Azure AD

# The Identity Problems facing many companies/developers

We have resources that could literally be anywhere!

1. On-prem resources
2. Resources in a partner organization
3. Public cloud (O365)
4. Private Cloud
5. Multi-Hop scenarios
6. Impersonation (Server acting on behalf of another person)

Our user, using many different devices simply want to gain access to those resources with no issues.

# The basic idea behind Azure AD

All your synchronized users from your On-Prem AD DS are stored out in the cloud, where you can manage them with:

* The Azure Management portal
* Powershell scripts
* Graph APIs (For tooling vendors)

By doing this, you now have access to federated protocols

* OpenID Connect/OAuth 2.0
* WS-Federation and SAML
* Windows Kerberos Authentication
* Multi-factor Authentication building
* Conditional Access
* Identity Protection

# That tool is Azure AD Connect

Best practice: Azure AD Connect needs to use a Service account to grab usernames and passwords, but need not have any additional privileges. Avoid the temptation to use a domain admin account. Only give the account the permissions it needs.

https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-accounts-permissions

AD Connect is a continuously evolving product so Set-ADSyncAutoUpgrade to true.