

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.

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	Passwordless sign-in:	
Microsoft Authenticator	First-time sign-in for new users:	
SMS		
Temporary Access Pass		
Voice call		

- 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 an Azure subscription named Sub1 that contains a storage account named storage1

Sub1 has Microsoft Defender for Storage enabled. Defender for Storage has on-upload malware scanning enabled.

The security team at your company requires that all malicious files be processed automatically by a serverless workflow for quarantine and notification.

You need to ensure that the malware scan results trigger an automated response. The solution must minimize operational effort.

What should you configure?

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

Answer: A

Explanation:

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

NEW QUESTION 3

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 4

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 5

You have an Azure key vault named KV1 that uses role-based access control (RBAC) for data plane authorization.

You have a user named User1 and an Azure App Service web app named App1 that has a system-assigned managed identity.

You need to configure authorization to meet the following requirements:

- App1 must be able to retrieve secrets from KV1.
- User1 must manage the KV1 settings without accessing secret values.

The solution must follow the principle of least privilege.

Which role should you assign to each identity for KV1? To answer, drag the appropriate roles to the correct identities. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Roles

Key Vault Administrator
Key Vault Contributor
Key Vault Secrets Officer
Key Vault Secrets User

Answer Area

User1:	
App1:	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

User1: Key Vault Contributor;

App1: Key Vault Secrets User

Key Vault Contributor can manage vault settings but cannot read secret values, so it fits User1. Key Vault Secrets User permits reading secret contents without granting vault administration, so it fits App1. Key Vault Administrator and Key Vault Secrets Officer are too broad because they allow broader secret or vault

administration. This split enforces RBAC separation between management-plane administration and data-plane secret retrieval. This domain is tested through precise scope control: tenant, subscription, resource, application, and data-plane authorization are not interchangeable. The correct choice applies the smallest identity or governance control that enforces the stated requirement. Options that only add users, create registrations, or provide broad administrator access fail because they do not directly enforce the requested access behavior. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Key Vault access; Microsoft Learn > Key Vault RBAC built-in roles.

NEW QUESTION 6

You have an Azure subscription that contains a user named User1 and an Azure Container Registry named ContReg1.

You enable content trust for ContReg1.

You need to ensure that User1 can create trusted images in ContReg1. The solution must use the principle of least privilege.

Which two roles should you assign to User1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. AcrQuarantineWriter
- B. Contributor
- C. AcrQuarantineReader
- D. AcrPush
- E. AcrImageSigner

Answer: DE

Explanation:

To create trusted images, the user must be able to push images and sign them. AcrPush allows pushing image content to the registry, while AcrImageSigner allows signing trusted images. Contributor would be excessive because it grants broad management rights. Quarantine reader/writer roles relate to quarantine workflows, not content trust signing. The combination of AcrPush and AcrImageSigner matches least privilege for trusted image creation. 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 Container Registry security; Microsoft Learn > ACR roles for push and image signing.

NEW QUESTION 7

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 8

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

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

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

You need to implement the planned change for 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 9

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 10

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

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

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

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

NOTE: Each correct selection is worth one point.

Actions

⋮ Apply a label to the assets.

⋮ Set the asset state to Dependency.

⋮ Mark the observations as non-applicable.

⋮ Set the asset state to Requires Investigation.

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

Answer Area

Inventory cleanup:

Finding suppression:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Inventory cleanup: Remove the seed and remove the assets discovered by using that seed; Finding suppression: Mark the observations as non-applicable
When a seed domain is no longer owned, the clean inventory action is to remove the seed and remove assets discovered from that seed. Leaving those assets as dependencies or merely labeling them would keep stale assets in the inventory. For findings that do not apply to confirmed inventory, marking the observations as non-applicable prevents them from influencing finding counts while retaining the operational history needed for audit and review. For this domain, least privilege means granting only the required data operation or allowing only the required network flow. The correct response avoids shared keys, broad peering, general contributor roles, or log-only controls when the scenario demands prevention, routing, event triggering, or account-specific configuration. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Defender EASM; Microsoft Learn > inventory and observation state management.

NEW QUESTION 10

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 14

HOTSPOT - Overview - Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas. Contoso has a hybrid environment that contains on-premises servers connected to Azure, a Microsoft 365 E5 subscription, and an Azure subscription named Sub1. Existing Environment. Microsoft Entra tenant Contoso has a Microsoft Entra tenant named contoso.com that contains the users shown in the following table.

Name	Tier
DeviceInfo	Analytics
DnsEvents	Analytics

Requirements. Planned changes - Contoso plans to implement the following changes: Integrate AKS1 with Vault1. Enable Microsoft Entra Kerberos authentication for all supported storage. Configure auditing for sql1 by using the Azure portal and store audit logs in a centralized location. Requirements. Technical requirements Contoso identifies the following technical requirements: Protect Server1 by using file integrity monitoring. Protect AKS1 by using Microsoft Defender for Cloud. Configure Microsoft Sentinel to retain data for the maximum supported duration without changing the tier. Store objects used for authentication and encryption in

Vault1 and ensure that Vault1 regenerates the objects every 30 days, whenever possible.

User1 has requested to use the AI Administrator role.

Which approvers can approve the request, and how long will User1 be an AI administrator after the role is approved? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Eligible approvers:

Admin1 and Admin3 only	▼
Admin1 only	
Admin1 and Admin2 only	
Admin1 and Admin3 only	
Admin2 and Admin3 only	

Maximum active duration of the role:

1 day	▼
8 hours	
1 day	
2 days	
7 days	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Eligible approvers: Admin1 and Admin3 only; Maximum active duration of the role: 1 day

The answer area indicates that Admin1 and Admin3 are the eligible approvers and that the active AI Administrator role duration is one day. This is consistent with PIM role settings: approvers are explicitly configured for a role activation policy, and maximum active duration controls how long the activated role remains available. Other administrators who are not configured as approvers cannot approve the request merely because they hold unrelated roles. 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 > PIM activation approval and duration; Microsoft Learn > role settings in PIM.

NEW QUESTION 18

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 22

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 24

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 29

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 34

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 39

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 42

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 46

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 49

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 51

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 53

HOTSPOT

You have an Azure subscription named Sub1 that contains 50 virtual machines. Sub1 has Microsoft Defender for Cloud enabled.

Sub1 contains an Azure key vault named KV1 and an Azure policy that enforces storing all secrets in KV1.

Occasionally, the developers at your company store plaintext tokens and SSH private keys on the virtual machines.

You need to configure Defender for Cloud to detect plaintext secrets on the virtual machines. The solution must minimize administrative changes to the virtual machines.

How should you configure Defender for Cloud? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Plan to enable:

	▼
Defender Cloud Security Posture Management (CSPM)	
Microsoft Defender for Cloud Apps	
Microsoft Defender for Key Vault	

Feature to enable:

	▼
Agentless machine scanning	
Regulatory compliance	
Vulnerability assessment on the virtual machines	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Plan to enable: Defender Cloud Security Posture Management (CSPM)

Feature to enable: Agentless machine scanning

Defender CSPM supports agentless secrets scanning for Azure virtual machines. Enabling agentless machine scanning allows Defender for Cloud to analyze VM disk snapshots for exposed plaintext tokens and SSH private keys without requiring agents or configuration changes on the virtual machines.

Reference:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/secrets-scanning-servers> <https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-agentless-data-collection>

NEW QUESTION 55

For a site-to-site VPN connection to Azure, which protocol and configuration provide encrypted tunnels between on-premises and the Azure VPN gateway?

- A. Plain HTTP over a public IP
- B. FTP passive mode
- C. IPsec/IKE policy on the VPN gateway
- D. ICMP echo tunneling

Answer: C

Explanation:

Site-to-site VPNs to Azure use IPsec/IKE to establish encrypted tunnels between the on-premises VPN device and the Azure VPN gateway. Configuring a custom IPsec/IKE policy lets you enforce strong cipher suites and key exchange parameters.

NEW QUESTION 60

Which identity construct represents an AI agent in Microsoft Entra so you can apply Conditional Access and govern its access?

- A. Microsoft Entra Agent ID
- B. A shared mailbox
- C. A distribution group
- D. A guest user account

Answer: A

Explanation:

Microsoft Entra Agent ID gives AI agents their own first-class identity in Entra ID, enabling Conditional Access policies and access governance for agents. Treating agents as governed identities lets you control and audit what autonomous agents can access.

NEW QUESTION 62

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 64

You have an Azure management group named MG1 that contains two subscriptions named Sub1 and Sub2. Both subscriptions are linked to a Microsoft Entra tenant that contains a security group named Group1. You need to ensure that the members of Group1 can assign roles to the resources in Sub1 and Sub2. The solution must follow the principle of least privilege. Which role should you assign to Group1?

- A. Contributor at the MG1 scope
- B. Contributor at the Sub1 and Sub2 scopes
- C. User Access Administrator at the MG1 scopecorrect
- D. Owner at the MG1 scope

Answer: C

Explanation:

The User Access Administrator role permits members of Group1 to manage role assignments without granting them permission to modify the underlying Azure resources. Assigning the role at the MG1 scope causes the permission to be inherited by both Sub1 and Sub2 and their resources, providing centralized least-privilege access management.

Reference:

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

<https://learn.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin?tabs=azure-portal%2Centra-audit-logs>

<https://learn.microsoft.com/en-us/azure/role-based-access-control/scope-overview>

NEW QUESTION 65

You have an Azure Logic Apps Consumption workflow that uses a Request trigger. All supported authentication methods are enabled on the Request trigger. You need to ensure that the endpoint accepts only OAuth-based requests. The solution must minimize costs. What should you do?

- A. B.Use OAuth 2.0 authorization.
- C.Enable Secure Inputs and enable Secure Outputs for the Request trigger.
- D.Deploy Azure API Management.

Answer: A

NEW QUESTION 67

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 70

.....

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