CHAPTER 4

Manage Access and Security to Azure Virtual Desktop

The previous chapter took a deeper look into implementing and managing an Azure Virtual Desktop Architecture, including implementing and managing networking for Azure Virtual Desktop, implementing and managing storage for Azure Virtual Desktop, creating and configuring hostpools and sessions hosts, and creating and managing session host images.

This chapter covers the following main topics:

- Managing access to Azure Virtual Desktop
- Managing security to Azure Virtual Desktop
- Knowledge check

Technical Requirements

To complete the exercises in this book, you need to have access to a Microsoft 365 tenant. This can be attained by signing up for a trial subscription. Additionally, Azure Virtual Desktop services require one of the following licenses:

- Microsoft 365 Business Premium
- Microsoft 365 E5/E3
- Microsoft 365 A3/A5/Student Benefits
- Microsoft 365 F3

S. Darr, *Azure Virtual Desktop Specialist*, https://doi.org/10.1007/978-1-4842-7987-8_4

- Windows 10 Enterprise E3/E5
- Windows 10 Education A3/A5
- Windows 10 VDA per user

Managing Access to Azure Virtual Desktop

Microsoft cloud services that are hosted in Azure utilize role-based access control (RBAC), including Azure Virtual Desktop. RBAC allows you to give access to users depending on their role.

Azure has its standard built-in roles such as Owner, Contributor, and Reader; however, there are additional roles that are more specific to Azure Virtual Desktop. This section discusses these roles and the level of access they grant a user who is assigned the specific role.

Built-in Roles for Azure Virtual Desktop

The following built-in RBAC roles are specific to Azure Virtual Desktop and have different levels of access.

- **Desktop Virtualization Contributor**: This role allows you to handle and manage all areas of your Azure Virtual Desktop deployment. If you want to publish app groups to users or groups, you also need to assign the User Access Administrator with this role. This role will not enable you to access any of the compute resources. The following list shows the exact permissions that this role will grant you:
    - Microsoft.DesktopVirtualization/*
    - Microsft.Resources/Subscriptions/resourceGroups/read
    - Microsft.Resources/deployments/*
    - Microsoft.Authorizations/*/read
    - Microsoft.Insights/alertRules/*
    - Microsoft.Support/*

- **Desktop Virtualization Reader:** If you assign this role to a member of the admin team, they will be able to view everything in the Azure Virtual Desktop deployment; however, they will not be able to make any changes. The following list shows the exact permissions that this role will grant you:
  - Microsoft.DesktopVirtualization/*/read
  - Microsoft.Resources/Subscriptions/resourceGroups/read
  - Microsoft.Resources/deployments/read
  - Microsoft.Authorizations/*/read
  - Microsoft.Insights/alertRules/*
  - Microsoft.Support/*
- **Desktop Virtualization Hostpool Contributor:** This role will enable you to manage all areas of the hostpool as well as access all the resources. If you want to create virtual machines as part of this, you will additionally need the Virtual Machine Role Contributor role. If you want to create hostpools using the Azure Admin Portal, you need to assign the AppGroup and Workspace contributor roles, or the Desktop Virtualization Contributor role. The following list shows the permissions that this role will enable for you:
  - Microsoft.DesktopVirtualization/Hostpools/*
  - Microsoft.Resources/subscriptions/resourceGroups/read
  - Microsoft.Resources/deployments/*
  - Microsoft.Authorization/*/read
  - Microsoft.Insights/alertRules/*
  - Microsoft.Support/*
- **Desktop Virtualization Hostpool Reader:** This is a read-only role that will not allow the admin user to make any amendment; however it does allow them to view the entire hostpool. The following list shows the permissions that this role will enable for you:

    - Microsoft.DesktopVirtulization/Hostpools/*/read
    - Microsoft.Resources/subscriptions/resourceGroups/read
    - Microsoft.Resources/Deployments/read
    - Microsoft.Authorization/*/read
    - Microsoft.Insights/alertRules/*
    - Microsoft.Support/*
- **Desktop Virtualization Application Group Contributor:** If you assign this role to an administrator, it will enable them to manage all areas of app groups. You need to assign the User Access Administrator role if you want the same user to be able to publish app groups. The following list shows the permissions that this role will enable for you:
    - Microsoft.DesktopVirtualization/applicationgroups/*
    - Microsoft.DesktopVirtualization/hostpools/read
    - Microsoft.DesktopVirtualization/hostpools/sessionhosts/read
    - Microsoft.Resources/subscriptions/resourceGroups/read
    - Microsoft.Resources/deployments/*
    - Microsoft.Authorization/*/read
    - Microsoft.Insights/alertRules/*
    - Microsoft.Support/*
- **Desktop Virtualization Application Group Reader:** Assigning this role to an administrator will allow them to read all areas within an app group; however they cannot make changes. The following list shows the permissions that this role will enable for you:
    - Microsoft.DesktopVirtualization/applicationgroups/*/read
    - Microsoft.DesktopVirtualization/applicationgroups/read
    - Microsoft.DesktopVirtualization/hostpools/read
    - Microsoft.DesktopVirtualization/hostpools/sessionhosts/read

    - Microsoft.Resources/subscriptions/resourceGroups/read
    - Microsoft.Resources/deployments/read
    - Microsoft.Authorization/*/read
    - Microsoft.Insights/alertRules/*
    - Microsoft.Support/*
- **Desktop Virtualization Workspace Contributor:** This role will enable you to fully access and manage all areas of the workspace. You will need to assign the Application Group Reader role to the user if they require information on the application group. The following list shows the permissions that this role will enable for you:
    - Microsoft.DesktopVirtualization/workspaces/*
    - Microsoft.DesktopVirtualization/applicationgroups/read
    - Microsoft.Resources/subscriptions/resourceGroups/read
    - Microsoft.Resources/deployments/*
    - Microsoft.Authorization/*/read
    - Microsoft.Insights/alertRules/*
    - Microsoft.Support/*
- **Desktop Virtualization Workspace Reader:** This role will enable you to read/view all aspects of the workspace; however you cannot modify any resources. The following list shows the permissions that this role will enable for you:
    - Microsoft.DesktopVirtualization/workspaces/read
    - Microsoft.DesktopVirtualization/applicationgroups/read
    - Microsoft.Resources/subscriptions/resourceGroups/read
    - Microsoft.Resources/deployments/read
    - Microsoft.Authorization/*/read
    - Microsoft.Insights/alertRules/*
    - Microsoft.Support/*

- **Desktop Virtualization User Session Operator:** This role enables you to send messages, disconnect sessions, and log users off from the Azure Virtual Desktop Portal. This role does not give you permission to manage session home management, for example deleting a session host from the hostpool and enabling/disabling drain mode. The user who is assigned this role can view assignments, but they will not be able to amend admins. It is recommended to assign this role to a hostpool. The following list shows the permissions that this role will enable for you:
  - Microsoft.DesktopVirtualization/hostpools/read
  - Microsoft.DesktopVirtualization/hostpools/sessionhosts/read
  - Microsoft.DesktopVirtualization/hostpools/sessionhosts/usersessions/*
  - Microsoft.Resources/subscriptions/resourceGroups/read
  - Microsoft.Resources/deployments/read
  - Microsoft.Authorization/*/read
  - Microsoft.Insights/alertRules/*
  - Microsoft.Support/*
- **Desktop Virtualization Session Host Operator:** This role will enable you to see and delete session hosts and can enable/disable drain mode. Users need to have writer permissions to hostpool objects if they want to be able to add session hosts. You can add sessions hosts if you are assigned the Virtual Machine Contributor role (as long as the registration token is still valid). The following list shows the permissions that this role will enable for you:
  - Microsoft.DesktopVirtualization/hostpools/read
  - Microsoft.DesktopVirtualization/hostpools/sessionhosts/*
  - Microsoft.Resources/subscriptions/resourceGroups/read
  - Microsoft.Resources/deployments/read
  - Microsoft.Authorization/*/read

- Microsoft.Insights/alertRules/*
- Microsoft.Support/*

This section discussed RBAC roles that are specific to Azure Virtual Desktop. The next section is a lab exercise to assign a role to an Azure Virtual Desktop service via the Azure Portal and PowerShell.

Assigning Role-Based Assignment to Azure Virtual Desktop

The following two lab exercises walk you through how to assign roles via the Azure Portal and via PowerShell.

Assign Role-Based Assignment via Admin Center

The following lab walks through the steps to assign a role to an Azure Virtual Desktop resource.

1. Open a web browser and go to the Azure Portal via `https://portal.azure.com`.
2. Navigate to the Azure Virtual Desktop platform by typing it in the search box and selecting it from the list that appears. See Figure 4-1.

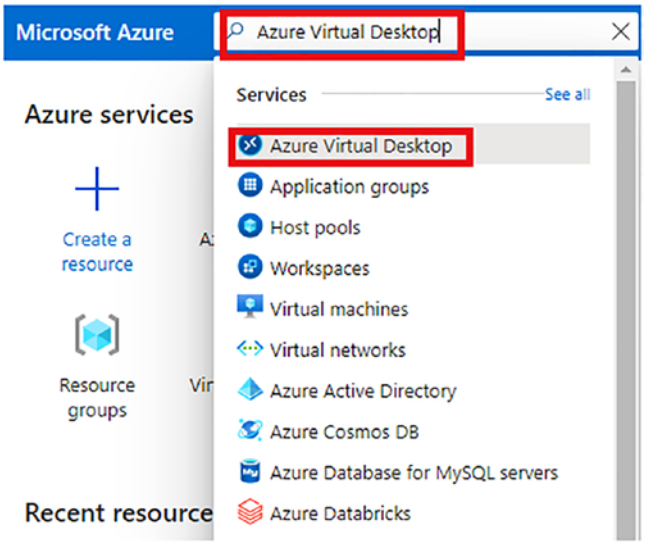

Figure 4-1. *Navigate to the Azure Virtual Desktop service in the portal*

3. In this example, we are going to assign a role to the hostpool, so we need to navigate to the hostpool section. If you want to assign a specific role to another resource (application groups or workspaces, for example), you need to navigate to those sections.

4. In the Hostpool menu, select Access Control (IAM). See Figure 4-2.

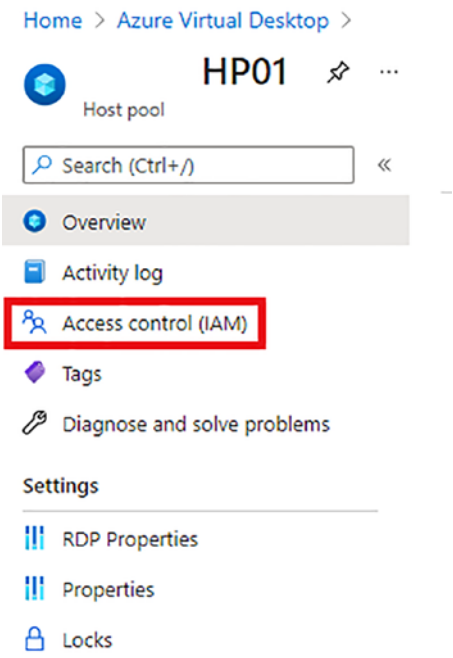

Figure 4-2. *Navigate to Access Control (IAM) section of Azure Virtual Desktop*

5. On the Access Control page, click the +Add option, as shown in Figure 4-3.

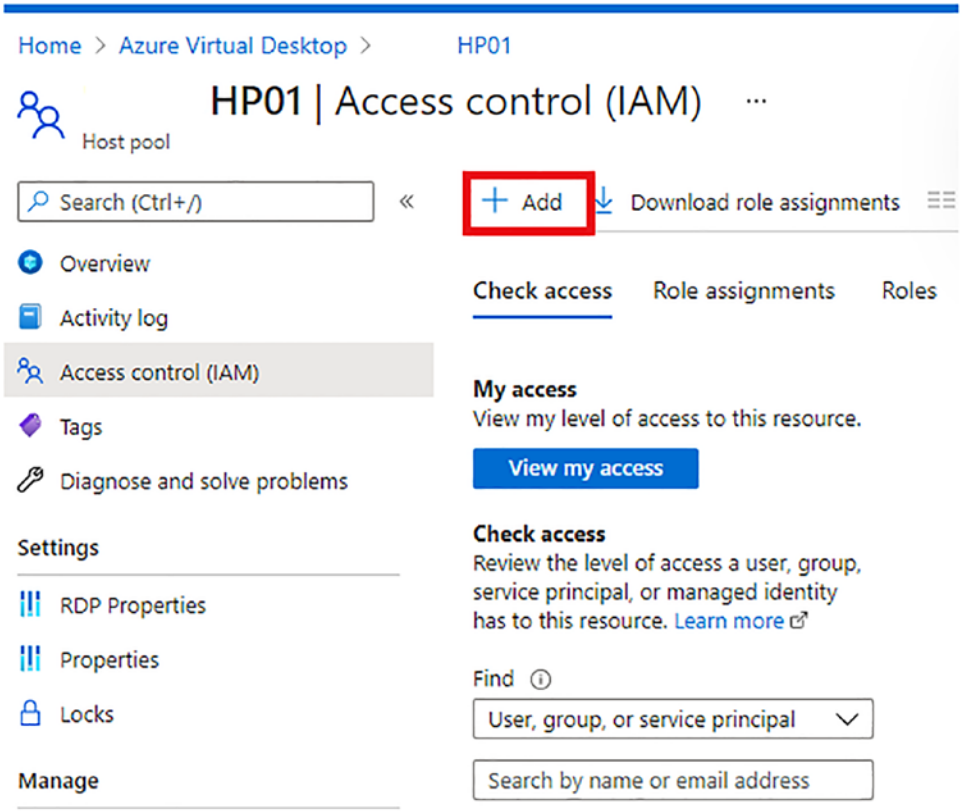

Figure 4-3. *Click Add*

6. Select Add Role Assignment, as shown in Figure 4-4.

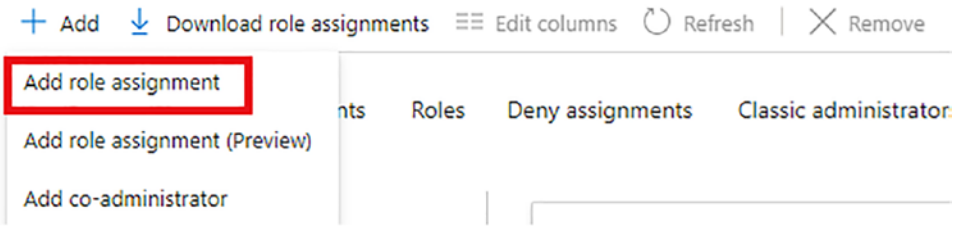

Figure 4-4. *Add Role Assignment*

7. In the Add Role Assignment section, in the Role text field, type ***desktop virtualization hostpool*** to show all the hostpool-related roles. See Figure 4-5.

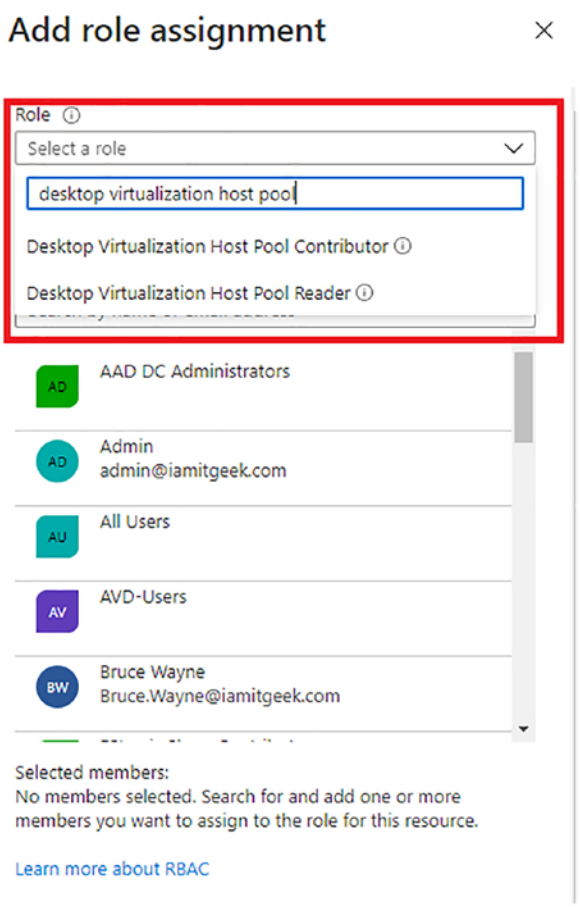

Figure 4-5. *Select the relevant role*

8. In this example, you assign the Desktop Virtualization Hostpool Contributor to an administrator account. Click Save.

Assign Role-Based Assignment via PowerShell

In this exercise, you learn how to assign a role via PowerShell:

1. Log in to Azure via PowerShell. Follow the instructions at `https://docs.microsoft.com/en-us/powershell/azure/authenticate-azureps?view=azps-6.4.0`.

2. Ensure you understand the specific role you want to grant access to. You can list the roles and get specific role IDs by using the cmdlet shown in Figure 4-6.

```
PS C:\WINDOWS\system32> Get-AzRoleDefinition | FT Name, IsCustom, Id
```

Figure 4-6. *Get a list of Azure roles and document the specific one you want to grant access to*

3. In this example, we will pick the Desktop Virtualization Application Group Reader role to a user, which is shown in Figure 4-7.

```
Desktop Virtualization Application Group Reader              False aebf23d0-b568-4e86-b8f9-fe83a2c6ab55
```

Figure 4-7. *Desktop Virtualization Application Group Reader Role in PowerShell*

4. There are different levels of scope you can assign permissions to, including:
   - **Resource scope:** You need the resource ID for this, which can be found in the properties of the resource in the Azure Portal.
   - **Resource group scope:** You need the name of the resource group for this, which can be found on the Resource Group page.
   - **Subscription scope:** You need the subscription ID, which can be found on the Subscriptions page.
   - **Management group scope:** You need the management group name, which can be found on the Management Groups page.

   In this example, we will assign the Desktop Virtualization Application Group Reader role to an admin user and specify the Application Group Resource.

5. Complete the cmdlet in Figure 4-8 to assign the Desktop Virtualization Application Group Reader to an admin user, scoped to the Application Group resource.

```
PS C:\WINDOWS\system32> New-AzRoleAssignment -SignInName shabaz@iamitgeek.com `
>> -RoleDefinitionName "Desktop Virtualization Application Group Reader" `
>> -ResourceName                -AppGroup `
>> -ResourceType Microsoft.DesktopVirtualization/applicationgroups `
>> -ResourceGroupName ITGEEKRG03
```

Figure 4-8. *New Role Assignment cmdlet*

This section discussed role-based access control (RBAC) and how you can use it to plan and implement roles for Azure Virtual Desktop. You also completed the lab exercises, which walk through how to assign roles to Azure Virtual Desktop via the Azure Center and via PowerShell.

The next section discusses delegated access in Azure Virtual Desktop and explains how you can configure user restrictions by utilizing Azure AD group policies and AD policies with Intune integration.

Delegated Access in Azure Virtual Desktop

When you utilize the delegated access model with Azure Virtual Desktop, it allows you to define the amount of access specific users can have by assigning them a specific role. There are three main components of a role assignment: security principal, role definition, and scope.

The following values are supported for each element when configuring delegated access for Azure Virtual Desktop:

- Security principal
  - Users
  - User groups
  - Service principals
- Role definition
  - Built-in roles
  - Custom roles
- Scope
  - Hostpools
  - App groups
  - Workspaces

In the following labs, we walk through how to add an Azure AD user to an app group via the Azure Portal and via PowerShell.

Add an Azure AD User to an Application Group via Azure Admin Center

1. Log in to the Azure Admin Center at `https://portal.azure.com` and navigate to the Azure Virtual Desktop services page.
2. Navigate to Application Groups, as shown in Figure 4-9.

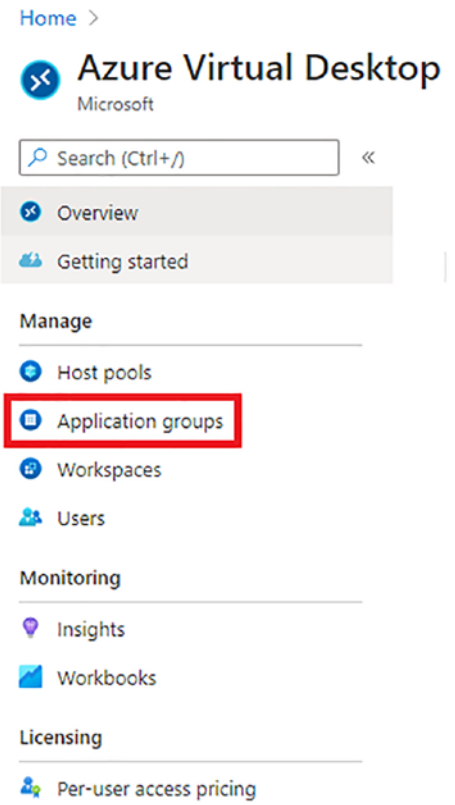

Figure 4-9. *Navigate to Application Groups*

3. Select the relevant application group you want to assign users or groups to, as shown in Figure 4-10.

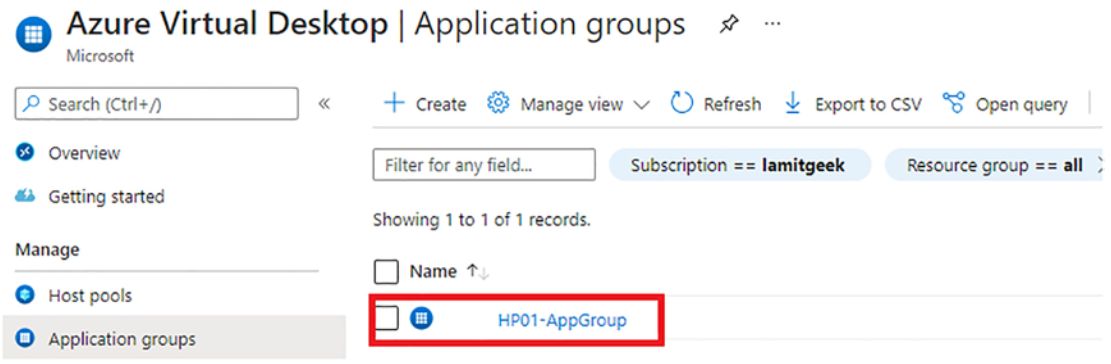

Figure 4-10. *Select the relevant application group*

4. On the Application Group page, navigate to Manage ➤ Assignments, as shown in Figure 4-11.

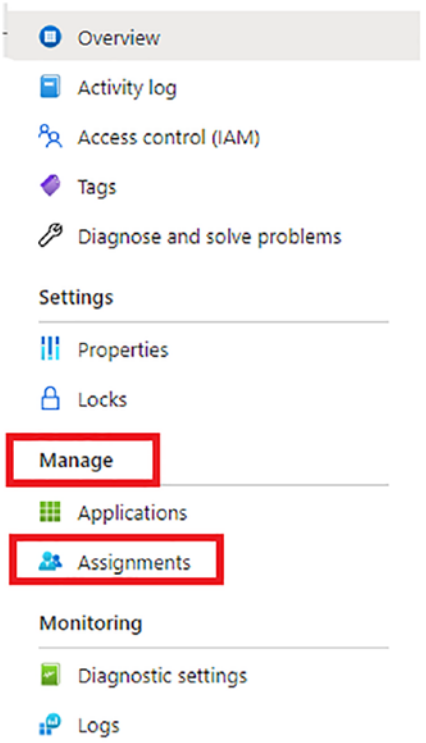

Figure 4-11. *Navigate to Assignments page*

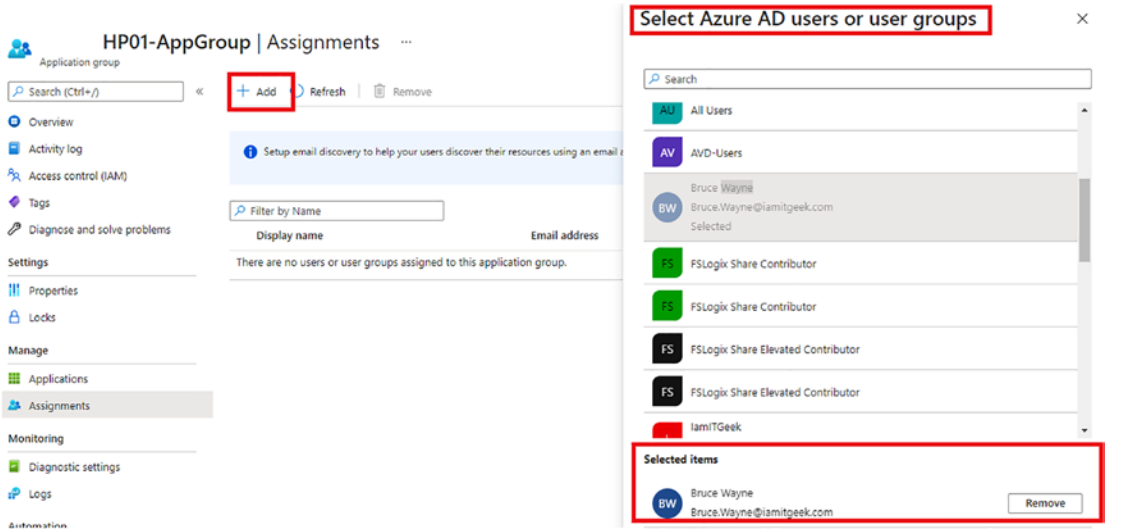

Figure 4-12. *Add a user/group assignment to an application group*

5. Click the +Add button and then select the user or group you want to assign permissions to in the application group. Click Select. See Figure 4-11.

Add an Azure AD User to an Application Group via PowerShell

1. First you need to set up the PowerShell module on your computer for Azure Virtual Desktop. Run the cmdlet shown in Figure 4-13 in an elevated PowerShell window to install the relevant module.

```
PS C:\WINDOWS\system32> Install-Module -Name Az.DesktopVirtualization
```

Figure 4-13. *Install Azure Virtual Desktop module for PowerShell*

2. Run the cmdlet shown in Figure 4-14 to connect to Azure via PowerShell. You will be prompted to enter your global admin credentials.

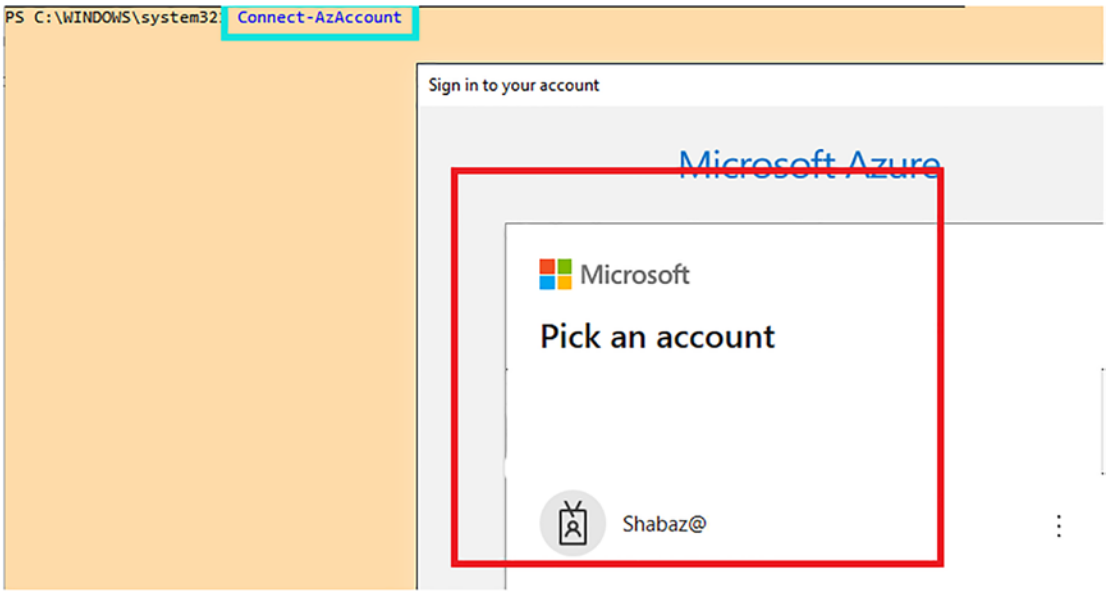

Figure 4-14. *Connect to Azure via PowerShell cmdlet*

3. Run the cmdlet shown in Figure 4-15 to grant user access to the application group.

```
PS C:\WINDOWS\system32> New-AzRoleAssignment -SignInName shabaz@i          -RoleDefinitionName "Desktop Virtualization User" -ResourceName
          -AppGroup -ResourceGroupName ITGEEKRG03 -ResourceType 'Microsoft.DesktopVirtualization/applicationGroups'
```

Figure 4-15. *Configure assignment to an application group via PowerShell*

This section discussed delegated access and completed lab exercises to assign access to an application group via the Azure Portal and PowerShell. The next section discusses how you can configure user restrictions by utilizing Azure AD group policies and AD policies with Intune integration.

Azure Virtual Desktop Integration with Intune

Azure Virtual Desktop is called a DaaS (Desktop as a Service) platform in which you can virtualize applications and Windows Desktops. Integrating this platform with Intune enables you to manage and secure the session hosts by utilizing policies once they are enrolled.

At the present, Intune integration supports the following Azure Virtual Desktop VM scenarios:

- Session hosts running Windows 10 Enterprise, version 1809 (or later)
- Session hosts need to be hybrid Azure AD joined (See more at https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-plan)
- Personal hostpool registered session hosts
- Intune enrolled. You can use one of the following methods to accomplish this:
  - Auto enroll devices by utilizing Group policy (Hybrid Azure AD Join)
  - Co-management with Config Manager (see more at https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview)
  - Azure AD join with user self-enrollment (see more at https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-methods#user-self-enrollment-in-intune)
  - Enable the feature to enroll the VM with Intune in the Azure Portal (see more at https://docs.microsoft.com/en-us/azure/virtual-desktop/deploy-azure-ad-joined-vm#deploy-azure-ad-joined-vms)

This section discussed various topics related to managing access to Azure Virtual Desktop, including built-in roles, assigning RBAC roles, delegating roles, and integration with Intune. The next section discusses how to manage security with Azure Virtual Desktop.

Managing Security on Azure Virtual Desktop

To manage security on your Azure Virtual Desktop, you first need to understand the responsibility model, as it is important to understand that Microsoft takes responsibility for securing specific services.

Table 4-1 outlines the Azure Virtual Desktop specific services that are managed by Microsoft.

Table 4-1. *Azure Virtual Desktop Microsoft Managed Services*

Service	Description
Web Access	Allows users to access the application group resources (desktop or remoteapp) via an HTMLv5-compatible Internet browser.
Gateway	Connects remote user's connection to a gateway, then creates a connection from the virtual machine back to the same gateway.
Broker	Allows load-balancing and facilitates reconnections to the application group resources (desktop and remoteapp).
Diagnostics	Allows event logs of actions on the AVD deployment as success or failure. Useful for troubleshooting
Infrastructure services (Azure)	Networking, storage, and other compute services in Azure are managed by Microsoft.

Table 4-2 outlines the Azure Virtual Desktop-specific components that are managed by the end users/clients.

Table 4-2. *Azure Virtual Desktop Client Managed Services*

Component	Description
End user profile management	Azure Files integration with FSLogix enables a containerized user profile experience.
End user host access	There are two types of load-balancing algorithms—depth and or breadth—which are defined when the hostpool is created.
Virtual machine scaling and sizing	Sizing components for virtual machines, including GPU-enabled VMs.
Policies for scaling	VMs (session hosts) can be load-balanced using scale sets.
Policies for networking	The consumer/client is required to create Network Security Groups (NSGs) that filter network traffic.

Ensuring secure access to the Azure Virtual Desktop environment is an essential part of the deployment, and it will also be important for the exam. Azure Active Directory allows you to configure Conditional Access policies and Multi-Factor Authentication (MFA) integration with the Azure Virtual Desktop platform, which creates an additional layer of security.

This section covered the responsibility model from an Azure Virtual Desktop perspective, which highlights the services that Microsoft manages and the services that the end consumer is required to manage. We will not look at securing Azure Virtual Desktop with Conditional Access Policies.

Configuring a Conditional Access Policy to Enable MFA

In the following lab exercise, we walk through how to configure a Conditional Access policy that will enforce the end user to register to MFA. They must use this whenever they connect to the Azure Virtual Desktop environment.

1. Log in to the Azure Portal at `https://portal.azure.com` with an account that is assigned one of the following roles:
   - Global Administrator
   - Security Administrator
   - Conditional Access Administrator
2. Navigate to Azure Active Directory ➤ Security ➤ Conditional Access, as shown in Figure 4-16.

Figure 4-16. *Navigate to Conditional Access Polices in Azure AD*

3. Click on + New Policy, as shown in Figure 4-17.

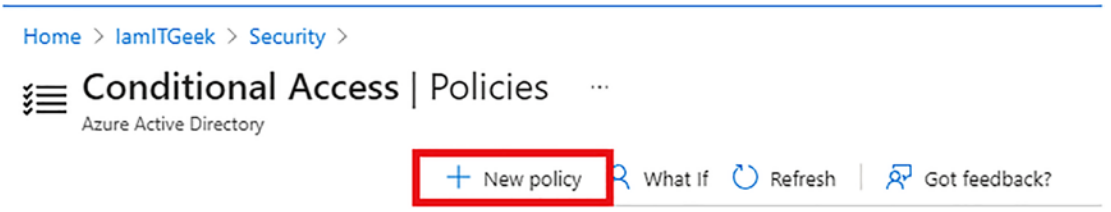

Figure 4-17. *Create a new conditional access policy*

4. In the Name field, give the policy an appropriate name.
5. *In* the Assignments - User and Groups field, select the users or groups you want this policy to be applicable to. See Figure 4-18.

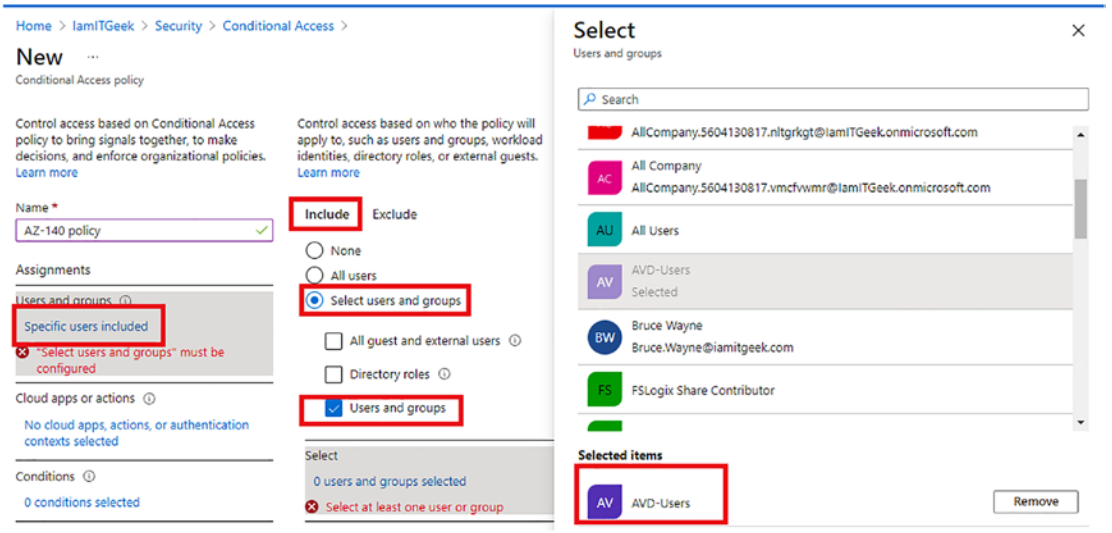

Figure 4-18. *Assign permissions to a user or group*

6. Choose Cloud Apps or Actions ➤ Include ➤ Select Apps. At this point you need to search for one of the following Azure Virtual Desktop apps if you are using the Classic version:
   - Azure Virtual Desktop (App ID 5a0aa725-4958-4b0c-80a9-34562e23f3b7)
   - Azure Virtual Desktop Client (App ID fa4345a4-a730-4230-84a8-7d9651b86739), which will let you set policies on the web client

Otherwise, you can search for the Windows Virtual Desktop app if you're using the Azure Resource Manager (ARM) version. See Figure 4-19.

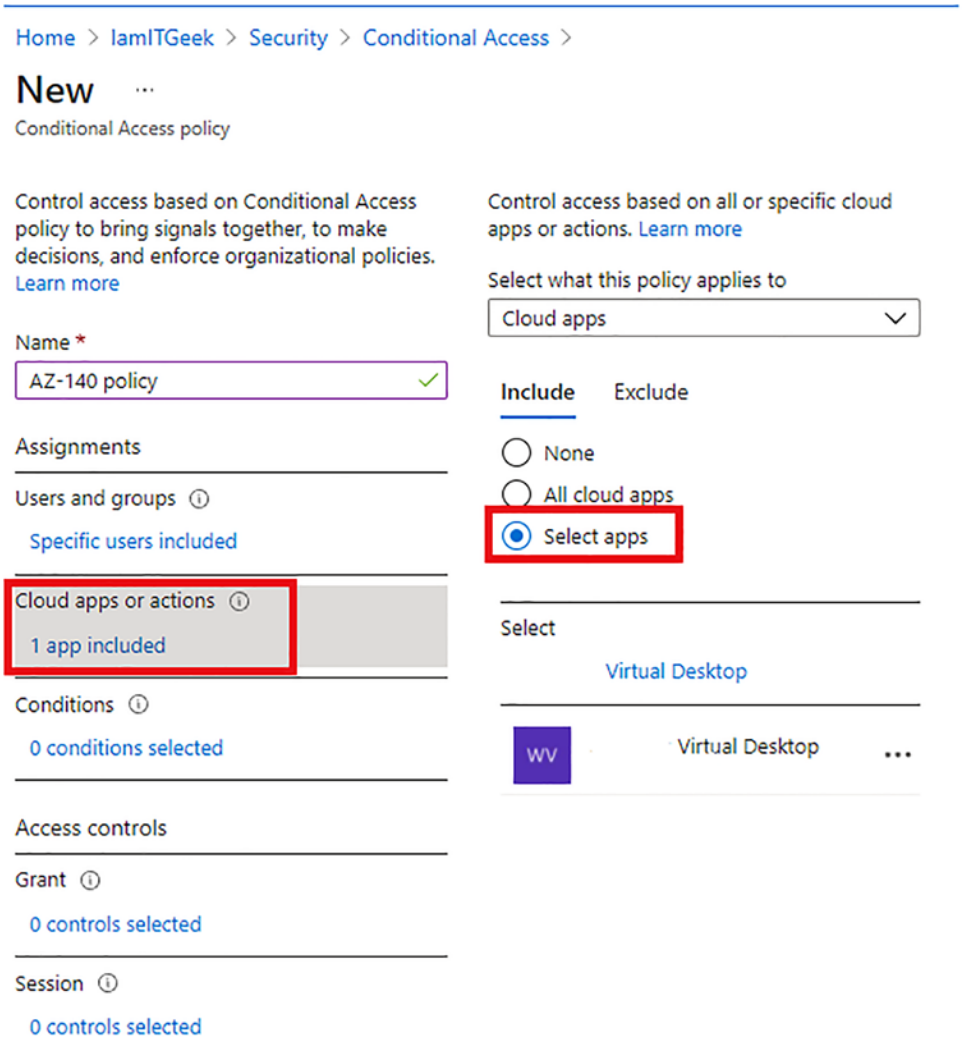

Figure 4-19. *Assign the Azure Virtual Desktop App to this policy*

7. Choose Conditions ➤ Client Apps. Click Yes on Configure and then ensure that only Mobile Apps and Desktop Clients is selected, as shown in Figure 4-20.

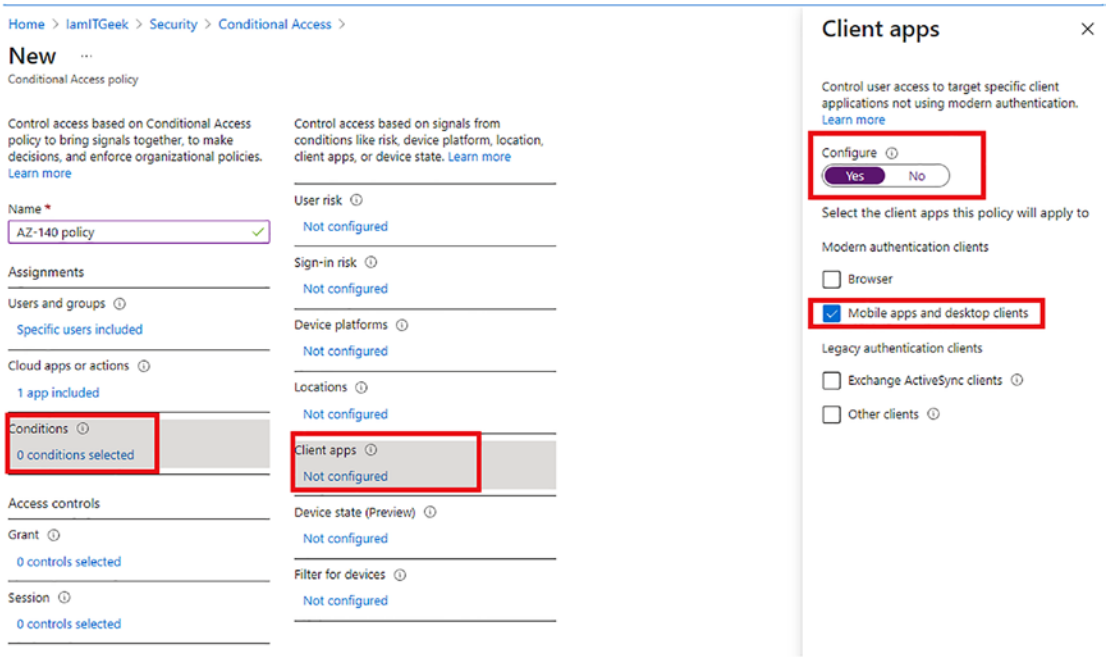

Figure 4-20. *Configure Client App conditions*

8. Under Access Controls, choose Grant Access and ensure you tick Require Multi-Factor Authentication. See Figure 4-21.

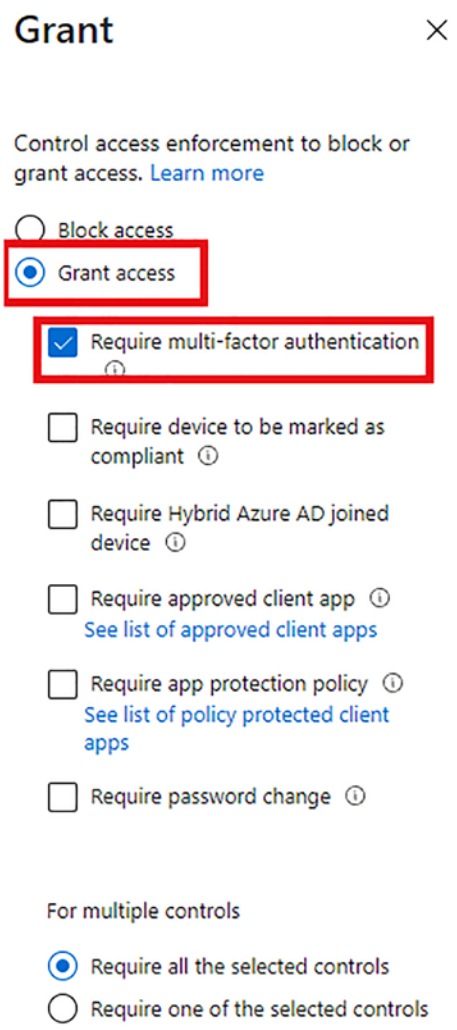

Figure 4-21. *Configure grant access controls*

9. Choose Session under Access Controls and tick the box next to Sign-in Frequency. You can then decide how much time you want to set between users being promoted for MFA authentication. In this example, we set it to five days. See Figure 4-22.

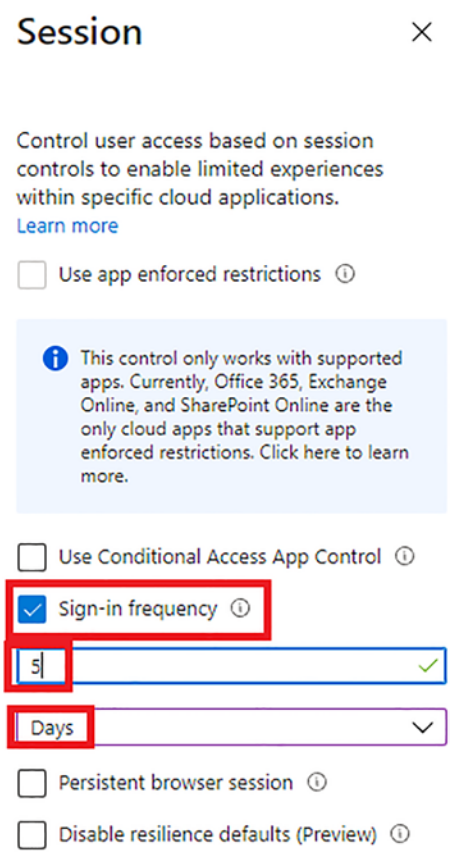

Figure 4-22. *Set the session time limit*

10. Once you have configured the policy, make sure you select On to turn the policy on. Then click Create at the bottom of the page; see Figure 4-23.

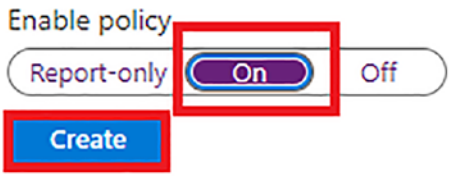

Figure 4-23. *Enable and create the policy*

This section included a lab exercise to enable MFA by configuring a Conditional Access policy. The next section covers some security best practices for Azure Virtual Desktop.

Azure Virtual Desktop Security Best Practices

There are multiple security controls that are built into the Azure Virtual Desktop platform. This section discusses what they are and how they integrate into this service.

Multi-Factor Authentication

In the previous section, you completed a lab exercise to configure multi-factor authentication. Making this a requirement for all users who are accessing Azure Virtual Desktop is an essential security best practice.

Configure Conditional Access

Conditional access policies will enable admins to control and manage risk before users can access the platform. It is recommended that you think about who the users are, how they are logging in, and the device users are connecting from before you give them access to the Azure Virtual Desktop platform.

Audit Logs

You can monitor admin activity associated with the Azure Virtual Desktop environment when you enable audit log collections. The following are some of the audit logs you can utilize:

- Key Vault logs (https://docs.microsoft.com/en-us/azure/key-vault/general/logging)
- Azure Activity log (https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log)
- Azure Virtual Desktop Diagnostic log (https://docs.microsoft.com/en-us/azure/virtual-desktop/diagnostics-log-analytics)
- Azure Active Directory Activity log (https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-activity-logs-azure-monitor)
- Session Hosts (https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agent-windows)

- Active Directory (https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis)

Utilize Azure Monitor

You can view your Azure Virtual Desktop service usage and its availability with Azure Monitor. You can receive notifications by configuring service health alerts for Azure Virtual Desktop. The following link provides further information on the Azure Monitor service: https://azure.microsoft.com/services/monitor/.

Utilize RemoteApps

There are two deployment model options with Azure Virtual Desktop—providing access to a full virtual desktop or to specific apps. You can deliver a seamless experience with remoteapps and reduce risk, as you are only exposing the specific application instead of a full Windows OS desktop.

This section discussed Azure Virtual Desktop security best practices. In the following section we look at specific session host security best practices.

Security Best Practices: Session Hosts

Session hosts are made up of Windows-based virtual machines that are connected to a virtual network. All these resources then sit in an Azure Subscription, which allows you to integrate Azure Virtual Desktop with several other security services.

The security of this environment is dependent on the controls and policies that are implemented on the session hosts. The following components should be integrated with this platform to ensure you are following best practices.

Endpoint Detection and Response

As with an on-premises computer, it is a recommendation that you deploy some type of endpoint protection software that has endpoint detection and response (EDR) capabilities on your session hosts. If you are deploying a Windows Server OS onto your session hosts, you can enable Azure Security Center (https://docs.microsoft.com/en-us/azure/security-center/security-center-services). You can also enable EDR, which will implement Defender ATP.

Endpoint Protection

It is a recommendation to enable endpoint protection on each session host. You have the choice of configuring a third-party tool or enabling Windows Defender Anti-Virus.

Patch Management

In the scenario in which a vulnerability has been identified, you have to ensure you patch it. The same rule should be utilized when managing virtual cloud environments like Azure Virtual Desktop. You should ensure that you have a reliable, strict, and robust patch-management policy for your environment that covers the OS and any applications on the session hosts.

This section discussed Azure Virtual Desktop security best practices and session host security best practices. In the next session, we take a closer look at securing Windows Virtual Desktop environments with Azure Security Center integration.

Azure Security Center Integration with AVD

Azure Security Center offers the following capabilities that cover the security posture and threat protection for Azure Virtual Desktop virtual machines:

- Adaptive application controls
- Secure score assessment
- Secure configuration assessment
- Vulnerability assessment
- Just-in-time (JIT) virtual machine access
- File integrity monitoring
- Host-level detections
- Agentless cloud network micro-segmentation and detections

Table 4-3 outlines the Azure Virtual Desktop security requirements and the Azure Security Center security and threat protection capabilities associated with it.

Table 4-3. *Azure Virtual Desktop Security Requirements*

Azure Virtual Desktop Requirements	Azure Security Center Security Capabilities	Azure Security Center Threat Protection Capabilities
Identity	Configuration assessment and secure score	Agentless cloud network micro-segmentation and detection
Network Security	Just-in-time (JIT) VM access Configuration assessment and secure score	Agentless cloud network micro-segmentation and detection
App Security	Vulnerability assessment File integrity monitoring Adaptive application control	Host-level detections
Configuration	Secure configuration assessment Secure score assessment	N/A
Session Host OS	Vulnerability assessment	Host-level detection

This section looked at the different security requirements for Azure Virtual Desktop and security best practices for session hosts. The next section includes a lab exercise that you use to enable Azure Security Center for Azure Virtual Desktop.

Enabling Azure Security Center for Azure Virtual Desktop

There are two tiers of Azure Security Center—the free tier and the standard tier. The free tier offers security suggestions and Secure Score for Azure Virtual Desktop; however, for this lab exercise, you need the standard tier.

The following lab exercise walks through enabling Azure Security Center for Azure Virtual Desktop:

1. Navigate to the Security Center service page by typing **Security Center** in the Azure Search bar at the top of the screen, as shown in Figure 4-24.

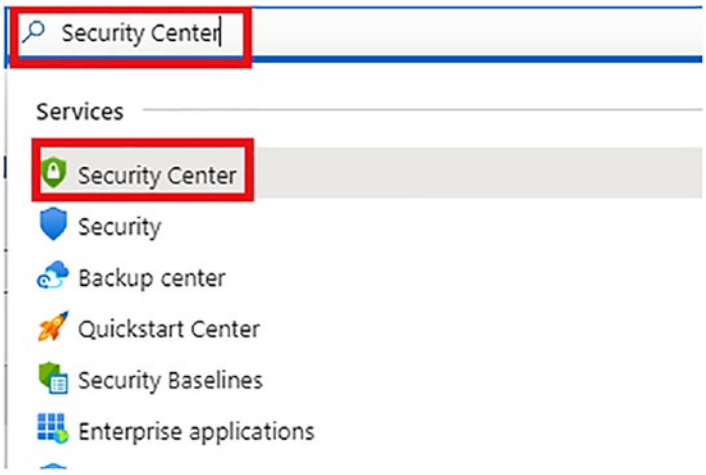

Figure 4-24. *Navigate to Azure Security Center*

2. Ensure the Standard Tier plan is enabled by navigating to Security Center ➤ Settings and clicking your trial subscription. See Figure 4-25.

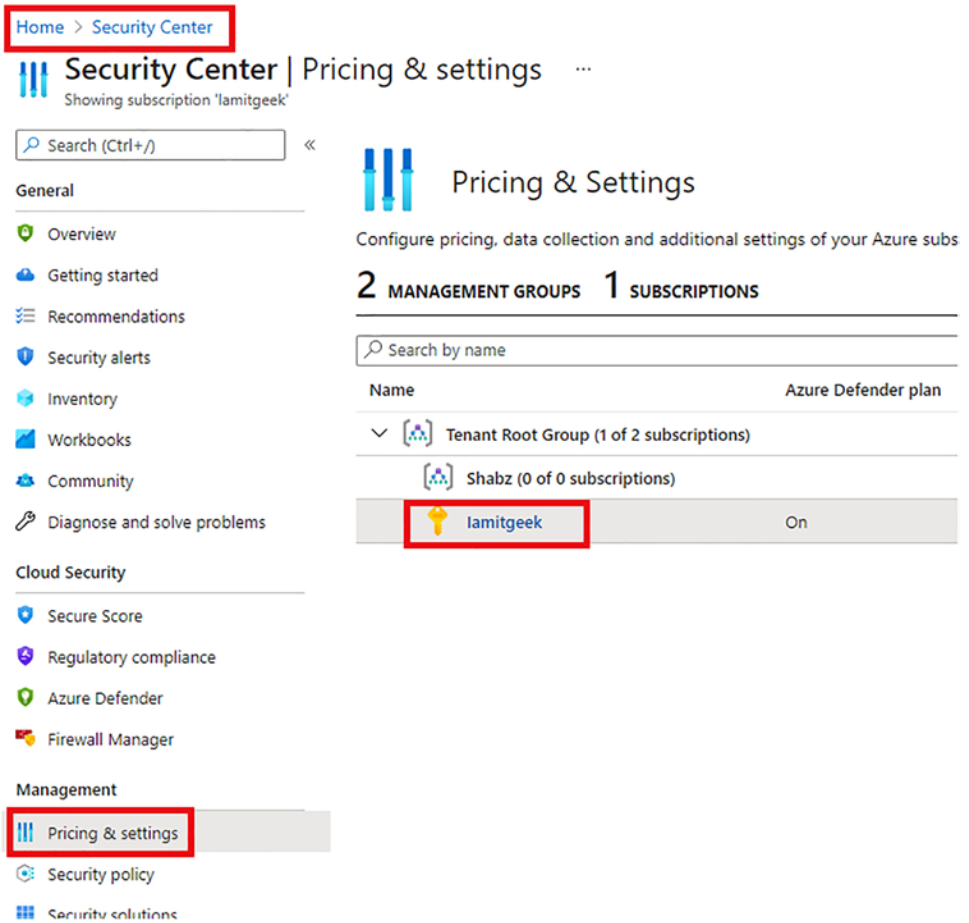

Figure 4-25. *Check Security Center Standard tier is enabled*

You should see the same detail as in Figure 4-26, which will confirm it is enabled.

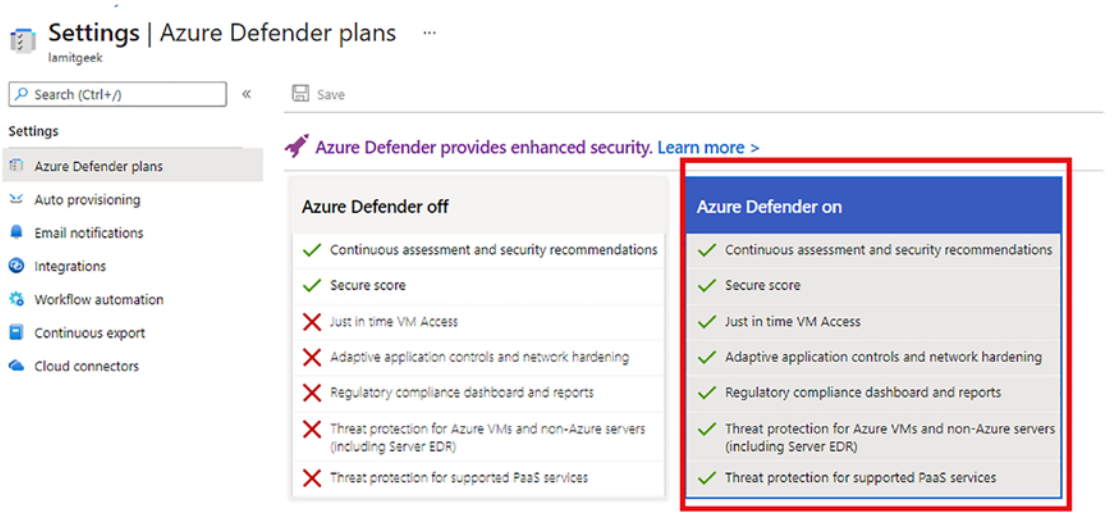

Figure 4-26. *Ensure Standard Tier is enabled*

3. You now need to enable threat protection for the virtual machine/servers, as shown in Figure 4-27.

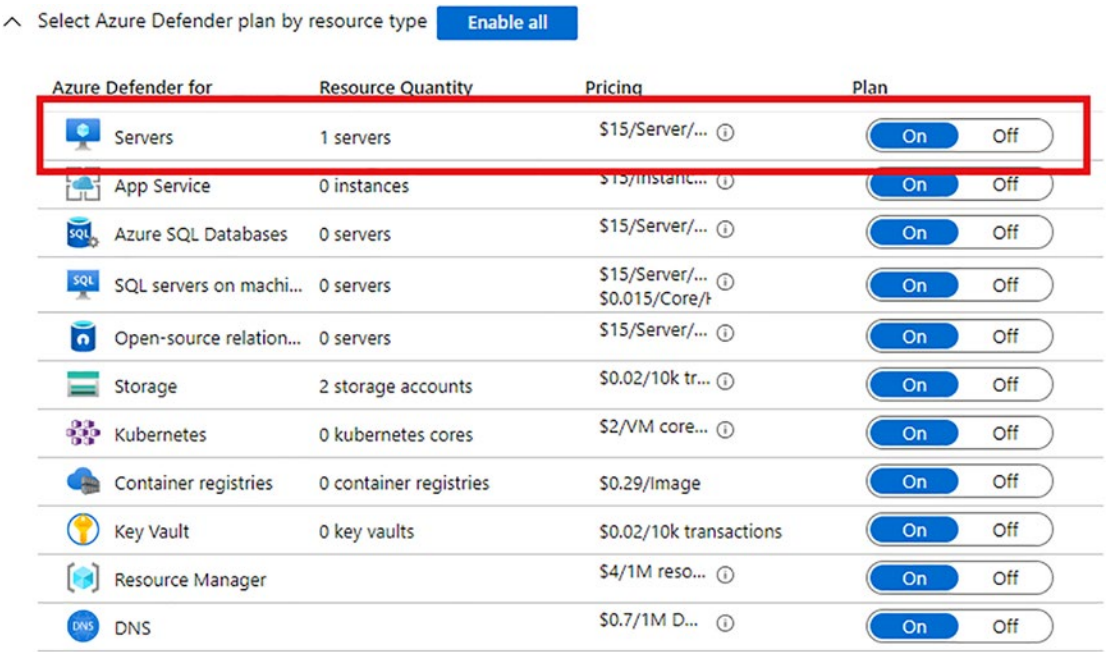

Figure 4-27. *Enable threat protection*

This section discussed Azure security integration with Azure Virtual Desktop. You also completed a lab exercise to enable it in the Azure Portal. You can now move on to the knowledge check to ensure you have understood the information in this chapter.

Knowledge Check

The following questions are aimed at testing your understanding of the information in this chapter. It is recommended that you complete all sections and labs in this chapter before attempting these questions.

Check Your Knowledge

1. You have been asked to give read-only access to a helpdesk team member to the Azure Virtual Desktop session hosts. Which built-in role should you grant access to? This must follow the Least Privilege Access model:
   - Desktop Virtualization Hostpool Reader
   - Desktop Virtualization Application Group Contributor
   - Desktop Virtualization Hostpool Contributor
2. Which of the following Azure Virtual Desktop services are managed by Microsoft? Choose three correct answers.
   - Web Access
   - Policies for Scaling
   - Diagnostics
   - Broker
   - End User Profile Management
3. Which of the following Azure Virtual Desktop services are managed by the end client? Choose three correct answers.
   - Gateway
   - End User Host Access

- Virtual Machine Scaling & Sizing
- Infrastructure Services
- Policies for Scaling

4. Which three Azure AD roles allow you to create and manage Conditional Access Policies?
   - Global Administrator
   - Helpdesk Administrator
   - Security Administrator
   - Conditional Access Administrator
   - Intune Administrator
5. What Azure Security Center tier is required to integrate with Azure Virtual Desktop?
   - Premium
   - Free
   - Standard
   - Basic

Summary

This chapter looked at managing access and security to Azure Virtual Desktop, including managing access to Azure Virtual Desktop and managing security in Azure Virtual Desktop.

Chapter 5 takes a deep dive into managing user environments and apps, including implementing and managing FSLogix, configuring user experience settings, and installing and configuring apps on a session host.