Identity and Access Management

Azure Identity and Access Management (IAM) is a framework within Microsoft Azure that allows administrators to manage user access, permissions, and roles for resources in Azure. It ensures that only authorized users can access specific resources or perform certain actions, thereby enhancing the security and control of your Azure environment.

Key Components of Azure IAM:

1. **Users**:
    - Individual accounts that can access Azure resources. These can be organizational (Azure AD) users, guest users, or service principals for applications.
2. **Groups**:
    - A collection of users with the same access permissions. Permissions assigned to a group automatically apply to all its members.
3. **Roles**:
    - Define what actions a user or group can perform on Azure resources. Roles can be:
        - **Built-in roles**: Predefined roles like Owner, Contributor, and Reader.
        - **Custom roles**: User-defined roles tailored to specific requirements.
4. **Role Assignments**:
    - Assigning roles to users, groups, or service principals to grant permissions for specific resources.
5. **Azure Active Directory (Azure AD)**:
    - The underlying identity platform that manages authentication and provides directory services, single sign-on (SSO), and multifactor authentication (MFA).
6. **Role-Based Access Control (RBAC)**:
    - A feature of Azure IAM that restricts access based on roles. For example:
        - **Reader role**: Allows viewing of resources but no changes.
        - **Contributor role**: Allows creating and modifying resources but no management of permissions.
        - **Owner role**: Full access, including managing access permissions.
7. **Conditional Access**:
    - Policies that control access based on conditions like user location, device type, or risk level.
8. **Managed Identities**:
    - Automatically managed identities for Azure resources to access other services securely, without managing credentials manually.

Benefits of Azure IAM:

- **Granular Access Control**: Enables precise permission assignment.
- **Enhanced Security**: Reduces the risk of unauthorized access.
- **Centralized Management**: Unified control over all Azure resources.
- **Compliance**: Helps meet organizational and regulatory compliance requirements.

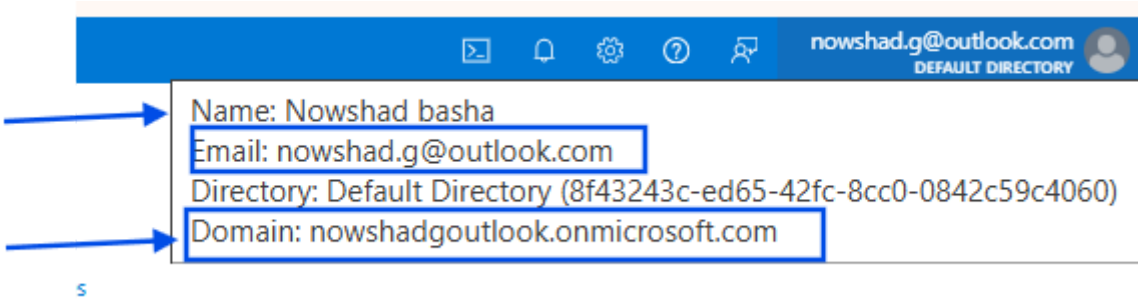
Use Cases:

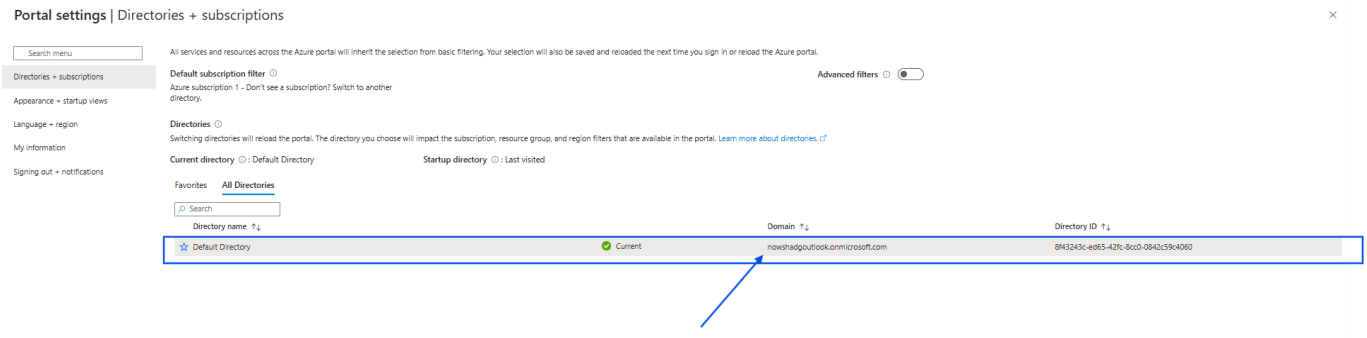
1. Granting developers access only to development environments.
2. Allowing external contractors access to specific resources for a limited period.
3. Assigning read-only roles to auditors for compliance reviews.
4. Automating access through managed identities for apps running on Azure.

Tools for Managing Azure IAM:

- **Azure Portal**: Provides a graphical interface for managing IAM settings.
- **Azure CLI**: Command-line tool for scripting IAM configurations.
- **Azure PowerShell**: For managing IAM via PowerShell commands.
- **Azure Resource Manager (ARM) Templates**: To deploy IAM settings programmatically.

Azure Entra ID (Azure Active Directory)



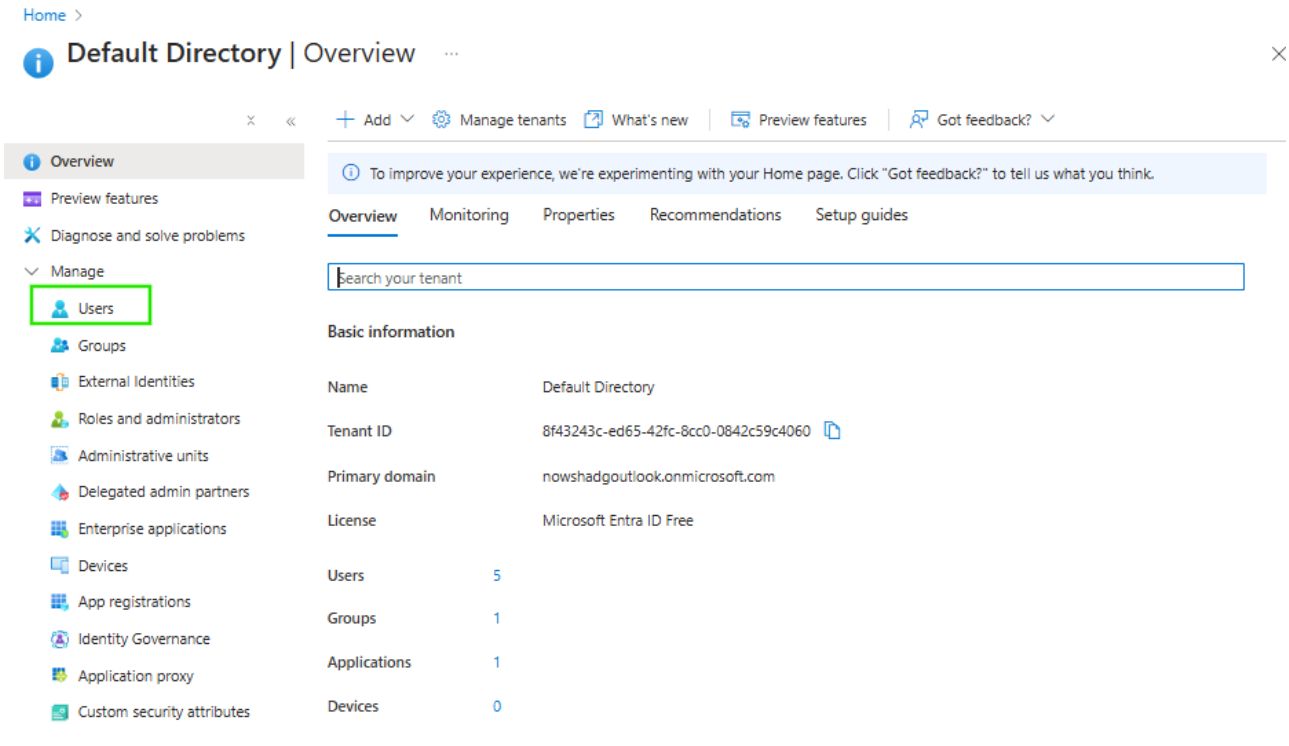


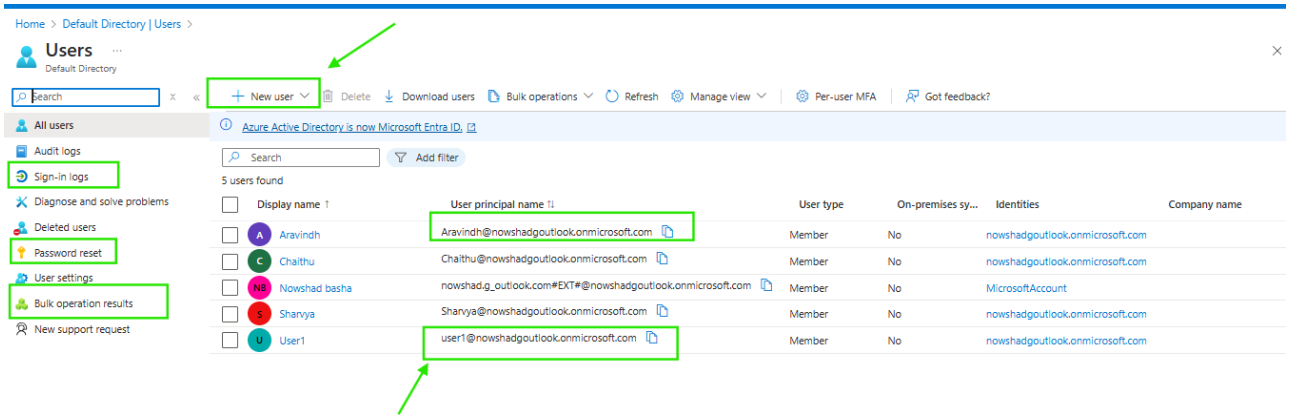
- When you create Azure account/ O365 account you will get access to Azure Entra ID.
- Azure Entra ID is a cloud-based identity and access management solution.
- where a new domain will be created for you with `username@onmicrosoft.com`.

User Creation

- when you create a user it will create username using the tenet domain.

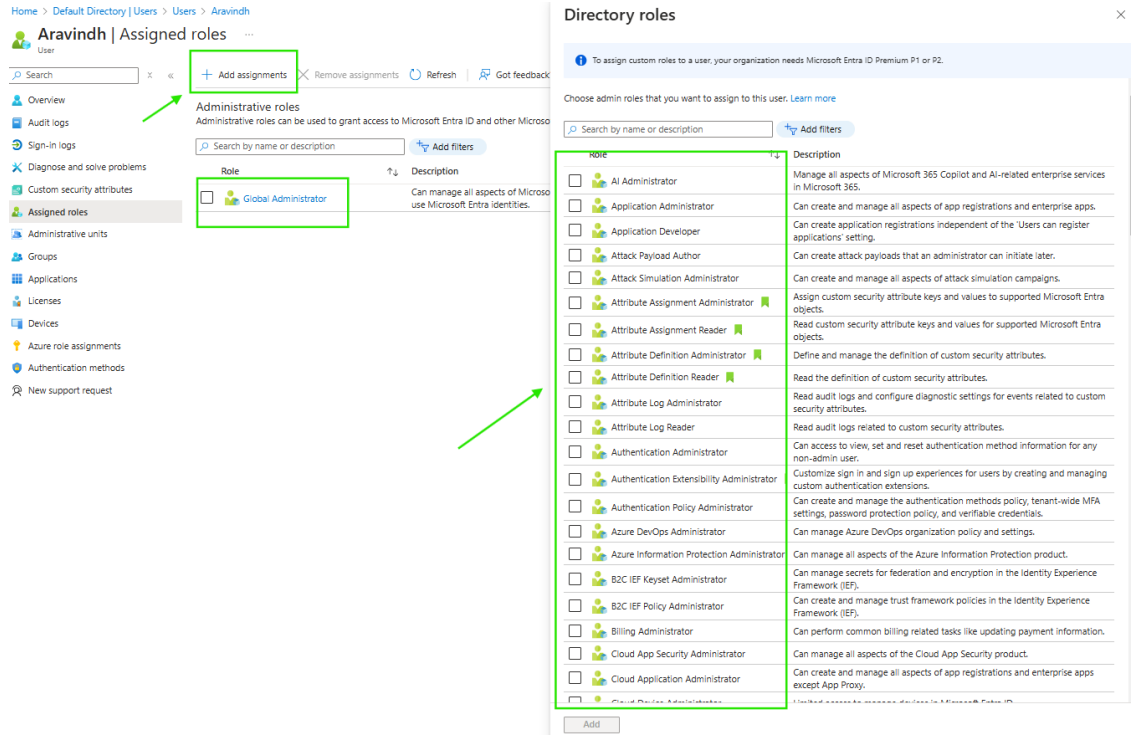
- you can also create user using the custom domain. ex: domain : `nowshadgoutlook.onmicrosoft.com`. New User: `User1` final Username : `User1@nowshadgoutlook.onmicrosoft.com`.





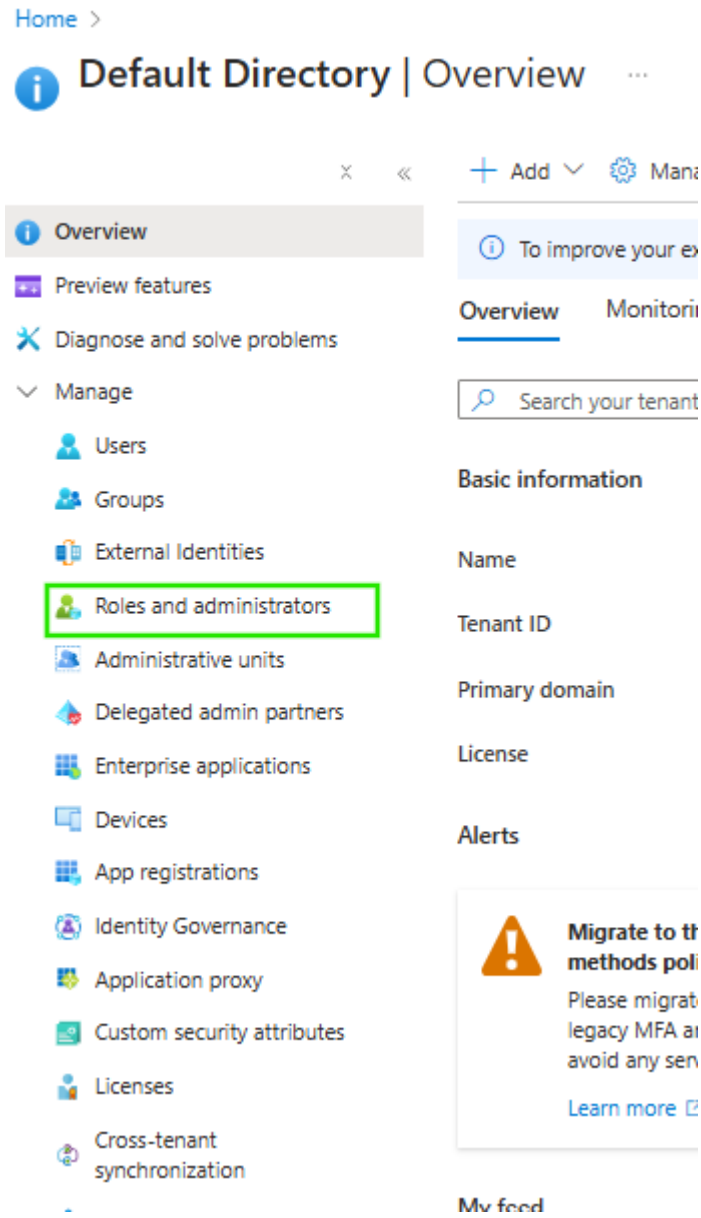
- Sign-in-logs:
  - sign in logs show user login activity
- Roles :
  - roles are used to assign permissions to users, there are two types od roles in Azure
    - Entra ID roles

- RBAC roles

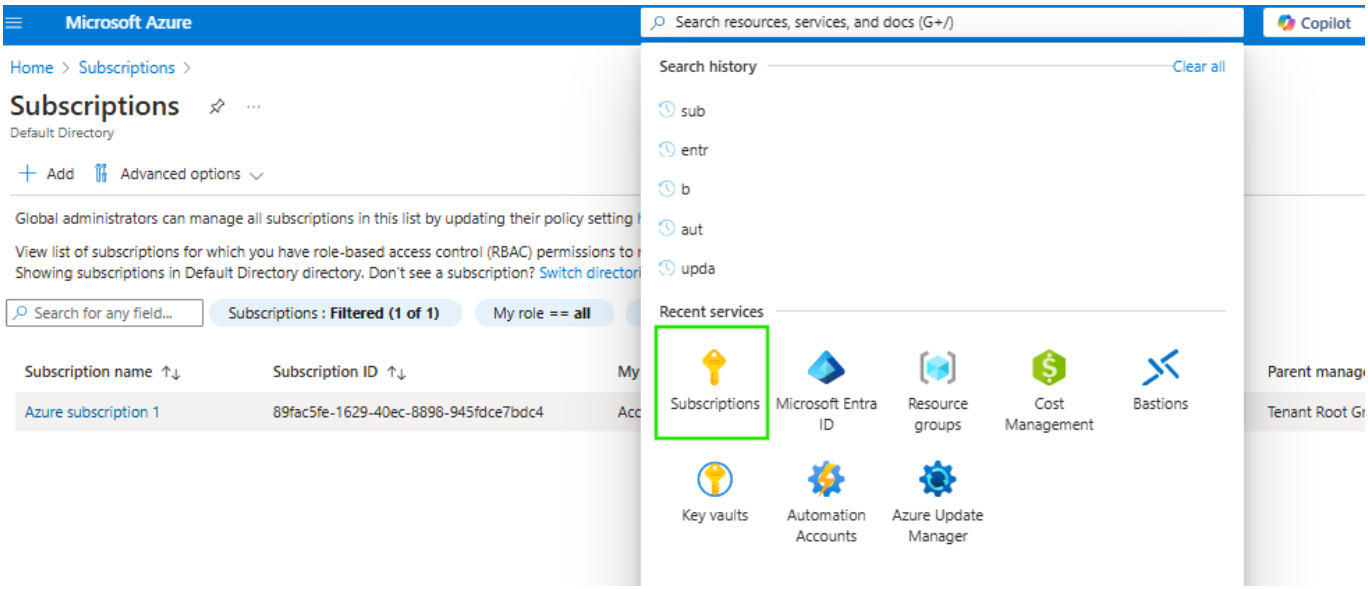


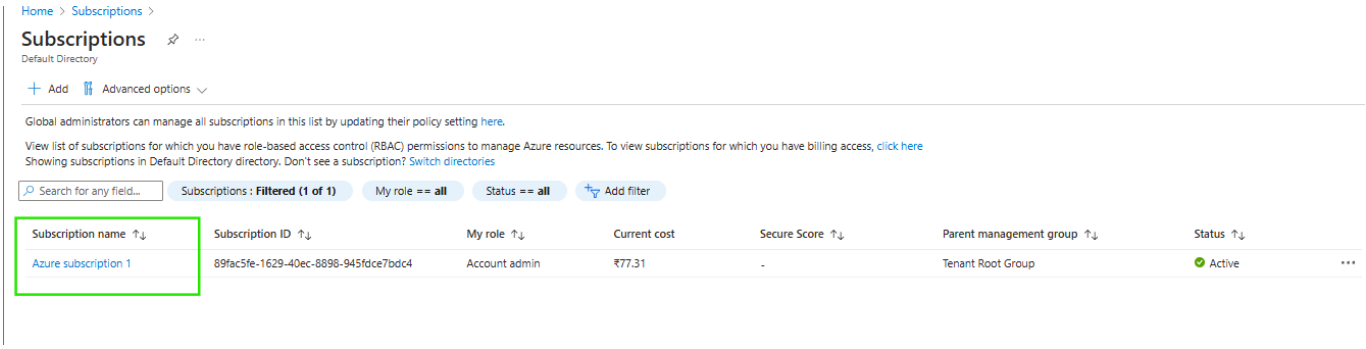
- Entra ID Roles :
  - Above image shows Entra ID roles, which gives permission for only Entra ID Access.
  - if a user is given access with Global Admin role of Entra ID he will get full permissions to do anything inside Entra ID. he won't be able to access any other services in Azure
  - these roles will be available inside User profile with name `Assigned roles`

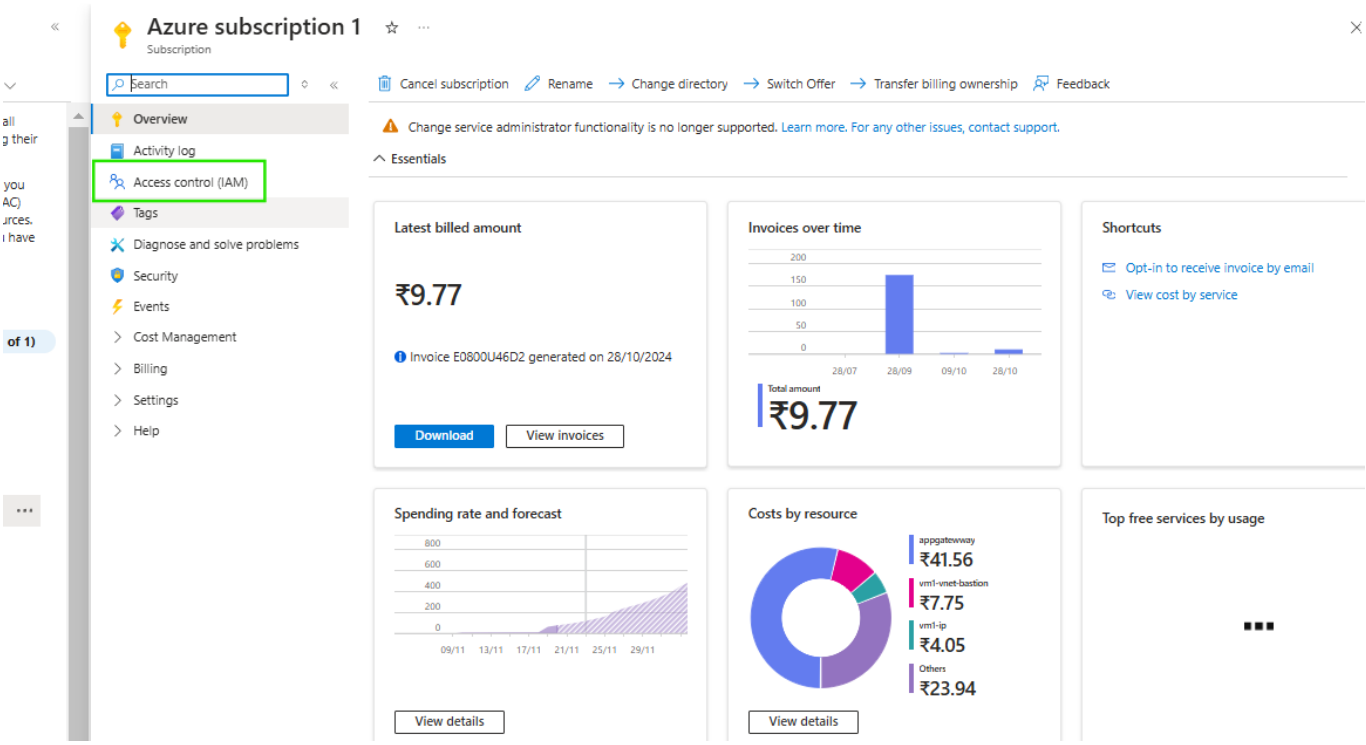
- All roles you can see in left blade `Roles and administrators`

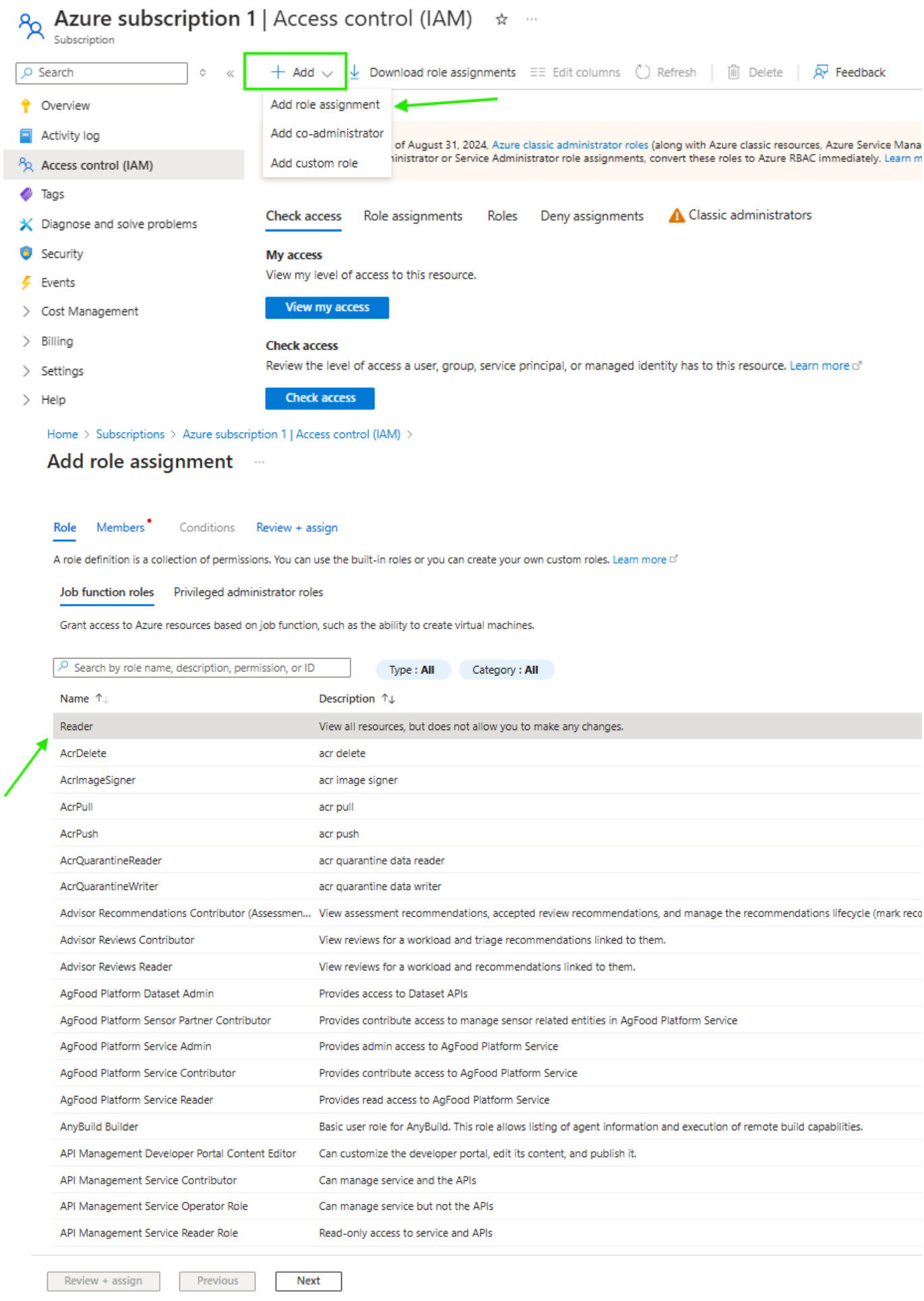


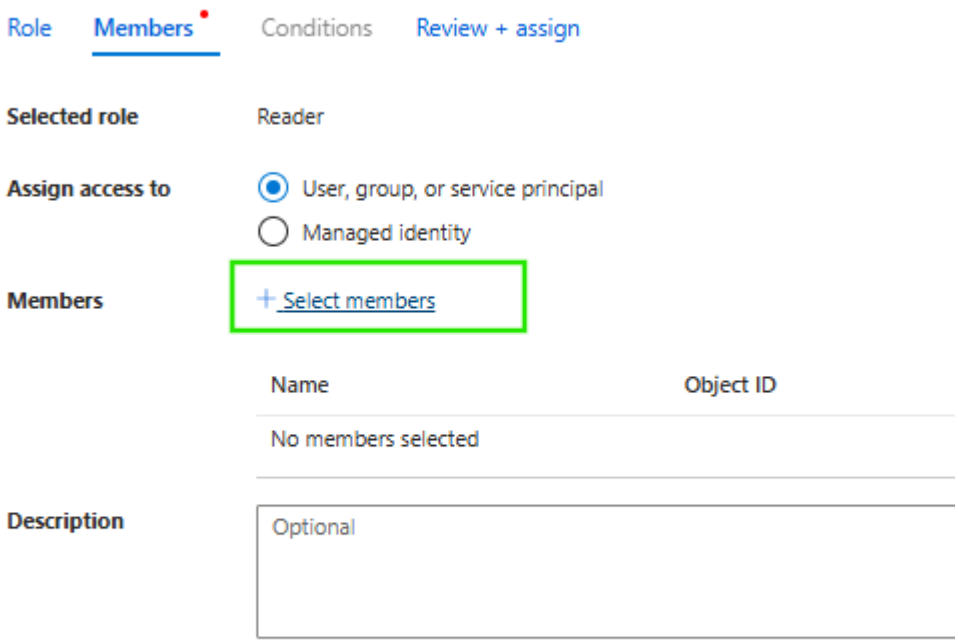
- RBAC roles :
  - These roles are used to provide access to Azure services, you can limit ones access to Azure using these roles.
  - How to Assign Azure access to User follow below images


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Subscriptions >
Subscriptions
Default Directory
Add
Advanced options
Global administrators can manage all subscriptions in this list by updating their policy setting
View list of subscriptions for which you have role-based access control (RBAC) permissions to
Showing subscriptions in Default Directory directory. Don't see a subscription? Switch directori
Search for any field...
Subscriptions : Filtered (1 of 1)
My role == all
Subscription name
Subscription ID
Azure subscription 1
89fac5fe-1629-40ec-8898-945fdce7bdc4
Search history
Clear all
sub
entr
b
aut
upda
Recent services
Subscriptions
Microsoft Entra ID
Resource groups
Cost Management
Bastions
Key vaults
Automation Accounts
Azure Update Manager


Home > Subscriptions >
Subscriptions
Default Directory
Add
Advanced options
Global administrators can manage all subscriptions in this list by updating their policy setting here.
View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have billing access, click here
Showing subscriptions in Default Directory directory. Don't see a subscription? Switch directories
Search for any field...
Subscriptions : Filtered (1 of 1)
My role == all
Status == all
Add filter
Subscription name
Subscription ID
My role
Current cost
Secure Score
Parent management group
Status
Azure subscription 1
89fac5fe-1629-40ec-8898-945fdce7bdc4
Account admin
₹77.31
-
Tenant Root Group
Active


Azure subscription 1
Subscription
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Security
Events
Cost Management
Billing
Settings
Help
Cancel subscription
Rename
Change directory
Switch Offer
Transfer billing ownership
Feedback
Change service administrator functionality is no longer supported. Learn more. For any other issues, contact support.
Essentials
Latest billed amount
₹9.77
Invoice E0800U46D2 generated on 28/10/2024
Download
View invoices
Invoices over time
Total amount
₹9.77
Shortcuts
Opt-in to receive invoice by email
View cost by service
Spending rate and forecast
View details
Costs by resource
appgatewway
₹41.56
vm1-vnet-bastion
₹7.75
vm1-ip
₹4.05
Others
₹23.94
View details
Top free services by usage


Azure subscription 1 | Access control (IAM)
Subscription
Search
Add
Download role assignments
Edit columns
Refresh
Delete
Feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Security
Events
Cost Management
Billing
Settings
Help
Add role assignment
Add co-administrator
Add custom role
of August 31, 2024, Azure classic administrator roles (along with Azure classic resources, Azure Service Mana
inistrator or Service Administrator role assignments, convert these roles to Azure RBAC immediately. Learn m
Check access
Role assignments
Roles
Deny assignments
Classic administrators
My access
View my level of access to this resource.
View my access
Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more
Check access
Home > Subscriptions > Azure subscription 1 | Access control (IAM) >
Add role assignment
Role
Members
Conditions
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
Job function roles
Privileged administrator roles
Grant access to Azure resources based on job function, such as the ability to create virtual machines.
Search by role name, description, permission, or ID
Type : All
Category : All
Name
Description
Reader
View all resources, but does not allow you to make any changes.
AcrDelete
acr delete
AcrImageSigner
acr image signer
AcrPull
acr pull
AcrPush
acr push
AcrQuarantineReader
acr quarantine data reader
AcrQuarantineWriter
acr quarantine data writer
Advisor Recommendations Contributor (Assessmen...
View assessment recommendations, accepted review recommendations, and manage the recommendations lifecycle (mark reco
Advisor Reviews Contributor
View reviews for a workload and triage recommendations linked to them.
Advisor Reviews Reader
View reviews for a workload and recommendations linked to them.
AgFood Platform Dataset Admin
Provides access to Dataset APIs
AgFood Platform Sensor Partner Contributor
Provides contribute access to manage sensor related entities in AgFood Platform Service
AgFood Platform Service Admin
Provides admin access to AgFood Platform Service
AgFood Platform Service Contributor
Provides contribute access to AgFood Platform Service
AgFood Platform Service Reader
Provides read access to AgFood Platform Service
AnyBuild Builder
Basic user role for AnyBuild. This role allows listing of agent information and execution of remote build capabilities.
API Management Developer Portal Content Editor
Can customize the developer portal, edit its content, and publish it.
API Management Service Contributor
Can manage service and the APIs
API Management Service Operator Role
Can manage service but not the APIs
API Management Service Reader Role
Read-only access to service and APIs
Review + assign
Previous
Next



Review and create, this will give access to a user for Azure Services.