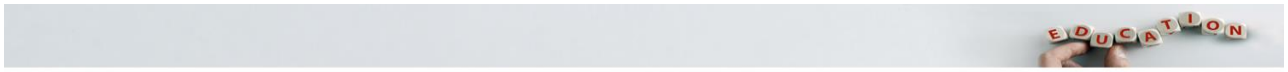
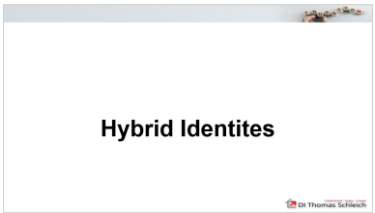
Azure Active Directory

DI Thomas Schleich

Understand - Apply - Create
DI Thomas Schleich

1





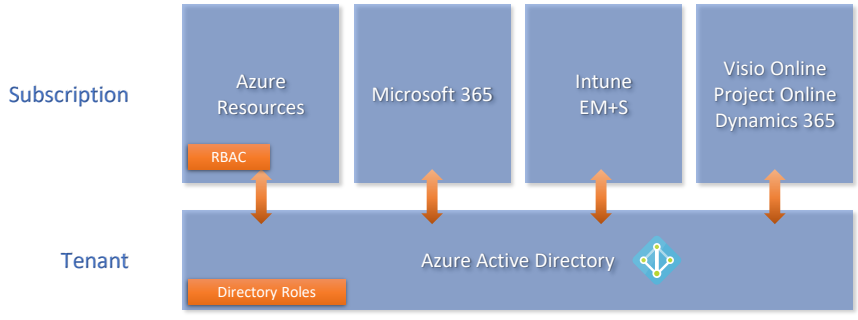
Understand - Apply - Create
DI Thomas Schleich

2

What is Azure Active Directory?

3

What is Azure Active Directory?



4

Hybrid Identites

Understand - Apply - Create
DI Thomas Schleich

5

Hybrid Identities

Today, companies using on-premises and cloud applications to be productive. Users require access to both type of these applications. To avoid to manage multiple user accounts per employee and to offer a single sign on experience to the users a synchronization of two directories (on-premises AD DS and Azure AD) is necessary. This is called hybrid identity.

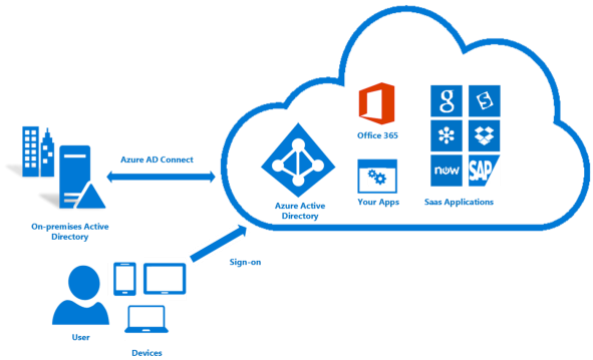
- **Three authentication methods:**
  - Password hash synchronization (PHS)
  - Pass-through authentication (PTA)
  - Federation (AD FS)

Understand - Apply - Create
DI Thomas Schleich

6

Azure AD Connect

- **Tool to get hybrid identities**
- **Features:**
  - supports PHS, PTA, Federation integration
  - Synchronization
  - Health Monitoring
- **Get tool from download center**



7

Password hash synchronization (PHS)

- **Synchronization of groups, users and their password hash to Azure AD**
- **Users are able to use their AD credentials to get access to cloud resources**
  - Azure resources
  - Microsoft 365, Dynamics 365
  - Intune
  - …
- **PHS creates 'Synchronized Identities'**
  - managed on-premises
  - authenticated in cloud

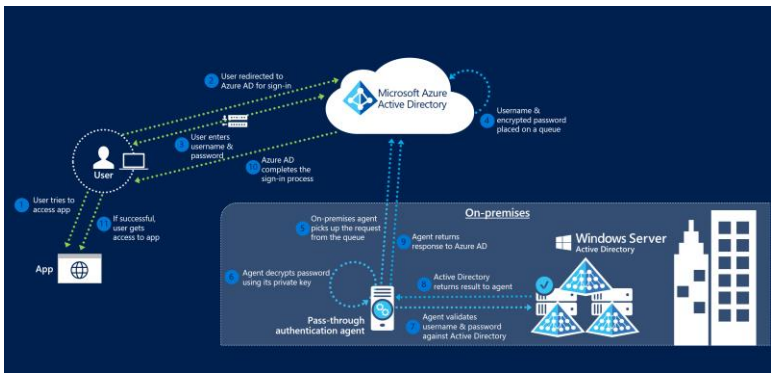
8

Pass-through Authentication

- **synchronization of users to Azure AD**
- **Password hash sync optional**
- **PTA creates 'Federated Identities'**
  - managed on-premises
  - authenticated on-premises

9

Pass-through Authentication – How it works



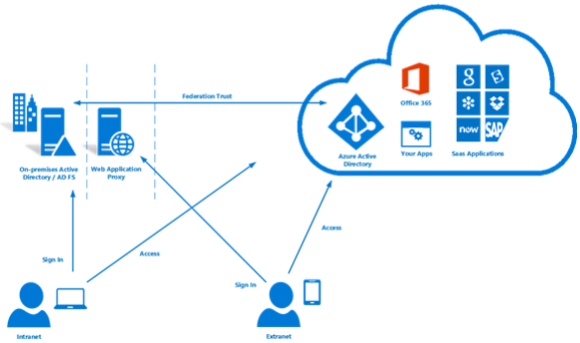
- User uses online portal for authentication and provides name and password
- PTA puts this into a queue
- PTA agent pulls the queue and performs an authentication with DC
- If successful, agent return response to Azure AD

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-how-it-works

10

Federation

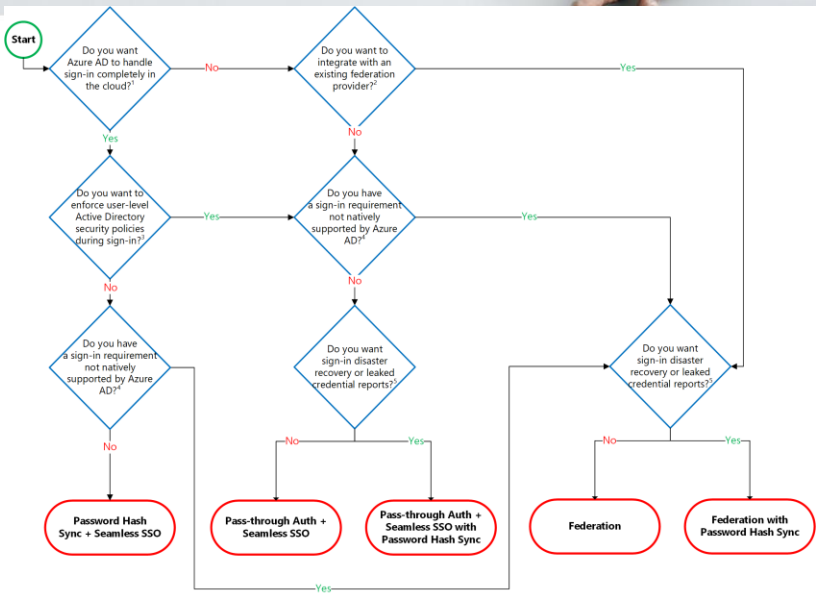
- **similar to PTA**
- **Federation services (AD FS) required**
  - AD FS
  - Web Application proxy
  - Certificate
  - …



Understand - Apply - Create
DI Thomas Schleich

11

Decision Tree

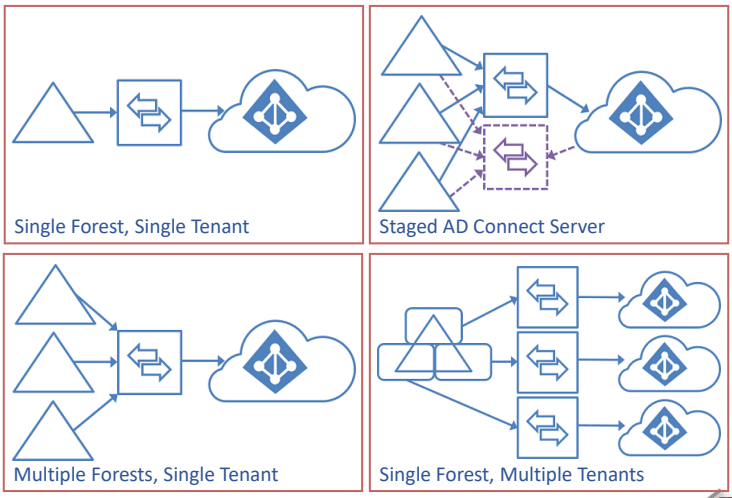


Understand - Apply - Create
DI Thomas Schleich

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

12

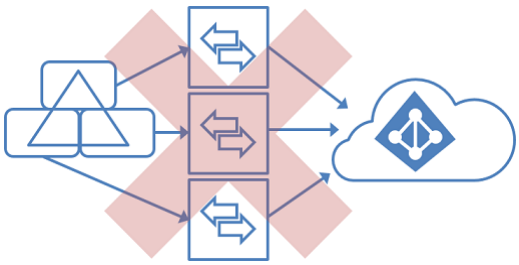
AD Connect Supported Topologies



https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies

13

AD Connect Unsupported Topology



14

AAD DS

Understand - Apply - Create
DI Thomas Schleich

15

What if …

- **… Kerberos Authentication is required for applications hosted in Azure VMs?**
- **… GPOs are required for users using Azure VMs?**
- **Solutions:**
  - Site-to-site VPN
    - Resources running in Azure use the on-premises ADDS infrastructure for Authentication
  - Replica DC in Azure Vnet
    - requires a Site-to-Site VPN and an AD site and replication configuration
  - Deploying a standalone ADDS in Azure
  - AAD DS

Understand - Apply - Create
DI Thomas Schleich

16

Azure AD Domain Services

- **Provides managed domain services**
- **Features**
  - NTLM and Kerberos authentication
  - Domain join
  - Group policy
  - LDAP read and write support (not for Azure AD resources)
  - Simplified deployment
  - High available
- **for VMs and Apps in a Vnet**
- **AAD DS replicates ID information from Azure AD to managed DCs.**
- **Azure AD Connect integration possible**

Understand - Apply - Create
DI Thomas Schleich

17