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.pass4itsure.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 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. adaptive application controls in Defender for Cloud

B. app protection policies in Microsoft Endpoint Manager

C. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps

D. Azure Security Benchmark compliance controls in Defender for Cloud

Correct Answer: A

Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machines.

Often, organizations have collections of machines that routinely run the same processes. Microsoft Defender for Cloud uses machine learning to analyze the applications running on your machines and create a list of the known-safe software.

Allowlists are based on your specific Azure workloads, and you can further customize the recommendations using the instructions below.

When you\\'ve enabled and configured adaptive application controls, you\\'ll get security alerts if any application runs other than the ones you\\'ve defined as safe.

Incorrect:

Not B: App protection policies (APP) are rules that ensure an organization\\'s data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of

actions that are prohibited or monitored when the user is inside the app. A managed app is an app that has app protection policies applied to it, and can be managed by Intune.

Not C: Cloud Discovery anomaly detection policy reference. 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.

Not D: The Azure Security Benchmark (ASB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure. This benchmark is part of a set of holistic security guidance.

Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls

https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy

https://docs.microsoft.com/en-us/defender-cloud-apps/cloud-discovery-anomaly-detection-policy

https://docs.microsoft.com/en-us/security/benchmark/azure/overview

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 based on HTTP headers that have the Front Door ID.

Does this meet the goal?

A. Yes

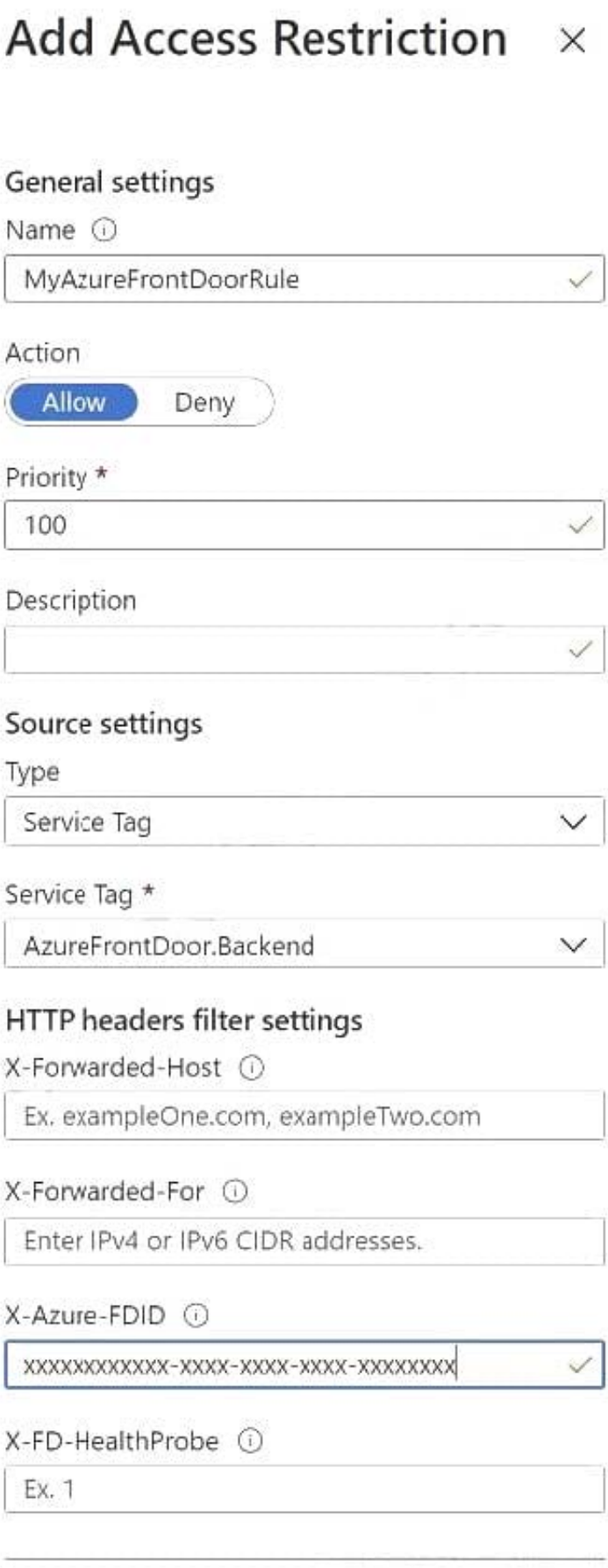
B. No

Correct Answer: A

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

QUESTION 3

HOTSPOT

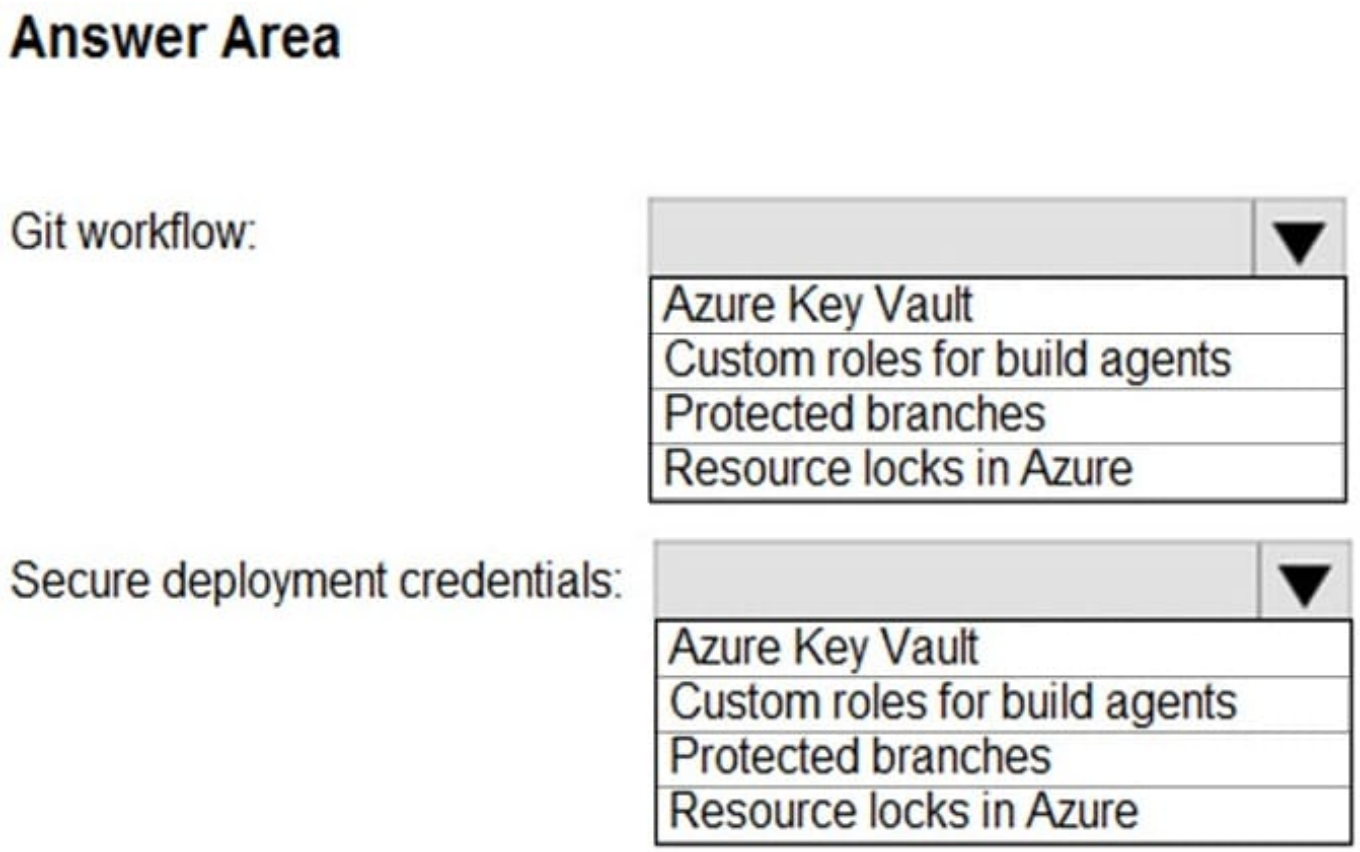
You use Azure Policy with Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows.

You need to recommend best practices to secure the stages of the CI/CD workflows based on the Microsoft Cloud Adoption Framework for Azure.

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

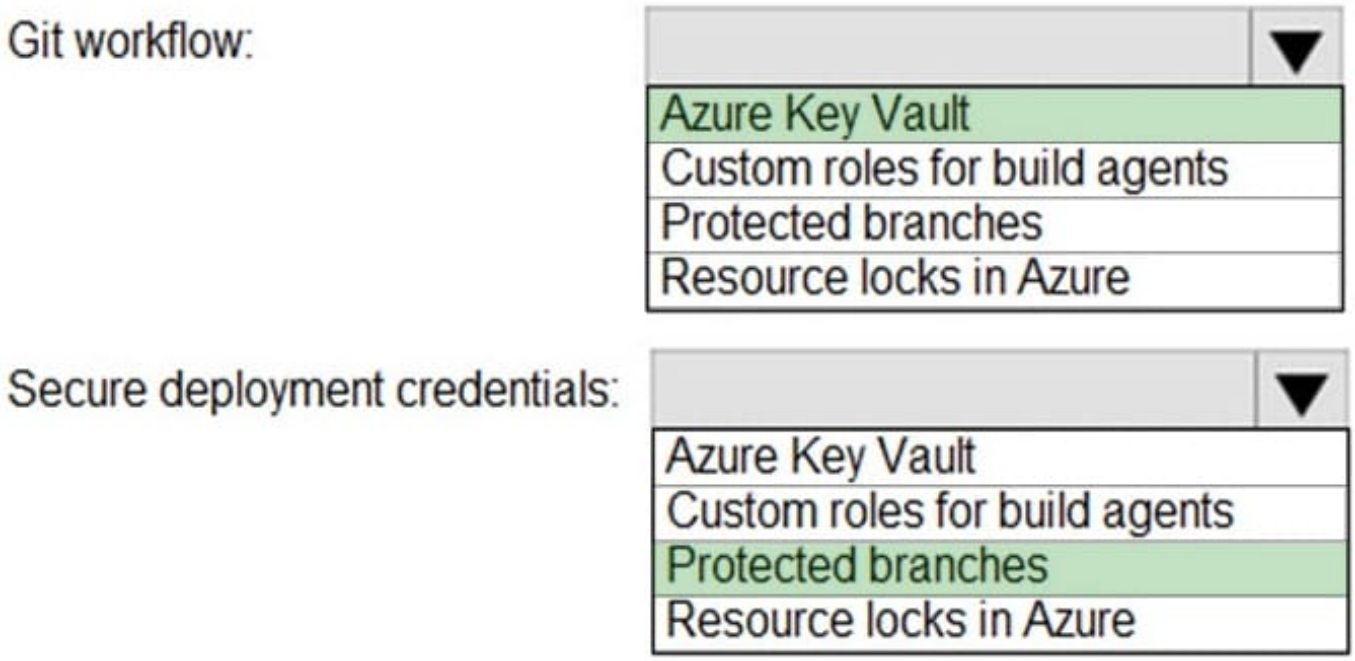
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area



Box 1: Protected branches

Git workflow

The pull request workflow is designed to introduce healthy friction, which is why it should only be applied to secure specific Git branches. Especially the branches that will trigger automated workflows that can deploy, configure, or in any other

way affect your cloud resources. These branches are called protected branches.

Restrict access to protected branches

The pull request workflow is used together with restricted access controls. The pull request workflow can\\'t be enforced however, unless the server is configured to reject direct changes to protected branches.

A developer can\\'t push directly to the production branch, but instead must create a pull request that targets the protected branch. Each SCM vendor has a different flavor for achieving restricted access to protected branches. For example, with

GitHub this feature is only available for organizations using GitHub team or GitHub Enterprise cloud.

Box 2: Azure Key Vault

Secure your deployment credentials

Pipelines and code repositories should not include hard-coded credentials and secrets. Credentials and secrets should be stored elsewhere and use CI vendor features for security. Because pipelines run as headless agents, they should

never use an individual\\'s password.

Azure Key Vault

If your CI platform supports it, consider storing credentials in a dedicated secret store, for example Azure Key Vault. Credentials are fetched at runtime by the build agent and your attack surface is reduced.

Reference:

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/best-practices/secure-devops

QUESTION 4

Your company has on-premises Microsoft SQL Server databases.

The company plans to move the databases to Azure.

You need to recommend a secure architecture for the databases that will minimize operational requirements for patching and protect sensitive data by using dynamic data masking. The solution must minimize costs.

What should you include in the recommendation?

A. Azure SQL Managed Instance

B. Azure Synapse Analytics dedicated SQL pools

C. Azure SQL Database

D. SQL Server on Azure Virtual Machines

Correct Answer: C

Azure SQL Database is a general-purpose relational database, provided as a managed service. Categorized as a platform as a service (PaaS), Azure SQL Databases are built on standardized hardware and software that is owned, hosted, and maintained by Microsoft. When using Azure SQL Database, you pay-as-you-go, with the option to scale up or out with no service interruption.

Within Azure SQL Database, you have the option to deploy a managed instance. Azure SQL Database Managed Instance is a collection of system and user databases with a shared set of resources. In addition to all the PaaS benefits of Azure SQL Database, this option provides a native virtual network (VNet) and near 100 percent compatibility with on-premises SQL Server. Azure SQL Database Managed Instance provides you with full SQL Server access and feature compatibility for migrating SQL Servers to Azure.

Recommendation: Choose Azure SQL Database for your modern cloud applications, or when you have time constraints in development and marketing.

QUESTION 5

Your company is preparing for cloud adoption.

You are designing security for Azure landing zones.

Which two preventative controls can you implement to increase the secure score? Each NOTE: Each correct selection is worth one point.

A. Azure Firewall

B. Azure Web Application Firewall (WAF)

C. Microsoft Defender for Cloud alerts

D. Azure Active Directory (Azure AD Privileged Identity Management (PIM)

E. Microsoft Sentinel

Correct Answer: AB

This question is to increase secure score. Here is a long reference page from Microsoft of security recommendations that can increase your secure score. Sentinel and PIM are not on it. The explanation makes a great point about alerts not being preventive, which is a key aspect of the required solution.

https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

SC-100 Study Guide SC-100 Exam Questions SC-100 Braindumps