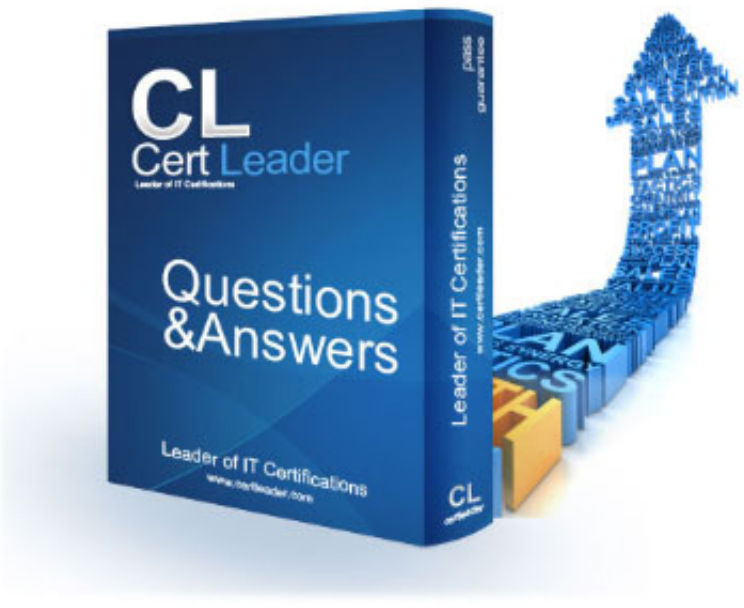
SC-500 Dumps

Microsoft Certified: Cloud and AI Security Engineer Associate

https://www.certleader.com/SC-500-dumps.html



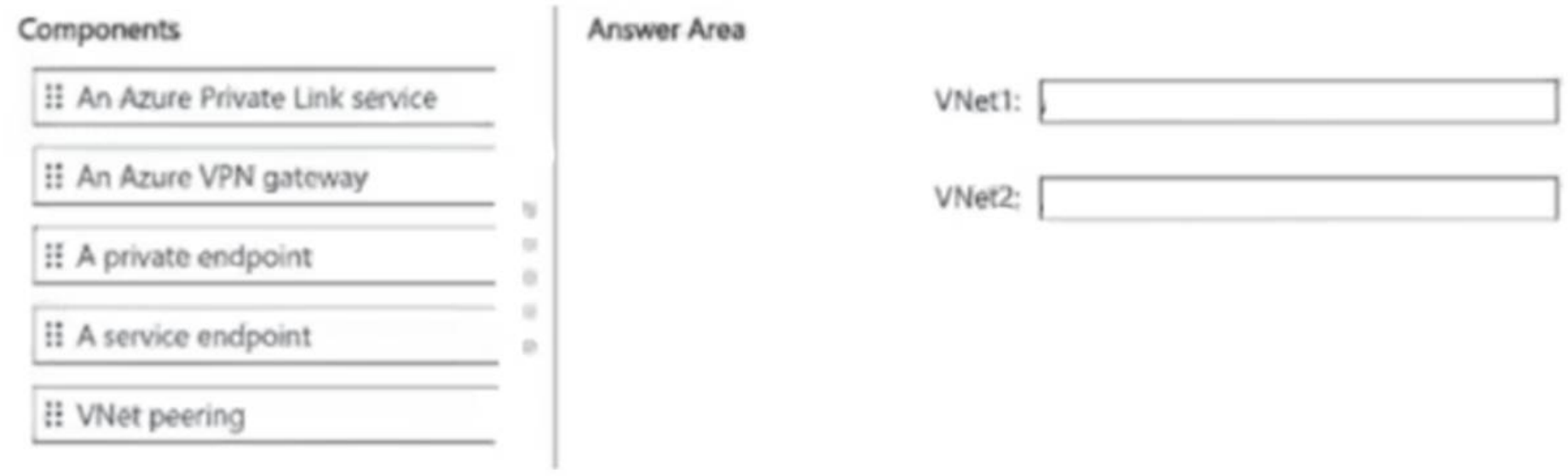
NEW QUESTION 1
You have a Microsoft Entra tenant that has user consent for applications disabled.
You register an application named App1 that requests the following Microsoft Graph delegated permissions:
•user.Read
•Mail.Read
You need to configure tenant permissions to meet the following requirements:
•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 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.



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.

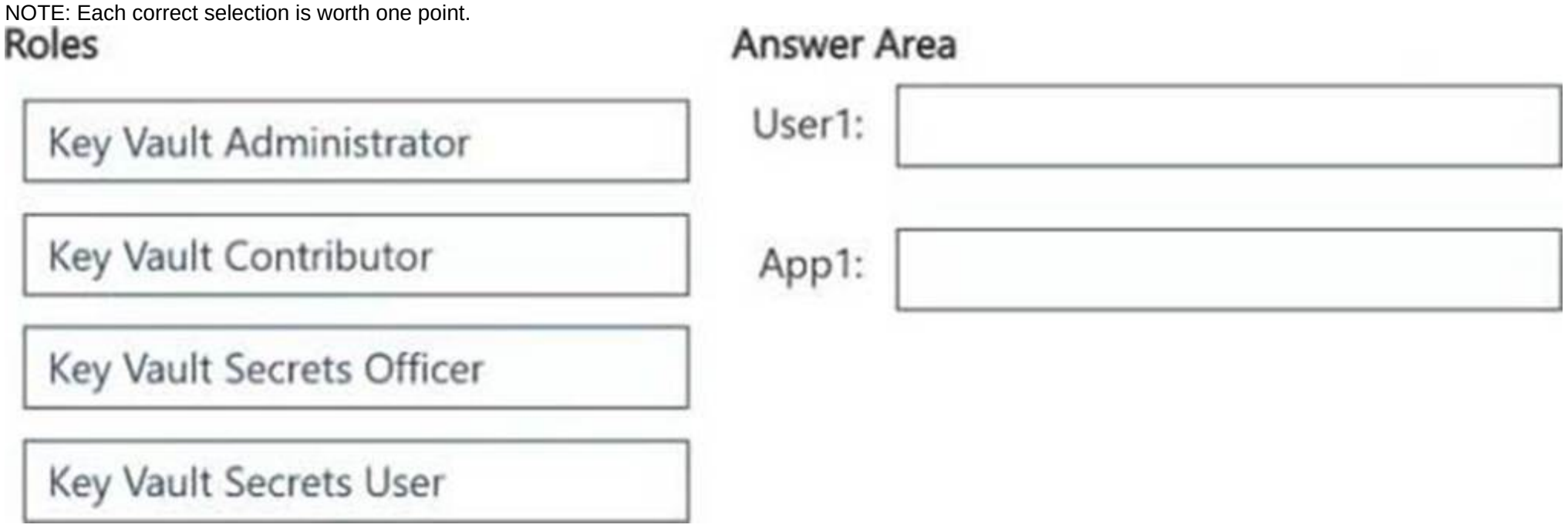
NEW QUESTION 3
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You have an Amazon Web Services (AWS) account connected to Defender for Cloud that has the Defender Cloud Security Posture Management (CSPM) plan enabled.
You need to identify the potential impact of security incidents that exploit multiple risks reported by Defender CSPM.
What should you use?

A. Regulatory compliance
B. Cloud security explorer
C. Security recommendations
D. Attack path analysis

Answer: D

Explanation:
Attack path analysis in Defender CSPM identifies how multiple misconfigurations and risks can be chained to produce business impact. The scenario asks for potential impact of incidents that exploit multiple risks, which is exactly the attack path use case. Regulatory compliance shows framework alignment, security recommendations show individual controls, and Cloud Security Explorer is useful for querying posture data but does not automatically rank chained exploit paths. The SC-500 study guide places these tasks under security posture, event collection, Defender CSPM, EASM, Sentinel, and Security Copilot operations. The exam expects the control that minimizes analyst effort while preserving correct permissions and data flow. The selected answer reflects that service boundary and avoids a broader or merely investigative alternative. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Defender CSPM; Microsoft Learn > attack path analysis.

NEW QUESTION 4
You have an Azure key vault named KV1 that uses role-based access control (RBAC) for data plane authorization.
You have a user named User1 and an Azure App Service web app named App1 that has a system-assigned managed identity.
You need to configure authorization to meet the following requirements:
•App1 must be able to retrieve secrets from KV1.
•User1 must manage the KV1 settings without accessing secret values.
The solution must follow the principle of least privilege.
Which role should you assign to each identity for KV1? To answer, drag the appropriate roles to the correct identities. Each role 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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
User1: Key Vault Contributor;
App1: Key Vault Secrets User
Key Vault Contributor can manage vault settings but cannot read secret values, so it fits User1. Key Vault Secrets User permits reading secret contents without granting vault administration, so it fits App1. Key Vault Administrator and Key Vault Secrets Officer are too broad because they allow broader secret or vault administration. This split enforces RBAC separation between management-plane administration and data-plane secret retrieval. 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 > Key Vault access; Microsoft Learn > Key Vault RBAC built-in roles.

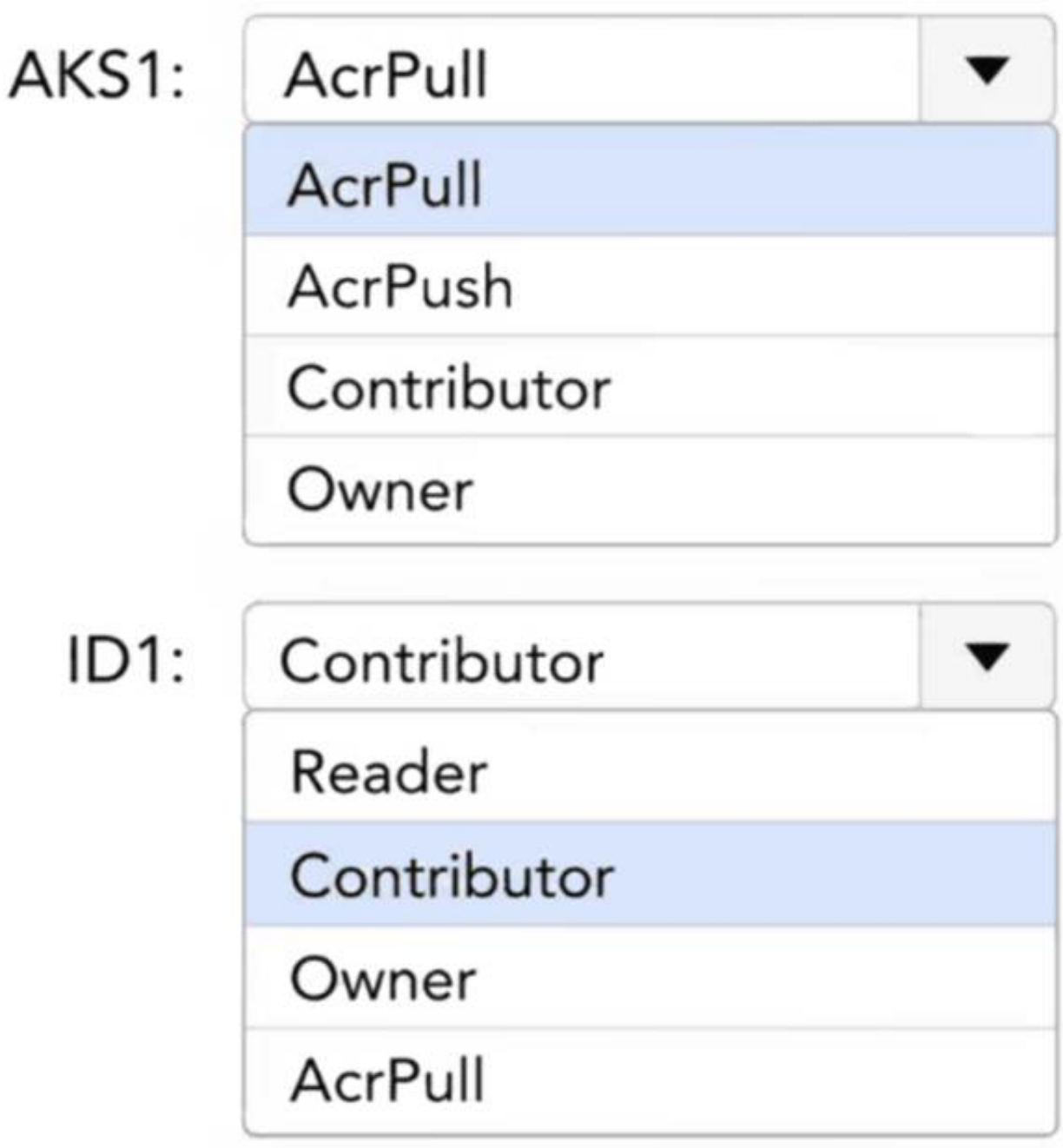
NEW QUESTION 5
Note. This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible 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 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 6
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.



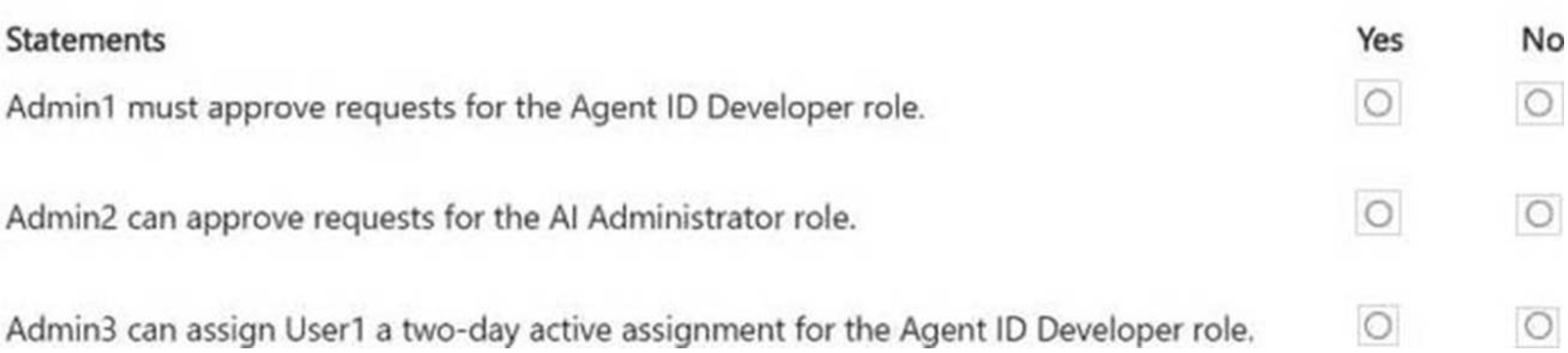
A. Mastered
B. Not Mastered

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 7
For each of the following statements, select Yes if the statement is true Otherwise, select No.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Yes; 2) No; 3) Yes
The visible PIM settings indicate that Admin1 must approve Agent ID Developer activations, Admin2 is not an approver for the AI Administrator role, and Admin3 can assign User1 a two-day active assignment for Agent ID Developer. The controlling factors are the configured approver list and active assignment duration policy for each role. PIM evaluates those settings per role, so approval authority or duration for one role cannot be assumed for another role. 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 > PIM role settings and Agent ID governance; Microsoft Learn > approvers and maximum activation duration.

NEW QUESTION 8
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 9
You have an Azure key vault named KV1 that uses role-based access control (RBAC) authorization KV1 stores database connection strings for an Azure App Service web app named App1.
You enable a firewall on KV1 and allow access to KV1 from only the virtual network that contains App1.
You need to ensure that App1 can retrieve secrets from KV1 without using credentials stored in the application configuration.
What should you create?

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

Answer: A

Explanation:
The security team wants a serverless workflow to run when scan results are produced. Defender for Storage malware scanning emits events that can be subscribed to through Azure Event Grid, and Event Grid can trigger Azure Functions, Logic Apps, or other serverless handlers. Diagnostic settings and Log Analytics are useful for investigation but are not the lowest-effort event trigger for each malicious upload. Lifecycle policies are storage-management controls, not security remediation workflows. Microsoft platform security questions usually hinge on where enforcement occurs: at the resource, server, subnet, firewall policy, private endpoint, or subscription level. The selected answer uses the control plane that owns that enforcement point. Other options are rejected when they only log activity, broaden network access, or protect a different service category. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Defender for Storage; Microsoft Learn > Event Grid events for malware scanning results.

NEW QUESTION 10
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 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 13
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 17
You have an Azure subscription that contains a resource group named RG1.
RG1 contains a Microsoft Security Copilot deployment that is integrated with a Microsoft Sentinel workspace named Workspace1.
Analysts use the Security Copilot standalone experience to retrieve incidents by using the Microsoft Sentinel plugin.
A user named User1 can sign in to Security Copilot but cannot retrieve incidents from Workspace1. You verify that User1 lias only the Security Copilot Contributor role.
You need to ensure that User1 can retrieve the incidents. The solution must follow the principle of least privilege and NOT require any configuration changes to Security Copilot.

Which role should you assign to User1?

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

Answer: B

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

NEW QUESTION 19
You have Microsoft Security Copilot agents that authenticate by using Microsoft Entra service principals.
You receive a Microsoft Defender alert triggered by the anomalous OAuth authentication of an agent ' s Microsoft Entra service principal.
You need to assess the impact of the agent identity and identify which resources are affected if the identity is abused for lateral movement The solution must minimize administrative effort.
What should you do?

A. From Advanced hunting, create a query against the IdentityLogonEvents table to list all the sign-ins performed by the identity.
B. From Attack paths, select the identity and view the blast radius.
C. From AI Observability in Microsoft Purview Data Security Posture Management (DSPM), review the agent activity.
D. From Microsoft Purview Audit, query the audit logs for all the role assignments granted to the identity.
E. From Incidents, review incidents related to OAuth events reported by Microsoft Defender for Cloud Apps.

Answer: B

Explanation:
The security team needs impact and lateral-movement exposure for an abused service principal. Defender XDR attack paths show the identity blast radius by connecting permissions, exposed resources, and reachable assets. Advanced hunting and audit logs can provide raw evidence, but they require more manual analysis. AI Observability and incident review do not directly answer which resources are affected by identity abuse across the environment. 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 > analyze blast radius by using Defender XDR; Microsoft Learn > attack paths for identity risk.

NEW QUESTION 21
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 25
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 an Azure Storage account named storage1 that hosts a blob container named container1.
You have an Azure Functions app named app1 that uses a managed identity.
You need to configure app1 to read, write, and delete blobs in container1. The solution must follow the principle of least privilege.
What should you do?

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

Answer: D

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

NEW QUESTION 29
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

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 31
HOTSPOT \You have an Azure subscription. \You need to create and deploy an Azure policy that meets the following requirements: - When a new virtual machine is deployed, automatically install a custom security extension. - Trigger an autogenerated remediation task for non-compliant virtual machines to install the extension. What should you include in the policy? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Definition effect: DeployIfNotExists
For remediation, define: A managed identity that has the Contributor role
The DeployIfNotExists effect deploys the custom security extension when a virtual machine does not already have the required extension. Remediation tasks use the deployment template in this policy effect to correct existing non-compliant virtual machines. The policy assignment requires a managed identity with the permissions needed to deploy the extension; the Contributor role provides the required resource deployment permissions.
Reference:
https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effect-deploy-if-not-exists
https://learn.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources?tabs=azure-portal
https://learn.microsoft.com/en-us/azure/governance/policy/overview

NEW QUESTION 33
You have an Azure subscription named Sub1 that contains a storage account named storage1. Sub1 has Microsoft Defender for Storage enabled. Defender for Storage has on-upload malware scanning enabled for a monthly cap of 10,000 GB per storage account. You use a Microsoft Sentinel workspace to monitor security events on all Azure resources. You need to configure storage1 to use a malware scanning cap of 2,000 GB per month. What should you do?

A. Enable the Override Defender for Storage subscription-level settings for storage1.
B. From Microsoft Sentinel, modify the data collection rule (DCR) to restrict log ingestion from storage1.
C. Modify the malware scanning configuration of Sub1.
D. From the Microsoft Sentinel workspace, modify the daily cap.

Answer: A

Explanation:
Defender for Storage settings can be overridden for an individual storage account when the subscription-level configuration applies a different malware scanning cap. Enabling the override for storage1 allows its on-upload malware scanning monthly cap to be changed to 2,000 GB while the subscription-level 10,000-GB setting continues to apply to other storage accounts.
Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-introduction
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-azure-portal-enablement?tabs=enable-subscription

NEW QUESTION 37
You have an Azure virtual network that contains 100 virtual machines and an Azure Firewall instance named FW1.
All the traffic from the virtual machines is routed through FW1.
You need to ensure that FW1 allows access to only a URL of updates.contoso.com and blocks all other outbound traffic.
What should you use?

A. an inbound NAT rule
B. an application rule

C. an outbound NAT rule
D. a network rule

Answer: B

Explanation:
An Azure Firewall application rule permits outbound HTTP or HTTPS access based on a fully qualified domain name, such as updates.contoso.com. With only that destination allowed, traffic to other outbound web destinations is denied when no matching allow rule exists.
Reference:
https://learn.microsoft.com/en-us/azure/firewall/firewall-faq

NEW QUESTION 38
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 43
You have an Azure subscription named Sub1 that contains an Azure Kubernetes Service (AKS) cluster named cluster1 and an Azure container registry named ACR1 Sub1 has Microsoft Defender for Containers enabled, and runtime protection is active on cluster!
The developers at your company deploy pods that have elevated privileges, and the deployments are created in cluster1
You need to prevent pods with elevated privileges from being accepted by cluster!
What should you do?

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

Answer: A

Explanation:
Privileged pods must be rejected before they are admitted to the AKS cluster. Azure Policy for AKS integrates with admission control to enforce policies such as denying privileged containers. Runtime alerts can detect privileged activity after deployment, but the requirement is prevention. Agentless Kubernetes discovery and image vulnerability assessment provide visibility; they do not block a privileged pod specification during admission. For SC-500, compute controls are evaluated by workload type: VM, Arc server, AKS, container registry, container group, Functions, Logic Apps, App Service, and AI agent runtime. The right answer uses the Microsoft control that is native to that workload. Broad Azure roles or unrelated monitoring services would either overgrant access or fail to enforce the required security state. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > AKS security controls; Microsoft Learn > Azure Policy for AKS admission control.

NEW QUESTION 44
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

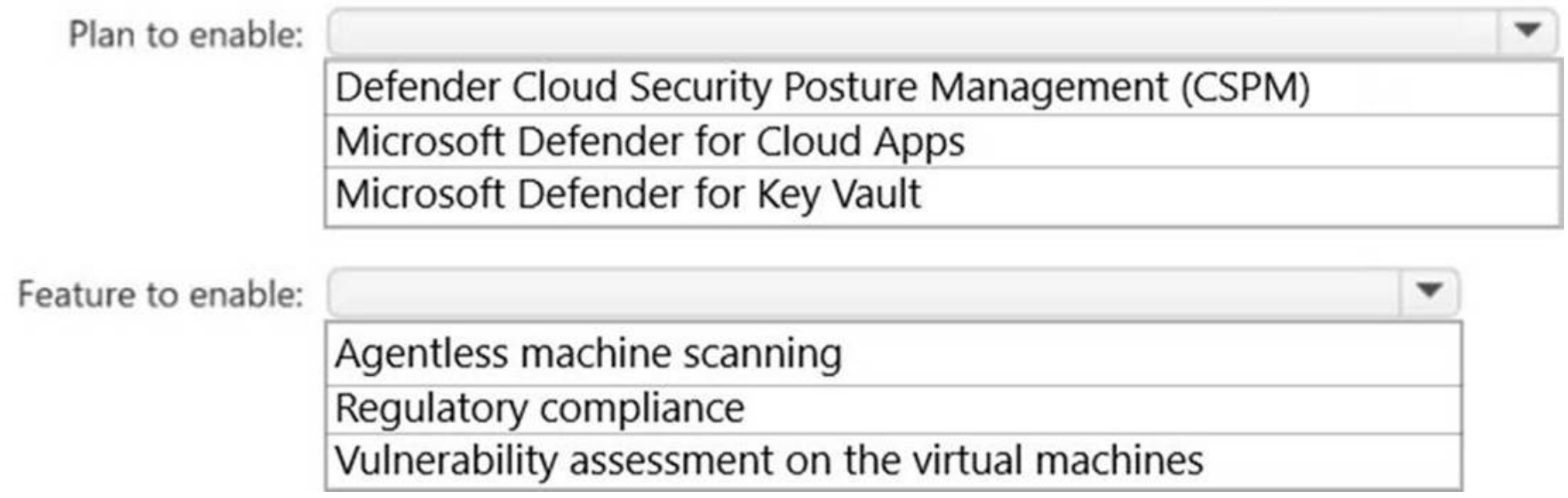
Answer: B

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 46
HOTSPOT
You have an Azure subscription named Sub1 that contains 50 virtual machines. Sub1 has Microsoft Defender for Cloud enabled.
Sub1 contains an Azure key vault named KV1 and an Azure policy that enforces storing all secrets in KV1.
Occasionally, the developers at your company store plaintext tokens and SSH private keys on the virtual machines.
You need to configure Defender for Cloud to detect plaintext secrets on the virtual machines. The solution must minimize administrative changes to the virtual machines.
How should you configure Defender for Cloud? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Plan to enable: Defender Cloud Security Posture Management (CSPM)
Feature to enable: Agentless machine scanning
Defender CSPM supports agentless secrets scanning for Azure virtual machines. Enabling agentless machine scanning allows Defender for Cloud to analyze VM disk snapshots for exposed plaintext tokens and SSH private keys without requiring agents or configuration changes on the virtual machines.
Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/secrets-scanning-servers https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-agentless-data-collection

NEW QUESTION 49
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 51
Which Security Copilot role assignment grants a user the ability to use the product but not manage its settings and roles?

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

Answer: D

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

NEW QUESTION 52
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 54
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 58
An AI development team stores secrets, API keys, and connection strings within application configuration files. A security review recommends a more secure approach. What should the team implement?

A. B.Azure Key Vault C.Azure Advisor D.Azure Resource Graph

Answer: B

NEW QUESTION 63
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SC-500 Exam with Our Prep Materials Via below:

https://www.certleader.com/SC-500-dumps.html