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.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

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

QUESTION 1

You need to recommend a strategy for routing internet-bound traffic from the landing zones. The solution must meet the landing zone requirements.

What should you recommend as part of the landing zone deployment?

A. service chaining

B. local network gateways

C. forced tunneling

D. a VNet-to-VNet connection

Correct Answer: A

Service chaining.

Service chaining enables you to direct traffic from one virtual network to a virtual appliance or gateway in a peered network through user-defined routes.

You can deploy hub-and-spoke networks, where the hub virtual network hosts infrastructure components such as a network virtual appliance or VPN gateway. All the spoke virtual networks can then peer with the hub virtual network. Traffic

flows through network virtual appliances or VPN gateways in the hub virtual network.

Virtual network peering enables the next hop in a user-defined route to be the IP address of a virtual machine in the peered virtual network, or a VPN gateway. You can\\'t route between virtual networks with a user-defined route that specifies

an Azure ExpressRoute gateway as the next hop type.

Incorrect:

Not B: Forced tunneling lets you redirect or "force" all Internet-bound traffic back to your on-premises location via a Site-to-Site VPN tunnel for inspection and auditing. This is a critical security requirement for most enterprise IT policies. If you

don\\'t configure forced tunneling, Internet-bound traffic from your VMs in Azure always traverses from the Azure network infrastructure directly out to the Internet, without the option to allow you to inspect or audit the traffic. Unauthorized

Internet access can potentially lead to information disclosure or other types of security breaches.

ExpressRoute forced tunneling is not configured via this mechanism, but instead, is enabled by advertising a default route via the ExpressRoute BGP peering sessions.

Note:

Requirements. Planned Changes

Litware plans to implement the following changes:

Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

Requirements. Azure Landing Zone Requirements

Litware identifies the following landing zone requirements:

1.

Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.

2.

Provide a secure score scoped to the landing zone.

3.

Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.

4.

Minimize the possibility of data exfiltration.

5.

Maximize network bandwidth.

The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:

1.

Be created in a dedicated subscription.

2.

Use a DNS namespace of litware.com.

Reference: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview#service-chaining https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm

QUESTION 2

You need to recommend a solution to meet the security requirements for the InfraSec group. What should you use to delegate the access?

A. a subscription

B. a custom role-based access control (RBAC) role

C. a resource group

D. a management group

Correct Answer: B

Scenario: Requirements. Security Requirements include:

Only members of a group named InfraSec must be allowed to configure network security groups (NSGs) and instances of Azure Firewall, WAF, and Front Door in Sub1.

If the Azure built-in roles don\\'t meet the specific needs of your organization, you can create your own custom roles. Just like built-in roles, you can assign custom roles to users, groups, and service principals at management group (in preview

only), subscription, and resource group scopes.

Incorrect:

Not D: Management groups are useful when you have multiple subscriptions. This is not what is addressed in this question.

Scenario: Fabrikam has a single Azure subscription named Sub1.

Note: If your organization has many Azure subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions. Management groups provide a governance scope above subscriptions. You

organize subscriptions into management groups the governance conditions you apply cascade by inheritance to all associated subscriptions.

Management groups give you enterprise-grade management at scale no matter what type of subscriptions you might have. However, all subscriptions within a single management group must trust the same Azure Active Directory (Azure AD)

tenant.

Reference: https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

QUESTION 3

You need to design a strategy for securing the SharePoint Online and Exchange Online data. The solution must meet the application security requirements.

Which two services should you leverage in the strategy? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Azure AD Conditional Access

B. access reviews in Azure AD

C. Microsoft Defender for Cloud

D. Microsoft Defender for Cloud Apps

E. Microsoft Defender for Endpoint

Correct Answer: BD

Scenario: Litware identifies the following application security requirements:

Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

B: Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User\\'s access can be reviewed on a regular basis to make sure only the right people have continued access.

D: The Defender for Cloud Apps framework Discover and control the use of Shadow IT: Identify the cloud apps, IaaS, and PaaS services used by your organization. Investigate usage patterns, assess the risk levels and business readiness of more than 25,000 SaaS apps against more than 80 risks. Start managing them to ensure security and compliance.

Protect your sensitive information anywhere in the cloud: Understand, classify, and protect the exposure of sensitive information at rest. Leverage out-of-the box policies and automated processes to apply controls in real time across all your cloud apps.

Etc.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview
https://docs.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps

QUESTION 4

You have a Microsoft 365 subscription.

You need to design a solution to block file downloads from Microsoft SharePoint Online by authenticated users on unmanaged devices.

Which two services should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Azure AD Conditional Access

B. Azure Data Catalog

C. Microsoft Purview Information Protection

D. Azure AD Application Proxy

E. Microsoft Defender for Cloud Apps

Correct Answer: AE

Explanation:

Blocking or limiting access on unmanaged devices relies on Azure AD conditional access policies.

Create a block download policy for unmanaged devices

Defender for Cloud Apps session policies allow you to restrict a session based on device state. To accomplish control of a session using its device as a condition, create both a conditional access policy AND a session policy.

Incorrect:

Not B: Azure Data Catalog is an enterprise-wide metadata catalog that makes data asset discovery straightforward. It\\'s a fully-managed service that lets you — from analyst to data scientist to data developer — register, enrich, discover,

understand, and consume data sources.

Not C: Implement capabilities from Microsoft Purview Information Protection (formerly Microsoft Information Protection) to help you discover, classify, and protect sensitive information wherever it lives or travels.

Reference:

https://learn.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices

https://learn.microsoft.com/en-us/defender-cloud-apps/use-case-proxy-block-session-aad

QUESTION 5

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