# 😊 Azure Active Directory

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service. It is designed to help organizations manage users and provide secure access to resources, such as applications, data, and services, both on-premises and in the cloud.

Azure AD serves as the foundation for identity and access management in the Microsoft cloud ecosystem, providing features such as:

1. **Single Sign-On (SSO):** Users can sign in once with their credentials and access all the applications and resources they need without having to sign in again.
2. **Multi-factor Authentication (MFA):** Enhances security by requiring users to provide multiple forms of verification before accessing resources.
3. **Identity Protection:** Helps detect and respond to suspicious activities and potential security risks related to user identities.
4. **Conditional Access:** Allows organizations to enforce specific access controls based on conditions such as user location, device health, and sign-in risk.
5. **Application Management:** Simplifies the management of access to cloud and on-premises applications, including provisioning, access reviews, and single sign-on integration.
6. **Integration with Microsoft 365:** Seamlessly integrates with other Microsoft cloud services, such as Microsoft 365, Azure, and Dynamics 365, to provide a unified identity and access management experience.
7. **Identity Governance:** Provides tools for managing identity lifecycle, access reviews, and access certification processes.

Azure AD is widely used by organizations of all sizes to centralize identity management, enhance security, and streamline access to resources across their IT environments.

## 😄 Use cases of Azure Active Directory:

Azure Active Directory (Azure AD) has a wide range of use cases across various industries and organizational sizes. Here are some common scenarios where Azure AD is utilized:

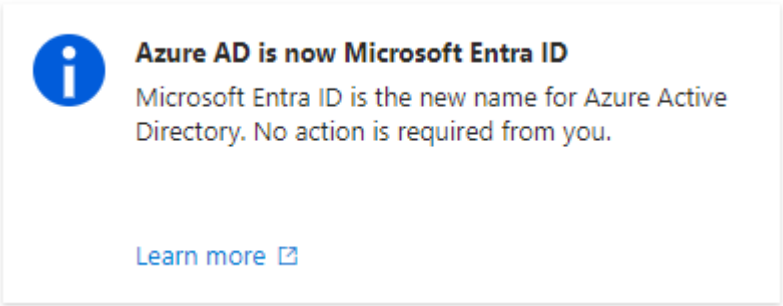
1. **Single Sign-On (SSO):** Users can sign in once with their Azure AD credentials and access multiple applications and services without needing to re-enter their credentials. This improves user experience and productivity while reducing the number of passwords users need to remember.
2. **Application Integration:** Azure AD integrates with thousands of popular cloud-based applications as well as on-premises applications. Organizations can easily manage user access to these applications, enforce security policies, and enable features like automated user provisioning and deprovisioning.
3. **Secure Remote Access:** With the increasing trend of remote work, Azure AD provides secure access to resources from anywhere and any device. Multi-factor authentication (MFA), conditional access policies, and identity protection features help ensure that only authorized users can access sensitive data and applications.

4. **Identity and Access Management (IAM):** Azure AD serves as the central hub for managing user identities, groups, and access permissions. Organizations can define granular access control policies based on user roles, groups, locations, and device compliance status, ensuring that users have the right level of access to resources.
5. **Hybrid Identity Management:** For organizations with a hybrid IT environment (combining on-premises and cloud resources), Azure AD seamlessly integrates with on-premises Active Directory (AD) to provide a unified identity management solution. This allows users to use their existing AD credentials to access cloud resources and enables features like password synchronization and seamless single sign-on.
6. **Identity Protection:** Azure AD's identity protection features help organizations detect and respond to potential security threats such as suspicious sign-in attempts, leaked credentials, and risky user behavior. Machine learning algorithms analyze sign-in patterns and user behavior to identify anomalies and trigger security alerts.
7. **Identity Governance:** Azure AD provides tools for managing the lifecycle of user identities, including user provisioning, access reviews, and access certification. This ensures that users have the appropriate level of access to resources and helps organizations maintain compliance with regulatory requirements.
8. **Business-to-Business (B2B) Collaboration:** Azure AD enables secure collaboration with external partners, vendors, and customers by providing guest access capabilities. Organizations can invite external users to access specific resources while maintaining control over access permissions and security policies.

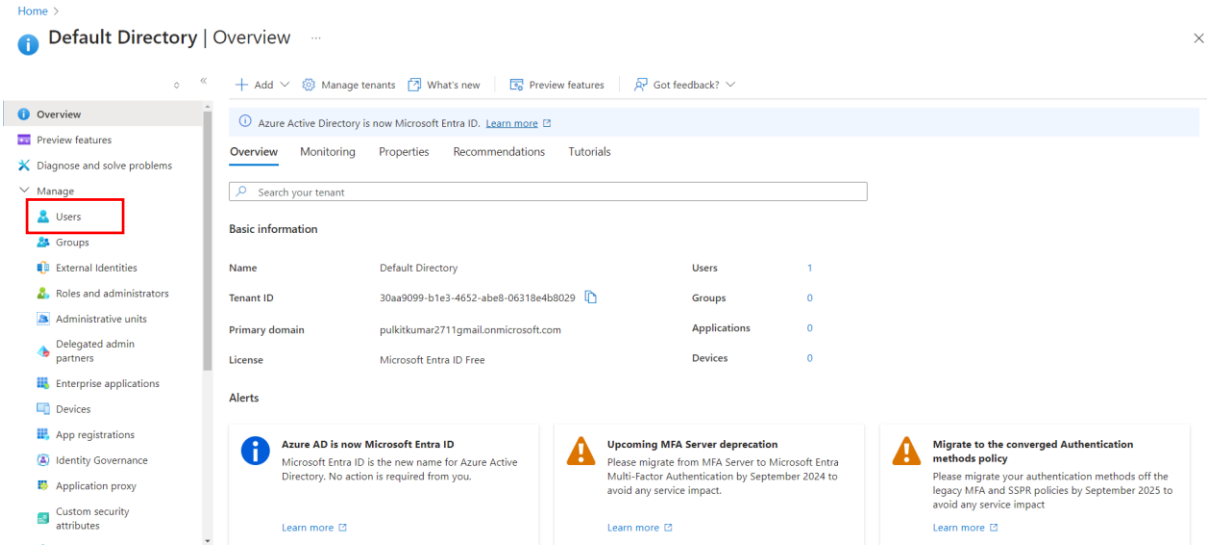
**In this lab, we're learning how to create a user in Azure Active Directory (Azure AD). The end goal is to understand the process of user management within Azure AD, from creating a new user to accessing resources with the newly created user account. This hands-on experience helps familiarize users with basic identity and access management tasks in Azure AD, setting the stage for more advanced configurations and security measures in future deployments.**

## 😄 To begin with the Lab:

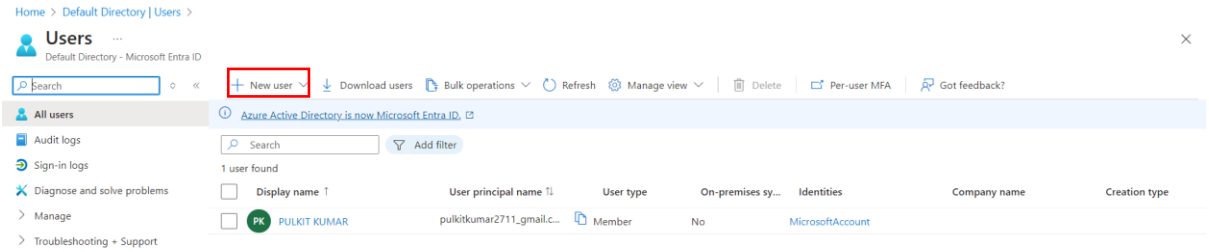
1. In this lab we will learn how to create a user in Azure Active Directory.
2. First log in to your Azure Portal. Then navigate to Microsoft Entra ID because Microsoft has changed its name to this from Microsoft active directory.



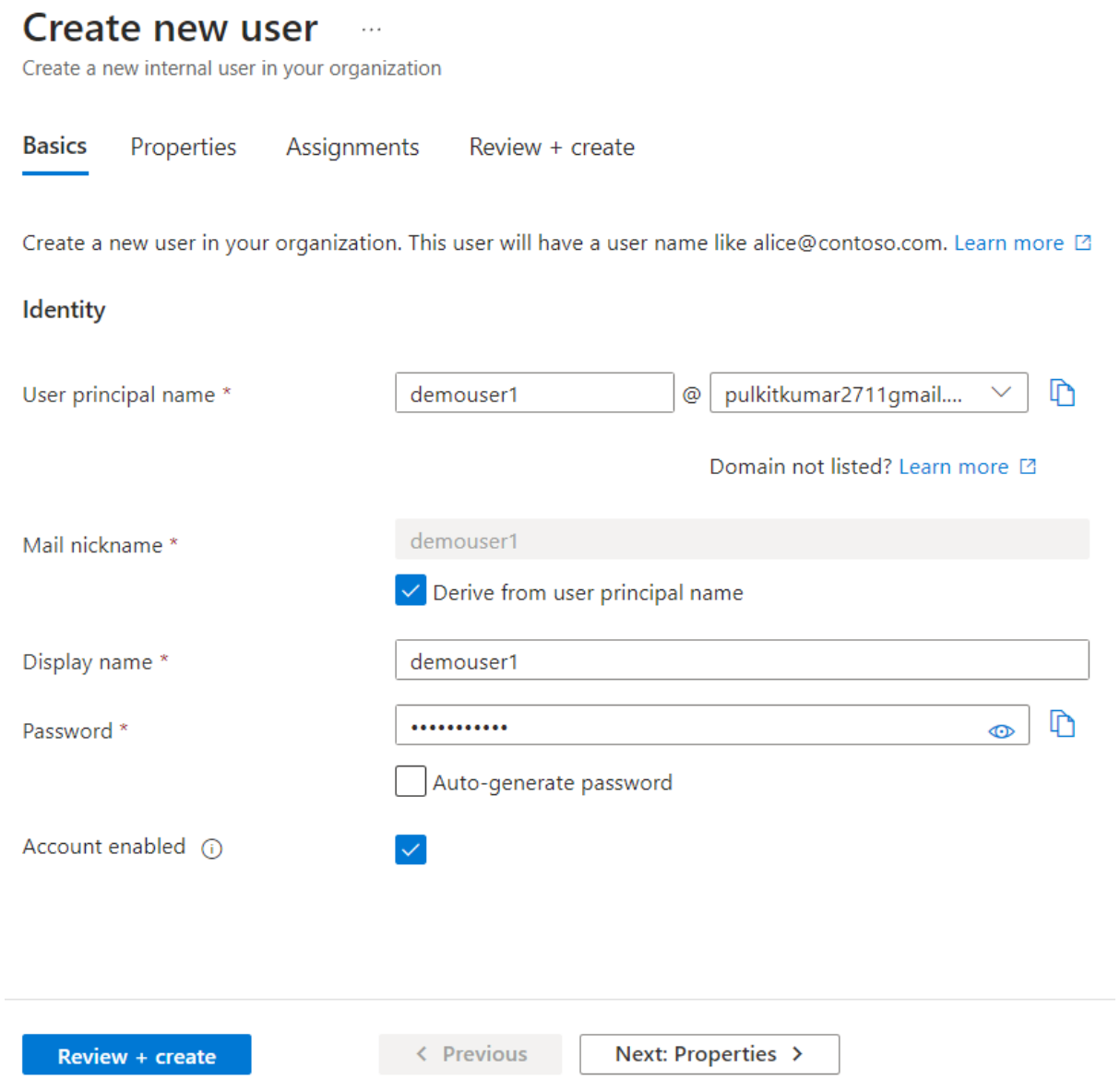

3. Now from its default page you need to choose users.



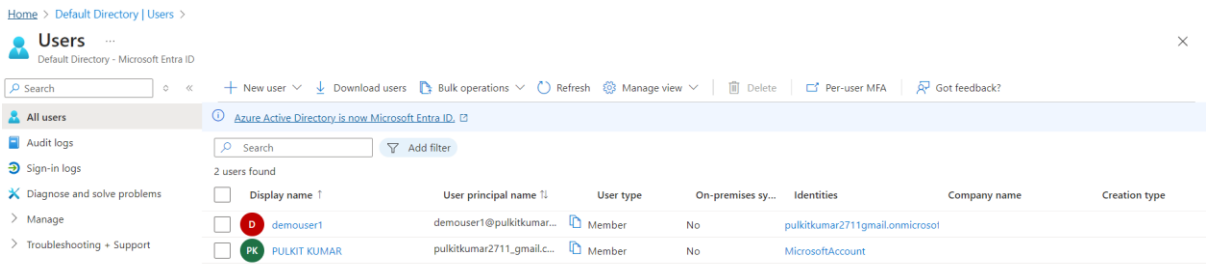

4. Then you'll be directed to a new page where you can all the users that have been created or has access to your account.
5. Currently you can see that we only have one user present which is the root user or say the owner of this account.
6. Now we are going to create a new user. For that click on new user then choose to create new user.



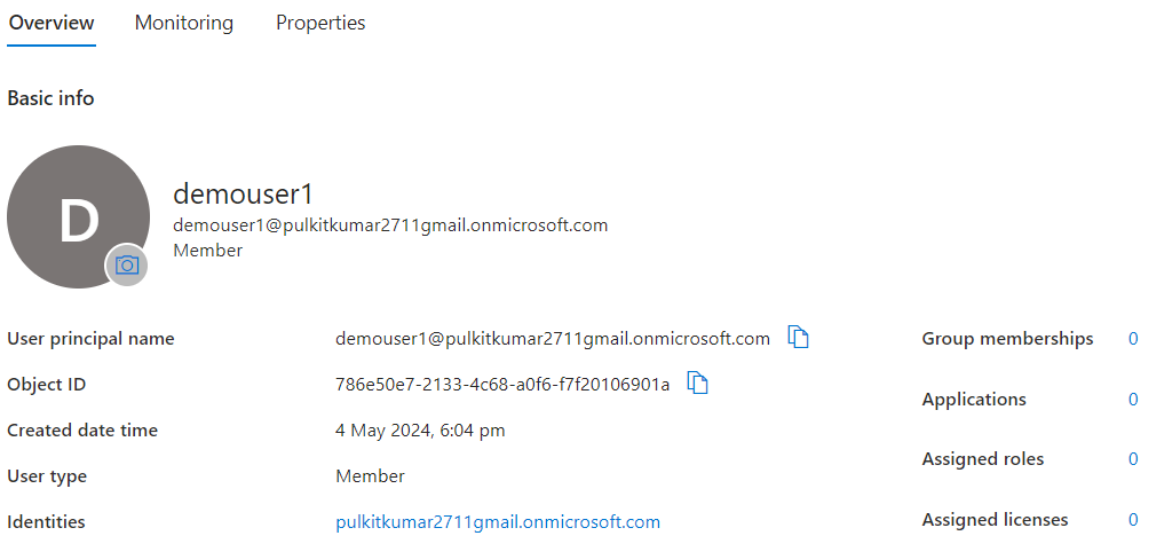

7. Now you need to give it a name then choose a password. You can either choose a auto generated password or you can create it yourself.
8. Then just move to review page and create your user.



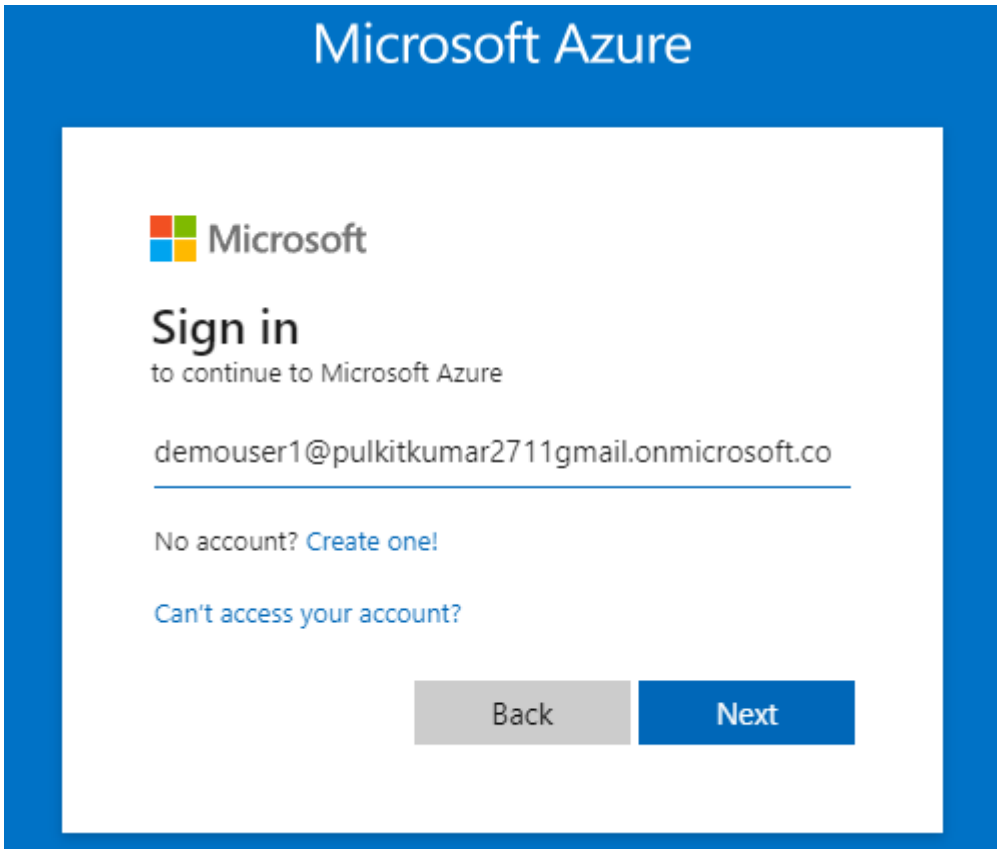

9. Once a user has been created then it will be visible on your all users list.



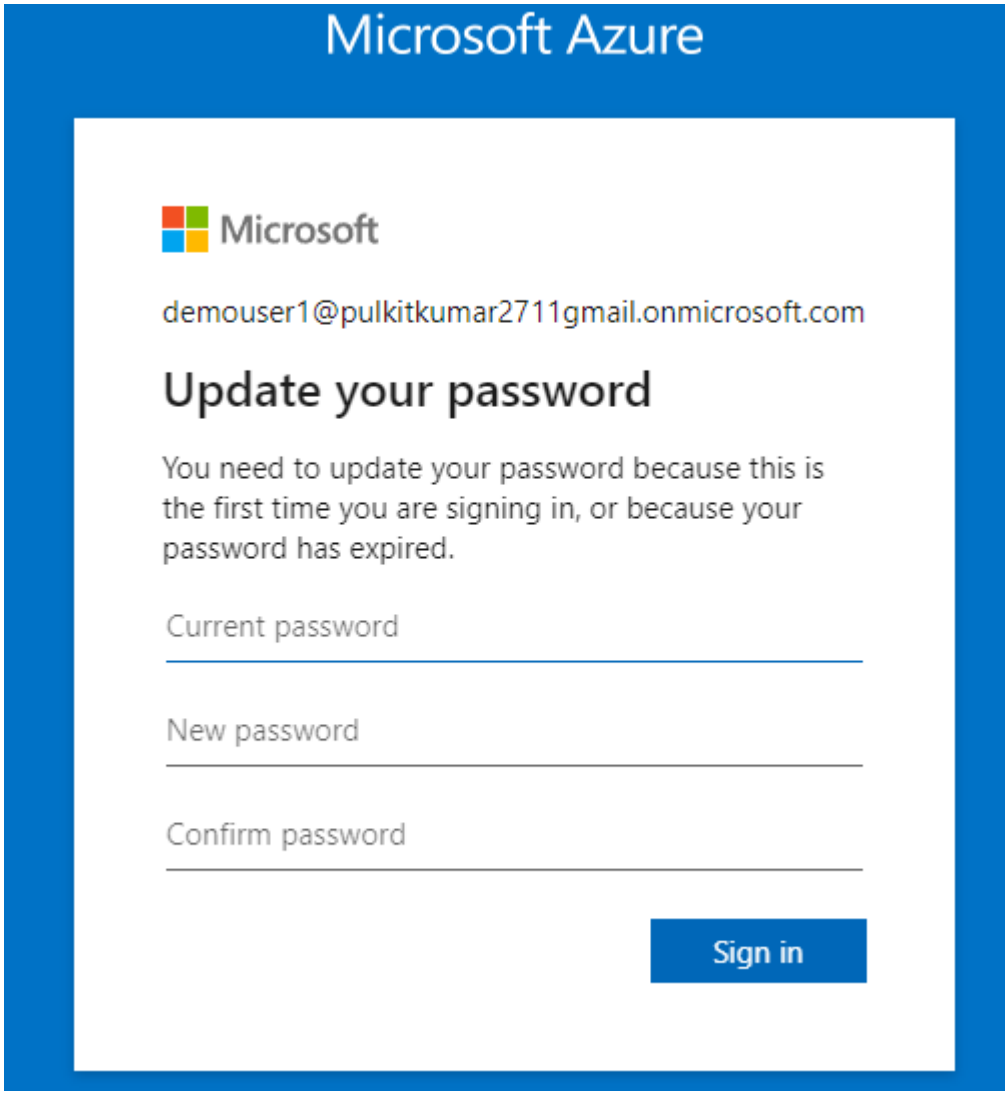

10. Now you need to open this user and in the overview, you can see the basic information for the user. Here you need to copy the user principal name because we are going to log in to this user.



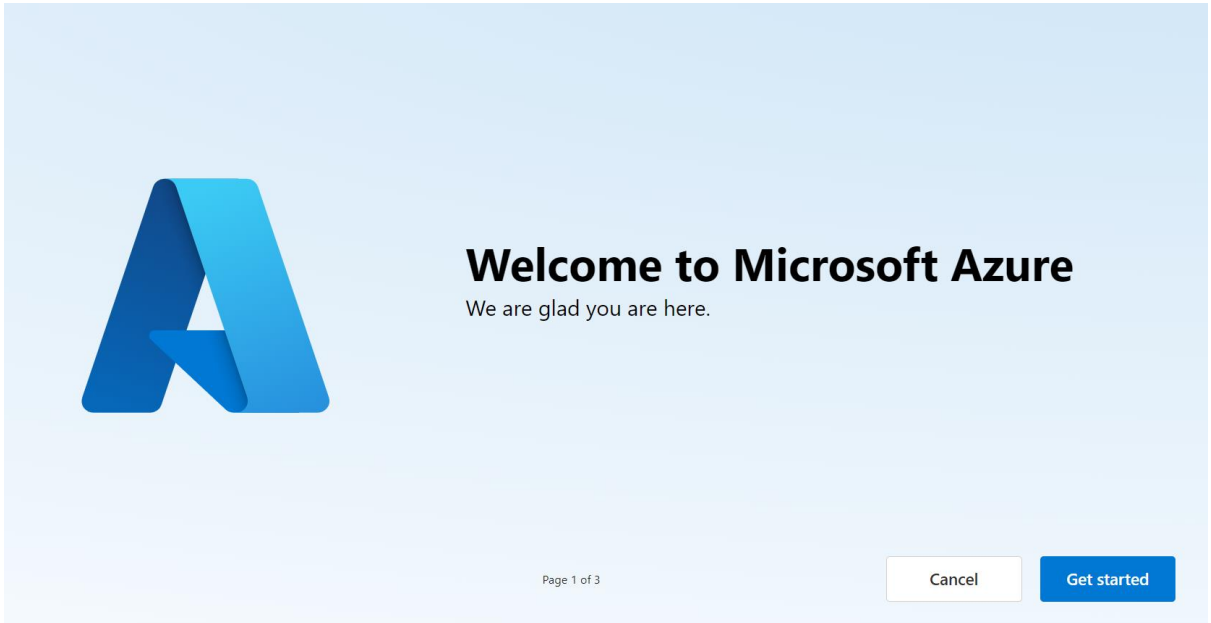

11. Then open you need open your azure portal in a new tab and click on use a different account.
12. Here you need to paste the user principal name then click on next and enter the password of your user.



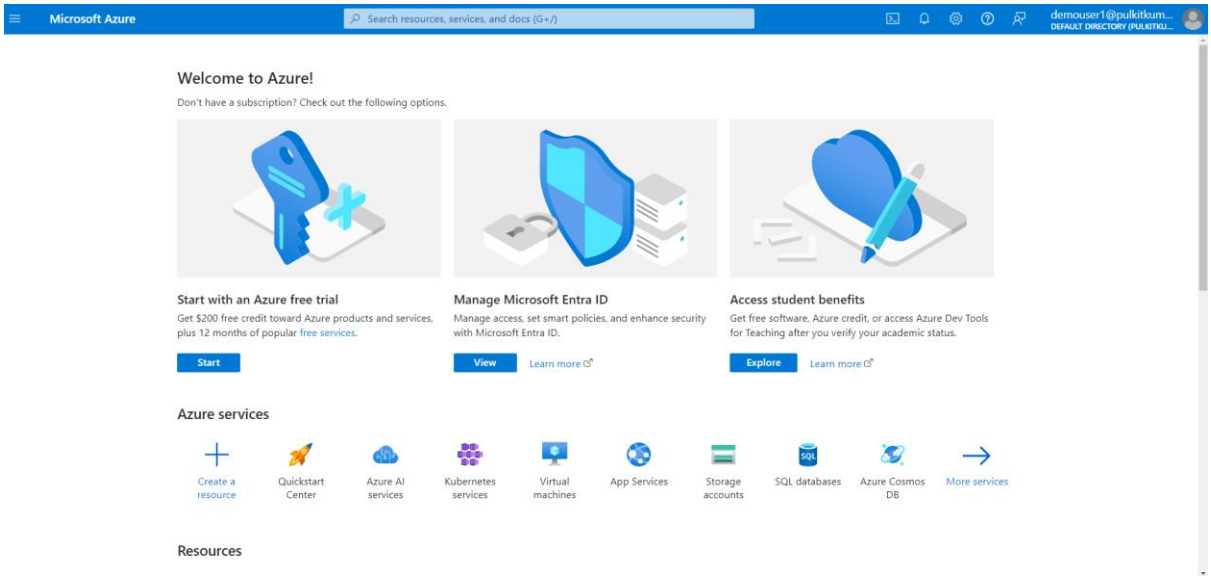

13. Then it will ask you again to change your password. So, create a new password again and then login.




14. After that you will see a welcome message, you can skip the procedure.




15. Below you can see the dashboard for your user.




16. Now if you will try to access any service as of now it will simply deny that by saying you don't have any subscription.
17. Up till now, we just created our new user, we didn't specify it any permission.