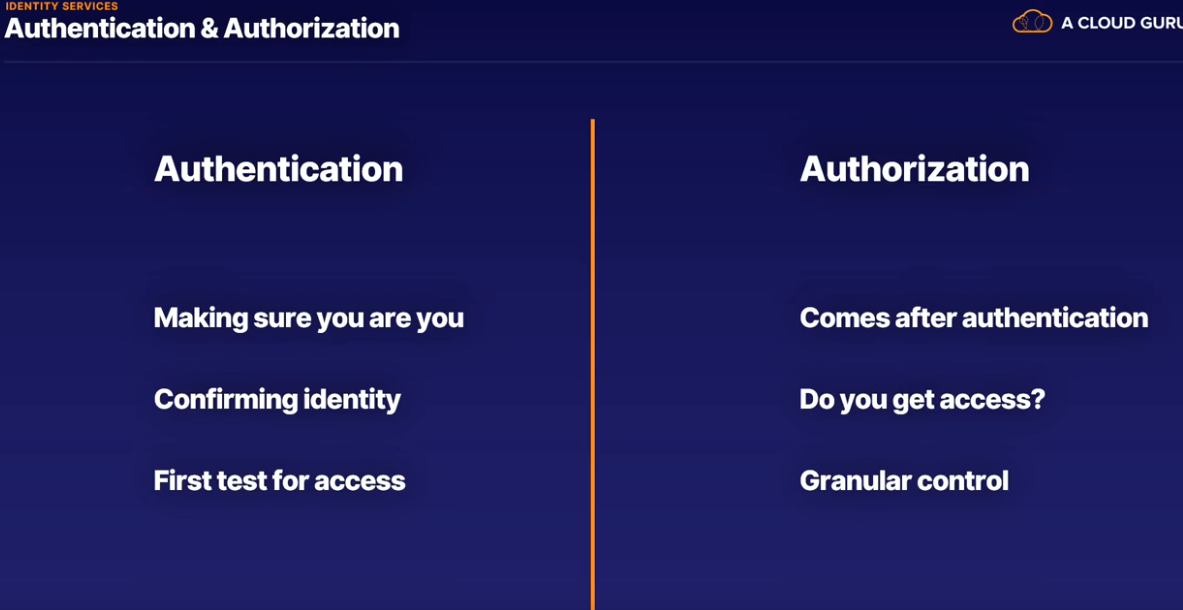
Identity Services



Azure Active Directory(AAD)

Active Directory:

* Traditional office usage- active directory is designed for traditional office use with computers and printers.
* Web- web services were not part of original vision for active directory in 2000
* Active directory authentication uses services that are not available in azure.

which is the main tool to manage users and permissions.

Azure Active Directory:

1.mandatory- because you can't have an Azure account without an AAD service.

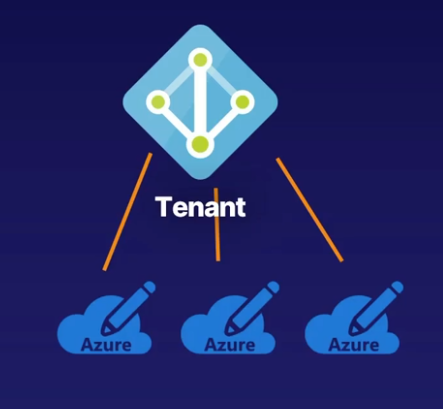
2.first user- Every Azure account has to have a first user and owner, and that user needs to be in an Azure Active Directory instance.

Tenant:

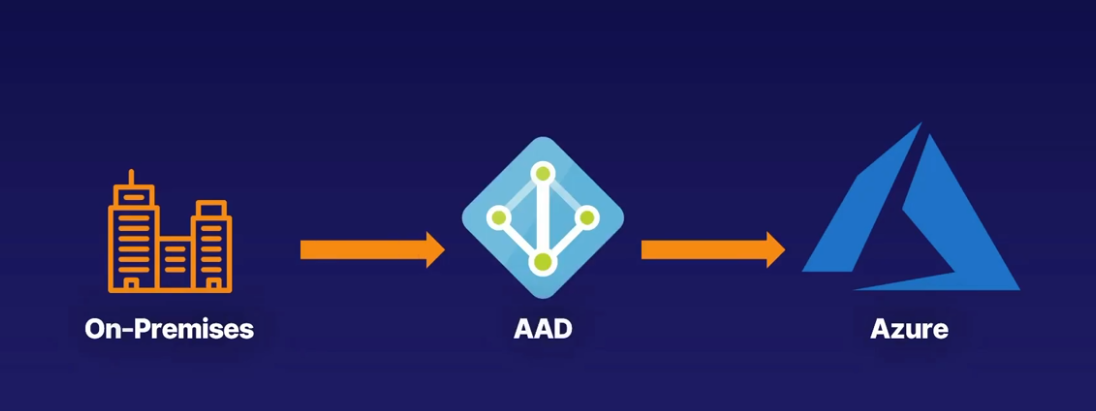
A tenant is a dedicated instance of Azure Active Directory, which is the first AAD instance that is created when a user signs up for Azure or another Microsoft Cloud service. It is the instance of AAD I mentioned just before; the one that is created as the first thing in a new Azure account. Each Azure AD tenant is distinct and separate from other Azure AD tenants. A user belongs to a tenant and only 1 tenant. All users in Azure are part of an AAD instance but can also be guests in others. This means that while a user belongs to a single tenant, they can be guests of others.

One user- one tenant

Subscriptions:

these are billing entities that will get an invoice each month for the Azure resources that have been used and are associated with that subscription. You can use subscriptions to separate who pays for what as you can have multiple subscriptions within a single tenant, and if you don't pay your Azure bill for a subscription, all the resources and services linked to it will stop working, pay your bills.

Hybrid Cloud Architecture:





1.Azure Active Directory is the main tool to manage users and permissions on Azure.

2.First of all, Active Directory, the tool for on-premises management of users, computers, printers, and more is not the same as Azure Active Directory.

3.It is unlikely you can transfer knowledge from AD to Azure AD, it is a different skillset.

4.You can't have an Azure account without an Azure AD service,

it is the first service that is created on a new Azure account.

5.A tenant is a dedicated instance of Azure AD and represents your organization.

It's also the first instance of Azure AD created on the account.

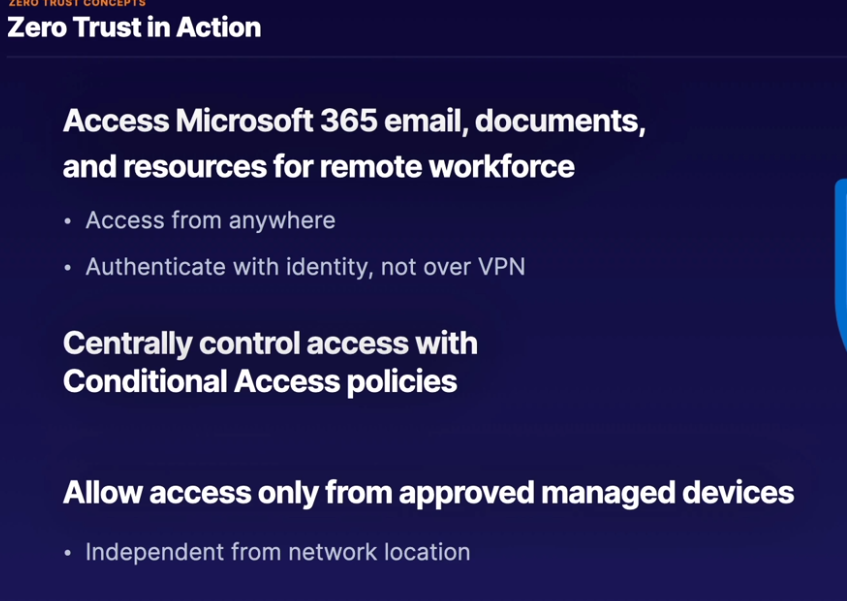
6.A user belongs to a single tenant but can be a guest on other tenants as well.

7.A subscription is a billing entity, and if the subscription is restricted,

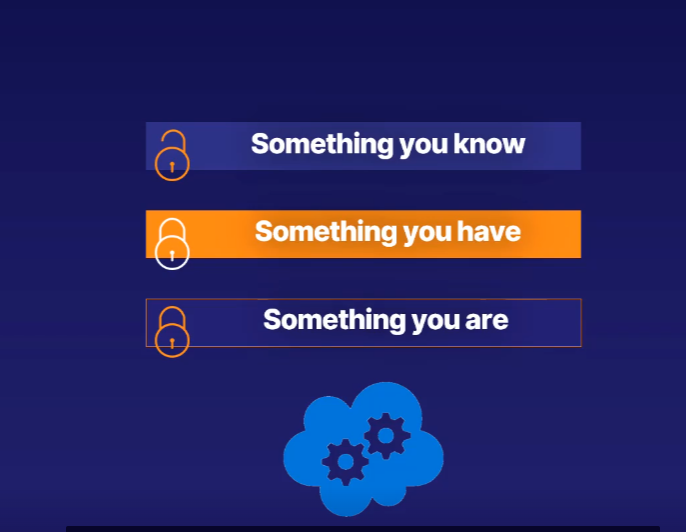
so are all the resources within it, and all resources belong to a single subscription.

8.Azure AD can help you manage users in a hybrid cloud setup as well.

Zero Trust Concepts

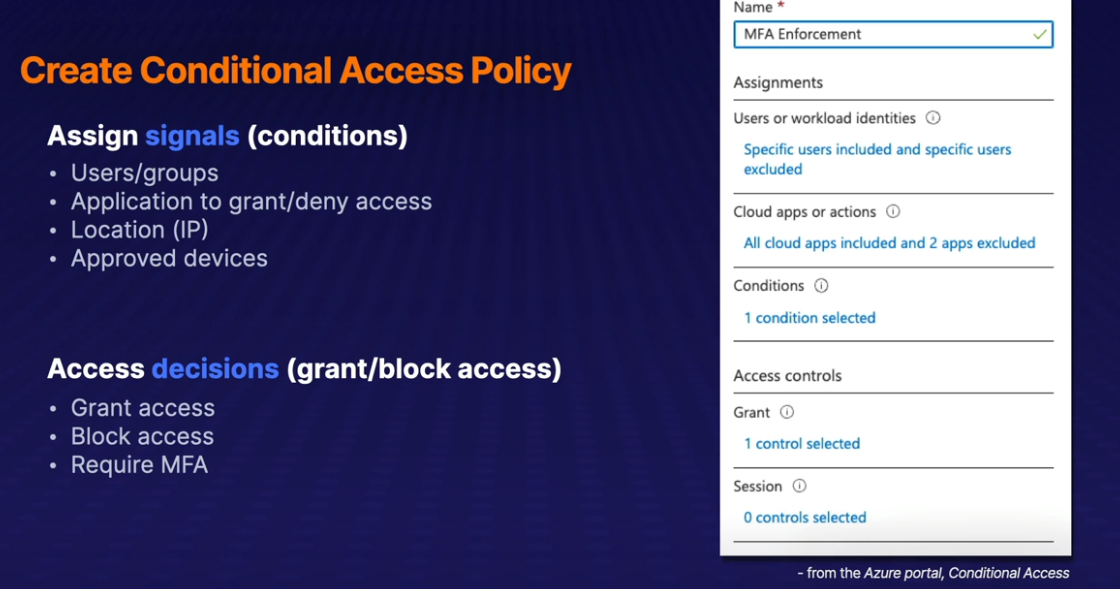


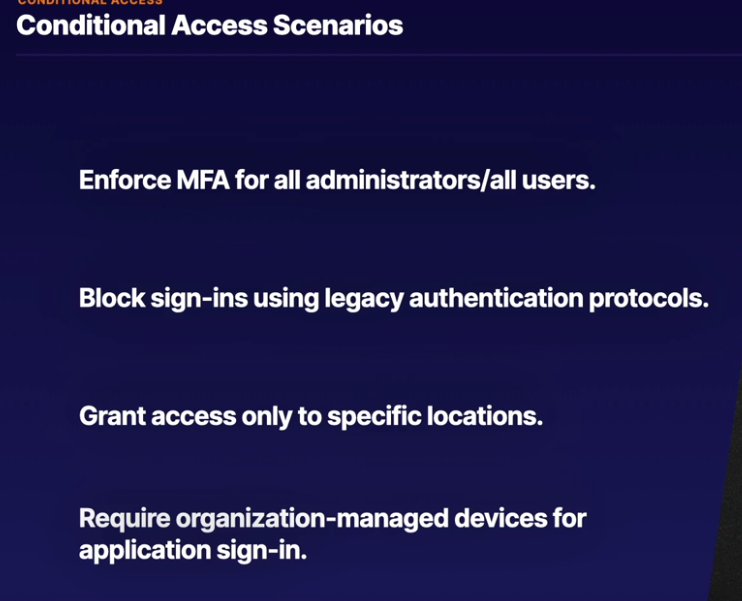
Multi-factor-authentication:



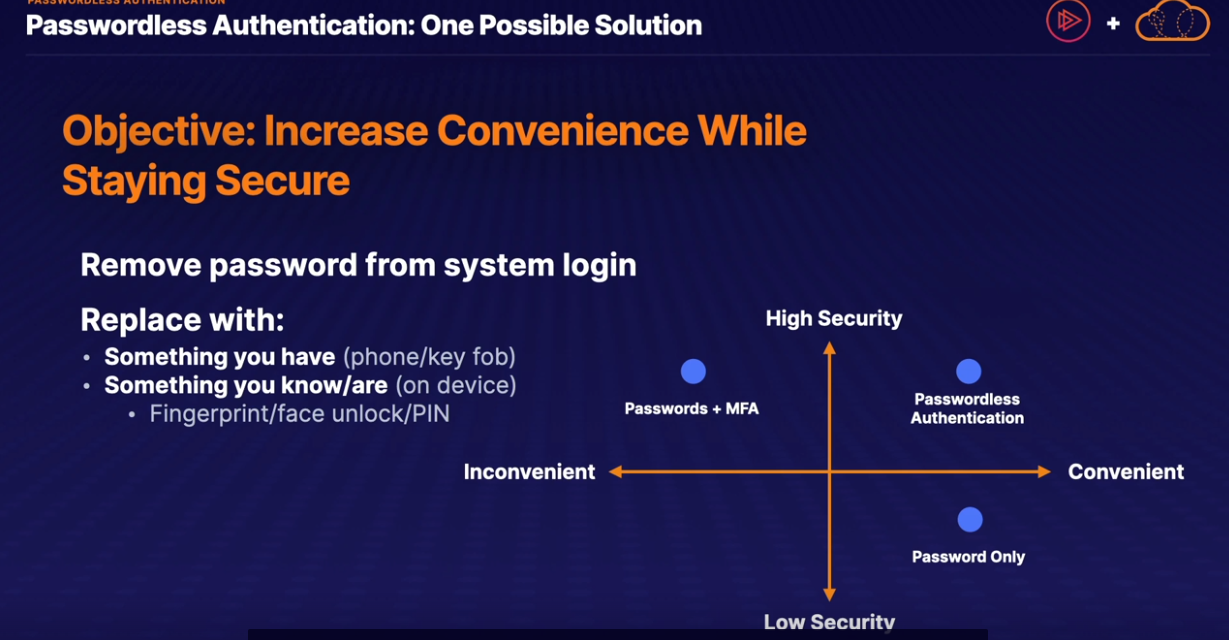
Conditional access policies

If you want to apply greater protections to identities hosted in Azure Active Directory, Conditional Access policies are your solution. Overall, Conditional Access policies are a premium feature built into Azure Active Directory, which provide different authentication protections beyond simply supplying a username and password.

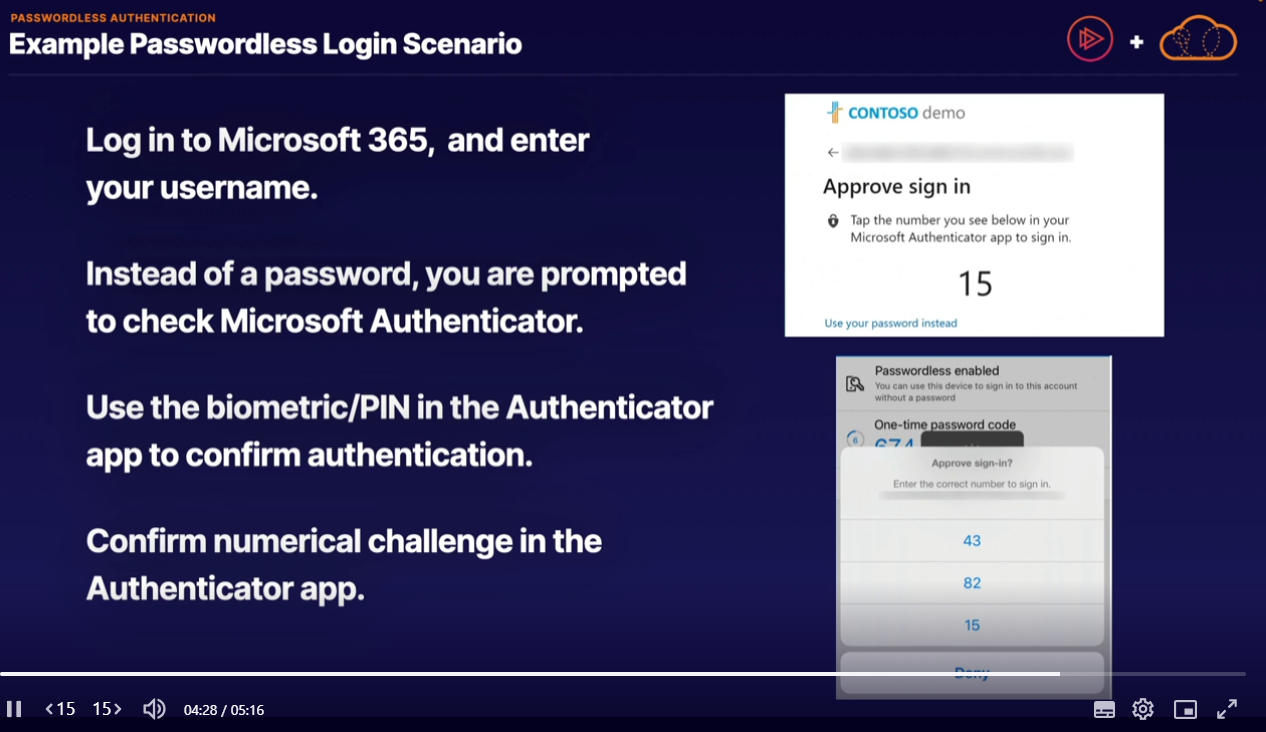




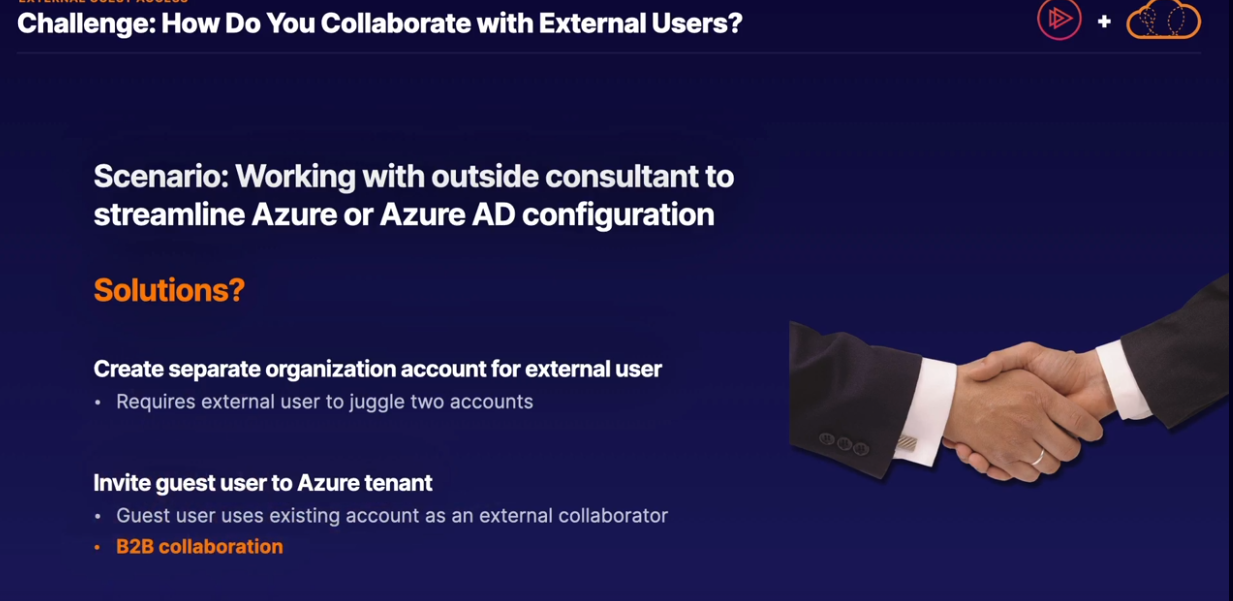
Password less Authentication

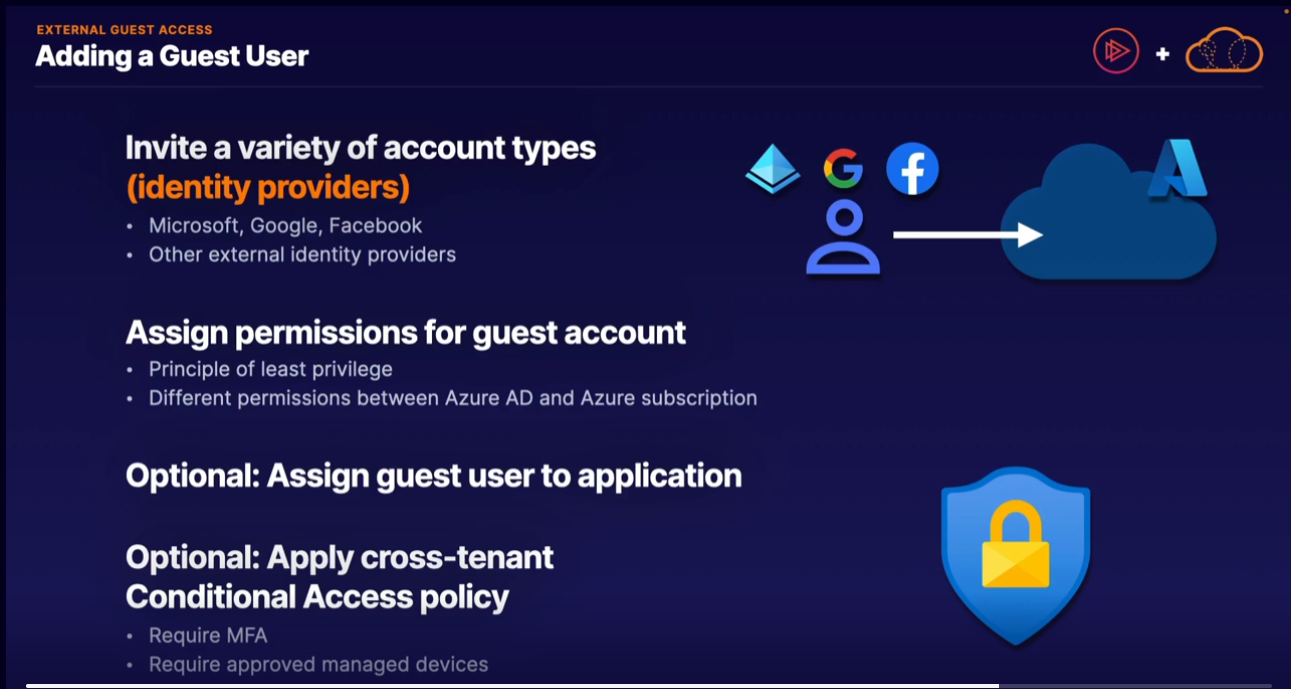


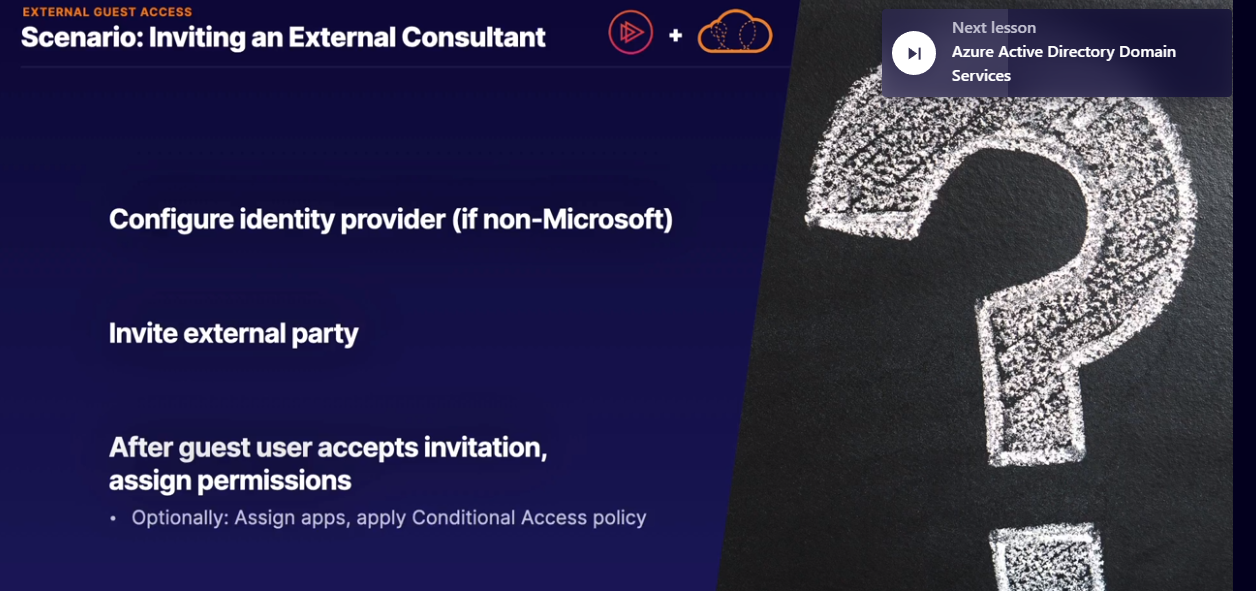




External Guest Access





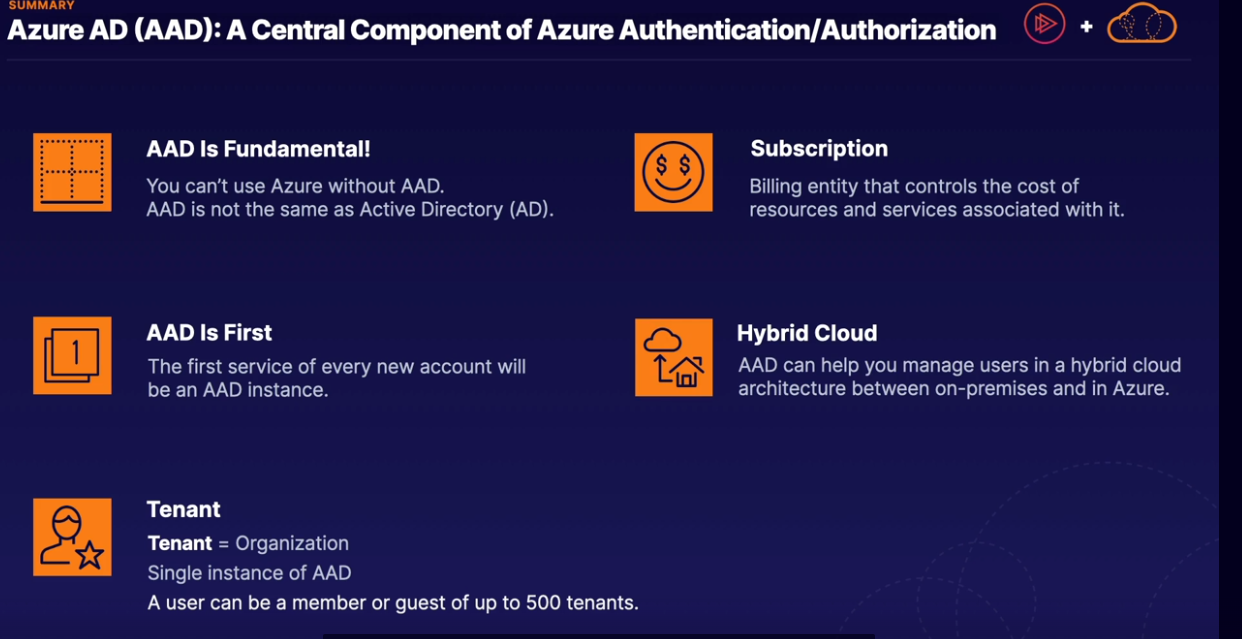


AAD Domain services

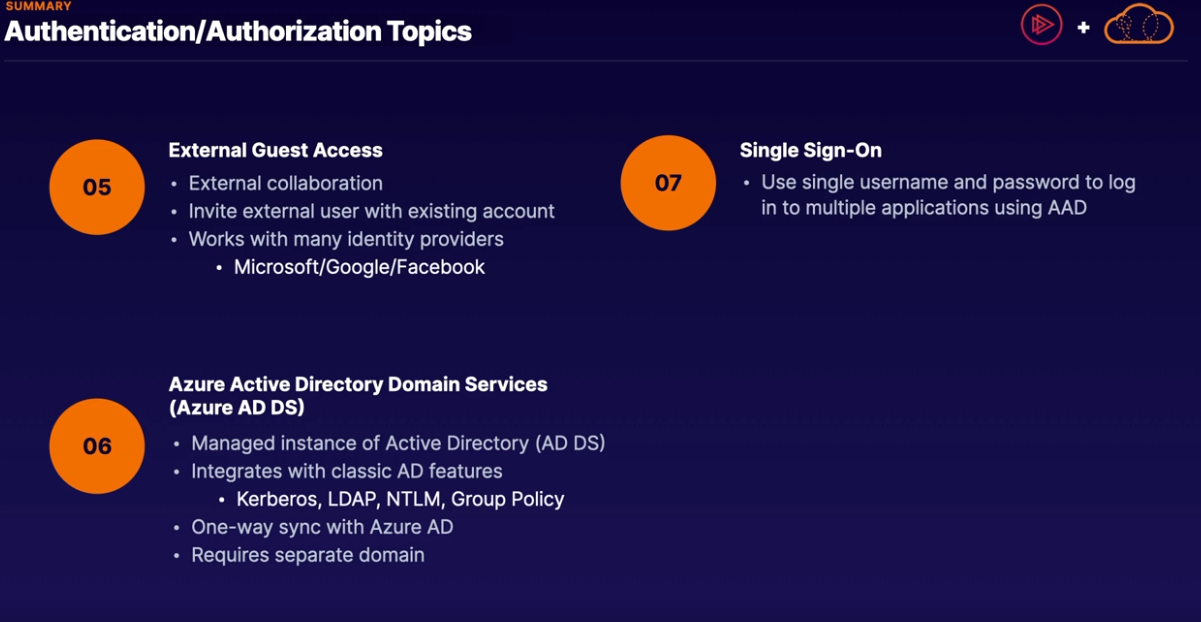
For larger organizations, one of the largest barriers to full cloud adoption is in how to properly integrate older applications with modern cloud services.

Single-sign-on

If you want to use just one username and password to log in to multiple applications, you can use single sign-on in Azure.







1.What are the two main components of a Conditional Access policy?

* SKU
* Redundancy method
* Signals
* Decisions

Correct Answer

Signals are the if/then conditions that determine if a policy is applied to a user login.

When the signals (conditions) of a Conditional Access policy are met, a decision is then made to either grant or block access, including requiring MFA at login.

2. Which types of management/protocols are ideal for using Azure Active Directory Domain Services (AADDS)?

* Kerberos
* Group Policy
* OAuth 2.0
* NTLM

Correct Answer

Kerberos is an authentication protocol traditionally handled by Active Directory Domain Services (AD DS). AADDS is able to replicate the protocols and management methods of traditional Active Directory in a managed cloud service.

Group Policy is a management tool traditionally handled by Active Directory Domain Services (AD DS), which is not supported in Azure AD. AADDS is able to replicate the protocols and management methods of traditional Active Directory in a managed cloud service.

NTLM is an authentication protocol traditionally handled by Active Directory Domain Services (AD DS). AADDS is able to replicate the protocols and management methods of traditional Active Directory in a managed cloud service.

3.Which are authentication methods used to verify a user with multi-factor authentication?

* Something you feel
* Something you are
* Something you say
* Something you have
* Something you can recall quickly
* Something you know

Good work!

Azure multi-factor authentication (MFA) helps safeguard access to data and applications while maintaining simplicity for users. It provides additional security by requiring a second form of authentication and delivers strong authentication via a range of easy-to-use authentication methods, which are something you know, have, or are.

4. What is a simple definition of the Zero Trust security model?

* All users are assumed to be untrustworthy unless they are in a trusted location, like a corporate network.
* No users ever have access to resources because they are not trusted.
* All users are assumed to be untrustworthy until proven otherwise using identity.
* Zero Trust is another name for Conditional Access policies.

Correct Answer

Identity-based authorization enables the "work from anywhere" model and does not limit users to a "trusted perimeter" to access trusted resources.

5. If you have multiple applications in Azure Active Directory that you want users to access, which is the best way to handle user access?

Using the built-in premium authentication service

Providing each user with a password for each app, as this is most secure

Using single sign-on

Using multi-factor authentication

Good work!

Single sign-on lets users use a single username and password to access all apps registered with Azure AD.

6. What is a preferred method of inviting an external user as a collaborator in your Azure AD environment?

* Create a separate organization account for the external user.
* Azure AD does not allow for external users. All users must belong to the primary tenant organization.
* Invite their existing account as an external guest user.
* Enable scoped views of your tenant that are accessible to approved external users.
* 7. What is a definition of authorization?
* Determination of access to a system based on assigned roles/permissions
* Being able to log in to the Azure portal from anywhere.
* Confirmation of your identity for a system.
* The ability of a system to determine your location when accessing it

Correct Answer

Authorization determines your access to a system once you have been authenticated. This could be the right to access a certain part, create a new customer, or install new software.

8.What is a definition of authentication?

* The ability of a system to determine your location when accessing it
* Being able to log in to the Azure portal from anywhere
* Determination of access to a system based on authorization
* Confirmation of your identity for a system

Good work!

Authentication is the process of determining that you are you. This is most commonly done using a username and password, but it could also be with a fingerprint or face recognition.

9.Select the true statements regarding Azure Active Directory tenants.

* An account/username can be an external guest for other tenants outside their organization.
* An account/username cannot be an external guest for other tenants outside their organization.
* A user account is tied to a single tenant.
* A user account can be tied to multiple tenants.

Good work!

A user account can be a guest of up to 499 tenants outside their organization

A user account can be a member of a single tenant.

10. How does password less authentication ease the burden of signing in with multi-factor authentication?

* A username is replaced by a secure PIN code.
* Removes system password and replaces it with device authentication combined with biometrics/PIN.
* No password is required to log in, only a valid username.
* Password less authentication requires both a system password and multi-factor authentication from an approved device.