Microsoft

Exam Questions SC-500

Microsoft Certified: Cloud and AI Security Engineer Associate

NEW QUESTION 1
You have an Azure subscription named Sub1 that contains a storage account named storage1
Sub1 has Microsoft Defender for Storage enabled. Defender for Storage has on-upload malware scanning enabled.
The security team at your company requires that all malicious files be processed automatically by a serverless workflow for quarantine and notification.
You need to ensure that the malware scan results trigger an automated response. The solution must minimize operational effort.
What should you configure?

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

Answer: A

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

NEW QUESTION 2
You have an Azure subscription that 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 3
Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.
After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.
You have a Microsoft Sentinel workspace
You have a multi-tier Security Operations Center (SOC) team.
You need to ensure that all new security incidents are assigned immediately to the Tier 1 analysts group and flagged for triage.
Solution: You create an automation rule.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
An automation rule is the native Sentinel control for applying actions automatically when incidents are created or updated. It can assign incidents to users or groups, change status/severity, add tags, and run playbooks. This directly matches the requirement to assign all new incidents immediately and flag them for triage. It is more direct than hunting queries and is intended for incident-handling automation. The posture and monitoring objective focuses on turning security data into usable operational outcomes. The correct answer either collects the right signal, grants the right security-operations role, or automates incident handling at the correct layer. Distractors often provide dashboards, queries, or broad permissions, but those do not create the requested workflow or least-privilege security capability. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Sentinel automation rules; Microsoft Learn > automation rule actions for incident assignment.

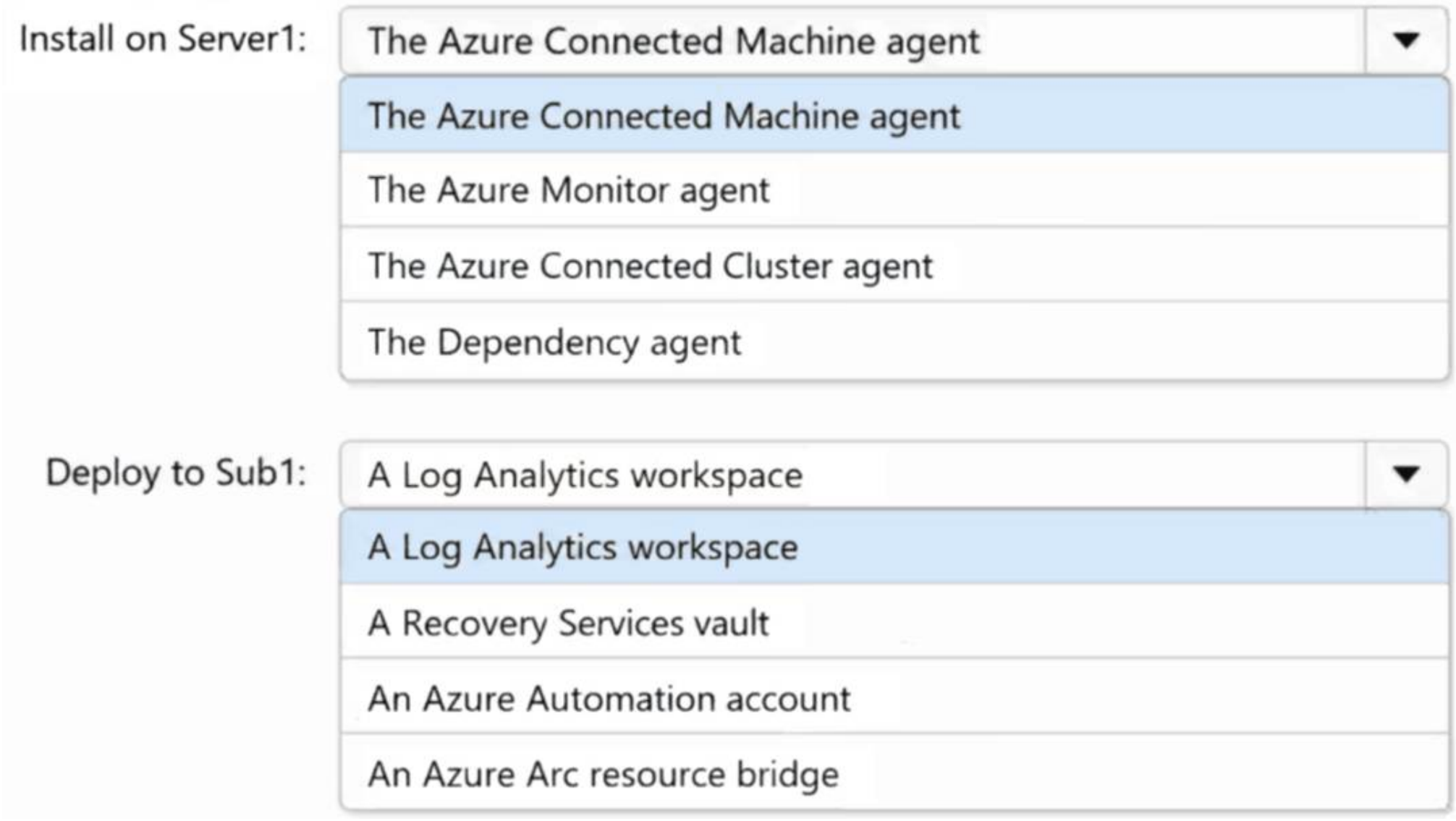
NEW QUESTION 4
You need to configure the AKS1 and ID 1 managed identities to meet the technical requirements. The solution must follow the principle of least privilege.
Which role should you assign to each identity? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
AKS1: AcrPull; ID1: Contributor
AKS1 needs to pull images from Azure Container Registry, so AcrPull is the least-privilege registry role for the cluster identity. ID1 requires Contributor in the visible answer area because the referenced technical requirement requires resource changes beyond a read-only or pull-only role. The important distinction is scope: AKS image retrieval should not receive Contributor, while the separate managed identity receives the broader role only for its implementation task. This domain is tested through precise scope control: tenant, subscription, resource, application, and data-plane authorization are not interchangeable. The correct choice applies the smallest identity or governance control that enforces the stated requirement. Options that only add users, create registrations, or provide broad administrator access fail because they do not directly enforce the requested access behavior. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > AKS and managed identities; Microsoft Learn > ACR pull role and Azure RBAC.

NEW QUESTION 5
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.

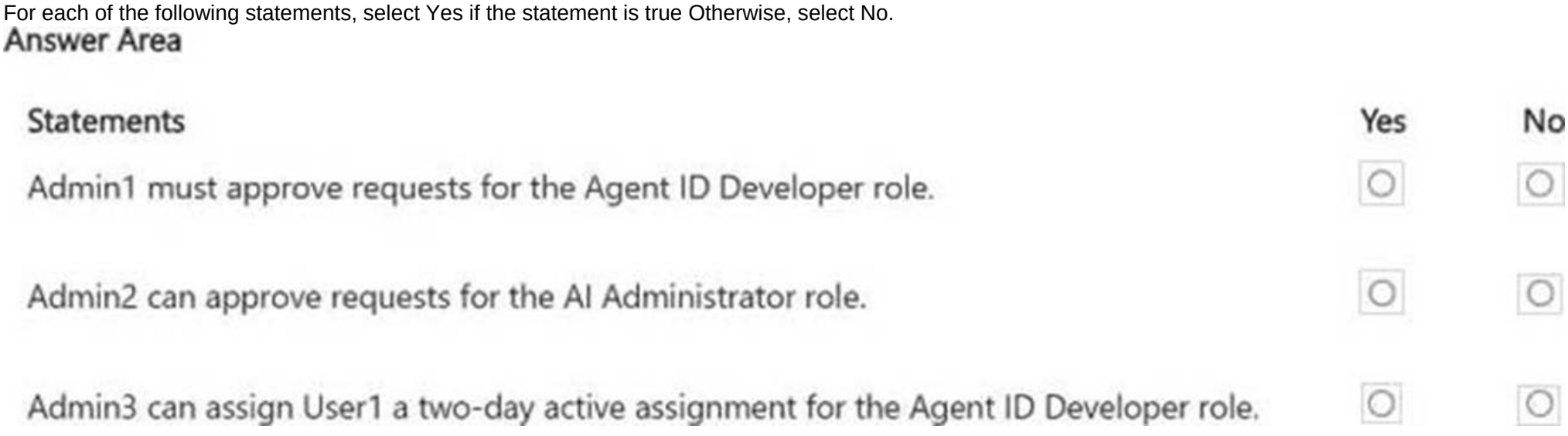


A. Mastered
B. Not Mastered

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 6
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 7
Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.
After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.
You have 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 create a user-assigned managed identity, assign the identity to each virtual machine, and then add each managed identity to a role on storage1.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
A user-assigned managed identity can be attached to multiple virtual machines and then granted an Azure Storage data role. The applications running on VM1 and VM2 can request tokens for that identity and access storage1 without account keys. Public network access is already enabled, so the missing control is authorization. Assigning the user-assigned managed identity to the correct storage role satisfies the access 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 > managed identities; Microsoft Learn > user-assigned managed identities and role assignment to storage.

NEW QUESTION 8
You need to delegate a user to implement the planned change for Defender for Cloud. The solution must follow the principle of least privilege.
Which user should you choose?

A. Admin1
B. Admin2
C. Admin3
D. Admin4

Answer: A

Explanation:
Admin1 is the visible least-privilege delegate for the planned Defender for Cloud change. Defender for Cloud administration should be delegated to the user with the specific security or Defender permissions needed for the task, not to broader administrators unless required. Choosing a higher privileged account would violate the least-privilege requirement. The source file??s case-study background is not visible, so the answer follows the displayed answer selection and the general Defender for Cloud RBAC model. 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 for Cloud least-privilege administration; Microsoft Learn > built-in Azure roles for Defender for Cloud.

NEW QUESTION 9
You have an Azure subscription named Sub1. Sub1 contains 20 virtual machines that run Windows Server.
Sub1 has the Microsoft Defender for Cloud Defender Cloud Security Posture Management (CSPM) plan enabled.
You need to ensure that all the virtual machines are scanned automatically for known security flaws and misconfigurations.
What should you use?

A. Attack path analysis
B. Microsoft Cloud Security Benchmark (MCSB)
C. Cloud security explorer
D. Just-in-time (JIT) VM access
E. Vulnerability assessment on the virtual machines

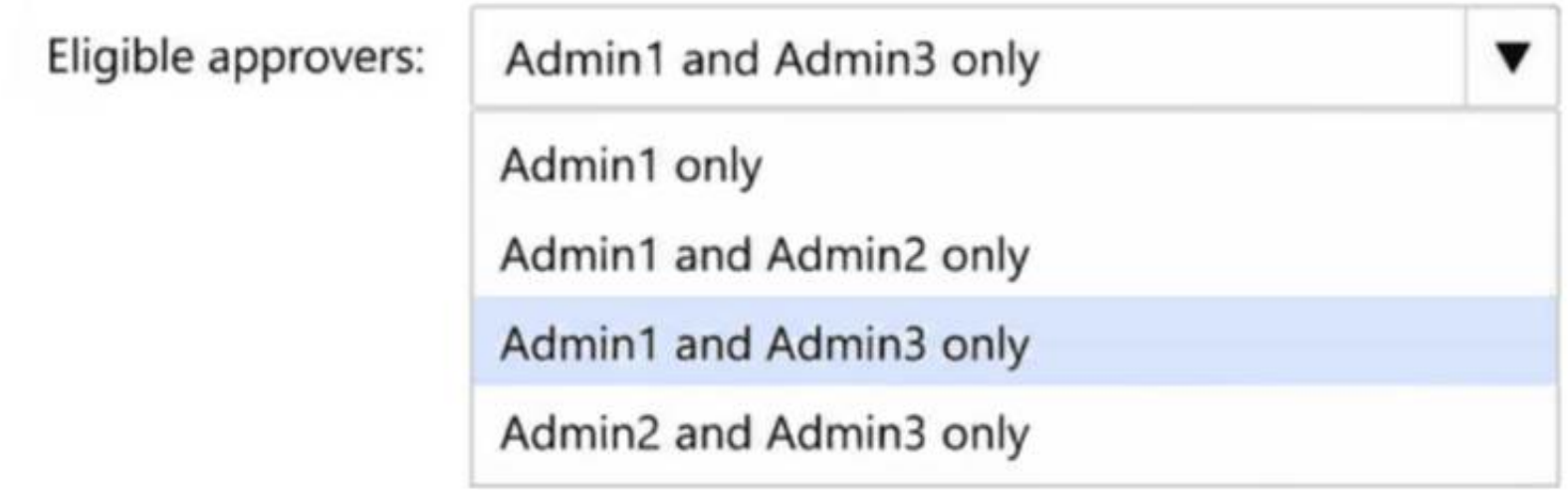
Answer: E

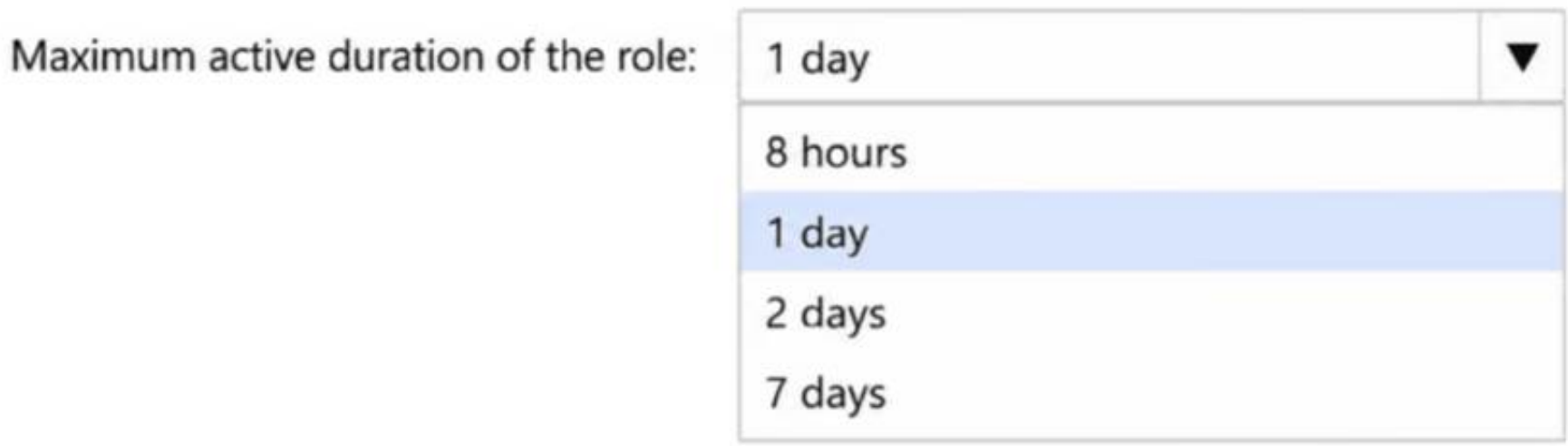
Explanation:
Vulnerability assessment on virtual machines is the feature that scans machines for known security flaws and misconfigurations. Attack path analysis correlates risk paths after findings exist; it is not the scanner itself. Cloud Security Explorer is an investigation query experience, and MCSB is a security benchmark framework. JIT VM access limits management exposure, not vulnerability discovery. The VM vulnerability assessment capability satisfies the automated scanning requirement. 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 Servers settings; Microsoft Learn > vulnerability assessment for machines.

NEW QUESTION 10
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.





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 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 12
Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.
After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.
You have 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 18
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?

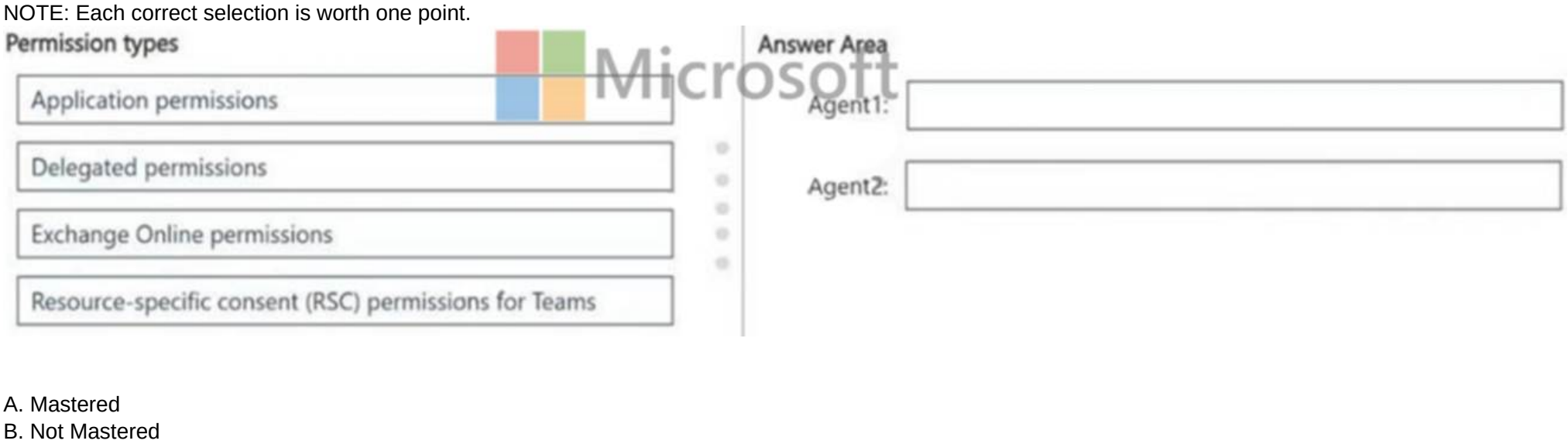
A. From Advanced hunting, create a query against the IdentityLogonEvents table to list all the sign-ins performed by the identity.
B. From Attack paths, select the identity and view the blast radius.
C. From AI Observability in Microsoft Purview Data Security Posture Management (DSPM), review the agent 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 22
You have a Microsoft 365 subscription. All users have Microsoft Exchange Online mailboxes.
You use Microsoft Entra Agent ID to register and manage AI agents.
The developers at your company create the following two agents:
•Agent 1: An interactive agent that helps users summarize their own Exchange Online email
•Agent2: An autonomous agent that sends nightly updates to a Microsoft Teams channel
You need to grant each agent access to Microsoft Graph. The solution must minimize the access scope, while meeting each agent ' s operating model.
Which type of permission should you assign to each agent? To answer, drag the appropriate permission types to the correct agents. Each permission type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Agent1: Delegated permissions;
Agent2: Application permissions
Agent1 is interactive and acts for a signed-in user against that user's mailbox, so delegated permissions are appropriate. Agent2 operates autonomously without a signed-in user; application permissions are the app-only model for Microsoft Graph access in that operating mode. Exchange Online permissions and Teams RSC can be valid in narrow service-specific designs, but the answer area asks for the general permission type aligned to interactive versus autonomous agents. The exam objective emphasizes practical identity enforcement rather than cosmetic configuration. A valid answer must identify who authenticates, what permission is granted, where the scope is applied, and whether the method continues to work without passwords or secrets. That is why the selected answer is preferred over broader administrative roles or unrelated access settings. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Manage Entra Agent ID access; Microsoft Learn > delegated vs application permissions.

NEW QUESTION 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.

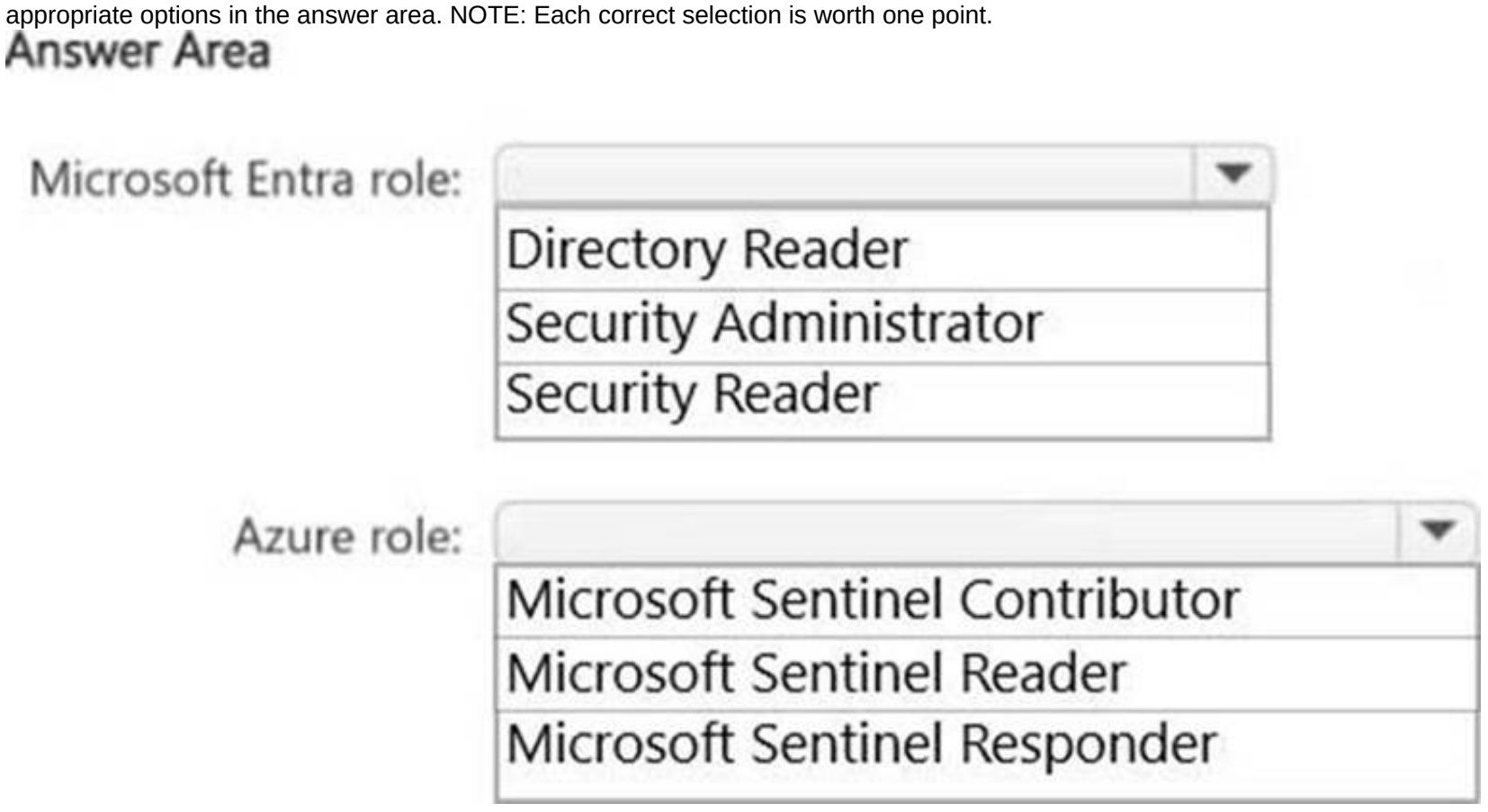
NEW QUESTION 27
You have three internet-facing Azure App Service web apps named App1, App2, and App1 Each app uses built-in authentication.
App2 hosts a backend API.
Some corporate users can sign in to App2, even though they should NOT be able to use the API.
You need to restrict App2 access to assigned Microsoft Entra users and groups.
What should you configure for App2? To answer, drag the appropriate configurations to the correct methods. Each configuration may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Authentication method: The Microsoft identity provider;
Access control method: Enterprise app assignment required
Built-in authentication for App Service should use the Microsoft identity provider for Microsoft Entra sign-in. To restrict access to selected users and groups, require enterprise app assignment on the corresponding enterprise application. IP restrictions only filter network source and cannot identify assigned corporate users. Local authentication and broad admin consent do not implement assigned-user enforcement for the backend API. This domain is tested through precise scope control: tenant, subscription, resource, application, and data-plane authorization are not interchangeable. The correct choice applies the smallest identity or governance control that enforces the stated requirement. Options that only add users, create registrations, or provide broad administrator access fail because they do not directly enforce the requested access behavior. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > App Service authentication; Microsoft Learn > App Service built-in authentication and enterprise app assignment.

NEW QUESTION 30
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.



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 32
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 37
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?

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

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 39
You have an Azure subscription named Sub1 that contains a storage account named storage1. Sub1 has Microsoft Defender for Storage enabled. Defender for Storage has malware scanning enabled.
You need to configure a solution that automates the remediation of malware detected in storage1.
What should you include in the solution?

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

Answer: C

Explanation:
Azure Event Grid publishes Defender for Storage malware scan results as events, enabling event-driven automated remediation workflows such as quarantining, deleting, or moving malicious files after detection.
Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-configure-malware-scan
https://learn.microsoft.com/en-us/azure/defender-for-cloud/understand-malware-scan-results

NEW QUESTION 40
You have an Azure subscription.
You need to deploy an Azure virtual WAN to meet the following requirements:
- Create three secured virtual hubs located in the East US, West US, and North Europe Azure regions.
- Ensure that security rules sync between the regions.
What should you use?

A. Azure Network Function Manager
B. Azure Firewall Manager
C. Azure Virtual Network Manager
D. Azure Front Door

Answer: B

Explanation:
Azure Firewall Manager is used to create and manage secured virtual hubs for Azure Virtual WAN. It supports centrally managed Azure Firewall policies across multiple secured virtual hubs in different Azure regions, allowing the same security rules to be consistently applied to the hubs in East US, West US, and North Europe.
Reference:
https://learn.microsoft.com/en-us/azure/firewall-manager/overview
https://learn.microsoft.com/en-us/azure/firewall-manager/secured-virtual-hub
https://learn.microsoft.com/en-us/azure/firewall-manager/policy-overview

NEW QUESTION 44
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 46
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 50
You have a hybrid environment that contains the following servers:

•50 Azure virtual machines that run Windows Server 2019
•20 physical, on premises servers that run Windows Server 2019
All the servers use a third-party antivirus solution that must remain active during a phased security rollout
You need to onboard all the servers to Microsoft Defender for Endpoint by using a centralized deployment method. The solution must meet the following requirements:
•Endpoint detection and response (EDR) capabilities must be enabled.
•Antivirus conflicts must be prevented during onboarding.
What should you do on the servers?

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

Answer: C

NEW QUESTION 51
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 54
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 55
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

E.Expire active assignments after
A. C.Expire eligible 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 57
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?

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

Answer: B

NEW QUESTION 58

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

SC-500 Practice Exam Features:

* SC-500 Questions and Answers Updated Frequently

* SC-500 Practice Questions Verified by Expert Senior Certified Staff

* SC-500 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SC-500 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year