

Microsoft

Exam Questions SC-500

Microsoft Certified: Cloud and AI Security Engineer Associate



NEW QUESTION 1

You have a Microsoft Entra tenant that has user consent for applications disabled.
You register an application named App1 that requests the following Microsoft Graph delegated permissions:

- user.Read
- Mail.Read

You need to configure tenant permissions to meet the following requirements:

- Enable users to grant consent for low-risk permissions without administrator interaction.
- Ensure that applications requesting higher-privilege permissions require administrator approval.

What should you do?

- A. Grant tenant-wide admin consent to App1.
- B. Configure application assignments for App1.
- C. Configure Privileged Identity Management (PIM) role assignments.
- D. Create an app consent policy.

Answer: D

Explanation:

An app consent policy allows the tenant to define which delegated permissions are considered low risk and may be consented to by users. Higher-privilege permissions can remain subject to admin consent. Tenant-wide admin consent would approve App1 broadly rather than creating an ongoing policy boundary. Application assignments and PIM role assignments control user access or privileged roles, not delegated permission consent behavior. This domain is tested through precise scope control: tenant, subscription, resource, application, and data-plane authorization are not interchangeable. The correct choice applies the smallest identity or governance control that enforces the stated requirement. Options that only add users, create registrations, or provide broad administrator access fail because they do not directly enforce the requested access behavior. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > app consent settings; Microsoft Learn > app consent policies.

NEW QUESTION 2

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.

Roles

Key Vault Administrator

Key Vault Contributor

Key Vault Secrets Officer

Key Vault Secrets User

Answer Area

User1:

App1:

- 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 3

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

AKS1:

AcrPull

▼

AcrPull

AcrPush

Contributor

Owner

ID1:

Contributor

▼

Reader

Contributor

Owner

AcrPull

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 4

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 5

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

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

Answer: A

Explanation:

Admin1 is the visible least-privilege delegate for the planned Defender for Cloud change. Defender for Cloud administration should be delegated to the user with the specific security or Defender permissions needed for the task, not to broader administrators unless required. Choosing a higher privileged account would violate the least-privilege requirement. The source file??s case-study background is not visible, so the answer follows the displayed answer selection and the general Defender for Cloud RBAC model. The SC-500 study guide places these tasks under security posture, event collection, Defender CSPM, EASM, Sentinel, and Security Copilot operations. The exam expects the control that minimizes analyst effort while preserving correct permissions and data flow. The selected answer reflects that service boundary and avoids a broader or merely investigative alternative. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Defender for Cloud least-privilege administration; Microsoft Learn > built-in Azure roles for Defender for Cloud.

NEW QUESTION 6

You have a Microsoft Defender External Attack Surface Management (Defender EASM) resource for a company named Contoso. Ltd.

You need to update the Defender EASM workflow to meet the following requirements:

- Assets from a business domain that Contoso no longer owns must be removed from inventory.
- Findings that do NOT apply to confirmed inventory must NOT affect reported counts.

What should you do for each requirement? To answer, drag the appropriate actions to the correct requirements. Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Actions

⋮ Apply a label to the assets.

⋮ Set the asset state to Dependency.

⋮ Mark the observations as non-applicable.

⋮ Set the asset state to Requires Investigation.

⋮ Remove the seed and remove the assets discovered by using that seed.

Answer Area

Inventory cleanup:

Finding suppression:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

means granting only the required data operation or allowing only the required network flow. The correct response avoids shared keys, broad peering, general contributor roles, or log-only controls when the scenario demands prevention, routing, event triggering, or account-specific configuration. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Defender EASM; Microsoft Learn > inventory and observation state management.

NEW QUESTION 7

You have an Azure key vault named KV1 that uses role-based access control (RBAC) authorization KV1 stores database connection strings for an Azure App Service web app named App1.

You enable a firewall on KV1 and allow access to KV1 from only the virtual network that contains App1.

You need to ensure that App1 can retrieve secrets from KV1 without using credentials stored in the application configuration.

What should you create?

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

Answer: A

Explanation:

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

NEW QUESTION 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	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 9

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 10

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 10

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 14

You have a management group named MG1 that contains two subscriptions named Sub1 and Sub2

Sub1 contains a resource group named RG-Exception and a resource group named RG1 that hosts Microsoft Foundry resources.

You need to assign an Azure policy to force new Foundry deployments in MG1 to use private endpoints. The solution must NOT restrict deployments in RG-Exception.

How should you configure the policy?

- A. Assign the policy to MG1 and exclude RG-Exception.
- B. Assign the policy to Sub1 and RG-Exception.
- C. Assign the policy to MG1 and RG-Exception.
- D. Assign the policy to Sub1 and exclude RG-Exception.

Answer: A

Explanation:

The policy must apply across the entire management group MG1 because both Sub1 and Sub2 are in scope for new Foundry deployments. The exception must be expressed as an exclusion for RG-Exception, not by assigning the policy directly to that resource group. Assigning only to Sub1 misses Sub2. Including RG-Exception in the assignment would restrict the resource group that the requirement explicitly excludes. 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 > Azure Policy; Microsoft Learn > policy assignment scopes and exclusions.

NEW QUESTION 17

HOTSPOT You have a Microsoft Sentinel workspace named Workspace1. You hire a security consultant. You provide the consultant with a guest account named User1 in your Microsoft Entra tenant. You need to enable User1 to assign incidents in Workspace1. Which roles should you assign to User1? To answer, select the appropriate options in the answer area. **NOTE:** Each correct selection is worth one point.

Answer Area

Microsoft Entra role:

Directory Reader
Security Administrator
Security Reader

Azure role:

Microsoft Sentinel Contributor
Microsoft Sentinel Reader
Microsoft Sentinel Responder

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Microsoft Entra role: Directory Reader

Azure role: Microsoft Sentinel Responder

Because User1 is a guest user, the Directory Reader role is required to assign Microsoft Sentinel incidents to users in the tenant. The Microsoft Sentinel Responder role grants the permissions needed to investigate and manage incidents, including updating incident ownership in Workspace1.

Reference:

<https://learn.microsoft.com/en-us/azure/sentinel/roles>

<https://learn.microsoft.com/en-us/azure/sentinel/investigate-incidents>

NEW QUESTION 21

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

Answer Area

Definition effect:

Append
DeployIfNotExists
EnforceOPAConstraint
EnforceRegoPolicy
Modify

For remediation, define:

A managed identity that has the Contributor role
A managed identity that has the User Access Administrator role
A service principal that has the Contributor role
A service principal that has the User Access Administrator role

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Definition effect: DeployIfNotExists

For remediation, define: A managed identity that has the Contributor role

The DeployIfNotExists effect deploys the custom security extension when a virtual machine does not already have the required extension. Remediation tasks use the deployment template in this policy effect to correct existing non-compliant virtual machines. The policy assignment requires a managed identity with the permissions needed to deploy the extension; the Contributor role provides the required resource deployment permissions.

Reference:

<https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effect-deploy-if-not-exists>

<https://learn.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources?tabs=azure-portal>

<https://learn.microsoft.com/en-us/azure/governance/policy/overview>

NEW QUESTION 22

You have an Azure virtual network that contains 100 virtual machines and an Azure Firewall instance named FW1.

All the traffic from the virtual machines is routed through FW1.

You need to ensure that FW1 allows access to only a URL of updates.contoso.com and blocks all other outbound traffic.

What should you use?

- A. an inbound NAT rule
- B. an application rule
- C. an outbound NAT rule
- D. a network rule

Answer: B

Explanation:

An Azure Firewall application rule permits outbound HTTP or HTTPS access based on a fully qualified domain name, such as updates.contoso.com. With only that destination allowed, traffic to other outbound web destinations is denied when no matching allow rule exists.

Reference:

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq>

NEW QUESTION 27

You have an Azure SQL Database logical server named Server1 that contains multiple databases.

The databases contain legacy SQL authentication logins that must no longer be usable for sign-in but must NOT be removed from the databases.

You need to ensure that SQL authentication is denied for connections.

What should you do?

- A. Run CREATE USER ... FROM EXTERNAL PROVIDER on each database.
- B. Create a Conditional Access policy.
- C. Enable Microsoft Entra-only authentication for Server1.
- D. Assign the SQL Server Contributor role to Server1.

Answer: C

Explanation:

Microsoft Entra-only authentication at the logical server level disables SQL authentication for all databases on that server while leaving existing SQL principals in place. That matches the requirement to deny SQL authentication without removing legacy logins. Creating external-provider users adds Entra users; it does not block SQL logins. Conditional Access can govern Entra sign-ins but cannot disable SQL authentication. SQL Server Contributor is an Azure management role, not

an authentication mode. The exam objective emphasizes practical identity enforcement rather than cosmetic configuration. A valid answer must identify who authenticates, what permission is granted, where the scope is applied, and whether the method continues to work without passwords or secrets. That is why the selected answer is preferred over broader administrative roles or unrelated access settings. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Azure SQL platform security; Microsoft Learn > Microsoft Entra-only authentication.

NEW QUESTION 31

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 cluster1.

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 cluster1.

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 36

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 40

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 44

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

- A. C. Expire eligible assignments after
- E. Expire active 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 45

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The SC-500 Practice Test Here](#)