

# Microsoft

## Exam Questions SC-500

Microsoft Certified: Cloud and AI Security Engineer Associate



**NEW QUESTION 1**

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 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**

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 5**

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 6

You need to configure Server1 to meet the technical requirements.  
What should you do? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Install on Server1:

The Azure Connected Machine agent

The Azure Connected Machine agent

The Azure Monitor agent

The Azure Connected Cluster agent

The Dependency agent

Deploy to Sub1:

A Log Analytics workspace

A Log Analytics workspace

A Recovery Services vault

An Azure Automation account

An Azure Arc resource bridge

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Install on Server1: The Azure Connected Machine agent; Deploy to Sub1: A Log Analytics workspace

The Azure Connected Machine agent is required to onboard a non-Azure server as an Azure Arc-enabled server. Once the server is represented in Azure, telemetry and security data can be directed to a Log Analytics workspace in the subscription. This combination supports Defender for Cloud and Sentinel-style monitoring without treating the server as a native Azure VM. Deploying only a workspace would not onboard Server1; installing only the agent would not provide the analytics destination. 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 Arc and Sentinel data collection; Microsoft Learn > Connected Machine agent and Log Analytics workspace.

**NEW QUESTION 7**

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 8

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 9

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 10**

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   | Type                             | Microsoft Entra role                    | Azure role assignment for Sub1 |
|--------|----------------------------------|-----------------------------------------|--------------------------------|
| Admin1 | User                             | Privileged Authentication Administrator | Resource Policy Contributor    |
| Admin2 | User                             | Compliance Administrator                | User Access Administrator      |
| Admin3 | User                             | Authentication Administrator            | Contributor                    |
| Admin4 | User                             | Global Administrator                    | None                           |
| User1  | User                             | None                                    | Reader                         |
| AKS1   | System-assigned managed identity | None                                    | None                           |
| ID1    | User-assigned managed identity   | None                                    | None                           |

The tenant contains the groups shown in the following table.

| Name   | Type          | Role assignments allowed |
|--------|---------------|--------------------------|
| Group1 | Security      | Yes                      |
| Group2 | Security      | No                       |
| Group3 | Microsoft 365 | Yes                      |
| Group4 | Microsoft 365 | No                       |

All devices are enrolled in Microsoft Intune. Existing Environment. Sub1 Resources Sub1 contains a resource group named RG1 that contains the resources shown in the following table.

| Name       | Description                            | Location |
|------------|----------------------------------------|----------|
| SQLServer1 | Azure SQL Database logical server      | East US  |
| SQLdb1     | Database on SQLServer1                 | East US  |
| VM1        | Virtual machine                        | East US  |
| AKS1       | Azure Kubernetes Service (AKS) cluster | East US  |
| Registry1  | Azure container registry               | East US  |
| storage1   | Storage account                        | East US  |
| AKV1       | Azure key vault                        | East US  |

SQLServer1 uses Microsoft SQL Server authentication. Sub1 has an Azure Web Application Firewall (WAF) named WAF1 that has the following types of rule sets: - Bot Manager 1.1 - Azure-managed Default Rule Set (DRS) Sub1 has the following compliance standards assigned in Microsoft Defender for Cloud: - NIST SP 800-53 Rev. 4 - Microsoft cloud security benchmark (MCSB) - System and Organization Controls (SOC) 2 Type 2 Existing Environment. Sub2 Resources Sub2 contains a resource group named RG2. Planned Changes and Requirements. Planned Changes Fabrikam plans to implement the following changes: - Deploy the following key vaults to RG1: \* AKV2 in the West Europe Azure region \* AKV3 in the Central US Azure region \* AKV4 in the East US Azure region - Deploy the following key vaults to RG2: \* AKV5 in the East US region - Configure VM1 to read data from storage1. - Create function apps that have the following hosting plans: \* Fa1: Flex Consumption hosting plan \* Fa2: Consumption hosting plan \* Fa3: Dedicated hosting plan - For WAF1, implement rate limiting rules based on the request location. - Enable the NIST SP 800-53 Rev. 5 compliance standard in Defender for Cloud. - Create a new storage account named storage2 that supports Azure Table storage. - Enforce multifactor authentication (MFA) when database administrators access SQLdb1. - Implement ExpressRoute circuits to the on-premises network as 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 function apps to meet the technical requirements.

Which apps should you include in the implementation?

- A. Fa1 and Fa2 only
- B. Fa2 and Fa3 only
- C. Fa1 and Fa3 only
- D. Fa1, Fa2, and Fa3

**Answer: C**

**Explanation:**

The correct implementation includes Fa1 and Fa3 only according to the visible answer area. In Azure Functions security scenarios, apps are included only when their hosting, authentication, identity, or network configuration matches the stated technical controls. Including Fa2 would apply the implementation to an app that does not meet those requirements. The selected set therefore narrows the change to the function apps that require the security implementation. 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 > Azure Functions security controls; Microsoft Learn > App Service/Functions authentication and network security.

**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 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 11**

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 16

You have an Azure SQL Database logical server named Server1 that contains a database named DB1.  
 You need to configure authentication for Server1 to meet the following requirements;

- SQL authentication cannot be used for any databases on Server1.
- The solution must be enforced centrally at the server level.

What should you do?

- A. Configure a Microsoft Entra administrator for Server1.
- B. Enable a managed identity for Server1.
- C. Enable Microsoft Entra-only authentication for Server1.
- D. Remove SQL logins from DB1.

**Answer: C**

### Explanation:

The requirement is centralized enforcement for all databases on the logical server. Microsoft Entra-only authentication disables SQL authentication at the server level, so SQL logins cannot be used against any database hosted there. Configuring an Entra administrator is typically a prerequisite or supporting step, but by itself it does not disable SQL authentication. A managed identity for the server and deleting logins from one database do not meet the central enforcement requirement. 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 > Azure SQL authentication; Microsoft Learn > Microsoft Entra-only authentication for Azure SQL.

### NEW QUESTION 18

You have a Microsoft Sentinel workspace

You need to collect Windows security events from 200 Azure virtual machines that run Windows Server. The solution must meet the following requirements:

- Use direct agent based data collection from each virtual machine.
- Use a supported agent for new virtual machine deployments

Which Microsoft Sentinel connector should you use?

- A. Windows Forwarded Events
- B. Windows Security Events via AMA
- C. Security Events via Legacy Agent

- D. Syslog via AMA
- E. Azure Resource Graph

**Answer:** B

**Explanation:**

The Windows Security Events via AMA connector uses Azure Monitor Agent and data collection rules for direct collection from Windows machines. It is the supported path for new deployments and avoids the legacy Log Analytics agent. Windows Forwarded Events is for a Windows Event Collector model, not direct agent collection. Syslog via AMA is for Linux Syslog, and Azure Resource Graph is not an event-collection connector. 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 > Windows Security events using DCRs; Microsoft Learn > Windows Security Events via AMA connector.

**NEW QUESTION 23**

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 24**

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 27**

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 31**

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 32**

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 34**

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 37**

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 39**

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 43**

After an AI agent identity is suspected of compromise, which Defender XDR capability helps you analyze the potential blast radius of that Entra Agent ID?

- A. Blast radius analysis for Entra Agent ID in Defender XDR
- B. Storage lifecycle reports
- C. Azure Cost alerts
- D. Network Watcher packet capture

**Answer:** A

**Explanation:**

Defender XDR can analyze the blast radius of an Entra Agent ID, showing what resources and data the agent could reach if abused. Understanding this exposure helps responders scope containment and prioritize remediation for AI agents.

**NEW QUESTION 47**

You have a Microsoft Entra tenant that uses Privileged Identity Management (PIM). You need to modify the AI Administrator role settings to meet the following requirements: - Elevated access must be evaluated by another administrator before it is granted. - Privileged access must be removed automatically after a fixed period. Which two settings should you configure? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Require justification on activation

- A. C. Expire eligible assignments after
- E. Expire active assignments after

**Answer:** BD

**Explanation:**

Requiring approval to activate ensures that a designated administrator must evaluate and approve an eligible user's elevation request before privileged access is granted. Setting an activation maximum duration makes each activated role assignment time-bound, automatically removing the elevated access when the configured activation period expires.

Reference:

<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-change-default-settings>

<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-activate-role>

**NEW QUESTION 50**

.....

## 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](#)**