



Microsoft

Exam Questions SC-500

Microsoft Certified: Cloud and AI Security Engineer Associate

NEW QUESTION 1

You have a Microsoft Entra tenant that has user consent for applications disabled.

You register an application named App1 that requests the following Microsoft Graph delegated permissions:

- user.Read
- Mail.Read

You need to configure tenant permissions to meet the following requirements:

- Enable users to grant consent for low-risk permissions without administrator interaction.
- Ensure that applications requesting higher-privilege permissions require administrator approval.

What should you do?

- A. Grant tenant-wide admin consent to App1.
- B. Configure application assignments for App1.
- C. Configure Privileged Identity Management (PIM) role assignments.
- D. Create an app consent policy.

Answer: D

Explanation:

An app consent policy allows the tenant to define which delegated permissions are considered low risk and may be consented to by users. Higher-privilege permissions can remain subject to admin consent. Tenant-wide admin consent would approve App1 broadly rather than creating an ongoing policy boundary. Application assignments and PIM role assignments control user access or privileged roles, not delegated permission consent behavior. 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 > app consent settings; Microsoft Learn > app consent policies.

NEW QUESTION 2

You have a Microsoft Copilot Studio agent.

A Microsoft Power Platform administrator configures external threat detection for the agent by using a Microsoft Entra application.

You need to ensure that real-time protection is enabled during agent runtime.

What should you do in the Microsoft Defender portal?

- A. Configure Microsoft Defender for Cloud Apps session policies.
- B. Connect the Microsoft 365 app connector.
- C. Enable Global Secure Access for Agents.
- D. From Microsoft Sentinel, configure the Microsoft Purview data connector.

Answer: B

Explanation:

For external threat detection and real-time agent protection to work, Defender must receive app activity through the Microsoft 365 app connector. Session policies in Defender for Cloud Apps govern user sessions, Global Secure Access controls network access, and a Sentinel connector is for log ingestion and investigation. The Microsoft 365 app connector is the required Defender portal-side integration for this runtime protection scenario. 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 > AI workload runtime protection; Microsoft Learn > Microsoft 365 app connector and Copilot agent protection.

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 hunting query.

Does this meet the goal??

- A. Yes
- B. No

Answer: B

Explanation:

A hunting query is an investigation tool. It can find suspicious activity or support manual threat hunting, but it does not automatically assign every new incident to a group or flag it for triage. The requirement is an operational automation requirement on incident creation. Therefore, a hunting query alone does not meet the goal even though it may help analysts review incidents later. In Microsoft Sentinel and Defender scenarios, collection, detection, investigation, and automation are separate functions. The selected answer maps to the function requested by the question rather than a neighboring capability. This is why analytics, hunting, workbooks, connectors, automation rules, and playbooks must not be treated as interchangeable. 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 hunting and automation; Microsoft Learn > hunting queries versus incident automation.

NEW QUESTION 4

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 role on storage1.
Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:
The solution as worded adds virtual machine resources to a role. Azure Storage authorization through Azure RBAC is granted to security principals such as managed identities, users, groups, and service principals, not to VM compute objects as resource containers. Since each VM already has a system-assigned managed identity, the correct approach would be to assign the storage data role to those identities. As stated, this solution does not meet the goal. 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 > managed identities and storage access; Microsoft Learn > RBAC role assignments are made to identities.

NEW QUESTION 5

You have multiple Microsoft Security Copilot workspaces.
A user named User1 accesses Security Copilot by using the default workspace.
You create a new workspace named Workspace 1 and assign a capacity to Workspace1.
You plan to route Security Copilot agent traffic to Workspace1.
You need to ensure that User1 can use embedded experiences without errors.
What should you do before switching to Workspace1?

- A. Add User1 to Workspace1.
- B. Assign User1 the Security Operator role in Microsoft Entra.
- C. Disassociate the capacity from the default workspace.
- D. Create a new capacity for Workspace1.

Answer: A

Explanation:
Security Copilot workspaces have membership and capacity associations. Before routing embedded experience traffic to Workspace1, User1 must be granted access to that workspace. Assigning a generic Security Operator role in Microsoft Entra does not make the user a member of the Security Copilot workspace. Disassociating capacity from the default workspace or creating more capacity does not resolve the user-access error. 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 > Security Copilot workspaces; Microsoft Learn > workspace access and capacity.

NEW QUESTION 6

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 7

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 an analytics rule.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

An analytics rule creates alerts and incidents from detection logic. It is not a global mechanism for assigning every new incident from all sources or adding triage flags after incident creation. While a specific analytics rule can set some incident details for incidents it generates, it does not meet the stated goal for all new incidents in the workspace. Sentinel automation rules or playbooks are the correct tools. In Microsoft Sentinel and Defender scenarios, collection, detection, investigation, and automation are separate functions. The selected answer maps to the function requested by the question rather than a neighboring capability. This is why analytics, hunting, workbooks, connectors, automation rules, and playbooks must not be treated as interchangeable. 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 analytics rules; Microsoft Learn > analytics rules create incidents, not global assignment handling.

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 SQL Database logical server named Server1 that contains multiple databases.

The databases contain legacy SQL authentication logins that must no longer be usable for sign-in but must NOT be removed from the databases.

You need to ensure that SQL authentication is denied for connections.

What should you do?

A. Run CREATE USER ... FROM EXTERNAL PROVIDER on each database.

B. Create a Conditional Access policy.

C. Enable Microsoft Entra-only authentication for Server1.

D. Assign the SQL Server Contributor role to Server1.

Answer: C

Explanation:

Microsoft Entra-only authentication at the logical server level disables SQL authentication for all databases on that server while leaving existing SQL principals in place. That matches the requirement to deny SQL authentication without removing legacy logins. Creating external-provider users adds Entra users; it does not block SQL logins. Conditional Access can govern Entra sign-ins but cannot disable SQL authentication. SQL Server Contributor is an Azure management role, not an authentication mode. 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 platform security; Microsoft Learn > Microsoft Entra-only authentication.

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 15

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 16

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 20

Which identity construct represents an AI agent in Microsoft Entra so you can apply Conditional Access and govern its access?

- A. Microsoft Entra Agent ID
- B. A shared mailbox
- C. A distribution group
- D. A guest user account

Answer: A

Explanation:

Microsoft Entra Agent ID gives AI agents their own first-class identity in Entra ID, enabling Conditional Access policies and access governance for agents. Treating agents as governed identities lets you control and audit what autonomous agents can access.

NEW QUESTION 21

You have an Azure Logic Apps Consumption workflow that uses a Request trigger. All supported authentication methods are enabled on the Request trigger. You need to ensure that the endpoint accepts only OAuth-based requests. The solution must minimize costs. What should you do?

- A. B.Use OAuth 2.0 authorization. C.Enable Secure Inputs and enable Secure Outputs for the Request trigger. D.Deploy Azure API Management.

Answer: A

NEW QUESTION 26

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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](#)