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.leads4pass.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 need to recommend a solution to secure the MedicalHistory data in the ClaimsDetail table. The solution must meet the Contoso developer requirements.

What should you include in the recommendation?

A. row-level security (RLS)

B. Transparent Data Encryption (TDE)

C. Always Encrypted

D. data classification

E. dynamic data masking

Correct Answer: C

Anyone with admin privileges can see masked data. https://docs.microsoft.com/en-us/learn/modules/protect-data-transit-rest/4-explain-object-encryption-secure-enclaves

---

QUESTION 2

Your company has an Azure subscription that uses Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Defender for Cloud, review the Azure security baseline for audit report.

B. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

C. From Defender for Cloud, enable Defender for Cloud plans.

D. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

Correct Answer: D

The Azure Policy Regulatory Compliance built-in initiative definition maps to compliance domains and controls in NIST SP 800-53 Rev. 5.

The following mappings are to the NIST SP 800-53 Rev. 5 controls. Use the navigation on the right to jump directly to a specific compliance domain. Many of the controls are implemented with an Azure Policy initiative definition. To review the complete initiative definition, open Policy in the Azure portal and select the Definitions page. Then, find and select the NIST SP 800-53 Rev. 5 Regulatory Compliance built-in initiative definition. Reference: https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-53-r5

QUESTION 3

Reference: https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-pricing

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 have an Azure subscription that has Microsoft Defender for Cloud enabled.

You are evaluating the Azure Security Benchmark V3 report.

In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.

You need to recommend configurations to increase the score of the Secure management ports controls.

Solution: You recommend enabling adaptive network hardening.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead: You recommend enabling just-in-time (JIT) VM access on all virtual machines.

Note:

Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time VM access and network security groups.

Recommendations:

-Internet-facing virtual machines should be protected with network security groups

-

Management ports of virtual machines should be protected with just-in-time network access control

-

Management ports should be closed on your virtual machines Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

QUESTION 4

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

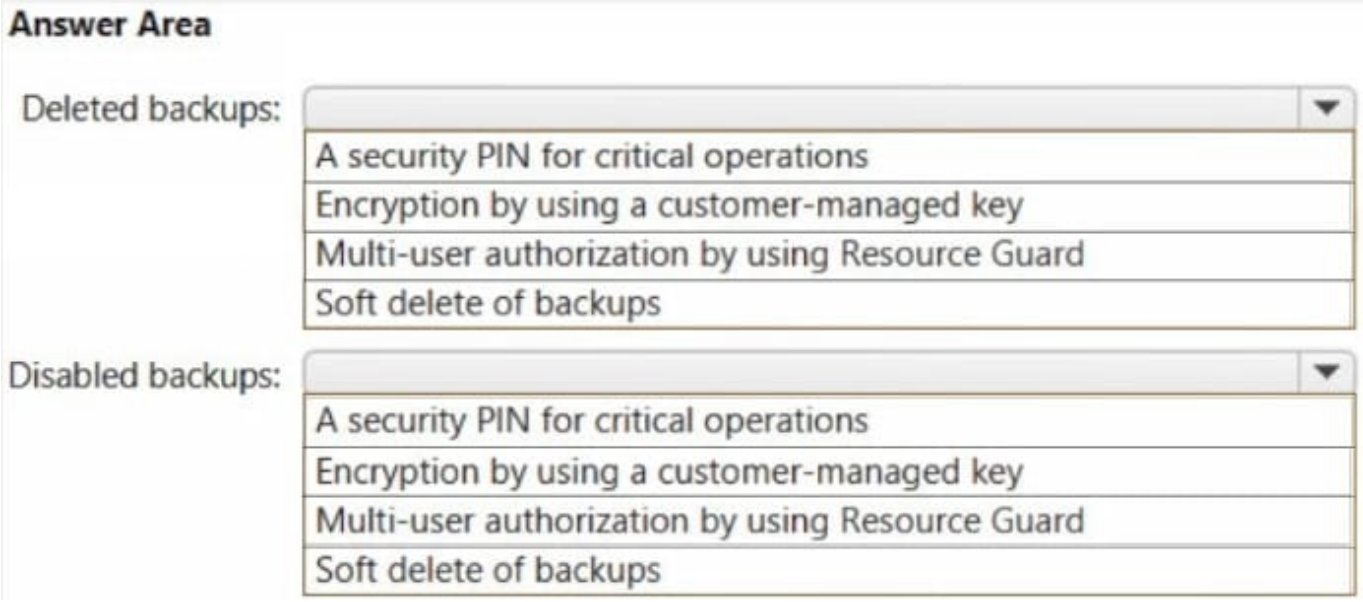
2.

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

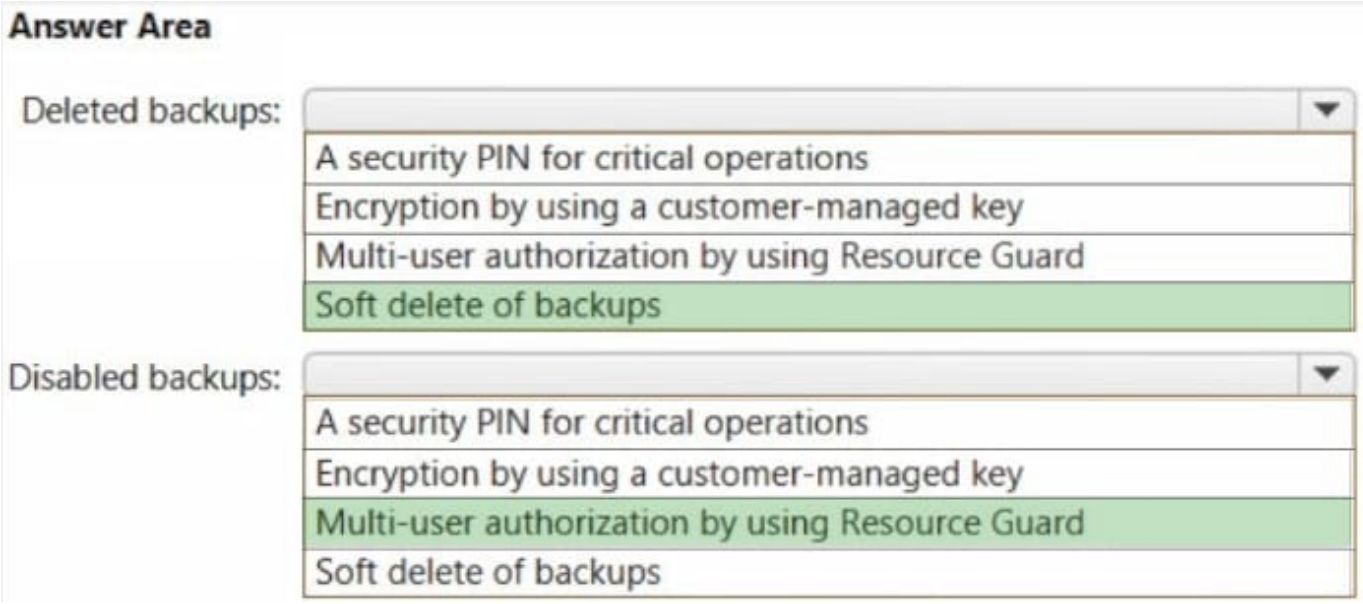
What should you use for each risk? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



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

---

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 AD

B. application control policies in Microsoft Defender for Endpoint

C. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps

D. Azure AD Conditional Access App Control policies

Correct Answer: B

Explanation:

Windows Defender Application Control is designed to protect devices against malware and other untrusted software. It prevents malicious code from running by ensuring that only approved code, that you know, can be run.

Application Control is a software-based security layer that enforces an explicit list of software that is allowed to run on a PC.

Incorrect:

Not C: A Cloud Discovery anomaly detection policy enables you to set up and configure continuous monitoring of

unusual increases in cloud application usage. Increases in downloaded data, uploaded data, transactions, and users are

considered for each cloud application. Each increase is compared to the normal usage pattern of the application as learned from past usage. The most extreme increases trigger security alerts.

Reference:

https://learn.microsoft.com/en-us/mem/configmgr/protect/deploy-use/use-device-guard-with-configuration-manager

QUESTION 6

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 7

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:

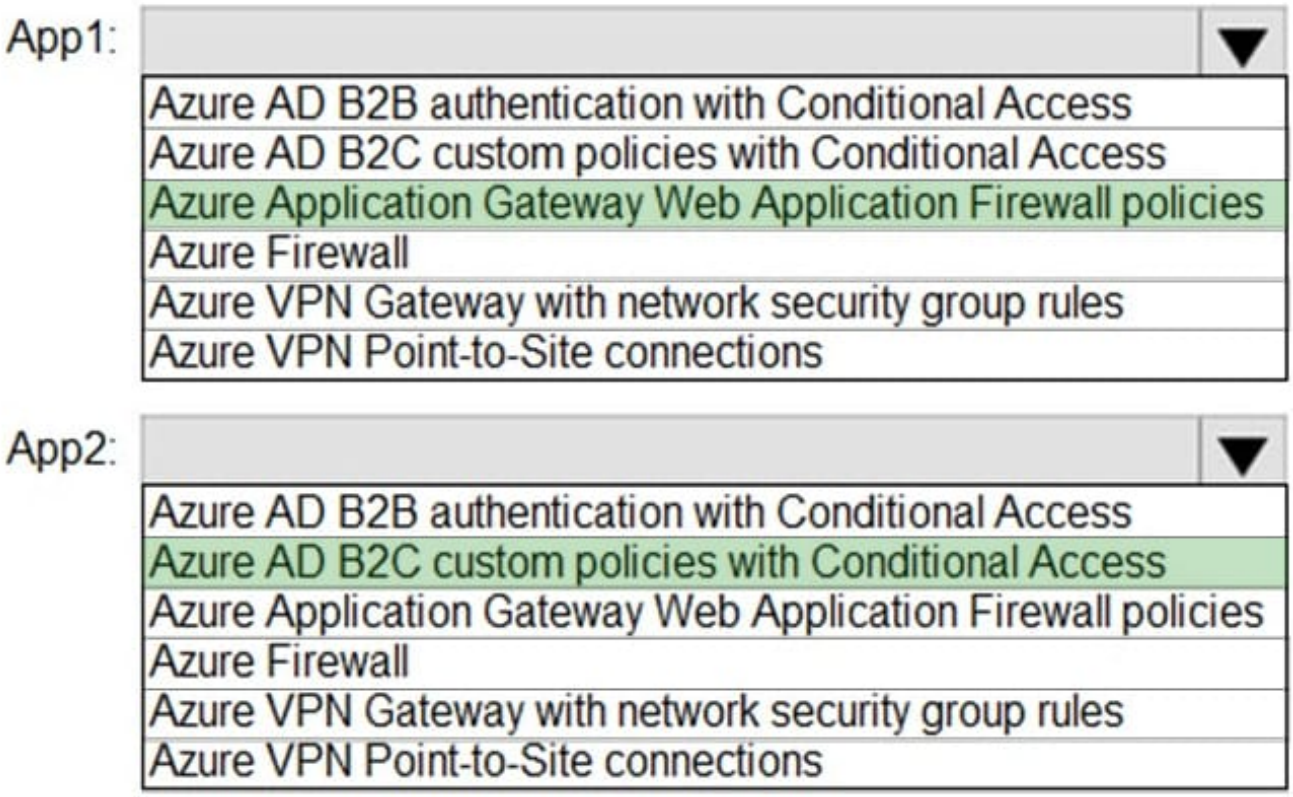
- Azure AD B2B authentication with Conditional Access
- Azure AD B2C custom policies with Conditional Access
- Azure Application Gateway Web Application Firewall policies
- Azure Firewall
- Azure VPN Gateway with network security group rules
- Azure VPN Point-to-Site connections

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

QUESTION 8

HOTSPOT

You need to recommend a solution to meet the compliance requirements.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To enforce compliance to the regulatory standard, create:

An Azure Automation account
A blueprint
A managed identity
Workflow automation

To exclude TestRG from the compliance assessment:

Edit an Azure blueprint
Modify a Defender for Cloud workflow automation
Modify an Azure policy definition
Update an Azure policy assignment

Correct Answer:

Answer Area

To enforce compliance to the regulatory standard, create:

An Azure Automation account
A blueprint
A managed identity
Workflow automation

To exclude TestRG from the compliance assessment:

Edit an Azure blueprint
Modify a Defender for Cloud workflow automation
Modify an Azure policy definition
Update an Azure policy assignment

Box 1: A blueprint Scenario: Requirements. Compliance Requirements Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPAA HITRUST standard.

Microsoft releases automation for HIPAA/HITRUST compliance I am excited to share our new Azure Security and Compliance Blueprint for HIPAA/HITRUST

QUESTION 9

You have a Microsoft 365 subscription that syncs with Active Directory Domain Services (AD DS).

You need to define the recovery steps for a ransomware attack that encrypted data in the subscription. The solution must follow Microsoft Security Best Practices.

What is the first step in the recovery plan?

A. From Microsoft Defender for Endpoint, perform a security scan.

B. Recover files to a cleaned computer or device.

C. Contact law enforcement.

D. Disable Microsoft OneDrive sync and Exchange ActiveSync.

Correct Answer: D

The following containment steps can be done concurrently as new threat vectors are discovered.

Step 1: Assess the scope of the situation

Which user accounts were compromised?

Which devices are affected? Which applications are affected? Step 2: Preserve existing systems

*

Disable all privileged user accounts except for a small number of accounts used by your admins to assist in resetting the integrity of your AD DS infrastructure. If a user account is believed to be compromised, disable it immediately.

*

Isolate compromised systems from the network, but do not shut them off.

*

Etc.

Note:

With OneDrive, you can sync files between your computer and the cloud, so you can get to your files from anywhere - your computer, your mobile device, and even through the OneDrive website at OneDrive.com.

ActiveSync is a client protocol that lets users synchronize their Exchange mailbox with a mobile device.

Reference: https://learn.microsoft.com/en-us/security/compass/incident-response-playbook-dart-ransomware-approach

QUESTION 10

For a Microsoft cloud environment, you are designing a security architecture based on the Microsoft Cloud Security Benchmark.

What are three best practices for identity management based on the Azure Security Benchmark? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Manage application identities securely and automatically.

B. Manage the lifecycle of identities and entitlements

C. Protect identity and authentication systems.

D. Enable threat detection for identity and access management.

E. Use a centralized identity and authentication system.

Correct Answer: ACE

QUESTION 11

Your company is developing an invoicing application that will use Azure AD B2C. The application will be deployed as an App Service web app.

You need to recommend a solution to the application development team to secure the application from identity-related attacks.

Which two configurations should you recommend? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Azure AD Conditional Access integration with user flows and custom policies

B. smart account lockout in Azure AD B2C

C. access packages in Identity Governance

D. custom resource owner password credentials (ROPC) flows in Azure AD B2C

Correct Answer: AB

Explanation:

A: Add Conditional Access to user flows in Azure Active Directory B2C Conditional Access can be added to your Azure Active Directory B2C (Azure AD B2C) user flows or custom policies to manage risky sign-ins to your applications. Azure Active Directory (Azure AD) Conditional Access is the tool used by Azure AD B2C to bring signals together, make decisions, and enforce organizational policies.

B: Mitigate credential attacks in Azure AD B2C with smart lockout Credential attacks lead to unauthorized access to resources. Passwords that are set by users are required to be reasonably complex. Azure AD B2C has mitigation techniques in place for credential attacks. Mitigation includes detection of brute-force credential attacks and dictionary credential attacks. By using various signals, Azure Active Directory B2C (Azure AD B2C) analyzes the integrity of requests. Azure AD B2C is designed to intelligently differentiate intended users from hackers and botnets.

Incorrect:

Not C: Identity Governance though useful, does not address this specific scenario: to secure the application from identity-related attack in an Azure AD B2C environment.

Note: Identity Governance gives organizations the ability to do the following tasks across employees, business partners and vendors, and across services and applications both on-premises and in clouds:

Govern the identity lifecycle

Govern access lifecycle

Secure privileged access for administration

Specifically, it is intended to help organizations address these four key questions:

Which users should have access to which resources?

What are those users doing with that access?

Are there effective organizational controls for managing access?

Can auditors verify that the controls are working?

Note: An access package enables you to do a one-time setup of resources and policies that automatically administers access for the life of the access package.

Not D: In Azure Active Directory B2C (Azure AD B2C), the resource owner password credentials (ROPC) flow is an OAuth standard authentication flow. In this flow, an application, also known as the relying party, exchanges valid credentials

for tokens. The credentials include a user ID and password.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user-flow

https://docs.microsoft.com/en-us/azure/active-directory/governance/identity-governance-overview

https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management

---

QUESTION 12

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 13

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 Microsoft-managed keys.

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 14

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 15

You have an Azure subscription that has Microsoft Defender for Cloud enabled. Suspicious authentication activity alerts have been appearing in the Workload protections dashboard.

You need to recommend a solution to evaluate and remediate the alerts by using workflow automation. The solution must minimize development effort. What should you include in the recommendation?

A. Azure Monitor webhooks

B. Azure Logics Apps

C. Azure Event Hubs

D. Azure Functions apps

Correct Answer: B

The workflow automation feature of Microsoft Defender for Cloud feature can trigger Logic Apps on security alerts, recommendations, and changes to regulatory compliance.Note: Azure Logic Apps is a cloud-based platform for creating and running automated workflows that integrate your apps, data, services, and systems. With this platform, you can quickly develop highly scalable integration solutions for your enterprise and business-to-business (B2B) scenarios.