SC-100 Q&As

Microsoft Cybersecurity Architect

QUESTION 1

You are designing an auditing solution for Azure landing zones that will contain the following components:

1.

SQL audit logs for Azure SQL databases

2.

Windows Security logs from Azure virtual machines

3.

Azure App Service audit logs from App Service web apps

You need to recommend a centralized logging solution for the landing zones. The solution must meet the following requirements:

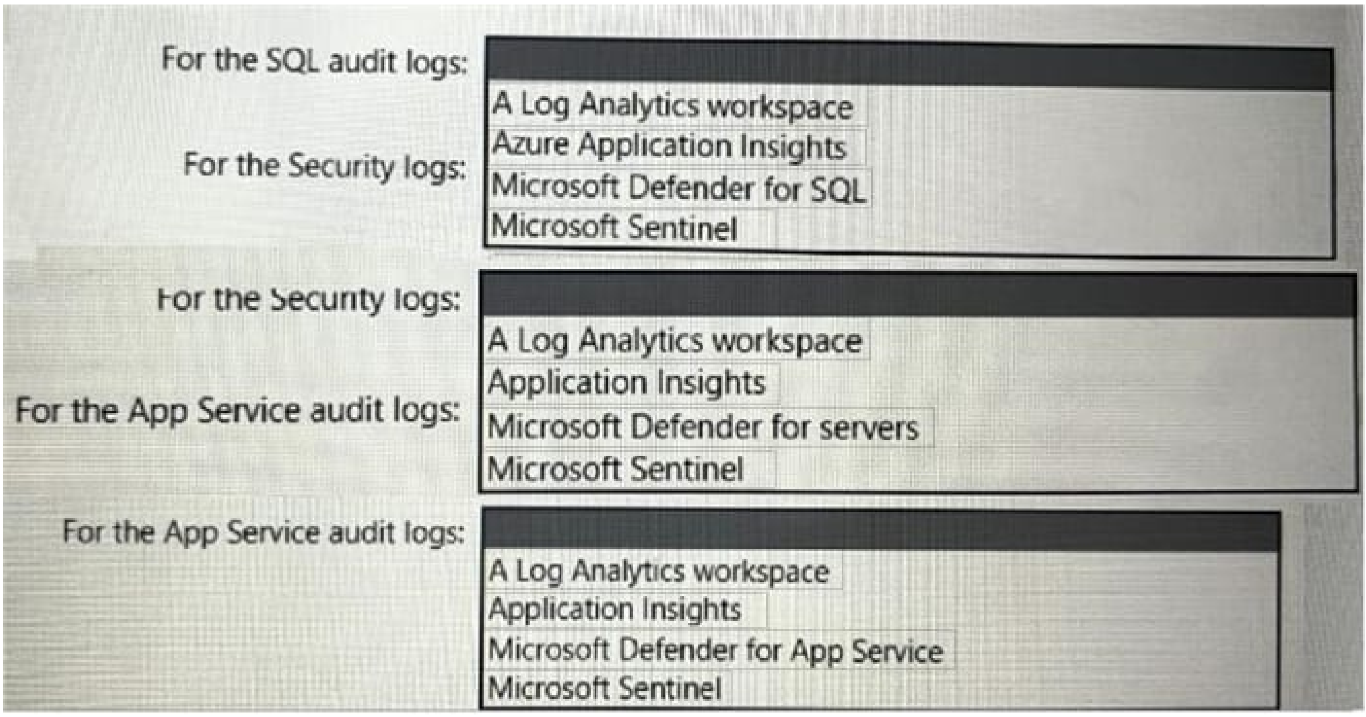
Log all privileged access.

Retain logs for at least 365 days.

Minimize costs.

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:



For the SQL audit logs:

For the Security logs:

A Log Analytics workspace
Azure Application Insights
Microsoft Defender for SQL
Microsoft Sentinel

For the Security logs:

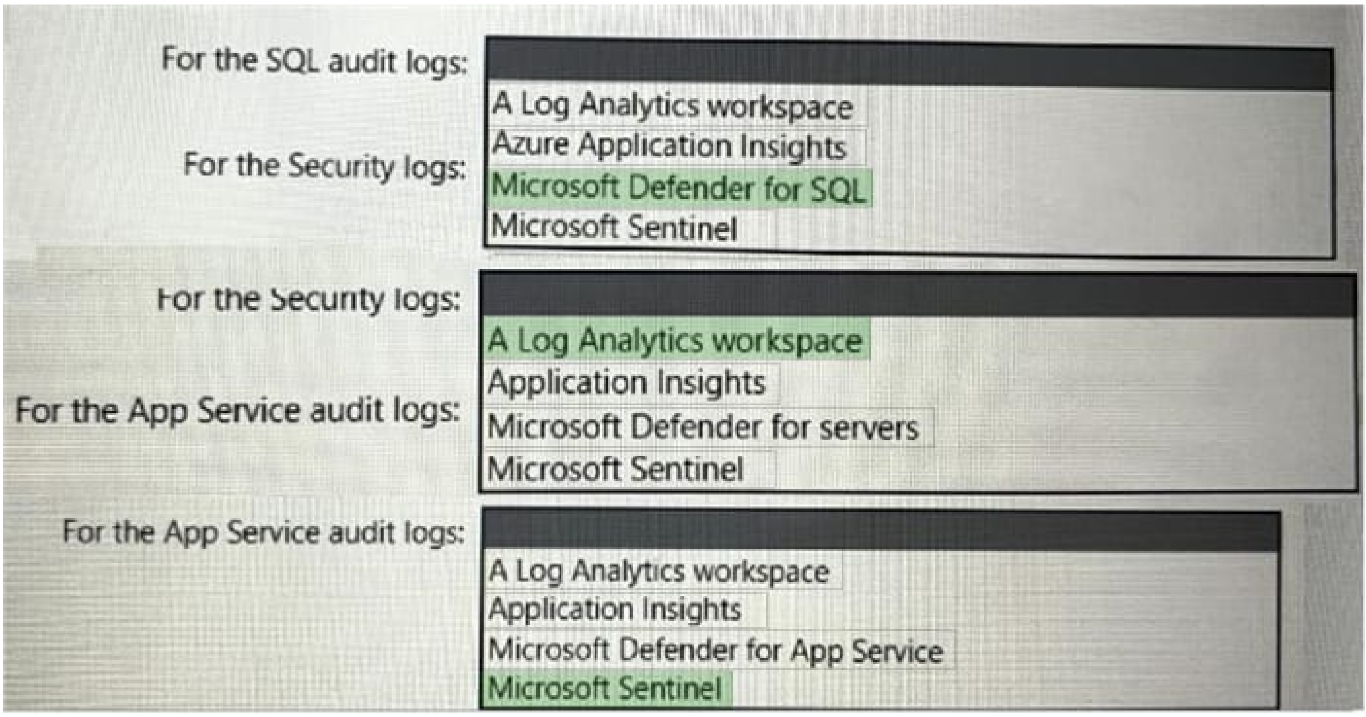
For the App Service audit logs:

A Log Analytics workspace
Application Insights
Microsoft Defender for servers
Microsoft Sentinel

For the App Service audit logs:

A Log Analytics workspace
Application Insights
Microsoft Defender for App Service
Microsoft Sentinel

Correct Answer:



For the SQL audit logs:

For the Security logs:
- A Log Analytics workspace
- Azure Application Insights
- [✓ Microsoft Defender for SQL]
- Microsoft Sentinel

For the Security logs:

For the App Service audit logs:
- [✓ A Log Analytics workspace]
- Application Insights
- Microsoft Defender for servers
- Microsoft Sentinel

For the App Service audit logs:
- A Log Analytics workspace
- Application Insights
- Microsoft Defender for App Service
- [✓ Microsoft Sentinel]

QUESTION 2

Your company plans to deploy several Azure App Service web apps. The web apps will be deployed to the West Europe Azure region. The web apps will be accessed only by customers in Europe and the United States.

You need to recommend a solution to prevent malicious bots from scanning the web apps for vulnerabilities. The solution must minimize the attach surface.

What should you include in the recommendation?

A. Azure Firewall Premium

B. Azure Traffic Manager and application security groups

C. Azure Application Gateway Web Application Firewall (WAF)

D. network security groups (NSGs)

Correct Answer: B

*

Application security groups enable you to configure network security as a natural extension of an application\\'s structure, allowing you to group virtual machines and define network security policies based on those groups. You can reuse your security policy at scale without manual maintenance of explicit IP addresses. The platform handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.

*

Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions. Traffic Manager also provides your public endpoints with high availability and quick responsiveness.

Traffic Manager uses DNS to direct the client requests to the appropriate service endpoint based on a traffic-routing method. Traffic manager also provides health monitoring for every endpoint.

Incorrect:

Not C: Azure Application Gateway Web Application Firewall is too small a scale solution in this scenario.

Note: Attacks against a web application can be monitored by using a real-time Application Gateway that has Web Application Firewall, enabled with integrated logging from Azure Monitor to track Web Application Firewall alerts and easily

monitor trends.

Reference: https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/app-service-security-baseline

QUESTION 3

You have Windows 11 devices and Microsoft 365 E5 licenses.

You need to recommend a solution to prevent users from accessing websites that contain adult content such as gambling sites.

What should you include in the recommendation?

A. Microsoft Endpoint Manager

B. Compliance Manager

C. Microsoft Defender for Cloud Apps

D. Microsoft Defender for Endpoint

Correct Answer: D

Web content filtering is part of the Web protection capabilities in Microsoft Defender for Endpoint. It enables your organization to track and regulate access to websites based on their content categories. Many of these websites, while not

malicious, might be problematic because of compliance regulations, bandwidth usage, or other concerns.

Note: Turn on web content filtering

From the left-hand navigation in Microsoft 365 Defender portal, select Settings > Endpoints > General > Advanced Features. Scroll down until you see the entry for Web content filtering. Switch the toggle to On and Save preferences.

Configure web content filtering policies

Web content filtering policies specify which site categories are blocked on which device groups. To manage the policies, go to Settings > Endpoints > Web content filtering (under Rules).

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering

QUESTION 4

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 5

Your company has a Microsoft 365 E5 subscription.

Users use Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive for sharing and collaborating.

The company identifies protected health information (PHI) within stored documents and communications.

What should you recommend using to prevent the PHI from being shared outside the company?

A. sensitivity label policies

B. data loss prevention (DLP) policies

C. insider risk management policies

D. retention policies

Correct Answer: B

DLP policies in Microsoft 365 allow you to identify, monitor, and protect sensitive information, such as PHI, within your organization. You can create DLP policies that identify PHI within stored documents and communications and then set rules to prevent the PHI from being shared outside the company. For example, you can create a DLP policy that blocks emails containing PHI from being sent to external recipients, or that prevents documents containing PHI from being shared outside the organization.

Sensitivity label policies allow you to classify and protect sensitive information, but they do not specifically prevent the information from being shared outside the organization. Insider risk management policies are designed to detect and mitigate risks posed by insider threats, but they are not directly related to preventing the sharing of sensitive information. Retention policies allow you to specify how long certain types of information should be retained, but they do not prevent the sharing of sensitive information.