the Azure portal to protect their organizations
- Additional verification may come in the form of authentication methods such as:

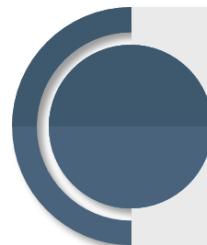
- ▶ A code provided in an email or text message
- ▶ A phone call
- ▶ A notification or code on their phone
- ▶ Answers to security questions



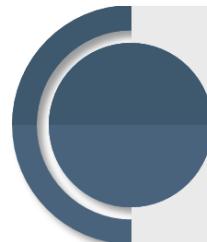
Azure Multi-Factor Authentication (MFA)

Azure MFA is Microsoft's two-step verification solution that helps safeguard your access to data and applications, while meeting the demand for a simple sign-in process

It is recommended that you require Azure MFA for user sign-ins because:



It delivers strong authentication with a range of easy verification options



It enables your organization to protect and recover from account compromises



How Multi-Factor Authentication Works?

Because of Azure MFA's layered approach, even if an attacker manages to learn the user's password, it is useless without also having possession of the additional authentication method

It works by requiring two or more of the following authentication methods:



- Something you know, such as a password



- Something you have - a trusted device that is not easily duplicated, like a phone



- Something you are - biometrics

Azure Multi-Factor Authentication Limitations

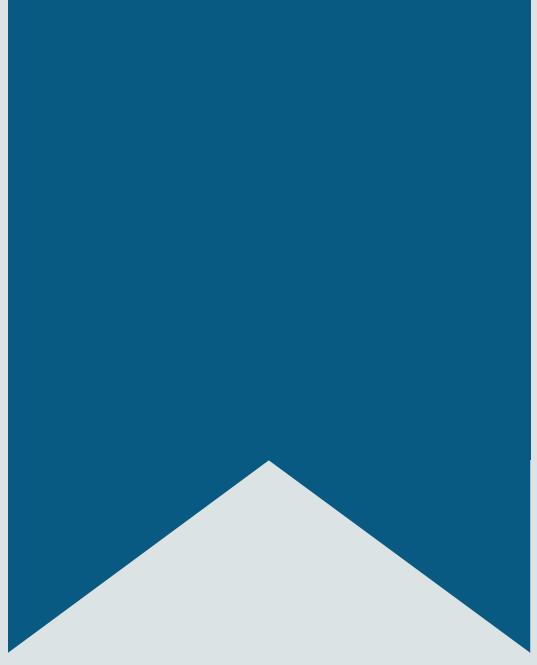
Following are the limitations of the MFA authentication method:



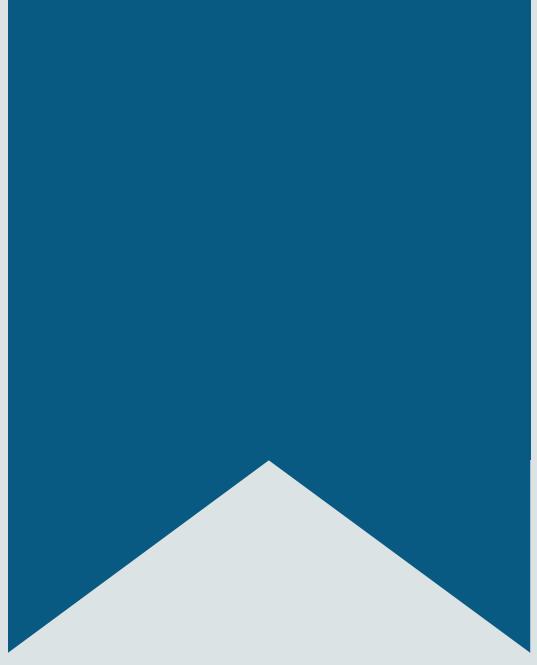
Compromised
Device

Hijacked
Session

Compromised
Data



Demo 2 – Implement Multi-factor Authentication (MFA)



Managing Multiple Directories in Azure

Adding Sub-directories in Azure : Pre-Requisite

Before you can associate or add your subscription, you must perform the following tasks:

1. Sign in using an account that:
 - Has RBAC Owner access to the subscription
 - Exists in both the current directory that's associated with the subscription and in the new directory that's where you want to associate the subscription going forward
2. Make sure you're not using an Azure Cloud Service Providers (CSP) subscription (MS-AZR-0145P, MS-AZR-0146P, MS-AZR-159P), a Microsoft Internal subscription (MS-AZR-0015P), or a Microsoft Imagine subscription (MS-AZR-0144P).

Changing Directory

The screenshot shows the Microsoft Azure portal interface. In the top left, the 'Microsoft Azure' logo is visible. The top navigation bar includes a search bar with the placeholder 'subscription', and icons for 'Dashboard', 'Subscriptions', 'EduDev (Pay-As-You-Go)', 'Manage', 'Transfer', 'Cancel subscription', 'Rename', and 'Change directory'. The 'Change directory' button is highlighted with a green box and a red arrow pointing to it. On the far right of the top bar, there is a user profile icon with the email 'cloud@edureka.co' and the text 'DEFAULT DIRECTORY'. The main content area displays the 'EduDev (Pay-As-You-Go)' subscription details, including the Subscription ID (01b35b80-3ba8-469f-8c59-1450494934ba), Directory (Default Directory (cloudedureka.onmicrosoft.com)), My role (Account admin), Offer (Pay-As-You-Go), Offer ID (MS-AZR-0003P), and various status metrics like Current billing period (Loading...), Currency (INR), and Status (Active). Below this, there is a section for 'Cost Management' with links to 'Cost analysis', 'Budgets', and 'Advisor recommendations'. A large blue callout bubble at the bottom left provides instructions: 'Sign in and select the subscription you want to use from the Subscriptions page in Azure portal > Select Change directory.'

Changing Directory (Cont.)

The screenshot shows the Microsoft Azure portal interface. On the left is the navigation sidebar with various service icons. The main area displays the 'EduDev (Pay-As-You-Go)' subscription dashboard, including sections for Overview, Access control (IAM), Diagnose and solve problems, Security, Events, Cost Management, and Billing. A 'Change the directory' modal window is open over the dashboard. The modal contains two informational cards: one about removing access for Role-Based Access Control users and another about billing ownership. It also shows the current directory (Default Directory) and a dropdown for selecting a new directory ('azureedureka'). A large blue callout bubble with rounded corners points to the 'Change' button at the bottom right of the modal, which is highlighted with a green border and a red arrow pointing to it.

Review any warnings that appear, and then select **Change**

Updated Directory in Portal

The screenshot shows the Microsoft Azure portal's Subscriptions page. On the left, the navigation menu includes options like Create a resource, Home, Dashboard, All services, Favorites (with All resources, Resource groups, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, and Storage accounts), and a blue callout box at the bottom stating: "Use the Directory switcher to go to your new directory. It might take up to 10 minutes for everything to show up properly."

The main content area displays the Subscriptions page with the following details:

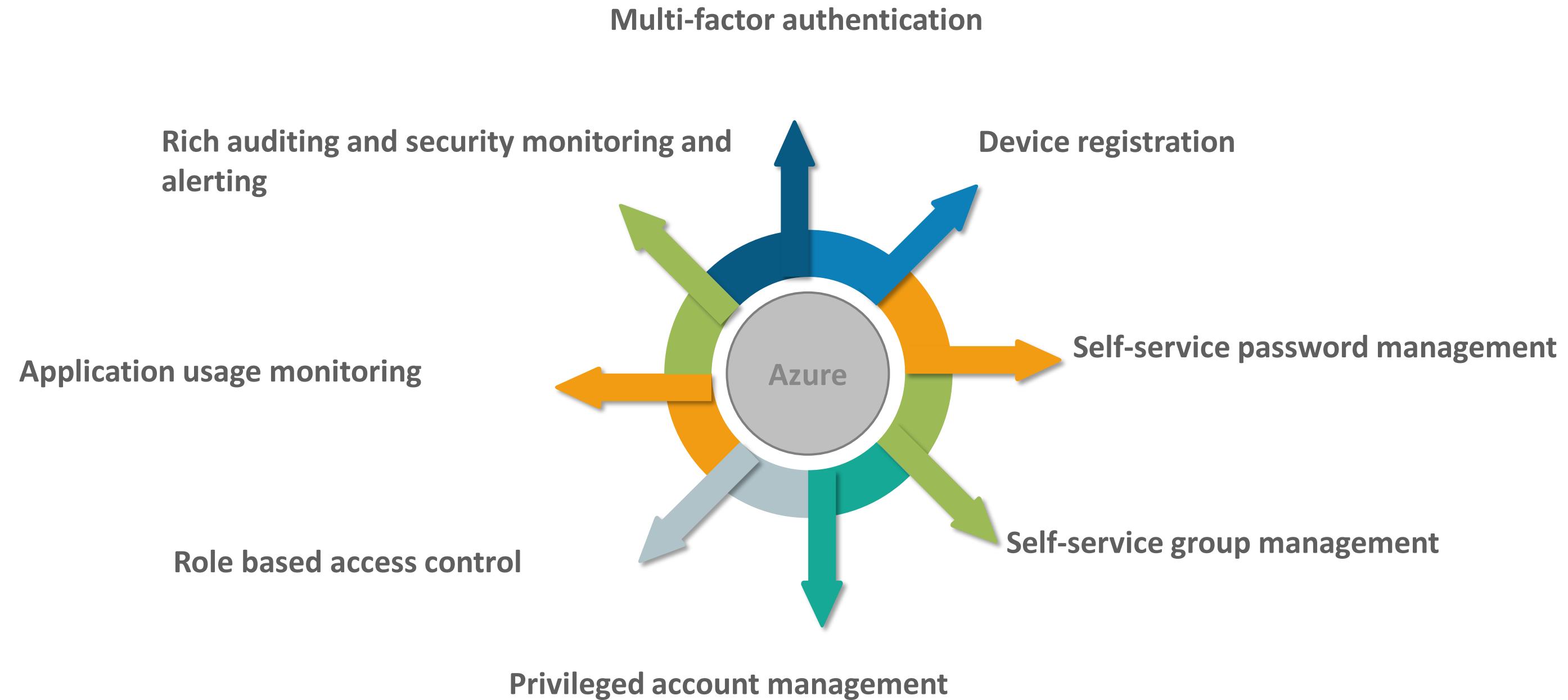
SUBSCRIPTION	SUBSCRIPTION ID	MY ROLE
EduDev (Pay-As-You-Go)	01b35b80-3ba8-469f-8c59-1450494934ba	Account admin

A red box highlights the "MY ROLE" column. To the right, a modal window titled "Directory + subscription" provides information about the global subscription filter:

- Global subscription filter: The portal will show data only for these subscriptions.
- Current directory: cloudedureka.onmicrosoft.com
- Learn about directories and subscriptions

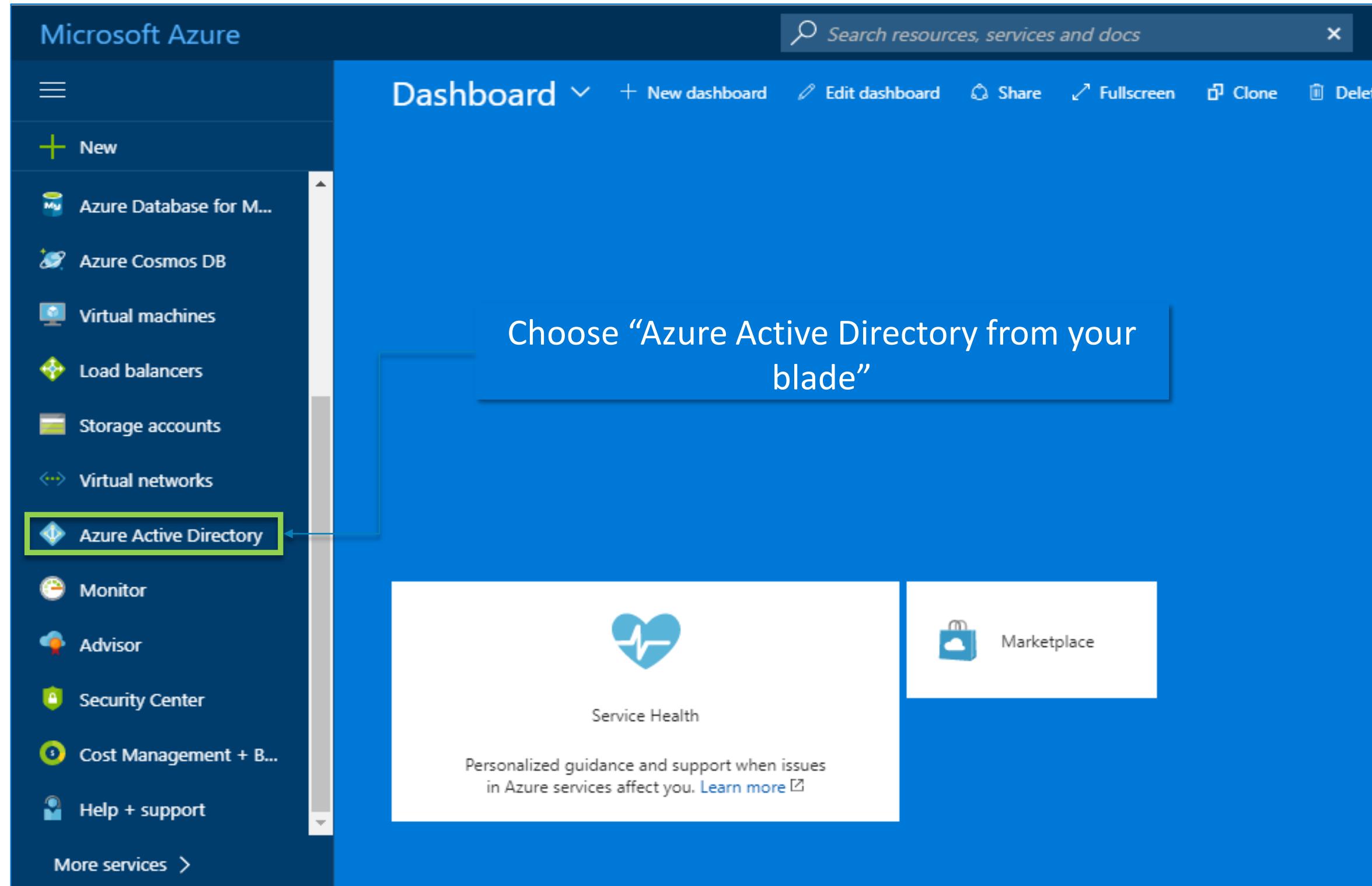
The modal also includes a "Switch directory" section with a dropdown for "Sign in to your last visited directory". Below it are tabs for "Favorites" and "All Directories" (which is selected), and a search bar.

Azure AD Identity Management Capabilities



These capabilities can help secure cloud based applications, streamline IT processes, cut costs and help ensure that corporate compliance goals are met.

Azure AD



Azure AD – Users and Groups Overview

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Database, Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + B..., Help + support, and More services >. The main area is titled 'omagarwal211gmail (default directory) Azure Active Directory'. It has a navigation bar with 'Overview' (selected), 'Quick start', 'Switch directory', and 'Delete directory'. Below this is a 'MANAGE' section with 'Users and groups' (highlighted with a green box), 'Enterprise applications', 'Devices (Preview)', 'App registrations', 'Application proxy', 'Licenses', 'Azure AD Connect', 'Domain names', 'Mobility (MDM and MAM)', and 'Password reset'. To the right is a 'Quick tasks' panel with links to 'Add a user', 'Add a guest user', 'Add a group', 'Find a user', 'Find a group', and 'Find an enterprise app'. At the bottom, there's a 'Start a free trial to use this feature.' button, a timestamp '5:30 AM', and a 'App registrations' section showing '0'.

- Azure AD follows “Identity as a service” model
- In management of users you can arrange those users in groups
- Then based on the roles you can assign those permissions to those groups

Azure AD – Quick Task Overview

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Azure Database, Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management, and Help + support. The main area is titled 'omagarwal211gmail (default directory) Azure Active Directory'. It has sections for 'Overview', 'Quick start', 'MANAGE' (with options like Users and groups, Enterprise applications, Devices (Preview), App registrations, Application proxy, Licenses, Azure AD Connect, Domain names, Mobility (MDM and MAM), and Password reset), and 'Enterprise applications' (with a 'Start a free trial to use this feature.' button). A 'Quick tasks' section is highlighted with a green border and contains links for Add a user, Add a guest user, Add a group, Find a user, Find a group, and Find an enterprise app. The top right corner shows a search bar, a notification bell with 2 notifications, and a gear icon.

Here you can perform Quick tasks like:

- Add User, Guest user
- Add a Group
- Perform search

Azure AD Connect

The screenshot shows the Microsoft Azure portal interface. The left sidebar lists various services: Azure Database for MySQL, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory (selected), Monitor, Advisor, Security Center, Cost Management + Billing, Help + support, and More services >. The main content area is titled 'omagarwal211gmail (default directory)' and 'Azure Active Directory'. It features an 'Overview' card with a globe icon and 'B9' users. Below it is a 'Users and groups' section with a globe icon and 'B9' users. To the right is a 'Quick tasks' panel with links: Add a user, Add a guest user, Add a group, Find a user, Find a group, and Find an enterprise app. A callout box highlights the 'Azure AD Connect' link under the 'Enterprise applications' section, which is described as the 'Synchronization' feature.

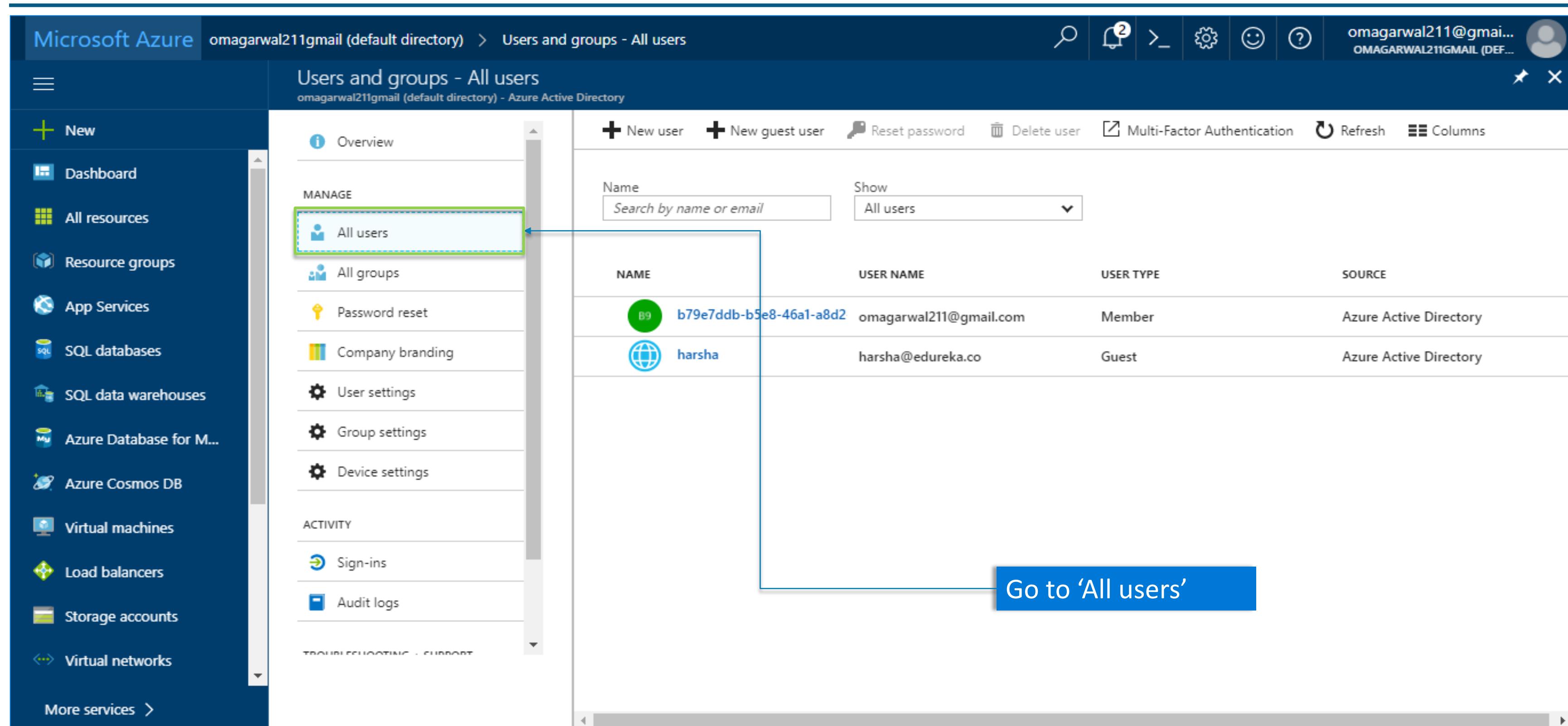
Here we can connect Azure Active Directory and on premises Active Directory

This is the Synchronization



Adding New User to AD

Adding New User to AD



Microsoft Azure omagarwal211gmail (default directory) > Users and groups - All users

Users and groups - All users

MANAGE

- All users
- All groups
- Password reset
- Company branding
- User settings
- Group settings
- Device settings

ACTIVITY

- Sign-ins
- Audit logs

New user New guest user Reset password Delete user Multi-Factor Authentication Refresh Columns

NAME	USER NAME	USER TYPE	SOURCE	
B9	b79e7ddb-b5e8-46a1-a8d2	omagarwal211@gmail.com	Member	Azure Active Directory
	harsha	harsha@edureka.co	Guest	Azure Active Directory

Go to 'All users'

Adding New User to AD (Cont.)

The screenshot shows the Microsoft Azure portal interface for managing users in an Azure Active Directory. The left sidebar lists various services like Dashboard, All resources, Resource groups, App Services, etc. The main area is titled 'Users and groups - All users' and shows a table of existing users. A green box highlights the '+ New user' button in the top navigation bar. A blue callout box points to this button with the text 'Click – ‘Add New user’'.

Users and groups - All users

MANAGE

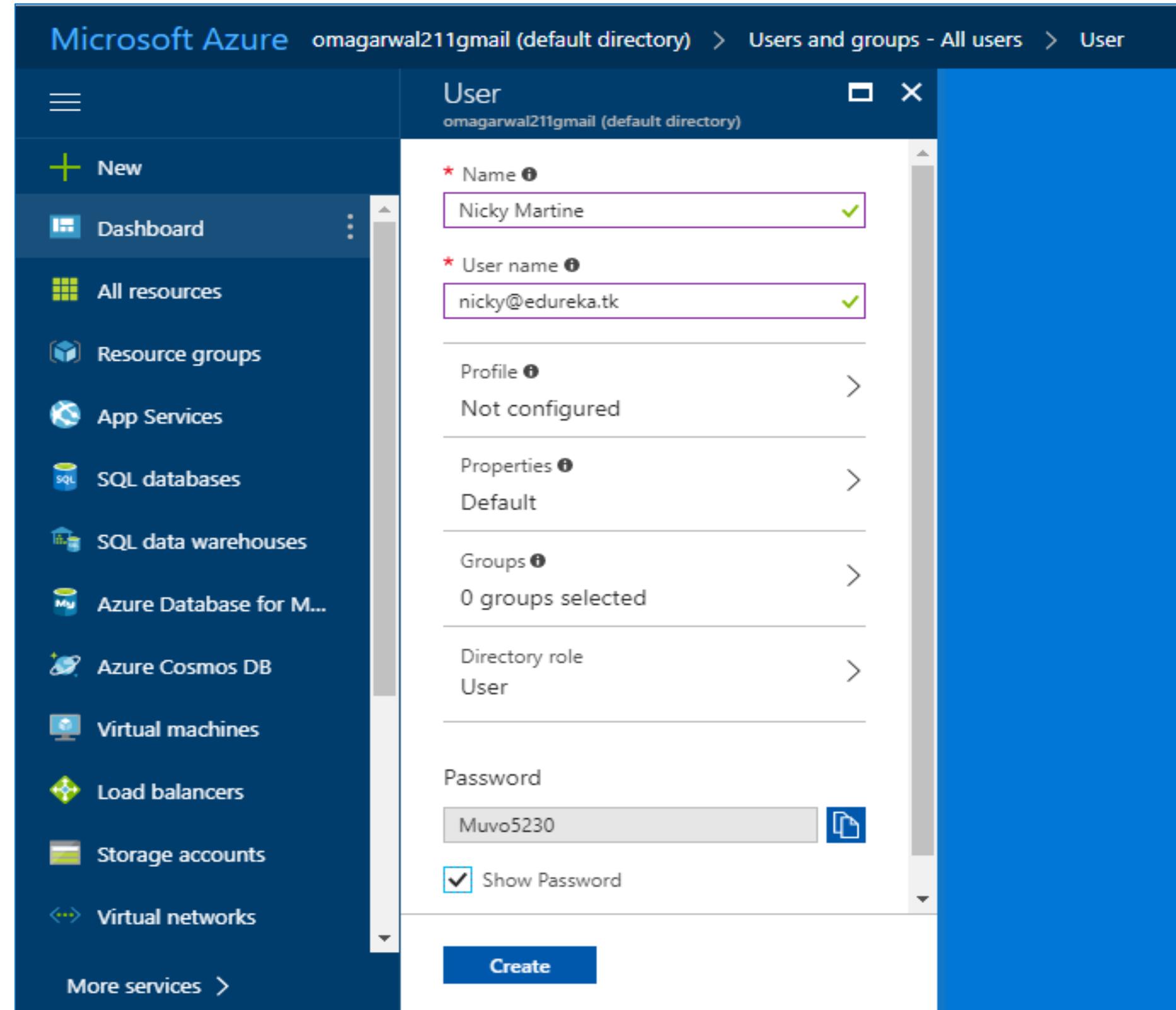
- + New user
- + New guest user
- Reset password
- Delete user
- Multi-Factor Authentication
- Refresh
- Columns

NAME	USER NAME	USER TYPE	SOURCE
B9 b79e7ddb-b5e8-46a1-a8d2	omagarwal211@gmail.com	Member	Azure Active Directory
harsha	harsha@edureka.co	Guest	Azure Active Directory

Click – ‘Add New user’

Registering New User

Register new user here and click – ‘Create’

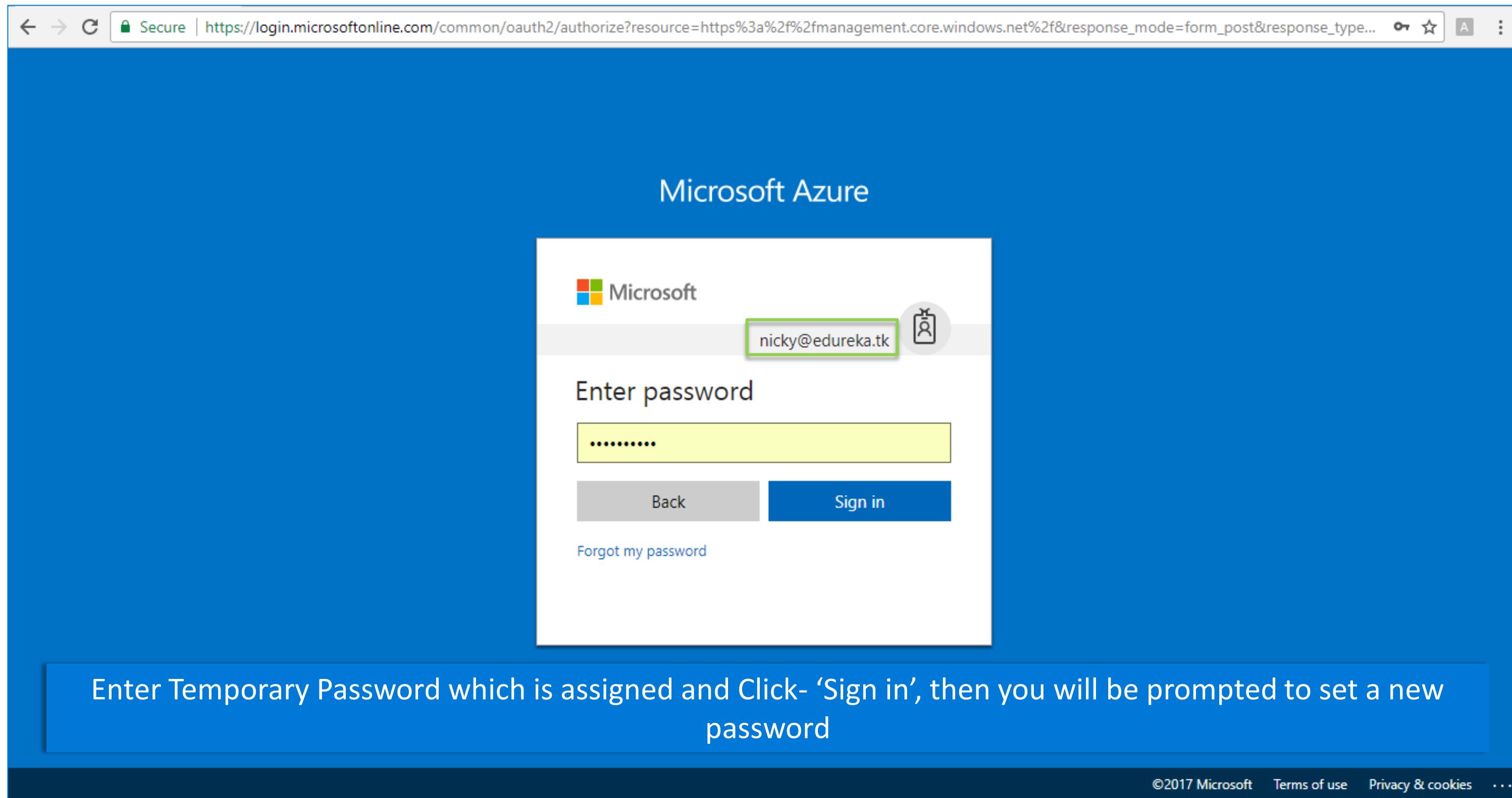


Successfully Added New User

The screenshot shows the Microsoft Azure portal interface for managing users in the 'omagarwal211gmail (default directory)' tenant. The left sidebar lists various Azure services like Dashboard, All resources, Resource groups, App Services, etc. The main content area is titled 'Users and groups - All users' under 'Azure Active Directory'. The 'New user' button is highlighted with a blue border. The user list table has columns: NAME, USER NAME, USER TYPE, and SOURCE. It shows three users: one with a green circular profile picture (b79e7ddb-b5e8-46a1-a8d2), one with a blue globe icon (harsha), and one with a pink circle (Nicky Martine). A green rectangular callout box with the text 'New User is created' points to the last row. The top right corner shows the user's email (omagarwal211@gmail.com) and name (OMAGARWAL211GMAIL).

NAME	USER NAME	USER TYPE	SOURCE
B9 b79e7ddb-b5e8-46a1-a8d2	omagarwal211@gmail.com	Member	Azure Active Directory
harsha	harsha@edureka.co	Guest	Azure Active Directory
NM Nicky Martine	nicky@edureka.tk	Member	Azure Active Directory

Successfully Added New User (Cont.)



Successfully Added New User (Cont.)

The screenshot shows the Microsoft Azure portal dashboard at <https://portal.azure.com/#dashboard/private/e216cb6d-a752-4387-8c74-9c3452966011>. The top navigation bar includes a search bar, notification icons, and a user profile for "nicky@edureka.tk OMAGARWAL211GMAIL (DEFA...)".

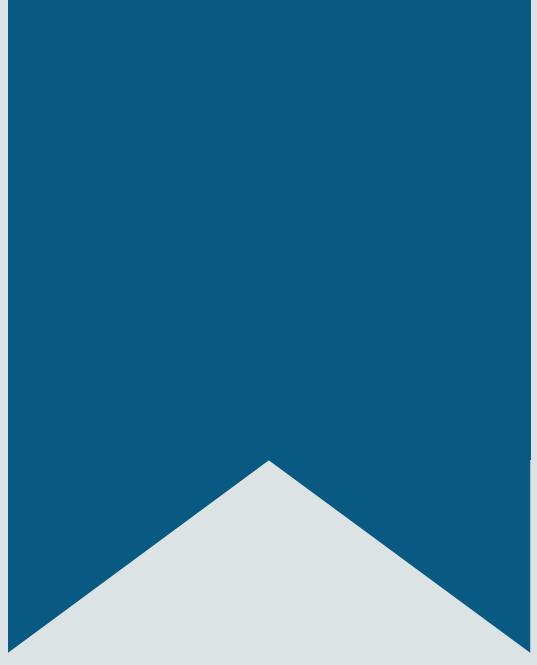
The left sidebar lists various Azure services: Dashboard, All resources, Resource groups, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, and Monitor. A "New" button is also present.

The main dashboard area displays a list of "All resources" from "ALL SUBSCRIPTIONS". The list includes:

- demo-acc Automation Account
- AzureAutomationTutorial Runbook
- AzureAutomationTutorialPython2 Runbook
- AzureAutomationTutorialScript Runbook
- AzureClassicAutomationTutorial Runbook
- AzureClassicAutomationTutorial... Runbook
- demorgdiag661 Storage account
- demo-rg-vnet Virtual network
- demo-vm Virtual machine
- demo-vm_OsDisk_1_a494edb95... Disk
- demo-vm906 Network interface
- demo-vm-ip Public IP address
- demo-vm-nsg Network security gro...

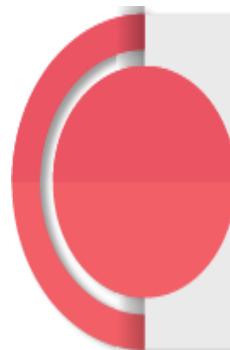
A central callout box titled "Azure getting started made easy!" encourages users to "Launch an app of your choice on Azure in a few quick steps" and provides a "Create DevOps Project" button. Below this, there are "Quickstart tutorials" for Windows Virtual Machines, Linux Virtual Machines, App Service, and Functions.

A blue banner at the bottom states: "Post Sign-in you are redirected to users Dashboard".



Access Reviews in Azure

Introduction to Access Review



To reduce the risk associated with stale access assignments, administrators can use Azure AD to create access reviews for group members or application access



Azure Active Directory (Azure AD) Access Reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments



User's access can be reviewed on a regular basis to make sure only the right people have continued access



Access to groups and applications for employees and guests changes over time and If you need to routinely review access, you can also create recurring access reviews



Enable Access Review

Microsoft Azure

Home > Access reviews

Access reviews

Quick start

Overview

Manage

- Programs
- Controls
- Onboard

Activity

Audit logs

Use Access Reviews to

- Review and reduce employee and guest's group memberships and access to enterprise applications
- Organize and track reviews for compliance and risk management initiatives
- Clean up guest users in Office Groups

1. What are Access Reviews

2. How to create Access Reviews

Onboard to start using these features
Default Directory has not yet onboarded. Click the "Onboard" link to get started using these features.

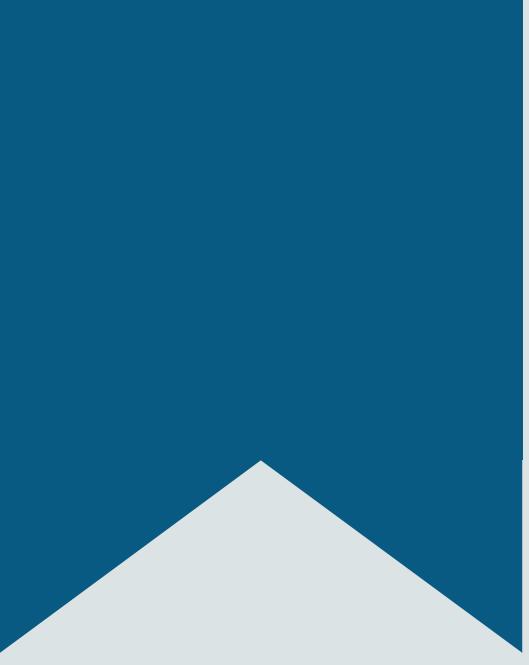
Search for *Access Review* in the Azure Search box > Select Access Reviews > Click on Onboard

Enable Access Review (Cont.)

The screenshot shows the 'Onboard access reviews' page in the Microsoft 365 Admin Center. The URL in the address bar is [https://admin.microsoft.com/AdminPortal/Home#/AccessReviews/OnboardAccessReviews](#). The page title is 'Onboard access reviews'. It displays a 'Default Directory' section with a lock icon and a 'Using access reviews you are able to:' list:

- Leverage attestation to increase visibility of access rights in your organization
- Manage guest user access
- Recertify group memberships and application access

A callout box with a blue border and white text points to the 'Create' button at the bottom left of the page. The text inside the callout box reads: 'Click on Create > When you open the Access Review tab next time, the access review options will be enabled'.



Authentication

Understanding Authentication

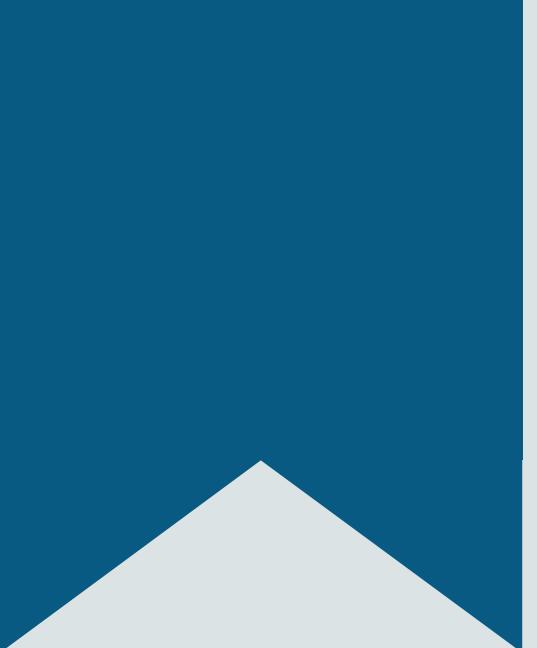
- 1 Authentication is about validating your credentials such as Username/User ID and password to verify your identity
- 2 The system then checks whether you are what you say you are using your credentials and when it comes to security at least two or all the three authentication factors must be verified in order to grant someone permission to the system
- 3 Whether in public or private networks, the system authenticates the user identity through login passwords
- 4 Authentication factors determine the many different elements the system uses to verify one's identity before granting the individual access to anything



Authorization

Understanding Authorization

- 1 Authorization occurs after your identity is successfully authenticated by the system, which therefore gives you full access to resources such as information, files, databases, funds, etc.
- 2 Authorization verifies your rights to grant you access to resources only after determining your ability to access the system and up to what extent
- 3 Authorization is the process to determine whether the authenticated user has access to the particular resources
- 4 A good example of this is, once verifying and confirming employee ID and passwords through authentication, the next step would be determining which employee has access to which floor and that is done through authorization

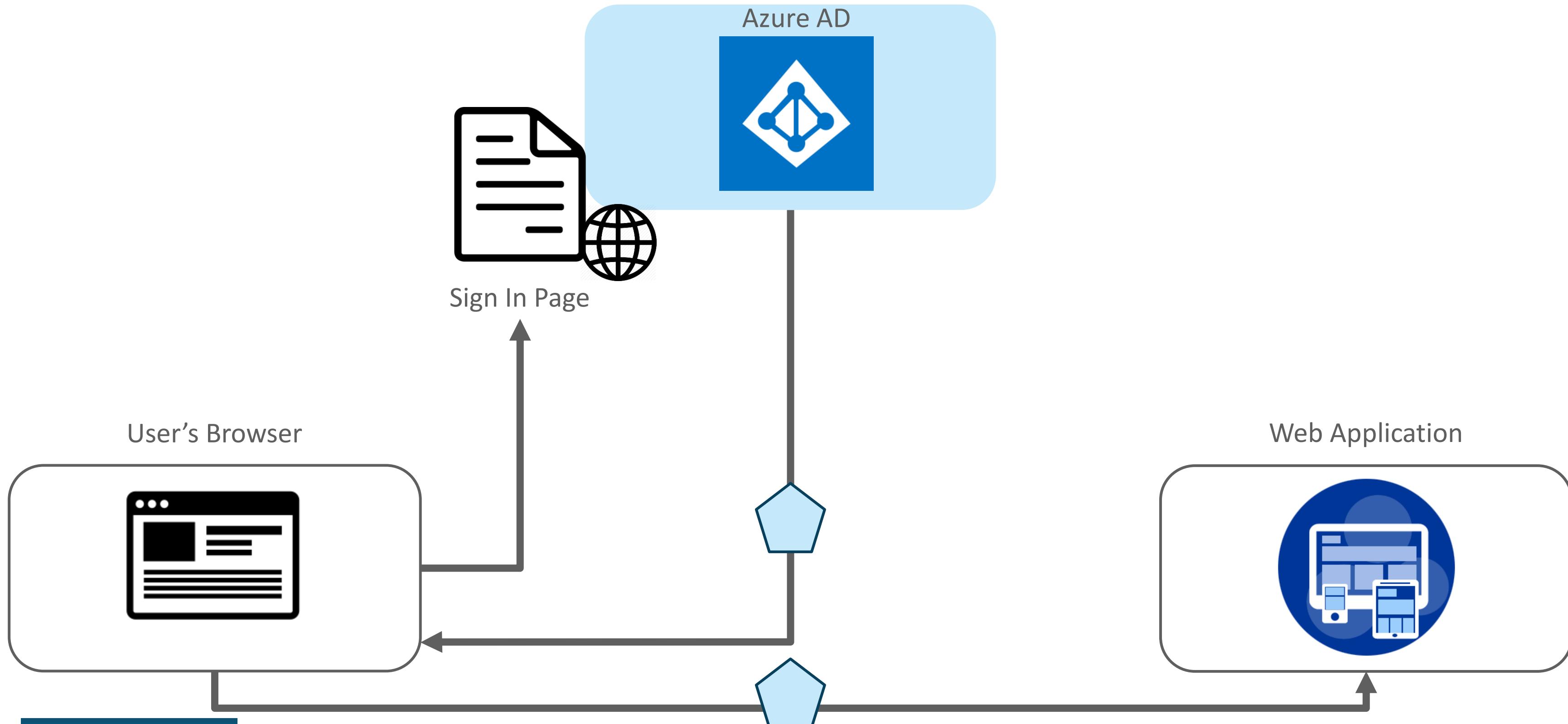


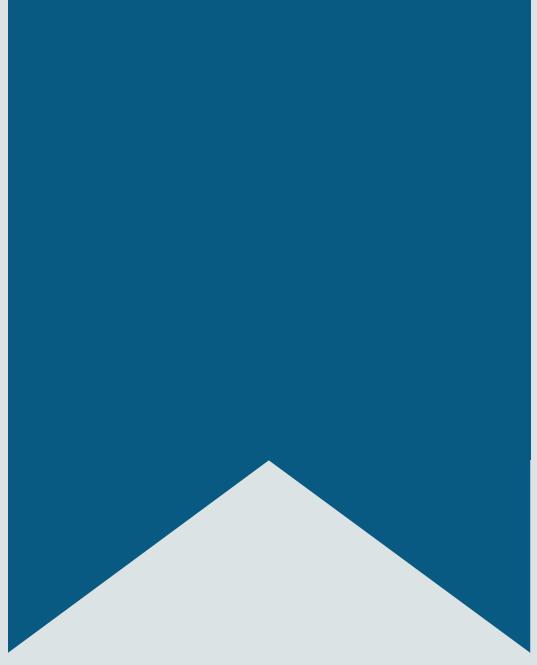
Authentication in Azure Active Directory

Authentication in Azure AD

Authentication is the act of challenging a party for legitimate credentials, providing the basis for creation of a security principal to be used for identity and access control. In simpler terms, it's the process of proving you are who you say you are. Authentication is sometimes shortened to AuthN. Azure Active Directory (Azure AD) simplifies authentication for application developers by providing identity as a service, with support for industry-standard protocols such as OAuth 2.0 and OpenID Connect, as well as open-source libraries for different platforms to help you start coding quickly.

Authentication Workflow in Azure AD





Claim Based Architecture

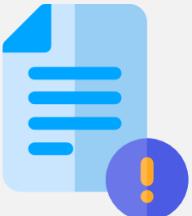
Claim Based Architectural Aspects

Securable Entity And Its Attributes



Refers to User, Application or service entity which makes **service requests**

Claim



Assertion made on entity attribute

Security Token



Collection of Claims which often signed, encrypted and transferred through **secured channel**

Service Provider/ Relaying Party



Provides requested services and relies on **third-party** for identity management

Identity Provider



Issues security token to Relaying Party and **authenticates** entity

Trust



Relationship that ties Service Provider and Identity Provider together

Authentication

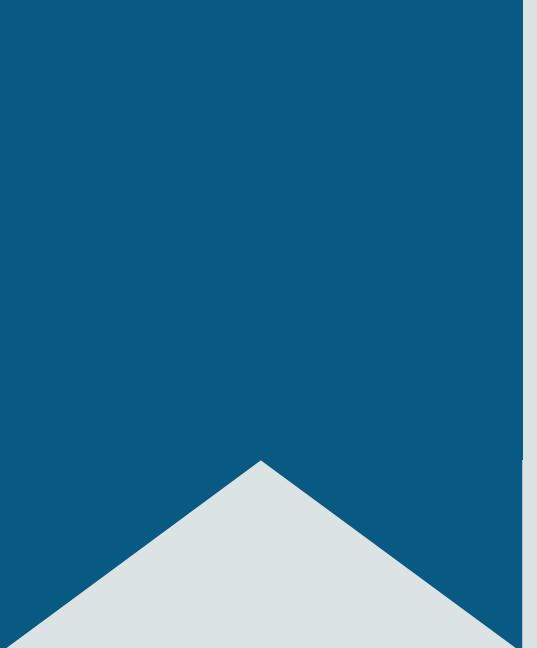


Verifies whether an entity is indeed what it **claims** itself to be

Authorization



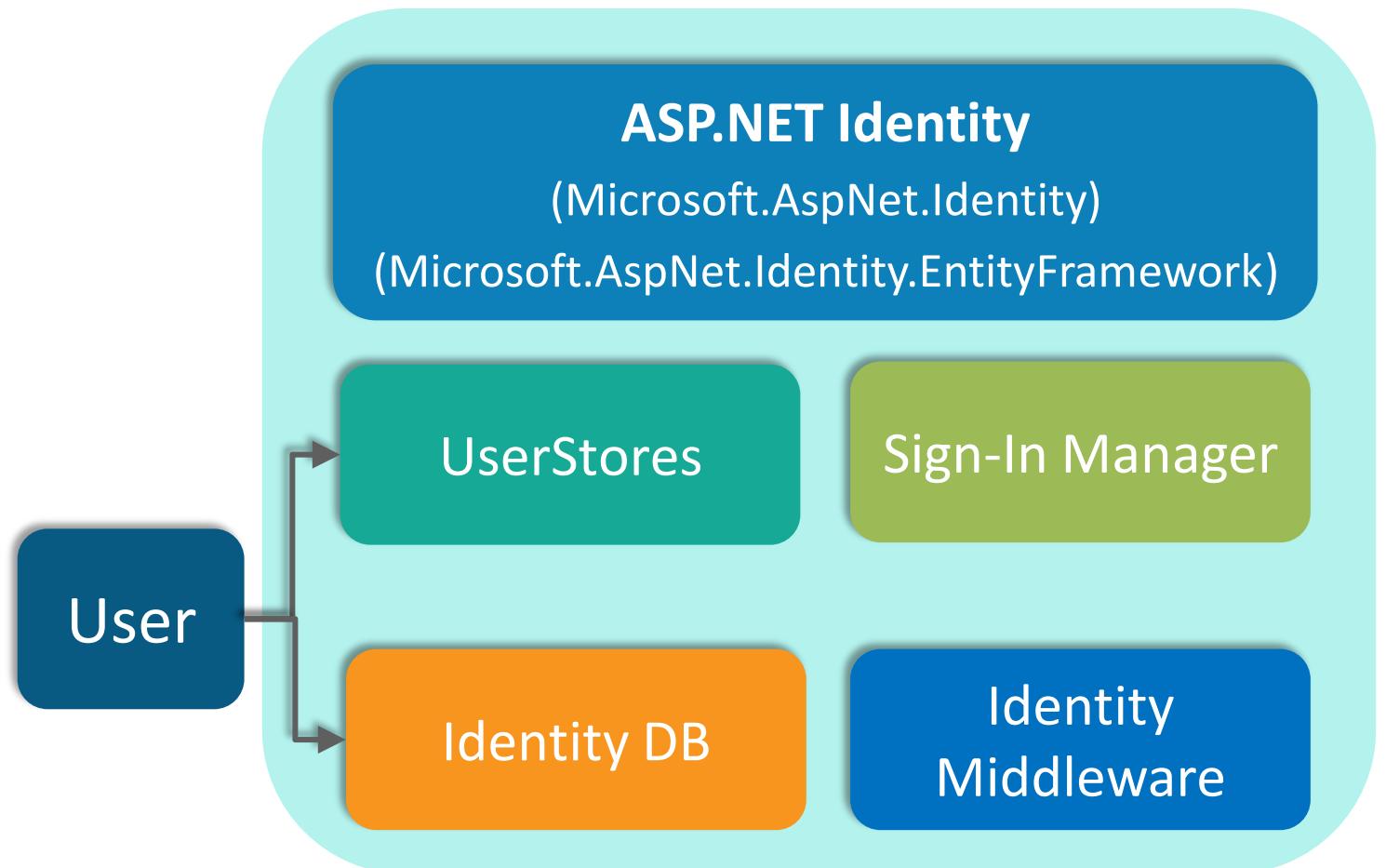
Process to decide whether an **authenticated** user has access to certain functionalities



Azure Active Directory – Authentication Frameworks

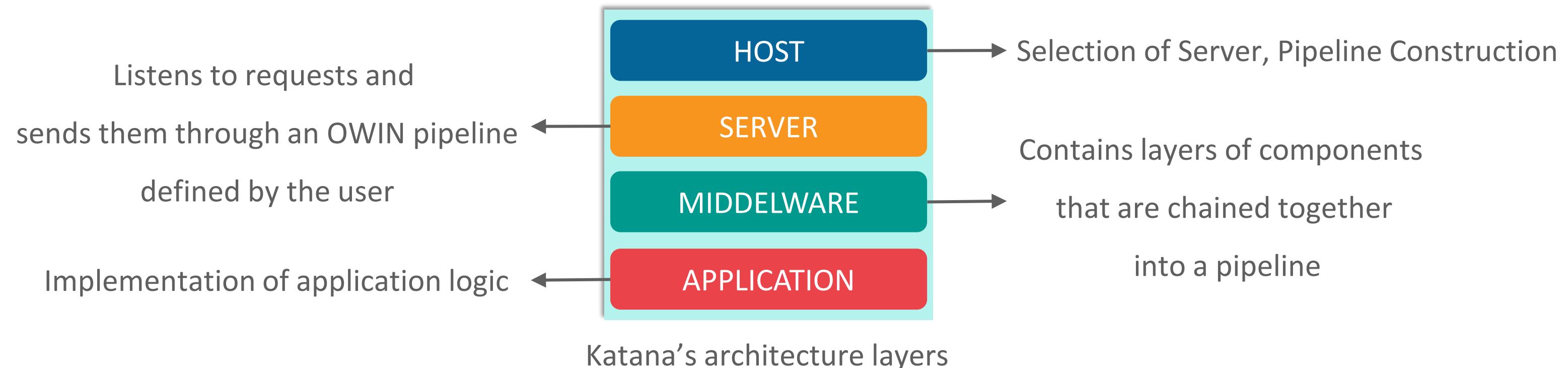
ASP.NET Core Identity

- ASP.NET and ASP.NET Core uses different Authentication Frameworks
- ASP.NET 5 uses OWIN Authentication Middleware
- ASP.NET uses ASP.NET Core Identity
- **ASP.NET Core Identity**
 - Membership system
 - Allows built in support for Authentication and User Management
 - Need to configure a User Store such as a SQL Server database
 - Authentication with External Identity Providers
 - Need to configure User application to use the OAuth 2.0 protocol to work with selected Identity Provider

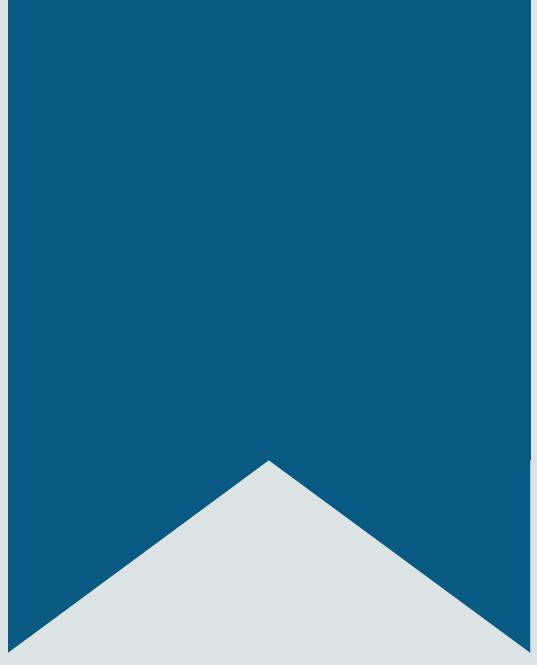


Open Web Interface for .NET (OWIN)

- Defines an abstraction layer between web applications and web servers
- Decouples web applications and web server
- Katana is an implementation of OWIN
- Katana has layered architecture

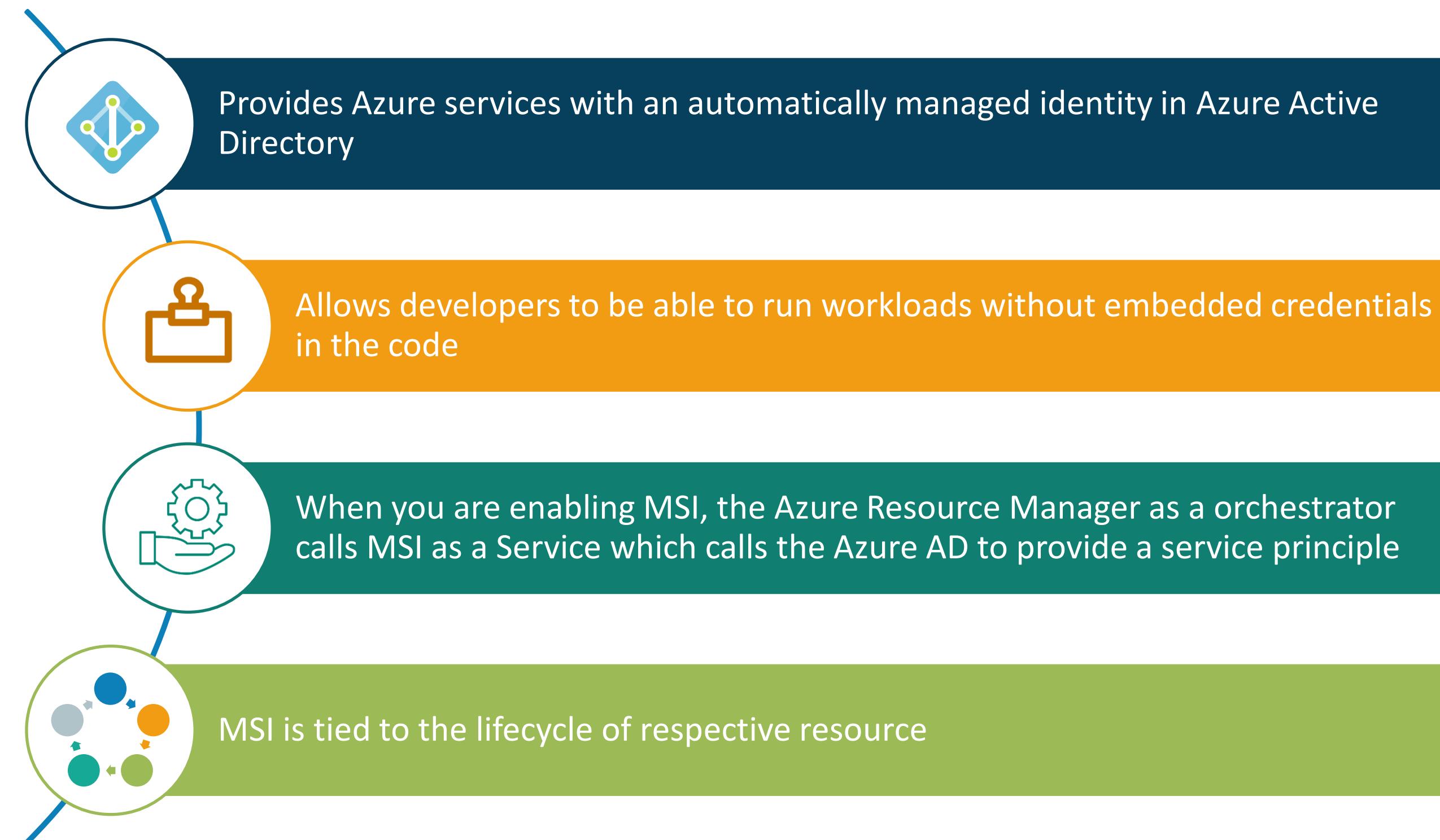


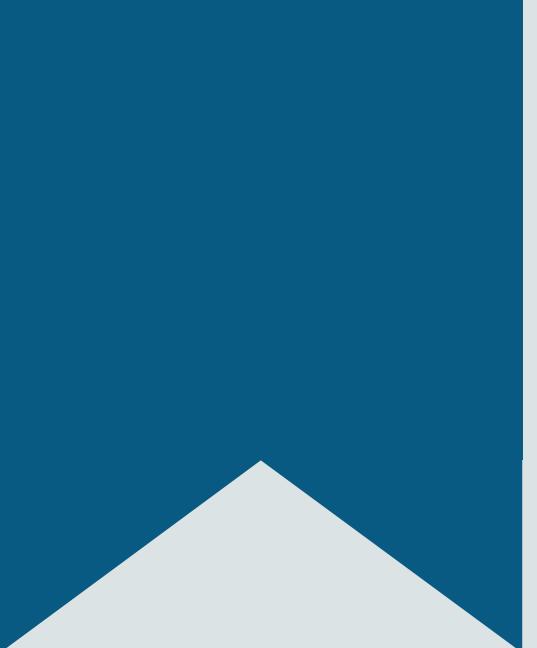
For more information about Katana and OWIN [click here](#)



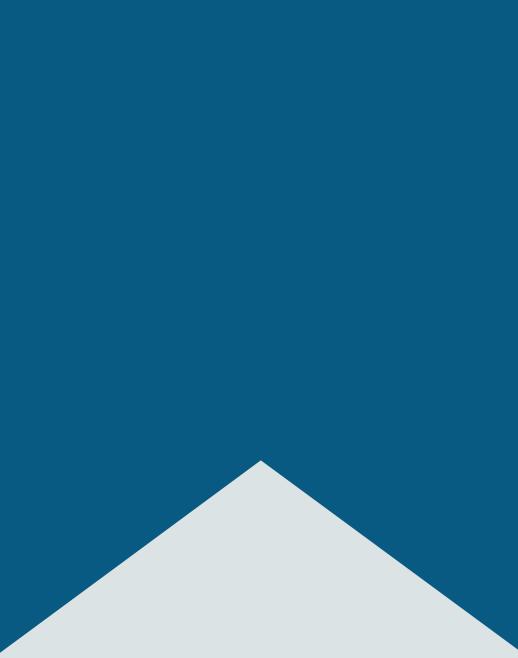
Azure Managed Service Identity

Managed Service Identity (MSI)





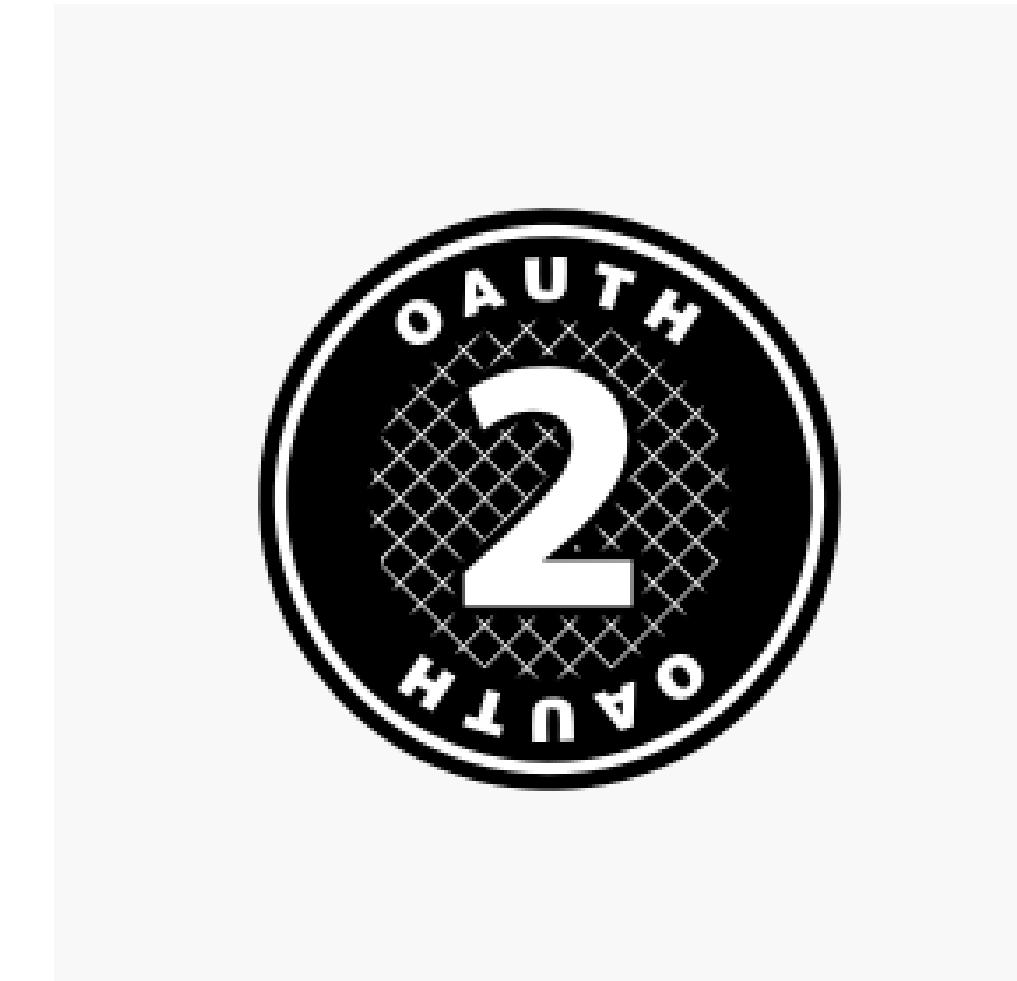
Demo 3 – Implement Managed Service Identity (MSI)



Implementing OAuth 2.0 Authorization

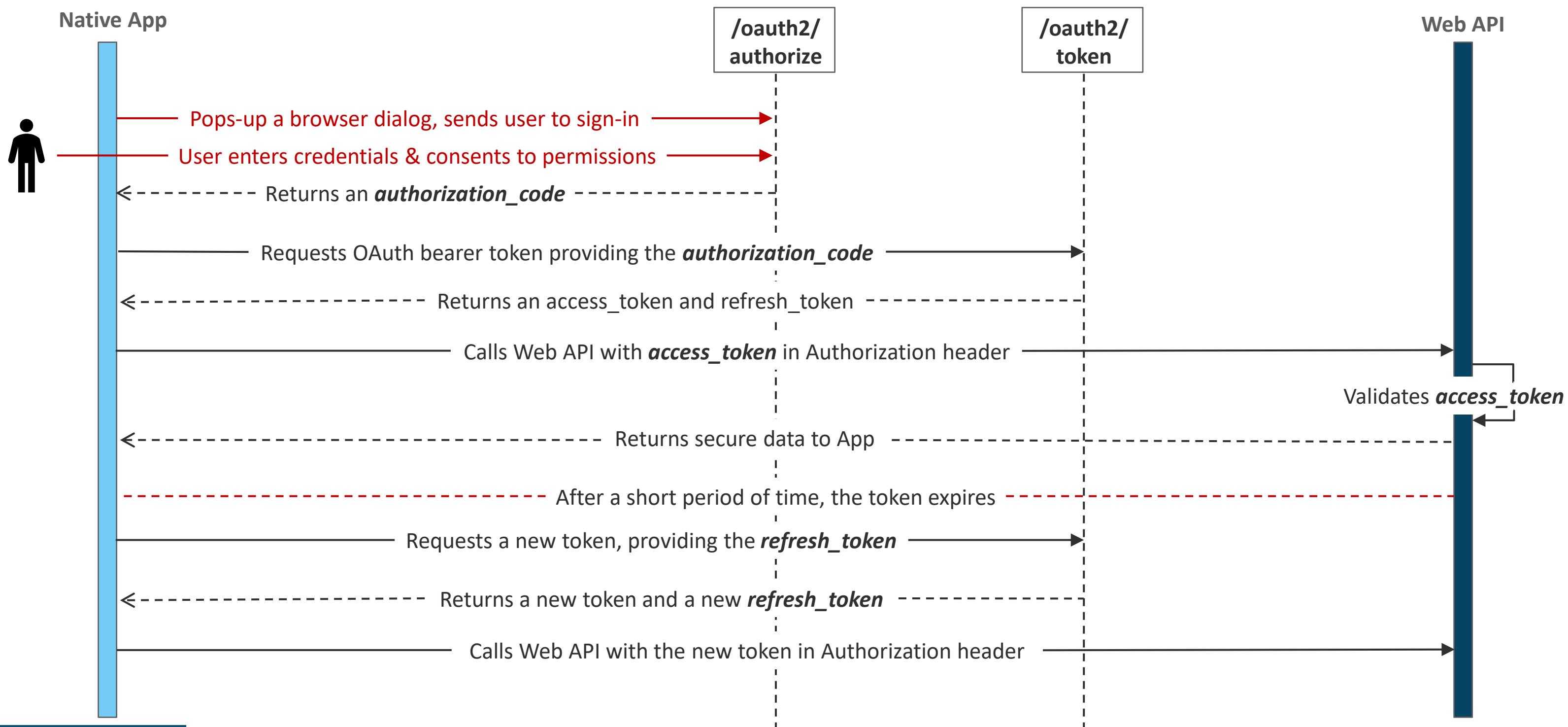
Authorize Access to Azure AD Web Applications

- Azure Active Directory (Azure AD) uses OAuth 2.0 to enable you to *authorize access* to web applications and web APIs in your Azure AD tenant
- The OAuth 2.0 code grant flow is used to perform *authentication* and *authorization* in most application types, including web apps and natively installed apps



OAuth 2.0 Authorization Flow

At a high level, the entire authorization flow for an application looks a bit like this:



Steps to Implement OAuth2 Authorization

1. Register your application with your AD tenant
2. Request an authorization code
3. Use the authorization code to request an access token
4. Use the access token to access the resource
5. Refreshing the access tokens

Summary

RBAC – Security Principal

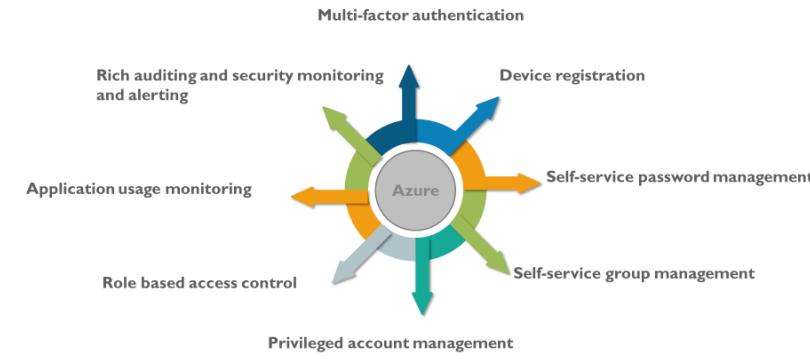
- A **Security Principal** is an object that represents a user, group, or service principal that is requesting access to Azure resources
- User** - An individual who has a profile in Azure Active Directory. Roles can be assigned to users in other tenants
- Group** - A set of users created in Azure Active Directory. When you assign a role to a group, all users within that group have that role
- Service Principal** - A security identity used by applications or services to access specific Azure resources. It functions like a user ID for an application



edureka!

Copyright © edureka and/or its affiliates. All rights reserved.

Azure AD Identity Management Capabilities



edureka!

Copyright © edureka and/or its affiliates. All rights reserved.

Azure Active Directory (AD)

Azure AD is Microsoft's multi-tenant, cloud-based directory and identity-management service that combines core directory services, application access management, and identity protection into a single solution

- If you already have an on-premises directory, it can be extended to the cloud using the directory integration capabilities of Azure AD
- Azure AD helps users to sign in and access external resources in Azure portal and many other SaaS applications
- It also allows internal access to apps on your corporate network and intranet, along with any cloud apps developed by your own organization



edureka!

Copyright © edureka and/or its affiliates. All rights reserved.

Azure Multi-Factor Authentication (MFA)

Azure MFA is Microsoft's two-step verification solution that helps safeguard your access to data and applications, while meeting the demand for a simple sign-in process

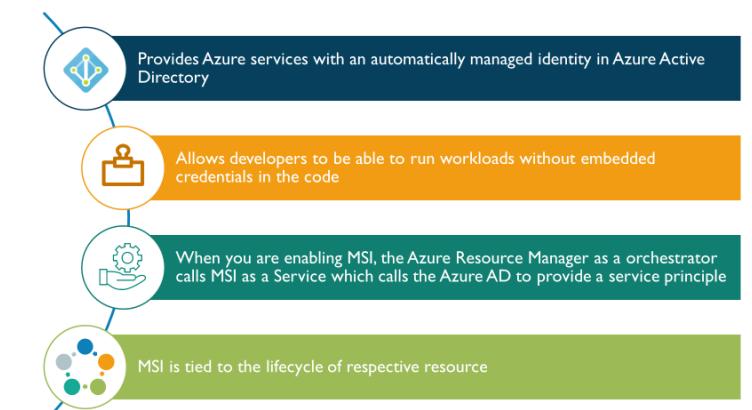
It is recommended that you require Azure MFA for user sign-ins because:

- It delivers strong authentication with a range of easy verification options
- It enables your organization to protect and recover from account compromises



Copyright © edureka and/or its affiliates. All rights reserved.

Managed Service Identity (MSI)

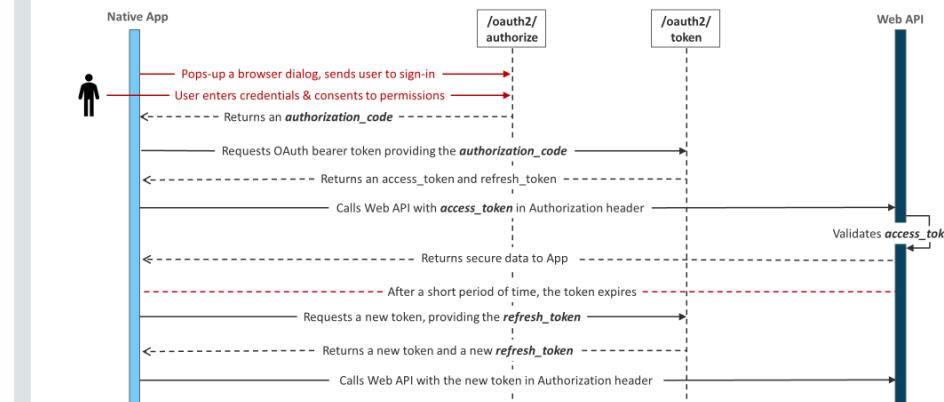


edureka!

Copyright © edureka and/or its affiliates. All rights reserved.

OAuth 2.0 Authorization Flow

At a high level, the entire authorization flow for an application looks a bit like this:



Copyright © edureka and/or its affiliates. All rights reserved.

Questions

FEEDBACK



Survey



Ratings



Ideas



Comments



Suggestions



Likes



Thank You

For more information please visit our website
www.edureka.co