Stories 3 : Subscription,Azure Active Directory , Users and group in Azure

Azure Subscription

Azure Subscription refers to a user account that has been set up to use the Microsoft Azure cloud computing platform. Azure is a comprehensive set of cloud services offered by Microsoft, including computing power, storage, and networking, among others.

When you create an Azure Subscription, you essentially create an agreement with Microsoft to use their services based on a pay-as-you-go or a subscription-based model. This subscription is associated with a unique Azure AD (Active Directory) tenant, which helps manage access and permissions.

Key points about Azure Subscriptions:

1. **Billing and Usage:** Azure Subscriptions are associated with billing, and you are charged based on your usage of the Azure services. There are different pricing models, including pay-as-you-go, monthly subscriptions, and enterprise agreements.

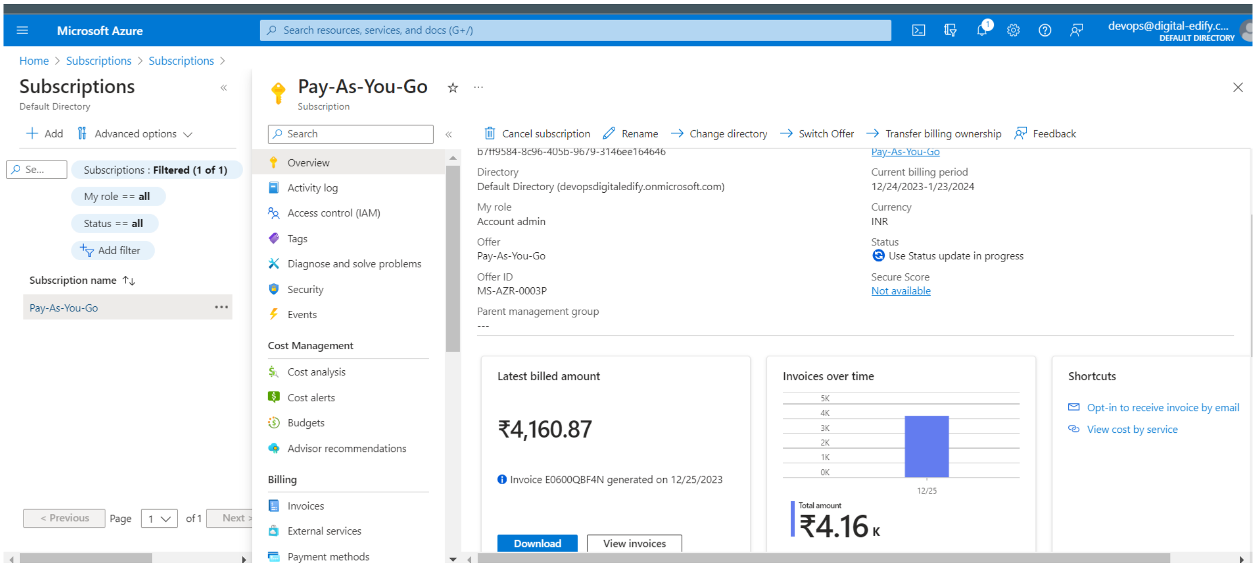
2. **Resource Management:** Resources in Azure, such as virtual machines, storage accounts, databases, etc., are organized within a subscription. Resource groups are used to logically organize and manage these resources.

3. **Access Control:** Azure provides role-based access control (RBAC), allowing you to assign specific roles to users or groups within your subscription. This helps in managing permissions and controlling access to Azure resources.

4. **Service Limits:** Each Azure subscription has certain service limits to prevent misuse and ensure fair usage. These limits can be increased upon request.

5. **Azure AD Tenant:** Every Azure Subscription is associated with an Azure Active Directory (Azure AD) tenant. Azure AD is Microsoft's cloud-based identity and access management service.

6. **Management Groups:** In addition to subscriptions, Azure provides the concept of management groups, which allows you to organize subscriptions and apply policies at scale.



Subscriptions
Default Directory

Subscriptions : **Filtered (1 of 1)**
My role == **all**
Status == **all**

Subscription name ↑↓
Pay-As-You-Go

Page 1 of 1

Pay-As-You-Go
Subscription

b7ff9584-8c96-405b-9679-3146ee164646
Pay-As-You-Go

Directory
Default Directory (devopsdigitaledify.onmicrosoft.com)

Current billing period
12/24/2023-1/23/2024

My role
Account admin

Currency
INR

Offer
Pay-As-You-Go

Status
Use Status update in progress

Offer ID
MS-AZR-0003P

Secure Score
Not available

Parent management group

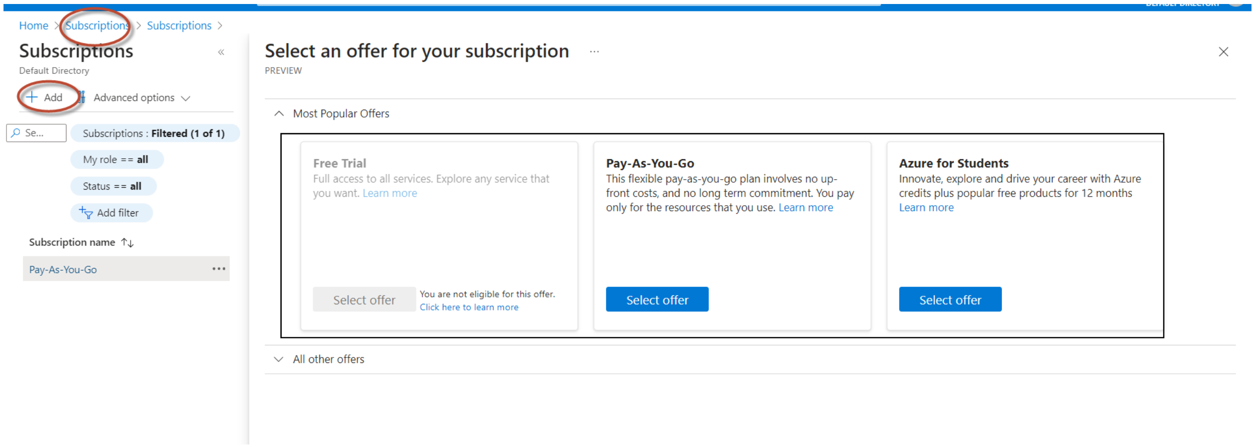
Latest billed amount
₹4,160.87
Invoice E0600QBF4N generated on 12/25/2023

Invoices over time
Total amount
₹4.16 K

Shortcuts

When you create any resource you need to select a subscription for billing

may be you may have multiple subscription



Home > Subscriptions > Subscriptions >

Subscriptions

Default Directory

+ Add | Advanced options ⌵

Se... | Subscriptions : **Filtered (1 of 1)**

My role == **all**

Status == **all**

Add filter

Subscription name ↑↓

Pay-As-You-Go ···

Select an offer for your subscription ···

PREVIEW

Most Popular Offers

Free Trial
Full access to all services. Explore any service that you want. Learn more

Select offer — You are not eligible for this offer. Click here to learn more

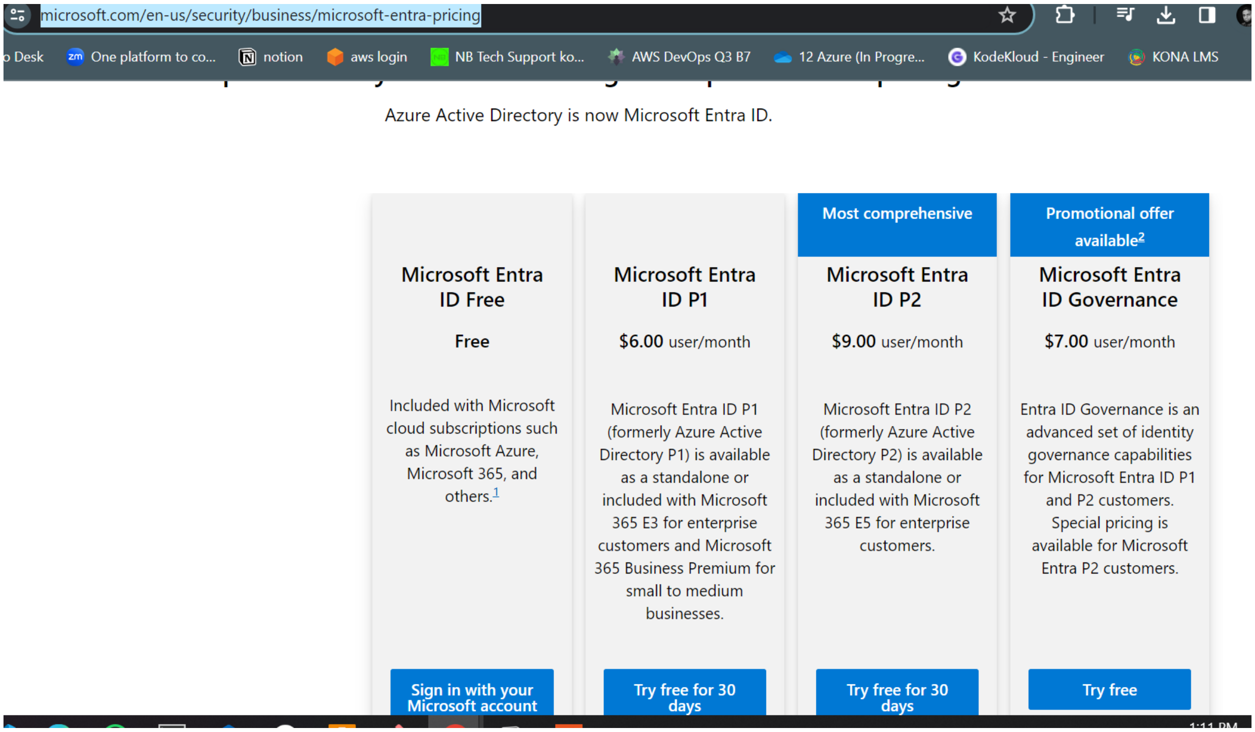
Pay-As-You-Go
This flexible pay-as-you-go plan involves no up-front costs, and no long term commitment. You pay only for the resources that you use. Learn more

Select offer

Azure for Students
Innovate, explore and drive your career with Azure credits plus popular free products for 12 months
Learn more

Select offer

All other offers



microsoft.com/en-us/security/business/microsoft-entra-pricing

Azure Active Directory is now Microsoft Entra ID.

		Most comprehensive	Promotional offer available[2]
Microsoft Entra ID Free	Microsoft Entra ID P1	Microsoft Entra ID P2	Microsoft Entra ID Governance
Free	$6.00 user/month	$9.00 user/month	$7.00 user/month
Included with Microsoft cloud subscriptions such as Microsoft Azure, Microsoft 365, and others.[1]	Microsoft Entra ID P1 (formerly Azure Active Directory P1) is available as a standalone or included with Microsoft 365 E3 for enterprise customers and Microsoft 365 Business Premium for small to medium businesses.	Microsoft Entra ID P2 (formerly Azure Active Directory P2) is available as a standalone or included with Microsoft 365 E5 for enterprise customers.	Entra ID Governance is an advanced set of identity governance capabilities for Microsoft Entra ID P1 and P2 customers. Special pricing is available for Microsoft Entra P2 customers.
Sign in with your Microsoft account	Try free for 30 days	Try free for 30 days	Try free

USERS:

In Azure Active Directory (Azure AD), users are entities that represent individuals or system accounts that need to access resources and services within an Azure AD tenant.

Each user has a unique identity and associated credentials.

1. **User Identity:** Users in Azure AD have a unique identity associated with their account. This identity is often represented by a user principal name (UPN), which typically looks like an email address (e.g., user@domain.com).
2. **Credentials:** Users have credentials, usually in the form of a username and password, which they use to authenticate and access Azure AD-integrated services and applications.
3. **Authentication:** Azure AD provides authentication services, allowing users to sign in securely. It supports various authentication methods, including username and password, multi-factor authentication (MFA), and integration with identity providers.
4. **Groups:** Users can be members of groups in Azure AD. Groups help organize users for easier management and simplify access assignment to resources. There are different types of groups, such as security groups and Microsoft 365 groups.
5. **Roles and Permissions:** Azure AD supports role-based access control (RBAC), allowing administrators to assign roles to users based on their responsibilities. Roles define what actions a user can perform in Azure resources.
6. **Self-Service Password Reset:** Azure AD provides self-service password reset capabilities, allowing users to reset their passwords without administrator intervention, enhancing security and user convenience.
7. **User Attributes:** Additional information about users, such as their job title, department, and contact details, can be stored as user attributes in Azure AD. This information can be used for reporting, compliance, and management purposes.
8. **License Assignment:** Users may require licenses for specific services within Azure, such as Microsoft 365 applications. Administrators can assign licenses to users based on their needs.

Group:

In Azure Active Directory (Azure AD), groups play a crucial role in organizing and managing users, providing access to resources, and simplifying administrative tasks. Here are key aspects of groups in Azure AD:

1. **Group Types:**
    - **Security Groups:** These are used to manage access to resources. Users can be added as members, and security groups can be used in role assignments for resource access.
    - **Microsoft 365 Groups:** Formerly known as Office 365 Groups, these are used for collaboration in Microsoft 365 services. They include shared resources like a shared inbox, calendar, and document library.
2. **Membership:**
    - **User Membership:** Groups can contain users, making it easier to manage permissions and access for a set of users rather than managing each user individually.
    - **Nested Groups:** Groups can also include other groups as members, allowing for hierarchical and easier management of access.
3. **Group Naming Policies:**
    - Organizations can establish naming policies for groups, enforcing consistency and making it easier to identify the purpose or function of a group.
4. **Dynamic Groups:**
    - Azure AD supports dynamic groups where membership is defined by rules rather than being manually managed. For example, a dynamic group could include all users from a specific department.

EX: we'll create a dynamic group based on the department attribute. The goal is to include all users whose department is "Marketing."

Example: Creating a Dynamic Group for Marketing Department

1. **Sign in to Azure Portal:**

- Navigate to the Azure portal and sign in with your Azure AD administrator account.

2. **Access Azure Active Directory:**
   - In the left-hand navigation pane, click on "Azure Active Directory."
3. **Create Dynamic Group:**
   - Under "Azure Active Directory," click on "Groups" and then click the "+ New group" button.
4. **Choose Group Type:**
   - Select "Security" as the group type.
5. **Configure Dynamic User Members:**
   - Choose "Dynamic user" as the membership type.
   - Provide a name for the group, e.g., "Marketing Dynamic Group."
6. **Define Membership Rules:**
   - In the "Rules" section, click on "Add a rule."
   - For the rule, select the attribute you want to use for dynamic membership. In this example, choose "Department."
   - Set the condition to "Equals" and provide the value "Marketing."

   Example Rule:

   - Attribute: Department
   - Operator: Equals
   - Value: Marketing
7. **Review and Create:**
   - Review the configured settings to ensure they match your requirements.
   - Click on "Create" to create the dynamic group.
8. **Verify Membership:**
   - After the dynamic group is created, it will automatically include users whose department attribute is set to "Marketing." Users meeting this criteria will be

dynamically added to the group.

5. **Group Ownership:**
   - Groups have owners who are responsible for managing group membership and settings. Owners can add or remove members and modify group settings.
6. **Access Control (RBAC):**
   - Security groups are often used in Azure Role-Based Access Control (RBAC) to assign permissions to users for specific Azure resources. This simplifies the process of managing access at scale.
7. **Group-Based Licensing:**
   - Azure AD supports group-based licensing, allowing administrators to assign licenses to groups rather than individual users. This can simplify license management, especially in large organizations.
8. **Mail-Enabled Groups:**
   - Some groups, like distribution lists, can be mail-enabled. This allows them to be used for email distribution purposes.
9. **Microsoft 365 Group Collaboration:**
   - Microsoft 365 Groups provide collaboration features, such as a shared mailbox, calendar, and SharePoint document library, making them suitable for team collaboration.
10. **Usage in Applications:**
    - Groups in Azure AD are commonly used in applications to manage access and permissions. For example, an application might grant access to a specific feature based on group membership.