Evaluating Requirements and Solutions for Authentication

examlabpractice.com

https://t.me/learningnets

Authentication Methods

- When the Azure AD hybrid identity solution is your new control plane, authentication is the foundation of cloud access.
- Choosing the correct authentication method is a crucial first decision in setting up an Azure AD hybrid identity solution.
- Implement the authentication method that is configured by using Azure AD Connect, which also provisions users in the cloud.

To choose an authentication method, you need to consider the time, existing infrastructure, complexity, and cost of implementing your choice. These factors are different for every organization and might change over time.

https://t.me/learningnets

Cloud authentication

- **Azure AD password hash synchronization.**
  - The simplest way to enable authentication for on-premises directory objects in Azure AD.
  - Users can use the same username and password that they use on-premises without having to deploy any additional infrastructure.
  - Some premium features of Azure AD, like Identity Protection and Azure AD Domain Services, require password hash synchronization, no matter which authentication method you choose.
- **Azure AD Pass-through Authentication.**
  - Provides a simple password validation for Azure AD authentication services by using a software agent that runs on one or more on-premises servers.
  - The servers validate the users directly with your on-premises Active Directory, which ensures that the password validation doesn't happen in the cloud.
  - Companies with a security requirement to immediately enforce on-premises user account states, password policies, and sign-in hours might use this authentication method.

https://t.me/learningnets

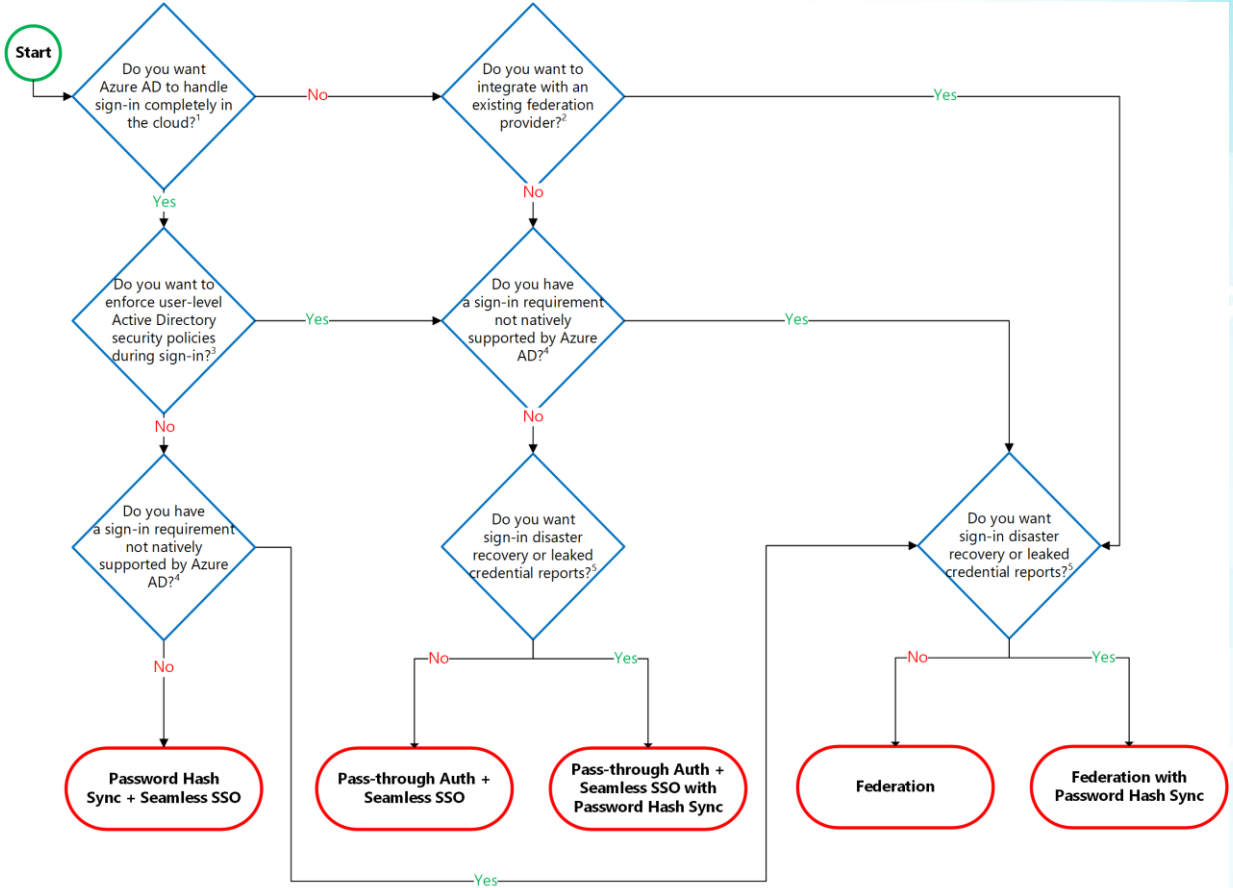
Federated Authentication

- When you choose this authentication method, Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user's password.

- The authentication system can provide additional advanced authentication requirements. Examples are smartcard-based authentication or third-party multifactor authentication.

https://t.me/learningnets

Deciding on which solutions is best



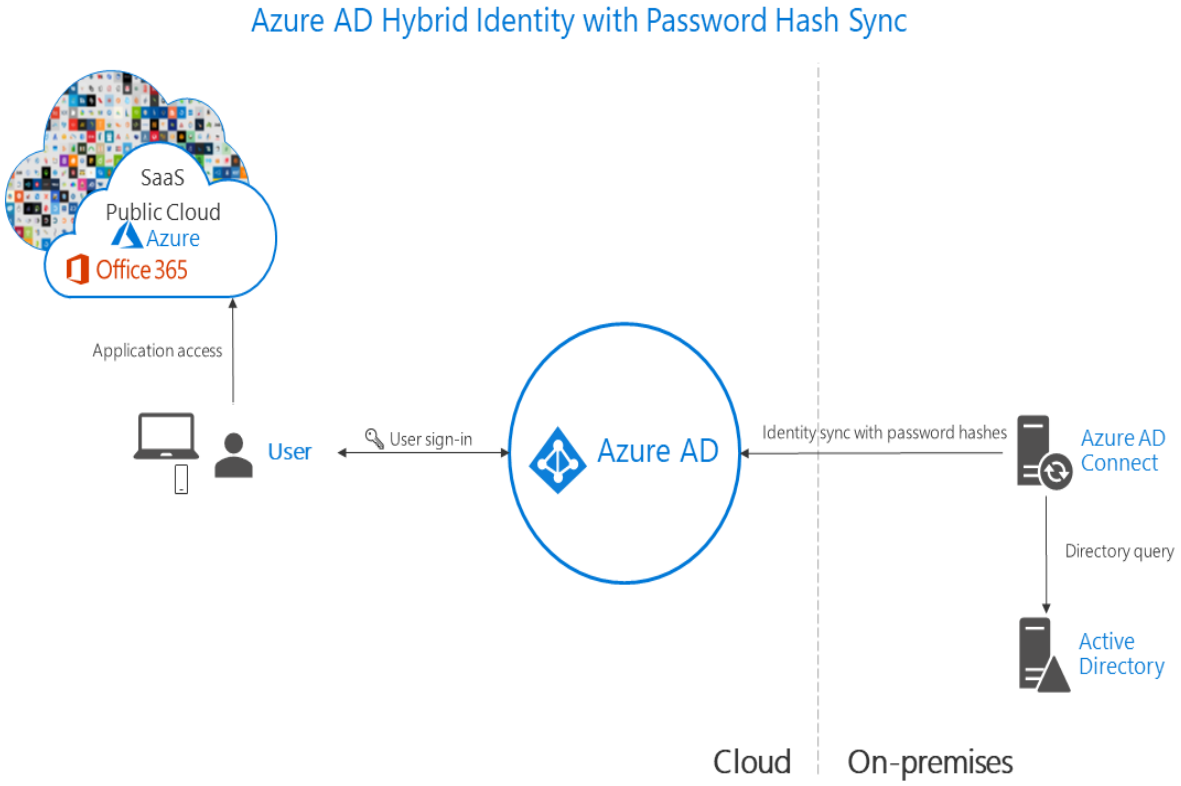
https://t.me/learningnets

Considerations for Password Hash Sync

- Password hash synchronization requires the least effort regarding deployment, maintenance, and infrastructure.
- This level of effort typically applies to organizations that only need their users to sign in to Microsoft 365, SaaS apps, and other Azure AD-based resources.
- When turned on, password hash synchronization is part of the Azure AD Connect sync process and runs **every two minutes**.
- To improve users' sign-in experience, deploy seamless SSO with password hash synchronization. Seamless SSO eliminates unnecessary prompts when users are signed in.

https://t.me/learningnets

Password Hash Sync



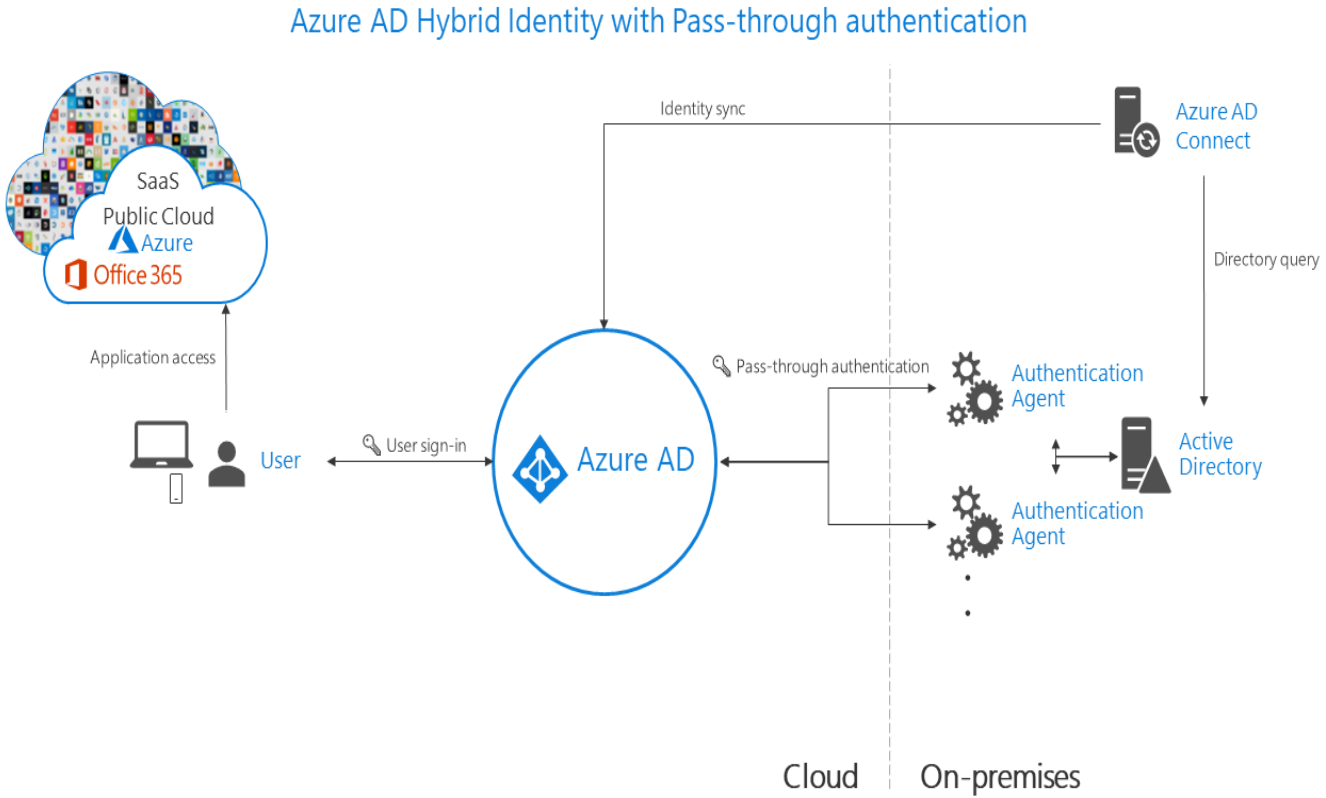
https://t.me/learningnets

Considerations for Pass-Through Authentication

- For pass-through authentication, you need one or more (we recommend three) lightweight agents installed on existing servers.
- These agents must have access to your on-premises Active Directory Domain Services, including your on-premises AD domain controllers.
- They need outbound access to the Internet and access to your domain controllers. For this reason, it's not supported to deploy the agents in a perimeter network.
- To improve users' sign-in experience, deploy seamless SSO with Pass-through Authentication. Seamless SSO eliminates unnecessary prompts after users sign in

https://t.me/learningnets

Pass-Through Authentication



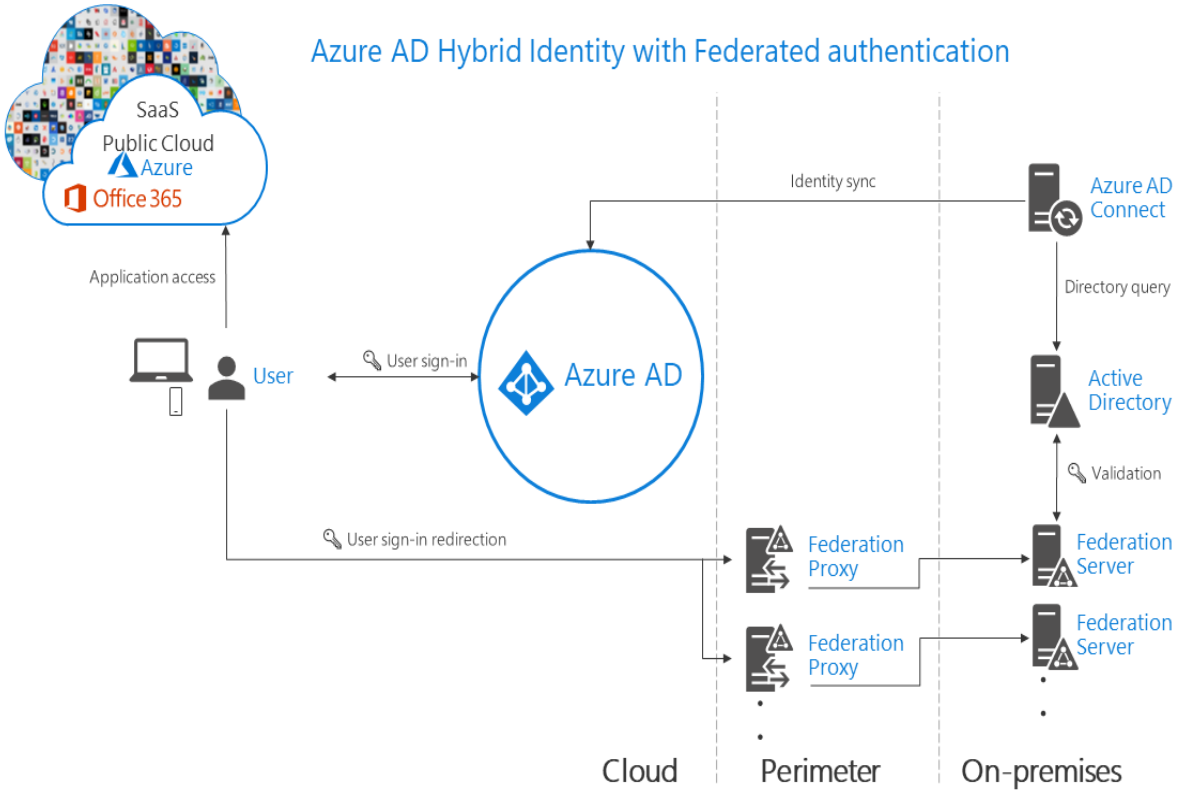
https://t.me/learningnets

Considerations for Federated Authentication

- A federated authentication system relies on an external trusted system to authenticate users.
- Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution.
- The maintenance and management of the federated system falls outside the control of Azure AD.
- It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.
- Federated systems typically require a more significant investment in on-premises infrastructure.
- Most organizations choose this option if they already have an on-premises federation investment.

https://investstrippers

Federated Authentication



https://t.me/learningnets