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 subscription that contains a user named User1 and an Azure Container Registry named ContReg1.
You enable content trust for ContReg1.
You need to ensure that User1 can create trusted images in ContReg1 The solution must use the principle of least privilege.
Which two roles should you assign to User1? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. AcrQuarantineWriter

B. Contributor
C. AcrQuarantineReader
D. AcrPush
E. AcrImageSigner

Answer: DE

Explanation:
To create trusted images, the user must be able to push images and sign them. AcrPush allows pushing image content to the registry, while AcrImageSigner allows signing trusted images. Contributor would be excessive because it grants broad management rights. Quarantine reader/writer roles relate to quarantine workflows, not content trust signing. The combination of AcrPush and AcrImageSigner matches least privilege for trusted image creation. 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 Container Registry security; Microsoft Learn > ACR roles for push and image signing.

NEW QUESTION 4
Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.
After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.
You have 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 5
You have multiple Microsoft Security Copilot workspaces.
A user named User1 accesses Security Copilot by using the default workspace.
You create a new workspace named Workspace 1 and assign a capacity to Workspace1.
You plan to route Security Copilot agent traffic to Workspace1.
You need to ensure that User1 can use embedded experiences without errors.
What should you do before switching to Workspace1?

A. Add User1 to Workspace1.
B. Assign User1 the Security Operator role in Microsoft Entra.
C. Disassociate the capacity from the default workspace.
D. Create a new capacity for Workspace1.

Answer: A

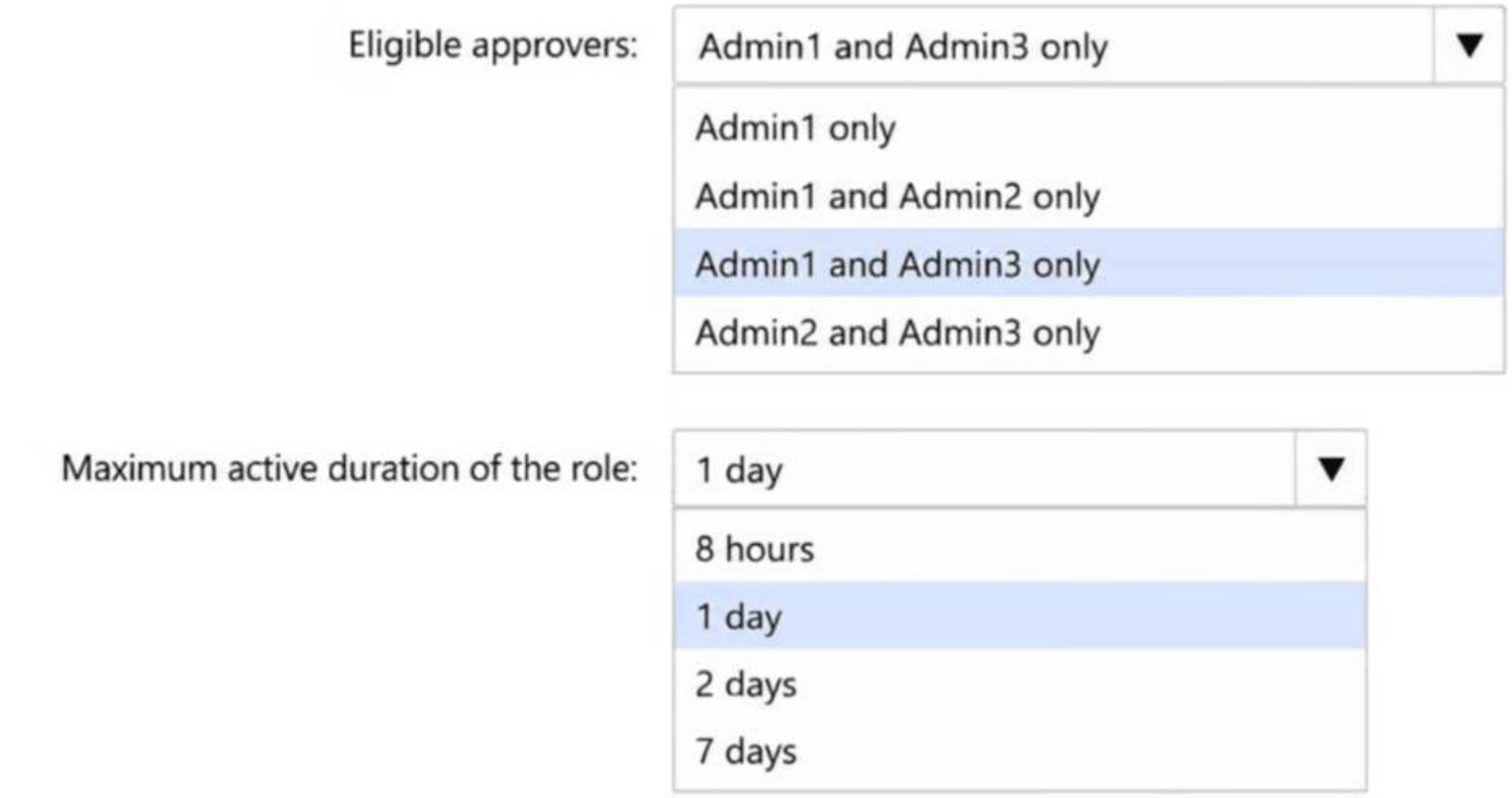
Explanation:
Security Copilot workspaces have membership and capacity associations. Before routing embedded experience traffic to Workspace1, User1 must be granted access to that workspace. Assigning a generic Security Operator role in Microsoft Entra does not make the user a member of the Security Copilot workspace. Disassociating capacity from the default workspace or creating more capacity does not resolve the user-access error. 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 > Security Copilot workspaces; Microsoft Learn > workspace access and capacity.

NEW QUESTION 6
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 7
Overview - Fabrikam, Inc. is a consulting company. The company has a main office in New York City and branch offices in Amsterdam and Singapore. Existing Environment. Network environment The on-premises network contains a datacenter in each office. Existing Environment. Cloud environment Fabrikam has two Azure subscriptions named Sub1 and Sub2 and a Microsoft 365 subscription that includes Microsoft 365 E5 licenses. All the subscriptions are linked to a Microsoft Entra tenant named fabrikam.com that contains the identities shown in the following table.

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

For RG1, create a new Privileged Identity Management (PIM) eligible role assignment that assigns the Contributor role to supported groups. Planned Changes and Requirements. Technical Requirements Fabrikam has the following technical requirements: If VM1 is deleted, the permissions for VM1 must be removed automatically. The AKS1 managed identity must only be able to pull images from Registry1. The ID1 managed identity must be able to push images to and pull images from Registry1. All the data in the storage accounts must be encrypted by using Fabrikam-managed keys. All outbound traffic from the function apps to the on-premises network must use ExpressRoute circuits. ExpressRoute connectivity between the on-premises network and the Azure environment must be encrypted by using Layer 2 or Layer 3 encryption.
You need to implement the planned change for 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 8
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 9
You need to protect the applications hosted on AKS1. The solution must meet the technical requirements.
Which Defender for Cloud plan should you enable?

A. Microsoft Defender for Servers
B. Microsoft Defender for App Service
C. Microsoft Defender for Containers
D. Microsoft Defender for Resource Manager
E. Microsoft Defender for Storage

Answer: C

Explanation:
AKS workload protection is provided by Microsoft Defender for Containers. That plan covers Kubernetes posture, runtime threat detection, image risk signals, and container workload protections. Defender for Servers protects VMs and Arc servers, Defender for App Service protects web apps, Resource Manager protects control-plane operations, and Defender for Storage protects storage accounts. Because the applications are hosted on AKS1, Defender for Containers is the correct plan. The compute domain tests whether protection is applied before deployment, during runtime, or through posture assessment. The selected answer matches the phase described in the requirement. Detection-only tools are not acceptable when the requirement says prevent, and local installation methods are inferior when Defender for Cloud, Azure Policy, or Azure Machine Configuration can enforce the control centrally. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Defender for Containers; Microsoft Learn > AKS workload protection.

NEW QUESTION 10
You have an Azure subscription named Sub1 that contains multiple virtual machines. Sub1 has the Microsoft Defender Cloud Security Posture Management (CSPM) plan enabled.
You discover that Defender for Cloud falls to identify plaintext connection strings and SSH keys stored on the virtual machines.
You need to ensure that secrets can be identified on the virtual machines.
What should you do?

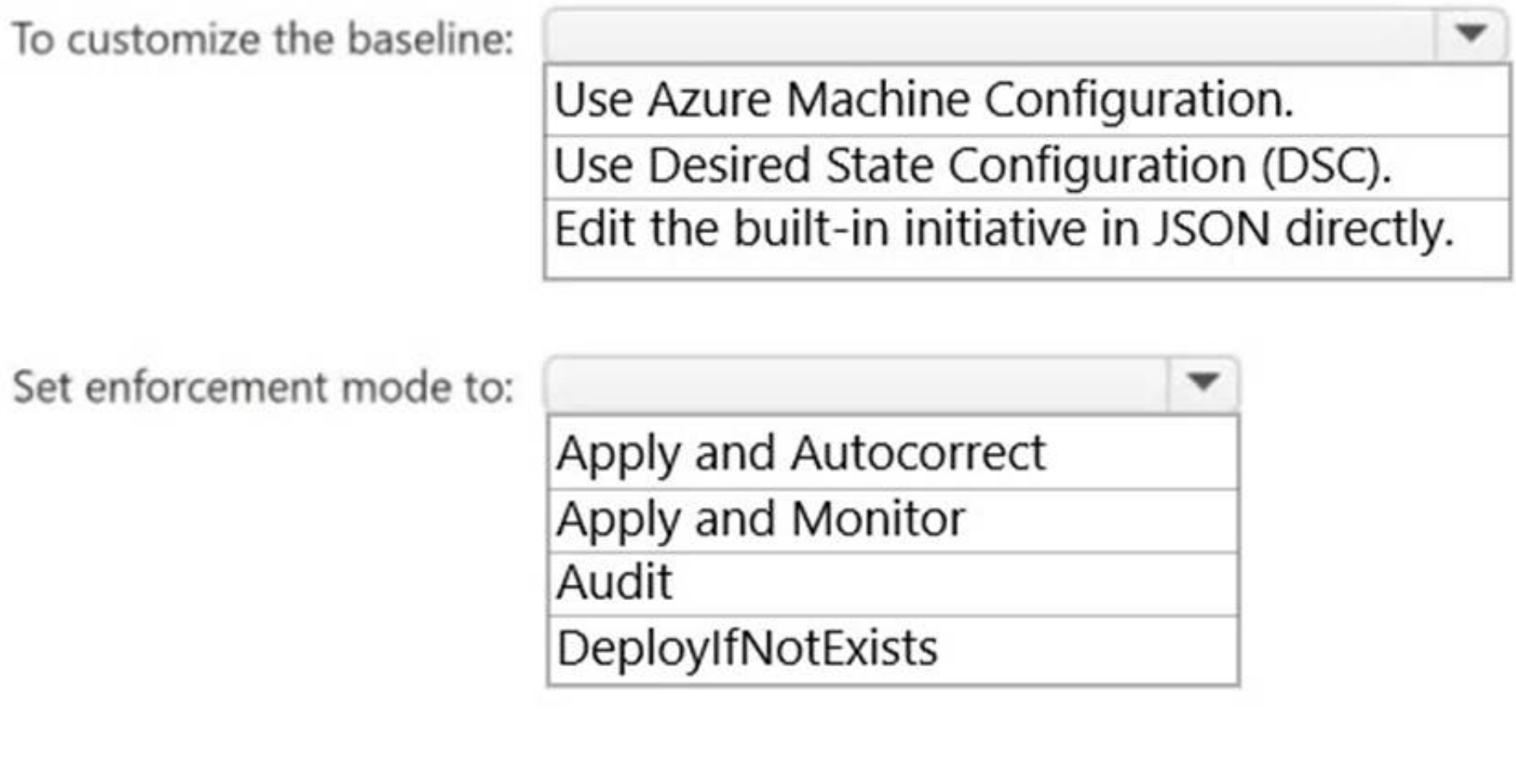
A. Configure the Defender for Cloud data connector in Microsoft Sentinel.
B. Enable agentless machine scanning.
C. Deploy the Azure Monitor Agent to all the virtual machines.
D. Enable Microsoft Defender for Key Vault.

Answer: B

Explanation:
Defender CSPM identifies secrets such as plaintext connection strings and SSH keys on machines through agentless machine scanning. If those secrets are not being identified, the missing capability is the agentless scan feature. The Sentinel data connector only forwards alerts and posture data, the Azure Monitor Agent collects telemetry, and Defender for Key Vault protects vault access; none of those scan VM disks for exposed secrets. 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 > scan for secrets by Defender CSPM; Microsoft Learn > agentless scanning for machines.

NEW QUESTION 10
You have an Azure subscription that contains the following servers:
•200 virtual machines that run either Windows Server or Ubuntu Server
•50 Azure Arc enabled servers
You use Azure Policy to manage compliance across all the servers.
You need to enforce an organization-specific security baseline. The solution must meet the following requirements:
•Customize a built-in security baseline.
•Ensure that configuration changes to the servers are enforced automatically after the security baseline is deployed.
?Minimize administrative effort.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
To customize the baseline: Use Azure Machine Configuration;
Set enforcement mode to: Apply and Autocorrect
Azure Machine Configuration is the correct mechanism for applying and customizing guest configuration baselines across Azure VMs and Azure Arc-enabled servers. It integrates with Azure Policy and can enforce configuration through assignment modes such as Apply and Autocorrect. This provides centralized compliance and automatic correction without building a separate configuration-management pipeline for Windows and Linux servers. The compute domain tests whether protection is applied before deployment, during runtime, or through posture assessment. The selected answer matches the phase described in the requirement. Detection-only tools are not acceptable when the requirement says prevent, and local installation methods are inferior when Defender for Cloud, Azure Policy, or Azure Machine Configuration can enforce the control centrally. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Azure Machine Configuration; Microsoft Learn > assignment modes and remediation.

NEW QUESTION 15
You have an Azure SQL Database logical server named Server1 that contains a database named DB1.
You need to configure authentication for Server1 to meet the following requirements;
•SQL authentication cannot be used for any databases on Server1.
•The solution must be enforced centrally at the server level.
What should you do?

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

Answer: C

Explanation:
The requirement is centralized enforcement for all databases on the logical server. Microsoft Entra-only authentication disables SQL authentication at the server level, so SQL logins cannot be used against any database hosted there. Configuring an Entra administrator is typically a prerequisite or supporting step, but by itself it does not disable SQL authentication. A managed identity for the server and deleting logins from one database do not meet the central enforcement requirement. For SC-500, the decisive distinction is whether the control authenticates an identity, grants authorization, or merely changes configuration visibility. The incorrect choices generally either grant excessive privilege, change the application model, or operate at the wrong scope. Microsoft expects the least-privilege identity path that satisfies the scenario without introducing shared secrets or unnecessary tenant-wide rights. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Azure SQL authentication; Microsoft Learn > Microsoft Entra-only authentication for Azure SQL.

NEW QUESTION 18
You have a Microsoft Sentinel workspace
You need to collect Windows security events from 200 Azure virtual machines that run Windows Server. The solution must meet the following requirements:
•Use direct agent based data collection from each virtual machine.
•Use a supported agent for new virtual machine deployments
Which Microsoft Sentinel connector should you use?

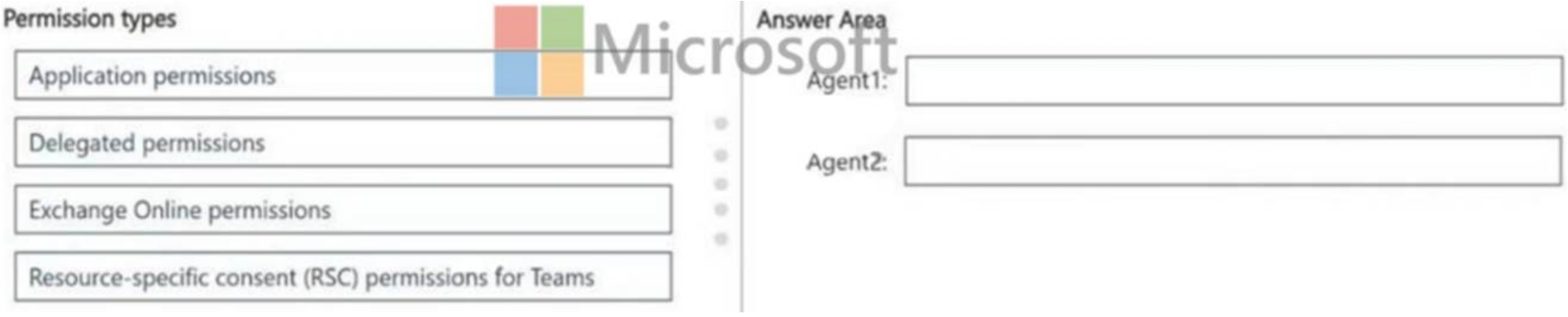
A. Windows Forwarded Events
B. Windows Security Events via AMA
C. Security Events via Legacy Agent

D. Syslog via AMA
E. Azure Resource Graph

Answer: B

Explanation:
The Windows Security Events via AMA connector uses Azure Monitor Agent and data collection rules for direct collection from Windows machines. It is the supported path for new deployments and avoids the legacy Log Analytics agent. Windows Forwarded Events is for a Windows Event Collector model, not direct agent collection. Syslog via AMA is for Linux Syslog, and Azure Resource Graph is not an event-collection connector. In Microsoft Sentinel and Defender scenarios, collection, detection, investigation, and automation are separate functions. The selected answer maps to the function requested by the question rather than a neighboring capability. This is why analytics, hunting, workbooks, connectors, automation rules, and playbooks must not be treated as interchangeable. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Windows Security events using DCRs; Microsoft Learn > Windows Security Events via AMA connector.

NEW QUESTION 20
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 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 27
You have a Microsoft Entra tenant that has the following configurations:
•User consent for applications is disabled.
•Only administrators can grant permissions to applications.
You register an application named App1 that uses delegated Microsoft Graph permissions.
You need to configure App1 to meet the following requirements:
•Enable user sign-ins without interactive consent prompts.
•Enable App1 to access Microsoft Graph on behalf of the signed-in user.
What should you do?

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

Answer: D

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

NEW QUESTION 28
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 33
You have an Azure subscription named Sub1 that contains a storage account named storage1. Sub1 has Microsoft Defender for Storage enabled. Defender for Storage has on-upload malware scanning enabled for a monthly cap of 10,000 GB per storage account. You use a Microsoft Sentinel workspace to monitor security events on all Azure resources. You need to configure storage1 to use a malware scanning cap of 2,000 GB per month. What should you do?

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

Answer: A

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

NEW QUESTION 37
You have an Azure 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 39
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?

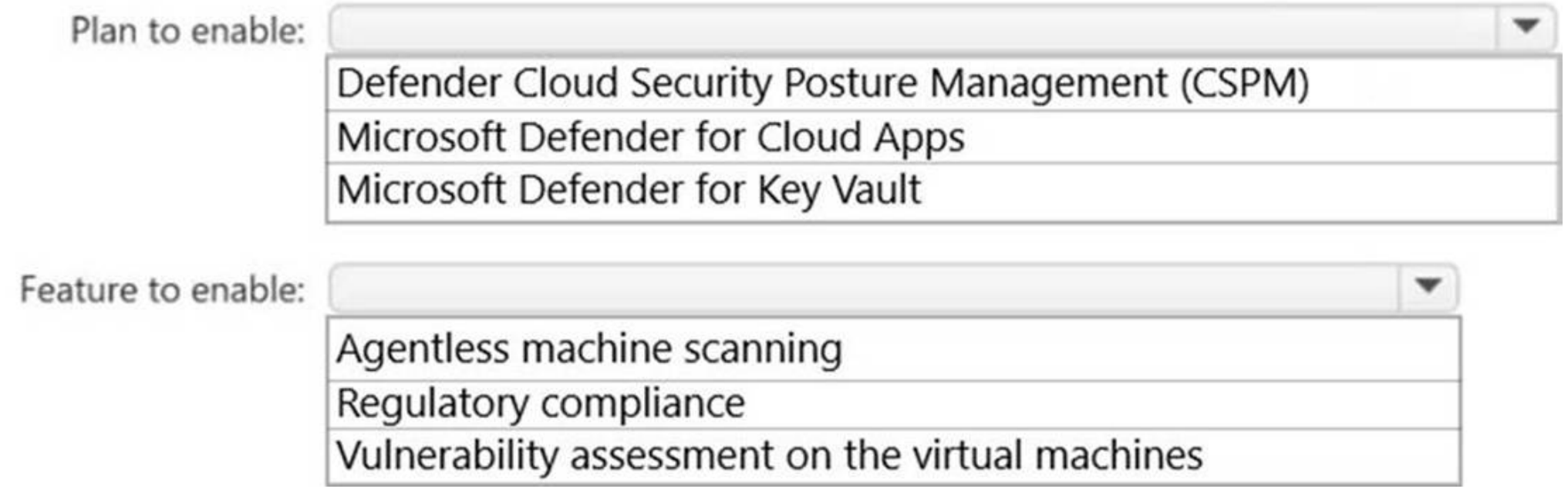
A. Azure Network Function Manager
B. Azure Firewall Manager
C. Azure Virtual Network Manager
D. Azure Front Door

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 40
HOTSPOT
You have an Azure subscription named Sub1 that contains 50 virtual machines. Sub1 has Microsoft Defender for Cloud enabled.
Sub1 contains an Azure key vault named KV1 and an Azure policy that enforces storing all secrets in KV1.
Occasionally, the developers at your company store plaintext tokens and SSH private keys on the virtual machines.
You need to configure Defender for Cloud to detect plaintext secrets on the virtual machines. The solution must minimize administrative changes to the virtual machines.
How should you configure Defender for Cloud? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 45
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 50
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 51
Which Azure Functions configuration limits the function app to accept requests only from a specific virtual network?

A. Private endpoints and access restrictions
B. Application Insights sampling
C. Durable Functions orchestration
D. Consumption plan scaling

Answer: A

Explanation:
Using private endpoints for inbound access plus access restriction rules lets you confine a function app to specific networks and deny public access. This network isolation reduces the exposure of serverless endpoints.

NEW QUESTION 54
After an AI agent identity is suspected of compromise, which Defender XDR capability helps you analyze the potential blast radius of that Entra Agent ID?

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

Answer: A

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

NEW QUESTION 56
You have an Azure management group named MG1 that contains two subscriptions named Sub1 and Sub2. Both subscriptions are linked to a Microsoft Entra tenant that contains a security group named Group1. You need to ensure that the members of Group1 can assign roles to the resources in Sub1 and Sub2. The solution must follow the principle of least privilege. Which role should you assign to Group1?

A. Contributor at the MG1 scope
B. Contributor at the Sub1 and Sub2 scopes
C. User Access Administrator at the MG1 scopecorrect
D. Owner at the MG1 scope

Answer: C

Explanation:
The User Access Administrator role permits members of Group1 to manage role assignments without granting them permission to modify the underlying Azure resources. Assigning the role at the MG1 scope causes the permission to be inherited by both Sub1 and Sub2 and their resources, providing centralized least-privilege access management.
Reference:
https://learn.microsoft.com/en-us/azure/role-based-access-control/role-definitions
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/scope-overview

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