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.geekcert.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 have an Azure subscription that is used as an Azure landing zone for an application. You need to evaluate the security posture of all the workloads in the landing zone. What should you do first?

A. Configure Continuous Integration/Continuous Deployment (CI/CD) vulnerability scanning.

B. Obtain Azure AD Premium Plan 2 licenses.

C. Add Microsoft Sentinel data connectors.

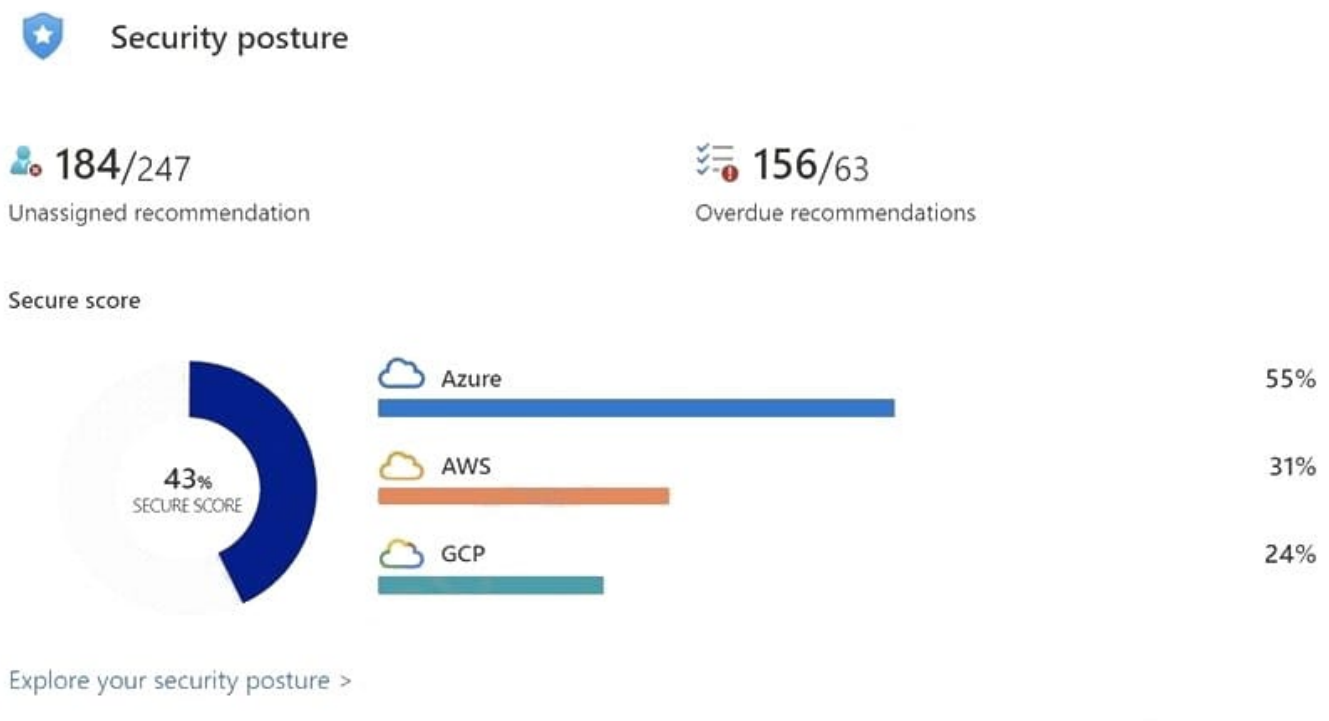
D. Enable the Defender plan for all resource types in Microsoft Defender for Cloud.

Correct Answer: D

You can evaluate security postures by using Microsoft Defender for Cloud.

Defender for Cloud continually assesses your resources, subscriptions, and organization for security issues. It then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation: the higher the

score, the lower the identified risk level.



Note: Security in the Azure landing zone accelerator

Security is at the core of the Azure landing zone accelerator. As part of the implementation, many tools and controls are deployed to help organizations quickly achieve a security baseline.

For example, the following are included:

Tools:

Microsoft Defender for Cloud, standard or free tier

Microsoft Sentinel

Azure DDoS standard protection plan (optional)

Azure Firewall

Web Application Firewall (WAF)

Privileged Identity Management (PIM)

Incorrect:

Not C: Microsoft Sentinel uses data from Microsoft Defender for Cloud, so would need setup Defender for Cloud first.

Reference: https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/3-postures-use-microsoft-defender-for-cloud https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/5-design-security-for-azure-landing-zone

---

QUESTION 2

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 access restrictions to allow traffic from the backend IP address of the Front Door instance.

Does this meet the goal?

A. Yes

B. No

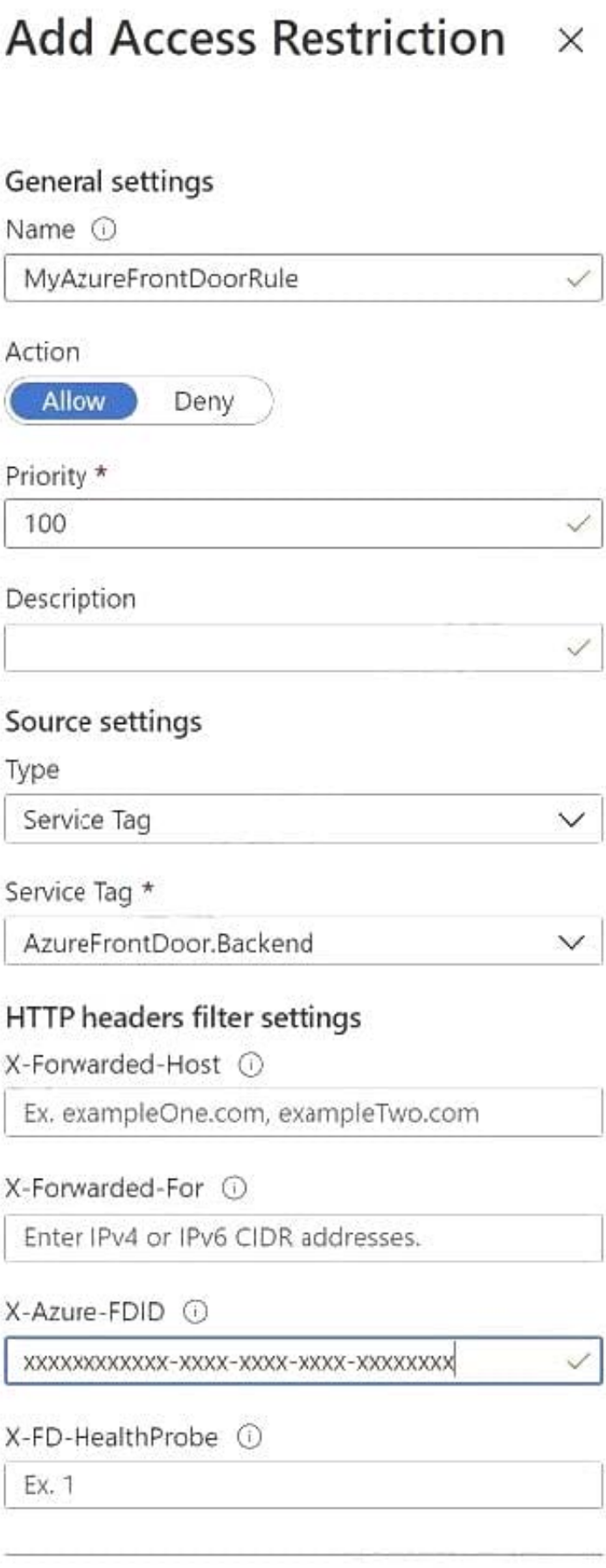
Correct Answer: B

Correct Solution: 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.

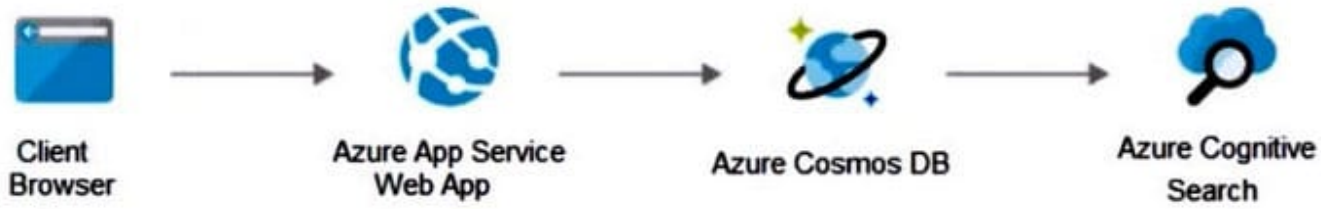

Add Access Restriction
General settings
Name
MyAzureFrontDoorRule
Action
Allow
Deny
Priority *
100
Description
Source settings
Type
Service Tag
Service Tag *
AzureFrontDoor.Backend
HTTP headers filter settings
X-Forwarded-Host
Ex. exampleOne.com, exampleTwo.com
X-Forwarded-For
Enter IPv4 or IPv6 CIDR addresses.
X-Azure-FDID
xxxxxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx
X-FD-HealthProbe
Ex. 1

Reference: https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#managing-access-restriction-rules Reference:

QUESTION 3

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.

Your on-premises network contains an e-commerce web app that was developed in Angular and Node,js. The web app uses a MongoDB database. You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.

Solution: You recommend creating private endpoints for the web app and the database layer.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

How to Use Azure Private Endpoints to Restrict Public Access to WebApps.

As an Azure administrator or architect, you are sometimes asked the question: “How can we safely deploy internal business applications to Azure App Services?”

These applications characteristically are:

Not accessible from the public internet.

Accessible from within the on-premises corporate network

Accessible via an authorized VPN client from outside the corporate network.

For such scenarios, we can use Azure Private Links, which enables private and secure access to Azure PaaS services over Azure Private Endpoints, along with the Site-to-Site VPN, Point-to-Site VPN, or the Express Route. Azure Private

Endpoint is a read-only network interface service associated with the Azure PAAS Services. It allows you to bring deployed sites into your virtual network, limiting access to them at the network level.

It uses one of the private IP addresses from your Azure VNet and associates it with the Azure App Services. These services are called Private Link resources. They can be Azure Storage, Azure Cosmos DB, SQL, App Services Web

App,

your own / partner owned services, Azure Backups, Event Grids, Azure Service Bus, or Azure Automations.

Reference: https://www.varonis.com/blog/securing-access-azure-webapps

QUESTION 4

HOTSPOT

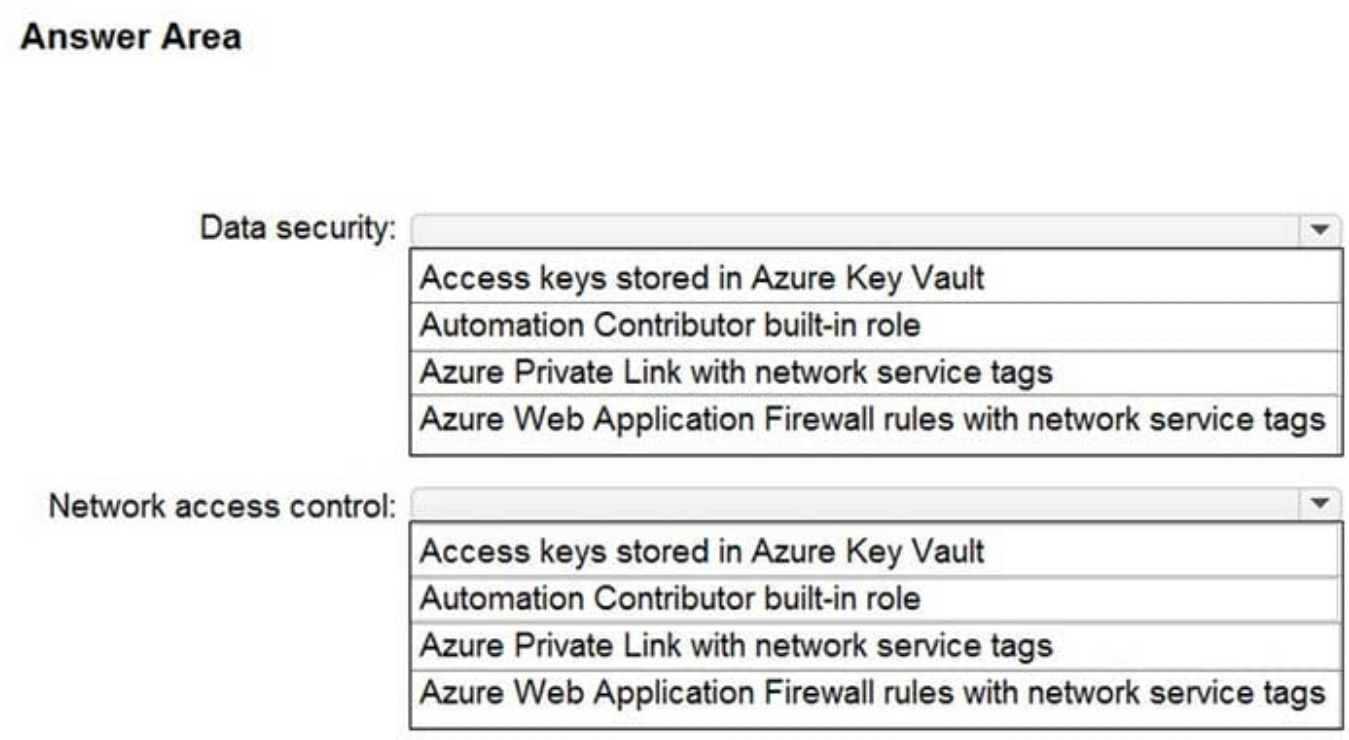
You are designing security for a runbook in an Azure Automation account. The runbook will copy data to Azure Data Lake Storage Gen2.

You need to recommend a solution to secure the components of the copy process.

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

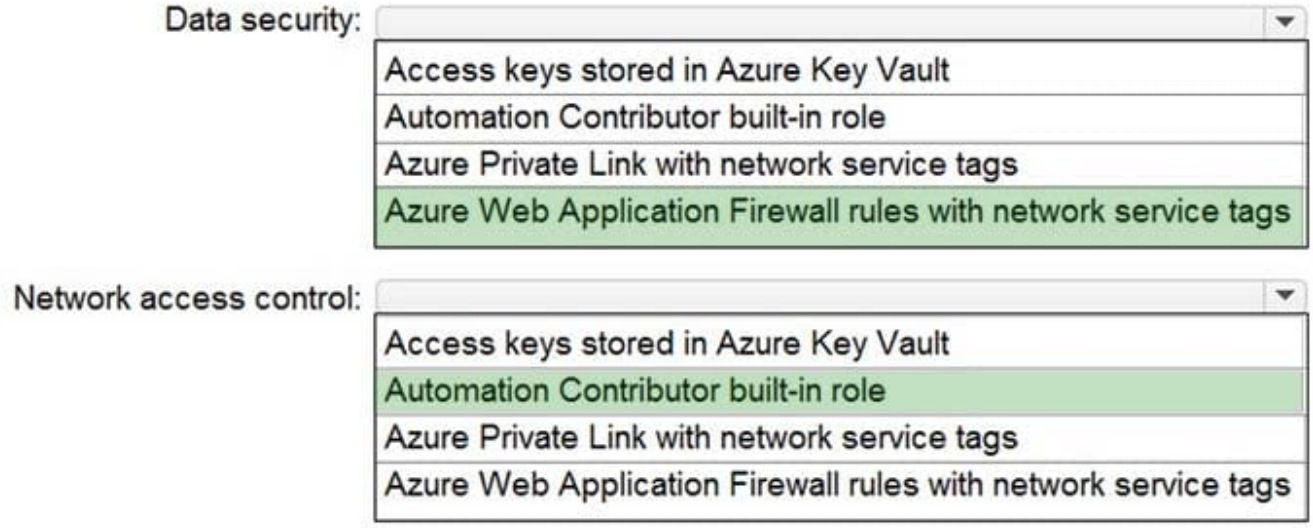
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area



Box 1: Azure Web Application Firewall with network service tags A service tag represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change, minimizing the complexity of frequent updates to network security rules.

You can use service tags to define network access controls on network security groups, Azure Firewall, and user-defined routes.

Incorrect:

* Not Azure private link with network service tags Network service tags are not used with Private links.

Box 2: Automation Contributor built-in role

The Automation Contributor role allows you to manage all resources in the Automation account, except modifying other user\\'s access permissions to an Automation account.

Reference: https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview

https://docs.microsoft.com/en-us/azure/automation/automation-role-based-access-control

QUESTION 5

You are creating an application lifecycle management process based on the Microsoft Security Development Lifecycle (SDL).

You need to recommend a security standard for onboarding applications to Azure. The standard will include recommendations for application design, development, and deployment

What should you include during the application design phase?

A. static application security testing (SAST) by using SonarQube

B. dynamic application security testing (DAST) by using Veracode

C. threat modeling by using the Microsoft Threat Modeling Tool

D. software decomposition by using Microsoft Visual Studio Enterprise

Correct Answer: C

Threat modeling is a core element of the Microsoft Security Development Lifecycle (SDL). It\\'s an engineering technique you can use to help you identify threats, attacks, vulnerabilities, and countermeasures that could affect your application.

You can use threat modeling to shape your application\\'s design, meet your company\\'s security objectives, and reduce risk.

Incorrect:

Not B: Advantages of Veracode\\'s DAST test solution

With a blackbox test tool from Veracode, you can:

Simulate the actions of an actual attacker to discover vulnerabilities not found by other testing techniques.

Run tests on applications developed in any language – JAVA/JSP, PHP and other engine-driven web applications.

Provide development and QA teams with a report on critical vulnerabilities along with information that lets them recreate the flaws.

Fix issues more quickly with detailed remediation information.

Develop long-term strategies for improving application security across your software portfolio using guidance and proactive recommendations from Veracode\\'s expert.

Not D: SonarQube is a leading automatic code review tool to detect bugs, vulnerabilities and code smells in your code. Using Static Application Security Testing (SAST) you can do an analysis of vulnerabilities in your code, also known as

white-box testing to find about 50% of likely issues.

Reference: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling