Microsoft

AZ-800 Administer Windows Server Hybrid Core Infrastructure

Agenda AZ-800

1 Deploy and manage identity infrastructure – Windows Server
2 Deploy and manage identity infrastructure – Hybrid

3 Administering Windows Server Hybrid Core Infrastructure – Windows Server
4 Administering Windows Server Hybrid Core Infrastructure – Hybrid

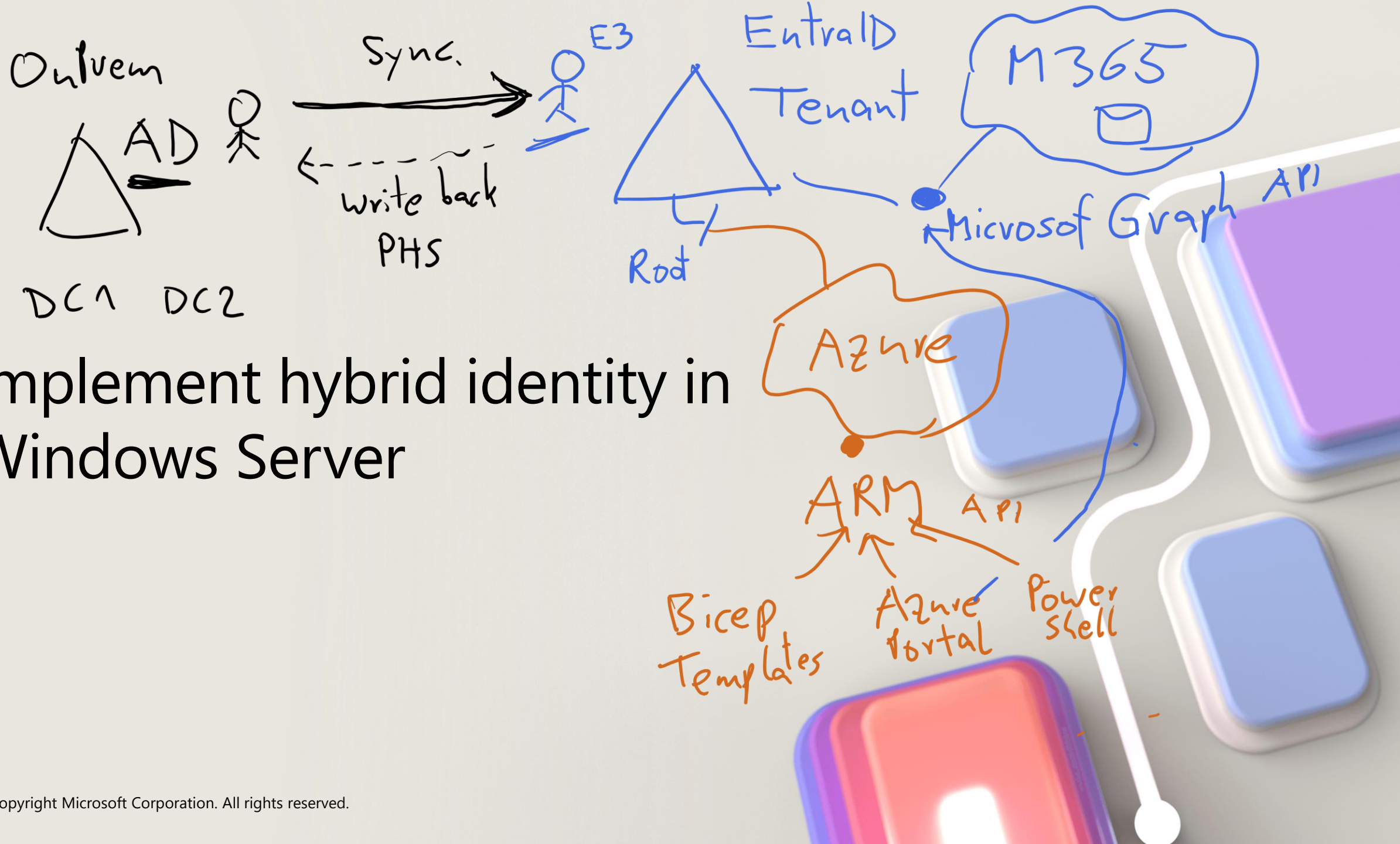
5 Manage virtualization and containers – Windows Server
6 Manage virtualization and containers – Hybrid

7 Implement and manage networking infrastructure – Windows Server
8 Implement and manage networking Infrastructure – Hybrid

9 Configure storage and file services – Windows Server
10 Configure storage and file services – Hybrid

Deploy and manage identity infrastructure (*Hybrid scenarios*)

- Implement hybrid identity in Windows Server
- Deploy and manage Azure IaaS Active Directory domain controllers in Azure
- Lab 02 – Implementing integration between AD DS and Microsoft Entra ID



Implement hybrid identity in Windows Server

Learning Objectives – Hybrid identity in Windows Server

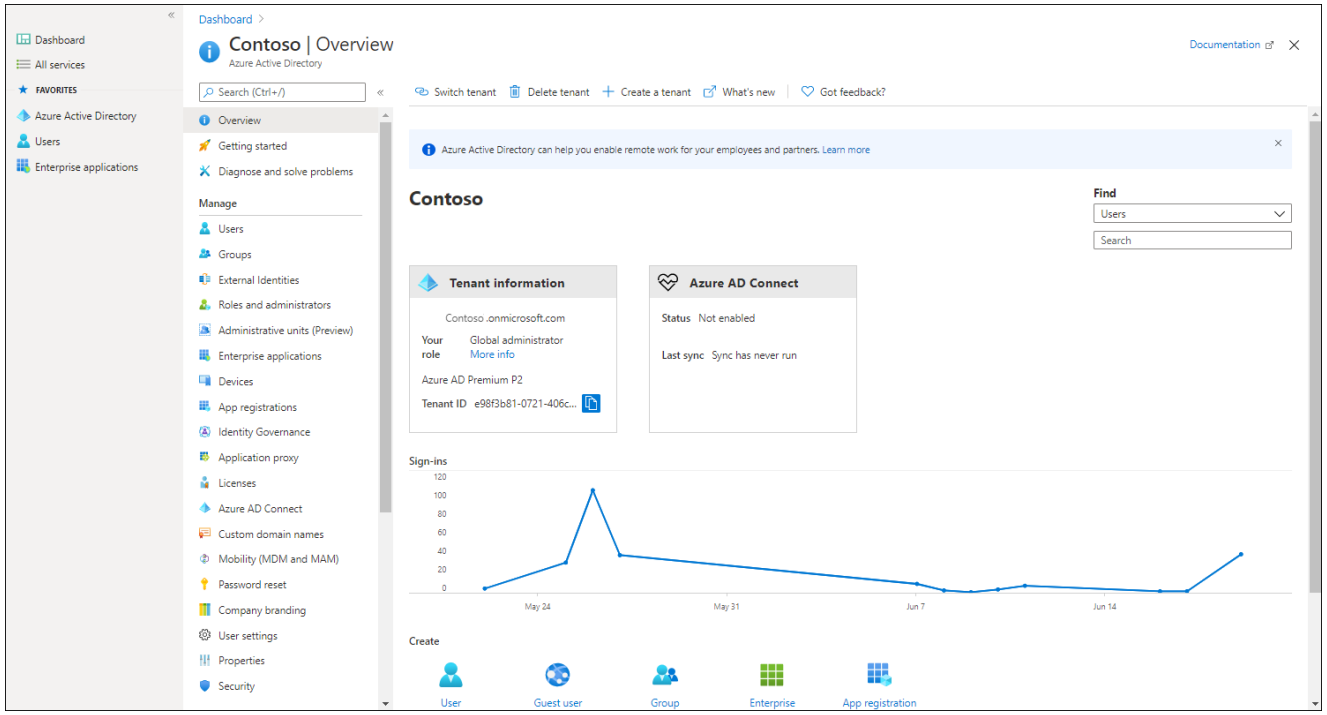
- Microsoft Entra ID integration
- Directory synchronization with Microsoft Entra Connect
- Implement Seamless Sign-on (SSO)
- Enable Microsoft Entra login for a Windows Server IaaS VM
- Microsoft Entra Domain Services
- Join a Windows Server VM to a Microsoft Entra Domain Services domain
- Learning recap

Select a Microsoft Entra integration model (1/3)

Overview of Microsoft Entra ID

Microsoft Entra ID is part of the platform as a service (PaaS) offering and operates as a Microsoft-managed directory service in the cloud.

- Cloud-native and hybrid Identity
- Users, Groups, devices management
- Open Cloud Standard Protocols
- Advanced security and protection of Identity objects, tokens and logon sessions



Select a Microsoft Entra ID integration model (2/3)

Microsoft Entra tenants

- Unlike on-premises AD DS, Microsoft Entra ID is multi-tenant by design and is implemented specifically to ensure isolation between its individual directory instances.
- It is the world's largest multi-tenant directory, hosting over a million directory services instances, with billions of authentication requests per week.

Characteristics of Entra ID vs AD DS

- No Kerberos → Oauth & OpenId
- No LDAP → Microsoft Graph, Rest API
- No Group Policy → Conditional Access / Intune
- No Forest/Domain → Federation WS-Fed
- No Virtual Machines → Redundant PAAS

Start-ADSyncSyncCycle

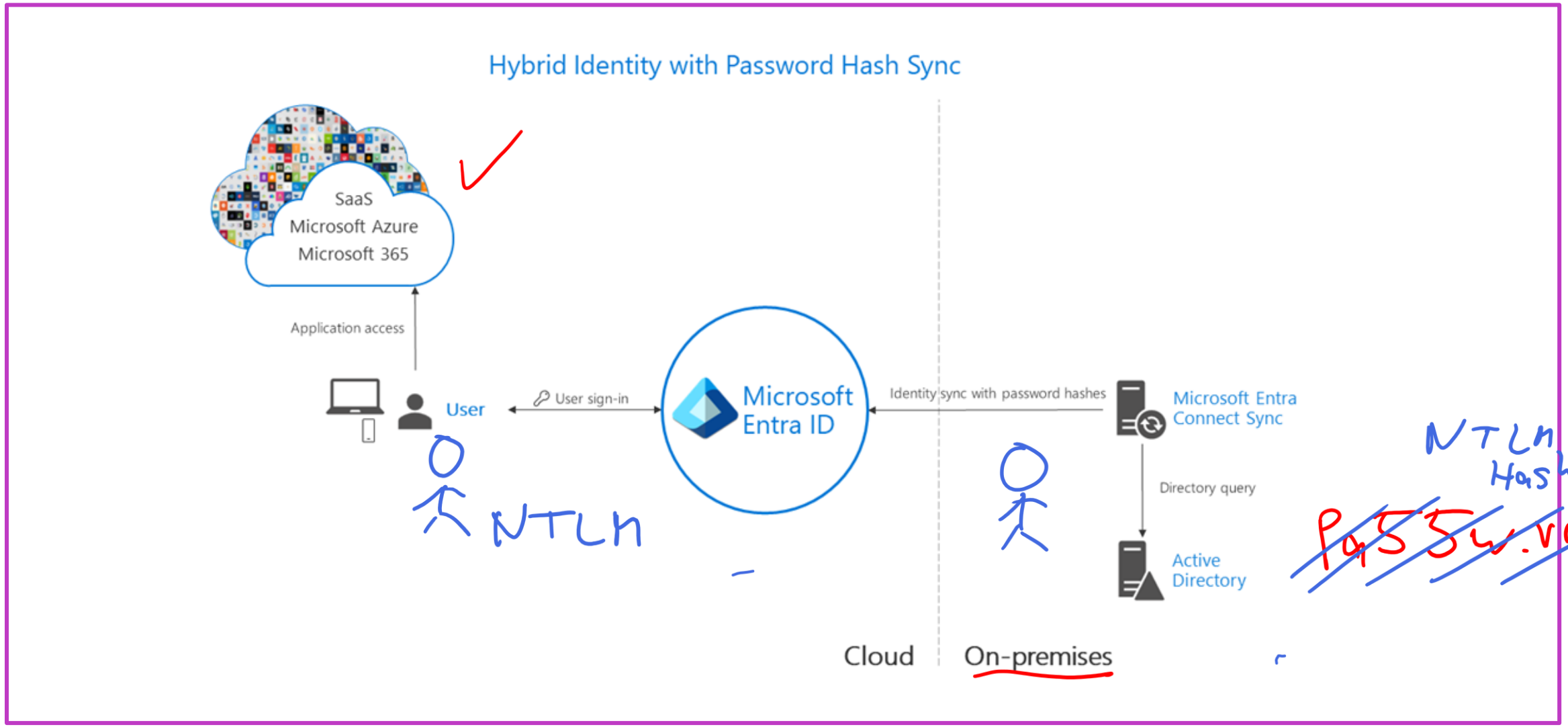
Select a Microsoft Entra ID integration model (3/3)

Microsoft Entra ID integration options

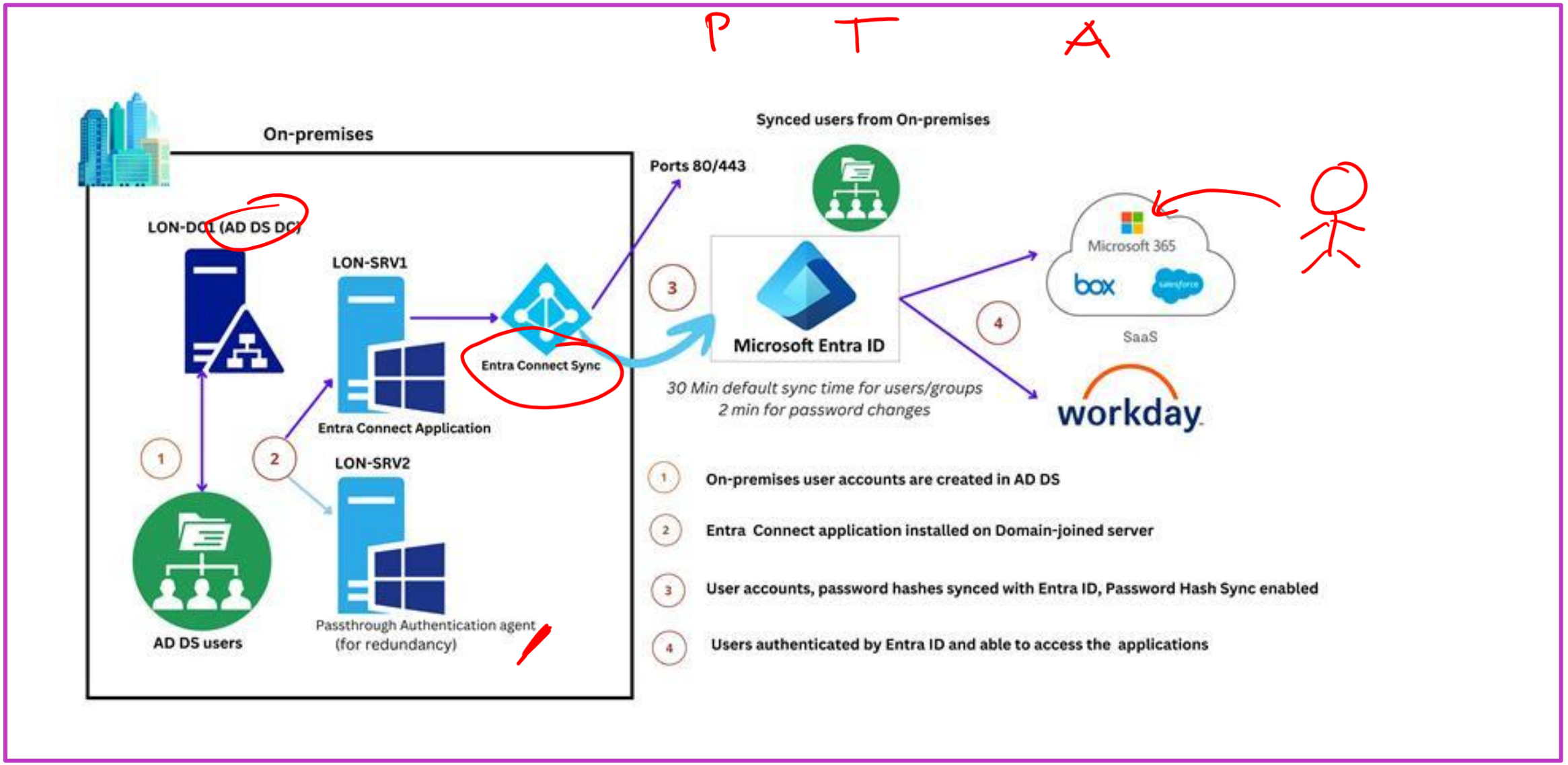
Microsoft offers cloud-scale identity and access management via Microsoft Entra ID, which provides several options for integrating AD DS with Azure.

- Extending on-premises AD DS to Azure
- Synchronizing on-premises AD DS with Microsoft Entra ID
- Synchronizing AD DS with Microsoft Entra ID, by using password hash synchronization
- Implementing SSO between on-premises AD DS and Microsoft Entra ID (AD FS, Microsoft Entra PTA)

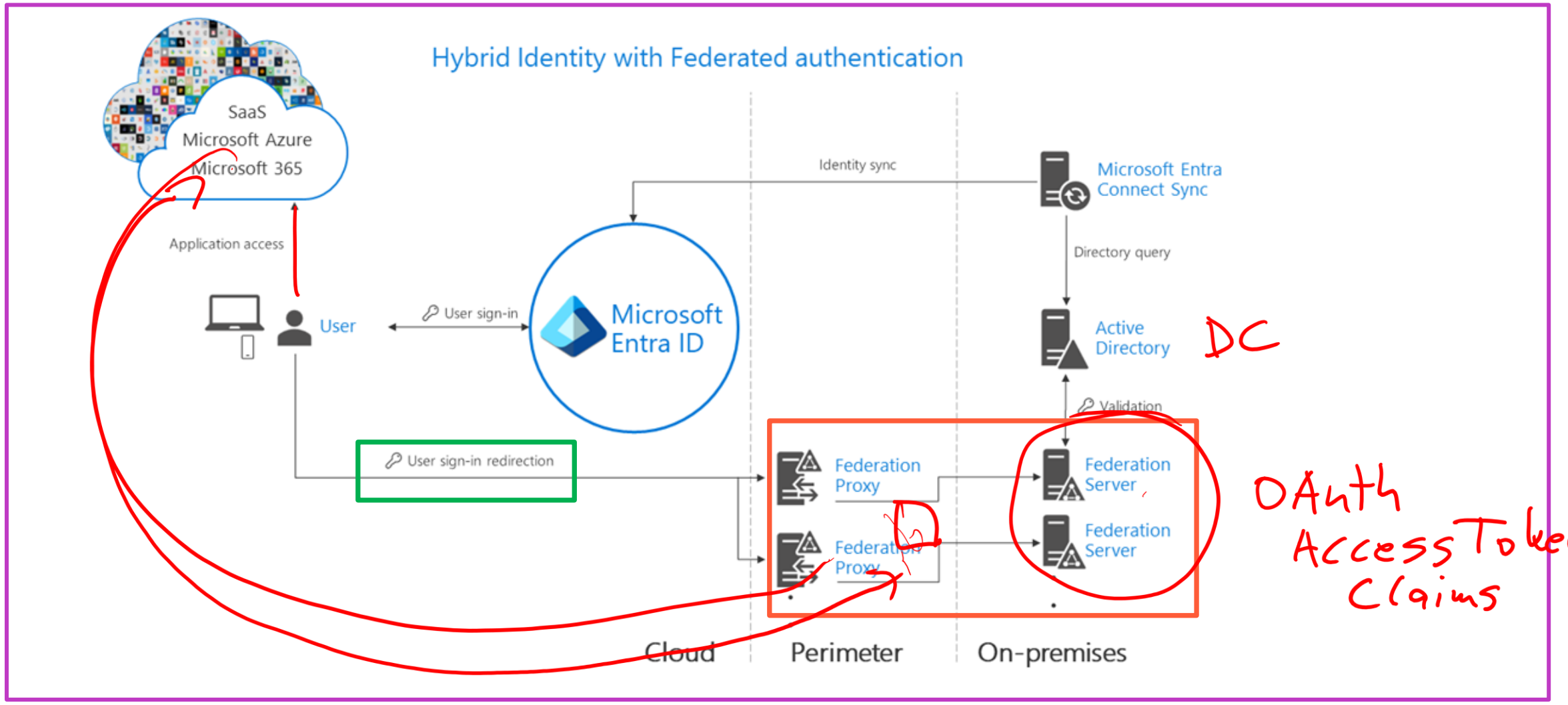
Microsoft Entra ID model – Password Hash Sync



Microsoft Entra ID model – Pass-through Authentication



Microsoft Entra ID model – Federation (ADFS)



Plan for Microsoft Entra ID integration (1/4)

Overview

- When IT staff at Contoso implements a cloud service or an application in their IT environment, they typically want to use a single identity store for their local and cloud-based applications.
- By using **directory synchronization**, they can connect their on-premises AD DS with Microsoft Entra ID.

What is directory synchronization?

- Directory synchronization enables synchronization between on-premises AD DS and Microsoft Entra ID for users, groups, and contacts.
- With Azure, the synchronization flow is one-way from local AD DS to Azure.

Plan for Microsoft Entra ID integration (2/4)

Microsoft Entra Connect

Microsoft Entra Connect is a wizard-based tool designed to enable connectivity between an on-premises AD DS identity infrastructure and Azure. Using the wizard, you can choose your topology and requirements and then the wizard deploys and configures all the required components for you.

Depending on the requirements selected, this can include:

- Microsoft Entra Sync
- Exchange Hybrid deployment
- Password change writeback
- AD FS and AD FS proxy servers or Web Application Proxy
- Microsoft Graph PowerShell module

Plan for Microsoft Entra ID integration (3/4)

Installing and configuring Microsoft Entra Connect requires the following accounts:

- An Azure account with Hybrid Identity Administrator permission in the Azure tenant
- An on-premises account with Enterprise Administrator permissions in the on-premises AD DS

In the on-premises environment, the account must have the following permissions:

- Enterprise Administrator permissions in AD DS
- Local machine administrator permissions

Plan for Microsoft Entra ID integration (4/4)

Microsoft Entra Connect – Cloud Sync

Microsoft Entra Connect Cloud Sync provides similar capabilities to Microsoft Entra Connect, but is based on a provisioning agent, instead of the Microsoft Entra Connect application

Benefits of using Microsoft Entra Connect Cloud Sync:

- Lightweight agent on-premises vs full server application
- Orchestration is managed from Microsoft Entra ID/Microsoft Online Services
- Provisioning information is stored in Microsoft Entra ID
- Cloud Sync agent also helps to sync Microsoft Entra ID to AD DS; bi-directional when configured

On-premises Active Directory – directory synchronization (1/2)

Pre-deployment checks

Pre-deployment checks should include:

- Analyzing the on-premises environment for invalid characters in AD DS object attributes, and for incorrect user principal names (UPNs)
- Performing domain email discovery and user counts
- Identifying domain-functional levels and schema extensions and identifying custom attributes in use
- Identifying proxy servers used for Microsoft Exchange or Skype for Business
- Identifying Microsoft SharePoint domains
- Evaluating client for SSO readiness
- Recording network port use, and DNS records related to Microsoft 365

On-premises Active Directory – Directory synchronization (2/2)

Active Directory health-check tools

To have directory synchronization work properly, you must ensure that on-premises Active Directory is well-prepared and error free. You can use the following AD DS health check tools can be used to identify and remediate issues.

IdFix tool

The Microsoft 365 IdFix tool enables you to identify and remediate the majority of object synchronization errors in Active Directory, including common issues such as duplicate or malformed proxyAddresses and userPrincipalName.

ADModify.NET tool

To make attribute changes to multiple objects, use PowerShell for bulk edits to attributes such as UPNs across OUs or domains.

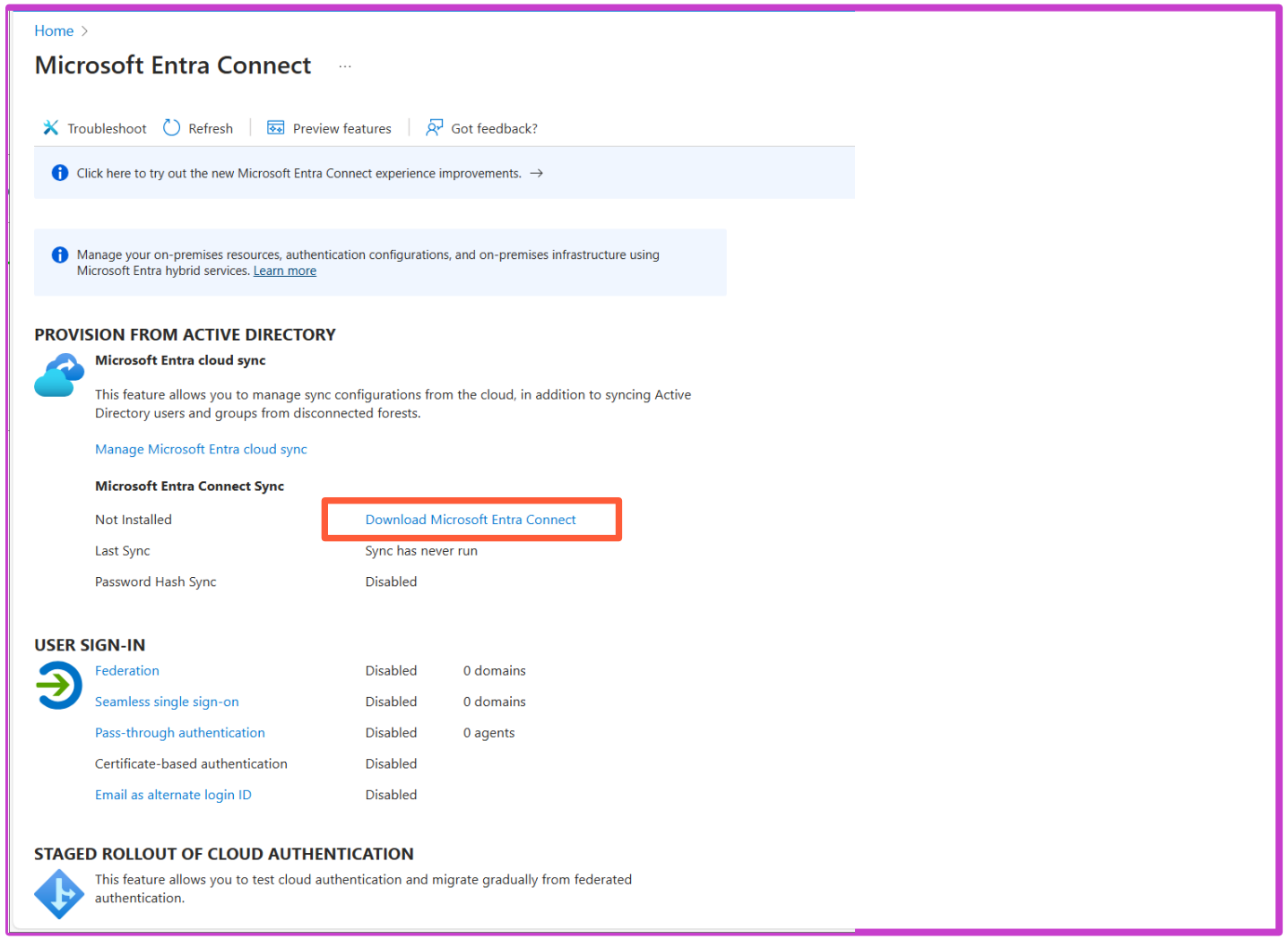
Install and configure directory synchronization with Microsoft Entra Connect (1/3)

Microsoft Entra Connect requires a domain-joined computer to host the synchronization service

Requirements

Complete the primary tasks to deploy directory synchronization using the following steps:

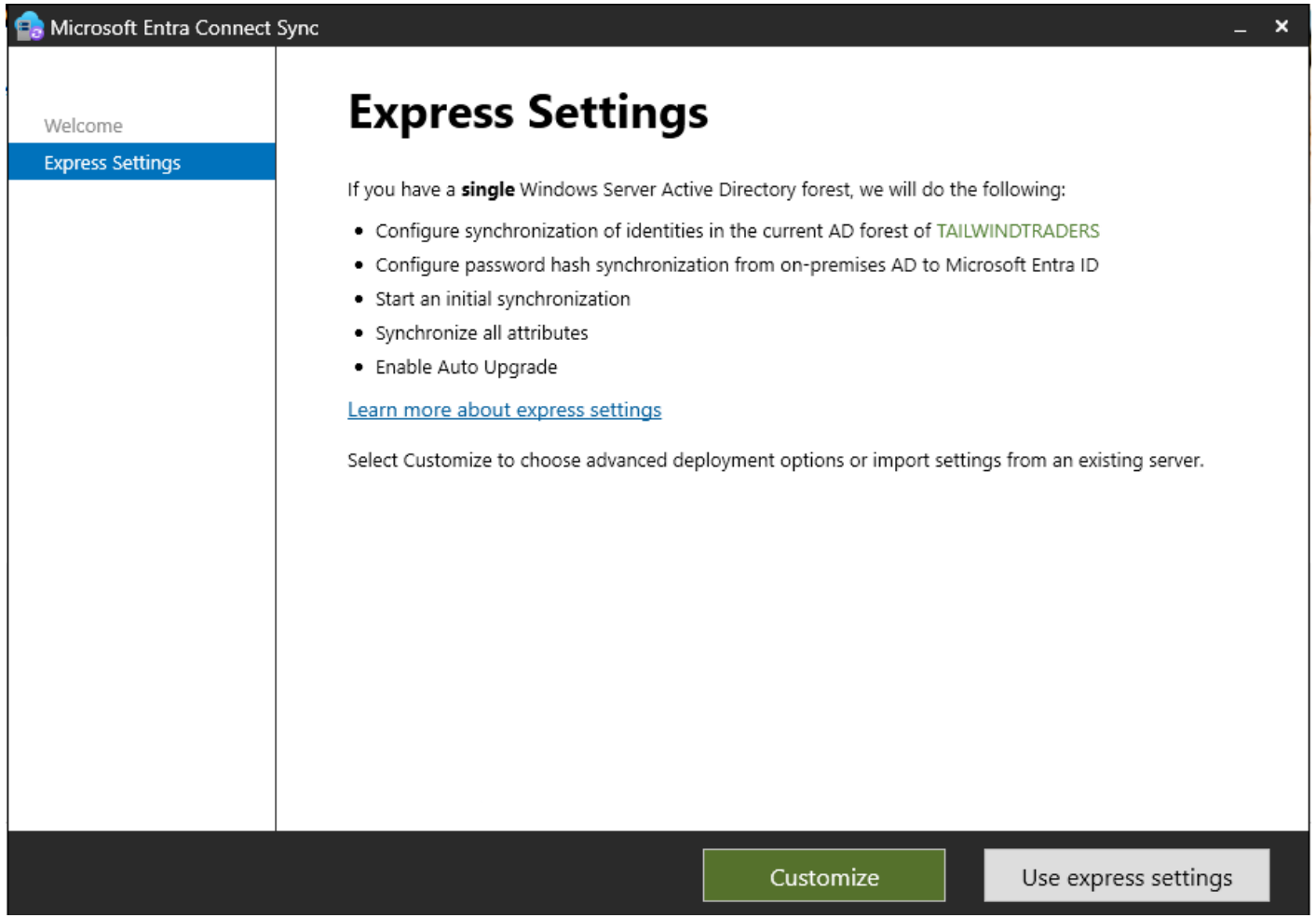
1. Add your AD DS domain into Azure, verify the domain, and then set the domain as the primary domain
2. Download and install Microsoft Entra Connect



Install and configure directory synchronization with Microsoft Entra Connect (2/3)

3. Run the **Microsoft Entra Connect Configuration Wizard**.

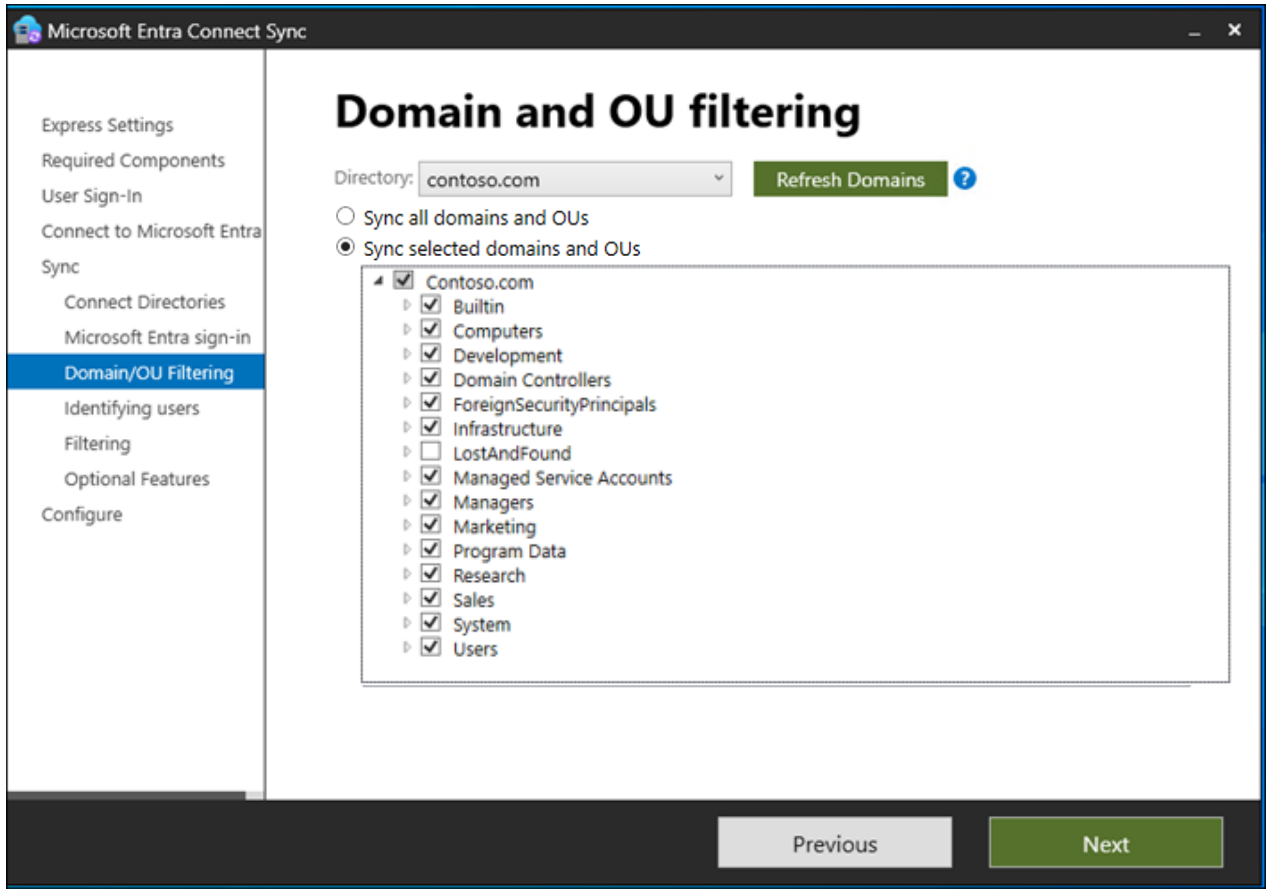
   - **Express**
     *Single AD DS Forest
     *Built-in database
     *Recommended for most scenarios
   - **Advanced**
     *Multiple AD DS Forests
     *Microsoft SQL database
     *Used for more complex scenarios



Install and configure directory synchronization with Microsoft Entra Connect (3/3)

4. Enable optional features such as password hash sync, password writeback, and Exchange hybrid deployment.
5. Run Microsoft Entra Connect, and let it configure the environment for directory synchronization.
6. Validate the synchronization results.

(Optionally, you can configure Microsoft Entra Connect to synchronize specific OUs from the on-premises AD DS environment).

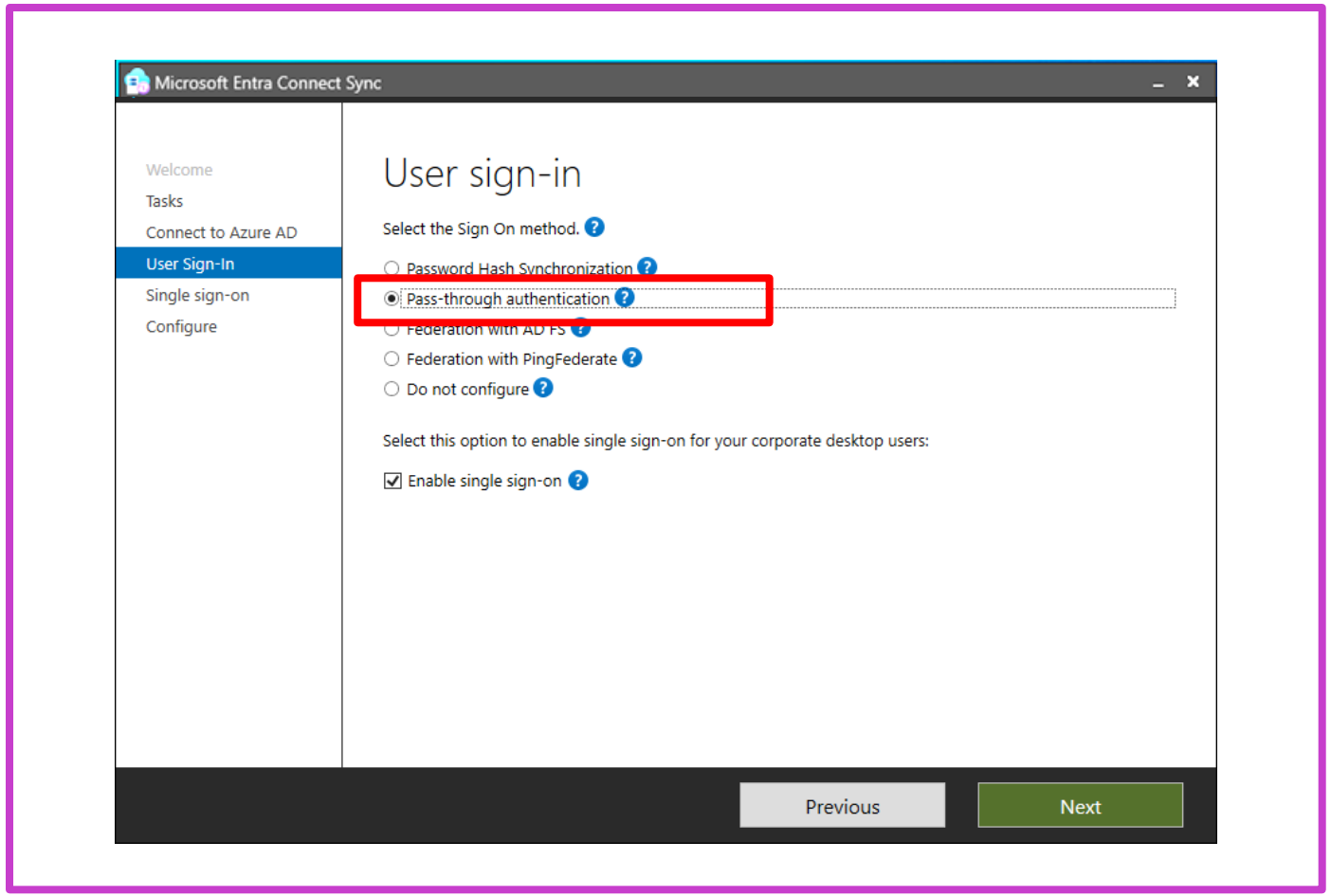


Implement seamless single sign-on (1/2)

Microsoft Entra seamless sign-on (SSO) is a technology that works with AD FS or with pass-through authentication.

Supported scenarios for pass-through authentication

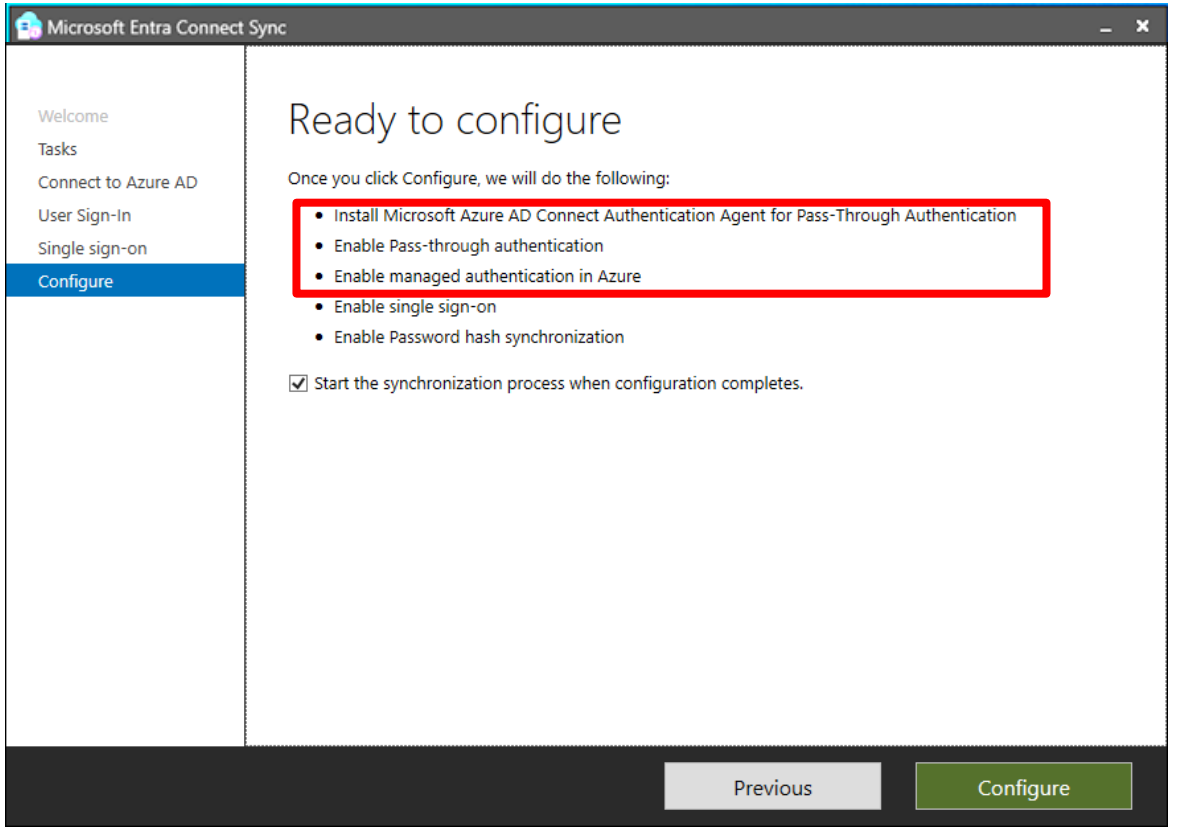
Microsoft Entra pass-through authentication helps ensure that services which rely on Microsoft Entra ID always validate passwords against an on-premises AD DS instance.



Implement seamless single sign-on (2/2)

How pass-through authentication works

- Pass-through authentication uses a component called Authentication Agent to authenticate users.
- Microsoft Entra Connect installs the Authentication Agent during configuration.
- After installation, the Authentication Agent registers itself in your Microsoft 365 tenant's Microsoft Entra ID.



Demonstration – Enable Microsoft Entra login in for Windows VM in Azure

Configure a new Windows Server IaaS virtual machine

Create a new virtual network and subnet separate from existing Microsoft Entra Domain Services subnet

Enable system-managed identity and add the Virtual Machine administrator Login role

Sign in to the new Windows Server IaaS virtual machine using the new Microsoft Entra account

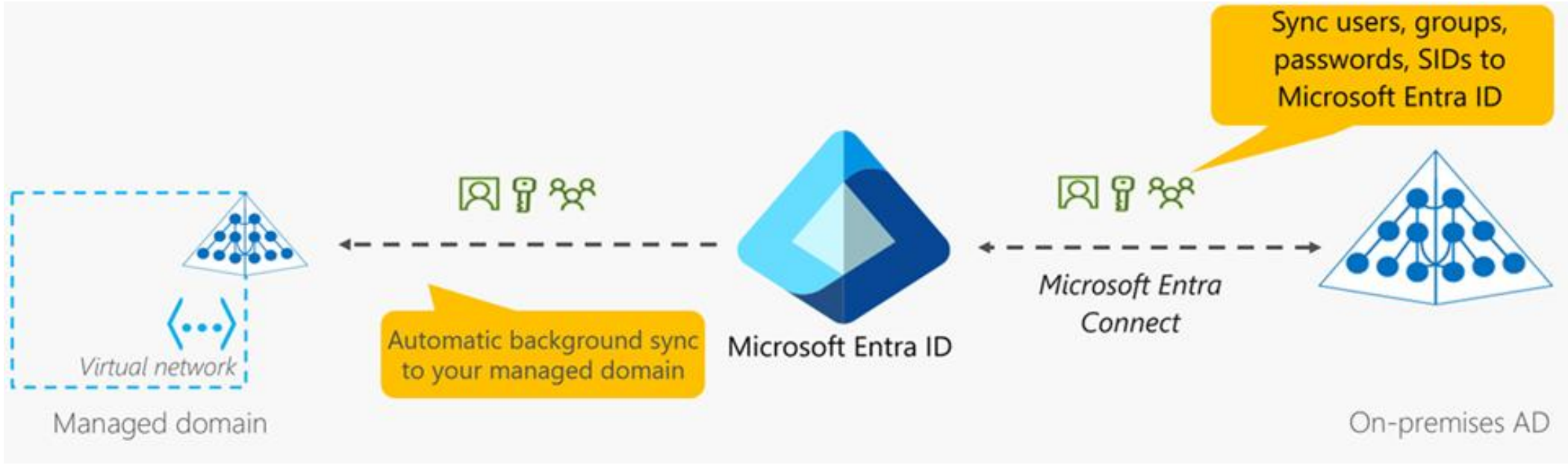
Learning recap – Microsoft Entra ID integration

Module assessment

Microsoft Learn Modules (docs.microsoft.com/Learn)

Implement hybrid identity with Windows Server

Describe Microsoft Entra Domain Services (1/2)



What is Microsoft Entra Domain Services?

Domain Services provides domain services such as Group Policy management, domain joining, and Kerberos authentication to your Microsoft Entra tenant.

These services are fully compatible with on-premises AD DS, so you can use them without deploying and managing additional domain controllers in the cloud.

Describe Microsoft Entra Domain Services (2/2)

Scenarios that utilize Domain Services

- Secure administration of Azure VMs
- On-premises applications that use LDAP bind authentication
- On-premises applications that use LDAP read to access the directory
- On-premises service or daemon application
- Remote desktop services in Azure

Considerations

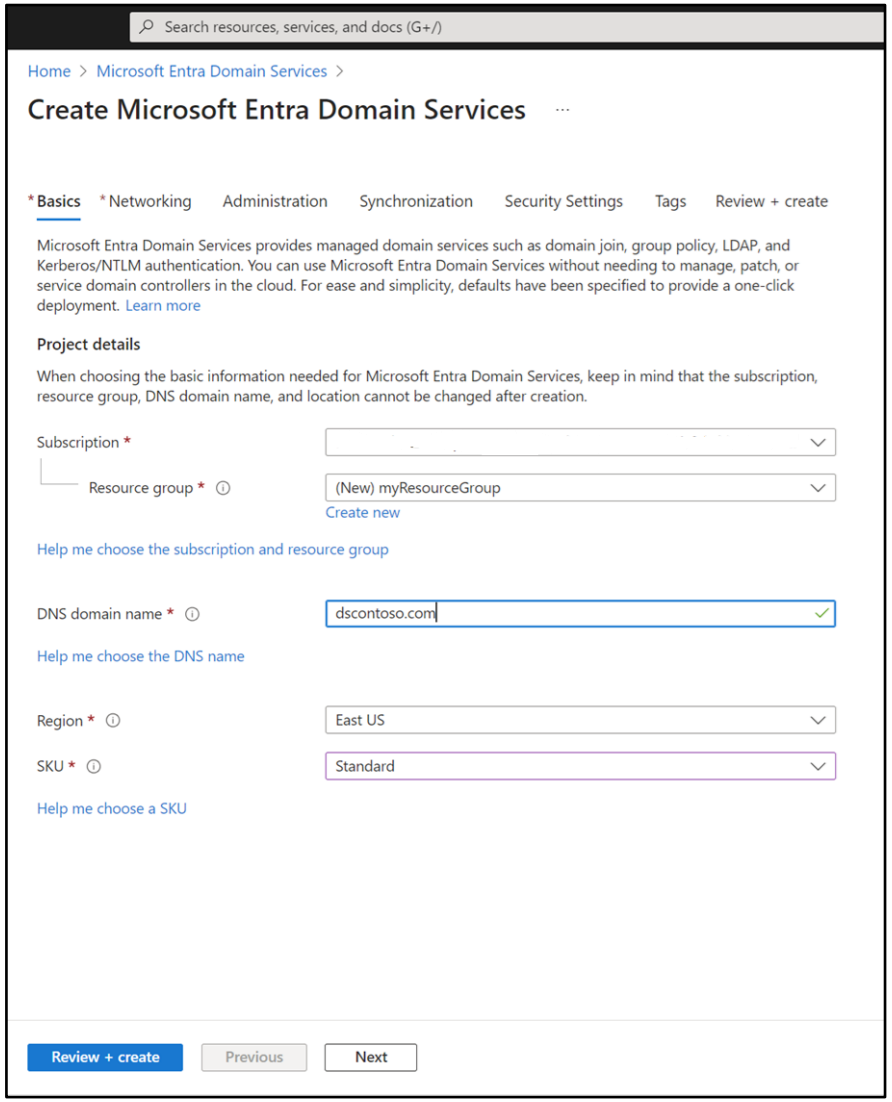
- Domain Services–managed domains use a single, flat OU structure by default.
- Domain Services uses a built-in GPO each for the users and computers containers.
- Domain Services supports the base Active Directory computer object schema.
- You can't change passwords directly in an Domain Services–managed domain.

[Implement and configure Microsoft Entra Domain Services (1/2)

Implement Domain Services

To implement, configure, and use Domain Services you must:

- Have a Microsoft Entra tenant created on an Entra ID subscription
- Have password hash synchronization deployed with Microsoft Entra Connect
- Select the DNS domain name that you will use for this service
- Select the domain that you will synchronize with your on-premises environment

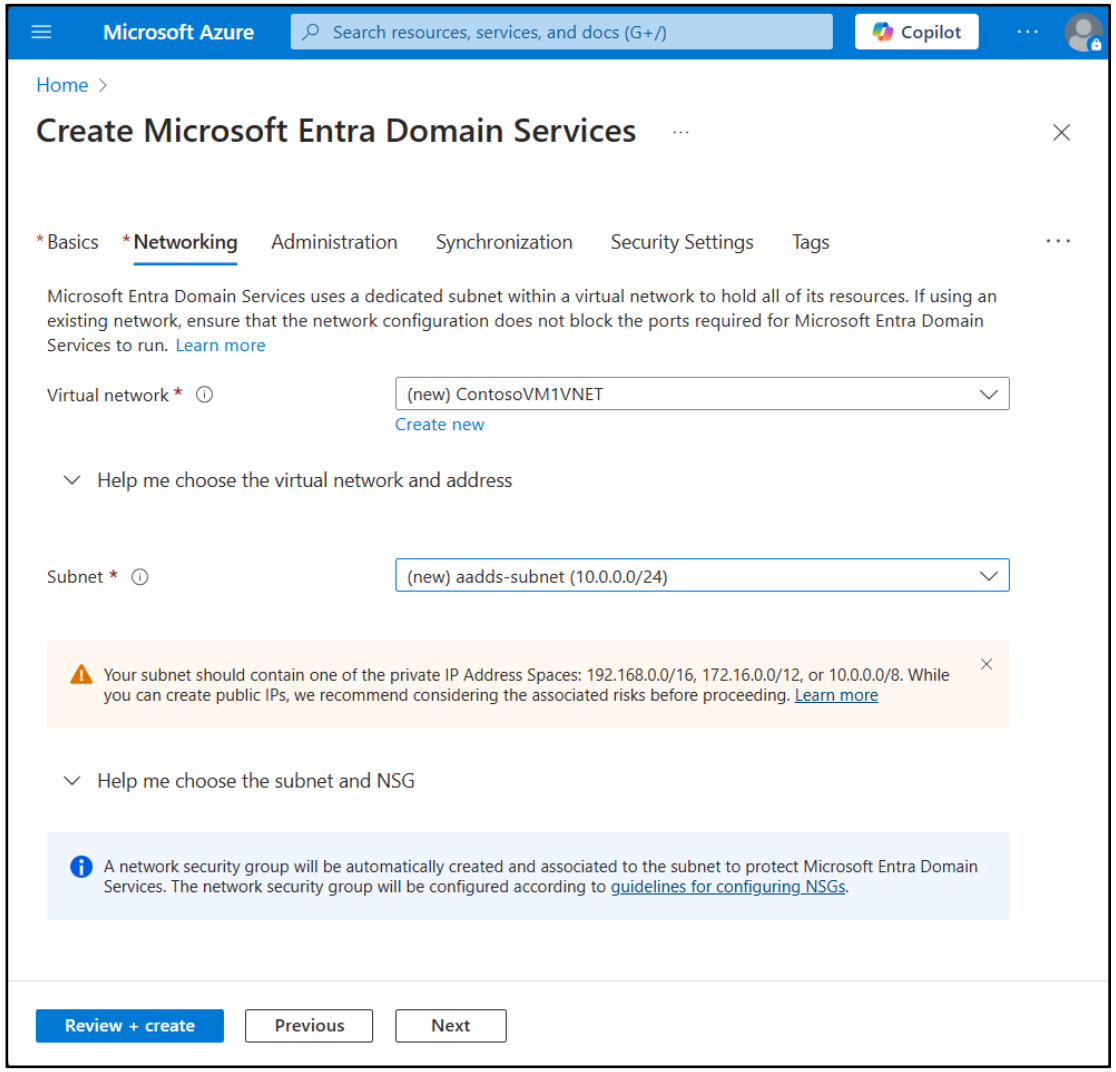


[Implement and configure Microsoft Entra Domain Services (2/2)

You must also select a VNet to which you will connect this service. Because Domain Services provides functionalities for on-premises resources, you must have a VNet between your local and Azure environments.

During provisioning, Domain Services creates two enterprise applications in your Microsoft Entra tenant:

- Domain Controller Services
- AzureActiveDirectoryDomainControllerServices



Demonstration – Create and configure a Microsoft Entra Domain Services instance

Deploy a Domain Services instance from the Azure portal	Configure a virtual network	Configure the virtual network DNS servers	Force password resets for Entra ID users

Manage Windows Server in a Microsoft Entra Domain Services environment (1/2)

Overview

Administrator can perform:

- Configure the built-in GPO for the containers AADDC Computers and AADDC Users, in the managed domain
- Administer DNS on the managed domain
- Create and administer custom OUs on the managed domain
- Gain administrative access to computers joined to the managed domain

Cannot perform:

- Extend the schema of the managed domain
- Connect to domain controllers for the managed domain using Remote Desktop
- Add domain controllers to the managed domain
- Employ Domain Administrator or Enterprise Administrator privileges for the managed domain

Manage Windows Server in a Microsoft Entra Domain Services environment (2/2)

Enable user accounts for Domain Services

- To authenticate users on the managed domain, Domain Services needs password hashes in a format that's suitable for NTLM and Kerberos authentication.
- Once appropriately configured, the usable password hashes are stored in the Microsoft Entra Domain Services managed domain.
- Synchronized credential information in Microsoft Entra ID can't be re-used if you later create a Domain Services–managed domain.
- The steps to generate and store these password hashes are different for cloud-only user accounts created in Microsoft Entra ID versus user accounts that are synchronized from your on-premises directory using Microsoft Entra Connect.
- For cloud-only user accounts, users must change their passwords before they can use Domain Services.

Demonstration – Join a VM to a managed domain

Create a Windows Server virtual machine

Select virtual network created in prior demonstration

Establish a connection to the VM

Configure the VM to connect to a Microsoft Entra Domain Services domain

Optional Demonstration – Join a Linux-OS VM to a managed domain

Create and connect to an Ubuntu Linux VM	Configure the hosts file	Install required packages and configure Network Time Protocol (NTP)	Join the VM to the managed domain

Module assessment– Microsoft Entra Domain Services

Module assessment

Microsoft Learn Modules (docs.microsoft.com/Learn)

Implement hybrid identity with Windows Server

Deploy and Manage Azure IaaS Active Directory Domain Controllers in Azure

Learning Objectives – Deploy and manage Azure IaaS AD domain controllers in Azure

- Implement directory and identity services by using Active Directory Domain Services (AD DS) in Azure
- Deploy and configure AD DS domain controllers in Azure VMs
- Install a replica AD DS domain controller in an Azure VM
- Install a new AD DS forest on an Azure VNet
- Learning recap

Select an option to implement directory and identity services using Active Directory Domain Services in Azure

Overview

The process of deploying an Active Directory domain controller on an Azure VM is similar to the process of deploying a domain controller in an on-premises environment. One primary difference is that when you deploy a domain controller in Azure, you must place the Active Directory database on the data disk of an Azure VM to avoid potential database corruption.

Deploy AD DS only on an Azure VM:

This scenario involves creating a VNet but doesn't require cross-premises connectivity. Typically, this deployment starts with a new forest and all the domain controllers run only on Azure VMs.

Deploy AD DS in both an on-premises infrastructure and on an Azure VM:

This scenario is common for apps that are LDAP–aware and that support Windows-integrated authentication.

Deploy and configure AD DS domain controllers in Azure VMs

Deployment considerations

- Network recommendations
- Inter-site connectivity
- Active Directory sites
- Trust relationship
  - Unidirectional (one-way)
  - Bidirectional (two-way)
- Read-only domain controllers (RODCs)
- Flexible single master operations (FSMO) roles and global catalog placement
- Availability
- Back up and restore
- Management
- Monitoring

Exercise: Install a replica Active Directory domain controller in an Azure VM

Task 1: Create an Azure virtual network with a site-to-site VPN

Task 2: Create a VM and assign an IP address.

Task 3: Install and configure DNS and AD DS server roles

Exercise: Install a new Active Directory forest on an Azure VNet

Task 1: Create an Azure VNet

Task 2: Create the VMs to run both the domain controller and DNS server roles.

Task 3: Install the AD DS and DNS server roles

Learning recap – Deploy and manage Azure IaaS Active Directory domain controllers in Azure

Module assessment

Microsoft Learn Modules (docs.microsoft.com/Learn)

Deploy and manage Azure IaaS Active Directory domain controllers in Azure

Lab 02 – Implementing integration between AD DS and Microsoft Entra ID

Lab 02: Implementing integration between AD DS and Microsoft Entra ID

Lab scenario

As part of the AD DS administration team at Contoso, you have been tasked with integrating on-premises AD DS and Microsoft Entra ID to address business concerns over management of multiple user accounts. You need to implement Microsoft Entra Password Protection for Active Directory and Self-Service Password Reset with password writeback. You also need to implement pass-through authentication between on-premises AD DS and Microsoft Entra ID.

Objectives

- Prepare Microsoft Entra ID for integration with on-premises AD DS
- Prepare on-premises AD DS for integration with Microsoft Entra ID
- Install and configure Microsoft Entra Connect
- Verify integration between AD DS and Microsoft Entra ID by testing the synchronization process
- Implement Microsoft Entra Password Protection for Active Directory and SSPR with password writeback

End of presentation