

Microsoft

Exam Questions SC-500

Microsoft Certified: Cloud and AI Security Engineer Associate



NEW QUESTION 1

You have a Microsoft Entra tenant.
You need to implement password less authentication. The solution must meet the following requirements:

- Users can sign in without a password by using a mobile device.
- New users that sign in for the first time must use a helpdesk issued sign in method that expires.

Which authentication method should you enable for each requirement? To answer, drag the appropriate methods to the correct requirements. Each method 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.

Methods

Hardware OATH tokens

Microsoft Authenticator

SMS

Temporary Access Pass

Voice call

Answer Area

Passwordless sign-in:

First-time sign-in for new users:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Passwordless sign-in: Microsoft Authenticator;
First-time sign-in for new users: Temporary Access Pass
Microsoft Authenticator supports passwordless phone sign-in, allowing users to authenticate from a mobile device without typing a password. Temporary Access Pass is a time-limited, helpdesk-issued credential designed for onboarding or recovery, so it fits first-time sign-in for new users. SMS and voice call are authentication methods but are not passwordless sign-in methods in the same strong sense, and hardware OATH tokens are not the requested mobile-device experience. For SC-500, the decisive distinction is whether the control authenticates an identity, grants authorization, or merely changes configuration visibility. The incorrect choices generally either grant excessive privilege, change the application model, or operate at the wrong scope. Microsoft expects the least-privilege identity path that satisfies the scenario without introducing shared secrets or unnecessary tenant-wide rights. 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 > passwordless authentication methods; Microsoft Learn > Microsoft Authenticator and Temporary Access Pass.

NEW QUESTION 2

You have an Azure subscription named Sub1 that contains a virtual network named VNet1.
VNet1 contains multiple virtual machines, including two virtual machines named VM1 and VM2.
Sub1 is linked to a Microsoft Entra tenant named contoso.com.
A partner company has an Azure subscription named Sub2 that contains a virtual network named VNet2. VNet2 contains a virtual machine named VM3.
Sub2 is linked to a Microsoft Entra tenant named fabrikam.com.
VM1 and VM2 contain data used by an application that runs on VM3.
You need to ensure that VM3 can access VM1 and VM2. The solution must deny VM3 access to any other resources in Sub1.
What should you configure on each virtual network? To answer, drag the components to the correct virtual networks. Each component 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.

Components

An Azure Private Link service

An Azure VPN gateway

A private endpoint

A service endpoint

VNet peering

Answer Area

VNet1:

VNet2:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

VNet1: An Azure Private Link service; VNet2: A private endpoint
 Private Link service and private endpoint provide one-way, explicitly scoped private connectivity. VNet1 hosts the target VMs and should expose only the intended service through an Azure Private Link service. VNet2, where VM3 runs, consumes that service through a private endpoint. VNet peering or VPN would create broader network reachability between the networks and would not inherently deny VM3 access to other resources in Sub1. 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 > Private Link services and private endpoints; Microsoft Learn > Azure Private Link architecture.

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 an automation rule.
 Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

An automation rule is the native Sentinel control for applying actions automatically when incidents are created or updated. It can assign incidents to users or groups, change status/severity, add tags, and run playbooks. This directly matches the requirement to assign all new incidents immediately and flag them for triage. It is more direct than hunting queries and is intended for incident-handling automation. 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 > Sentinel automation rules; Microsoft Learn > automation rule actions for incident assignment.

NEW QUESTION 4

You need to configure the AKS1 and ID 1 managed identities to meet the technical requirements. The solution must follow the principle of least privilege. Which role should you assign to each identity? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

AKS1:

AcrPull

▼

AcrPull

AcrPush

Contributor

Owner

ID1:

Contributor

▼

Reader

Contributor

Owner

AcrPull

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

AKS1: AcrPull; ID1: Contributor

AKS1 needs to pull images from Azure Container Registry, so AcrPull is the least-privilege registry role for the cluster identity. ID1 requires Contributor in the visible answer area because the referenced technical requirement requires resource changes beyond a read-only or pull-only role. The important distinction is scope: AKS image retrieval should not receive Contributor, while the separate managed identity receives the broader role only for its implementation task. 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 > AKS and managed identities; Microsoft Learn > ACR pull role and Azure RBAC.

NEW QUESTION 5

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 6

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 7

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 8

You have a Microsoft 365 subscription.

You use Microsoft Entra Agent ID to manage an agent identity.

You manage AI agents from the Microsoft 365 admin center.

An autonomous agent named Agent1 runs without a signed-in user. The agent must access Microsoft Graph and read secrets from a single Azure key vault.

You need to grant Agent 1 access to Microsoft Graph and Key Vault without requiring user interaction or consent at runtime.

What should you do for the agent identity? To answer, drag the appropriate actions to the correct services. Each action 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.

MISSING

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To access Microsoft Graph: Grant an application permission;

To access Key Vault: Assign a role-based access control (RBAC) role

An autonomous agent has no signed-in user at runtime, so Microsoft Graph access must use application permissions rather than delegated permissions. Key Vault is protected through Azure RBAC, so the agent identity should receive an appropriate Key Vault role at the smallest possible scope. This avoids runtime user consent and avoids embedding secrets. Delegated permissions would fail for a background agent because there is no user context. For SC-500, the decisive distinction is whether the control authenticates an identity, grants authorization, or merely changes configuration visibility. The incorrect choices generally either grant excessive privilege, change the application model, or operate at the wrong scope. Microsoft expects the least-privilege identity path that satisfies the scenario without introducing shared secrets or unnecessary tenant-wide rights. 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 > Graph application permissions and Key Vault RBAC.

NEW QUESTION 9

You have a Microsoft Entra tenant that has the following configurations:

- User consent for applications is disabled.
 - Only administrators can grant permissions to applications.
- You register an application named App1 that uses delegated Microsoft Graph permissions.
- You need to configure App1 to meet the following requirements:
- Enable user sign-ins without interactive consent prompts.
 - Enable App1 to access Microsoft Graph on behalf of the signed-in user.

What should you do?

- A. Configure enterprise applications to require user assignment and assign users to App1.
- B. Modify the app registration to use application permissions instead of delegated permissions.
- C. Add the required delegated Microsoft Graph permissions to the app registration and rely on user consent during sign-in.
- D. Grant admin consent to App1 for the required delegated permissions.

Answer: D

Explanation:

Delegated Microsoft Graph permissions allow an application to act on behalf of the signed-in user. Because user consent is disabled and only administrators may grant permissions, users cannot complete the consent prompt themselves. Granting admin consent for the required delegated permissions pre-authorizes the app and removes the interactive consent prompt while still preserving the delegated model. Switching to application permissions would change the operating model and grant app-only access. For SC-500, the decisive distinction is whether the control authenticates an identity, grants authorization, or merely changes configuration visibility. The incorrect choices generally either grant excessive privilege, change the application model, or operate at the wrong scope. Microsoft expects the least-privilege identity path that satisfies the scenario without introducing shared secrets or unnecessary tenant-wide rights. 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 > OAuth permission grants and consent; Microsoft Learn > admin consent for delegated permissions.

NEW QUESTION 10

You have three internet-facing Azure App Service web apps named App1, App2, and App1 Each app uses built-in authentication.

App2 hosts a backend API.

Some corporate users can sign in to App2, even though they should NOT be able to use the API.

You need to restrict App2 access to assigned Microsoft Entra users and groups.

What should you configure for App2? To answer, drag the appropriate configurations to the correct methods. Each configuration 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.

Configurations

Enterprise app assignment required

IP access restrictions

Local authentication

The Microsoft identity provider

A role-based access control (RBAC) assignment

Tenant wide admin consent

Answer Area

Authentication method:

Access control method:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Authentication method: The Microsoft identity provider;
Access control method: Enterprise app assignment required
Built-in authentication for App Service should use the Microsoft identity provider for Microsoft Entra sign-in. To restrict access to selected users and groups, require enterprise app assignment on the corresponding enterprise application. IP restrictions only filter network source and cannot identify assigned corporate users. Local authentication and broad admin consent do not implement assigned-user enforcement for the backend API. 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 Service authentication; Microsoft Learn > App Service built-in authentication and enterprise app assignment.

NEW QUESTION 10

HOTSPOT You have a Microsoft Sentinel workspace named Workspace1. You hire a security consultant. You provide the consultant with a guest account named User1 in your Microsoft Entra tenant. You need to enable User1 to assign incidents in Workspace1. Which roles should you assign to User1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Microsoft Entra role:

Directory Reader

Security Administrator

Security Reader

Azure role:

Microsoft Sentinel Contributor

Microsoft Sentinel Reader

Microsoft Sentinel Responder

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Microsoft Entra role: Directory Reader
Azure role: Microsoft Sentinel Responder
Because User1 is a guest user, the Directory Reader role is required to assign Microsoft Sentinel incidents to users in the tenant. The Microsoft Sentinel Responder role grants the permissions needed to investigate and manage incidents, including updating incident ownership in Workspace1.
Reference:
<https://learn.microsoft.com/en-us/azure/sentinel/roles>
<https://learn.microsoft.com/en-us/azure/sentinel/investigate-incidents>

NEW QUESTION 12

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 16

You have an Azure subscription named Sub1 that contains an Azure Database for PostgreSQL instance Sub1 has Microsoft Defender for Cloud enabled.

You need to configure Microsoft Defender for Databases to minimize costs.

Which Defender plan should you enable?

- A. Microsoft Defender for Servers
- B. Microsoft Defender for Open-Source Relational Databases
- C. Microsoft Defender for SQL Servers on Machines
- D. Microsoft Defender for Azure SQL Databases
- E. Microsoft Defender for Storage

Answer: B

Explanation:

The protected resource is Azure Database for PostgreSQL, which is an open-source relational database service. Microsoft Defender for Open-Source Relational Databases is scoped to PostgreSQL and MySQL style services, so it satisfies the requirement without enabling broader plans. Defender for Azure SQL Databases applies to Azure SQL, Defender for SQL Servers on Machines applies to SQL Server on VMs or Arc-enabled machines, and Defender for Servers or Storage would charge for unrelated workloads. 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 Databases; Microsoft Learn > Defender for open-source relational databases.

NEW QUESTION 17

Which Azure Functions configuration limits the function app to accept requests only from a specific virtual network?

- A. Private endpoints and access restrictions
- B. Application Insights sampling
- C. Durable Functions orchestration
- D. Consumption plan scaling

Answer: A

Explanation:

Using private endpoints for inbound access plus access restriction rules lets you confine a function app to specific networks and deny public access. This network isolation reduces the exposure of serverless endpoints.

NEW QUESTION 20

.....

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](#)