Exam Questions SC-500

Microsoft Certified: Cloud and AI Security Engineer Associate

https://www.2passeasy.com/dumps/SC-500/

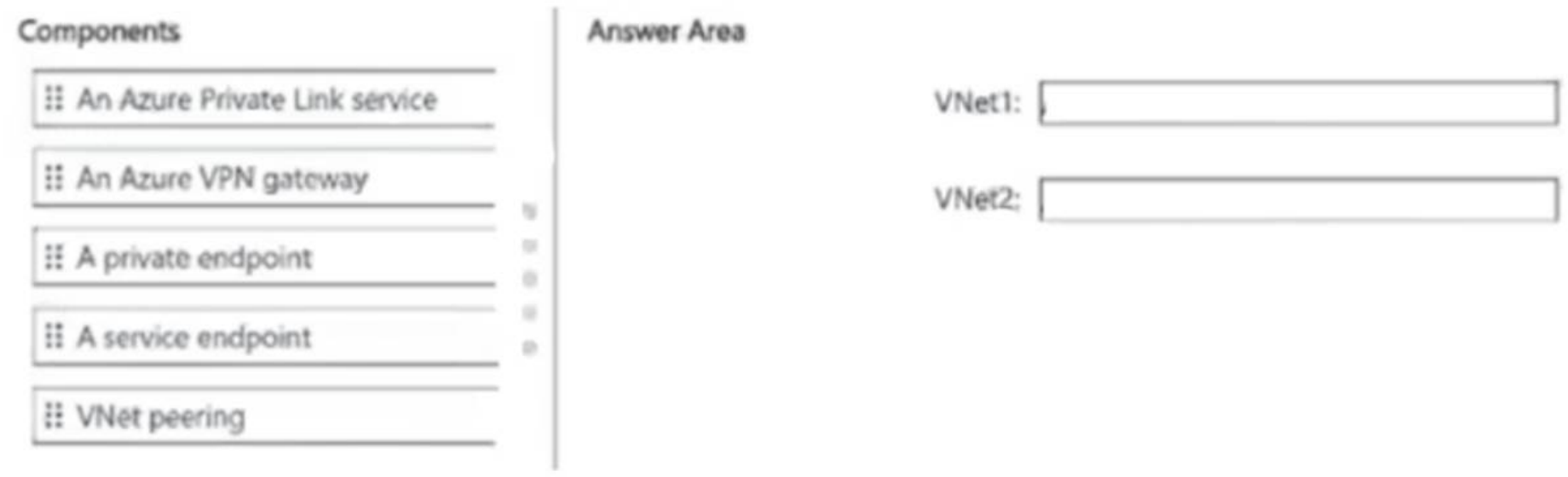
NEW QUESTION 1
You have a Microsoft Entra tenant that has user consent for applications disabled.
You register an application named App1 that requests the following Microsoft Graph delegated permissions:
•user.Read
•Mail.Read
You need to configure tenant permissions to meet the following requirements:
•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 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.



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.

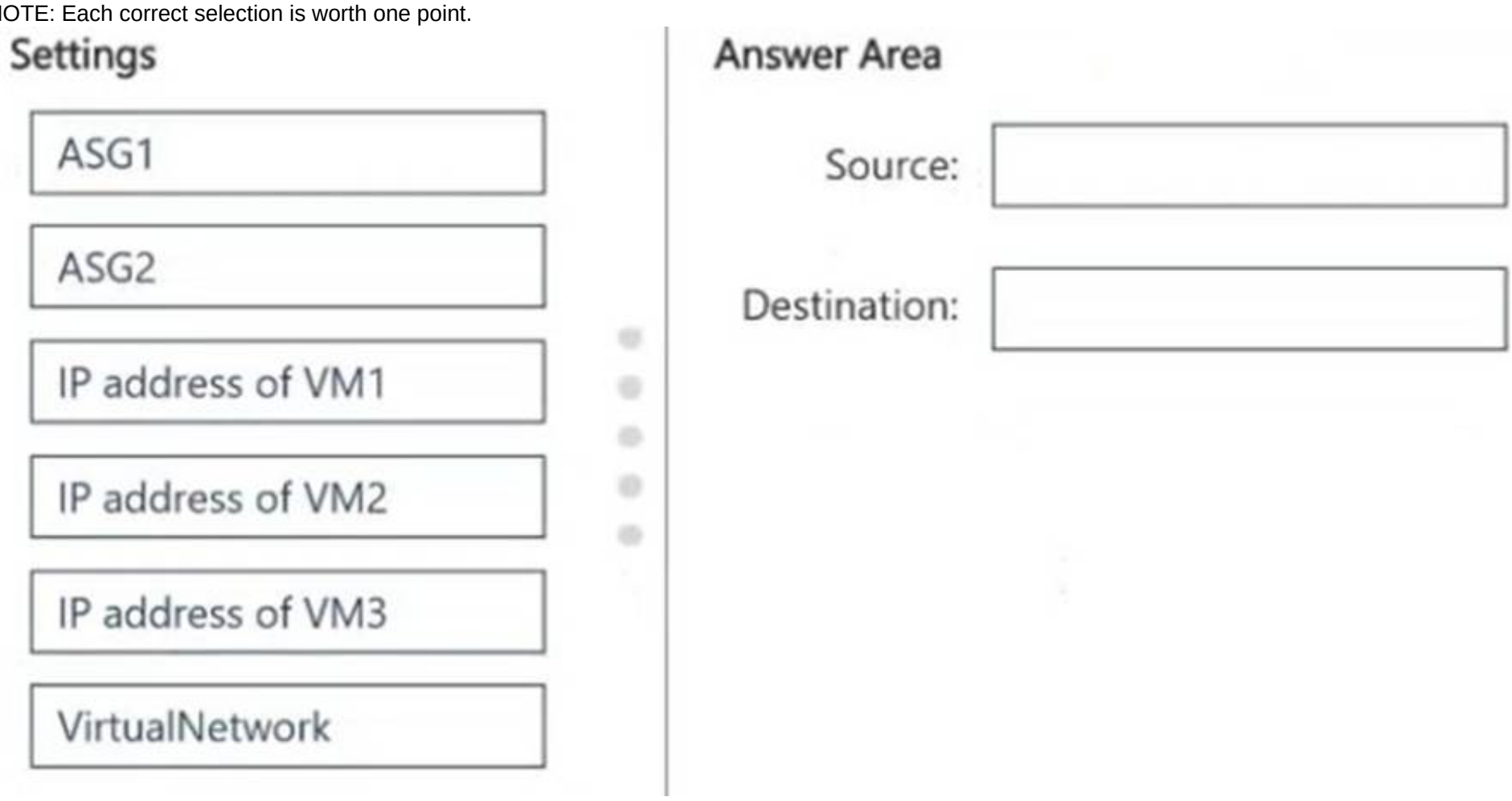
NEW QUESTION 3
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You have an Amazon Web Services (AWS) account connected to Defender for Cloud that has the Defender Cloud Security Posture Management (CSPM) plan enabled.
You need to identify the potential impact of security incidents that exploit multiple risks reported by Defender CSPM.
What should you use?

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

Answer: D

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

NEW QUESTION 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.



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
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.

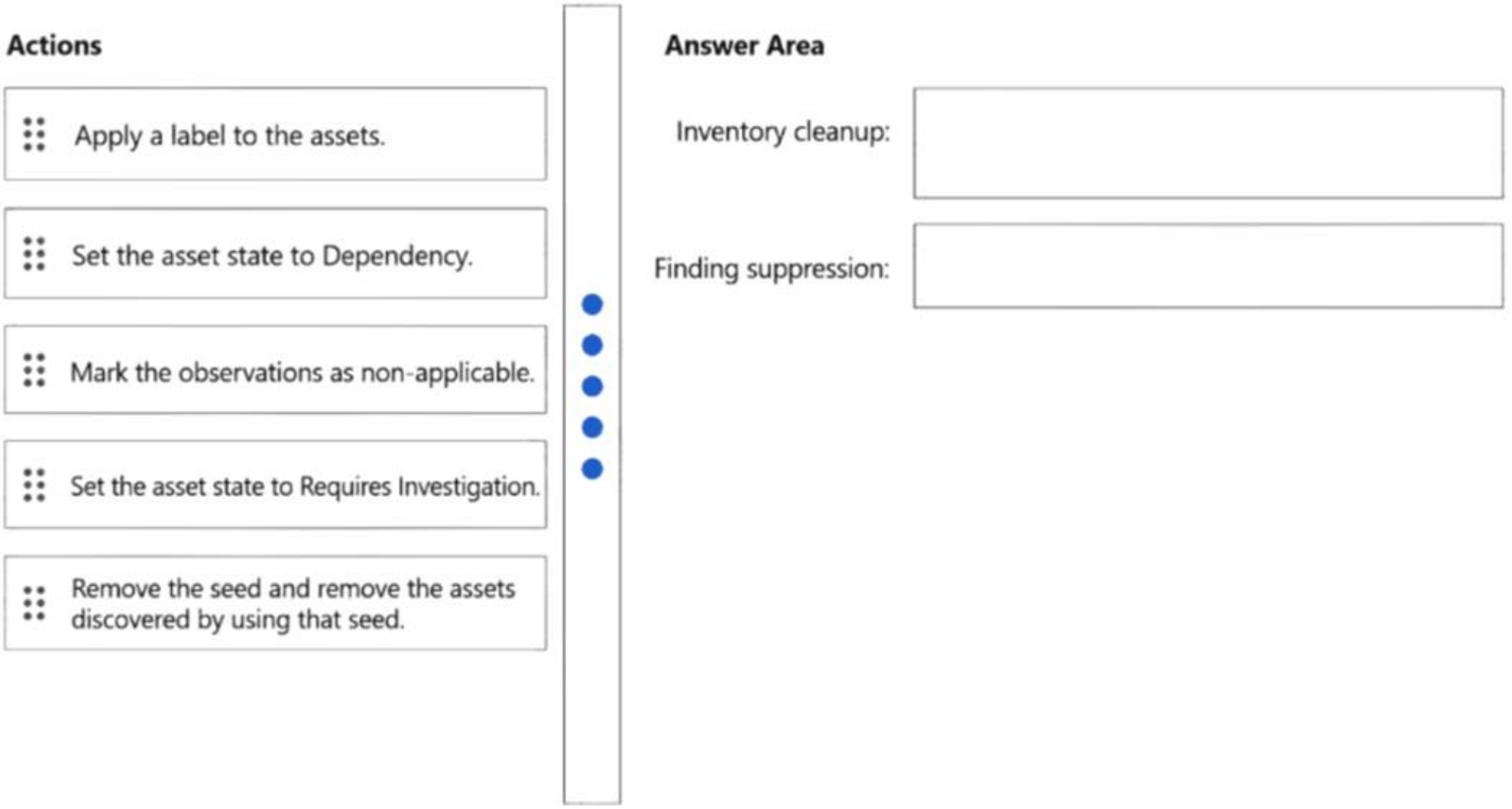
You need to ensure that all new security incidents are assigned immediately to the Tier 1 analysts group and flagged for triage.
Solution You create a hunting query.
Does this meet the goal??

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 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.



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

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

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

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

Answer: C

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

NEW QUESTION 8
Overview - Fabrikam, Inc. is a consulting company. The company has a main office in New York City and branch offices in Amsterdam and Singapore. Existing Environment. Network environment The on-premises network contains a datacenter in each office. Existing Environment. Cloud environment Fabrikam has two Azure subscriptions named Sub1 and Sub2 and a Microsoft 365 subscription that includes Microsoft 365 E5 licenses. All the subscriptions are linked to a Microsoft Entra tenant named fabrikam.com that contains the identities shown in the following table.

Name	Type	Microsoft Entra role	Azure role assignment for Sub1
Admin1	User	Privileged Authentication Administrator	Resource Policy Contributor
Admin2	User	Compliance Administrator	User Access Administrator
Admin3	User	Authentication Administrator	Contributor
Admin4	User	Global Administrator	*None*
User1	User	*None*	Reader
AKS1	System-assigned managed identity	*None*	*None*
ID1	User-assigned managed identity	*None*	*None*

The tenant contains the groups shown in the following table.

Name	Type	Role assignments allowed
Group1	Security	Yes
Group2	Security	No
Group3	Microsoft 365	Yes
Group4	Microsoft 365	No

All devices are enrolled in Microsoft Intune. Existing Environment. Sub1 Resources Sub1 contains a resource group named RG1 that contains the resources shown in the following table.

Name	Description	Location
SQLServer1	Azure SQL Database logical server	East US
SQLdb1	Database on SQLServer1	East US
VM1	Virtual machine	East US
AKS1	Azure Kubernetes Service (AKS) cluster	East US
Registry1	Azure container registry	East US
storage1	Storage account	East US
AKV1	Azure key vault	East US

SQLServer1 uses Microsoft SQL Server authentication. Sub1 has an Azure Web Application Firewall (WAF) named WAF1 that has the following types of rule sets: - Bot Manager 1.1 - Azure-managed Default Rule Set (DRS) Sub1 has the following compliance standards assigned in Microsoft Defender for Cloud: - NIST SP 800-53 Rev. 4 - Microsoft cloud security benchmark (MCSB) - System and Organization Controls (SOC) 2 Type 2 Existing Environment. Sub2 Resources Sub2 contains a resource group named RG2. Planned Changes and Requirements. Planned Changes Fabrikam plans to implement the following changes: - Deploy the following key vaults to RG1: * AKV2 in the West Europe Azure region * AKV3 in the Central US Azure region * AKV4 in the East US Azure region - Deploy the following key vaults to RG2: * AKV5 in the East US region - Configure VM1 to read data from storage1. - Create function apps that have the following hosting plans: * Fa1: Flex Consumption hosting plan * Fa2: Consumption hosting plan * Fa3: Dedicated hosting plan - For WAF1, implement rate limiting rules based on the request location. - Enable the NIST SP 800-53 Rev. 5 compliance standard in Defender for Cloud. - Create a new storage account named storage2 that supports Azure Table storage. - Enforce multifactor authentication (MFA) when database administrators access SQLdb1. - Implement ExpressRoute circuits to the

on-premises network as shown in the following table.

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

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

A. Fa1 and Fa2 only
B. Fa2 and Fa3 only
C. Fa1 and Fa3 only
D. Fa1, Fa2, and Fa3

Answer: C

Explanation:
The correct implementation includes Fa1 and Fa3 only according to the visible answer area. In Azure Functions security scenarios, apps are included only when their hosting, authentication, identity, or network configuration matches the stated technical controls. Including Fa2 would apply the implementation to an app that does not meet those requirements. The selected set therefore narrows the change to the function apps that require the security implementation. For SC-500, compute controls are evaluated by workload type: VM, Arc server, AKS, container registry, container group, Functions, Logic Apps, App Service, and AI agent runtime. The right answer uses the Microsoft control that is native to that workload. Broad Azure roles or unrelated monitoring services would either overgrant access or fail to enforce the required security state. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Azure Functions security controls; Microsoft Learn > App Service/Functions authentication and network security.

NEW QUESTION 9
You have an Azure subscription named Sub1 that contains multiple virtual machines. Sub1 has the Microsoft Defender Cloud Security Posture Management (CSPM) plan enabled.
You discover that Defender for Cloud falls to identify plaintext connection strings and SSH keys stored on the virtual machines.
You need to ensure that secrets can be identified on the virtual machines.
What should you do?

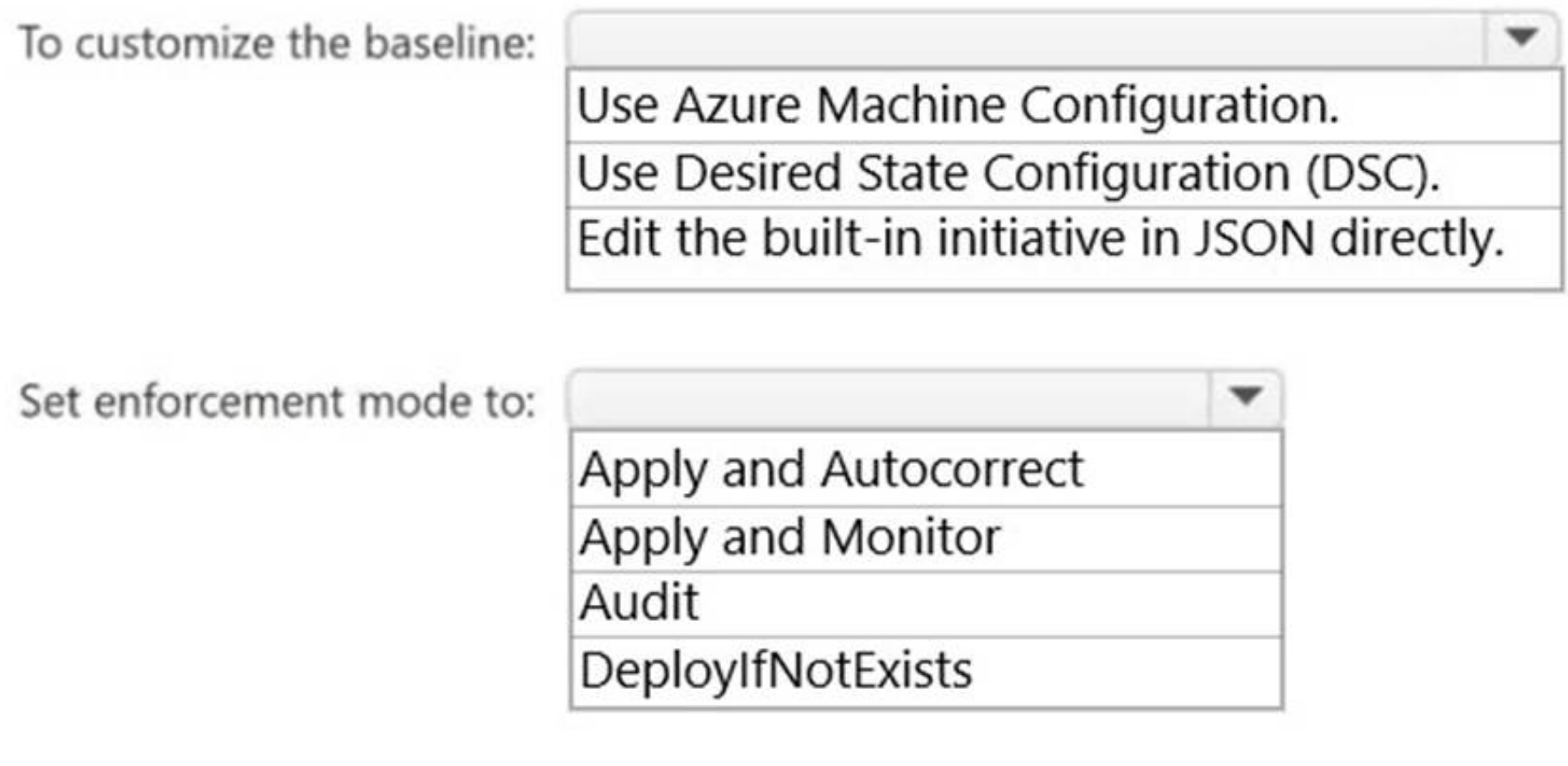
A. Configure the Defender for Cloud data connector in Microsoft Sentinel.
B. Enable agentless machine scanning.
C. Deploy the Azure Monitor Agent to all the virtual machines.
D. Enable Microsoft Defender for Key Vault.

Answer: B

Explanation:
Defender CSPM identifies secrets such as plaintext connection strings and SSH keys on machines through agentless machine scanning. If those secrets are not being identified, the missing capability is the agentless scan feature. The Sentinel data connector only forwards alerts and posture data, the Azure Monitor Agent collects telemetry, and Defender for Key Vault protects vault access; none of those scan VM disks for exposed secrets. The posture and monitoring objective focuses on turning security data into usable operational outcomes. The correct answer either collects the right signal, grants the right security-operations role, or automates incident handling at the correct layer. Distractors often provide dashboards, queries, or broad permissions, but those do not create the requested workflow or least-privilege security capability. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > scan for secrets by Defender CSPM; Microsoft Learn > agentless scanning for machines.

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

Answer Area



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 10
You have Microsoft Security Copilot agents that authenticate by using Microsoft Entra service principals.
You receive a Microsoft Defender alert triggered by the anomalous OAuth authentication of an agent ' s Microsoft Entra service principal.
You need to assess the impact of the agent identity and identify which resources are affected if the identity is abused for lateral movement The solution must minimize administrative effort.
What should you do?

A. From Advanced hunting, create a query against the IdentityLogonEvents table to list all the sign-ins performed by the identity.
B. From Attack paths, select the identity and view the blast radius.
C. From AI Observability in Microsoft Purview Data Security Posture Management (DSPM), review the agent activity.
D. From Microsoft Purview Audit, query the audit logs for all the role assignments granted to the identity.
E. From Incidents, review incidents related to OAuth events reported by Microsoft Defender for Cloud Apps.

Answer: B

Explanation:
The security team needs impact and lateral-movement exposure for an abused service principal. Defender XDR attack paths show the identity blast radius by connecting permissions, exposed resources, and reachable assets. Advanced hunting and audit logs can provide raw evidence, but they require more manual analysis. AI Observability and incident review do not directly answer which resources are affected by identity abuse across the environment. 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 > analyze blast radius by using Defender XDR; Microsoft Learn > attack paths for identity risk.

NEW QUESTION 11
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?

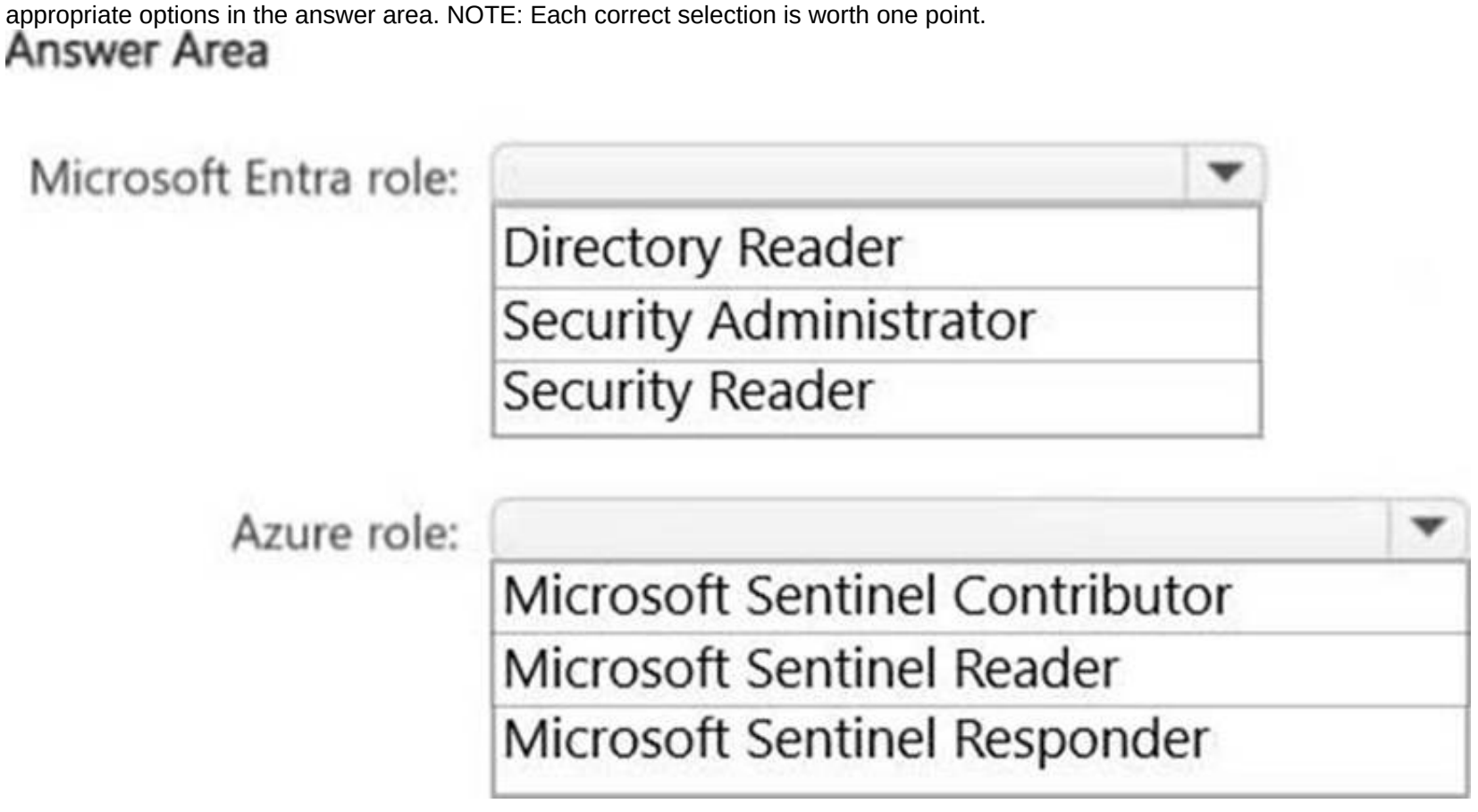
A. An Advanced Security Information Model (ASIM) parser

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 16
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.



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 19
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 23
You have an Azure subscription named Sub1 that contains an Azure Kubernetes Service (AKS) cluster named cluster1 and an Azure container registry named ACR1 Sub1 has Microsoft Defender for Containers enabled, and runtime protection is active on cluster!
The developers at your company deploy pods that have elevated privileges, and the deployments are created in cluster1
You need to prevent pods with elevated privileges from being accepted by cluster!
What should you do?

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

Answer: A

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

NEW QUESTION 24
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 25
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 28
You are configuring a new Microsoft Sentinel workspace named Workspace1. You have an external IT Service Management (ITSM) system that is NOT supported by any Microsoft Sentinel solutions in Azure Marketplace. You need to ensure that Workspace1 creates service tickets in the ITSM system for all new security incidents. What should you create?
A.a playbook

D.an analytics rule
A. C.a watchlist

Answer: A

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

NEW QUESTION 31
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SC-500 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SC-500 Product From:

https://www.2passeasy.com/dumps/SC-500/

Money Back Guarantee

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