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.

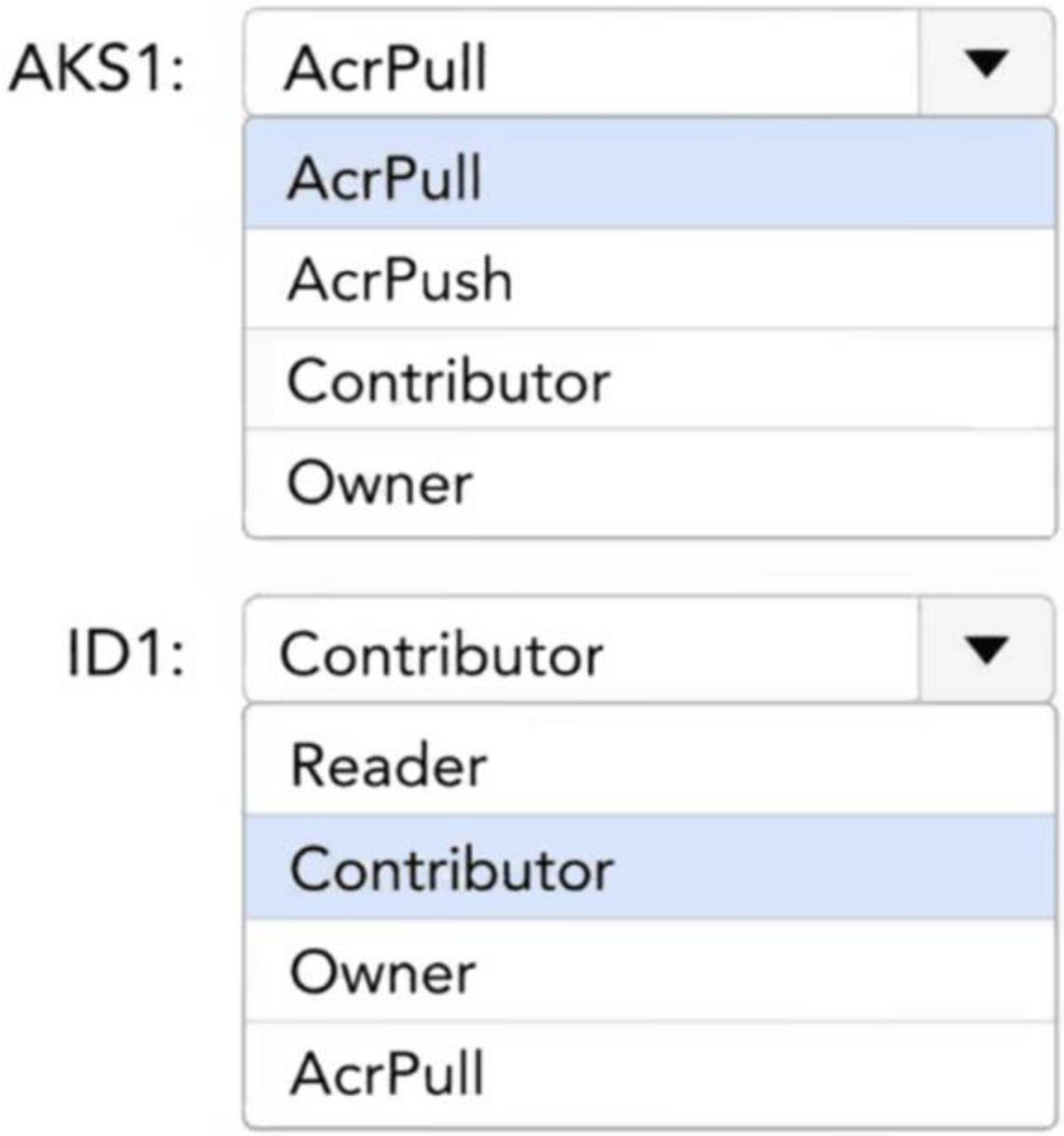
NEW QUESTION 2
Note. This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible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

A. Yes
B. No

Answer: B

Explanation:
A hunting query is an investigation tool. It can find suspicious activity or support manual threat hunting, but it does not automatically assign every new incident to a group or flag it for triage. The requirement is an operational automation requirement on incident creation. Therefore, a hunting query alone does not meet the goal even though it may help analysts review incidents later. In Microsoft Sentinel and Defender scenarios, collection, detection, investigation, and automation are separate functions. The selected answer maps to the function requested by the question rather than a neighboring capability. This is why analytics, hunting, workbooks, connectors, automation rules, and playbooks must not be treated as interchangeable. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Sentinel hunting and automation; Microsoft Learn > hunting queries versus incident automation.

NEW QUESTION 3
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.

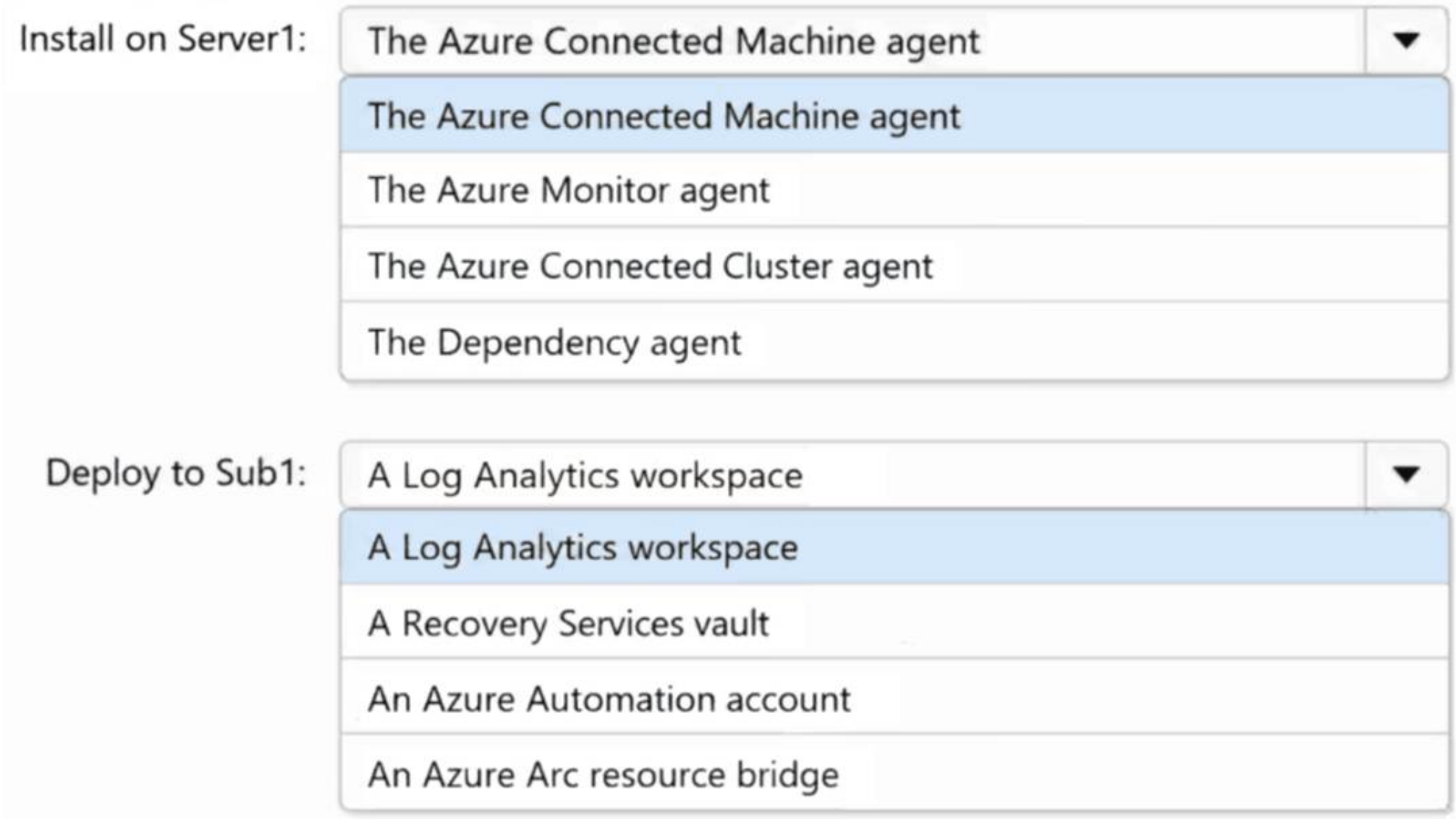


A. Mastered
B. Not Mastered

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 4
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 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 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 6
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 7
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 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 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 role on storage1.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
The solution as worded adds virtual machine resources to a role. Azure Storage authorization through Azure RBAC is granted to security principals such as managed identities, users, groups, and service principals, not to VM compute objects as resource containers. Since each VM already has a system-assigned managed identity, the correct approach would be to assign the storage data role to those identities. As stated, this solution does not meet the goal. 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 > managed identities and storage access; Microsoft Learn > RBAC role assignments are made to identities.

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

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

Answer: A

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

NEW QUESTION 10
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

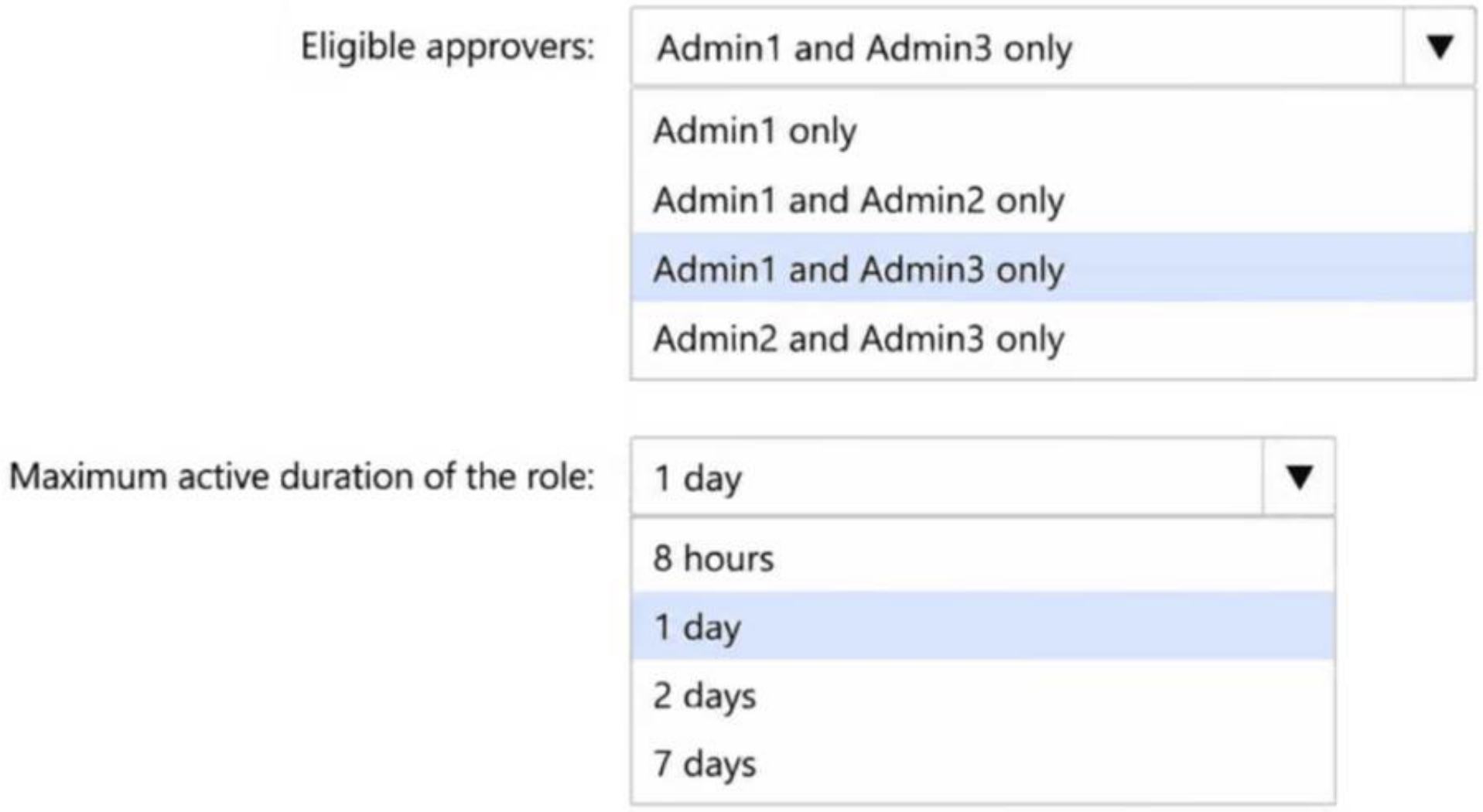
Answer: B

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 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 12
Overview - Fabrikam, Inc. is a consulting company. The company has a main office in New York City and branch offices in Amsterdam and Singapore. Existing Environment. Network environment The on-premises network contains a datacenter in each office. Existing Environment. Cloud environment Fabrikam has two Azure subscriptions named Sub1 and Sub2 and a Microsoft 365 subscription that includes Microsoft 365 E5 licenses. All the subscriptions are linked to a Microsoft Entra tenant named fabrikam.com that contains the identities shown in the following table.

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

For RG1, create a new Privileged Identity Management (PIM) eligible role assignment that assigns the Contributor role to supported groups. Planned Changes and Requirements. Technical Requirements Fabrikam has the following technical requirements: If VM1 is deleted, the permissions for VM1 must be removed automatically. The AKS1 managed identity must only be able to pull images from Registry1. The ID1 managed identity must be able to push images to and pull images from Registry1. All the data in the storage accounts must be encrypted by using Fabrikam-managed keys. All outbound traffic from the function apps to the on-premises network must use ExpressRoute circuits. ExpressRoute connectivity between the on-premises network and the Azure environment must be encrypted by using Layer 2 or Layer 3 encryption.
You need to implement the planned change for storage2 The solution must meet the technical requirements for storage encryption.
What should you do?

A. Enable purge protection for storage2.
B. Create an encryption scope in storage2.
C. Configure storage2 to use an account encryption key.
D. Assign an Azure role-based access control (Azure RBAC) role to storage2.

Answer: C

Explanation:
Because storage2 must support Azure Table storage, it must be created to use an encryption key scoped to the storage account. Azure Table storage can then be encrypted by using a Fabrikam-managed customer-managed key. Encryption scopes apply to Blob storage and do not meet the requirement for Table storage encryption.
Reference:
https://learn.microsoft.com/en-us/azure/storage/common/account-encryption-key-create?tabs=portal
https://learn.microsoft.com/en-us/azure/storage/blobs/encryption-scope-overview

NEW QUESTION 13
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 16
You have a Microsoft 365 subscription.
You use Microsoft Entra Agent ID to manage an agent identity.
You manage AI agents from the Microsoft 365 admin center.
An autonomous agent named Agent1 runs without a signed-in user. The agent must access Microsoft Graph and read secrets from a single Azure key vault.
You need to grant Agent 1 access to Microsoft Graph and Key Vault without requiring user interaction or consent at runtime.
What should you do for the agent identity? To answer, drag the appropriate actions to the correct services. Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.
MISSING

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To access Microsoft Graph: Grant an application permission;
To access Key Vault: Assign a role-based access control (RBAC) role
An autonomous agent has no signed-in user at runtime, so Microsoft Graph access must use application permissions rather than delegated permissions. Key Vault is protected through Azure RBAC, so the agent identity should receive an appropriate Key Vault role at the smallest possible scope. This avoids runtime user consent and avoids embedding secrets. Delegated permissions would fail for a background agent because there is no user context. For SC-500, the decisive distinction is whether the control authenticates an identity, grants authorization, or merely changes configuration visibility. The incorrect choices generally either grant excessive privilege, change the application model, or operate at the wrong scope. Microsoft expects the least-privilege identity path that satisfies the scenario without introducing shared secrets or unnecessary tenant-wide rights. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Manage Entra Agent ID access; Microsoft Learn > Graph application permissions and Key Vault RBAC.

NEW QUESTION 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 22
You have a Microsoft Entra tenant that has the following configurations:
•User consent for applications is disabled.
•Only administrators can grant permissions to applications.
You register an application named App1 that uses delegated Microsoft Graph permissions.
You need to configure App1 to meet the following requirements:
•Enable user sign-ins without interactive consent prompts.
•Enable App1 to access Microsoft Graph on behalf of the signed-in user.
What should you do?

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

Answer: D

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

NEW QUESTION 24
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

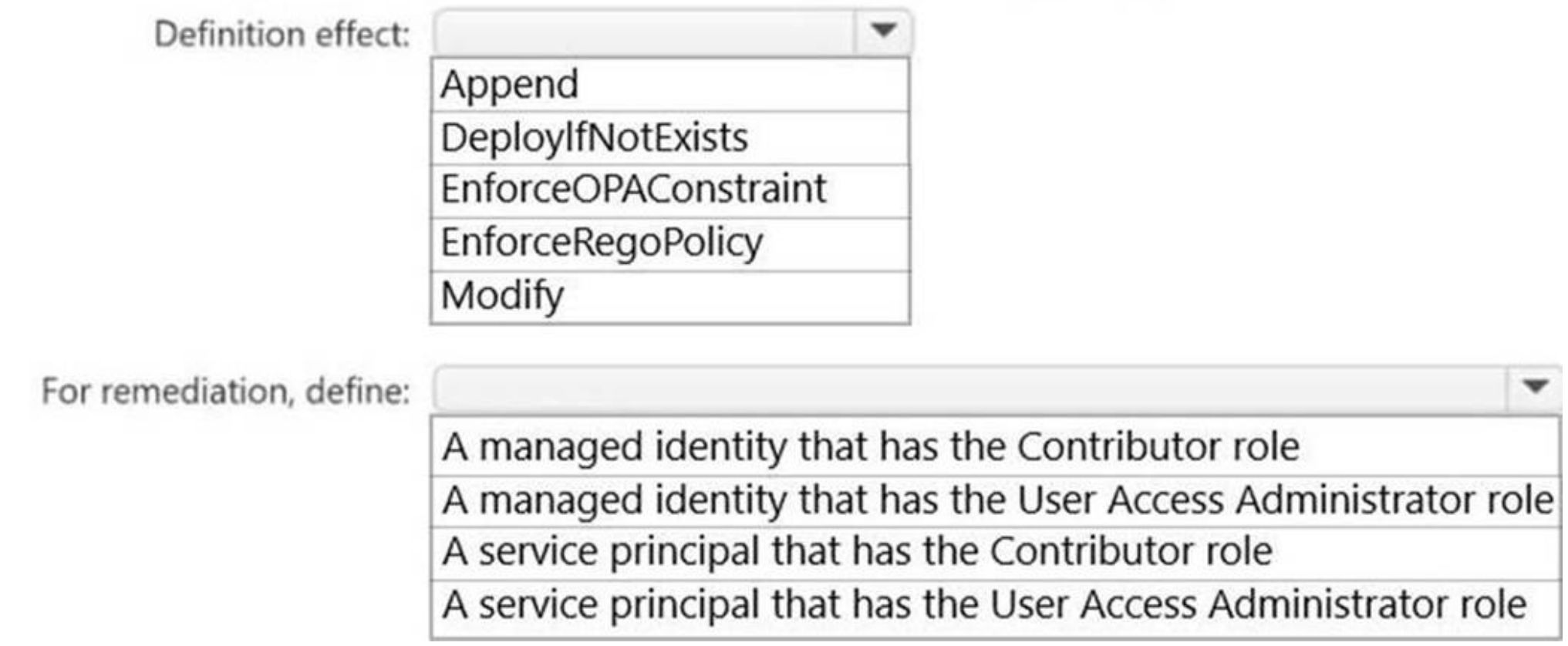
Answer: A

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

Answer Area



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 33
You have an Azure subscription.
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 34
You have two management groups named MG1 and MG2 that contain multiple Azure subscriptions. The subscriptions are linked to a Microsoft Entra tenant.
You have a user named User1 and a global administrator named Admin 1
You are informed that User1 created an Azure subscription named Sub1 under the MG2 management group and is the only owner of the subscription.
You need to ensure that Admin1 can remove the Owner role from User1 for Sub1.
What should you do first?

A. Move Sub1 to MG1.
B. Assign Admin1 the User Access Administrator role for Sub1.
C. Instruct Admin1 to use Privileged Identity Management (PIM) to request the Security Administrator role.
D. Instruct Admin1 to enable Access management for Azure resources.

Answer: D

Explanation:
Enabling Access management for Azure resources allows a Microsoft Entra Global Administrator to
elevate access and receive the User Access Administrator role at the root scope. This inherited access applies to Sub1 and enables Admin1 to remove User1??s Owner role assignment from the subscription.
Reference:
https://learn.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin?tabs=azure-portal%2Centra-audit-logs
https://learn.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles

NEW QUESTION 39
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 41
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 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 45
You are configuring a new Microsoft Sentinel workspace named Workspace1. You have an external IT Service Management (ITSM) system that is NOT supported by any Microsoft Sentinel solutions in Azure Marketplace. You need to ensure that Workspace1 creates service tickets in the ITSM system for all new security incidents. What should you create?
A.a playbook

D.an analytics rule
A. C.a watchlist

Answer: A

Explanation:
A Microsoft Sentinel playbook is an Azure Logic Apps workflow that automates response actions when incidents are created. It can integrate with an external ITSM system through an available connector or API call to create service tickets for new security incidents, even when no packaged Microsoft Sentinel solution exists for that system. Reference: https://learn.microsoft.com/en-us/azure/sentinel/automation/integrations https://learn.microsoft.com/en-us/azure/sentinel/automation/automation https://learn.microsoft.com/en-us/azure/sentinel/automation/playbook-recommendations

NEW QUESTION 48

.....

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