Introduction to Azure Active Directory

- **Azure Active Directory (Azure AD)** is a cloud-based identity and access management service. This service helps your employees access external resources, such as **Microsoft 365, the Azure portal, and thousands of other SaaS applications**. Azure Active Directory also helps them access internal resources like apps on your corporate intranet network, along with any cloud apps developed for your own organization. For more information about creating a tenant for your organization
- Link : https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

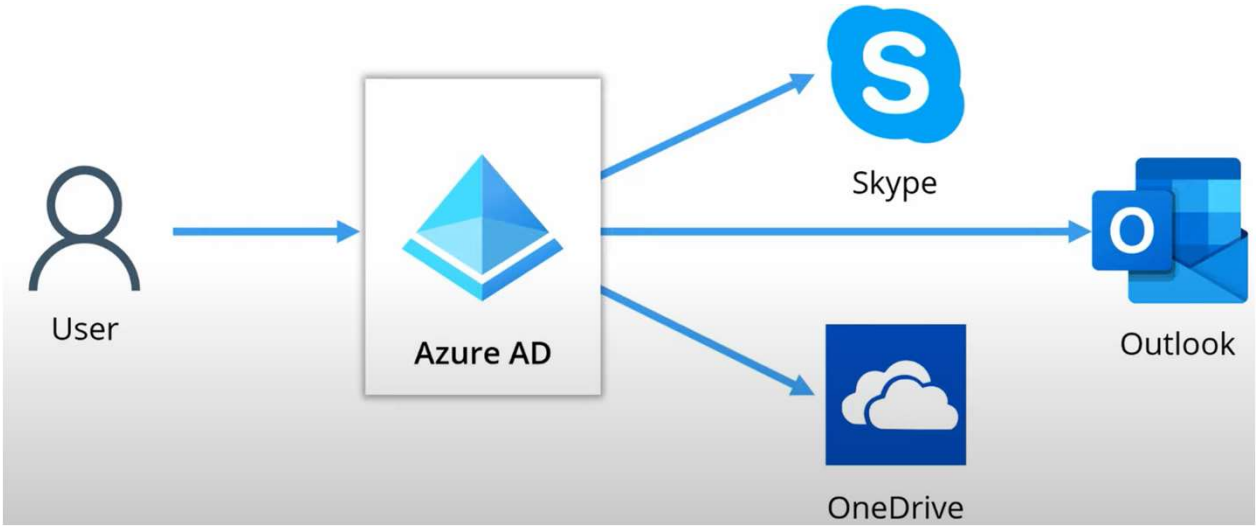
Compare Active Directory and Azure Active Directory

- Azure Active Directory is the next evolution of identity and access management solutions for the cloud. Microsoft introduced Active Directory Domain Services in Windows 2000 to give organizations the ability to manage multiple on-premises infrastructure components and systems using a single identity per user.
- Azure AD takes this approach to the next level by providing organizations with an Identity as a Service (IDaaS) solution for all their apps across cloud and on-premises.
- Link : https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-compare-azure-ad-to-ad

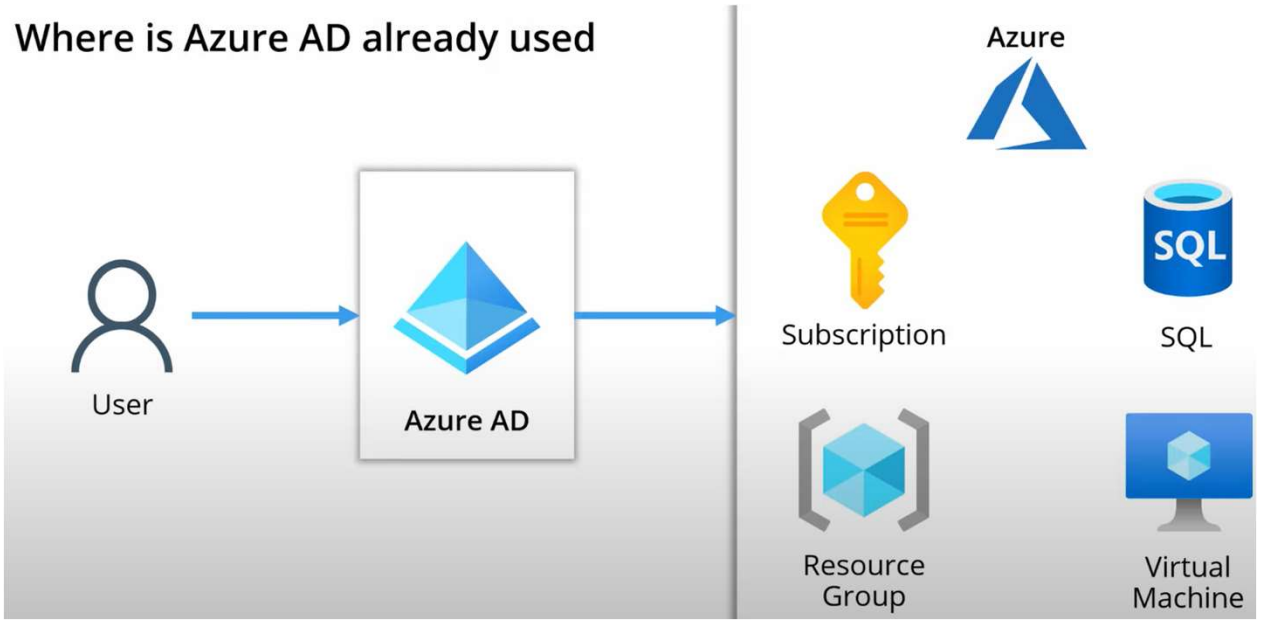
Who uses Azure AD?

- **IT admins**: As an IT admin, use Azure AD to control access to your apps and your app resources, based on your business requirements. For example, you can use Azure AD to require multi-factor authentication when accessing important organizational resources. You can also use Azure AD to automate user provisioning between your existing Windows Server AD and your cloud apps, including Microsoft 365. Finally, Azure AD gives you powerful tools to automatically help protect user identities and credentials and to meet your access governance requirements. To get started, sign up for a free 30-day Azure Active Directory Premium trial.
- **App developers**: As an app developer, you can use Azure AD as a standards-based approach for adding single sign-on (SSO) to your app, allowing it to work with a user's pre-existing credentials. Azure AD also provides APIs that can help you build personalized app experiences using existing organizational data. To get started, sign up for a free 30-day Azure Active Directory Premium trial. For more information, you can also see Azure Active Directory for developers.
- **Microsoft 365, Office 365, Azure, or Dynamics CRM Online subscribers**: As a subscriber, you're already using Azure AD. Each Microsoft 365, Office 365, Azure, and Dynamics CRM Online tenant is automatically an Azure AD tenant. You can immediately start to manage access to your integrated cloud apps.

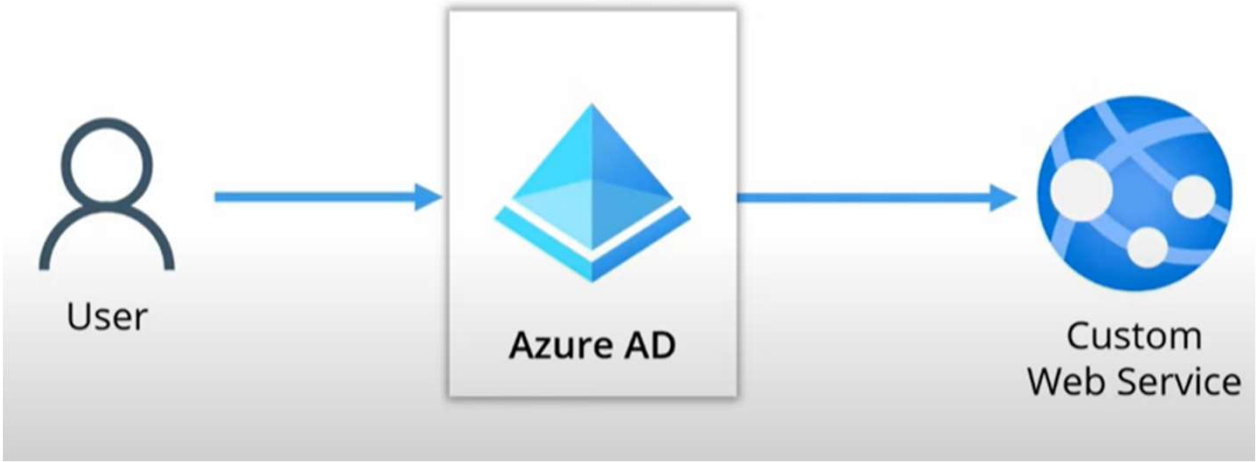
Existing/Default Active Directory and Azure Active Directory .1



Existing/Default Active Directory and Azure Active Directory.2



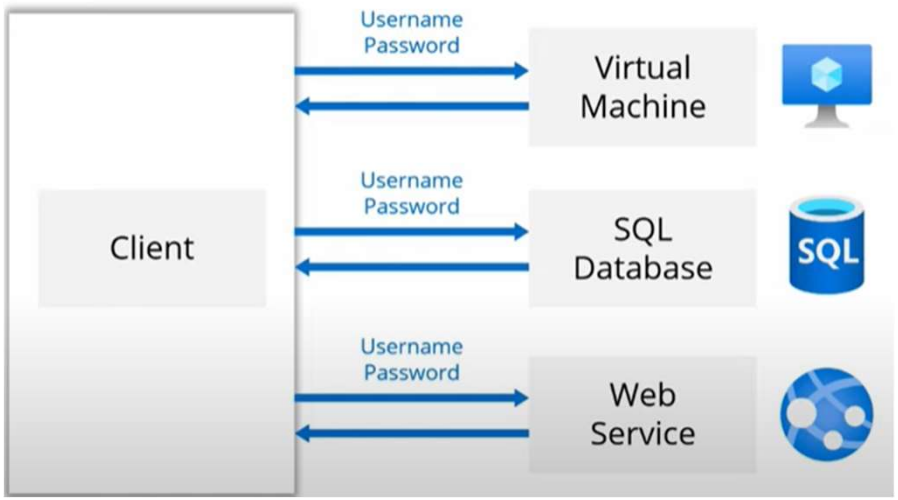
Existing/Default Active Directory and Azure Active Directory.3

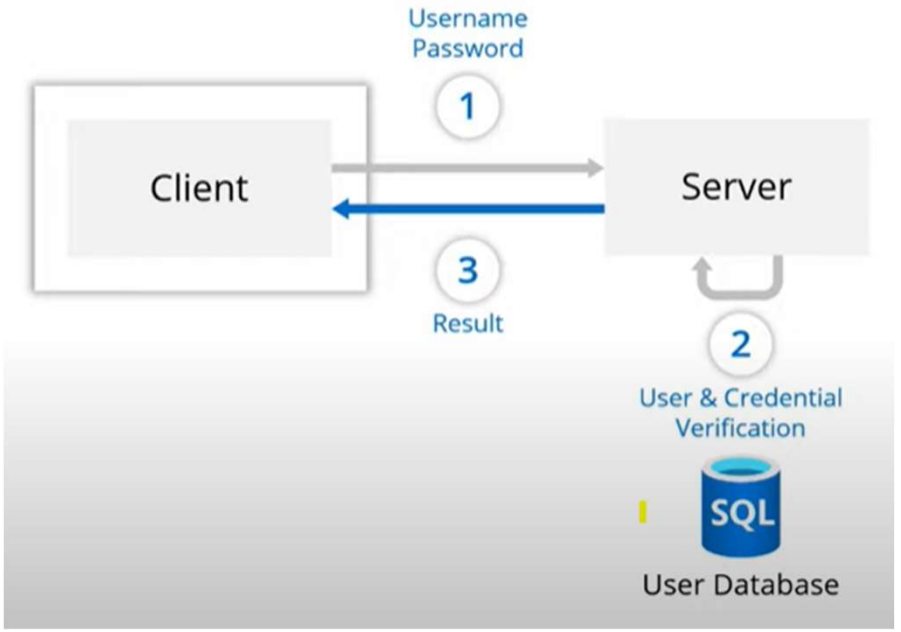


Identity and Authentication : What is Azure Active Directory authentication

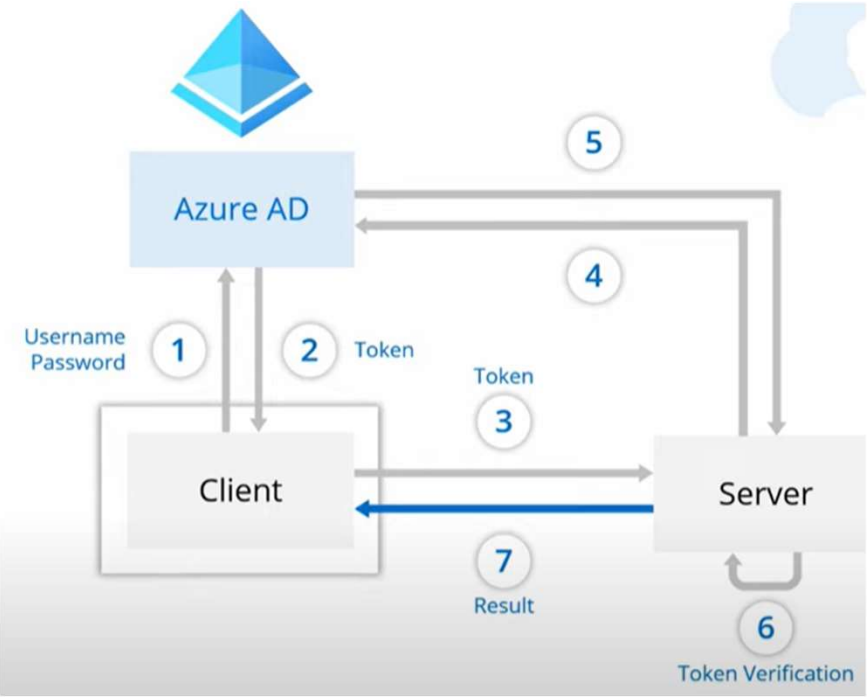
- Link : https://docs.microsoft.com/en-us/azure/active-directory/authentication/overview-authentication
- One of the main features of an identity platform is to verify, or *authenticate*, credentials when a user signs in to a device, application, or service. In Azure Active Directory (Azure AD), authentication involves more than just the verification of a username and password. To improve security and reduce the need for help desk assistance, Azure AD authentication includes the following components:
- Self-service password reset
- Azure AD Multi-Factor Authentication
- Hybrid integration to write password changes back to on-premises environment
- Hybrid integration to enforce password protection policies for an on-premises environment
- Passwordless authentication

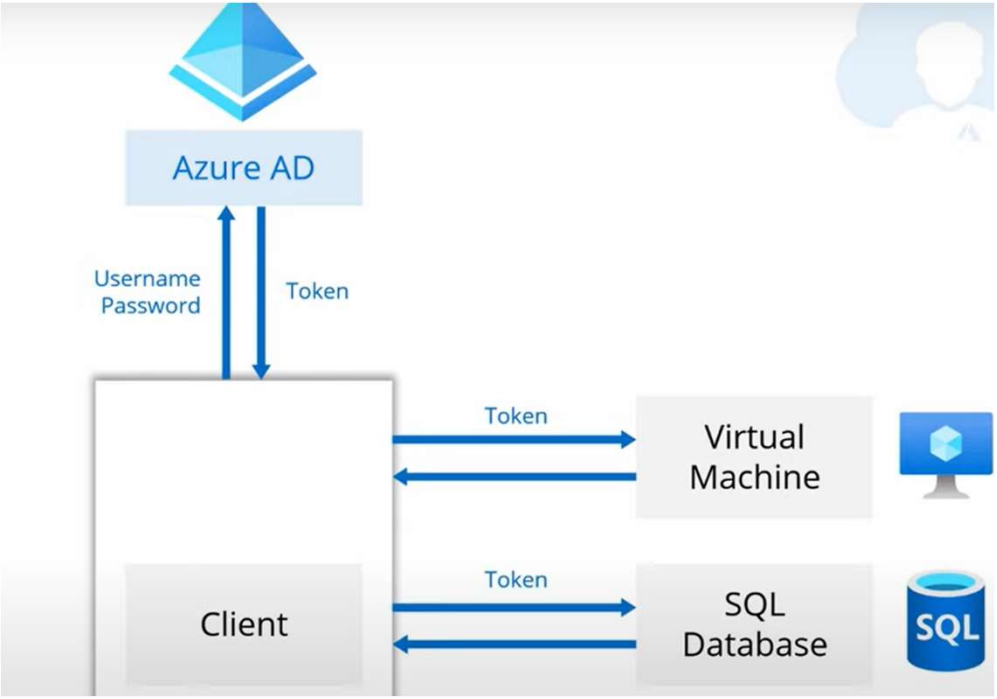
Traditional Identification using UserName and Password





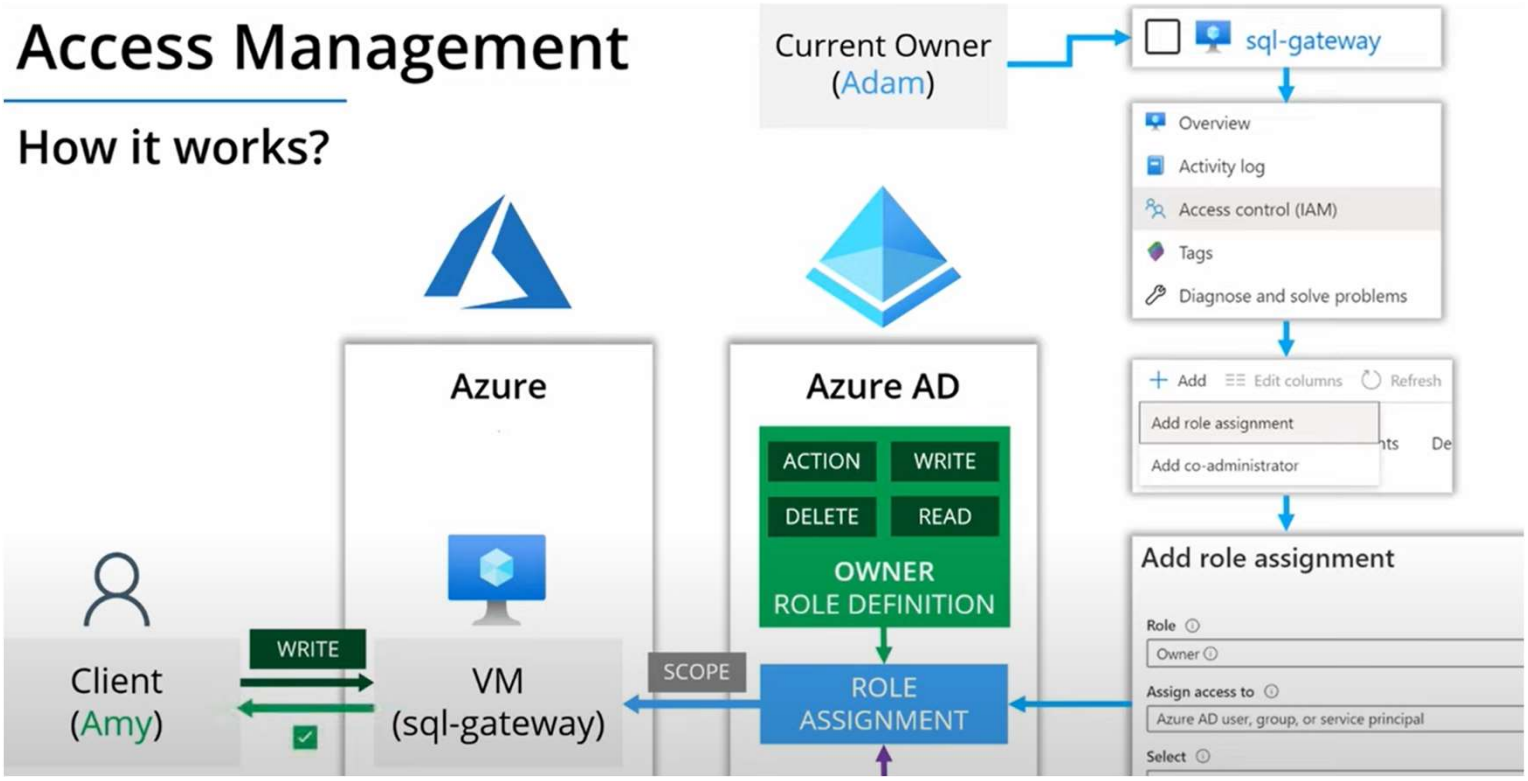
How Azure AD works for Identification






USERS
AZURE AD
SUBSCRIPTION
VM
RESOURCE GROUPS
DATABASE
AZURE

Azure Access Management




D
E

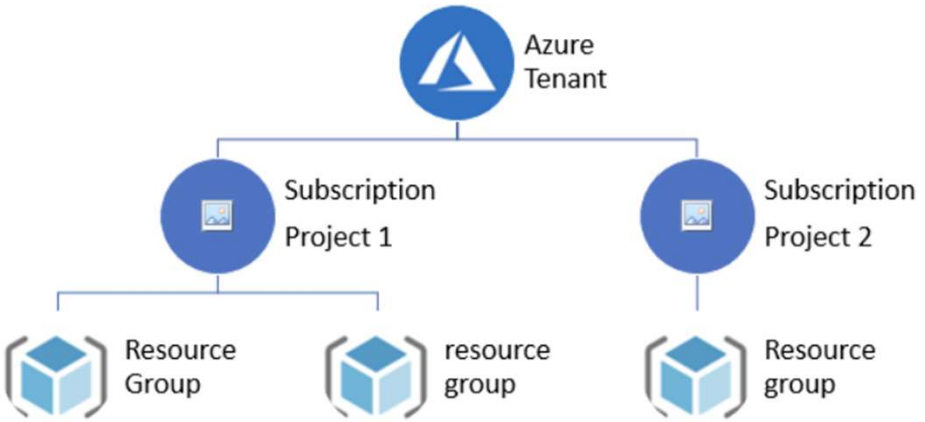
Azure Tenant, Directory, Azure Subscription, And Cost Management

- **Azure Tenant :** A tenant is an organization that owns and manages a specific instance of Microsoft cloud services. In other words, we can refer to the set of Office 365 services and Azure AD for an organization. An organization will have a Domain name and register to create a tenant. The core domain come in the form of xyz@onmicrosoft.com (xyz normally the organization name). A tenant may have multiple Azure subscriptions and one or more domains can be possible
- **Directory :** A **directory** is the Azure AD service and each directory may have one or more domains. An Azure subscription has a trust relationship with Azure Active Directory which means that the subscription trusts Azure AD to authenticate users, services, and devices.
- *A directory can have many subscriptions associated with it, but only one tenant. Multiple subscriptions can trust the same Azure AD directory, but each subscription can only trust a single directory.*

QuickStart/Demo: Create a new tenant in Azure Active Directory

- Link : https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant
- Link : https://buildcloudnext.com/2019/07/azure-tenant-directory-azure-subscription-and-cost-management/

- What is tenant in Azure/MS :




D
E