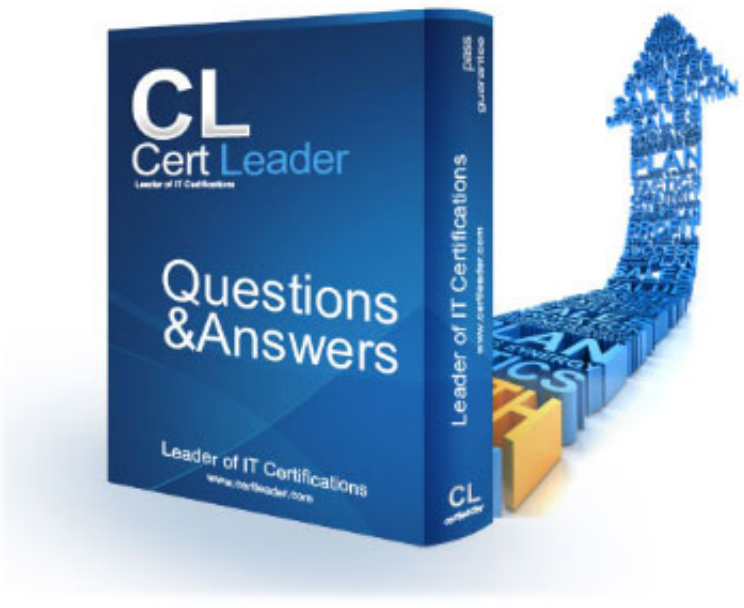
SC-500 Dumps

Microsoft Certified: Cloud and AI Security Engineer Associate

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



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

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

Answer: A

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

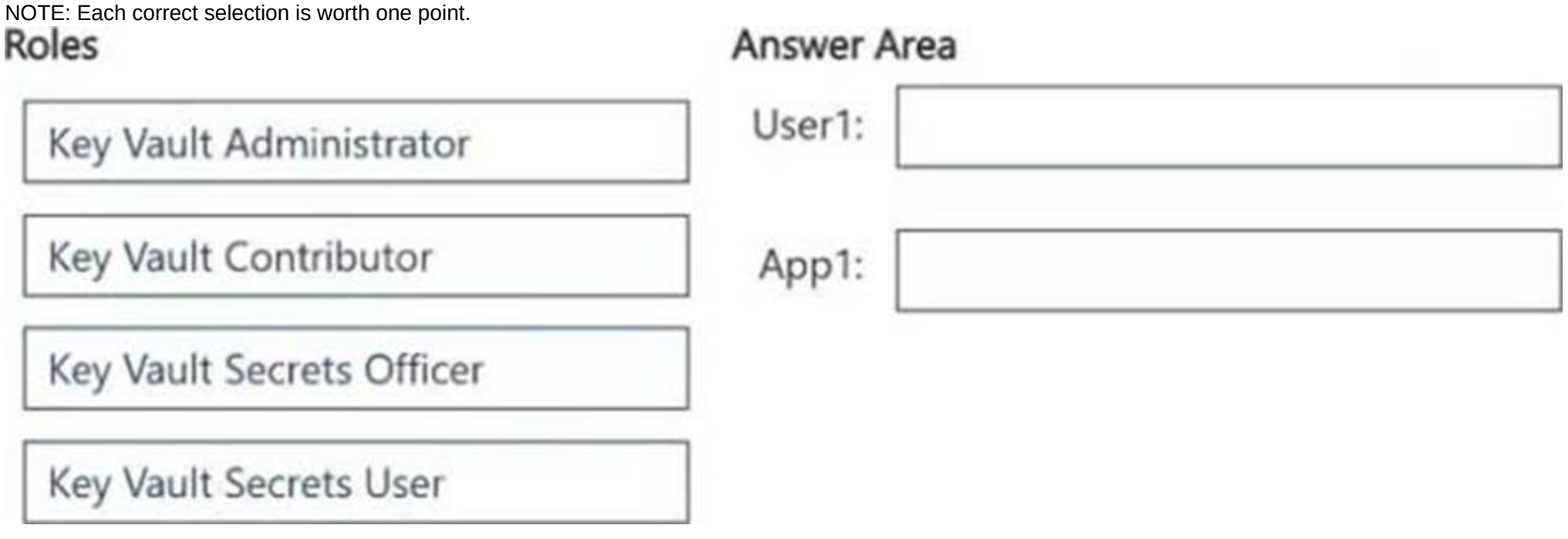
NEW QUESTION 2
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You have an Amazon Web Services (AWS) account connected to Defender for Cloud that has the Defender Cloud Security Posture Management (CSPM) plan enabled.
You need to identify the potential impact of security incidents that exploit multiple risks reported by Defender CSPM.
What should you use?

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

Answer: D

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

NEW QUESTION 3
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
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 5
For each of the following statements, select Yes if the statement is true Otherwise, select No.
Answer Area

Statements	Yes	No
Admin1 must approve requests for the Agent ID Developer role.	○	○
Admin2 can approve requests for the AI Administrator role.	○	○
Admin3 can assign User1 a two-day active assignment for the Agent ID Developer role.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Yes; 2) No; 3) Yes
The visible PIM settings indicate that Admin1 must approve Agent ID Developer activations, Admin2 is not an approver for the AI Administrator role, and Admin3 can assign User1 a two-day active assignment for Agent ID Developer. The controlling factors are the configured approver list and active assignment duration policy for each role. PIM evaluates those settings per role, so approval authority or duration for one role cannot be assumed for another role. For SC-500, the decisive distinction is whether the control authenticates an identity, grants authorization, or merely changes configuration visibility. The incorrect choices generally either grant excessive privilege, change the application model, or operate at the wrong scope. Microsoft expects the least-privilege identity path that satisfies the scenario without introducing shared secrets or unnecessary tenant-wide rights. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > PIM role settings and Agent ID governance; Microsoft Learn > approvers and maximum activation duration.

NEW QUESTION 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 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 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 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 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
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 need to protect the applications hosted on AKS1. The solution must meet the technical requirements.
Which Defender for Cloud plan should you enable?

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

Answer: C

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

NEW QUESTION 10
Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.
After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.
You have a Microsoft Sentinel workspace
You have a multi-tier Security Operations Center (SOC) team.
You need to ensure that all new security incidents are assigned immediately to the Tier 1 analysts group and flagged for triage.
Solution: You create an analytics rule.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
An analytics rule creates alerts and incidents from detection logic. It is not a global mechanism for assigning every new incident from all sources or adding triage flags after incident creation. While a specific analytics rule can set some incident details for incidents it generates, it does not meet the stated goal for all new incidents in the workspace. Sentinel automation rules or playbooks are the correct tools. In Microsoft Sentinel and Defender scenarios, collection, detection, investigation, and automation are separate functions. The selected answer maps to the function requested by the question rather than a neighboring capability. This is why analytics, hunting, workbooks, connectors, automation rules, and playbooks must not be treated as interchangeable. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Sentinel analytics rules; Microsoft Learn > analytics rules create incidents, not global assignment handling.

NEW QUESTION 13
You have an Azure 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 16
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 19
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?

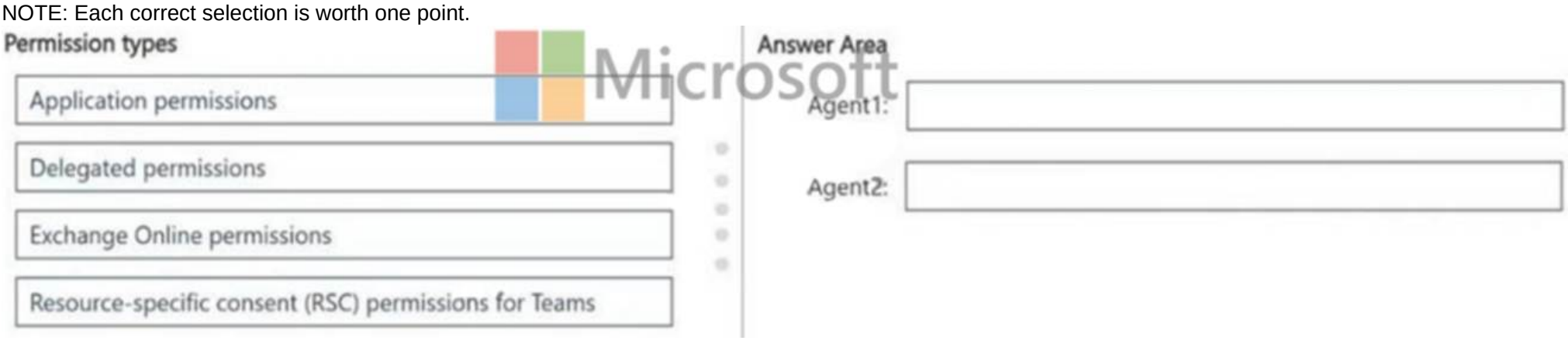
A. Windows Forwarded Events
B. Windows Security Events via AMA
C. Security Events via Legacy Agent
D. Syslog via AMA
E. Azure Resource Graph

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 21
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 26
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.

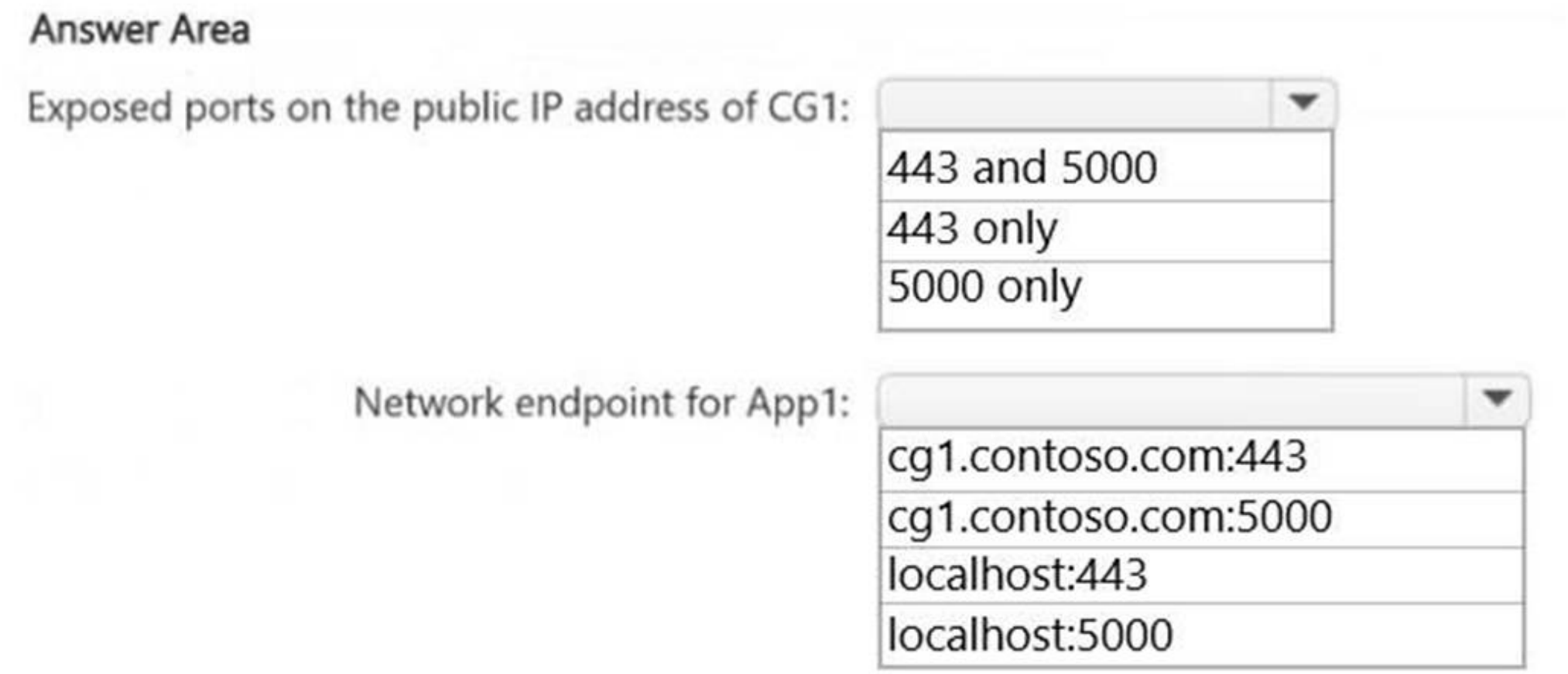
NEW QUESTION 28
You have an Azure Storage account named storage1 that hosts a blob container named container1.
You have an Azure Functions app named app1 that uses a managed identity.
You need to configure app1 to read, write, and delete blobs in container1. The solution must follow the principle of least privilege.
What should you do?

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

Answer: D

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

NEW QUESTION 29
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 30
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 31
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 35
You have an Azure subscription named Sub1 that contains an Azure Kubernetes Service (AKS) cluster named cluster1 and an Azure container registry named ACR1 Sub1 has Microsoft Defender for Containers enabled, and runtime protection is active on cluster!
The developers at your company deploy pods that have elevated privileges, and the deployments are created in cluster1
You need to prevent pods with elevated privileges from being accepted by cluster!
What should you do?

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

Answer: A

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

NEW QUESTION 40
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 41
You have a hybrid environment that contains the following servers:
•50 Azure virtual machines that run Windows Server 2019
•20 physical, on premises servers that run Windows Server 2019
All the servers use a third-party antivirus solution that must remain active during a phased security rollout
You need to onboard all the servers to Microsoft Defender for Endpoint by using a centralized deployment method. The solution must meet the following requirements:
•Endpoint detection and response (EDR) capabilities must be enabled.
•Antivirus conflicts must be prevented during onboarding.
What should you do on the servers?

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

Answer: C

NEW QUESTION 46
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 48
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 50
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 53
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 55
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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