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
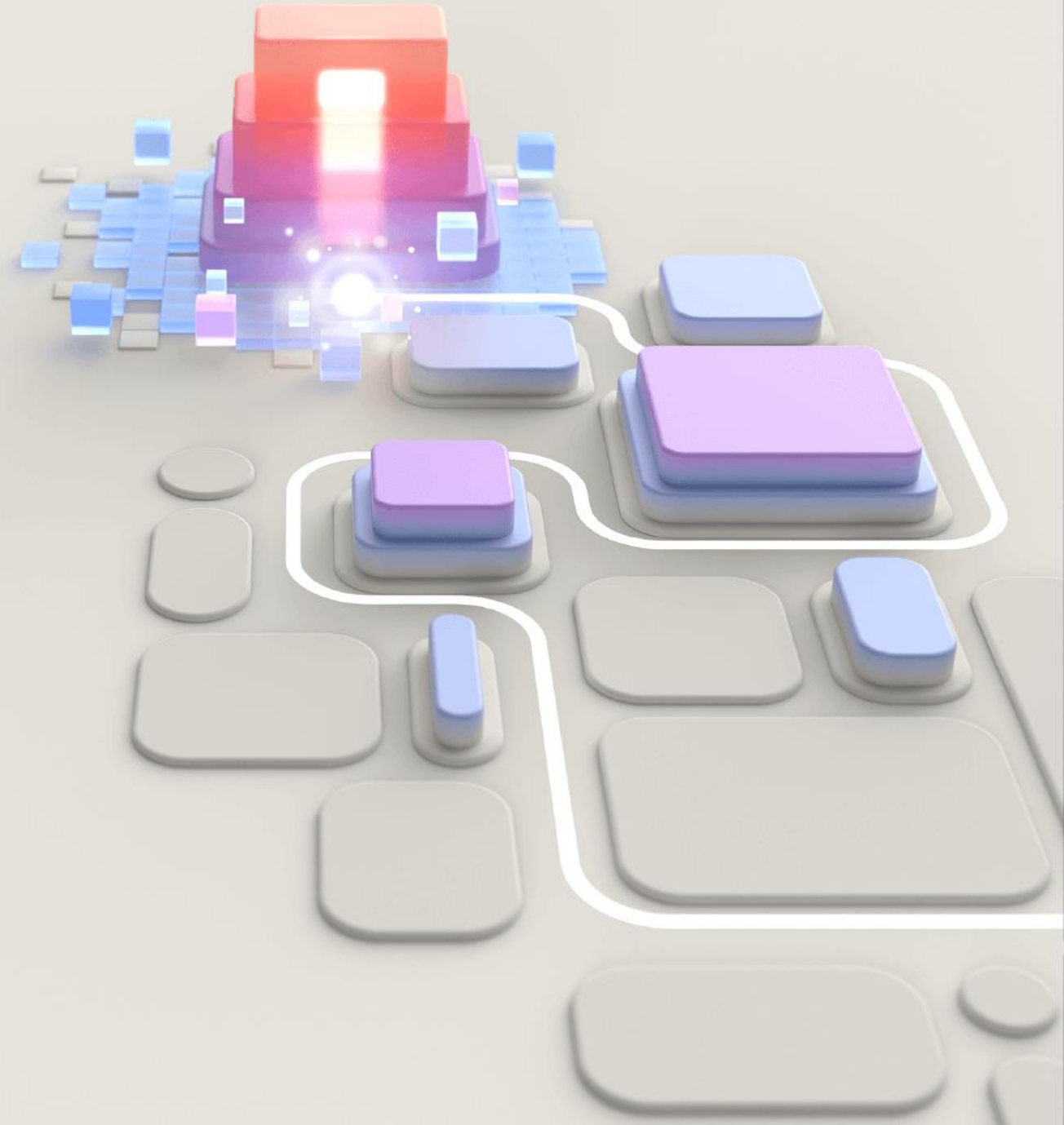
Learning Path 3

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

Learning Path 4

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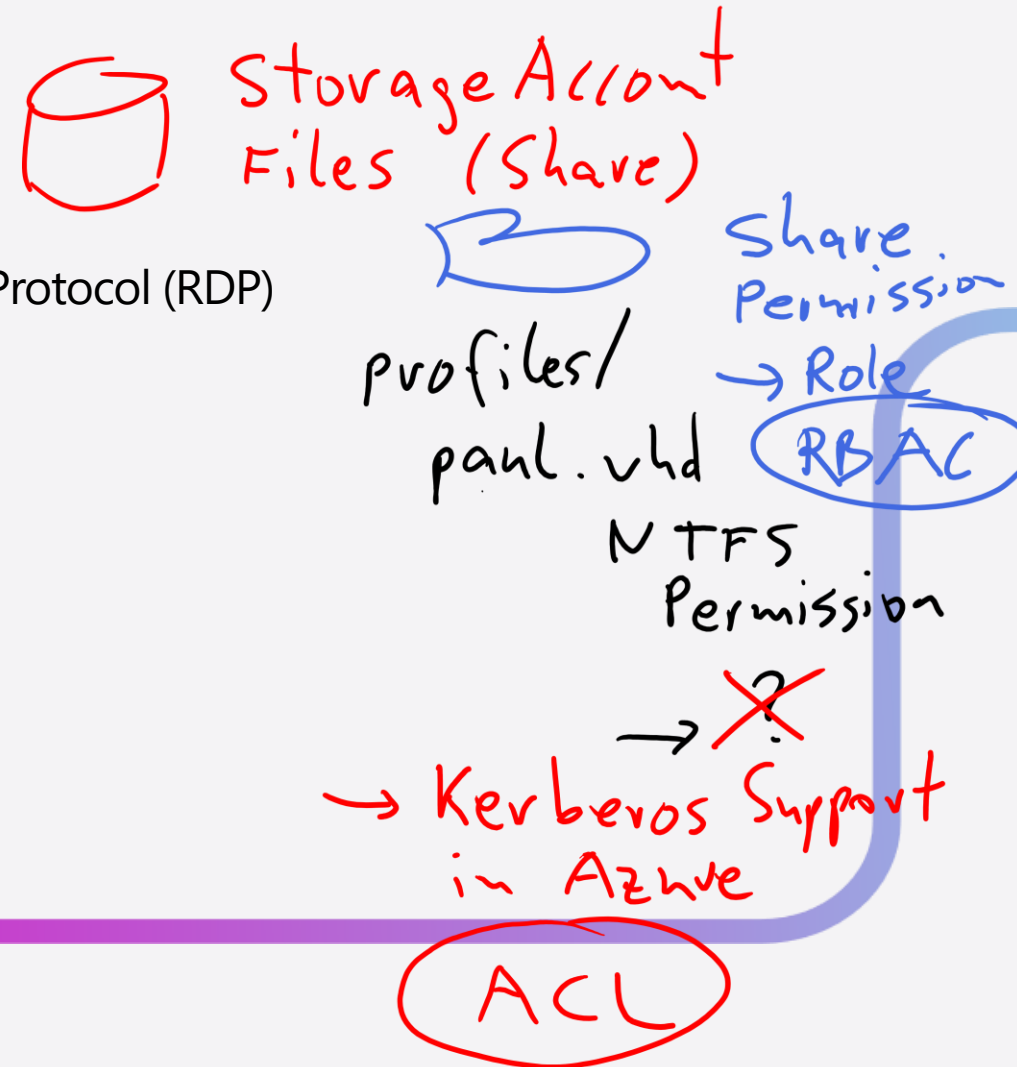12. Install and configure apps on a session host

Learning Path 5

13. Monitor and manage performance and health
14. Plan and implement updates, backups, and
    disaster recovery

Microsoft

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 Entra ID

Storage Account
Files (Share)

Share
Permission
→ Role

profiles/
paul.vhd   RBAC

NTFS
Permission
→ ✗?

→ Kerberos Support
in Azure

ACL

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

Licensing for Azure Virtual Desktop

Operating system (64-bit only)	Licensing method (Internal commercial purposes)	Licensing method (External commercial purposes)
•Windows 11 Enterprise multi-session •Windows 11 Enterprise •Windows 10 Enterprise multi-session •Windows 10 Enterprise	•Microsoft 365 E3, E5, A3, A5, F3, Business Premium, Student Use Benefit •Windows Enterprise E3, E5 •Windows Education A3, A5 •Windows VDA per user	•Per-user access pricing by enrolling an Azure subscription.
•Windows Server 2022 •Windows Server 2019 •Windows Server 2016	•Remote Desktop Services (RDS) Client Access License (CAL) with Software Assurance (per-user or per-device) •RDS User Subscription Licenses.	•Windows Server 2022 RDS Subscriber Access License (SAL). Per-user access pricing isn't available for Windows Server operating systems.

Personal and multi-session desktop scenarios

Comparing licensing options

Here's a summary of the two types of licenses for Azure Virtual Desktop you can choose from:

Component	Eligible Windows, Microsoft 365, or RDS license	Per-user access pricing
Access rights	Internal purposes only. It doesn't grant permission for external commercial purposes, not even identities you create in your own Microsoft Entra tenant.	External commercial purposes only. It doesn't grant access to members of your own organization or contractors for internal business purposes.
Billing	Licensing channels.	Pay-as-you-go through an Azure meter, billed to an Azure subscription.
User behavior	Fixed cost per user each month regardless of user behavior.	Cost per user each month depends on user behavior.
Other products	Dependent on the license.	Only includes access rights to Azure Virtual Desktop and FSlogix.

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
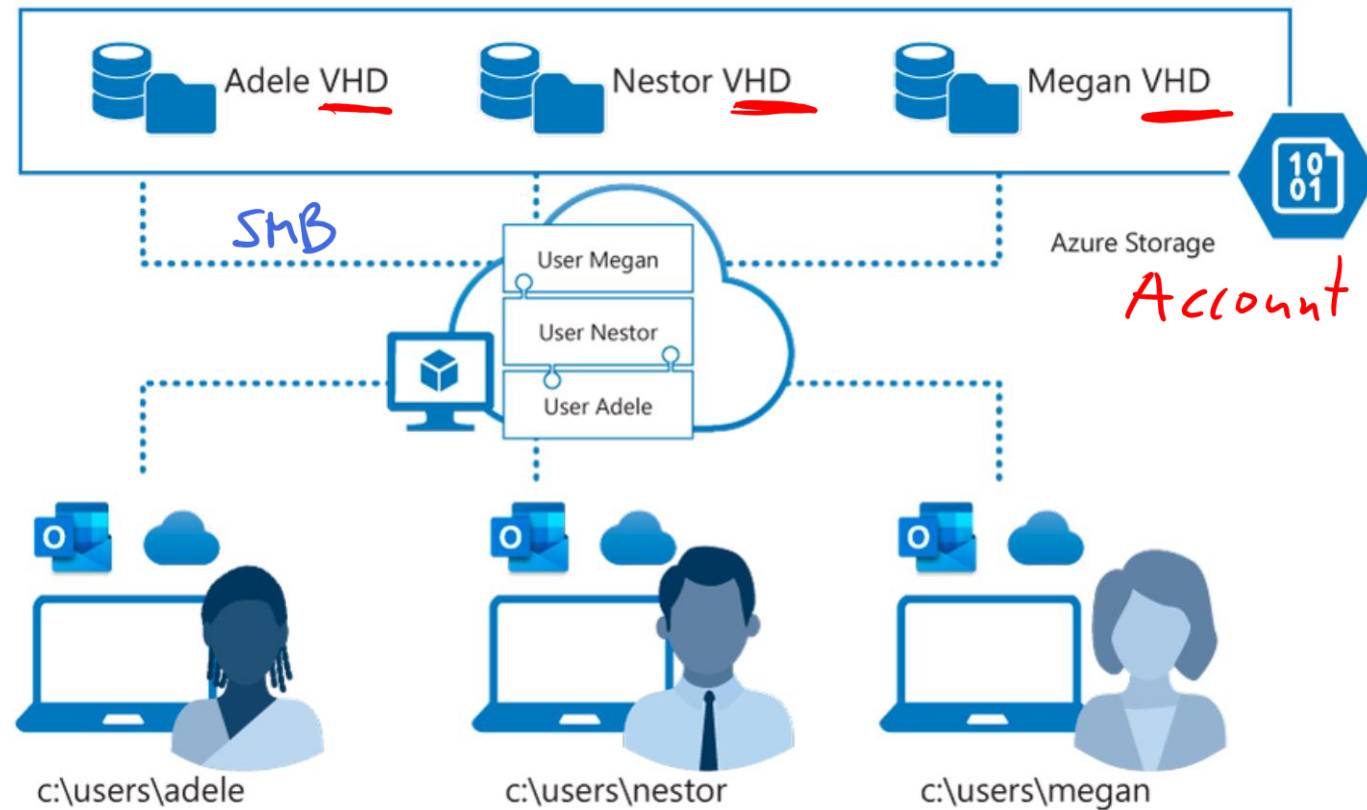
Plan for a Desktop client deployment

Microsoft Remote Desktop clients connect to Azure Virtual Desktop and use and control desktops and apps that your admin has made available to you.

| Platform	Documentation and download links	Version information
Windows	[Connect to Azure Virtual Desktop with the Remote Desktop client for Windows](#)	[What's new](#)
Web	[Connect to Azure Virtual Desktop with the Remote Desktop client for Web](#)	[What's new](#)
macOS	[Connect to Azure Virtual Desktop with the Remote Desktop client for macOS](#)	[What's new](#)
iOS/iPadOS	[Connect to Azure Virtual Desktop with the Remote Desktop client for iOS and iPadOS](#)	[What's new](#)
Android/Chrome OS	[Connect to Azure Virtual Desktop with the Remote Desktop client for Android and Chrome OS](#)	[What's new](#)

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
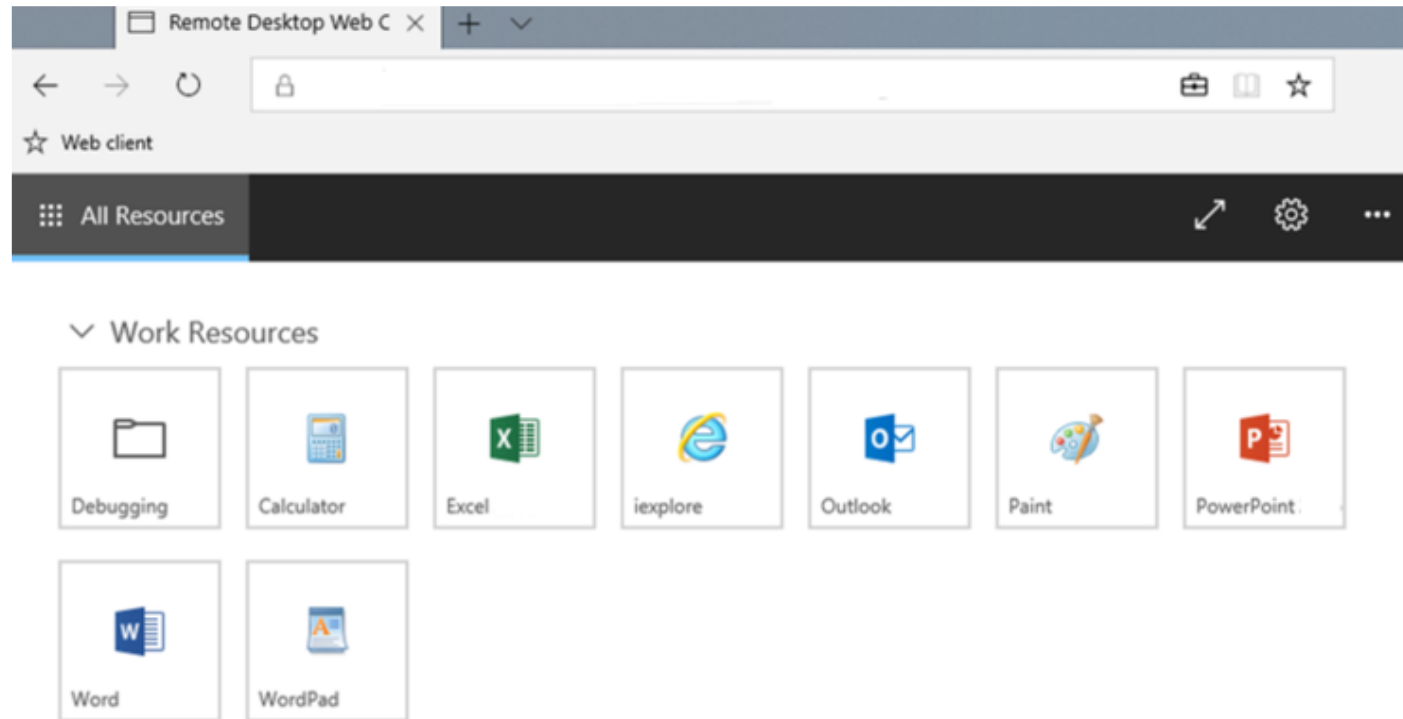
Windows Desktop client to multiple devices

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 Microsoft Entra ID

- **Hybrid Deployment**: Businesses are increasingly using a mix of on-premises and cloud applications, requiring user access across both environments.

- **Hybrid Identity**: Microsoft's identity solutions provide a unified user identity for authentication and authorization across all resources, regardless of location.

- **Provisioning**: This process involves creating, updating, and deleting objects based on specific conditions to maintain up-to-date user information.

- **Synchronization**: Ensures that identity information for on-premises users and groups matches the information in the cloud.

Hybrid Identity with Azure Active Directory

You can use the following authentication methods to implement hybrid identity with Entra ID

	AuthN AD	Entra ID	Azure
Password hash synchronization (PHS) *	✔	✔	
Pass-through authentication (PTA)	✔	✘	
Federation (AD FS)	✔	✘	

Fed Server on Prem

Auth

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 Entra Connect for user identities

Plan for Entra Connect for user identities

Integrating on-premises directories with Entra ID 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.

- Entra Connect replaces older versions of identity integration tools such as DirSync and Azure AD Sync.

On-premises Active Directory

Entra Connect

Office 365

Your Apps

Saas Applications

User

Devices

Sign on
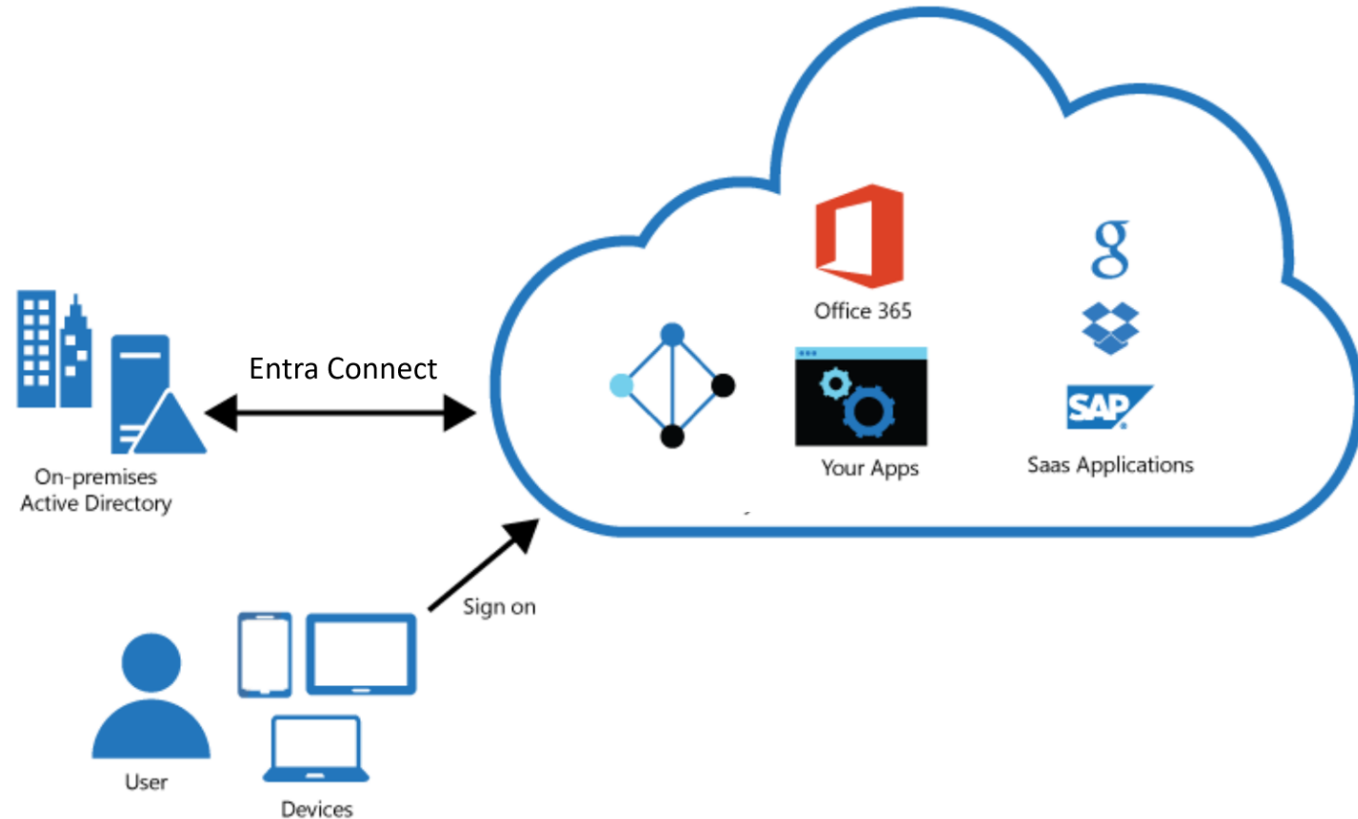
Summary

Summary

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