Foundational concepts for Azure AD Hybrid authentication

examlabpractice.com

Hybrid identity and directory synchronization for Microsoft 365

- Depending on your business needs and technical requirements, the hybrid identity model and directory synchronization is the most common choice for enterprise customers who are adopting Microsoft 365.
- Directory synchronization allows you to manage identities in your Active Directory Domain Services (AD DS) and all updates to user accounts, groups, and contacts are synchronized to the Azure Active Directory (Azure AD) tenant of your Microsoft 365 subscription.

Authentication for Hybrid Identity

There are two types of authentication when using the hybrid identity model:

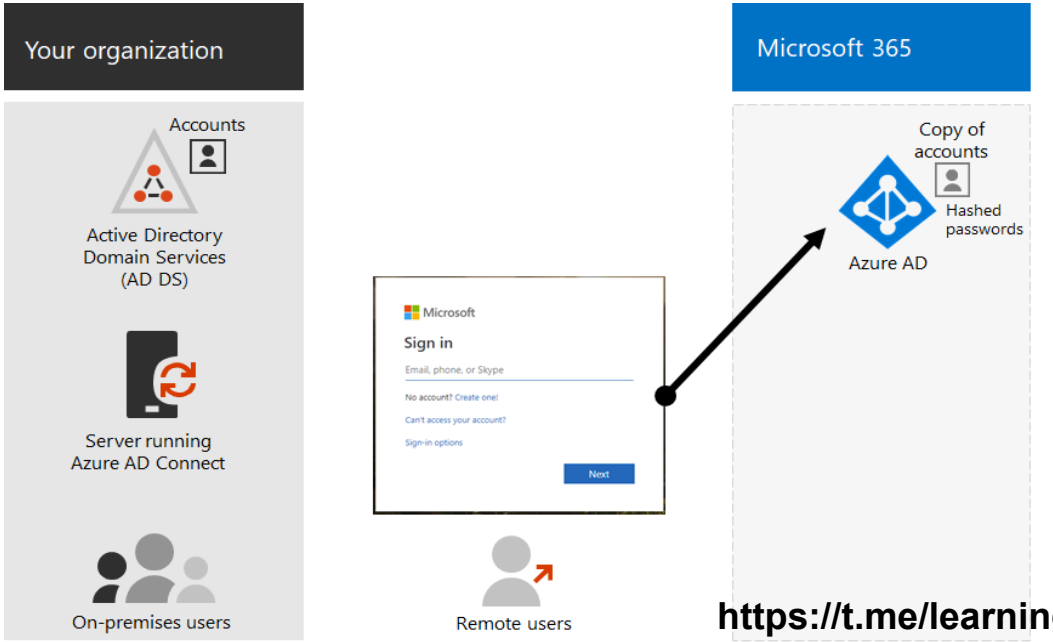
1. **Managed authentication**
   - Azure AD will handle the authentication process by using a locally-stored hashed version of the password or sends the credentials to an on-premises software agent to be authenticated by the on-premises AD DS.
2. **Federated authentication**
   - Azure AD redirects the client computer requesting authentication to another identity provider.

Managed Authentication

There are two types of managed authentication:

1. **Password hash synchronization (PHS)**
   - Azure AD performs the authentication itself.
2. **Pass-through authentication (PTA)**
   - Azure AD has AD DS perform the authentication.

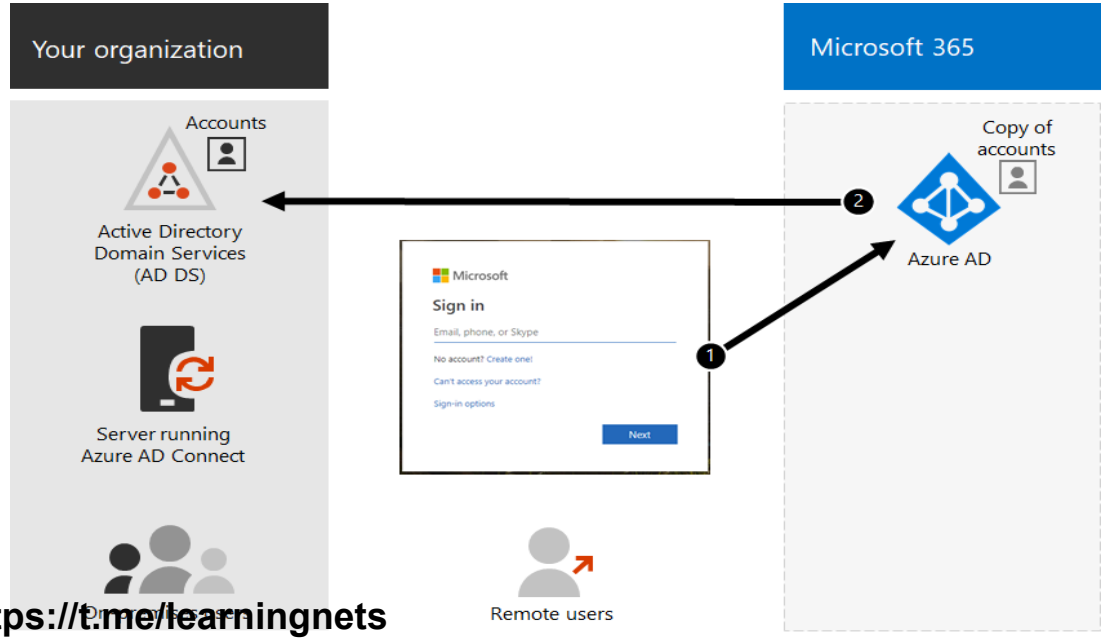
Password Hash synchronization (PHS)



With PHS, you synchronize your AD DS user accounts with Microsoft 365 and manage your users on-premises. Hashes of user passwords are synchronized from your AD DS to Azure AD so that the users have the same password on-premises and in the cloud. This is the simplest way to enable authentication for AD DS identities in Azure AD.

Pass-through authentication (PTA)

PTA provides a simple password validation for Azure AD authentication services using a software agent running on one or more on-premises servers to validate the users directly with your AD DS. With PTA, you synchronize AD DS user accounts with Microsoft 365 and manage your users on-premises.



Federated Authentication

- Federated authentication is primarily for large enterprise organizations with more complex authentication requirements.
- AD DS identities are synchronized with Microsoft 365 and users accounts are managed on-premises.
- With federated authentication, users have the same password on-premises and in the cloud and they do not have to sign in again to use Microsoft 365.
- Federated authentication can support additional authentication requirements, such as smartcard-based authentication or a third-party multi-factor authentication and is typically required when organizations have an authentication requirement not natively supported by Azure AD.