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

Manage access for Azure Virtual Desktop

Introduction

After completing this module, you'll be able to:

- Select an identity strategy for Azure Virtual Desktop
- Select an authentication strategy for Azure Virtual Desktop
- Describe Role-based access control (RBAC) for Azure Virtual Desktop
- Plan and implement Azure roles and role-based access control (RBAC) for Azure Virtual Desktop
- Assign RBAC roles to the Azure Virtual Desktop service principals
- Enforce Microsoft Entra MFA for Azure Virtual Desktop using Conditional Access

Selecting an identity strategy for Azure Virtual Desktop

Types of Identities

Azure Virtual Desktop supports different types of identities depending on which configuration you choose.

Azure Virtual Desktop doesn't support signing in to Microsoft Entra ID with one user account, then signing in to Windows with a separate user account. Signing in with two different accounts at the same time can lead to users reconnecting to the wrong session host, incorrect or missing information in the Azure portal, and error messages appearing while using app attach or MSIX app attach.

On-premises identity

Since users must be discoverable through Microsoft Entra ID to access the Azure Virtual Desktop, user identities that exist only in Active Directory Domain Services (AD DS) aren't supported. This includes standalone Active Directory deployments with Active Directory Federation Services (AD FS).

Hybrid identity

Azure Virtual Desktop supports hybrid identities through Microsoft Entra ID, including those federated using AD FS. You can manage these user identities in AD DS and sync them to Microsoft Entra ID using Microsoft Entra Connect.

Types of Identities (continued)

Cloud-only identity

Azure Virtual Desktop supports cloud-only identities when using Microsoft Entra joined VMs. These users are created and managed directly in Microsoft Entra ID.

You can also assign hybrid identities to Azure Virtual Desktop Application groups that host Session hosts of join type Microsoft Entra joined.

Third-party identity providers

If you're using an Identity Provider (IdP) other than Microsoft Entra ID to manage your user accounts, you must ensure that:

- Your IdP is federated with Microsoft Entra ID.
- Your session hosts are Microsoft Entra joined or Microsoft Entra hybrid joined.
- You enable Microsoft Entra authentication to the session host.

External identity

Azure Virtual Desktop currently doesn't support external identities.

Google

Selecting an authentication strategy for Azure Virtual Desktop

Selecting an authentication strategy for Azure Virtual Desktop

When connecting to a remote session, there are three separate authentication points:

- **Service authentication to Azure Virtual Desktop:** retrieving a list of resources the user has access to when accessing the client. The experience depends on the Microsoft Entra account configuration. For example, if the user has multifactor authentication enabled, the user is prompted for their user account and a second form of authentication, in the same way as accessing other services.

- **Session host:** when starting a remote session. A username and password is required for a session host, but this is seamless to the user if single sign-on (SSO) is enabled.

- **In-session authentication:** connecting to other resources within a remote session.

Service authentication

You must first authenticate to the service by signing in with a Microsoft Entra account. Authentication happens when you subscribe to a workspace to retrieve your resources and connect to apps or desktops.

Multifactor authentication

Follow the instructions in Enforce Microsoft Entra multifactor authentication for Azure Virtual Desktop using Conditional Access to learn how to enforce Microsoft Entra multifactor authentication for your deployment.

Passwordless authentication

You can use any authentication type supported by Microsoft Entra ID, such as Windows Hello for Business and other passwordless authentication options (for example, FIDO keys), to authenticate to the service.

Smart card authentication

To use a smart card to authenticate to Microsoft Entra ID, you must first configure AD FS for user certificate authentication or configure Microsoft Entra certificate-based authentication.

Role-based access control (RBAC) for Azure Virtual Desktop

Roles in Azure Virtual Desktop

Desktop Virtualization Contributor

Allows managing all your Azure Virtual Desktop resources. You also need the *User Access Administrator* role to assign application groups to user accounts or user groups. This role doesn't grant users access to compute resources..

Desktop Virtualization User

Allows users to use an application on a session host from an application group as a non-administrative user

Desktop Virtualization Host Pool Contributor

Allows managing all aspects of a host pool. You also need the *Virtual Machine Contributor* role to create virtual machines and the *Desktop Virtualization Application Group Contributor* and *Desktop Virtualization Workspace Contributor* roles to deploy Azure Virtual Desktop using the portal, or you can use the *Desktop Virtualization Contributor* role.

Desktop Virtualization Application Group Contributor

Allows managing all aspects of an application group. If you want to assign user accounts or user groups to application groups too, you also need the *User Access Administrator* role.

Roles in Azure Virtual Desktop (continued)

Desktop Virtualization Workspace Contributor

Allows managing all aspects of workspaces. To get information on applications added to a related application group, you also need the *Desktop Virtualization Application Group Reader* role.

Desktop Virtualization User Session Operator

Allows sending messages, disconnecting sessions, and using the *logoff* function to sign users out of a session host. However, this role doesn't allow host pool or session host management like removing a session host, changing drain mode, and so on. This role can see assignments, but can't modify members. We recommend you assign this role to specific host pools.

Desktop Virtualization Session Host Operator

Allows viewing and removing session hosts, and changing drain mode. This role can't add session hosts using the Azure portal because it doesn't have write permission for host pool objects.

Plan and implement Azure roles and role-based access control (RBAC) for Azure Virtual Desktop

Roles in Azure Virtual Desktop

The Azure Virtual Desktop delegated access model is based on the Azure RBAC model.

Azure Virtual Desktop delegated access supports the following values for each element of the role assignment:

Security principal

- Users
- User groups
- Service principals

Role definition

- Built-in roles
- Custom roles

Scope

- Host pools
- App groups
- Workspaces

Assign RBAC roles to the Azure Virtual Desktop service principals

Assign RBAC roles to the Azure Virtual Desktop service principals

Several Azure Virtual Desktop features require you to assign Azure role-based access control (Azure RBAC) roles to one of the Azure Virtual Desktop service principals. Features that you need to assign a role to an Azure Virtual Desktop service principal include:

- Autoscale.
- Start VM on Connect.
- App attach (when using Azure Files and your session hosts joined to Microsoft Entra ID).

Depending on when you registered the `Microsoft.DesktopVirtualization` resource provider, the service principal names begin with either *Azure Virtual Desktop* or *Windows Virtual Desktop*.

Azure Virtual Desktop service principals

You can make sure you're assigning roles to the correct service principal by checking its application ID. The application ID for each service principal are as follows:

Service principal	Application ID
Azure Virtual Desktop Windows Virtual Desktop	9cdead84-a844-4324-93f2-b2e6bb768d07
Azure Virtual Desktop Client Windows Virtual Desktop Client	a85cf173-4192-42f8-81fa-777a763e6e2c
Azure Virtual Desktop ARM Provider Windows Virtual Desktop ARM Provider	50e95039-b200-4007-bc97-8d5790743a63

Enforce Microsoft Entra multifactor authentication for Azure Virtual Desktop using Conditional Access

Enforce Microsoft Entra multifactor authentication for Azure Virtual Desktop

Users can sign into Azure Virtual Desktop from anywhere using different devices and clients.

- Using Microsoft Entra multifactor authentication (MFA) with Azure Virtual Desktop prompts users during the sign-in process for another form of identification in addition to their username and password.
- You can enforce MFA for Azure Virtual Desktop using Conditional Access and configure whether it applies to the web client, mobile apps, desktop clients, or all clients.
- When a user connects to a remote session, they need to authenticate to the Azure Virtual Desktop service and the session host.
- If MFA is enabled, it's used when connecting to the Azure Virtual Desktop service and the user is prompted for their user account and a second form of authentication, in the same way as accessing other services.
- When a user starts a remote session, a username and password is required for the session host, but this is seamless to the user if single sign-on (SSO) is enabled.

Using Azure Virtual Desktop with Microsoft Intune

Using Azure Virtual Desktop with Microsoft Intune

Device configuration support in Microsoft Intune for Windows 10 or Windows 11 Enterprise multi-session is Generally Available (GA).

- Policies defined in the OS scope and apps configured to install in the system context can be applied to Azure Virtual Desktop multi-session VMs.
- Multi-session configurations can be targeted to devices or device groups.

User configuration support in Microsoft Intune for Windows 11 multi-session VMs allow you to:

- Configure user scope policies using **Settings catalog** and assign to groups of users. You can use the search bar to search all configurations with scope set to "user".
- Configure user certificates and assign to users.
- Configure PowerShell scripts to install in the user context and assign to users.

Knowledge check

Knowledge check

What role should be assigned to allow a user to manage all aspects of Azure Virtual Desktop host pools, including access to resources?

Choices:

1. Application Group Reader
2. Host Pool Contributor
3. Workspace Contributor

Knowledge check

A system administrator needs to view and remove session hosts and change drain mode in a Desktop Virtualization environment. Which role should be assigned to the administrator?

Choices:

1. Desktop Virtualization Virtual Machine Contributor
2. Desktop Virtualization Power On Contributor
3. Desktop Virtualization Session Host Operator

Knowledge check

A system administrator is tasked with managing all aspects of a host pool in Azure Virtual Desktop. Which role should the administrator be assigned to successfully complete this task?

Choices:

1. Desktop Virtualization Workspace Contributor
2. Desktop Virtualization User
3. Desktop Virtualization Host Pool Contributor

Knowledge check

A system administrator is tasked with setting up authentication for Azure Virtual Desktop. They need to ensure that users can authenticate using a smart card. Which of the following steps should they take?

Choices:

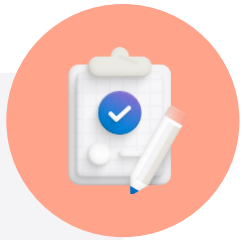
1. Configure AD FS for user certificate authentication and enable single sign on

2. Enable passwordless authentication and configure Microsoft Entra certificate based authentication

3. Configure AD FS for user certificate authentication or configure Microsoft Entra certificate based authentication

Summary

Summary



What you learned:

- Select an identity strategy for Azure Virtual Desktop
- Select an authentication strategy for Azure Virtual Desktop
- Describe Role-based access control (RBAC) for Azure Virtual Desktop
- Plan and implement Azure roles and role-based access control (RBAC) for Azure Virtual Desktop
- Assign RBAC roles to the Azure Virtual Desktop service principals
- Enforce Microsoft Entra MFA for Azure Virtual Desktop using Conditional Access