Exam Session - Knowledge Check: Managing Security on Azure Virtual Desktop

cloudacademy.com/quiz/exam/3731087/results

#1

Which of the following conditions is not a requirement for integrating Azure Virtual Desktop with Microsoft Defender for Cloud?

✕

You have active session hosts within your Azure Virtual Desktop environment.

✓

Some type of endpoint protection is enabled on your session host virtual machines.

✕

The Standard tier in Microsoft Defender for Cloud is enabled.

✕

You have provisioned your Azure Virtual Desktop environment.

Explanation

Let's start off by taking a look at some of the requirements that need to be fulfilled in order to integrate Azure Virtual Desktop with Microsoft Defender for Cloud. There are two levels of Microsoft Defender for Cloud, Basic and Standard. Before you can integrate this service with AVD, you need to ensure you have enabled the Standard tier in Microsoft Defender for Cloud. Finally, you need to ensure you have provisioned your Azure Virtual Desktop environment and have active session hosts within this environment.

/course/managing-security-azure-virtual-desktop-2356/managing-security-by-using-microsoft-defender-for-cloud/

#2

Which feature of an Azure Virtual Desktop/Microsoft Defender for Cloud integration allows you to control access to the session hosts and limit the level of access and amount of time a user can access a VM?

✓

just-in-time VM access

✗

adaptive application control

✗

file integrity monitoring

✗

security score

Explanation

I also want to mention just-in-time VM access as an important feature. This feature allows you to control access to the sessions hosts and limit not only the level of access, but the amount of time a user can access a VM.

🔗 /course/managing-security-azure-virtual-desktop-2356/managing-security-by-using-microsoft-defender-for-cloud/

#3

Which mode in Microsoft Defender Antivirus does not remediate threats and is not utilized as the primary antivirus application on the device?

✓

Passive

✗

Off

✗

Disabled

✗

Background

Explanation

We have passive mode, where Microsoft Defender Antivirus is not utilized as the primary antivirus, so it does not remediate threats.

🔗 /course/managing-security-azure-virtual-desktop-2356/configuring-microsoft-defender-antivirus-for-session-hosts/

#4

Microsoft ______ combines machine learning, big data analysis, and in-depth resistance research to offer a robust protection layer for Windows 11, 10, and Server OS.

✓

Defender Antivirus

✗

Virtual Desktop

✗

Security Central

✗

Secure Score

Explanation

Let's start off by explaining what Microsoft Defender Antivirus is. This is a set of next-generation protection services that are hosted by Microsoft 365 and part of its wider security suite. It combines machine learning, big data analysis, and in-depth resistance research to offer a robust protection layer for Windows 11, 10, and Server OS.

🔗 /course/managing-security-azure-virtual-desktop-2356/configuring-microsoft-defender-antivirus-for-session-hosts/

#5

Which option in session control configuration for an Azure Virtual Desktop conditional access policy allows you to control the amount of time before a user needs to authenticate their MFA?

✗

inactive default

✗

sign-in trigger

✗

re-authentication threshold

✓

sign-in frequency

Explanation

Before we are ready to create the policy, we need to configure session control. If we click on this, now we see several options in the right-hand pane. For your example, we want to tick sign-in frequency, which allows us to control the amount of time before a user needs to authenticate their MFA.

🔗 /course/managing-security-azure-virtual-desktop-2356/planning-and-implementing-conditional-access-policies-for-connections-to-azure-virtual-desktop/

#6

In an Azure Virtual Desktop conditional access MFA policy, what does the fraud alert setting do when it is turned on?

✗

automatically reports fraud after three unsuccessful login attempts

✗

automatically blocks users after three unsuccessful login attempts

✓

automatically blocks users who report fraud

✗

allows users to report fraud

Explanation

With the fraud alert settings, it is turned off by default; therefore, you have the ability to enable this. This will automatically turn on the setting to automatically block users who report fraud.

🔗 /course/managing-security-azure-virtual-desktop-2356/planning-and-implementing-multi-factor-authentication-in-azure-virtual-desktop/

#7

Which feature of an Azure Virtual Desktop/Microsoft Defender for Cloud integration is an intelligent and automated solution for defining allow lists of known, safe applications for your session hosts?

✗

file integrity monitoring

✗

security configuration assessment

✓

adaptive application control

✗

just-in-time VM access

Explanation

The final feature I will touch on is adaptive application control. This is an intelligent and automated solution for defining allow lists of known, safe applications for your session hosts.

🔗 /course/managing-security-azure-virtual-desktop-2356/managing-security-by-using-microsoft-defender-for-cloud/

#8

What is the minimum license a Microsoft 365 tenant needs to have in order to implement conditional access policies in Azure Virtual Desktop?

✗

Azure AD P4

✗

Azure AD P3

✗

Azure AD P2

✓

Azure AD P1

Explanation

Let's start by discussing conditional access policy requirements for Azure Virtual Desktop. We need to ensure that the Microsoft 365 tenant has the relevant licensing, which includes the conditional access feature. This is covered by the Azure AD P1 licenses and above.

🔗 /course/managing-security-azure-virtual-desktop-2356/planning-and-implementing-conditional-access-policies-for-connections-to-azure-virtual-desktop/

#9

In Microsoft Defender Antivirus, _____ updates are designed to protect you from network threats, including exploits, as they are transmitted.

✗

Threat Detector

✗

Global Compliance

✓

Network Inspection System

✗

Azure Virtual Desktop

Explanation

Network Inspection System updates are designed to protect you from network threats, including exploits, as they are transmitted.

🔗 /course/managing-security-azure-virtual-desktop-2356/configuring-microsoft-defender-antivirus-for-session-hosts/

#10

Which setting in an Azure Virtual Desktop conditional access MFA policy allows you to review which users have been completing MFA authentication, the time, the app that was being used, and the authentication method, among other details?

✗

user details

✗

logging

✓

activity reports

✗

auditing

Explanation

The final setting I mentioned was activity reports, which allow you to review which users have been completing MFA authentication, the time, and the app that was being used, as well as the authentication method, among other details.

🔗 /course/managing-security-azure-virtual-desktop-2356/planning-and-implementing-multi-factor-authentication-in-azure-virtual-desktop/