

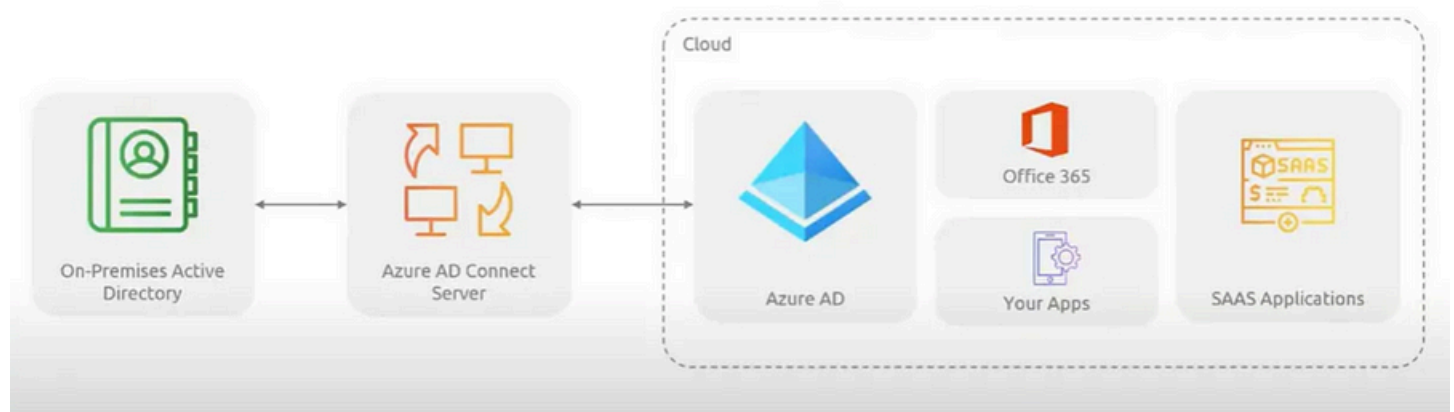
Azure AD Connect: Hybrid Identity Management

Syncing On-Prem Active Directory with Microsoft Entra ID

This guide provides a comprehensive overview of setting up a hybrid identity management system using Azure AD Connect. It facilitates the synchronization of on-premises Active Directory (AD) with Microsoft Entra ID, ensuring a seamless transition to a cloud environment.

Understanding the Components

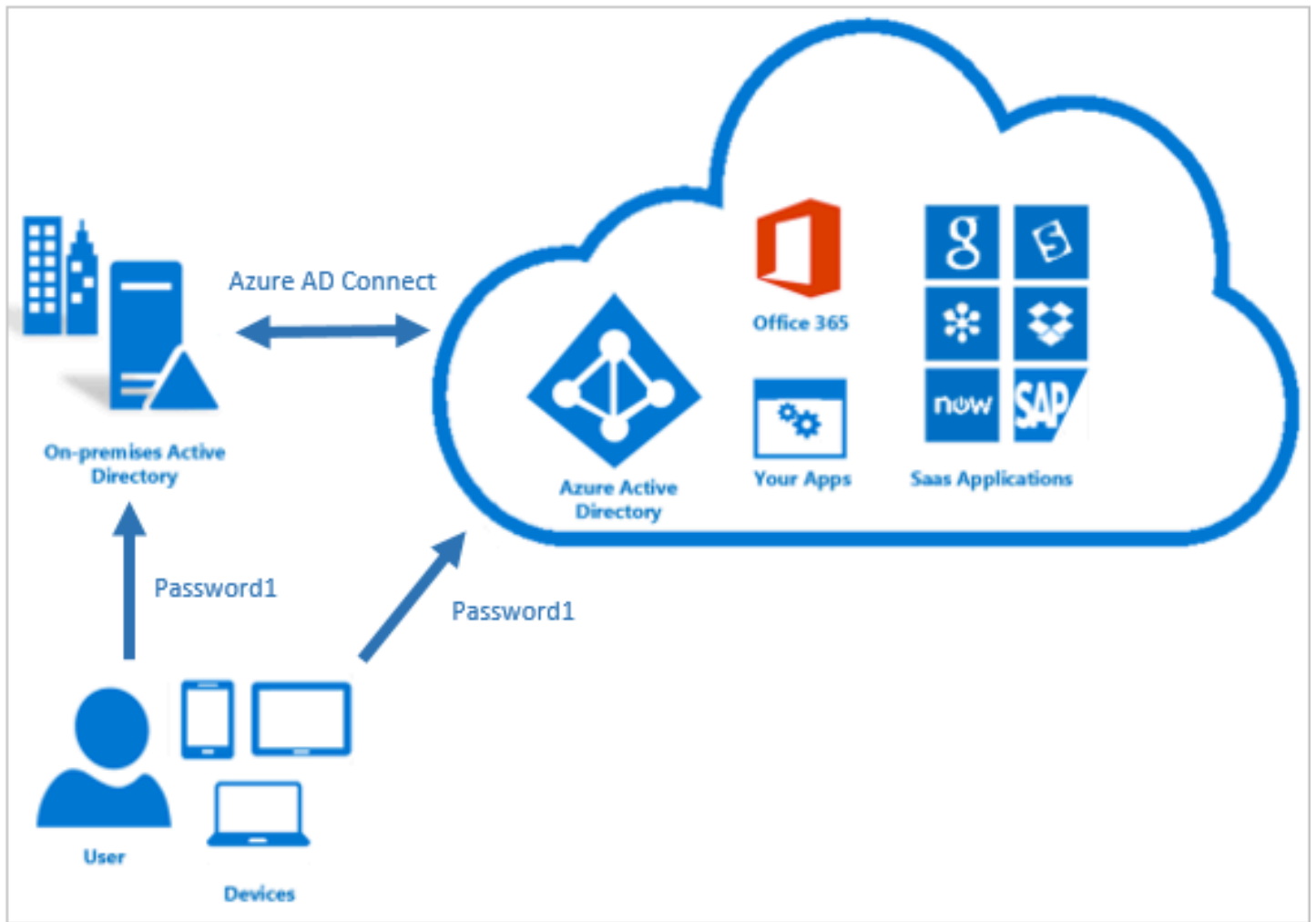
Before we delve into the implementation, it's crucial to understand the main players in our hybrid setup:



On-premises Active Directory (AD): This is our traditional AD Domain Services running on a Windows Server, often referred to as “on-prem AD”

- **Microsoft Entra ID:** Formerly known as Azure AD, this is our cloud-based identity and access management service
- **Azure AD Connect:** The vital tool that synchronizes identities between our on-premises AD and Entra ID

Interestingly, Entra ID can also serve as an identity provider for your on-premises environment, showcasing its versatility.



The Problem We're Solving

Example: Our client is transitioning from an on-premises Microsoft AD to a cloud environment with Microsoft Entra ID. The challenge lies in migrating identities without disrupting operations or creating redundant user accounts. Our solution? Implement a hybrid identity management system that synchronizes existing on-premises identities with Entra ID.

The Solution: Azure AD Connect

Azure AD Connect is our go-to tool for this project. It consists of two main components:

1. **Azure AD Connect Sync component: Installed in the on-premises environment**
2. **Azure AD Connect Sync service: Runs in Azure AD**

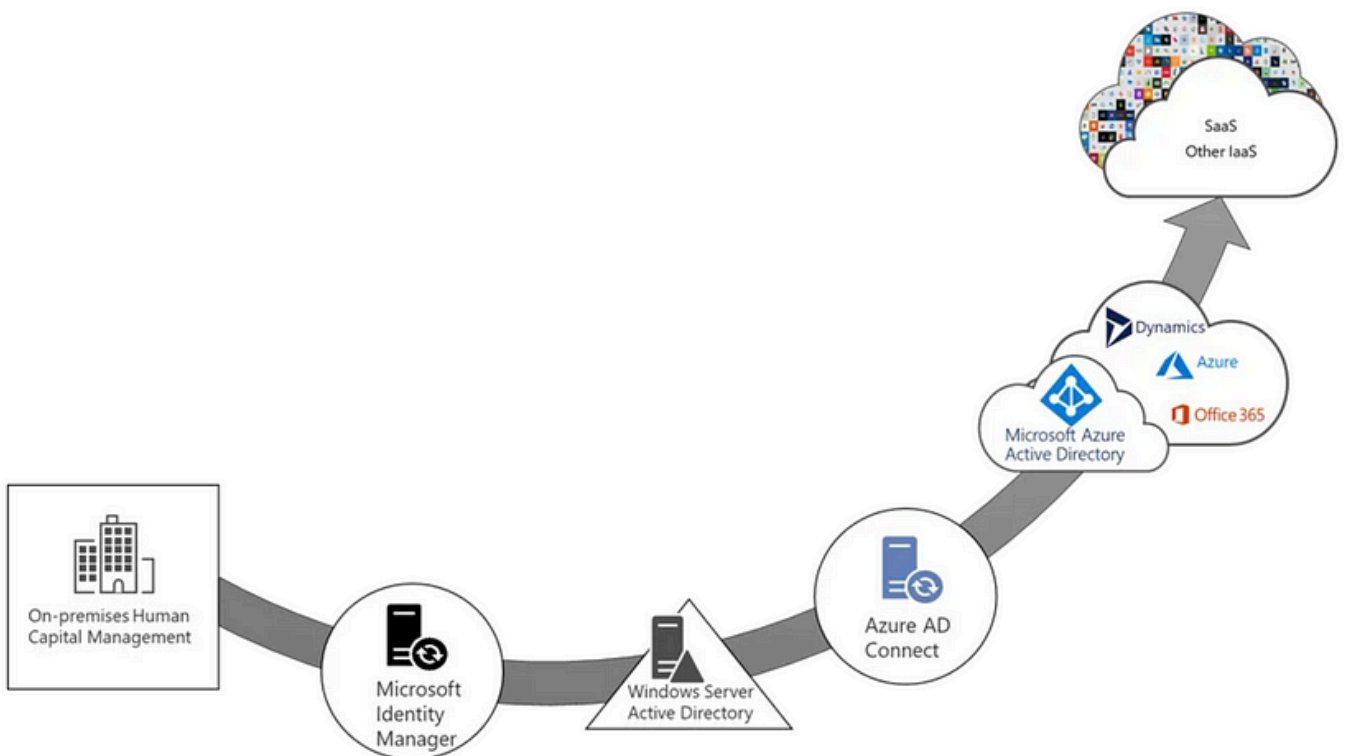
This setup allows users to access both on-premises and cloud resources using a single set of credentials, significantly simplifying identity management and enhancing overall security.



Domain controller



Domain Server VM

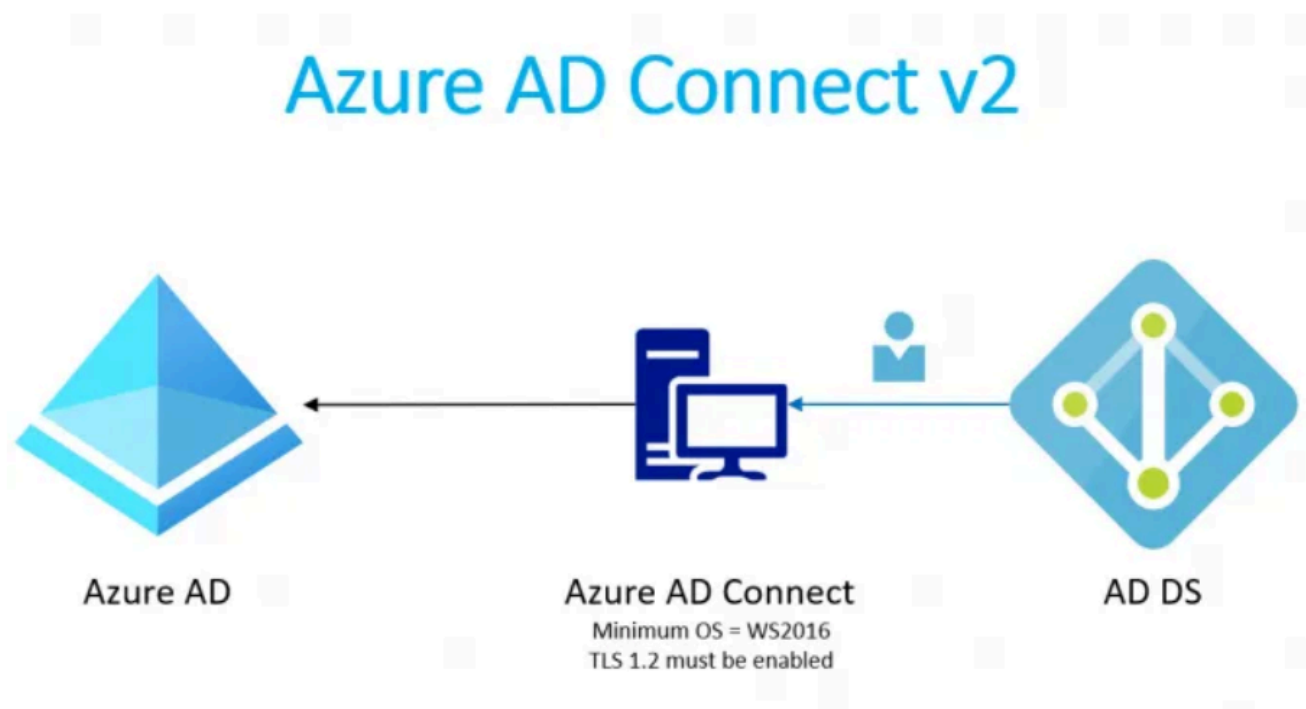


Prerequisites and Implementation Steps

Before diving into the implementation, we ensured the following prerequisites were in place:

- An Azure AD tenant
- A verified domain in Azure AD
- Windows Server 2012 Standard or better for the Azure AD Connect sync component
- SQL Server database for storing identity data (Azure AD Connect installs SQL Server 2012 Express LocalDB by default)
- Azure AD Global Administrator account
- Enterprise Administrator account for on-premises Active Directory

We also ensured that the Azure AD Connect server had proper DNS resolution for both intranet and internet, allowing it to resolve names for both on-premises AD and Azure AD endpoints.



Key Considerations

Throughout the implementation, we kept these important factors in mind:

- We used the IdFix tool to identify and resolve any errors, duplicates, or formatting issues in the on-premises directory before synchronization
- The Azure AD Connect sync component was installed on a domain-joined server separate from the domain controller for best practices

- We ensured all necessary accounts were properly set up and had the required permissions before beginning the synchronization process

Cloud Sync — How it works

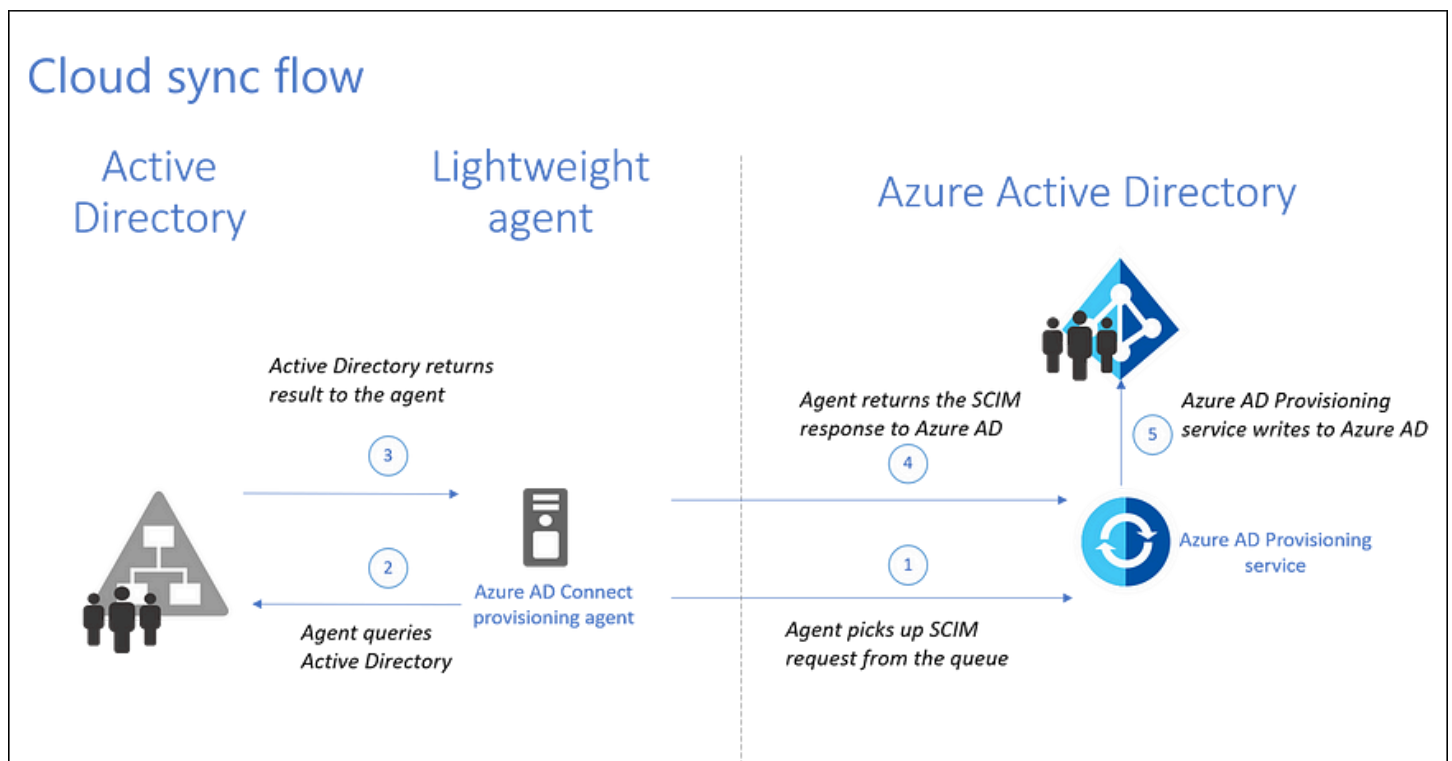
Cloud sync is built on top of the Azure AD services and has 2 key components:

Provisioning agent: The Azure AD Connect cloud provisioning agent is the same agent as Workday inbound and built on the same server-side technology as app proxy and Pass Through Authentication. It requires an outbound connection only and agents are auto-updated.

Provisioning service: Same provisioning service as outbound provisioning and Workday inbound provisioning which uses a scheduler-based model. In case of cloud sync, the changes are provisioned every 2 mins.

Ref: <https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/concept-how-it-works>


Synchronization flow



Step 1: Setting Up On-Premises Active Directory

1. **Create a virtual machine (VM) for your on-premises AD: WindowsServer22 , And specific Size**

Create a virtual machine ...

 Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.



Help me create a low cost VM



Help me create a VM optimized for high availability



Help me choose the right VM size for my work


VM architecture ⓘ

- ☐ Arm64
☒ x64

Run with Azure Spot discount ⓘ

☐

Size * ⓘ

Standard_D2s_v3 - 2 vcpus, 8 GiB memory (₹6,376.87/month) 

[See all sizes](#)

Enable Hibernation ⓘ

☐

 Hibernation does not currently support Trusted launch and Confidential virtual machines for Linux images. [Learn more](#) 

Administrator account

Authentication type ⓘ

- ☐ SSH public key
☒ Password

Username * ⓘ

jameel 

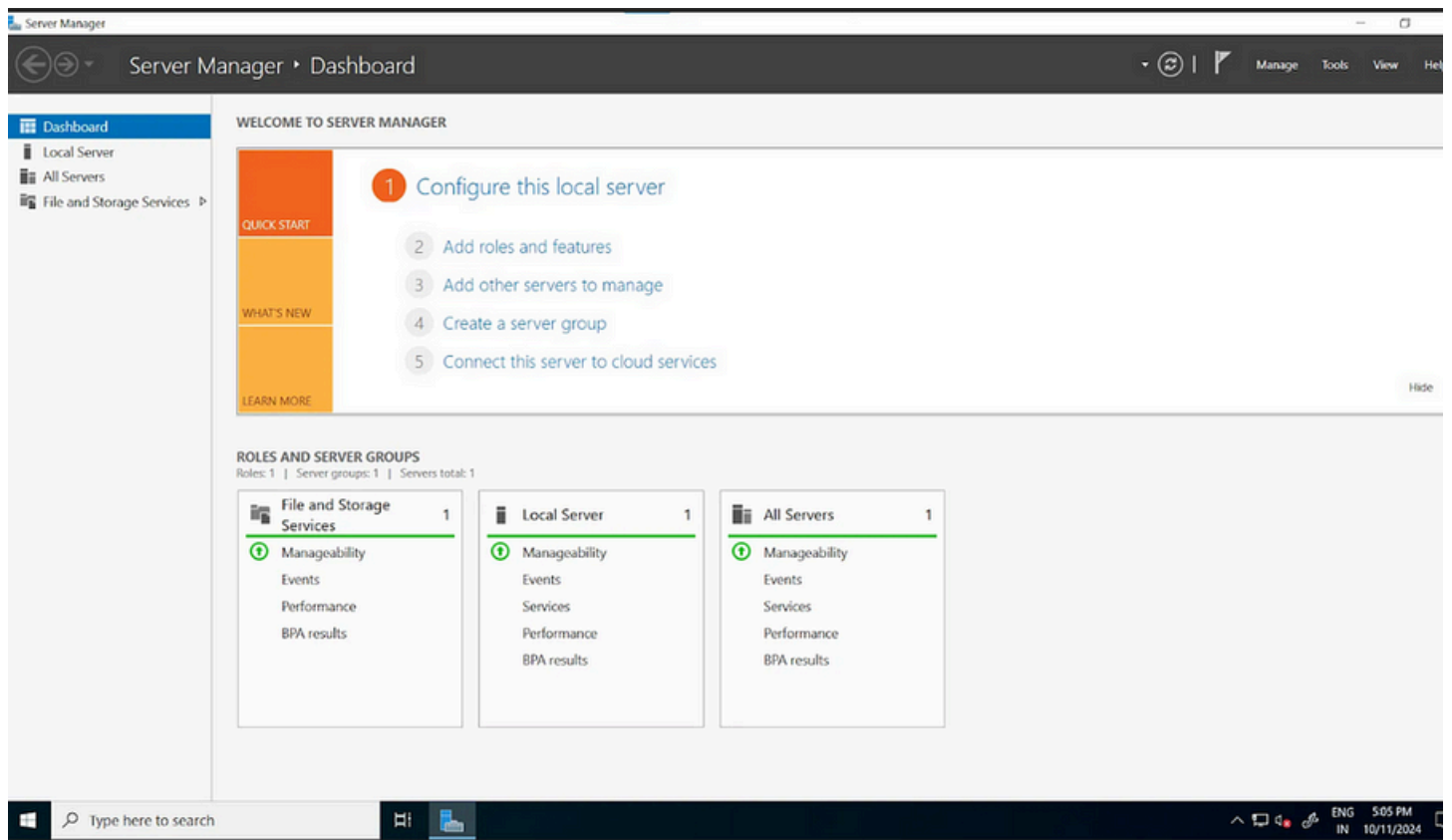
Password *

..... 

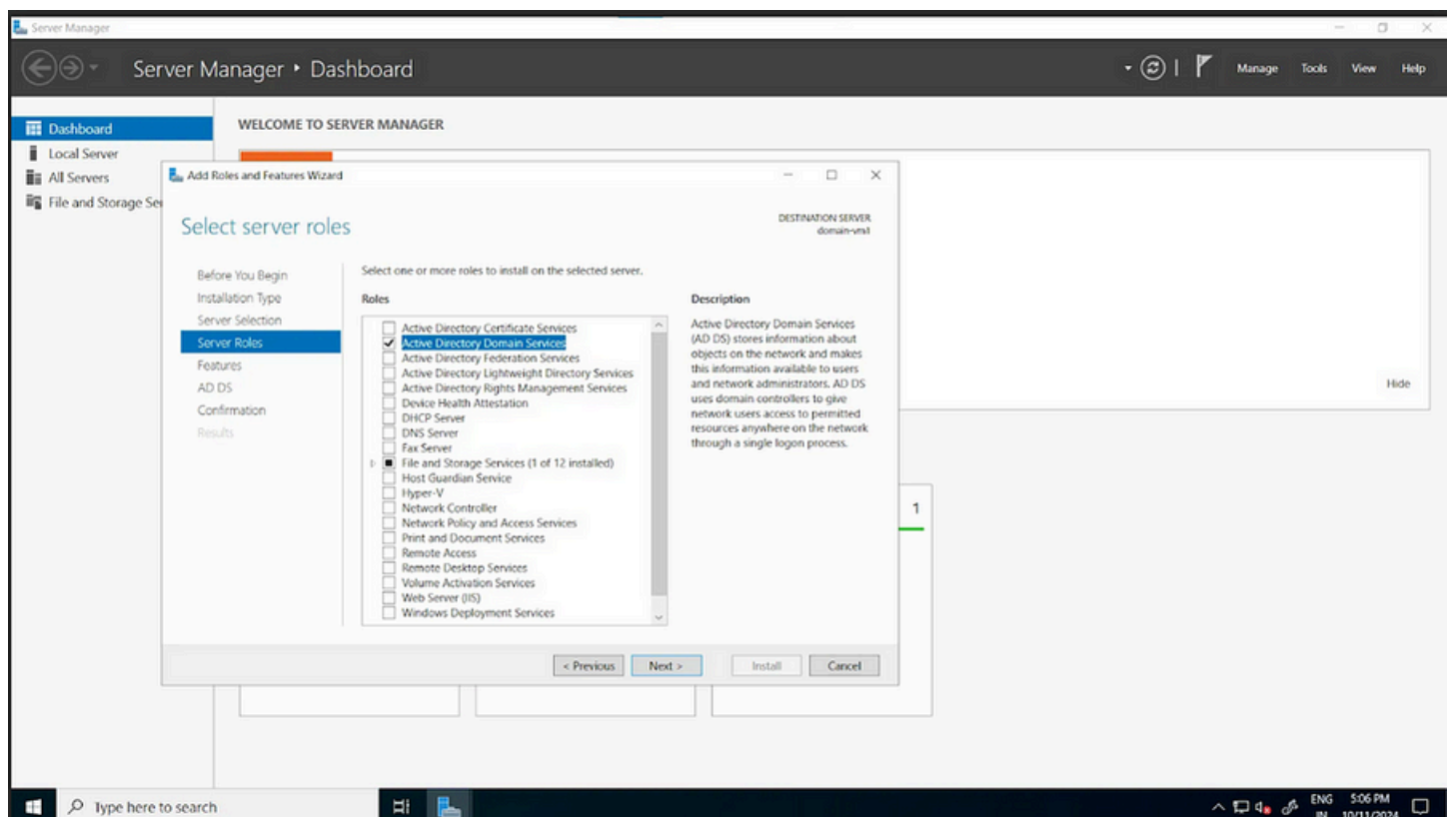
Confirm password *

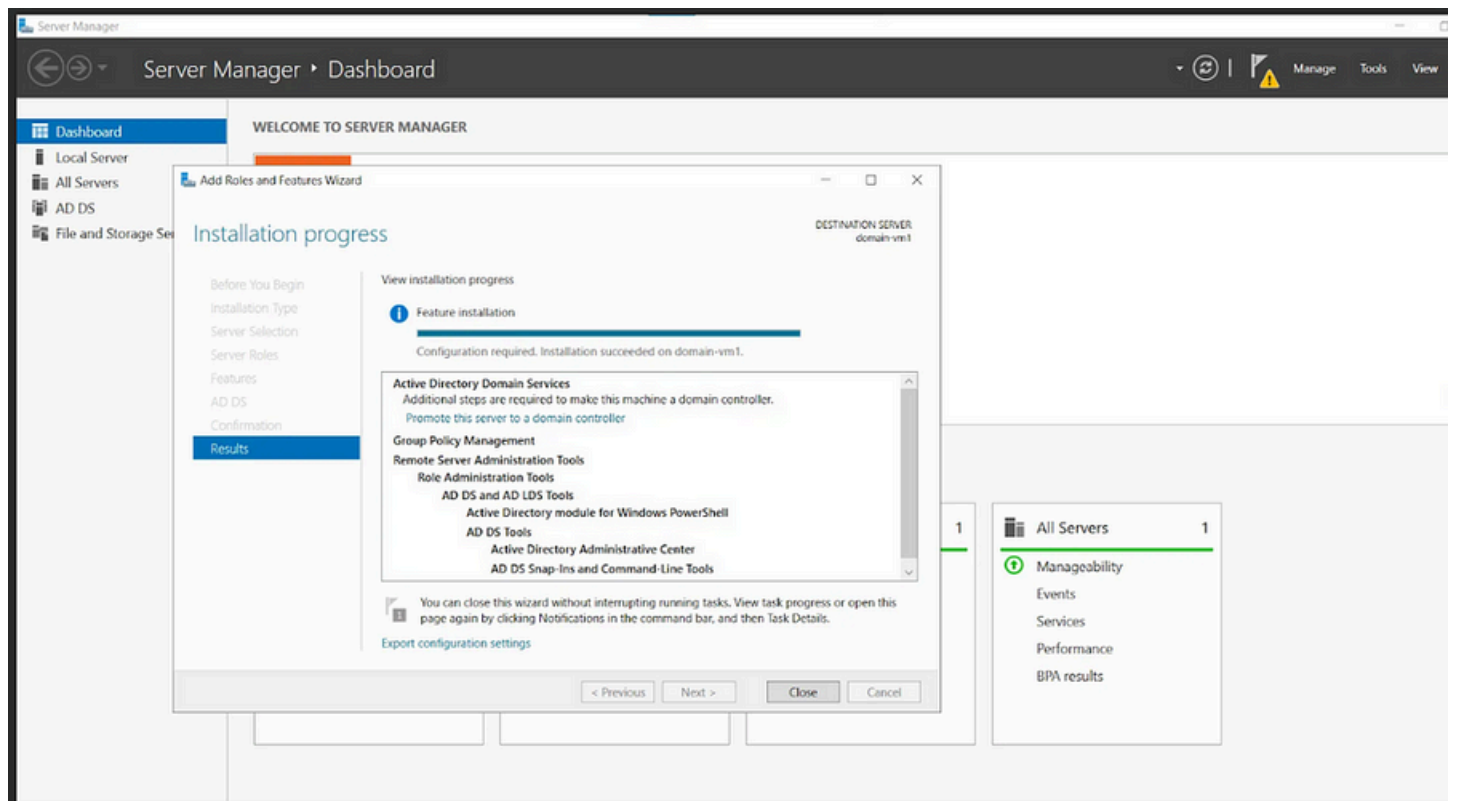
..... 

2. Connect to the VM using RDP and open Server Manager.



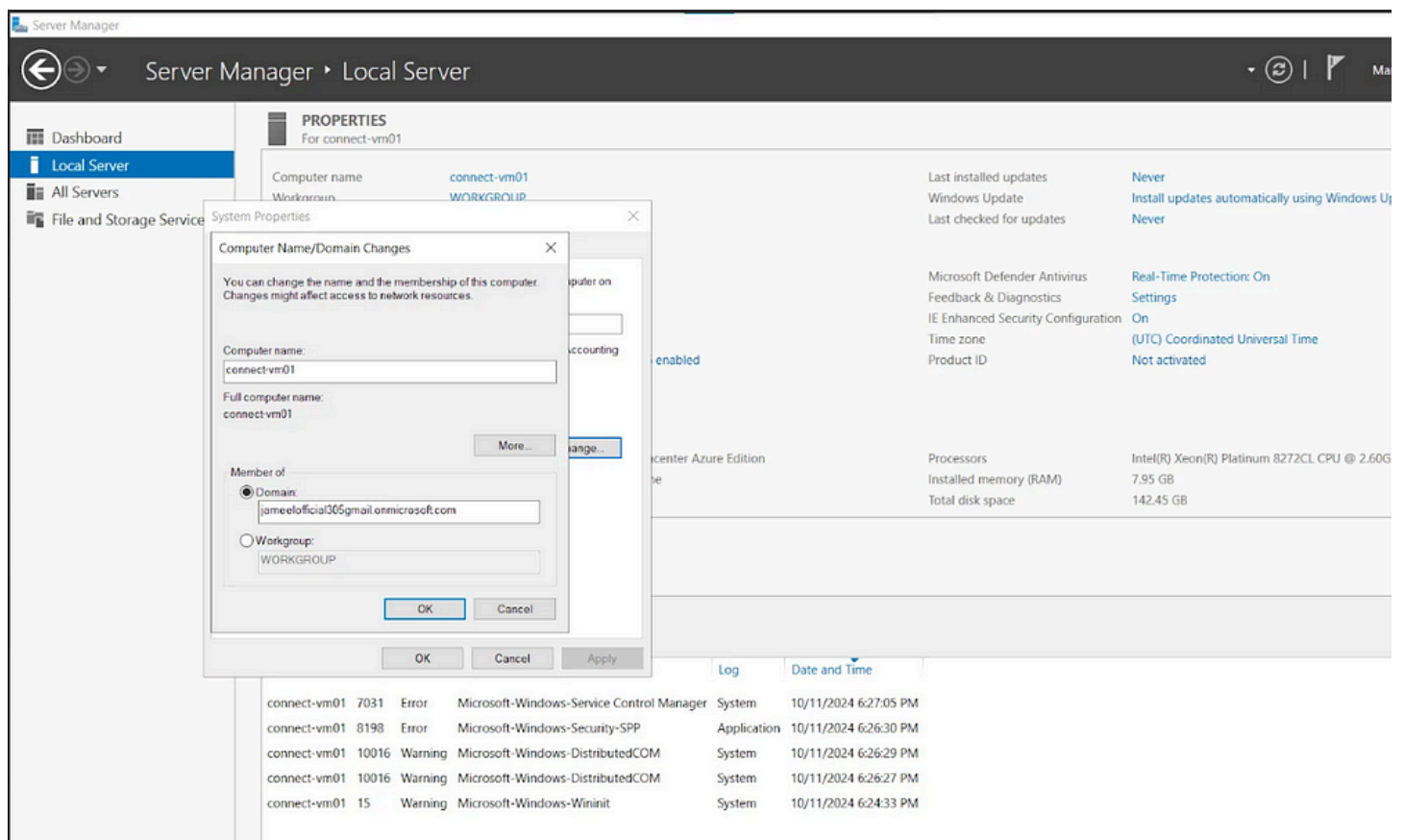
3. Add the Active Directory Domain Services (AD DS) role:



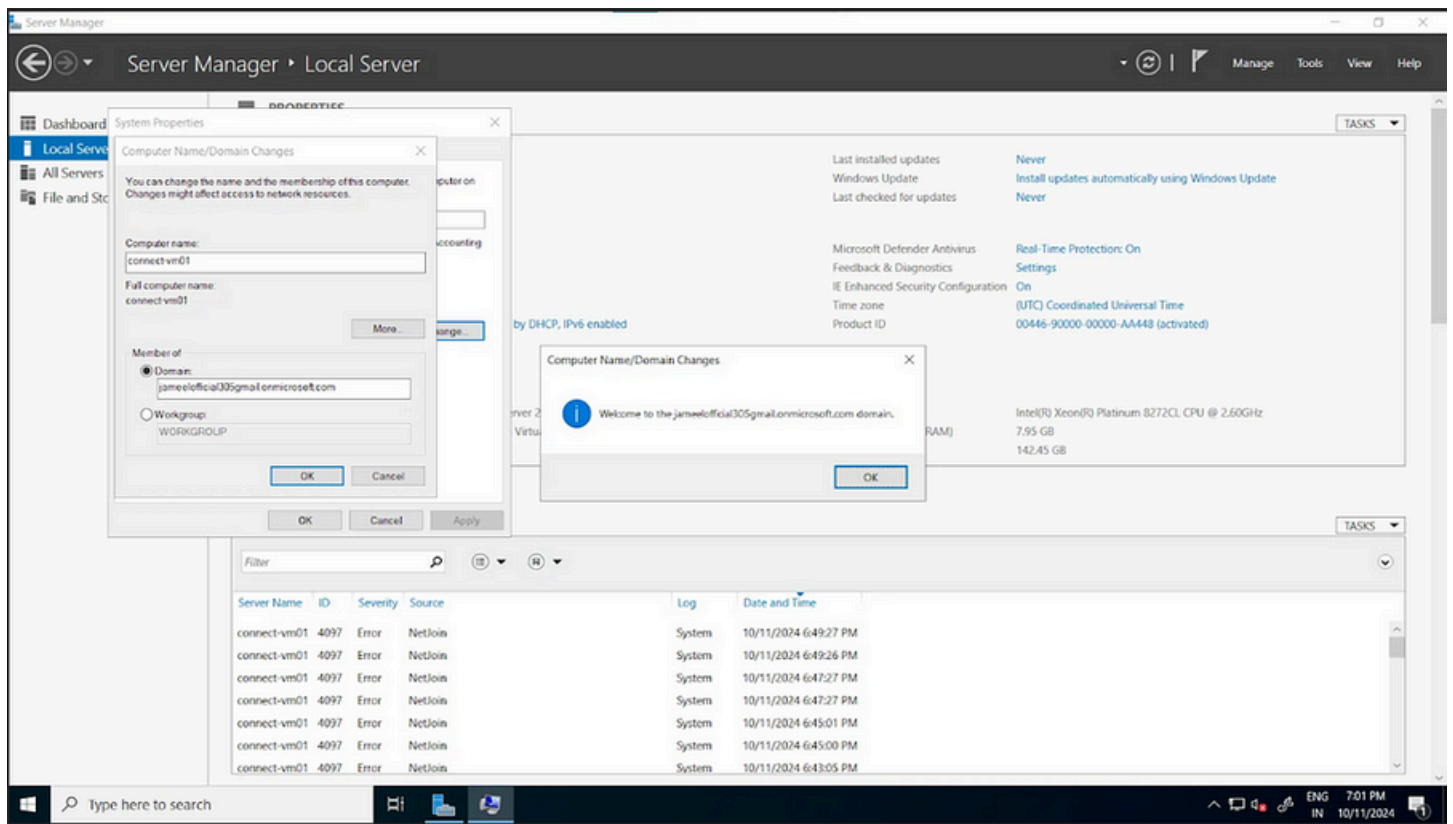


4. Promote the server to a domain controller and set up your forest and domain.

In Server Manager, go to Local Server, then click on “Workgroup”. Select “Change”, then click on “Domain” and enter your domain



next will ask password and provide the domain password — — give the credentials of domainvm1

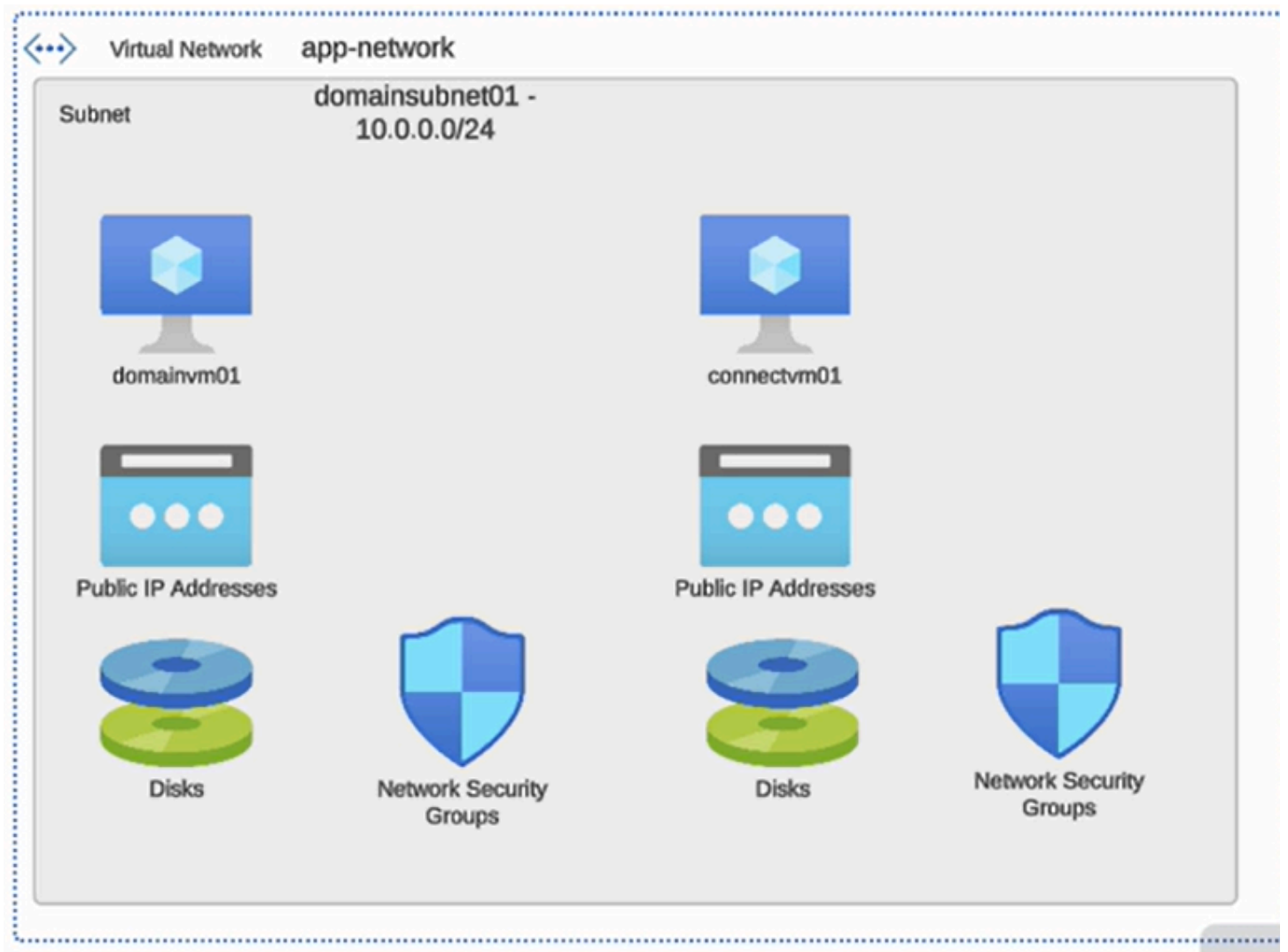


restart the machine

5. Create test users in your on-premises AD.

Step 2: Configuring DNS for Hybrid Connectivity

1. Note the private IP address of your domain controller VM.
2. In the Azure portal, go to your virtual network's DNS settings and add the domain controller's IP as a custom DNS server.
3. Restart the domain controller VM to apply changes.



Step 3: Setting Up Azure AD Connect

To set up Azure AD Connect and synchronize your on-premises Active Directory with Microsoft Entra ID, follow these steps:

1. Create another virtual machine for Azure AD Connect:
 - Name it "connect-vm01"
 - Ensure it has sufficient resources to run Azure AD Connect

The screenshot displays the Microsoft Azure portal interface. At the top, the navigation bar shows 'Microsoft Azure' and a search bar. Below the navigation bar, the breadcrumb trail indicates the path: 'Home > CreateVm-MicrosoftWindowsServer.WindowsServer-202-20241011235255 | Overview >'. The main content area is titled 'connect-vm01' and 'Virtual machine'. A warning banner at the top states: 'connect-vm01 virtual machine agent status is not ready. Troubleshoot the issue →'. Below the banner, there are action buttons: 'Connect', 'Start', 'Restart', 'Stop', 'Hibernate', 'Capture', 'Delete', 'Refresh', 'Open in mobile', 'Feedback', and 'CLI / PS'. The 'Essentials' section provides key information: Resource group (ad-connect), Status (Running), Location (Central India (Zone 1)), Subscription (Azure for Students), Subscription ID (6d22a8ee-03b5-4abb-9464-8aa65560ccf6), Availability zone (1), Operating system (Windows), Size (Standard D2s v3 (2 vcpus, 8 GiB memory)), Public IP address (20.197.46.20), Virtual network/subnet (ad-connect-vm/domain-subnet), DNS name (Not configured), Health state (-), and Time created (10/11/2024, 6:24 PM UTC). The 'Tags' section shows 'Add tags'. The 'Properties' tab is selected, showing details for the 'Virtual machine' and 'Networking' sections. The 'Virtual machine' section lists: Computer name (connect-vm01), Operating system (Windows), VM generation (V2), VM architecture (x64), Agent status (Not Ready), and Agent version (Unknown). The 'Networking' section lists: Public IP address (20.197.46.20 (Network interface connect-vm01810_21)), Public IP address (IPv6) (-), Private IP address (10.0.0.5), Private IP address (IPv6) (-), Virtual network/subnet (ad-connect-vm/domain-subnet), and DNS name (Configure).

2. Connect to the new VM using Remote Desktop Protocol (RDP)

3. Join the VM to your on-premises domain:

- In Server Manager, go to Local Server
- Click on “Workgroup”, then select “Change”
- Click on “Domain” and enter your domain name

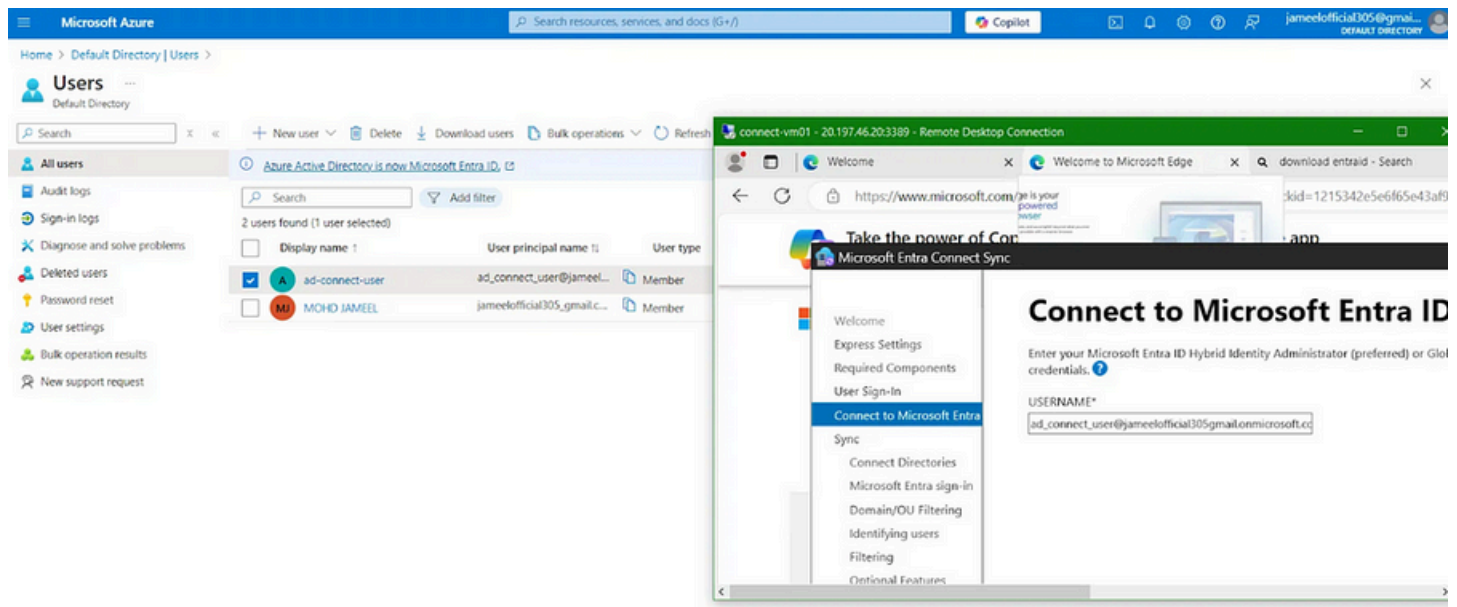
Provide the domain credentials:

- When prompted, enter the password for the domain administrator account (from domainvm1)
1. Restart the machine to apply the domain join changes
 2. Install Azure AD Connect on connect-vm01:
 - Download the latest version of Azure AD Connect from the Microsoft website
 - Run the installer and follow the setup wizard

Configure Azure AD Connect:

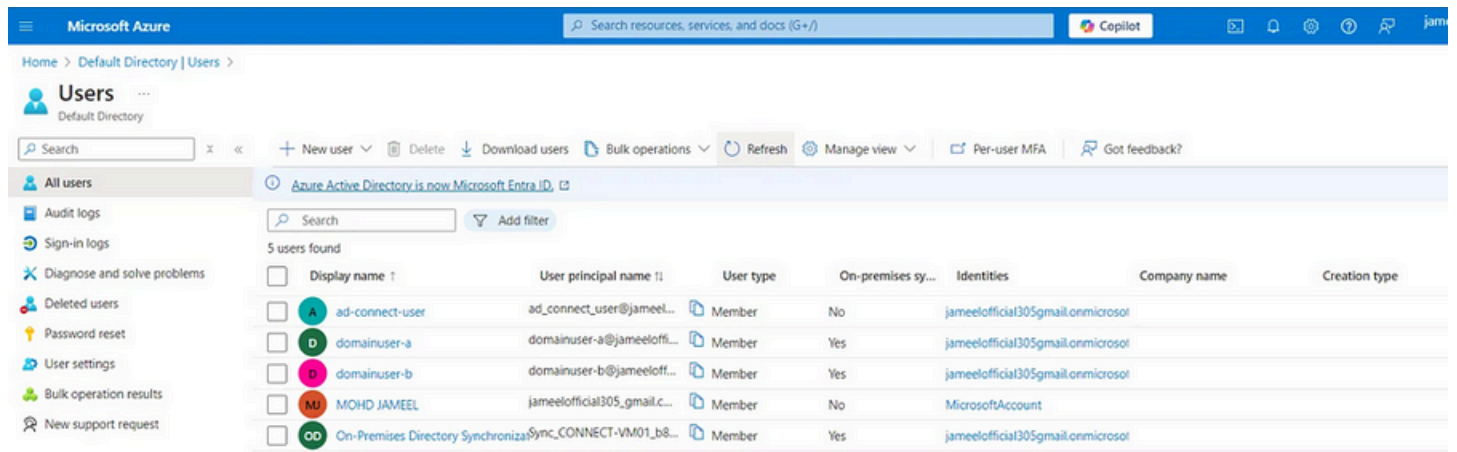
- Connect using the global administrator account you created earlier for Azure AD
- Choose the option to connect a new on-premises directory

After completing the configuration, Azure AD Connect will begin synchronizing your on-premises Active Directory users to Microsoft Entra ID. You can verify the synchronization by checking the Azure portal, where you should see the synced users appearing in your Entra ID director



Step 4: Verifying Synchronization

After configuration, you should see your synced users in the Azure portal:

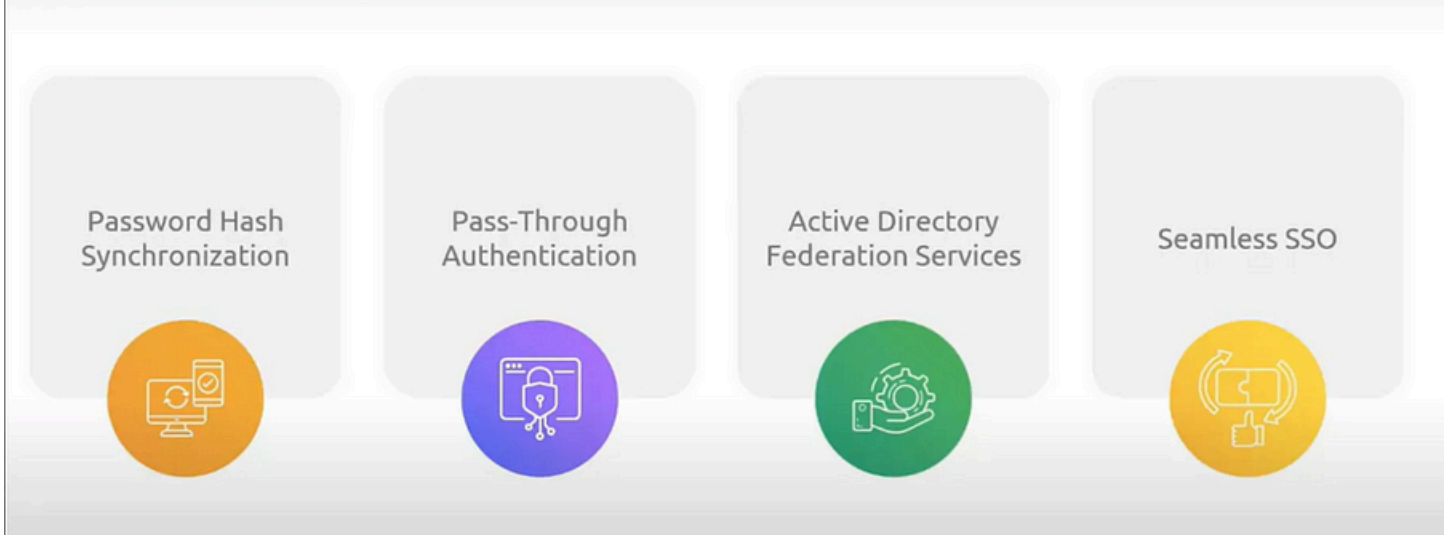


Additional Considerations

Authentication Options for Hybrid Identity

When setting up a hybrid identity environment, you have several authentication options to choose from:

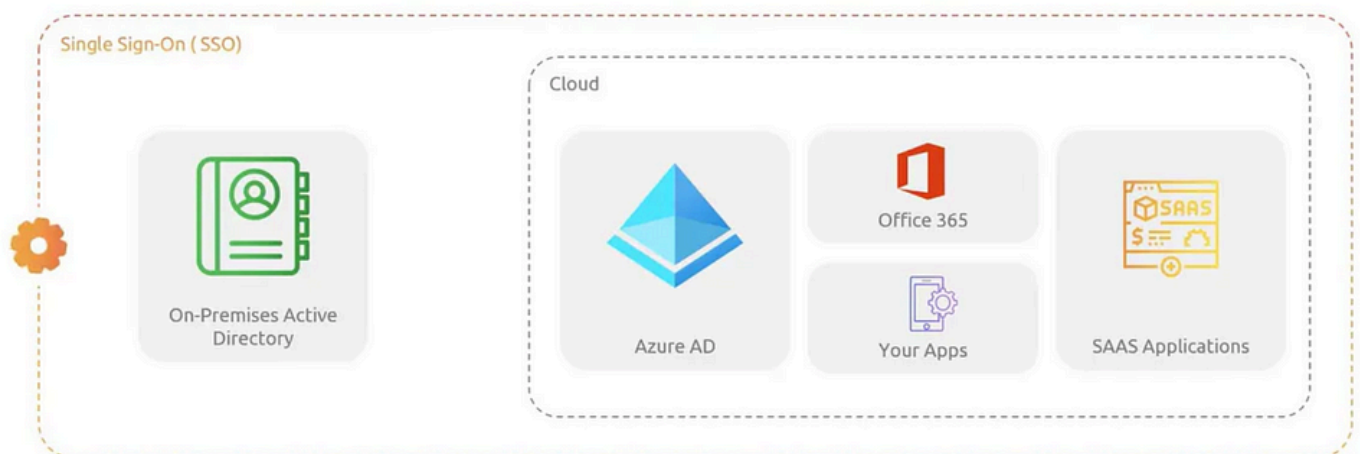
Authentication Options



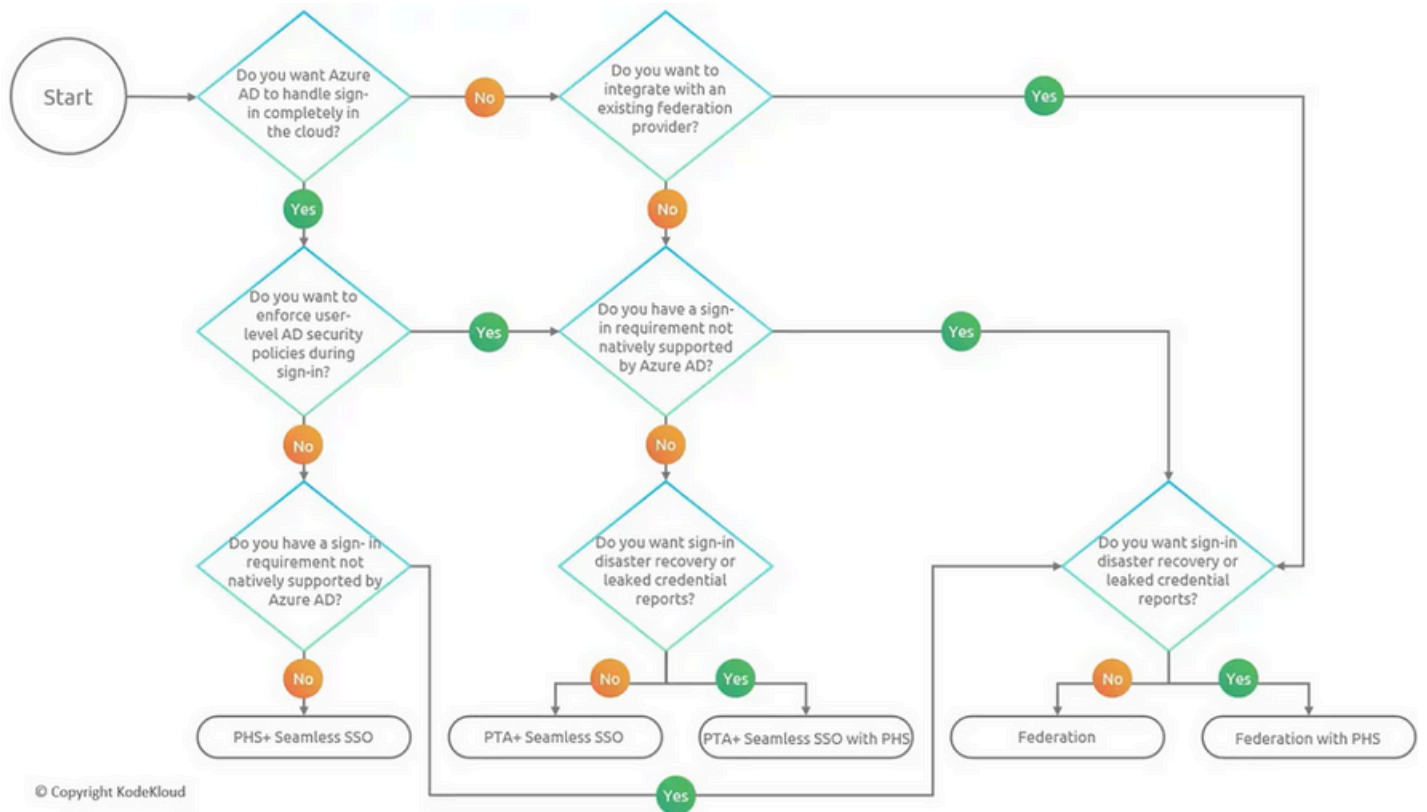
1. **Password Hash Synchronization:** This method synchronizes a hash of the user's password from on-premises AD to Azure AD. It's simple to implement and requires minimal infrastructure.
2. **Pass-through Authentication:** With this option, passwords are validated directly against the on-premises AD. It allows for real-time enforcement of on-premises security policies.
3. **Federation:** This method delegates authentication to a separate identity provider, such as Active Directory Federation Services (AD FS).

Seamless SSO

Automatically signs in users to Azure AD and cloud-based applications using their on-premises credentials



Each option has its pros and cons, and the choice depends on your organization's specific needs and security requirements. To help you decide, consider the following decision tree:



Decision Tree

This decision tree can guide you in selecting the most appropriate authentication method for your hybrid setup. Consider factors such as:

- Security requirements
- Existing infrastructure
- Need for on-premises password policy enforcement
- Desire for seamless single sign-on (SSO) experience

Remember, you can change the authentication method later if your requirements change. Azure AD Connect allows you to modify these settings post-installation.

Implementing Your Chosen Authentication Method

Once you've decided on an authentication method, you'll implement it during the Azure AD Connect setup process. Here's a brief overview of each method:

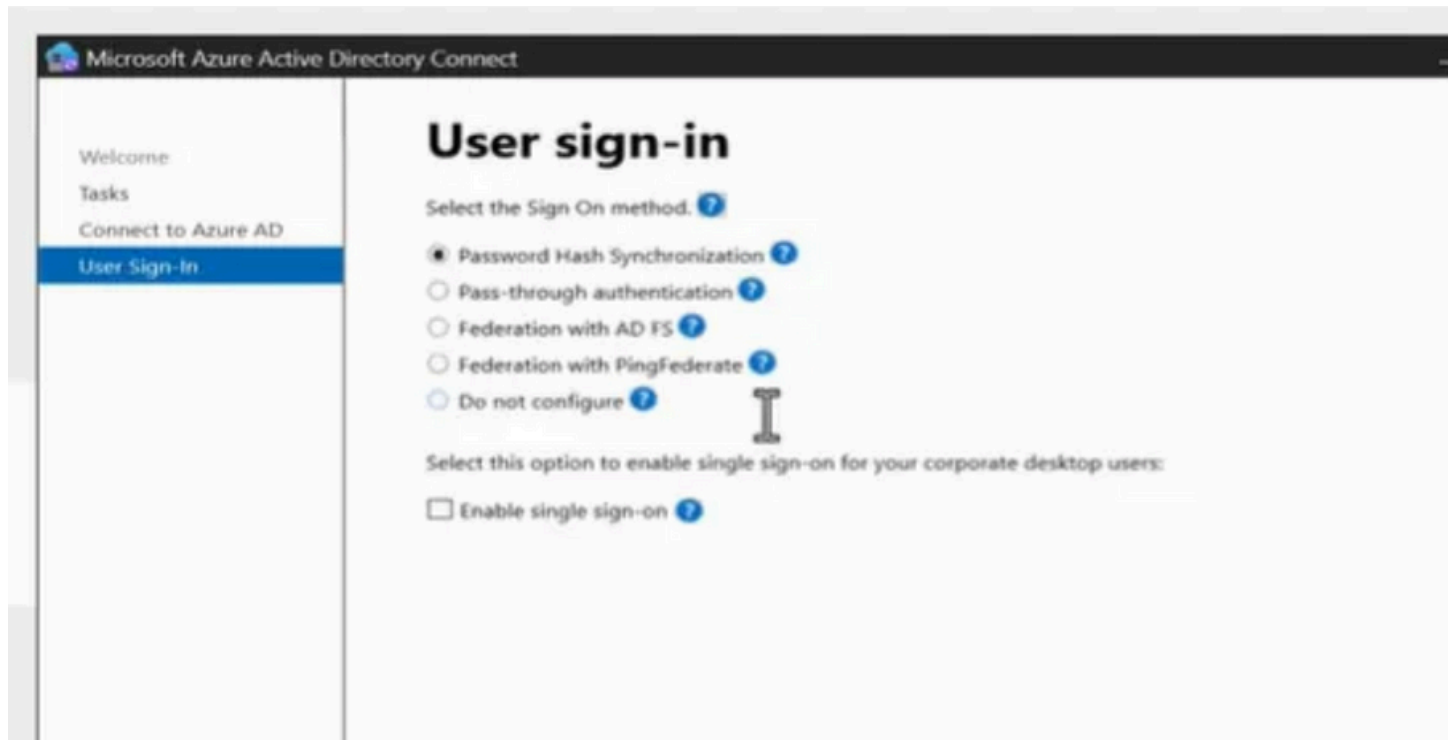
1. Password Hash Synchronization:- Easiest to set up
 - Provides a good balance of security and user experience
 - Allows for cloud-based password reset
2. Pass-through Authentication:- Requires additional agents to be installed on-premises
 - Provides real-time authentication against on-premises AD
 - Useful when you need to maintain all authentication on-premises
3. Federation:- Most complex to set up and maintain

- Provides the highest level of customization for authentication
- Typically used by large enterprises with specific security requirements

When setting up Azure AD Connect, you'll be prompted to choose your desired authentication method:

By carefully considering your authentication options and using the decision tree as a guide, you can ensure that your hybrid identity setup meets your organization's needs for security, compliance, and user experience.

You can change the authentication method later if needed:



Password Management

Two important points about password management in a hybrid setup:

- Synced user properties cannot be modified directly in Entra ID.
- Password writeback can be enabled to sync password changes from Entra ID back to on-premises AD.

Conclusion

Setting up a hybrid identity environment with Azure AD Connect provides a seamless experience for users while allowing organizations to maintain control over their on-premises infrastructure. This setup is ideal for businesses in transition to the cloud or those requiring a mix of on-premises and cloud services.

Remember to regularly monitor your synchronization health and keep Azure AD Connect updated to ensure smooth operation of your hybrid identity environment.