

Exam Questions SC-500

Microsoft Certified: Cloud and AI Security Engineer Associate

<https://www.2passeasy.com/dumps/SC-500/>



NEW QUESTION 1

You need to delegate a user to implement the planned change for Defender for Cloud. The solution must follow the principle of least privilege. Which user should you choose?

- A. Admin1
- B. Admin2
- C. Admin3
- D. Admin4

Answer: A

Explanation:

Admin1 is the visible least-privilege delegate for the planned Defender for Cloud change. Defender for Cloud administration should be delegated to the user with the specific security or Defender permissions needed for the task, not to broader administrators unless required. Choosing a higher privileged account would violate the least-privilege requirement. The source file's case-study background is not visible, so the answer follows the displayed answer selection and the general Defender for Cloud RBAC model. The SC-500 study guide places these tasks under security posture, event collection, Defender CSPM, EASM, Sentinel, and Security Copilot operations. The exam expects the control that minimizes analyst effort while preserving correct permissions and data flow. The selected answer reflects that service boundary and avoids a broader or merely investigative alternative. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Defender for Cloud least-privilege administration; Microsoft Learn > built-in Azure roles for Defender for Cloud.

NEW QUESTION 2

HOTSPOT - Overview - Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas. Contoso has a hybrid environment that contains on-premises servers connected to Azure, a Microsoft 365 E5 subscription, and an Azure subscription named Sub1. Existing Environment. Microsoft Entra tenant Contoso has a Microsoft Entra tenant named contoso.com that contains the users shown in the following table.

Name	Tier
DeviceInfo	Analytics
DnsEvents	Analytics

Requirements. Planned changes - Contoso plans to implement the following changes: Integrate AKS1 with Vault1. Enable Microsoft Entra Kerberos authentication for all supported storage. Configure auditing for sql1 by using the Azure portal and store audit logs in a centralized location. Requirements. Technical requirements Contoso identifies the following technical requirements: Protect Server1 by using file integrity monitoring. Protect AKS1 by using Microsoft Defender for Cloud. Configure Microsoft Sentinel to retain data for the maximum supported duration without changing the tier. Store objects used for authentication and encryption in Vault1 and ensure that Vault1 regenerates the objects every 30 days, whenever possible.

User1 has requested to use the AI Administrator role.

Which approvers can approve the request, and how long will User1 be an AI administrator after the role is approved? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Eligible approvers:

Admin1 and Admin3 only ▼

Admin1 only

Admin1 and Admin2 only

Admin1 and Admin3 only

Admin2 and Admin3 only

Maximum active duration of the role:

1 day ▼

8 hours

1 day

2 days

7 days

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Eligible approvers: Admin1 and Admin3 only; Maximum active duration of the role: 1 day

The answer area indicates that Admin1 and Admin3 are the eligible approvers and that the active AI Administrator role duration is one day. This is consistent with PIM role settings: approvers are explicitly configured for a role activation policy, and maximum active duration controls how long the activated role remains available. Other administrators who are not configured as approvers cannot approve the request merely because they hold unrelated roles. This domain is tested through precise scope control: tenant, subscription, resource, application, and data-plane authorization are not interchangeable. The correct choice applies the smallest identity or governance control that enforces the stated requirement. Options that only add users, create registrations, or provide broad administrator

access fail because they do not directly enforce the requested access behavior. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > PIM activation approval and duration; Microsoft Learn > role settings in PIM.

NEW QUESTION 3

Overview - Fabrikam, Inc. is a consulting company. The company has a main office in New York City and branch offices in Amsterdam and Singapore. Existing Environment. Network environment The on-premises network contains a datacenter in each office. Existing Environment. Cloud environment Fabrikam has two Azure subscriptions named Sub1 and Sub2 and a Microsoft 365 subscription that includes Microsoft 365 E5 licenses. All the subscriptions are linked to a Microsoft Entra tenant named fabrikam.com that contains the identities shown in the following table.

Name	Location	Deployment type
ER1	West Europe	ExpressRoute with a connectivity provider
ER2	West Europe	ExpressRoute Metro with a connectivity provider
ER3	East US	ExpressRoute Direct
ER4	Southeast Asia	ExpressRoute Metro Direct

For RG1, create a new Privileged Identity Management (PIM) eligible role assignment that assigns the Contributor role to supported groups. Planned Changes and Requirements. Technical Requirements Fabrikam has the following technical requirements: If VM1 is deleted, the permissions for VM1 must be removed automatically. The AKS1 managed identity must only be able to pull images from Registry1. The ID1 managed identity must be able to push images to and pull images from Registry1. All the data in the storage accounts must be encrypted by using Fabrikam-managed keys. All outbound traffic from the function apps to the on-premises network must use ExpressRoute circuits. ExpressRoute connectivity between the on-premises network and the Azure environment must be encrypted by using Layer 2 or Layer 3 encryption.

You need to implement the planned change for storage2 The solution must meet the technical requirements for storage encryption.

What should you do?

- A. Enable purge protection for storage2.
- B. Create an encryption scope in storage2.
- C. Configure storage2 to use an account encryption key.
- D. Assign an Azure role-based access control (Azure RBAC) role to storage2.

Answer: C

Explanation:

Because storage2 must support Azure Table storage, it must be created to use an encryption key scoped to the storage account. Azure Table storage can then be encrypted by using a Fabrikam-managed customer-managed key. Encryption scopes apply to Blob storage and do not meet the requirement for Table storage encryption.

Reference:

<https://learn.microsoft.com/en-us/azure/storage/common/account-encryption-key-create?tabs=portal>

<https://learn.microsoft.com/en-us/azure/storage/blobs/encryption-scope-overview>

NEW QUESTION 4

You need to protect the applications hosted on AKS1. The solution must meet the technical requirements.

Which Defender for Cloud plan should you enable?

- A. Microsoft Defender for Servers
- B. Microsoft Defender for App Service
- C. Microsoft Defender for Containers
- D. Microsoft Defender for Resource Manager
- E. Microsoft Defender for Storage

Answer: C

Explanation:

AKS workload protection is provided by Microsoft Defender for Containers. That plan covers Kubernetes posture, runtime threat detection, image risk signals, and container workload protections. Defender for Servers protects VMs and Arc servers, Defender for App Service protects web apps, Resource Manager protects control-plane operations, and Defender for Storage protects storage accounts. Because the applications are hosted on AKS1, Defender for Containers is the correct plan. The compute domain tests whether protection is applied before deployment, during runtime, or through posture assessment. The selected answer matches the phase described in the requirement. Detection-only tools are not acceptable when the requirement says prevent, and local installation methods are inferior when Defender for Cloud, Azure Policy, or Azure Machine Configuration can enforce the control centrally. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Defender for Containers; Microsoft Learn > AKS workload protection.

NEW QUESTION 5

You have an Azure subscription that contains the following servers:

- 200 virtual machines that run either Windows Server or Ubuntu Server
- 50 Azure Arc enabled servers

You use Azure Policy to manage compliance across all the servers.

You need to enforce an organization-specific security baseline. The solution must meet the following requirements:

- Customize a built-in security baseline.
- Ensure that configuration changes to the servers are enforced automatically after the security baseline is deployed.
- ?Minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Answer Area

To customize the baseline:

Use Azure Machine Configuration.
 Use Desired State Configuration (DSC).
 Edit the built-in initiative in JSON directly.

Set enforcement mode to:

Apply and Autocorrect
 Apply and Monitor
 Audit
 DeployIfNotExists

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To customize the baseline: Use Azure Machine Configuration;

Set enforcement mode to: Apply and Autocorrect

Azure Machine Configuration is the correct mechanism for applying and customizing guest configuration baselines across Azure VMs and Azure Arc-enabled servers. It integrates with Azure Policy and can enforce configuration through assignment modes such as Apply and Autocorrect. This provides centralized compliance and automatic correction without building a separate configuration-management pipeline for Windows and Linux servers. The compute domain tests whether protection is applied before deployment, during runtime, or through posture assessment. The selected answer matches the phase described in the requirement. Detection-only tools are not acceptable when the requirement says prevent, and local installation methods are inferior when Defender for Cloud, Azure Policy, or Azure Machine Configuration can enforce the control centrally. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Azure Machine Configuration; Microsoft Learn > assignment modes and remediation.

NEW QUESTION 6

You have an Azure subscription that contains a resource group named RG1.

RG1 contains a Microsoft Security Copilot deployment that is integrated with a Microsoft Sentinel workspace named Workspace1.

Analysts use the Security Copilot standalone experience to retrieve incidents by using the Microsoft Sentinel plugin.

A user named User1 can sign in to Security Copilot but cannot retrieve incidents from Workspace1. You verify that User1 has only the Security Copilot Contributor role.

You need to ensure that User1 can retrieve the incidents. The solution must follow the principle of least privilege and NOT require any configuration changes to Security Copilot.

Which role should you assign to User1?

- A. The Security Reader role in Microsoft Entra
- B. The Microsoft Sentinel Reader role for Workspace1
- C. The Security Copilot Owner role
- D. The Security Administrator role in Microsoft Entra
- E. The Contributor role in Azure for RG1

Answer: B

Explanation:

The user can already sign in to Security Copilot, so the missing permission is not a Security Copilot role. The Sentinel plugin retrieves incidents from the Sentinel workspace and therefore requires the appropriate Microsoft Sentinel data-plane role. Microsoft Sentinel Reader at the Workspace1 scope is the least-privilege role for viewing incidents. Security Administrator, Azure Contributor, or Security Copilot Owner would grant broader permissions than required. The posture and monitoring objective focuses on turning security data into usable operational outcomes. The correct answer either collects the right signal, grants the right security-operations role, or automates incident handling at the correct layer. Distractors often provide dashboards, queries, or broad permissions, but those do not create the requested workflow or least-privilege security capability. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Security Copilot plugins and Sentinel roles; Microsoft Learn > Microsoft Sentinel Reader role.

NEW QUESTION 7

You have a Microsoft Sentinel workspace named Workspace1

You have 100 on-premises servers that run Linux and have the Azure Monitor Agent installed.

You need to collect Syslog events from the Linux servers. The solution must meet the following requirements:

- Ensure that filtering occurs before data is written to Workspace1
- Reduce ingestion costs by excluding low value Syslog messages.

What should you include in the solution?

- A. An Advanced Security Information Model (ASIM) parser
- B. A data collection rule (DCR)
- C. An analytics rule
- D. A table-level filter and split transformation

Answer: B

Explanation:

Filtering must happen before data is written to the Log Analytics workspace. With Azure Monitor Agent, Syslog collection is governed by data collection rules, and DCR transformations or filtering can reduce ingestion before records reach the workspace. An ASIM parser normalizes queried data after ingestion, an analytics rule detects conditions after data exists, and a table-level transformation is not the primary collection control for Linux Syslog from AMA in this scenario. The posture and monitoring objective focuses on turning security data into usable operational outcomes. The correct answer either collects the right signal, grants the right security-operations role, or automates incident handling at the correct layer. Distractors often provide dashboards, queries, or broad permissions, but those do not create the requested workflow or least-privilege security capability. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Syslog event collection; Microsoft Learn > data collection rules for Azure Monitor Agent.

NEW QUESTION 8

You have an Azure Storage account named storage1 that hosts a blob container named container1.

You have an Azure Functions app named app1 that uses a managed identity.

You need to configure app1 to read, write, and delete blobs in container1. The solution must follow the principle of least privilege.

What should you do?

- A. Assign the Storage Account Contributor role to the managed identity of app1 at the scope of storage1.
- B. Assign the Storage Blob Delegator role to the managed identity of app1 at the scope of container1.
- C. Assign the Owner role to the managed identity of app1 at the scope of container1.
- D. Assign the Storage Blob Data Contributor role to the managed identity of app1 at the scope of container1.

Answer: D

Explanation:

Read, write, and delete blob access is data-plane access, and Storage Blob Data Contributor is the least-privilege built-in role for that operation set. Assigning it at the container scope keeps App1 constrained to container1 instead of the entire account. Storage Account Contributor is a management-plane role and is too broad. Storage Blob Delegator is for user delegation keys, not direct blob CRUD. Owner is also unnecessarily privileged. For this domain, least privilege means granting only the required data operation or allowing only the required network flow. The correct response avoids shared keys, broad peering, general contributor roles, or log-only controls when the scenario demands prevention, routing, event triggering, or account-specific configuration. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Storage access; Microsoft Learn > Storage Blob Data Contributor role.

NEW QUESTION 9

You have an Azure virtual network that contains 100 virtual machines and an Azure Firewall instance named FW1.

All the traffic from the virtual machines is routed through FW1.

You need to ensure that FW1 allows access to only a URL of updates.contoso.com and blocks all other outbound traffic.

What should you use?

- A. an inbound NAT rule
- B. an application rule
- C. an outbound NAT rule
- D. a network rule

Answer: B

Explanation:

An Azure Firewall application rule permits outbound HTTP or HTTPS access based on a fully qualified domain name, such as updates.contoso.com. With only that destination allowed, traffic to other outbound web destinations is denied when no matching allow rule exists.

Reference:

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq>

NEW QUESTION 10

You have an Azure subscription named Sub1 that contains an Azure Kubernetes Service (AKS) cluster named cluster1 and an Azure container registry named ACR1. Sub1 has Microsoft Defender for Containers enabled, and runtime protection is active on cluster1.

The developers at your company deploy pods that have elevated privileges, and the deployments are created in cluster1.

You need to prevent pods with elevated privileges from being accepted by cluster1.

What should you do?

- A. Create an Azure Policy for cluster1.
- B. Enable agentless discovery for Kubernetes in Defender for Containers.
- C. Configure runtime threat protection alerts for privileged container activity.
- D. Enable vulnerability assessment for images in ACR1.

Answer: A

Explanation:

Privileged pods must be rejected before they are admitted to the AKS cluster. Azure Policy for AKS integrates with admission control to enforce policies such as denying privileged containers. Runtime alerts can detect privileged activity after deployment, but the requirement is prevention. Agentless Kubernetes discovery and image vulnerability assessment provide visibility; they do not block a privileged pod specification during admission. For SC-500, compute controls are evaluated by workload type: VM, Arc server, AKS, container registry, container group, Functions, Logic Apps, App Service, and AI agent runtime. The right answer uses the Microsoft control that is native to that workload. Broad Azure roles or unrelated monitoring services would either overgrant access or fail to enforce the

required security state. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > AKS security controls; Microsoft Learn > Azure Policy for AKS admission control.

NEW QUESTION 10

HOTSPOT

You have an Azure subscription named Sub1 that contains 50 virtual machines. Sub1 has Microsoft Defender for Cloud enabled.

Sub1 contains an Azure key vault named KV1 and an Azure policy that enforces storing all secrets in KV1.

Occasionally, the developers at your company store plaintext tokens and SSH private keys on the virtual machines.

You need to configure Defender for Cloud to detect plaintext secrets on the virtual machines. The solution must minimize administrative changes to the virtual machines.

How should you configure Defender for Cloud? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Plan to enable:

Defender Cloud Security Posture Management (CSPM)
 Microsoft Defender for Cloud Apps
 Microsoft Defender for Key Vault

Feature to enable:

Agentless machine scanning
 Regulatory compliance
 Vulnerability assessment on the virtual machines

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Plan to enable: Defender Cloud Security Posture Management (CSPM)

Feature to enable: Agentless machine scanning

Defender CSPM supports agentless secrets scanning for Azure virtual machines. Enabling agentless machine scanning allows Defender for Cloud to analyze VM disk snapshots for exposed plaintext tokens and SSH private keys without requiring agents or configuration changes on the virtual machines.

Reference:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/secrets-scanning-servers> <https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-agentless-data-collection>

NEW QUESTION 12

For a site-to-site VPN connection to Azure, which protocol and configuration provide encrypted tunnels between on-premises and the Azure VPN gateway?

- A. Plain HTTP over a public IP
- B. FTP passive mode
- C. IPsec/IKE policy on the VPN gateway
- D. ICMP echo tunneling

Answer: C

Explanation:

Site-to-site VPNs to Azure use IPsec/IKE to establish encrypted tunnels between the on-premises VPN device and the Azure VPN gateway. Configuring a custom IPsec/IKE policy lets you enforce strong cipher suites and key exchange parameters.

NEW QUESTION 16

You are configuring a new Microsoft Sentinel workspace named Workspace1. You have an external IT Service Management (ITSM) system that is NOT supported by any Microsoft Sentinel solutions in Azure Marketplace. You need to ensure that Workspace1 creates service tickets in the ITSM system for all new security incidents. What should you create?

A.a playbook

D.an analytics rule

A. C.a watchlist

Answer: A

Explanation:

A Microsoft Sentinel playbook is an Azure Logic Apps workflow that automates response actions when incidents are created. It can integrate with an external ITSM system through an available connector or API call to create service tickets for new security incidents, even when no packaged Microsoft Sentinel solution exists for that system. Reference: <https://learn.microsoft.com/en-us/azure/sentinel/automation/integrations> <https://learn.microsoft.com/en-us/azure/sentinel/automation/automation> <https://learn.microsoft.com/en-us/azure/sentinel/automation/playbook-recommendations>

NEW QUESTION 17

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SC-500 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SC-500 Product From:

<https://www.2passeasy.com/dumps/SC-500/>

Money Back Guarantee

SC-500 Practice Exam Features:

- * SC-500 Questions and Answers Updated Frequently
- * SC-500 Practice Questions Verified by Expert Senior Certified Staff
- * SC-500 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SC-500 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year