SC-100 Q&As

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/sc-100.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

You need to recommend a solution to resolve the virtual machine issue. What should you include in the recommendation?(Choose Two)

A. Onboard the virtual machines to Microsoft Defender for Endpoint.

B. Onboard the virtual machines to Azure Arc.

C. Create a device compliance policy in Microsoft Endpoint Manager.

D. Enable the Qualys scanner in Defender for Cloud.

Correct Answer: AD

Scenario: 20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud.

Existing Environment. Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation: Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

Note: Deploying Microsoft Defender for Endpoint is a two-step process.

Onboard devices to the service

Configure capabilities of the service

Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-vm https://docs.microsoft.com/en-us/microsoft-365/security/defenderendpoint/switch-to-mde-phase-3?view=o365-worldwide

QUESTION 2

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are designing the encryption standards for data at rest for an Azure resource.

You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.

Solution: For Azure SQL databases, you recommend Transparent Data Encryption (TDE) that uses customer-managed keys (CMKs).

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

We need to use customer-managed keys.

Transparent data encryption (TDE) helps protect Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics against the threat of malicious offline activity by encrypting data at rest. It performs real-time encryption and

decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.

In Azure, the default setting for TDE is that the Database Encryption Key (DEK) is protected by a built-in server certificate. The built-in server certificate is unique for each server and the encryption algorithm used is AES 256.

TDE protector is either a service-managed certificate (service-managed transparent data encryption) or an asymmetric key stored in Azure Key Vault (customer-managed transparent data encryption).

Note: Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our

recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices.

This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault. Please refer to specific Azure service documentation to see if the service covers endto-end rotation.

Reference: https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview

https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

QUESTION 3

Your company plans to apply the Zero Trust Rapid Modernization Plan (RaMP) to its IT environment.

You need to recommend the top three modernization areas to prioritize as part of the plan.

Which three areas should you recommend based on RaMP? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. data, compliance, and governance

B. infrastructure and development

C. user access and productivity

D. operational technology (OT) and IoT

E. modern security operations

Correct Answer: ACE

RaMP initiatives for Zero Trust

To rapidly adopt Zero Trust in your organization, RaMP offers technical deployment guidance organized in these

initiatives.

Critical security modernization initiatives:

(C) User access and productivity

1. Explicitly validate trust for all access requests Identities Endpoints (devices) Apps Network

(A) Data, compliance, and governance

2.

Ransomware recovery readiness

3.

Data

(E) Modernize security operations

4.

Streamline response

5.

Unify visibility

6.

reduce manual effort

Incorrect:

As needed

Additional initiatives based on Operational Technology (OT) or IoT usage, on-premises and cloud adoption, and security for in-house app development:

*

(not D) OT and Industrial IoT Discover Protect Monitor

*

Datacenter and DevOps Security Security Hygiene Reduce Legacy Risk DevOps Integration Microsegmentation

Reference: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview

QUESTION 4

You have a Microsoft 365 tenant.

Your company uses a third-party software as a service (SaaS) app named App1 that is integrated with an Azure AD tenant.

You need to design a security strategy to meet the following requirements:

- Users must be able to request access to App1 by using a self-service request.
- When users request access to App1, they must be prompted to provide additional information about their request.
- Every three months, managers must verify that the users still require access to App1. What should you include in the design?

A.

Microsoft Entra Identity Governance

B.

connected apps in Microsoft Defender for Cloud Apps

C.

access policies in Microsoft Defender for Cloud Apps

D.

Azure AD Application Proxy

Correct Answer: A

QUESTION 5

HOTSPOT

You have a hybrid cloud infrastructure.

You plan to deploy the Azure applications shown in the following table.

Name	Type	Requirement
App1	An Azure App Service web app accessed from Windows 11 devices on the on-premises network	Protect against attacks that use cross-site scripting (XSS).
App2	An Azure App Service web app accessed from mobile devices	Allow users to authenticate to App2 by using their LinkedIn account.

What should you use to meet the requirement of each app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

App1:

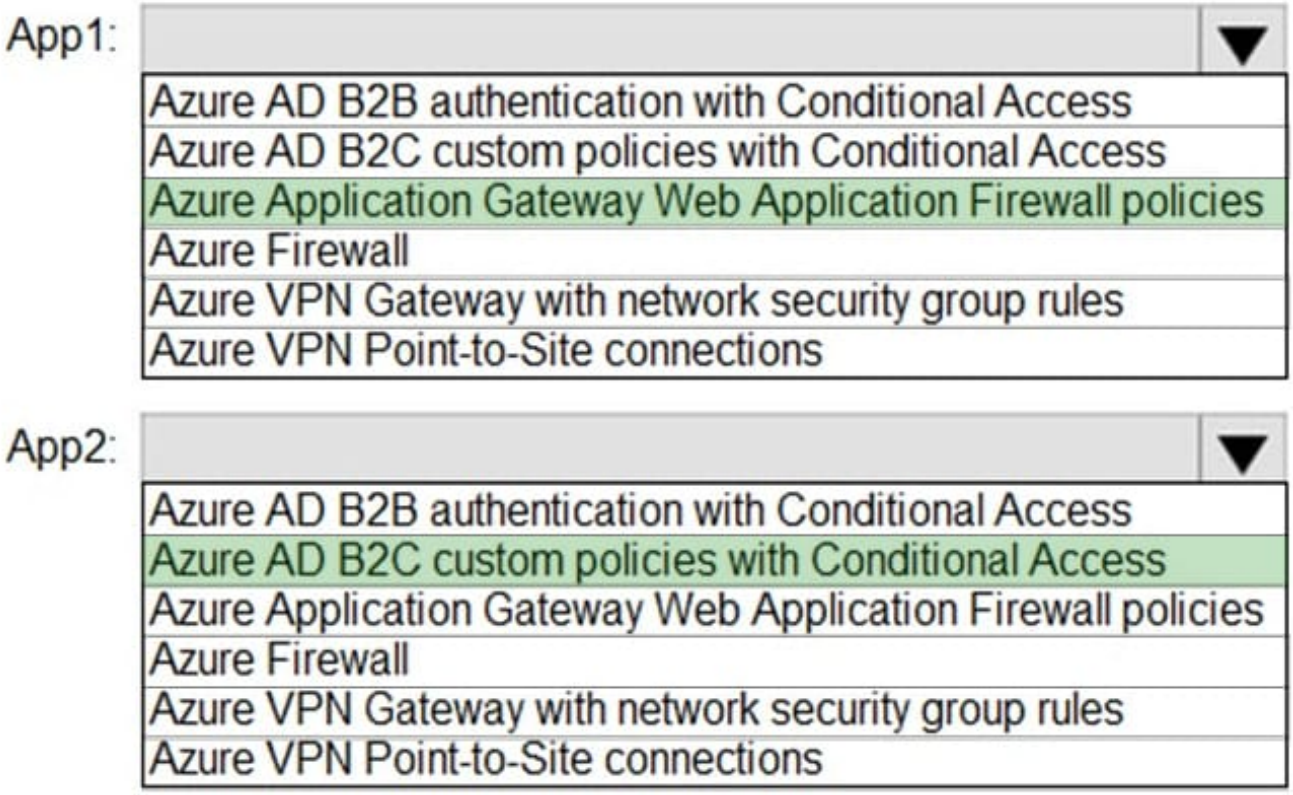
- Azure AD B2B authentication with Conditional Access
- Azure AD B2C custom policies with Conditional Access
- Azure Application Gateway Web Application Firewall policies
- Azure Firewall
- Azure VPN Gateway with network security group rules
- Azure VPN Point-to-Site connections

App2:

- Azure AD B2B authentication with Conditional Access
- Azure AD B2C custom policies with Conditional Access
- Azure Application Gateway Web Application Firewall policies
- Azure Firewall
- Azure VPN Gateway with network security group rules
- Azure VPN Point-to-Site connections

Correct Answer:

Answer Area



Box 1: Azure Application Gateway Web Application Firewall policies

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.

Azure Web Application Firewall is a cloud-native service that protects web apps from common web-hacking techniques such as SQL injection and security vulnerabilities such as cross-site scripting.

Box 2: Azure Active Directory B2C with Conditional Access

You can set up sign-up and sign-in with a LinkedIn account using Azure Active Directory B2C.

You can enhance the security of Azure Active Directory B2C (Azure AD B2C) with Azure AD Identity Protection and Conditional Access. Incorrect:

* Azure VPN Gateway with network security group rules NSGs cannot protect against XSS.

Reference: https://learn.microsoft.com/en-us/azure/application-gateway/overview https://azure.microsoft.com/en-us/products/web-application-firewall/#overview https://learn.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-linkedin