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.passapply.com/sc-100.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator

authorizes the application.

Which security control should you recommend?

A. app registrations in Azure Active Directory (Azure AD)

B. OAuth app policies in Microsoft Defender for Cloud Apps

C. Azure Security Benchmark compliance controls in Defender for Cloud

D. application control policies in Microsoft Defender for Endpoint

Correct Answer: B

Microsoft Defender for Cloud Apps OAuth app policies.

OAuth app policies enable you to investigate which permissions each app requested and which users authorized them for Office 365, Google Workspace, and Salesforce. You\\'re also able to mark these permissions as approved or banned.

Marking them as banned will revoke permissions for each app for each user who authorized it.

Incorrect:

Not D: Windows Defender Application cannot be used for virtual machines.

Reference: https://docs.microsoft.com/en-us/defender-cloud-apps/app-permission-policy

QUESTION 2

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 3

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 blob containers in Azure Storage, you recommend encryption 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.

Azure Storage encryption for data at rest.

Azure Storage uses service-side encryption (SSE) to automatically encrypt your data when it is persisted to the cloud. Azure Storage encryption protects your data and to help you to meet your organizational security and compliance

commitments.

Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption.

Data in a new storage account is encrypted with Microsoft-managed keys by default. You can continue to rely on Microsoft-managed keys for the encryption of your data, or you can manage encryption with your own keys. If you choose to

manage encryption with your own keys, you have two options. You can use either type of key management, or both:

*

You can specify a customer-managed key to use for encrypting and decrypting data in Blob Storage and in Azure Files.

*

You can specify a customer-provided key on Blob Storage operations. A client making a read or write request against Blob Storage can include an encryption key on the request for granular control over how blob data is encrypted and decrypted.

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

QUESTION 4

Your company is moving a big data solution to Azure.

The company plans to use the following storage workloads:

1.

Azure Storage blob containers

2.

Azure Data Lake Storage Gen2

3.

Azure Storage file shares

4.

Azure Disk Storage

Which two storage workloads support authentication by using Azure AD? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Azure Storage file shares

B. Azure Disk Storage

C. Azure Storage blob containers

D. Azure Data Lake Storage Gen2

Correct Answer: CD

C: Azure Storage supports using Azure Active Directory (Azure AD) to authorize requests to blob data. With Azure AD, you can use Azure role-based access control (Azure RBAC) to grant permissions to a security principal, which may be a user, group, or application service principal. The security principal is authenticated by Azure AD to return an OAuth 2.0 token. The token can then be used to authorize a request against the Blob service.

You can scope access to Azure blob resources at the following levels, beginning with the narrowest scope:

*

An individual container. At this scope, a role assignment applies to all of the blobs in the container, as well as container properties and metadata.

*

The storage account.

*

The resource group.

*

The subscription.

*

A management group.

D: You can securely access data in an Azure Data Lake Storage Gen2 (ADLS Gen2) account using OAuth 2.0 with an Azure Active Directory (Azure AD) application service principal for authentication. Using a service principal for authentication provides two options for accessing data in your storage account:

A mount point to a specific file or path

Direct access to data

Incorrect:

Not A: To enable AD DS authentication over SMB for Azure file shares, you need to register your storage account with AD DS and then set the required domain properties on the storage account. To register your storage account with AD DS,

create an account representing it in your AD DS.

Reference: https://docs.microsoft.com/en-us/azure/storage/blobs/authorize-access-azure-active-directory
https://docs.microsoft.com/en-us/azure/databricks/data/data-sources/azure/adls-gen2/azure-datalake-gen2-sp-access

QUESTION 5

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator

authorizes the application.

Which security control should you recommend?

A. app registrations in Azure Active Directory (Azure AD)

B. OAuth app policies in Microsoft Defender for Cloud Apps

C. Azure Security Benchmark compliance controls in Defender for Cloud

D. application control policies in Microsoft Defender for Endpoint

Correct Answer: D

This question has been updated on 8/3/22. Potential answers I\\'d expect to see are:

A. Azure Active Directory (Azure AD) Conditional Access App Control policies

B. OAuth app policies in Microsoft Defender for Cloud Apps

C. app protection policies in Microsoft Endpoint Manager

D. application control policies in Microsoft Defender for Endpoint Notice that only the wrong answers were changed. I\\'d vote D based on what I know about application control policies. https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/select-types-of-rules-to-create#windows-defender-application-control-policy-rules