



Microsoft

Exam Questions SC-500

Microsoft Certified: Cloud and AI Security Engineer Associate

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

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 2

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 3

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 4

For each of the following statements, select Yes if the statement is true Otherwise, select No.

Answer Area

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Yes; 2) No; 3) Yes
The visible PIM settings indicate that Admin1 must approve Agent ID Developer activations, Admin2 is not an approver for the AI Administrator role, and Admin3 can assign User1 a two-day active assignment for Agent ID Developer. The controlling factors are the configured approver list and active assignment duration policy for each role. PIM evaluates those settings per role, so approval authority or duration for one role cannot be assumed for another role. For SC-500, the decisive distinction is whether the control authenticates an identity, grants authorization, or merely changes configuration visibility. The incorrect choices generally either grant excessive privilege, change the application model, or operate at the wrong scope. Microsoft expects the least-privilege identity path that satisfies the

scenario without introducing shared secrets or unnecessary tenant-wide rights. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > PIM role settings and Agent ID governance; Microsoft Learn > approvers and maximum activation duration.

NEW QUESTION 5

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 6

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 7

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 8

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 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 SQL Database logical server named Server1 that contains a database named DB1.

You need to configure authentication for Server1 to meet the following requirements;

- SQL authentication cannot be used for any databases on Server1.
- The solution must be enforced centrally at the server level.

What should you do?

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

Answer: C

Explanation:

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

NEW QUESTION 10

You have a Microsoft Sentinel workspace

You need to collect Windows security events from 200 Azure virtual machines that run Windows Server. The solution must meet the following requirements:

- Use direct agent based data collection from each virtual machine.
- Use a supported agent for new virtual machine deployments

Which Microsoft Sentinel connector should you use?

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

Answer: B

Explanation:

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

NEW QUESTION 13

You have a Microsoft 365 subscription. All users have Microsoft Exchange Online mailboxes.

You use Microsoft Entra Agent ID to register and manage AI agents.

The developers at your company create the following two agents:

- Agent 1: An interactive agent that helps users summarize their own Exchange Online email
- Agent2: An autonomous agent that sends nightly updates to a Microsoft Teams channel

You need to grant each agent access to Microsoft Graph. The solution must minimize the access scope, while meeting each agent 's operating model.

Which type of permission should you assign to each agent? To answer, drag the appropriate permission types to the correct agents. Each permission type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Permission types

Application permissions

Delegated permissions

Exchange Online permissions

Resource-specific consent (RSC) permissions for Teams

Answer Area

Agent1:

Agent2:

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Agent1: Delegated permissions;

Agent2: Application permissions

Agent1 is interactive and acts for a signed-in user against that user's mailbox, so delegated permissions are appropriate. Agent2 operates autonomously without a signed-in user; application permissions are the app-only model for Microsoft Graph access in that operating mode. Exchange Online permissions and Teams RSC can be valid in narrow service-specific designs, but the answer area asks for the general permission type aligned to interactive versus autonomous agents. The exam objective emphasizes practical identity enforcement rather than cosmetic configuration. A valid answer must identify who authenticates, what permission is granted, where the scope is applied, and whether the method continues to work without passwords or secrets. That is why the selected answer is preferred over broader administrative roles or unrelated access settings. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Manage Entra Agent ID access; Microsoft Learn > delegated vs application permissions.

NEW QUESTION 16

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 21

You have a Microsoft Entra tenant that has the following configurations:

- User consent for applications is disabled.
 - Only administrators can grant permissions to applications.
- You register an application named App1 that uses delegated Microsoft Graph permissions.

You need to configure App1 to meet the following requirements:

- Enable user sign-ins without interactive consent prompts.
- Enable App1 to access Microsoft Graph on behalf of the signed-in user.

What should you do?

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

Answer: D

Explanation:

Delegated Microsoft Graph permissions allow an application to act on behalf of the signed-in user. Because user consent is disabled and only administrators may grant permissions, users cannot complete the consent prompt themselves. Granting admin consent for the required delegated permissions pre-authorizes the app and removes the interactive consent prompt while still preserving the delegated model. Switching to application permissions would change the operating model and grant app-only access. For SC-500, the decisive distinction is whether the control authenticates an identity, grants authorization, or merely changes

configuration visibility. The incorrect choices generally either grant excessive privilege, change the application model, or operate at the wrong scope. Microsoft expects the least-privilege identity path that satisfies the scenario without introducing shared secrets or unnecessary tenant-wide rights. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > OAuth permission grants and consent; Microsoft Learn > admin consent for delegated permissions.

NEW QUESTION 25

You have three internet-facing Azure App Service web apps named App1, App2, and App1. Each app uses built-in authentication. App2 hosts a backend API.

Some corporate users can sign in to App2, even though they should NOT be able to use the API.

You need to restrict App2 access to assigned Microsoft Entra users and groups.

What should you configure for App2? To answer, drag the appropriate configurations to the correct methods. Each configuration 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.

Configurations	Answer Area
☐ Enterprise app assignment required	Authentication method:
☐ IP access restrictions	Access control method:
☐ Local authentication	
☐ The Microsoft identity provider	
☐ A role-based access control (RBAC) assignment	
☐ Tenant-wide admin consent	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Authentication method: The Microsoft identity provider;

Access control method: Enterprise app assignment required

Built-in authentication for App Service should use the Microsoft identity provider for Microsoft Entra sign-in. To restrict access to selected users and groups, require enterprise app assignment on the corresponding enterprise application. IP restrictions only filter network source and cannot identify assigned corporate users.

Local authentication and broad admin consent do not implement assigned-user enforcement for the backend API. 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 Service authentication; Microsoft Learn > App Service built-in authentication and enterprise app assignment.

NEW QUESTION 26

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 29

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 31

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 33

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 37

Which Azure Functions configuration limits the function app to accept requests only from a specific virtual network?

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

Answer: A

Explanation:

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

NEW QUESTION 40

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

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

Answer: A

Explanation:

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

NEW QUESTION 44

You have a Microsoft Entra tenant that uses Privileged Identity Management (PIM). You need to modify the AI Administrator role settings to meet the following requirements: - Elevated access must be evaluated by another administrator before it is granted. - Privileged access must be removed automatically after a fixed period. Which two settings should you configure? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A.Require justification on activation

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

Answer: BD

Explanation:

Requiring approval to activate ensures that a designated administrator must evaluate and approve an eligible user's elevation request before privileged access is granted. Setting an activation maximum duration makes each activated role assignment time-bound, automatically removing the elevated access when the configured activation period expires.

Reference:

<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-change-default-settings>

<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-activate-role>

NEW QUESTION 45

An AI development team stores secrets, API keys, and connection strings within application configuration files. A security review recommends a more secure approach. What should the team implement?

- A. B.Azure Key Vault
- C.Azure Advisor
- D.Azure Resource Graph

Answer: B

NEW QUESTION 46

.....

Relate Links

100% Pass Your SC-500 Exam with ExamBible Prep Materials

<https://www.exambible.com/SC-500-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>