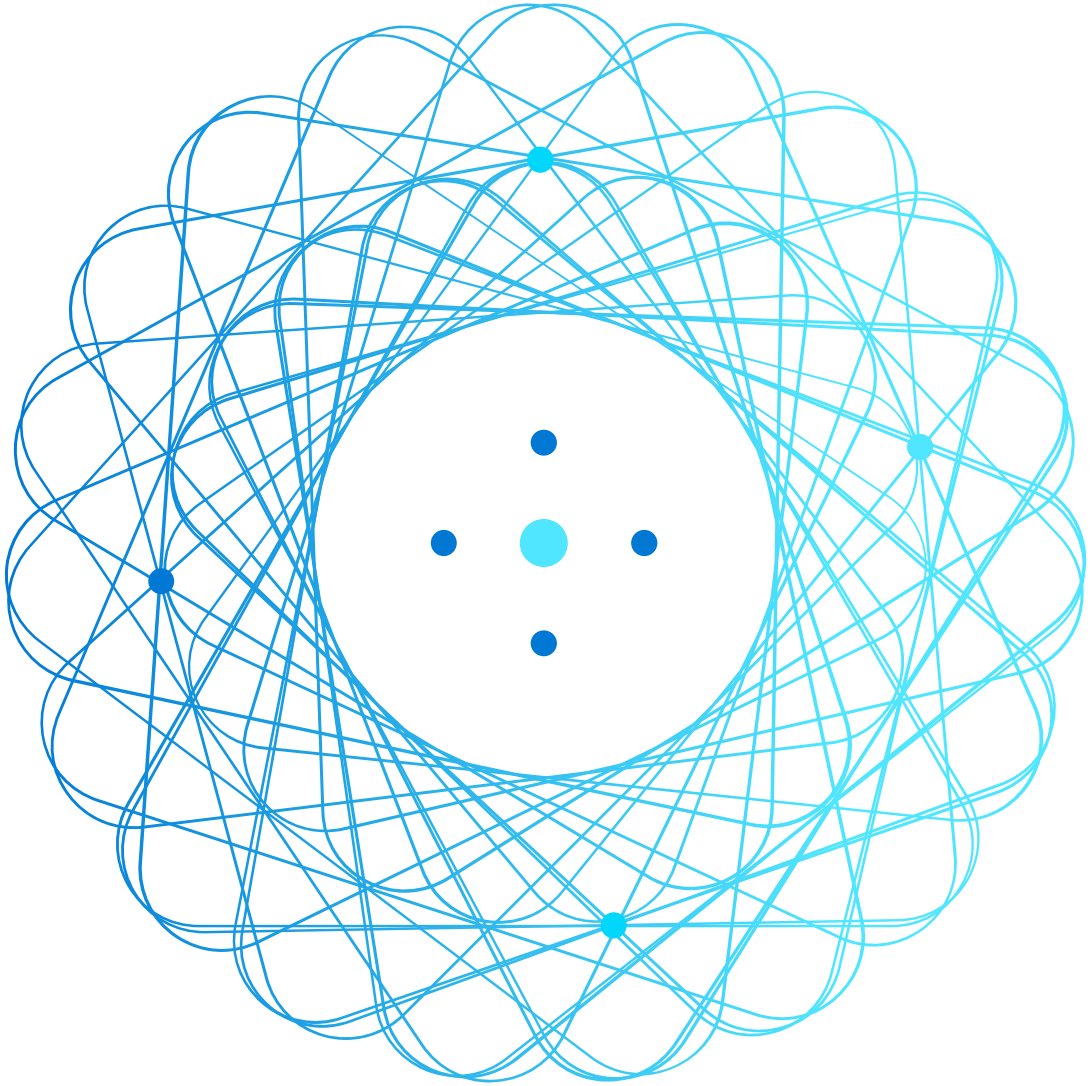
Microsoft Azure

AZ-140

Configuring and Operating Azure Virtual Desktop



AZ-140 Agenda

Learning Path 1

1. Azure Virtual Desktop Architecture
2. Design the Azure Virtual Desktop architecture
3. Design for user identities and profiles

Learning Path 2

4. Implement and manage networking for AVD
5. Implement and manage storage for AVD
6. Create and configure host pools and session hosts for AVD
7. Create and manage session host image for AVD

Learning Path 3

8. Manage access for AVD
9. Manage security for AVD

Learning Path 4

10. Implement and manage FSLogix
11. Configure user experience settings
12. Install and configure apps on a session host

Learning Path 5

13. Plan for disaster recovery
14. Automate Azure Virtual Desktop management tasks
15. Monitor and manage performance and health

Design for user identities and profiles

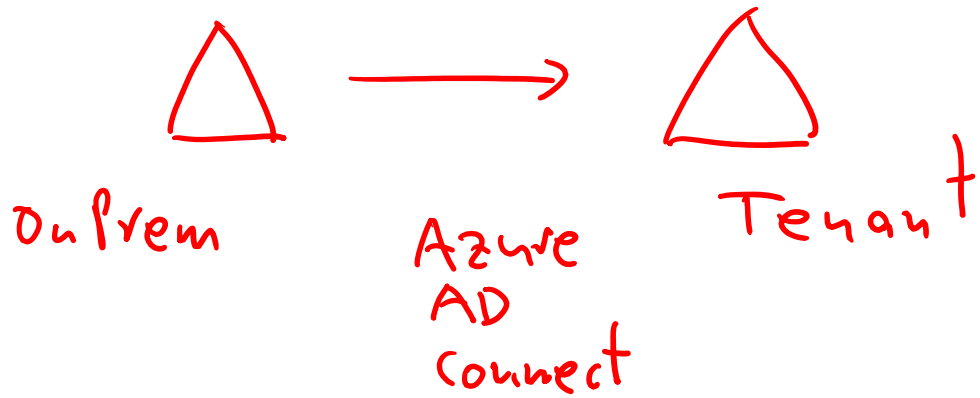
Introduction

- Select an appropriate licensing model for Azure Virtual Desktop based on requirements
- Personal and multi-session desktop scenarios
- Recommend an appropriate storage solution
- Plan for a Desktop client deployment
- Plan for Azure Virtual Desktop client deployment - Remote Desktop Protocol (RDP)
- Windows Desktop client to multiple devices
- Hybrid Identity with Azure Active Directory
- Plan for Azure AD Connect for user identities
- Knowledge check and Summary

AZ-140: Plan an Azure Virtual Desktop architecture (10-15%)

Design the Azure Virtual Desktop architecture

- Conceptual knowledge of Azure compute solutions.
- Working experience with virtual machines, virtual networks, and app service.



Select an appropriate licensing model for Azure Virtual Desktop based on requirements

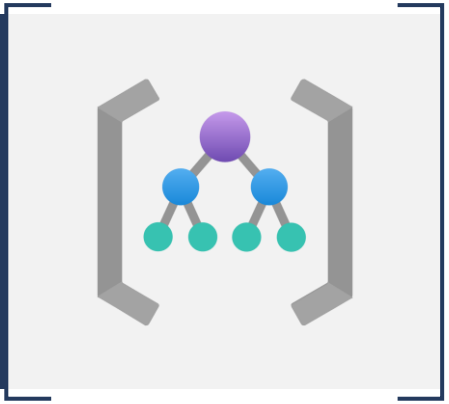
Licensing for Azure Virtual Desktop

- Access Windows 10 Enterprise and Windows 7 Enterprise desktops and apps at no additional cost if you have an eligible Windows or Microsoft 365 license

- Access to desktops powered by Windows Server Remote Desktop Services desktops and apps at no additional cost if you are an eligible Microsoft RDS and Client Access License (CAL) customer

TYPE	DESCRIPTION	ELIGIBILITY
Virtualize Windows 10 and Windows 7	Access Windows 10 Enterprise and Windows 7 Enterprise desktops and apps at no additional cost if you have an eligible Windows or Microsoft 365 license. Get free Extended Security Updates until January 2023 for your Windows 7 virtual desktop—offering more options to support legacy apps while you transition to Windows 10.	You are eligible to access Windows 10 and Windows 7 with Azure Virtual Desktop if you have one of the following per user licenses: Microsoft 365 E3/E5 Microsoft 365 A3/A5/Student Use Benefits Microsoft 365 F3 Microsoft 365 Business Premium** Windows 10 Enterprise E3/E5 Windows 10 Education A3/A5 Windows 10 VDA per user
Virtualize Windows Server	Access desktops powered by Windows Server Remote Desktop Services desktops and apps at no additional cost if you are an eligible Microsoft Remote Desktop Services (RDS) Client Access License (CAL) customer.	You are eligible to access Windows Server 2012 R2 and newer desktops and apps if you have a per-user or per-device RDS CAL license with active Software Assurance (SA).

Personal and multi-session desktop scenarios



Use case scenarios for single users accessing a persistent virtual desktop:

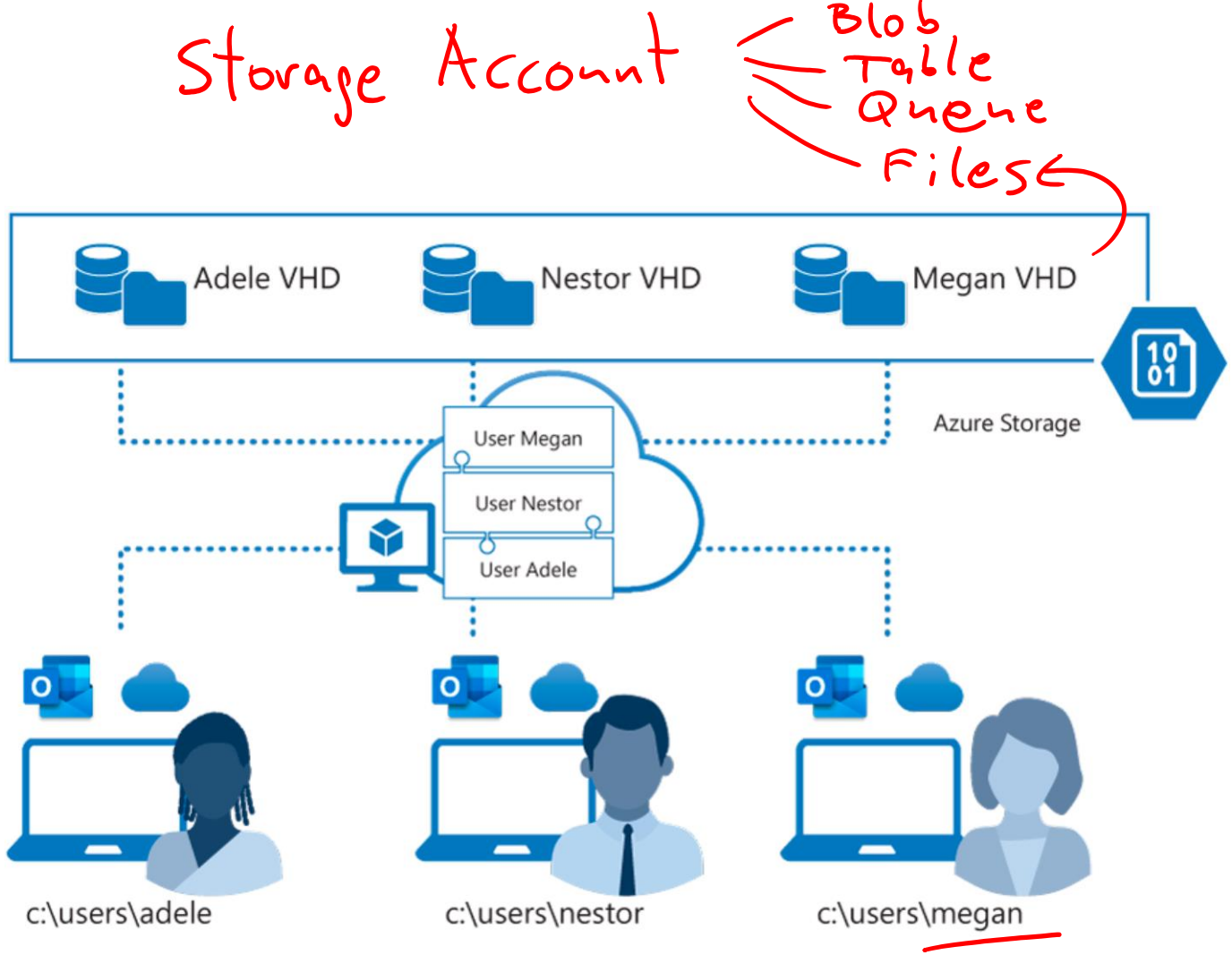
EXAMPLE WORKLOADS	NUMBER OF USERS IN SCENARIO	TYPE OF USER	VCPUS	RAM	EAST US PRICING	WEST EUROPE PRICING	SOUTHEAST ASIA PRICING
Graphics Workstation	100	Engineers and graphic designers with 3D modeling, simulations, and CAD workloads. Users spend 5-6 hours a day requiring workstation capability.	12	112 GB	See estimate	See estimate	See estimate
Microsoft Office	1000	Standard knowledge workers making use of Microsoft Office products. Users work 8-10 hour days.	2	4 GB	See estimate	See estimate	See estimate

Use case scenarios for multiple users sharing a pooled (non-persistent) virtual desktop:

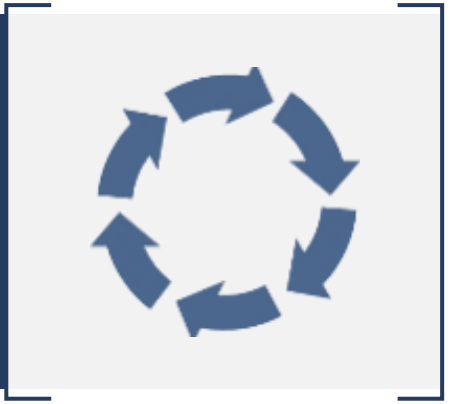
EXAMPLE WORKLOADS	NUMBER OF USERS IN SCENARIO	TYPE OF USER	USER DENSITY	EAST US PRICING	WEST EUROPE PRICING	SOUTHEAST ASIA PRICING
Microsoft Office	1000	Standard knowledge workers making use of Microsoft Office products. 24/7 RI is used to avoid need for management of virtual machines.	2 per vCPU	See estimate	See estimate	See estimate
Call center/data entry	1000	Call center users with low intensity workloads, primarily engaged in data entry. Users operate in three 8-hour shifts, making a 24/7 RI instance the most cost effective option.	6 per vCPU	See estimate	See estimate	See estimate

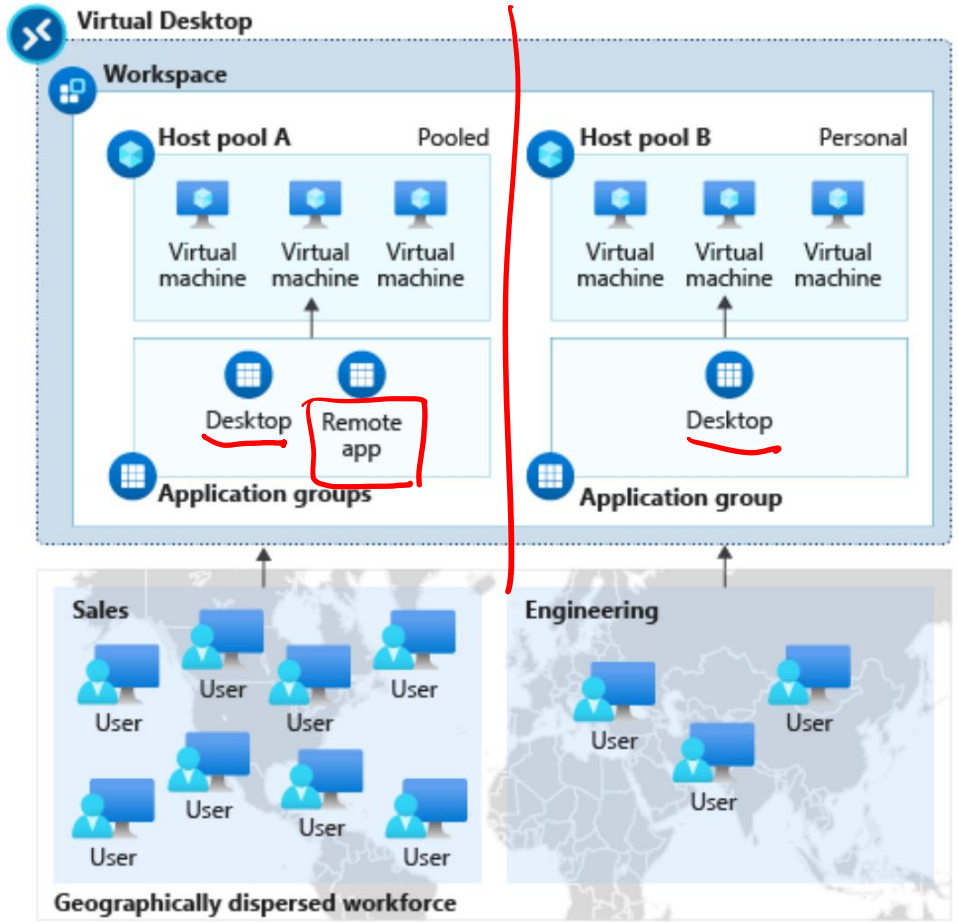
Recommend an appropriate storage solution

- FSLogix is designed to roam profiles in remote computing environments, such as Azure Virtual Desktop
- At sign-in, a container is dynamically attached to the computing environment using a natively supported VHD and a VHDX
- The user profile is immediately available and appears in the system exactly like a native user profile



Plan for a Desktop client deployment





The diagram below shows an Azure Virtual Desktop workspace with two host pools:

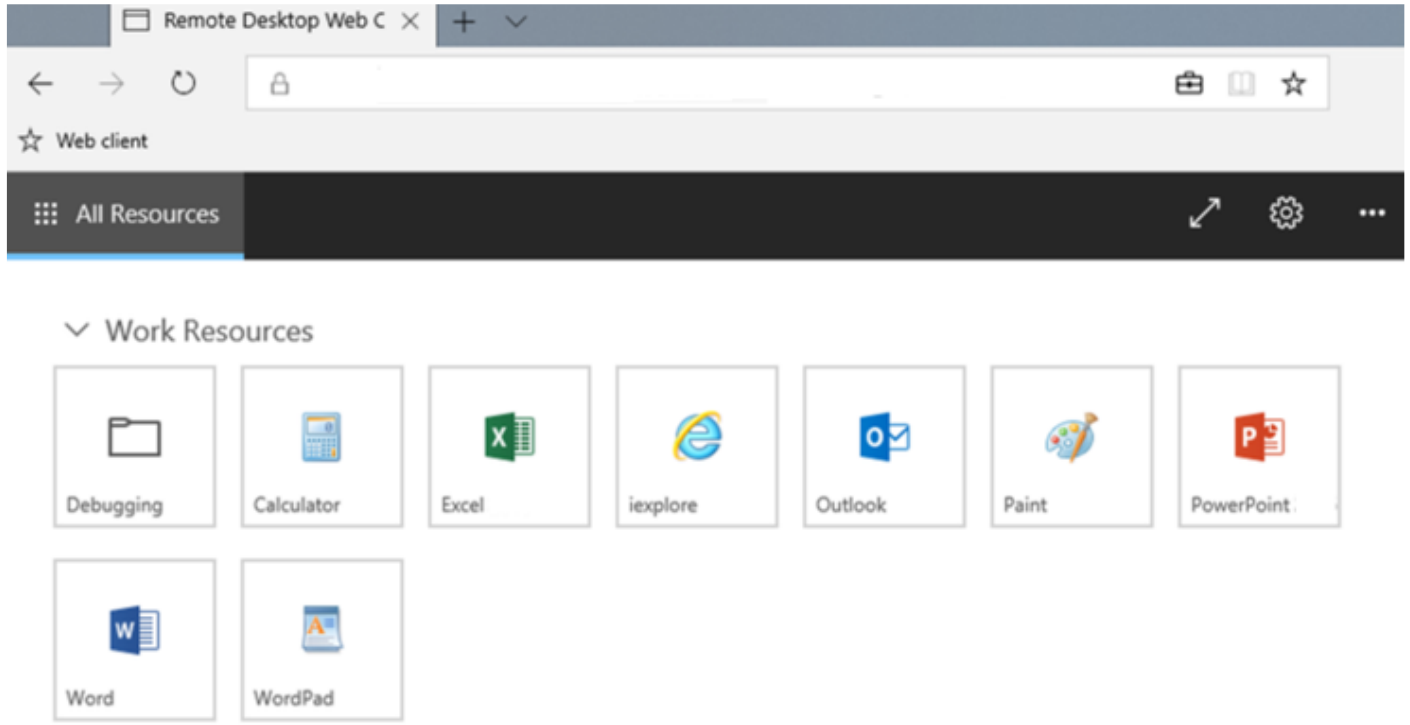
- **Host pool A** has two application groups: Desktop and RemoteApp. These resources are shared (pooled) across the sales team.
- **Host pool B** has a Desktop application group with personal desktops available to an engineering team.

Plan for Azure Virtual Desktop client deployment - Remote Desktop Protocol (RDP)

Remote Desktop web client uses a compatible web browser to access remote resources (apps and desktops) published to you by your admin.

For access to remote apps and desktops, users need:

- A domain
- Username
- Password
- URL (provided by the admin)
- A supported web browser



Windows Desktop client to multiple devices

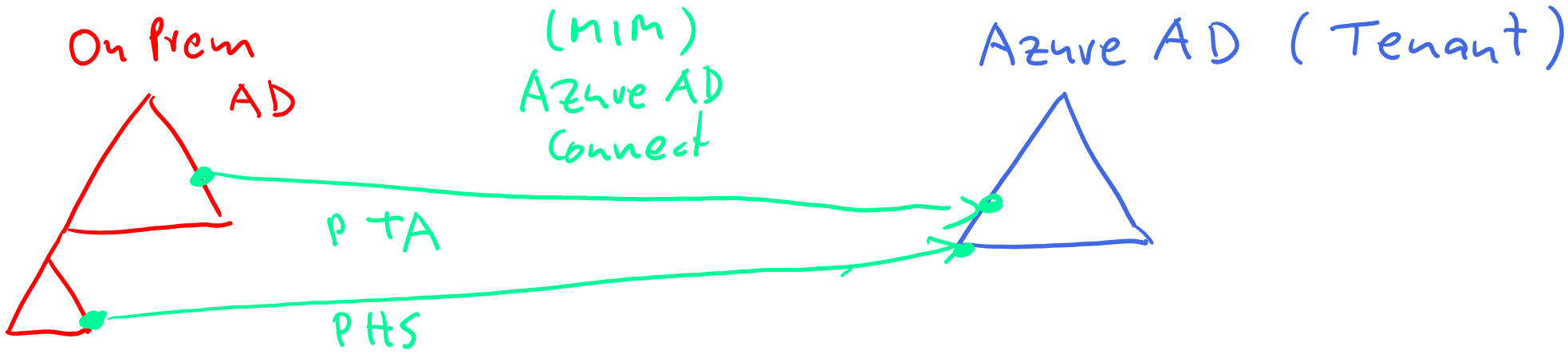
Deploying using group policies or the Microsoft Endpoint Configuration Manager lets you run the installer silently using a command line.

Per-device installation, run:

```
msiexec.exe /i <path to the MSI> /qn ALLUSERS=1
```

Per-user installation, run:

```
msiexec.exe /i `<path to the MSI>` /qn ALLUSERS=2 MSIINSTALLPERUSER=1
```



Hybrid Identity with Azure Active Directory

Forest, Trees, Domains
OUs
GPO
Kerbevos, NTLM

flat
AUs Admin Units
→ Intune (MEM)
OAuth 2.0 (Open ID Connect)
SAML

Hybrid Identity with Azure Active Directory

You can use the following authentication methods to implement hybrid identity with Azure AD

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

Common hybrid identity and access management scenarios with recommendations for hybrid identity options.

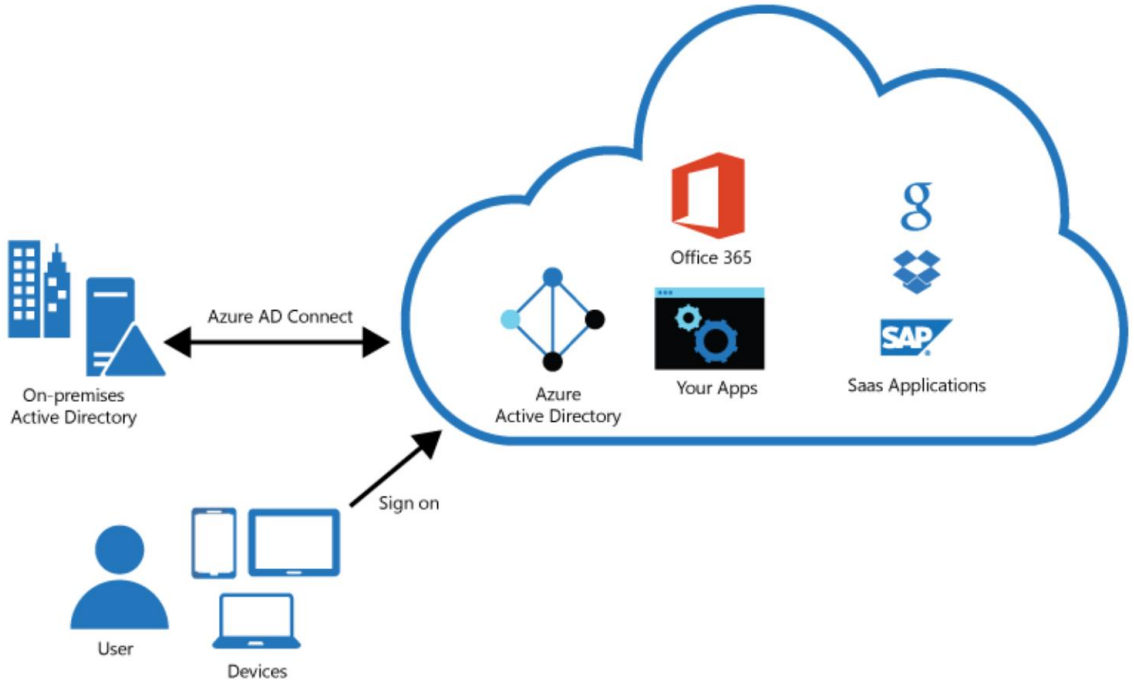
I need to:	PHS and SSO1	PTA and SSO2	AD FS3
Sync new user, contact, and group accounts created in my on-premises Active Directory to the cloud automatically.	**Yes**	**Yes**	**Yes**
Set up my tenant for Office 365 hybrid scenarios.	**Yes**	**Yes**	**Yes**
Enable my users to sign in and access cloud services using their on-premises password.	**Yes**	**Yes**	**Yes**
Implement single sign-on using corporate credentials.	**Yes**	**Yes**	**Yes**
Ensure no password hashes are stored in the cloud.		**Yes**	**Yes**
Enable cloud-based multifactor authentication solutions.	**Yes**	**Yes**	**Yes**
Enable on-premises multifactor authentication solutions.			**Yes**
Support smartcard authentication for my users.			**Yes**
Display password expiry notifications in the Office Portal and on the Windows 10 desktop.			**Yes**

Plan for Azure AD Connect for user identities

Plan for Azure AD Connect for user identities

Integrating on-premises directories with Azure AD provides a common identity for accessing both cloud and on-premises resources.

- Users can use a single identity to access on-premises applications and cloud services such as Office 365.
- Single tool to provide an easy deployment experience for synchronization and sign-in.
- Azure AD Connect replaces older versions of identity integration tools such as DirSync and Azure AD Sync.



Plan for Azure AD Connect for user identities (Cont)

Password hash synchronization - A sign-in method that synchronizes a hash of a users on-premises AD password with Azure AD.

Pass-through authentication - A sign-in method that allows users to use the same password on-premises and in the cloud but doesn't require the additional infrastructure of a federated environment.

Federation integration - Is used to configure a hybrid environment using an on-premises AD FS infrastructure. It also provides AD FS management capabilities such as certificate renewal and additional AD FS server deployments.

Synchronization - Responsible for creating users, groups, and other objects. As well as, making sure identity information for your on-premises users and groups is matching the cloud.

Health Monitoring - Azure AD Connect Health can provide robust monitoring and provide a central location in the Azure portal to view this activity.

Knowledge check and Summary

Check your knowledge

What you learned:

- Select a licensing model for Azure Virtual Desktop.
- Describe personal and multi-session desktop scenarios.
- Plan a storage solution storing FSLogix profile containers
- Plan for a Desktop client deployment
- Deploy Windows Desktop client to multiple devices.
- Describe Hybrid Identity for Azure Virtual Desktop.

End of presentation