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 are designing the security standards for a new Azure environment.

You need to design a privileged identity strategy based on the Zero Trust model.

Which framework should you follow to create the design?

A. Enhanced Security Admin Environment (ESAE)

B. Microsoft Security Development Lifecycle (SDL)

C. Rapid Modernization Plan (RaMP)

D. Microsoft Operational Security Assurance (OSA)

Correct Answer: C

RaMP initiatives for Zero Trust.

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

In particular, meet these deployment objectives to protect your privileged identities with Zero Trust.

1.

Deploy secured privileged access to protect administrative user accounts.

2.

Deploy Azure AD Privileged Identity Management (PIM) for a time-bound, just-in-time approval process for the use of privileged user accounts.

Note 1: RaMP guidance takes a project management and checklist approach:

* User access and productivity

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

* Data, compliance, and governance

2.

Ransomware recovery readiness

3.

Data

* Modernize security operations

4.

Streamline response

5.

Unify visibility

6.

Reduce manual effort

Note 2: As an alternative to deployment guidance that provides detailed configuration steps for each of the technology pillars being protected by Zero Trust principles, Rapid Modernization Plan (RaMP) guidance is based on initiatives and

gives you a set of deployment paths to more quickly implement key layers of protection.

By providing a suggested mapping of key stakeholders, implementers, and their accountabilities, you can more quickly organize an internal project and define the tasks and owners to drive them to conclusion.

By providing a checklist of deployment objectives and implementation steps, you can see the bigger picture of infrastructure requirements and track your progress.

Incorrect:

Not B: Enhanced Security Admin Environment (ESAE)

The Enhanced Security Admin Environment (ESAE) architecture (often referred to as red forest, admin forest, or hardened forest) is an approach to provide a secure environment for Windows Server Active Directory (AD) administrators.

Microsoft\\'s recommendation to use this architectural pattern has been replaced by the modern privileged access strategy and rapid modernization plan (RAMP) guidance as the default recommended approach for securing privileged users.

The ESAE hardened administrative forest pattern (on-prem or cloud-based) is now considered a custom configuration suitable only for exception cases listed below.

What are the valid ESAE use cases?

While not a mainstream recommendation, this architectural pattern is valid in a limited set of scenarios.

In these exception cases, the organization must accept the increased technical complexity and operational costs of the solution. The organization must have a sophisticated security program to measure risk, monitor risk, and apply consistent

operational rigor to the usage and maintenance of the ESAE implementation.

Example scenarios include:

Isolated on-premises environments - where cloud services are unavailable such as offline research laboratories, critical infrastructure or utilities, disconnected operational technology (OT) environments such as Supervisory control and data

acquisition (SCADA) / Industrial Control Systems (ICS), and public sector customers that are fully reliant on on-premises technology.

Highly regulated environments – industry or government regulation may specifically require an administrative forest configuration.

High level security assurance is mandated - organizations with low risk tolerance that are willing to accept the increased complexity and operational cost of the solution.

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

https://docs.microsoft.com/en-us/security/zero-trust/user-access-productivity-validate-trust#identities

https://docs.microsoft.com/en-us/security/compass/esae-retirement

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 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 3

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 4

You are designing a ransomware response plan that follows Microsoft Security Best Practices.

You need to recommend a solution to minimize the risk of a ransomware attack encrypting local user files.

What should you include in the recommendation?

A. Windows Defender Device Guard

B. Microsoft Defender for Endpoint

C. Azure Files

D. BitLocker Drive Encryption (BitLocker)

E. protected folders

Correct Answer: B

QUESTION 5

HOTSPOT

You have an Azure subscription and an on-premises datacenter. The datacenter contains 100 servers that run Windows Server. All the servers are backed up to a Recovery Services vault by using Azure Backup and the Microsoft Azure Recovery Services (MARS) agent.

You need to design a recovery solution for ransomware attacks that encrypt the on-premises servers. The solution must follow Microsoft Security Best Practices and protect against the following risks:

1.

A compromised administrator account used to delete the backups from Azure Backup before encrypting the servers

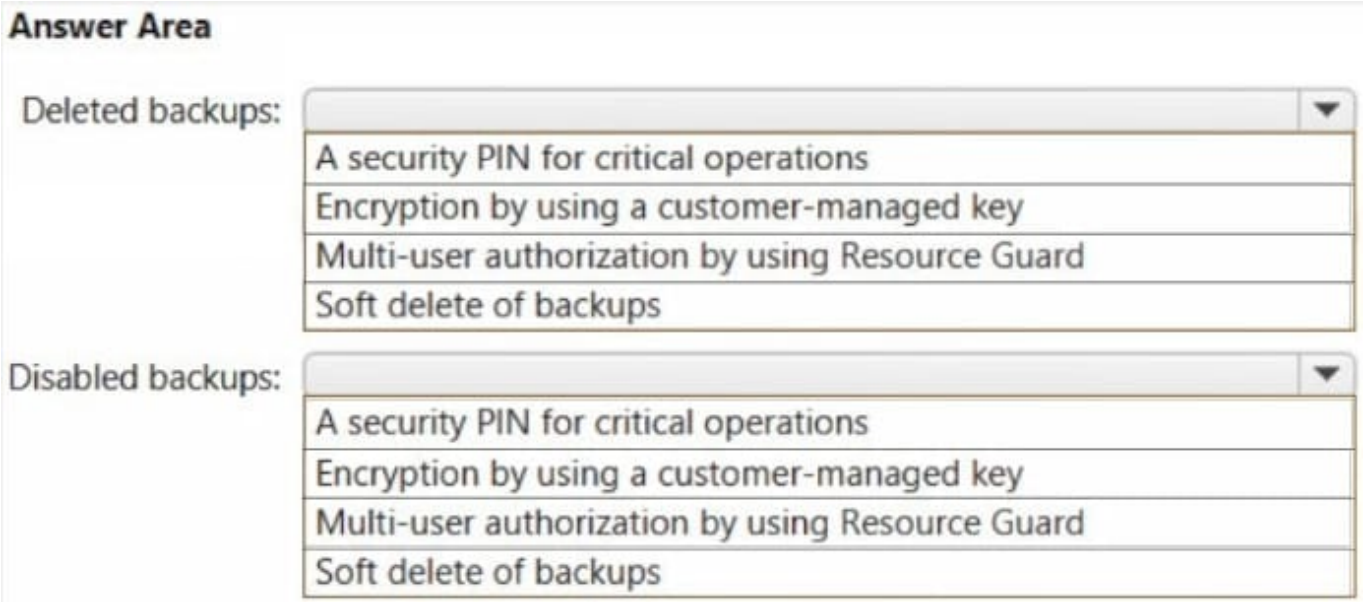
2.

A compromised administrator account used to disable the backups on the MARS agent before encrypting the servers

What should you use for each risk? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area

Deleted backups:

- A security PIN for critical operations
- Encryption by using a customer-managed key
- Multi-user authorization by using Resource Guard
- Soft delete of backups

Disabled backups:

- A security PIN for critical operations
- Encryption by using a customer-managed key
- Multi-user authorization by using Resource Guard
- Soft delete of backups

Box 1: Soft delete of backups

How to block intentional or unintentional deletion of backup data?

Enable Soft delete is enabled to protect backups from accidental or malicious deletes.

Soft delete is a useful feature that helps you deal with data loss. Soft delete retains backup data for 14 days, allowing the recovery of that backup item before it\\'s permanently lost.

Box 2: Multi-user authorization by using Resource Guard

Ensure Multi-user authorization (MUA) is enabled for an additional layer of protection.

MUA for Azure Backup uses a new resource called Resource Guard to ensure critical operations, such as disabling soft delete, stopping and deleting backups, or reducing retention of backup policies, are performed only with applicable

authorization.

Reference: https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq

SC-100 VCE Dumps SC-100 Practice Test SC-100 Study Guide