Microsoft

Exam Questions SC-500

Microsoft Certified: Cloud and AI Security Engineer Associate

NEW QUESTION 1
You have a Microsoft Entra tenant.
You need to implement password less authentication. The solution must meet the following requirements:
•Users can sign in without a password by using a mobile device.
•New users that sign in for the first time must use a helpdesk issued sign in method that expires.
Which authentication method should you enable for each requirement? To answer, drag the appropriate methods to the correct requirements. Each method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

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

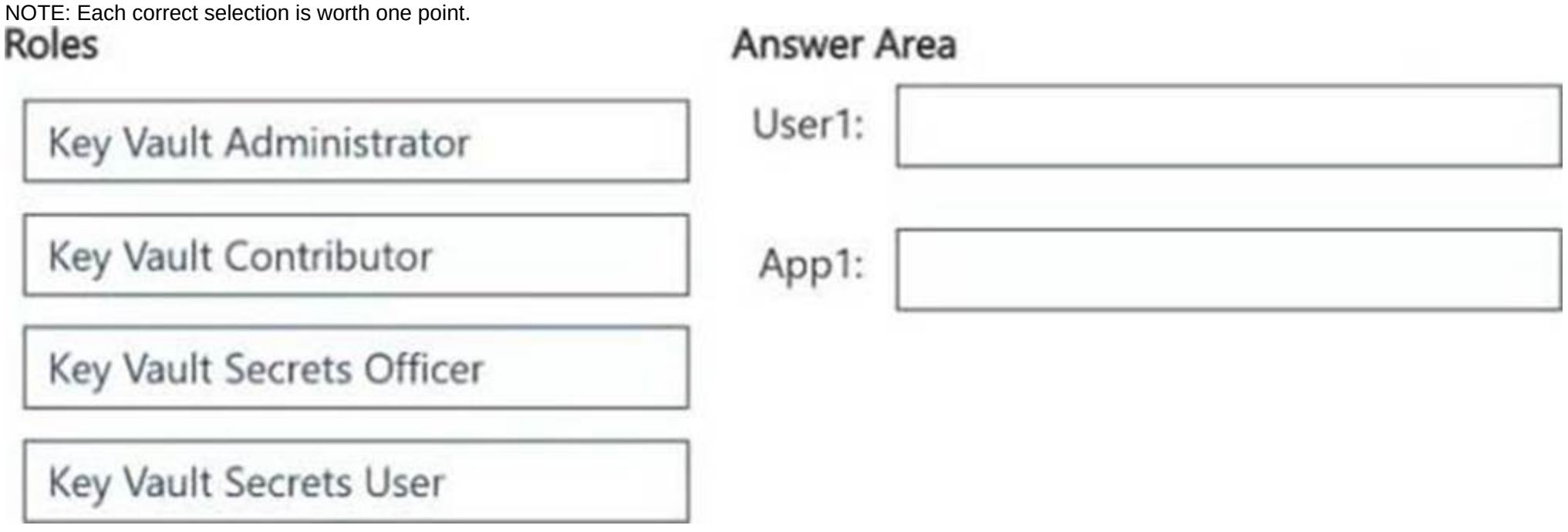
NEW QUESTION 2
You have a Microsoft Copilot Studio agent.
A Microsoft Power Platform administrator configures external threat detection for the agent by using a Microsoft Entra application.
You need to ensure that real-time protection is enabled during agent runtime.
What should you do in the Microsoft Defender portal?
A. Configure Microsoft Defender for Cloud Apps session policies.
B. Connect the Microsoft 365 app connector.
C. Enable Global Secure Access for Agents.
D. From Microsoft Sentinel, configure the Microsoft Purview data connector.

Answer: B

Explanation:
For external threat detection and real-time agent protection to work, Defender must receive app activity through the Microsoft 365 app connector. Session policies in Defender for Cloud Apps govern user sessions, Global Secure Access controls network access, and a Sentinel connector is for log ingestion and investigation. The Microsoft 365 app connector is the required Defender portal-side integration for this runtime protection scenario. For SC-500, compute controls are evaluated by workload type: VM, Arc server, AKS, container registry, container group, Functions, Logic Apps, App Service, and AI agent runtime. The right answer uses the Microsoft control that is native to that workload. Broad Azure roles or unrelated monitoring services would either overgrant access or fail to enforce the required security state. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > AI workload runtime protection; Microsoft Learn > Microsoft 365 app connector and Copilot agent protection.

NEW QUESTION 3
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.

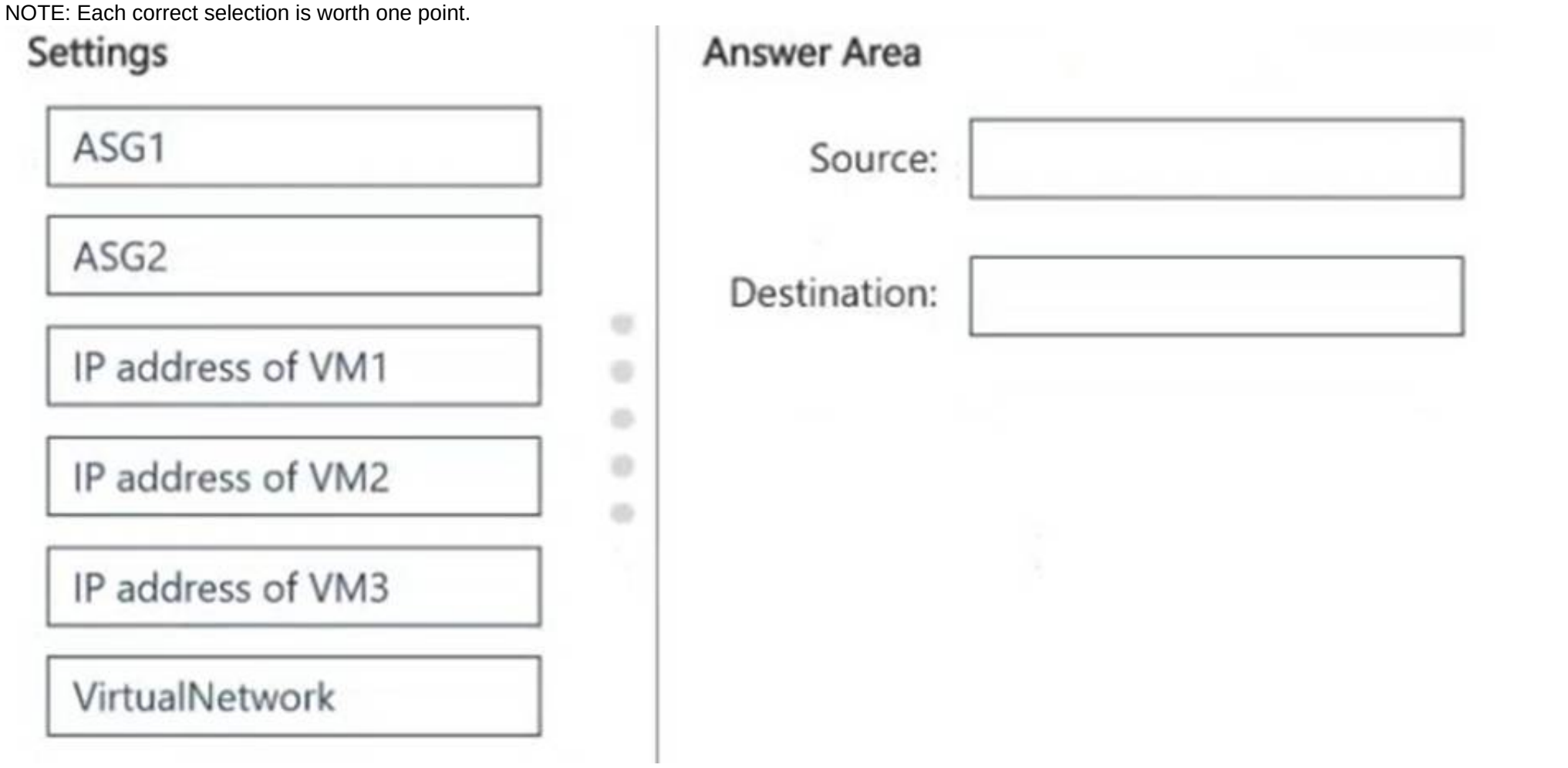


A. Mastered
B. Not Mastered

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 4
You have an Azure virtual network named VNet1 that contains three subnets named Subnet1, Subnet2 and Subnet3. A single network security group (NSG) named NSG1 is associated with all the subnets. You have the following virtual machines:
•VM1 on Subnet1
•VM2 on Subnet2
•VM3 on Subnet3
You create two application security groups named ASG1 and ASG2. VM2 is a member of ASG1, and VM3 is a member of ASG2.
You need to ensure that only VM2 can connect to VM3. The solution must continue to work if the private IP address of VM2 changes.
How should you configure the inbound rule on NSG1 ? To answer, drag the settings to the correct configurations. Each setting 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:
Source: ASG1; Destination: ASG2
The requirement is identity-stable network filtering between virtual machines even if VM2 receives a different private IP address. Application security groups solve exactly that problem: rules refer to VM membership instead of a fixed IP. Because VM2 is a member of ASG1 and VM3 is a member of ASG2, the inbound allow rule on the shared NSG must use ASG1 as source and ASG2 as destination. Choosing IP addresses would fail the change-resilience requirement. The important exam skill is separating data-plane access, management-plane administration, and network reachability. A storage, database, or firewall setting must be selected because it enforces the exact path requested in the scenario. Distractors often look plausible because they improve security generally, but they do not satisfy the protocol, scope, or automation requirement stated in the question. 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 > NSGs and ASGs; Microsoft Learn > Application security groups in network security rules.

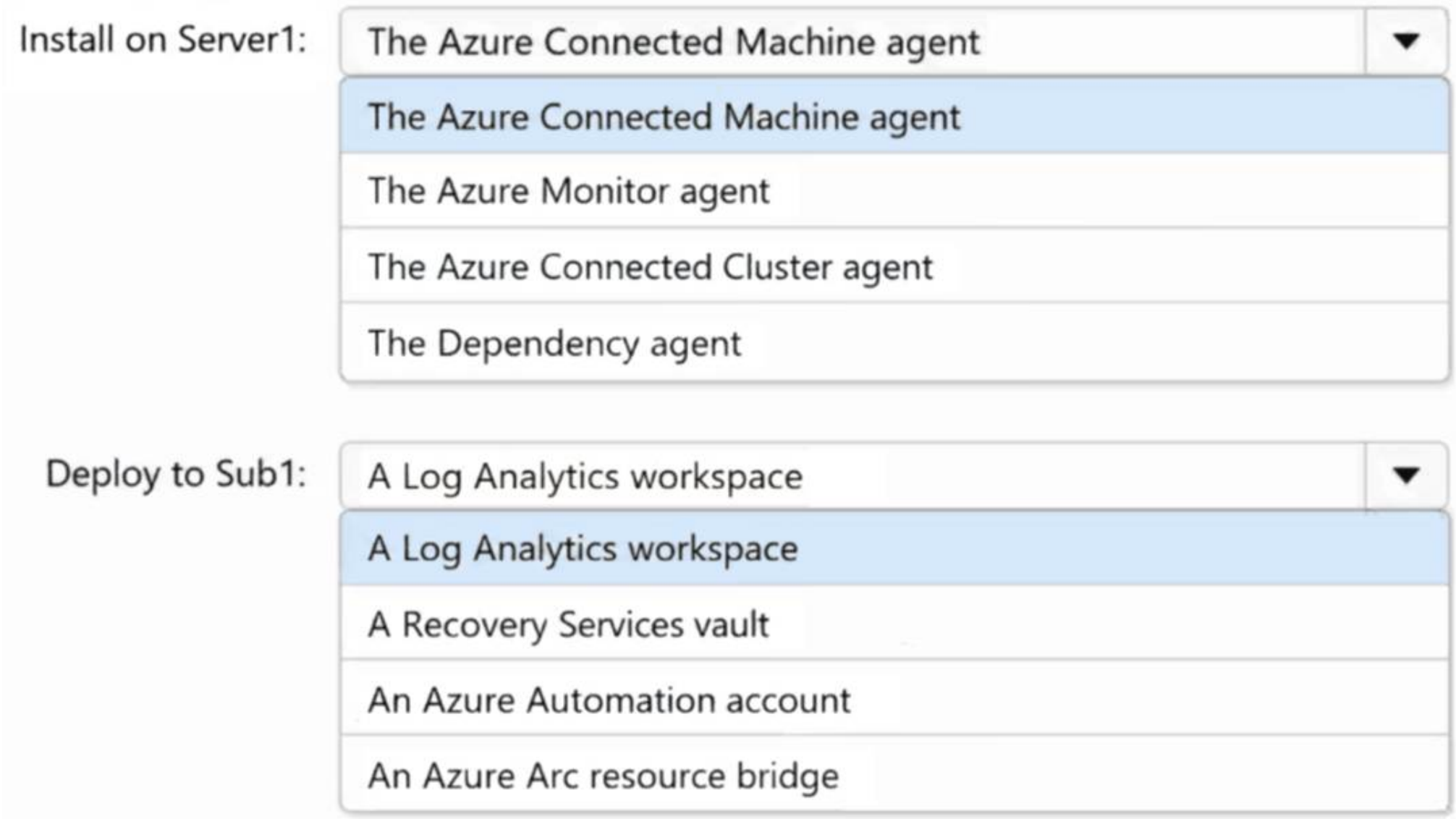
NEW QUESTION 5
Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible 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 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 6
You need to configure Server1 to meet the technical requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Install on Server1: The Azure Connected Machine agent; Deploy to Sub1: A Log Analytics workspace
The Azure Connected Machine agent is required to onboard a non-Azure server as an Azure Arc-enabled server. Once the server is represented in Azure, telemetry and security data can be directed to a Log Analytics workspace in the subscription. This combination supports Defender for Cloud and Sentinel-style monitoring without treating the server as a native Azure VM. Deploying only a workspace would not onboard Server1; installing only the agent would not provide the analytics destination. This answer also follows operational scalability. Microsoft security architecture favors policy-driven deployment, agentless assessment, managed identities, and Defender workload plans where possible. Those mechanisms reduce manual configuration while keeping enforcement tied to the resource type, which is why the selected choice is stronger than manual or after-the-fact alternatives. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Azure Arc and Sentinel data collection; Microsoft Learn > Connected Machine agent and Log Analytics workspace.

NEW QUESTION 7
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
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
Overview - Fabrikam, Inc. is a consulting company. The company has a main office in New York City and branch offices in Amsterdam and Singapore. Existing Environment. Network environment The on-premises network contains a datacenter in each office. Existing Environment. Cloud environment Fabrikam has two Azure subscriptions named Sub1 and Sub2 and a Microsoft 365 subscription that includes Microsoft 365 E5 licenses. All the subscriptions are linked to a Microsoft Entra tenant named fabrikam.com that contains the identities shown in the following table.

Name	Location	Deployment type
ER1	West Europe	ExpressRoute with a connectivity provider
ER2	West Europe	ExpressRoute Metro with a connectivity provider
ER3	East US	ExpressRoute Direct
ER4	Southeast Asia	ExpressRoute Metro Direct

For RG1, create a new Privileged Identity Management (PIM) eligible role assignment that assigns the Contributor role to supported groups. Planned Changes and Requirements. Technical Requirements Fabrikam has the following technical requirements: If VM1 is deleted, the permissions for VM1 must be removed automatically. The AKS1 managed identity must only be able to pull images from Registry1. The ID1 managed identity must be able to push images to and pull images from Registry1. All the data in the storage accounts must be encrypted by using Fabrikam-managed keys. All outbound traffic from the function apps to the on-premises network must use ExpressRoute circuits. ExpressRoute connectivity between the on-premises network and the Azure environment must be encrypted

by using Layer 2 or Layer 3 encryption.
You need to implement the planned change for SQLdb1
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point

A. Create a compliance policy.
B. Configure Microsoft Entra authentication for SQLServer1.
C. Create a Conditional Access policy.
D. Configure federated client identity for SQLdb1.
E. Configure a user-assigned managed identity for SQLdb1.

Answer: BC

Explanation:
Microsoft Entra authentication must be configured on the SQL server before Microsoft Entra identities and Conditional Access can govern database access. A Conditional Access policy then enforces the planned access control for SQLdb1. A compliance policy does not authenticate SQL connections. Federated client identity and a user-assigned managed identity are used for workload identity scenarios, not for enforcing user sign-in requirements against Azure SQL in this case. The exam objective emphasizes practical identity enforcement rather than cosmetic configuration. A valid answer must identify who authenticates, what permission is granted, where the scope is applied, and whether the method continues to work without passwords or secrets. That is why the selected answer is preferred over broader administrative roles or unrelated access settings. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Azure SQL authentication and conditional access; Microsoft Learn > Microsoft Entra authentication for Azure SQL.

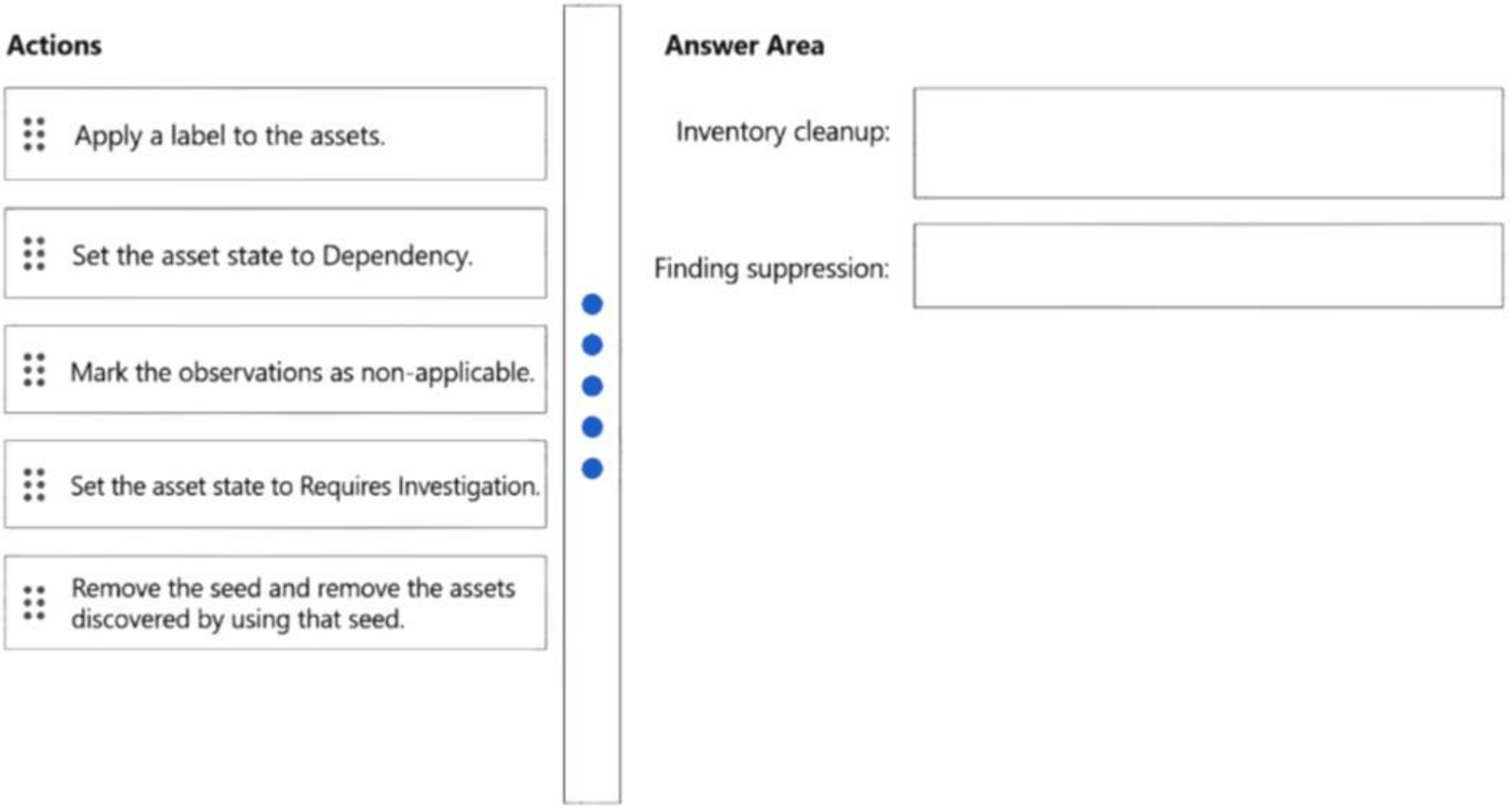
NEW QUESTION 10
You have an Azure subscription named Sub1. Sub1 contains 20 virtual machines that run Windows Server.
Sub1 has the Microsoft Defender for Cloud Defender Cloud Security Posture Management (CSPM) plan enabled.
You need to ensure that all the virtual machines are scanned automatically for 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
You have a Microsoft Defender External Attack Surface Management (Defender EASM) resource for a company named Contoso. Ltd.
You need to update the Defender EASM workflow to meet the following requirements:
•Assets from a business domain that Contoso no longer owns must be removed from inventory.
•Findings that do NOT apply to confirmed inventory must NOT affect reported counts.
What should you do for each requirement? To answer, drag the appropriate actions to the correct requirements. 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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Inventory cleanup: Remove the seed and remove the assets discovered by using that seed; Finding suppression: Mark the observations as non-applicable
When a seed domain is no longer owned, the clean inventory action is to remove the seed and remove assets discovered from that seed. Leaving those assets as dependencies or merely labeling them would keep stale assets in the inventory. For findings that do not apply to confirmed inventory, marking the observations as non-applicable prevents them from influencing finding counts while retaining the operational history needed for audit and review. 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 > Defender EASM; Microsoft Learn > inventory and observation state management.

NEW QUESTION 13
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 storage. Public access from all networks is enabled for storage1.
You need to ensure that VM1 and VM2 can access storage1.
Solution: You create a private endpoint on storage1.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
A private endpoint changes network routing so clients reach the storage account over a private IP address, but it does not grant data-plane authorization. The scenario already allows public network access, so network reachability is not the missing component. VM1 and VM2 still need Azure RBAC assignments for their managed identities or another valid authentication path. Therefore, a private endpoint alone does not meet the goal. 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 > private endpoints and storage access; Microsoft Learn > private endpoints provide network access, not authorization.

NEW QUESTION 14
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 16

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 18
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 23
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?

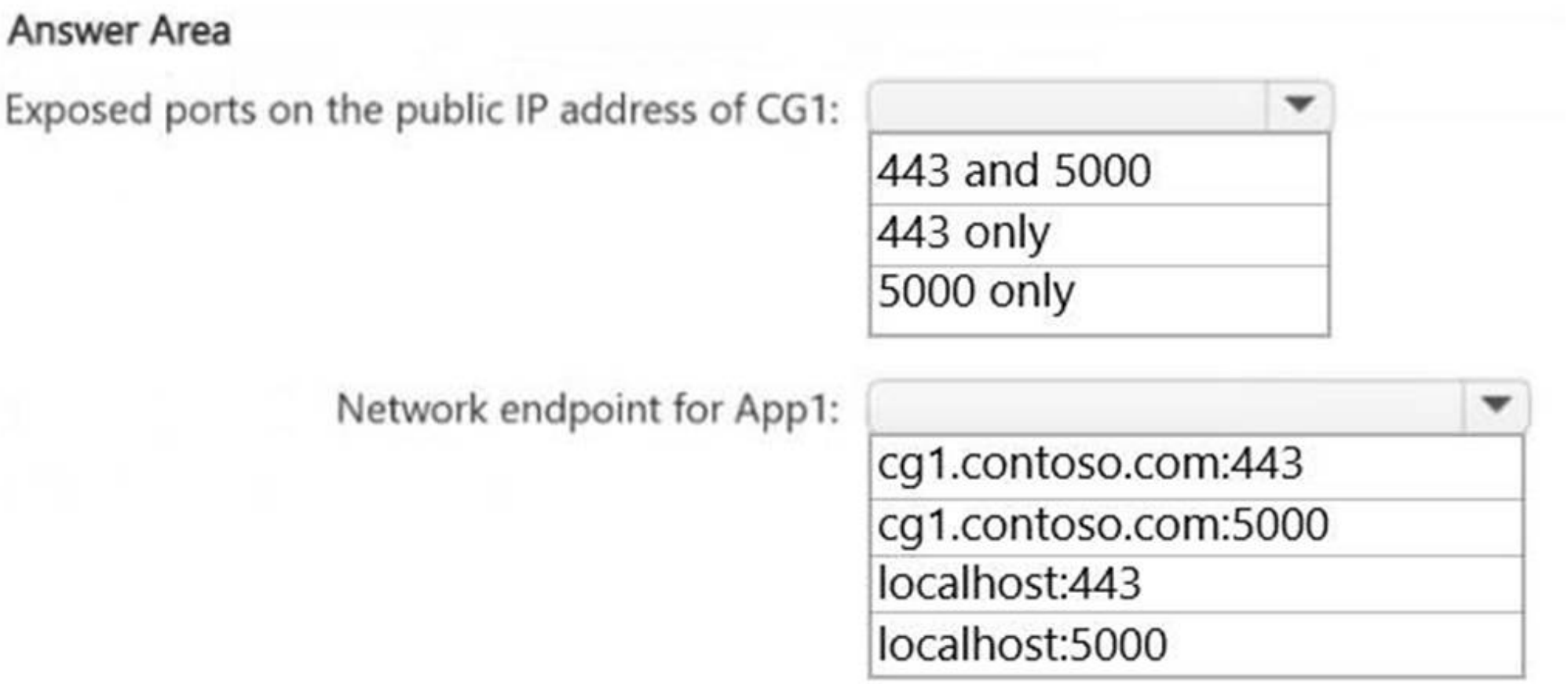
A. Assign the Storage Account Contributor role to the managed identity of app1 at the scope of storage1.
B. Assign the Storage Blob Delegator role to the managed identity of app1 at the scope of container1.
C. Assign the Owner role to the managed identity of app1 at the scope of container1.
D. Assign 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 27
You have an Azure Container Instances container group named CG1 that has a DNS name of cg1.contoso.com. CG1 has the following configurations:
•A Linux container named container1 that serves HTTPS over TCP port 443 and hosts an application named App1
•A Linux container named container2 that listens on TCP port 5000 and is accessed only by App1
•A public IP address
A security review finds that external clients can reach TCP port 5000 by using the public IP address of CG1.
You need to meet the following requirements:
•Ensure that the external clients can access container1 only by using TCP port 443.
•Ensure that container1 can continue to access container2

What should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

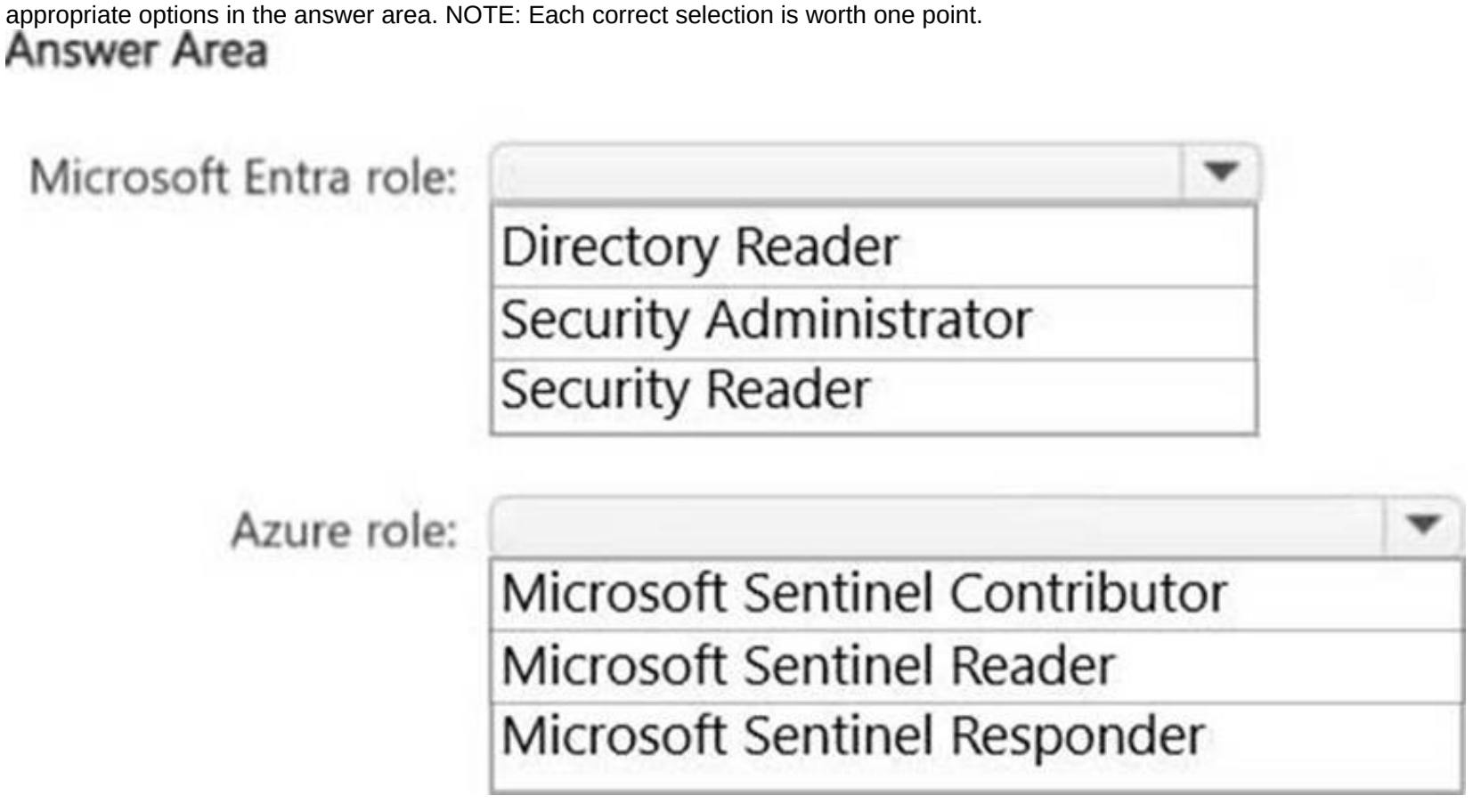


A. Mastered
B. Not Mastered

Answer: A

Explanation:
Exposed ports on the public IP address of CG1: 443 only;
Network endpoint for App1: localhost:5000
In an Azure Container Instances group with a public IP address, only the ports exposed on the container group public endpoint are reachable externally. The public exposed port should therefore be limited to 443. Containers inside the same container group can communicate with one another over localhost, so App1 can continue to reach container2 at localhost:5000 without exposing port 5000 publicly. 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 > Azure Container Instances security; Microsoft Learn > container group exposed ports and localhost communication.

NEW QUESTION 28
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 31
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 32
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 37
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 40
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 42
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 44
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 47
.....

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