SC-100Q&As

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

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

https://www.pass2lead.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

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 2

A customer is deploying Docker images to 10 Azure Kubernetes Service (AKS) resources across four Azure subscriptions.

You are evaluating the security posture of the customer.

You discover that the AKS resources are excluded from the secure score recommendations.

You need to produce accurate recommendations and update the secure score.

Which two actions should you recommend in Microsoft Defender for Cloud? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Enable Defender plans.

B. Configure auto provisioning.

C. Add a workflow automation.

D. Assign regulatory compliance policies.

E. Review the inventory.

Correct Answer: AB

QUESTION 3

You have an Azure subscription that contains several storage accounts. The storage accounts are accessed by legacy applications that are authenticated by using access keys.

You need to recommend a solution to prevent new applications from obtaining the access keys of the storage accounts. The solution must minimize the impact on the legacy applications.

What should you include in the recommendation?

A. Apply read-only locks on the storage accounts.

B. Set the AllowSharcdKeyAccess property to false.

C. Set the AllowBlobPublicAcccss property to false.

D. Configure automated key rotation.

Correct Answer: A

A read-only lock on a storage account prevents users from listing the account keys. A POST request handles the Azure Storage List Keys operation to protect access to the account keys. The account keys provide complete access to data

in

the storage account.

Incorrect:

Not A:

If any clients are currently accessing data in your storage account with Shared Key, then Microsoft recommends that you migrate those clients to Azure AD before disallowing Shared Key access to the storage account.

However, in this scenario we cannot migrate to Azure AD due to the legacy applications.

Note: Shared Key

A shared key is a very long string. You can simply access Azure storage by using this long string. It\\'s almost like a password. Actually, it\\'s worse: this is a master password. It gives you all sorts of rights on the Azure storage account. You can

imagine why this isn\\'t my favorite mechanism of accessing Azure storage. What happens when this key is compromised? You don\\'t get an alert. Perhaps you can set up monitoring to see misuse of your Azure storage account. But it\\'s still less

than an ideal situation. Alerts will tell you of damage after it has already occurred.

Not C: Data breaches caused by cloud misconfiguration have been seen for the past few years. One of the most common misconfigurations is granting public access to cloud storage service. Such a data is often unprotected, making them to

be accessed without any authentication method. Microsoft recently introduced a new protection feature to help avoid public access on storage account. The feature introduces a new property named allowBlobPublicAccess.

Not D: Key rotation would improve security.

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.

Reference: https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

https://docs.microsoft.com/en-us/azure/storage/common/shared-key-authorization-prevent

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

QUESTION 4

You have an on-premises network that has several legacy applications. The applications perform LDAP queries against an existing directory service.

You are migrating the on- premises infrastructure to a cloud-only infrastructure.

You need to recommend an identity solution for the infrastructure that supports the legacy applications. The solution must minimize the administrative effort to maintain the infrastructure.

Which identity service should you include in the recommendation?

A. Azure AD B2C

B. Azure Active Directory Domain Services (Azure AD DS)

C. Azure AD

D. Active Directory Domain Services (AD DS)

Correct Answer: B

Lightweight Directory Access Protocol (LDAP) is an application protocol for working with various directory services. Directory services, such as Active Directory, store user and account information, and security information like passwords. The service then allows the information to be shared with other devices on the network. Enterprise applications such as email, customer relationship managers (CRMs), and Human Resources (HR) software can use LDAP to authenticate, access, and find information.

Azure Active Directory (Azure AD) supports this pattern via Azure AD Domain Services (AD DS). It allows organizations that are adopting a cloud-first strategy to modernize their environment by moving off their on-premises LDAP resources

to the cloud. The immediate benefits will be:

Integrated with Azure AD. Additions of users and groups, or attribute changes to their objects are automatically synchronized from your Azure AD tenant to AD DS. Changes to objects in on-premises Active Directory are synchronized to

Azure AD, and then to AD DS.

Simplify operations. Reduces the need to manually keep and patch on-premises infrastructures. Reliable. You get managed, highly available services Reference: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/auth-ldap

QUESTION 5

You have a Microsoft 365 tenant. Your company uses a third-party software as a service (SaaS) app named App1. App1 supports authenticating users by using Azure AD credentials.

You need to recommend a solution to enable users to authenticate to App1 by using their Azure AD credentials.

What should you include in the recommendation?

A. Azure AD Application Proxy

B. Azure AD B2C

C. an Azure AD enterprise application

D. a relying party trust in Active Directory Federation Services (AD FS)

Correct Answer: A

Latest SC-100 Dumps SC-100 PDF Dumps SC-100 Study Guide