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 tenant.

Your company uses a third-party software as a service (SaaS) app named App1 that is integrated with an Azure AD tenant.

You need to design a security strategy to meet the following requirements:

- Users must be able to request access to App1 by using a self-service request.
- When users request access to App1, they must be prompted to provide additional information about their request.
- Every three months, managers must verify that the users still require access to App1. What should you include in the design?

A.

Microsoft Entra Identity Governance

B.

connected apps in Microsoft Defender for Cloud Apps

C.

access policies in Microsoft Defender for Cloud Apps

D.

Azure AD Application Proxy

Correct Answer: A

QUESTION 2

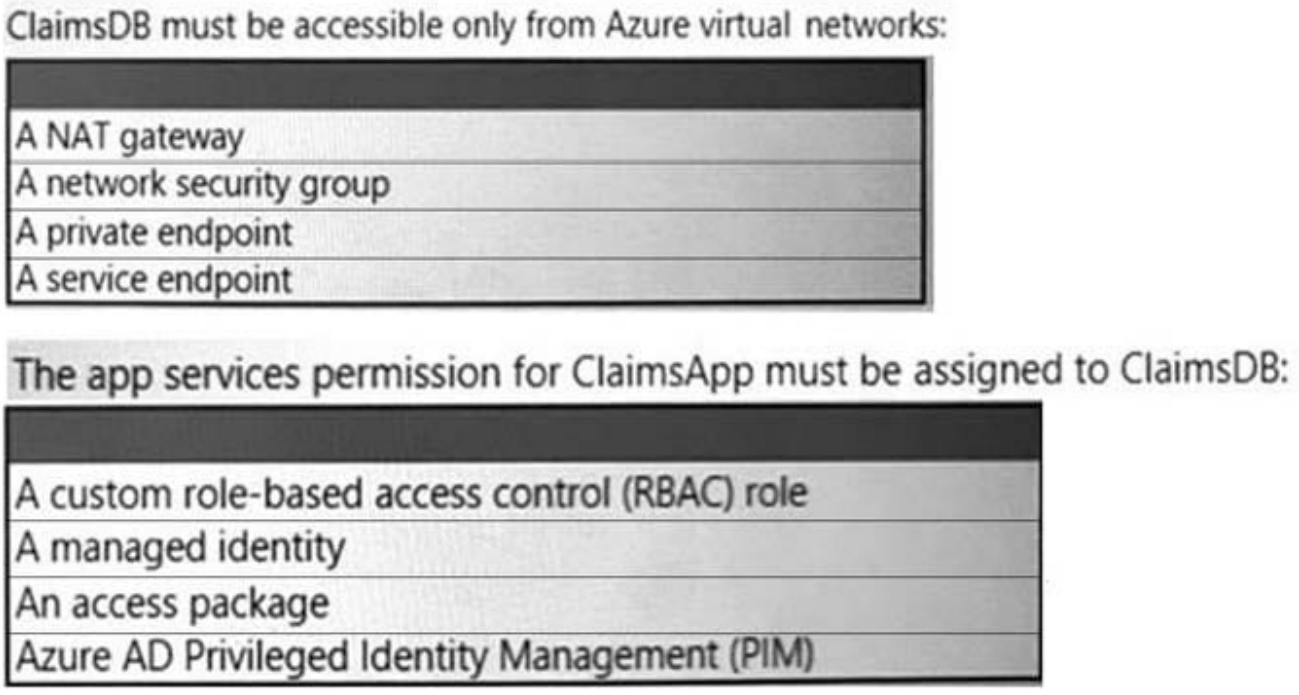
HOTSPOT

You need to recommend a solution to meet the requirements for connections to ClaimsDB.

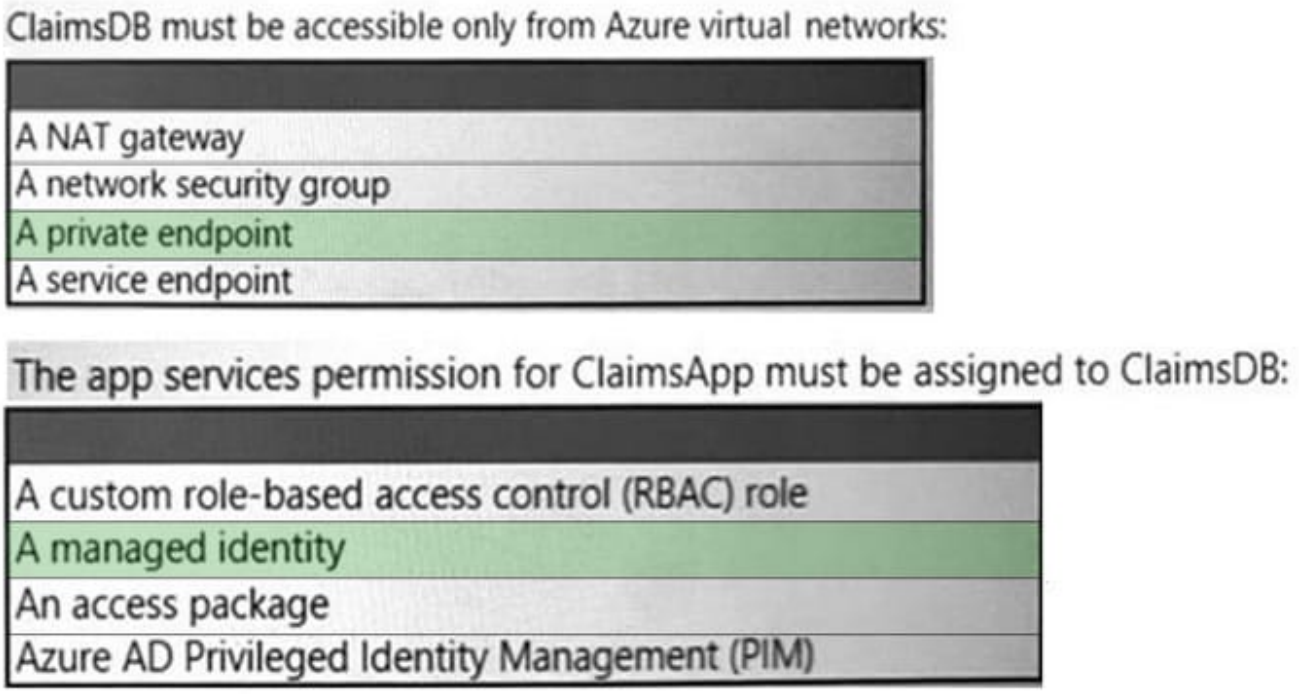
What should you recommend using for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: A private endpoint Scenario: An Azure SQL database named ClaimsDB that contains a table named ClaimDetails

Requirements. ClaimsApp Deployment.

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specifications:

1.

ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.

2.

Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.

3.

ClaimsApp will access data in ClaimsDB.

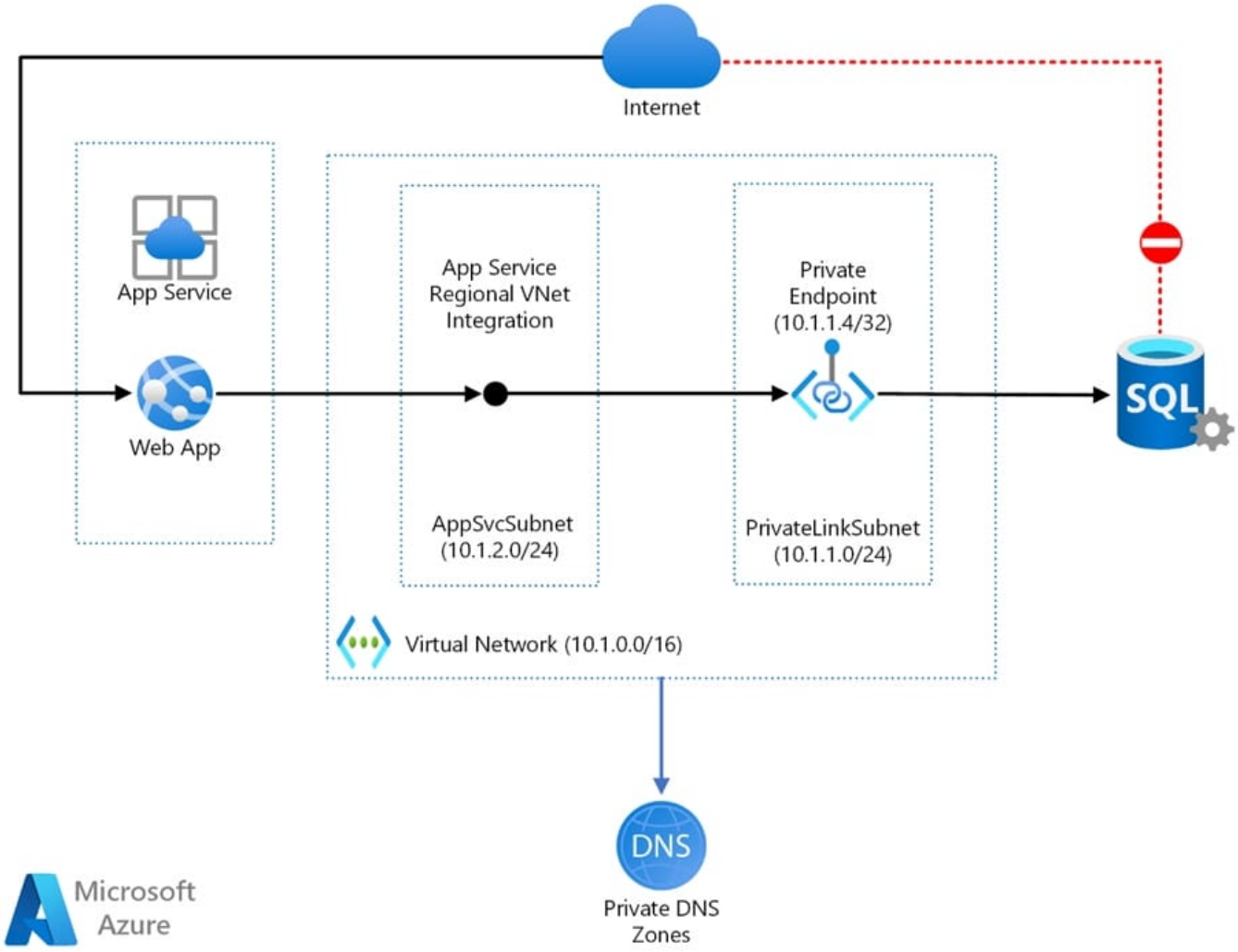
4.

ClaimsDB must be accessible only from Azure virtual networks.

5.

The app services permission for ClaimsApp must be assigned to ClaimsDB.

Web app private connectivity to Azure SQL Database. Architecture: Workflow



1.

Using Azure App Service regional VNet Integration, the web app connects to Azure through an AppSvcSubnet delegated subnet in an Azure Virtual Network.

2.

In this example, the Virtual Network only routes traffic and is otherwise empty, but other subnets and workloads could also run in the Virtual Network.

3.

The App Service and Private Link subnets could be in separate peered Virtual Networks, for example as part of a hub-and-spoke network configuration.

4.

Azure Private Link sets up a private endpoint for the Azure SQL Database in the PrivateLinkSubnet of the Virtual Network.

5.

The web app connects to the SQL Database private endpoint through the PrivateLinkSubnet of the Virtual Network.

The database firewall allows only traffic coming from the PrivateLinkSubnet to connect, making the database inaccessible from the public internet.

Box 2: A managed identity Managed identities for Azure resources provide Azure services with an automatically managed identity in Azure Active Directory. Using a managed identity, you can authenticate to any service that supports Azure AD authentication without managing credentials.

Reference: https://docs.microsoft.com/en-us/azure/architecture/example-scenario/private-web-app/private-web-app https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managed-identities-status

QUESTION 3

Your company has an Azure subscription that has enhanced security enabled for 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 secure score recommendations.

B. From Microsoft Sentinel, configure the Microsoft Defender for Cloud data connector.

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

D. From Defender for Cloud, add a regulatory compliance standard.

Correct Answer: D

Add a regulatory standard to your dashboard

The following steps explain how to add a package to monitor your compliance with one of the supported regulatory standards.

Add a standard to your Azure resources

1.

From Defender for Cloud\\'s menu, select Regulatory compliance to open the regulatory compliance dashboard. Here you can see the compliance standards currently assigned to the currently selected subscriptions.

2.

From the top of the page, select Manage compliance policies. The Policy Management page appears.

3.

Select the subscription or management group for which you want to manage the regulatory compliance posture.

4.

To add the standards relevant to your organization, expand the Industry and regulatory standards section and select Add more standards.

5.

From the Add regulatory compliance standards page, you can search for any of the available standards:

6.

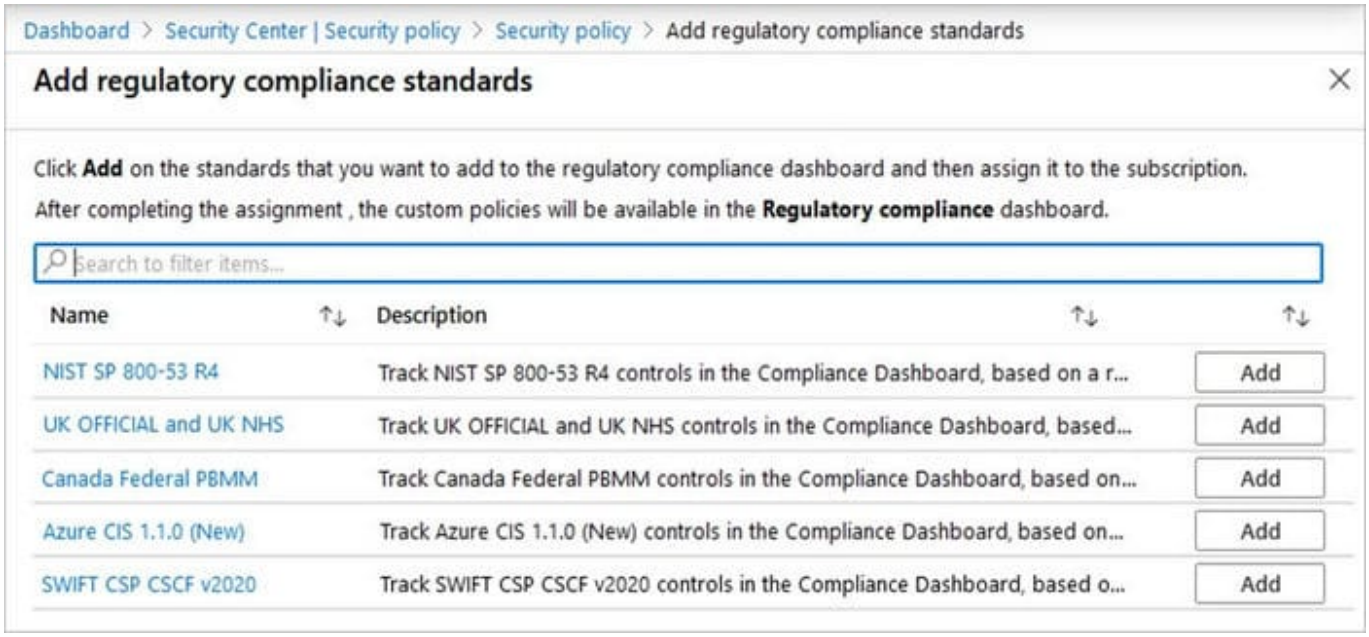
Select Add and enter all the necessary details for the specific initiative such as scope, parameters, and remediation.

7.

From Defender for Cloud\\'s menu, select Regulatory compliance again to go back to the regulatory compliance dashboard.

Your new standard appears in your list of Industry and regulatory standards.

Note: Customize the set of standards in your regulatory compliance dashboard.



Microsoft Defender for Cloud continually compares the configuration of your resources with requirements in industry standards, regulations, and benchmarks. The regulatory compliance dashboard provides insights into your compliance posture based on how you\\'re meeting specific compliance requirements. Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages

QUESTION 4

You have 50 Azure subscriptions.

You need to monitor the resource in the subscriptions for compliance with the ISO 27001:2013 standards. The solution must minimize the effort required to modify the list of monitored policy definitions for the subscriptions.

What are two ways to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Assign an initiative to a management group.

B. Assign a policy to each subscription.

C. Assign a policy to a management group.

D. Assign an initiative to each subscription.

E. Assign a blueprint to each subscription.

F. Assign a blueprint to a management group.

Correct Answer: AF

An Azure Management group is logical containers that allow Azure Administrators to manage access, policy, and compliance across multiple Azure Subscriptions en masse.

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.

F: Blueprint definition locations

When creating a blueprint definition, you\\'ll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have Contributor access to. If the location is a management group, the blueprint is

available to assign to any child subscription of that management group.

A: Create and assign an initiative definition

With an initiative definition, you can group several policy definitions to achieve one overarching goal. An initiative evaluates resources within scope of the assignment for compliance to the included policies.

Note: The Azure Policy Regulatory Compliance built-in initiative definition maps to compliance domains and controls in ISO 27001:2013.

The Azure Policy control mapping provides details on policy definitions included within this blueprint and how these policy definitions map to the compliance domains and controls in ISO 27001. When assigned to an architecture, resources

are evaluated by Azure Policy for non-compliance with assigned policy definitions.

Incorrect:

Not B, D, E: If you plan to apply this policy definition to multiple subscriptions, the location must be a management group that contains the subscriptions you assign the policy to. The same is true for an initiative definition.

Reference: https://docs.microsoft.com/en-us/azure/governance/management-groups/overview https://docs.microsoft.com/en-us/azure/governance/blueprints/overview https://docs.microsoft.com/en-us/azure/governance/policy/samples/iso-27001 https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

QUESTION 5

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 6

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 7

You have a Microsoft 365 E5 subscription and an Azure subscription.

You are designing a Microsoft deployment.

You need to recommend a solution for the security operations team. The solution must include custom views and a dashboard for analyzing security events.

What should you recommend using in Microsoft Sentinel?

A. playbooks

B. workbooks

C. notebooks

D. threat intelligence

Correct Answer: B

After you connected your data sources to Microsoft Sentinel, you get instant visualization and analysis of data so that you can know what\\'s happening across all your connected data sources. Microsoft Sentinel gives you workbooks that provide you with the full power of tools already available in Azure as well as tables and charts that are built in to provide you with analytics for your logs and queries. You can either use built-in workbooks or create a new workbook easily, from scratch or based on an existing workbook.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/get-visibility

QUESTION 8

You have an on-premises datacenter and an Azure Kubernetes Service (AKS) cluster named AKS1.

You need to restrict internet access to the public endpoint of AKS1. The solution must ensure that AKS1 can be accessed only from the public IP addresses associated with the on-premises datacenter.

What should you use?

A. a private endpoint

B. a network security group (NSG)

C. a service endpoint

D. an authorized IP range

Correct Answer: D

Explanation:

By default, the Kubernetes API server uses a public IP address and a fully qualified domain name (FQDN). You can limit access to the API server endpoint using authorized IP ranges. You can also create a fully private cluster to limit API

server access to your virtual network.

Reference:

https://learn.microsoft.com/en-us/azure/aks/concepts-security

QUESTION 9

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.

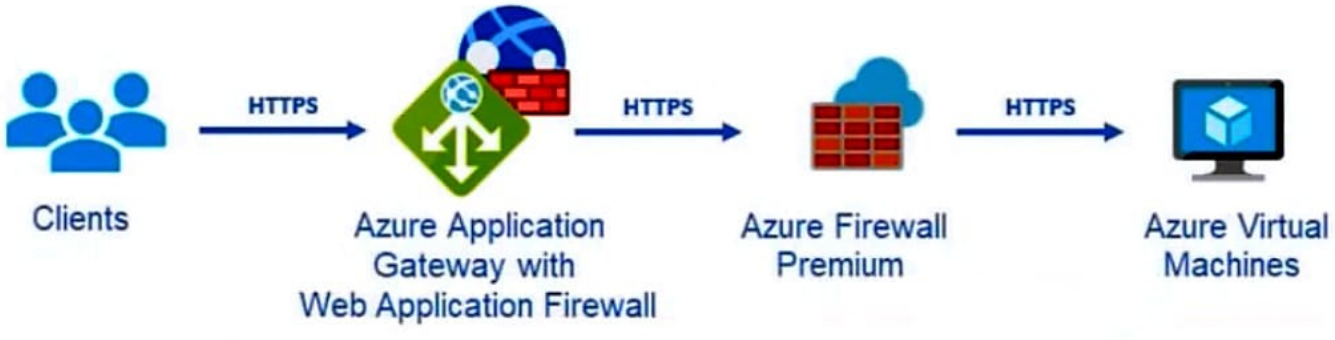
Reference: https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/app-service-security-baseline

QUESTION 10

HOTSPOT

Your company uses Microsoft Defender for Cloud and Microsoft Sentinel.

The company is designing an application that will have the architecture shown in the following exhibit.



You are designing a logging and auditing solution for the proposed architecture. The solution must meet the following requirements:

1.

Integrate Azure Web Application Firewall (WAF) logs with Microsoft Sentinel.

2.

Use Defender for Cloud to review alerts from the virtual machines.

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

NOTE: Each correct selection is worth one point.

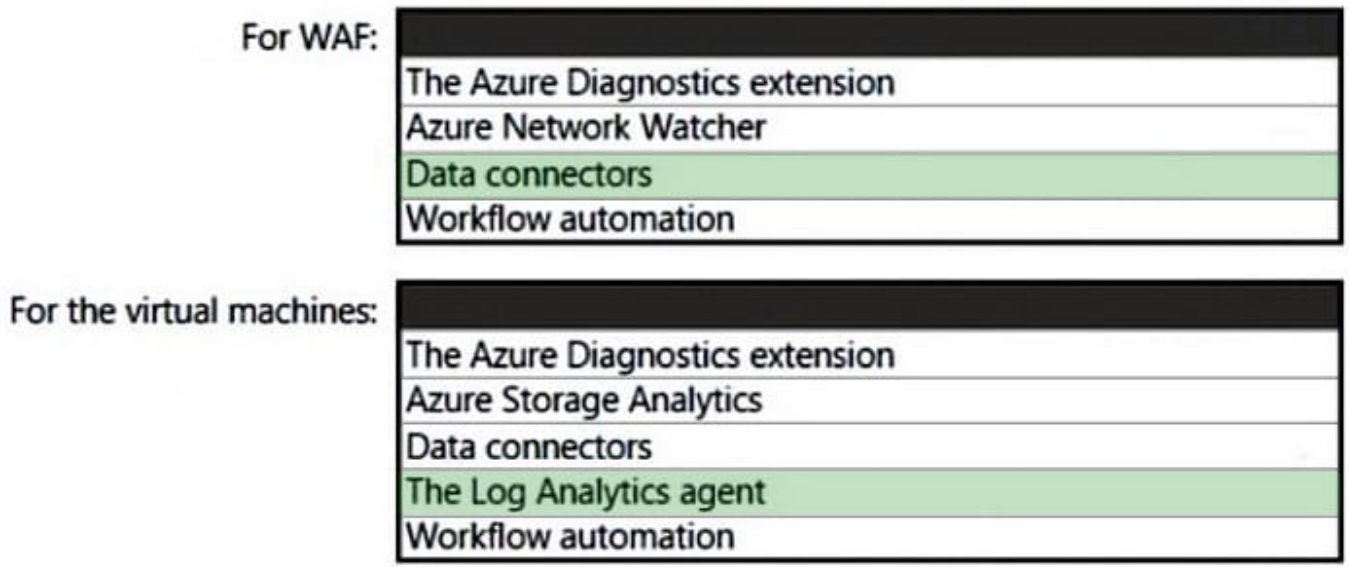
Hot Area:

Answer Area

For WAF:	The Azure Diagnostics extension Azure Network Watcher Data connectors Workflow automation
For the virtual machines:	The Azure Diagnostics extension Azure Storage Analytics Data connectors The Log Analytics agent Workflow automation

Correct Answer:

Answer Area



Box 1: Data connectors

Microsoft Sentinel connector streams security alerts from Microsoft Defender for Cloud into Microsoft Sentinel.

Launch a WAF workbook (see step 7 below)

The WAF workbook works for all Azure Front Door, Application Gateway, and CDN WAFs. Before connecting the data from these resources, log analytics must be enabled on your resource.

To enable log analytics for each resource, go to your individual Azure Front Door, Application Gateway, or CDN resource:

1.

Select Diagnostic settings.

2.

Select + Add diagnostic setting.

3.

In the Diagnostic setting page (details skipped)

4.

On the Azure home page, type Microsoft Sentinel in the search bar and select the Microsoft Sentinel resource.

5.

Select an already active workspace or create a new workspace.

6.

On the left side panel under Configuration select Data Connectors.

7.

Search for Azure web application firewall and select Azure web application firewall (WAF). Select Open connector page on the bottom right.

8.

Follow the instructions under Configuration for each WAF resource that you want to have log analytic data for if you haven\\'t done so previously.

9.

Once finished configuring individual WAF resources, select the Next steps tab. Select one of the recommended workbooks. This workbook will use all log analytic data that was enabled previously. A working WAF workbook should now exist for your WAF resources.

Box 2: The Log Analytics agent

Use the Log Analytics agent to integrate with Microsoft Defender for cloud.

Windows agents

	Azure Monitor agent	Diagnostics extension (WAD)	Log Analytics agent
Environments supported	Azure Other cloud (Azure Arc) On-premises (Azure Arc) Windows Client OS (preview)	Azure	Azure Other cloud On-premises
Agent requirements	None	None	None
Data collected	Event Logs Performance File based logs (preview)	Event Logs ETW events Performance File based logs IIS logs .NET app logs Crash dumps Agent diagnostics logs	Event Logs Performance File based logs IIS logs Insights and solutions Other services
Data sent to	Azure Monitor Logs Azure Monitor Metrics[1]	Azure Storage Azure Monitor Metrics Event Hub	Azure Monitor Logs
Services and features supported	Log Analytics Metrics explorer Microsoft Sentinel (view scope)	Metrics explorer	VM insights Log Analytics Azure Automation Microsoft Defender for Cloud Microsoft Sentinel

The Log Analytics agent is required for solutions, VM insights, and other services such as Microsoft Defender for Cloud.

Note: The Log Analytics agent in Azure Monitor can also be used to collect monitoring data from the guest operating system of virtual machines. You may choose to use either or both depending on your requirements.

Azure Log Analytics agent

Use Defender for Cloud to review alerts from the virtual machines.

The Azure Log Analytics agent collects telemetry from Windows and Linux virtual machines in any cloud, on-premises machines, and those monitored by System Center Operations Manager and sends collected data to your Log Analytics

workspace in Azure Monitor.

Incorrect:

The Azure Diagnostics extension does not integrate with Microsoft Defender for Cloud.

Reference: https://docs.microsoft.com/en-us/azure/web-application-firewall/waf-sentinel

https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview

QUESTION 11

Your company plans to apply the Zero Trust Rapid Modernization Plan (RaMP) to its IT environment.

You need to recommend the top three modernization areas to prioritize as part of the plan.

Which three areas should you recommend based on RaMP? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. data, compliance, and governance

B. infrastructure and development

C. user access and productivity

D. operational technology (OT) and IoT

E. modern security operations

Correct Answer: ACE

RaMP initiatives for Zero Trust

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

Critical security modernization initiatives:

(C) User access and productivity

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

(A) Data, compliance, and governance

2.

Ransomware recovery readiness

3.

Data

(E) Modernize security operations

4.

Streamline response

5.

Unify visibility

6.

reduce manual effort

Incorrect:

As needed

Additional initiatives based on Operational Technology (OT) or IoT usage, on-premises and cloud adoption, and security for in-house app development:

*

(not D) OT and Industrial IoT Discover Protect Monitor

*

Datacenter and DevOps Security Security Hygiene Reduce Legacy Risk DevOps Integration Microsegmentation

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

QUESTION 12

Your company has a Microsoft 365 ES subscription.

The Chief Compliance Officer plans to enhance privacy management in the working environment.

You need to recommend a solution to enhance the privacy management. The solution must meet the following requirements:

1.

Identify unused personal data and empower users to make smart data handling decisions.

2.

Provide users with notifications and guidance when a user sends personal data in Microsoft Teams.

3.

Provide users with recommendations to mitigate privacy risks. What should you include in the recommendation?

A. communication compliance in insider risk management

B. Microsoft Viva Insights

C. Privacy Risk Management in Microsoft Priva

D. Advanced eDiscovery

Correct Answer: C

Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Privacy Risk Management policies are meant to be internal

guides and can help you:

Detect overexposed personal data so that users can secure it.

Spot and limit transfers of personal data across departments or regional borders.

Help users identify and reduce the amount of unused personal data that you store.

Incorrect:

Not B: Microsoft Viva Insights provides personalized recommendations to help you do your best work. Get insights to build better work habits, such as following through on commitments made to collaborators and protecting focus time in the

day for uninterrupted, individual work.

Not D: The Microsoft Purview eDiscovery (Premium) solution builds on the existing Microsoft eDiscovery and analytics capabilities. eDiscovery (Premium) provides an end-to-end workflow to preserve, collect, analyze, review, and export

content that\\'s responsive to your organization\\'s internal and external investigations.

Reference: https://docs.microsoft.com/en-us/privacy/priva/risk-management

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 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 onboarding all virtual machines to Microsoft Defender for Endpoint.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

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 14

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 15

You design cloud-based software as a service (SaaS) solutions.

You need to recommend a recovery solution for ransomware attacks. The solution must follow Microsoft Security Best Practices.

What should you recommend doing first?

A. Develop a privileged identity strategy.

B. Implement data protection.

C. Develop a privileged access strategy.

D. Prepare a recovery plan.

Correct Answer: D

Recommend a ransomware strategy by using Microsoft Security Best Practices The three important phases of ransomware protection are:

*

create a recovery plan

*

limit the scope of damage

*

harden key infrastructure elements

Plan for ransomware protection and extortion-based attacks Phase 1 of ransomware protection is to develop a recovery plan. The first thing you should do for these attacks is prepare your organization so that it has a viable alternative to paying the ransom. While attackers in control of your organization have a variety of ways to pressure you into paying, the demands

primarily focus on two categories:

Pay to regain access

Pay to avoid disclosure

Reference:

https://learn.microsoft.com/en-us/training/modules/recommend-ransomware-strategy-by-using-microsoft-security-best-practices/

https://learn.microsoft.com/en-us/training/modules/recommend-ransomware-strategy-by-using-microsoft-security-best-practices/2-plan-for-ransomware-protection-extortion-based-attacks