

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.

Methods

Answer Area

Hardware OATH tokens

Microsoft Authenticator

SMS

Temporary Access Pass

Voice call

Passwordless sign-in:

First-time sign-in for new users:

- 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 named Sub1 that contains a virtual network named VNet1.

VNet1 contains multiple virtual machines, including two virtual machines named VM1 and VM2.

Sub1 is linked to a Microsoft Entra tenant named contoso.com.

A partner company has an Azure subscription named Sub2 that contains a virtual network named VNet2. VNet2 contains a virtual machine named VM3.

Sub2 is linked to a Microsoft Entra tenant named fabrikam.com.

VM1 and VM2 contain data used by an application that runs on VM3.

You need to ensure that VM3 can access VM1 and VM2. The solution must deny VM3 access to any other resources in Sub1.

What should you configure on each virtual network? To answer, drag the components to the correct virtual networks. Each component 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.

Components

An Azure Private Link service

An Azure VPN gateway

A private endpoint

A service endpoint

VNet peering

Answer Area

VNet1:

VNet2:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

VNet1: An Azure Private Link service; VNet2: A private endpoint
Private Link service and private endpoint provide one-way, explicitly scoped private connectivity. VNet1 hosts the target VMs and should expose only the intended service through an Azure Private Link service. VNet2, where VM3 runs, consumes that service through a private endpoint. VNet peering or VPN would create broader network reachability between the networks and would not inherently deny VM3 access to other resources in Sub1. 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 > Private Link services and private endpoints; Microsoft Learn > Azure Private Link architecture.

NEW QUESTION 4

You have an Azure virtual network named VNet1 that contains three subnets named Subnet1, Subnet2 and Subnet3. A single network security group (NSG) named NSG1 is associated with all the subnets. You have the following virtual machines:

- VM1 on Subnet1
- VM2 on Subnet2
- VM3 on Subnet3

You create two application security groups named ASG1 and ASG2. VM2 is a member of ASG1, and VM3 is a member of ASG2.
You need to ensure that only VM2 can connect to VM3. The solution must continue to work if the private IP address of VM2 changes.
How should you configure the inbound rule on NSG1 ? To answer, drag the settings to the correct configurations. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Settings

ASG1

ASG2

IP address of VM1

IP address of VM2

IP address of VM3

VirtualNetwork

Answer Area

Source:

Destination:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Source: ASG1; Destination: ASG2

The requirement is identity-stable network filtering between virtual machines even if VM2 receives a different private IP address. Application security groups solve exactly that problem: rules refer to VM membership instead of a fixed IP. Because VM2 is a member of ASG1 and VM3 is a member of ASG2, the inbound allow rule on the shared NSG must use ASG1 as source and ASG2 as destination. Choosing IP addresses would fail the change-resilience requirement. The important exam skill is separating data-plane access, management-plane administration, and network reachability. A storage, database, or firewall setting must be selected because it enforces the exact path requested in the scenario. Distractors often look plausible because they improve security generally, but they do not satisfy the protocol, scope, or automation requirement stated in the question. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > NSGs and ASGs; Microsoft Learn > Application security groups in network security rules.

NEW QUESTION 5

You have an Azure virtual network named VNet1 that contains an Azure Bastion Subnet. VNet1 contains a subnet named Subnet1 Subnet1 contains multiple virtual machines.

You plan to deploy Azure Bastion to provide secure RDP access to the virtual machines on Subnet1. You associate a network security group (NSG) named NSG1 to Azure Bastion Subnet.

You need to configure rules for NSG1. The solution must meet the following requirements:

- Allow required inbound access to Azure Bastion from the internet.
- Allow user access to the virtual machines by using Azure Bastion.

Which TCP ports should you allow for the NSG1 rules? To answer, drag the appropriate ports to the correct rules. Each port 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.

TCP Ports	Answer Area
21	Inbound from the internet:
22	
389	Outbound to Subnet1:
443	
3389	
8080	

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Inbound from the internet: 443; Outbound to Subnet1: 3389

Azure Bastion requires inbound HTTPS access on TCP 443 from the internet to the AzureBastionSubnet so users can reach the Bastion service. For RDP to Windows virtual machines, Bastion then needs outbound access to the target subnet on TCP 3389. Port 22 would be required for SSH, but the scenario is specifically secure RDP. Other listed ports do not satisfy Bastion RDP access requirements. 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 Bastion; Microsoft Learn > Azure Bastion NSG access and port requirements.

NEW QUESTION 6

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft Sentinel workspace

You have a multi-tier Security Operations Center (SOC) team.

You need to ensure that all new security incidents are assigned immediately to the Tier 1 analysts group and flagged for triage.

Solution: You create 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 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 hunting query.

Does this meet the goal??

- A. Yes
- B. No

Answer: B

Explanation:

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

NEW QUESTION 8

You need to configure Server1 to meet the technical requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Install on Server1:

The Azure Connected Machine agent

The Azure Connected Machine agent

The Azure Monitor agent

The Azure Connected Cluster agent

The Dependency agent

Deploy to Sub1:

A Log Analytics workspace

A Log Analytics workspace

A Recovery Services vault

An Azure Automation account

An Azure Arc resource bridge

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Install on Server1: The Azure Connected Machine agent; Deploy to Sub1: A Log Analytics workspace

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

required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Azure Arc and Sentinel data collection; Microsoft Learn > Connected Machine agent and Log Analytics workspace.

NEW QUESTION 9

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 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 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 10

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 14

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 16

You have an Azure subscription named Sub1. Sub1 contains 20 virtual machines that run Windows Server.

Sub1 has the Microsoft Defender for Cloud Defender Cloud Security Posture Management (CSPM) plan enabled.

You need to ensure that all the virtual machines are scanned automatically for known security flaws and misconfigurations.

What should you use?

- A. Attack path analysis
- B. Microsoft Cloud Security Benchmark (MCSB)
- C. Cloud security explorer
- D. Just-in-time (JIT) VM access
- E. Vulnerability assessment on the virtual machines

Answer: E

Explanation:

Vulnerability assessment on virtual machines is the feature that scans machines for known security flaws and misconfigurations. Attack path analysis correlates risk paths after findings exist; it is not the scanner itself. Cloud Security Explorer is an investigation query experience, and MCSB is a security benchmark framework. JIT VM access limits management exposure, not vulnerability discovery. The VM vulnerability assessment capability satisfies the automated scanning requirement. The compute domain tests whether protection is applied before deployment, during runtime, or through posture assessment. The selected answer matches the phase described in the requirement. Detection-only tools are not acceptable when the requirement says prevent, and local installation methods are inferior when Defender for Cloud, Azure Policy, or Azure Machine Configuration can enforce the control centrally. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Defender for Servers settings; Microsoft Learn > vulnerability assessment for machines.

NEW QUESTION 20

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		Answer Area
⋮ Apply a label to the assets.		Inventory cleanup:
⋮ Set the asset state to Dependency.		Finding suppression:
⋮ 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.	●	

- 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 22

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 25

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have an Azure subscription that contains two virtual machines named VM1 and VM2. Each virtual machine has system-assigned managed identity enabled.

You have an Azure Storage account named storage. Public access from all networks is enabled for storage1.

You need to ensure that VM1 and VM2 can access storage1.

Solution: You create a private endpoint on storage1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

A private endpoint changes network routing so clients reach the storage account over a private IP address, but it does not grant data-plane authorization. The scenario already allows public network access, so network reachability is not the missing component. VM1 and VM2 still need Azure RBAC assignments for their managed identities or another valid authentication path. Therefore, a private endpoint alone does not meet the goal. For this domain, least privilege means granting only the required data operation or allowing only the required network flow. The correct response avoids shared keys, broad peering, general contributor roles, or log-only controls when the scenario demands prevention, routing, event triggering, or account-specific configuration. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > private endpoints and storage access; Microsoft Learn > private endpoints provide network access, not authorization.

NEW QUESTION 29

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 33

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 38

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 43

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 46

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 50

You have a Microsoft Sentinel workspace named Workspace1

You have 100 on-premises servers that run Linux and have the Azure Monitor Agent installed.

You need to collect Syslog events from the Linux servers. The solution must meet the following requirements:

- Ensure that filtering occurs before data is written to Workspace1
- Reduce ingestion costs by excluding low value Syslog messages.

What should you include in the solution?

A. An Advanced Security Information Model (ASIM) parser

B. A data collection rule (DCR)

C. An analytics rule

D. A table-level filter and split transformation

Answer: B

Explanation:

Filtering must happen before data is written to the Log Analytics workspace. With Azure Monitor Agent, Syslog collection is governed by data collection rules, and DCR transformations or filtering can reduce ingestion before records reach the workspace. An ASIM parser normalizes queried data after ingestion, an analytics rule detects conditions after data exists, and a table-level transformation is not the primary collection control for Linux Syslog from AMA in this scenario. The posture and monitoring objective focuses on turning security data into usable operational outcomes. The correct answer either collects the right signal, grants the right security-operations role, or automates incident handling at the correct layer. Distractors often provide dashboards, queries, or broad permissions, but those do not create the requested workflow or least-privilege security capability. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Syslog event collection; Microsoft Learn > data collection rules for Azure Monitor Agent.

NEW QUESTION 54

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.

Answer Area

Exposed ports on the public IP address of CG1:

▼

443 and 5000
443 only
5000 only

Network endpoint for App1:

▼

cg1.contoso.com:443
cg1.contoso.com:5000
localhost:443
localhost:5000

- 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 59

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 62

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?

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

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 64

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 66

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 68

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 73

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 78

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 82

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 85

You have an Azure subscription named Sub1 that contains an Azure Database for PostgreSQL instance Sub1 has Microsoft Defender for Cloud enabled. You need to configure Microsoft Defender for Databases to minimize costs. Which Defender plan should you enable?

- A. Microsoft Defender for Servers
- B. Microsoft Defender for Open-Source Relational Databases
- C. Microsoft Defender for SQL Servers on Machines
- D. Microsoft Defender for Azure SQL Databases
- E. Microsoft Defender for Storage

Answer: B

Explanation:

The protected resource is Azure Database for PostgreSQL, which is an open-source relational database service. Microsoft Defender for Open-Source Relational Databases is scoped to PostgreSQL and MySQL style services, so it satisfies the requirement without enabling broader plans. Defender for Azure SQL Databases applies to Azure SQL, Defender for SQL Servers on Machines applies to SQL Server on VMs or Arc-enabled machines, and Defender for Servers or Storage would charge for unrelated workloads. 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 Databases; Microsoft Learn > Defender for open-source relational databases.

NEW QUESTION 87

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 90

You have an Azure Storage account named storage1 that contains Azure Files shares. You have an application named App1 that uses a system-assigned managed identity to access the shares. Administrators access the shares by using storage account keys. You need to ensure that App1 access the shares without using the storage account keys. What should you do on storage1?

- A. Store the storage account access keys in Azure Key Vault and regenerate them periodically.
- B. Set Allow storage account key access to Disabled.
- C. Select Default to Microsoft Entra authorization in the Azure portal.
- D. Assign the Storage File Data Privileged Reader role to the managed identity of App1.

Answer: D

Explanation:

Assigning the Storage File Data Privileged Reader role to App1's managed identity grants Microsoft Entra ID-based read access to files and directories in Azure Files, overriding existing ACL restrictions where necessary. This allows the application to authenticate by using its managed identity instead of storage account keys.

Reference:

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-assign-share-level-permissions?tabs=azure-portal>

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

NEW QUESTION 93

.....

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](#)