

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 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 an Azure subscription named Sub1 that contains a virtual network named VNet1.

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

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

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

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

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

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

What should you configure on each virtual network? To answer, drag the components to the correct virtual networks. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Components	Answer Area
An Azure Private Link service	VNet1:
An Azure VPN gateway	VNet2:
A private endpoint	
A service endpoint	
VNet peering	

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

VNet1: An Azure Private Link service; VNet2: A private endpoint

Private Link service and private endpoint provide one-way, explicitly scoped private connectivity. VNet1 hosts the target VMs and should expose only the intended service through an Azure Private Link service. VNet2, where VM3 runs, consumes that service through a private endpoint. VNet peering or VPN would create broader network reachability between the networks and would not inherently deny VM3 access to other resources in Sub1. Microsoft platform security questions usually hinge on where enforcement occurs: at the resource, server, subnet, firewall policy, private endpoint, or subscription level. The selected answer uses the control plane that owns that enforcement point. Other options are rejected when they only log activity, broaden network access, or protect a different service category. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Private Link services and private endpoints; Microsoft Learn > Azure Private Link architecture.

NEW QUESTION 4

You have an Azure 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

Answer Area

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

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 5

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

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

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

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

Which TCP ports should you allow for the NSG1 rules? To answer, drag the appropriate ports to the correct rules. Each port may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

Azure Bastion requires inbound HTTPS access on TCP 443 from the internet to the AzureBastionSubnet so users can reach the Bastion service. For RDP to Windows virtual machines, Bastion then needs outbound access to the target subnet on TCP 3389. Port 22 would be required for SSH, but the scenario is specifically secure RDP. Other listed ports do not satisfy Bastion RDP access requirements. For this domain, least privilege means granting only the required data operation or allowing only the required network flow. The correct response avoids shared keys, broad peering, general contributor roles, or log-only controls when the scenario demands prevention, routing, event triggering, or account-specific configuration. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Azure Bastion; Microsoft Learn > Azure Bastion NSG access and port requirements.

NEW QUESTION 6

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

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

You have a Microsoft Sentinel workspace

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

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

Solution: You create an automation rule.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

An automation rule is the native Sentinel control for applying actions automatically when incidents are created or updated. It can assign incidents to users or groups, change status/severity, add tags, and run playbooks. This directly matches the requirement to assign all new incidents immediately and flag them for triage. It is more direct than hunting queries and is intended for incident-handling automation. The posture and monitoring objective focuses on turning security data into usable operational outcomes. The correct answer either collects the right signal, grants the right security-operations role, or automates incident handling at the correct layer. Distractors often provide dashboards, queries, or broad permissions, but those do not create the requested workflow or least-privilege security capability. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Sentinel automation rules; Microsoft Learn > automation rule actions for incident assignment.

NEW QUESTION 7

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

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

You have a Microsoft Sentinel workspace

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

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

Solution You create a hunting query.

Does this meet the goal??

- A. Yes
- B. No

Answer: B

Explanation:

A hunting query is an investigation tool. It can find suspicious activity or support manual threat hunting, but it does not automatically assign every new incident to a

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

NEW QUESTION 8

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

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

Answer: A

Explanation:

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

NEW QUESTION 9

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

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

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

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

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

Solution: You add each virtual machine to a role on storage1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

The solution as worded adds virtual machine resources to a role. Azure Storage authorization through Azure RBAC is granted to security principals such as managed identities, users, groups, and service principals, not to VM compute objects as resource containers. Since each VM already has a system-assigned managed identity, the correct approach would be to assign the storage data role to those identities. As stated, this solution does not meet the goal. 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 > managed identities and storage access; Microsoft Learn > RBAC role assignments are made to identities.

NEW QUESTION 10

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

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

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

You need to implement the planned change for 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 10

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

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

You have a Microsoft Sentinel workspace

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

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

Solution: You create 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 15

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 fails 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 19

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

To customize the baseline:

Use Azure Machine Configuration.
 Use Desired State Configuration (DSC).
 Edit the built-in initiative in JSON directly.

Set enforcement mode to:

Apply and Autocorrect
 Apply and Monitor
 Audit
 DeployIfNotExists

- 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 23

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 25

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 30

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 35

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

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

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

How should you configure the policy?

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

Answer: A

Explanation:

The policy must apply across the entire management group MG1 because both Sub1 and Sub2 are in scope for new Foundry deployments. The exception must be expressed as an exclusion for RG-Exception, not by assigning the policy directly to that resource group. Assigning only to Sub1 misses Sub2. Including RG-Exception in the assignment would restrict the resource group that the requirement explicitly excludes. Microsoft platform security questions usually hinge on where enforcement occurs: at the resource, server, subnet, firewall policy, private endpoint, or subscription level. The selected answer uses the control plane that owns that enforcement point. Other options are rejected when they only log activity, broaden network access, or protect a different service category. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege.

Official Microsoft source/topic: SC-500 Study Guide > Azure Policy; Microsoft Learn > policy assignment scopes and exclusions.

NEW QUESTION 39

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

Answer Area

Microsoft Entra role:

Directory Reader
Security Administrator
Security Reader

Azure role:

Microsoft Sentinel Contributor
Microsoft Sentinel Reader
Microsoft Sentinel Responder

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Microsoft Entra role: Directory Reader

Azure role: Microsoft Sentinel Responder

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

Reference:

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

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

NEW QUESTION 43

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 48

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 50

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

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

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

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

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

Solution: You add each virtual machine to a security group, and then add the security group to a role on storage1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Adding virtual machines to a security group does not by itself grant Azure Storage access. The authorization principal used by Azure RBAC must be the managed identity or another supported security principal that the workload uses to request tokens. The solution also fails to state that the system-assigned managed identities are added to the group. Because the compute resources themselves are not the authenticating principals, this solution does not meet the goal. 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 > Azure RBAC and identities; Microsoft Learn > role assignment requires an identity principal at the scope.

NEW QUESTION 53

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 58

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 60

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 61

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 68

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 69

.....

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