Planning the Identity and Authentication Solution

examlabpractice.com

https://t.me/learningnets

Microsoft 365 Identity Models

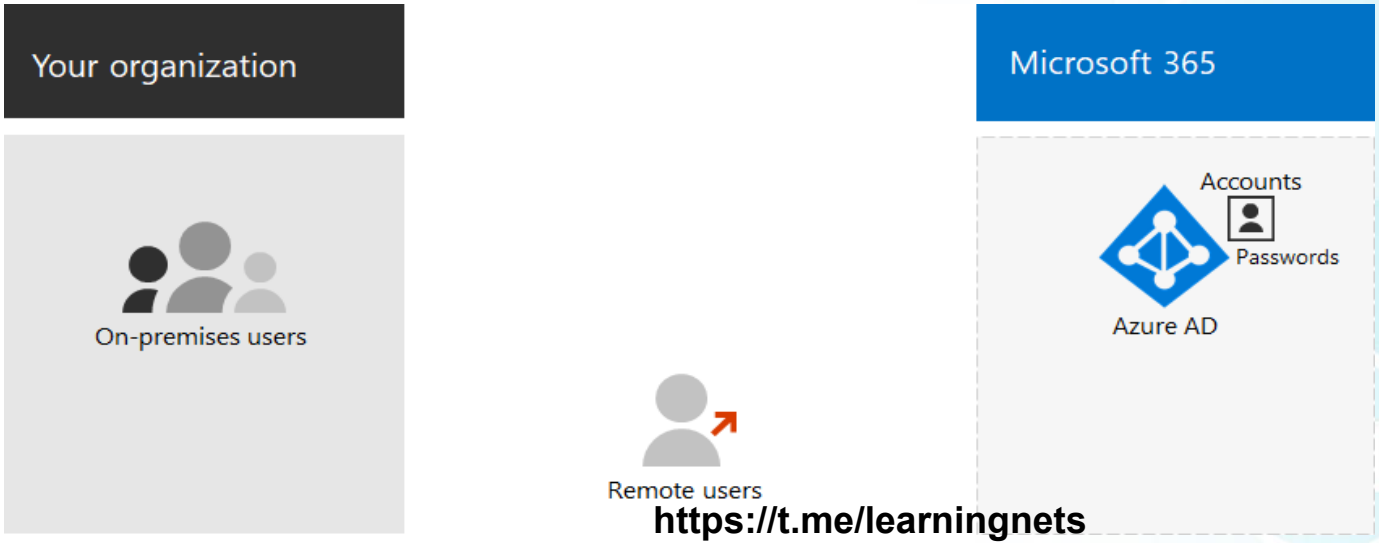
To plan for user accounts, you first need to understand the two identity models in Microsoft 365. You can maintain your organization's identities only in the cloud, or you can maintain your on-premises Active Directory Domain Services (AD DS) identities and use them for authentication when users access Microsoft 365 cloud services.

Attribute	Cloud-only identity	Hybrid identity
Definition	User account only exists in the Azure AD tenant for your Microsoft 365 subscription.	User account exists in AD DS and a copy is also in the Azure AD tenant for your Microsoft 365 subscription. The user account in Azure AD might also include a hashed version of the already hashed AD DS user account password.
How Microsoft 365 authenticates user credentials	The Azure AD tenant for your Microsoft 365 subscription performs the authentication with the cloud identity account.	The Azure AD tenant for your Microsoft 365 subscription either handles the authentication process or redirects the user to another identity provider.
Best for	Organizations that do not have or need an on-premises AD DS.	Organizations using AD DS or another identity provider.
Greatest benefit	Simple to use. No extra directory tools or servers required.	Users can use the same credentials when accessing on-premises or cloud-based resources.

https://t.me/learningnets

Cloud-only Identity

- A cloud-only identity uses user accounts that exist only in Azure AD.
- Cloud identity is typically used by small organizations that do not have on-premises servers or do not use AD DS to manage local identities.
- Both on-premises and remote (online) users use their Azure AD user accounts and passwords to access Microsoft 365 cloud services. Azure AD authenticates user credentials based on its stored user accounts and passwords.



https://t.me/learningnets

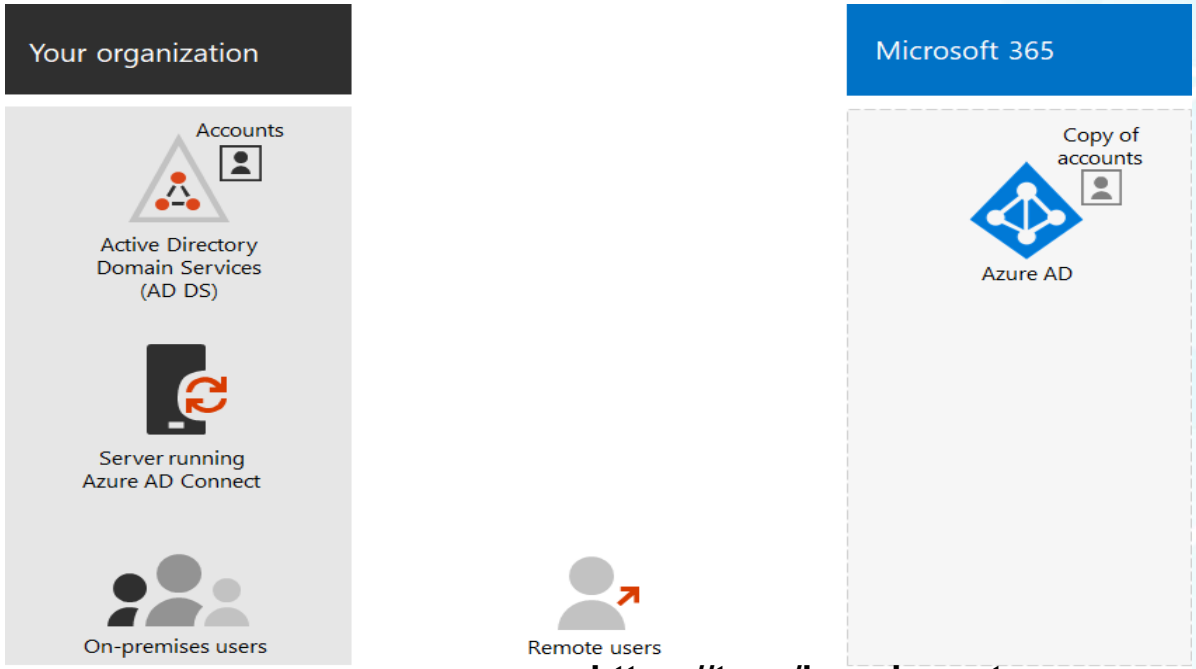
Hybrid Identity

- Hybrid identity uses accounts that originate in an on-premises AD DS and have a copy in the Azure AD tenant of a Microsoft 365 subscription.
- Most changes only flow one way. Changes that you make to AD DS user accounts are synchronized to their copy in Azure AD. But changes made to cloud-based accounts in Azure AD, such as new user accounts, are not synchronized with AD DS.
- Azure AD Connect provides the ongoing account synchronization. It runs on an on-premises server, checks for changes in the AD DS, and forwards those changes to Azure AD.
- Azure AD Connect provides the ability to filter which accounts are synchronized and whether to synchronize a hashed version of user passwords, known as password hash synchronization

https://t.me/learningnets

Components of Hybrid Identity

When implementing hybrid identity, your on-premises AD DS is the authoritative source for account information. This means that you perform administration tasks mostly on-premises, which are then synchronized to Azure AD.



https://t.me/learningnets

Administration of Hybrid Identities

- Because the original and authoritative user accounts are stored in the on-premises AD DS, you manage your identities with the same tools as AD DS, such as the Active Directory Users and Computers tool.
- You don't use the Microsoft 365 admin center or PowerShell for Microsoft 365 to manage synchronized user accounts in Azure AD..

https://t.me/learningnets