



Microsoft

Exam Questions SC-500

Microsoft Certified: Cloud and AI Security Engineer Associate

NEW QUESTION 1

You have an Azure subscription named Sub1 that contains a storage account named storage1. Sub1 has Microsoft Defender for Storage enabled. Defender for Storage has on-upload malware scanning enabled. The security team at your company requires that all malicious files be processed automatically by a serverless workflow for quarantine and notification. You need to ensure that the malware scan results trigger an automated response. The solution must minimize operational effort. What should you configure?

- A. An Azure Event Grid subscription
- B. Diagnostic settings to send logs to a Log Analytics workspace
- C. Lifecycle management policies
- D. An Azure Monitor alert rule

Answer: A

Explanation:

The security team wants a serverless workflow to run when scan results are produced. Defender for Storage malware scanning emits events that can be subscribed to through Azure Event Grid, and Event Grid can trigger Azure Functions, Logic Apps, or other serverless handlers. Diagnostic settings and Log Analytics are useful for investigation but are not the lowest-effort event trigger for each malicious upload. Lifecycle policies are storage-management controls, not security remediation workflows. Microsoft platform security questions usually hinge on where enforcement occurs: at the resource, server, subnet, firewall policy, private endpoint, or subscription level. The selected answer uses the control plane that owns that enforcement point. Other options are rejected when they only log activity, broaden network access, or protect a different service category. 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 Storage; Microsoft Learn > Event Grid events for malware scanning results.

NEW QUESTION 2

You have an Azure subscription that contains a user named User1 and an Azure Container Registry named ContReg1. You enable content trust for ContReg1. You need to ensure that User1 can create trusted images in ContReg1. The solution must use the principle of least privilege. Which two roles should you assign to User1? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. AcrQuarantineWriter
- B. Contributor
- C. AcrQuarantineReader
- D. AcrPush
- E. AcrImageSigner

Answer: DE

Explanation:

To create trusted images, the user must be able to push images and sign them. AcrPush allows pushing image content to the registry, while AcrImageSigner allows signing trusted images. Contributor would be excessive because it grants broad management rights. Quarantine reader/writer roles relate to quarantine workflows, not content trust signing. The combination of AcrPush and AcrImageSigner matches least privilege for trusted image creation. This answer also follows operational scalability. Microsoft security architecture favors policy-driven deployment, agentless assessment, managed identities, and Defender workload plans where possible. Those mechanisms reduce manual configuration while keeping enforcement tied to the resource type, which is why the selected choice is stronger than manual or after-the-fact alternatives. 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 Container Registry security; Microsoft Learn > ACR roles for push and image signing.

NEW QUESTION 3

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft Sentinel workspace.

You have a multi-tier Security Operations Center (SOC) team.

You need to ensure that all new security incidents are assigned immediately to the Tier 1 analysts group and flagged for triage.

Solution: You create a playbook.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

A playbook can automate incident response actions by using a Logic Apps workflow. When designed with the Microsoft Sentinel incident trigger or invoked from an automation rule, it can assign an incident and add a triage flag. Because the proposed solution is a playbook for new incidents, it can meet the goal. The essential point is that the workflow must run when incidents are created and update incident properties. 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 > Sentinel playbooks; Microsoft Learn > automate incident assignment and tagging.

NEW QUESTION 4

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 SQLdb1.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point

- A. Create a compliance policy.
- B. Configure Microsoft Entra authentication for SQLServer1.
- C. Create a Conditional Access policy.
- D. Configure federated client identity for SQLdb1.
- E. Configure a user-assigned managed identity for SQLdb1.

Answer: BC

Explanation:

Microsoft Entra authentication must be configured on the SQL server before Microsoft Entra identities and Conditional Access can govern database access. A Conditional Access policy then enforces the planned access control for SQLdb1. A compliance policy does not authenticate SQL connections. Federated client identity and a user-assigned managed identity are used for workload identity scenarios, not for enforcing user sign-in requirements against Azure SQL in this case. The exam objective emphasizes practical identity enforcement rather than cosmetic configuration. A valid answer must identify who authenticates, what permission is granted, where the scope is applied, and whether the method continues to work without passwords or secrets. That is why the selected answer is preferred over broader administrative roles or unrelated access settings. 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 SQL authentication and conditional access; Microsoft Learn > Microsoft Entra authentication for Azure SQL.

NEW QUESTION 5

You have an Azure key vault named KV1 that uses role-based access control (RBAC) authorization KV1 stores database connection strings for an Azure App Service web app named App1.

You enable a firewall on KV1 and allow access to KV1 from only the virtual network that contains App1.

You need to ensure that App1 can retrieve secrets from KV1 without using credentials stored in the application configuration.

What should you create?

- A. An access policy for KV1
- B. An app registration for App1
- C. A private endpoint for KV1
- D. A managed identity for App1

Answer: A

Explanation:

The security team wants a serverless workflow to run when scan results are produced. Defender for Storage malware scanning emits events that can be subscribed to through Azure Event Grid, and Event Grid can trigger Azure Functions, Logic Apps, or other serverless handlers. Diagnostic settings and Log Analytics are useful for investigation but are not the lowest-effort event trigger for each malicious upload. Lifecycle policies are storage-management controls, not security remediation workflows. Microsoft platform security questions usually hinge on where enforcement occurs: at the resource, server, subnet, firewall policy, private endpoint, or subscription level. The selected answer uses the control plane that owns that enforcement point. Other options are rejected when they only log activity, broaden network access, or protect a different service category. 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 Storage; Microsoft Learn > Event Grid events for malware scanning results.

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 365 subscription. All users have Microsoft Exchange Online mailboxes.

You use Microsoft Entra Agent ID to register and manage AI agents.

The developers at your company create the following two agents:

- Agent 1: An interactive agent that helps users summarize their own Exchange Online email
- Agent2: An autonomous agent that sends nightly updates to a Microsoft Teams channel

You need to grant each agent access to Microsoft Graph. The solution must minimize the access scope, while meeting each agent ' s operating model.

Which type of permission should you assign to each agent? To answer, drag the appropriate permission types to the correct agents. Each permission type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Permission types

Application permissions

Delegated permissions

Exchange Online permissions

Resource-specific consent (RSC) permissions for Teams

Answer Area

Agent1:

Agent2:

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Agent1: Delegated permissions;

Agent2: Application permissions

Agent1 is interactive and acts for a signed-in user against that user's mailbox, so delegated permissions are appropriate. Agent2 operates autonomously without a signed-in user; application permissions are the app-only model for Microsoft Graph access in that operating mode. Exchange Online permissions and Teams RSC can be valid in narrow service-specific designs, but the answer area asks for the general permission type aligned to interactive versus autonomous agents. The exam objective emphasizes practical identity enforcement rather than cosmetic configuration. A valid answer must identify who authenticates, what permission is granted, where the scope is applied, and whether the method continues to work without passwords or secrets. That is why the selected answer is preferred over broader administrative roles or unrelated access settings. 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 > Manage Entra Agent ID access; Microsoft Learn > delegated vs application permissions.

NEW QUESTION 8

You have an Azure subscription named Sub1 that contains a storage account named storage1. Sub1 has Microsoft Defender for Storage enabled. Defender for Storage has malware scanning enabled.

You need to configure a solution that automates the remediation of malware detected in storage1.

What should you include in the solution?

- A. Application Insights
B. Azure Event Hubs
C. Azure Event Grid
D. Azure Policy

Answer: C

Explanation:

Azure Event Grid publishes Defender for Storage malware scan results as events, enabling event-driven automated remediation workflows such as quarantining, deleting, or moving malicious files after detection.

Reference:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-configure-malware-scan>

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/understand-malware-scan-results>

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

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have an Azure subscription that contains two virtual machines named VM1 and VM2. Each virtual machine has system-assigned managed identity enabled.

You have an Azure Storage account named storage1. Public access from all networks is enabled for storage1.

You need to ensure that VM1 and VM2 can access storage1.

Solution: You add each virtual machine to a security group, and then add the security group to a role on storage1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Adding virtual machines to a security group does not by itself grant Azure Storage access. The authorization principal used by Azure RBAC must be the managed identity or another supported security principal that the workload uses to request tokens. The solution also fails to state that the system-assigned managed identities are added to the group. Because the compute resources themselves are not the authenticating principals, this solution does not meet the goal. 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 > Azure RBAC and identities; Microsoft Learn > role assignment requires an identity principal at the scope.

NEW QUESTION 10

You have a hybrid environment that contains the following servers:

- 50 Azure virtual machines that run Windows Server 2019
- 20 physical, on premises servers that run Windows Server 2019

All the servers use a third-party antivirus solution that must remain active during a phased security rollout

You need to onboard all the servers to Microsoft Defender for Endpoint by using a centralized deployment method. The solution must meet the following requirements:

- Endpoint detection and response (EDR) capabilities must be enabled.
- Antivirus conflicts must be prevented during onboarding.

What should you do on the servers?

- A. Set the Microsoft Defender for Endpoint service to Disabled.
- B. Disable Microsoft Defender Antivirus real-time protection by using Set-MpPreference.
- C. Configure the ForceDefenderPassiveMode registry value.
- D. Enable EDR in block mode.

Answer: C

NEW QUESTION 11

You have an Azure Storage account named storage1 that contains Azure Files shares. You have an application named App1 that uses a system-assigned managed identity to access the shares. Administrators access the shares by using storage account keys. You need to ensure that App1 access the shares without using the storage account keys. What should you do on storage1?

- A. Store the storage account access keys in Azure Key Vault and regenerate them periodically.
- B. Set Allow storage account key access to Disabled.
- C. Select Default to Microsoft Entra authorization in the Azure portal.
- D. Assign the Storage File Data Privileged Reader role to the managed identity of App1.

Answer: D

Explanation:

Assigning the Storage File Data Privileged Reader role to App1's managed identity grants Microsoft Entra ID-based read access to files and directories in Azure Files, overriding existing ACL restrictions where necessary. This allows the application to authenticate by using its managed identity instead of storage account keys.

Reference:

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-assign-share-level-permissions?tabs=azure-portal>

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

NEW QUESTION 14

Which Security Copilot role assignment grants a user the ability to use the product but not manage its settings and roles?

- A. Global Reader only
- B. Storage Blob Data Owner
- C. Network Contributor
- D. Copilot contributor (member) rather than Copilot owner

Answer: D

Explanation:

Security Copilot distinguishes between owners, who manage settings, role assignments, and plugins, and contributors or members, who can use the product. Assigning the member or contributor role follows least privilege for users who only need to run prompts.

NEW QUESTION 15

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The SC-500 Practice Test Here](#)