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

QUESTION 1

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 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 AD tenant that syncs with an Active Directory Domain Services (AD DS) domain.

You are designing an Azure DevOps solution to deploy applications to an Azure subscription by using continuous integration and continuous deployment (CI/CD) pipelines.

You need to recommend which types of identities to use for the deployment credentials of the service connection. The solution must follow DevSecOps best practices from the Microsoft Cloud Adoption Framework for Azure.

What should you recommend?

A. a managed identity in Azure

B. an Azure AD user account that has role assignments in Azure AD Privileged Identity Management (PIM)

C. a group managed service account (gMSA)

D. an Azure AD user account that has a password stored in Azure Key Vault

Correct Answer: D

QUESTION 4

You need to recommend a solution for securing the landing zones. The solution must meet the landing zone requirements and the business requirements. What should you configure for each landing zone?

A. Azure DDoS Protection Standard

B. an Azure Private DNS zone

C. Microsoft Defender for Cloud

D. an ExpressRoute gateway

Correct Answer: D

ExpressRoute provides direct connectivity to Azure cloud services and connecting Microsoft\\'s global network. All transferred data is not encrypted, and do not go over the public Internet. VPN Gateway provides secured connectivity to Azure

cloud services over public Internet.

Note:

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.

Litware identifies the following business requirements:

1.

Minimize any additional on-premises infrastructure.

2.

Minimize the operational costs associated with administrative overhead.

Reference: https://medium.com/awesome-azure/azure-difference-between-azure-expressroute-and-azure-vpn-gateway-comparison-azure-hybrid-connectivity-5f7ce02044f3

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 a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.

You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.

Solution: You recommend configuring gateway-required virtual network integration.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead: You recommend access restrictions based on HTTP headers that have the Front Door ID. Restrict access to a specific Azure Front Door instance

Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front

Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.

Incorrect:

Virtual Network (VNet) integration for an Azure service enables you to lock down access to the service to only your virtual network infrastructure. The VNet infrastructure also includes peered virtual networks and on-premises networks.

VNet integration provides Azure services the benefits of network isolation and can be accomplished by one or more of the following methods:

Deploying dedicated instances of the service into a virtual network. The services can then be privately accessed within the virtual network and from on-premises networks.

Using Private Endpoint that connects you privately and securely to a service powered by Azure Private Link. Private Endpoint uses a private IP address from your VNet, effectively bringing the service into your virtual network.

Accessing the service using public endpoints by extending a virtual network to the service, through service endpoints. Service endpoints allow service resources to be secured to the virtual network.

Using service tags to allow or deny traffic to your Azure resources to and from public IP endpoints.

Reference: https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions

https://docs.microsoft.com/en-us/azure/virtual-network/vnet-integration-for-azure-services