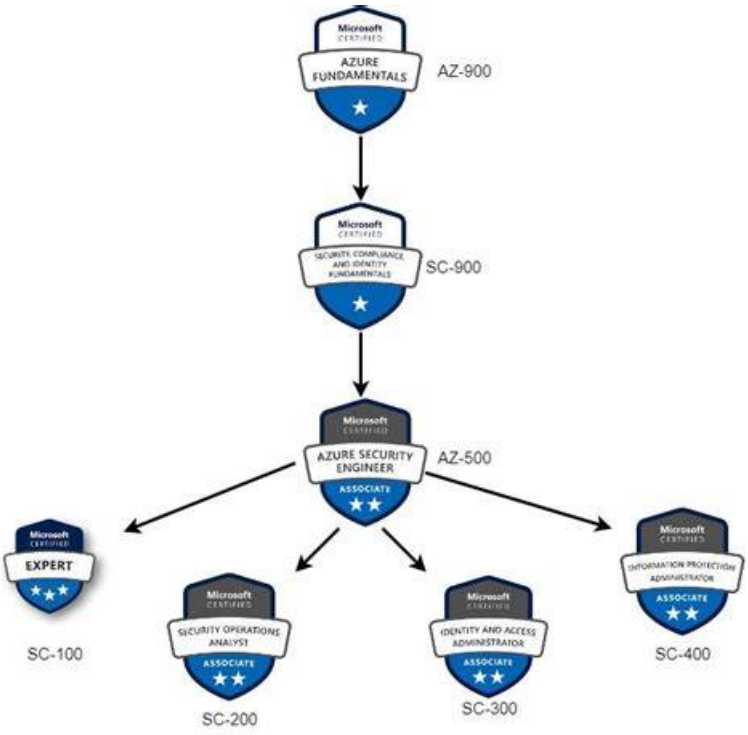
Training SC-500 Kit & SC-500 Reliable Exam Cram



Real4dumps is the website that has been known to learn IT technology. Real4dumps gets high praise from our customers in real test questions and answers. It is the real website that can help you to pass Microsoft SC-500 certificate. Why is Real4dumps very popular? Because Real4dumps has a group of IT elite which is committed to provide you with the best test questions and test answers. Therefore, Real4dumps will provide you with more and better certification training materials to satisfy your need.

Microsoft SC-500 Exam Syllabus Topics:

Section	Weight	Objectives
Topic 1: Secure storage, databases, and networking	25–30%	- Network security • 1. VPN security • 2. Network Watcher diagnostics • 3. Azure Firewall • 4. NSGs and ASGs • 5. Virtual WAN security • 6. Private endpoints and Private Link • 7. Azure Virtual Network Manager - Storage security • 1. Storage account security configuration • 2. Defender for Storage • 3. Access policies for storage • 4. Storage firewall rules - Database security • 1. Azure SQL security configuration • 2. Database auditing • 3. Defender for Databases

Topic 2: Manage identity, access, and governance	20–25%	- Secure secrets and keys using Azure Key Vault • 1. Keys, secrets, and certificates management • 2. Key Vault deployment and configuration • 3. Access policies and firewall settings • 4. Defender for Key Vault and CSPM scanning - Secure access to resources by using Microsoft Entra ID • 1. Authentication methods (MFA, passwordless) • 2. OAuth consent and permission grants • 3. Managed identities for Azure resources • 4. Privileged Identity Management (PIM) • 5. Conditional Access policies • 6. Enterprise applications and app registrations - Governance and compliance enforcement • 1. RBAC and role management (Azure & Entra roles) • 2. Microsoft Defender for Cloud compliance • 3. Resource locks • 4. Azure Policy (built-in and custom) • 5. Azure Backup security controls • 6. Infrastructure as Code security controls
Topic 3: Secure compute	20–25%	- Servers and virtual machines • 1. Azure Arc hybrid security • 2. Secure boot and vTPM • 3. Disk encryption • 4. Agentless scanning and EDR • 5. Just-in-time (JIT) VM access • 6. Defender for Servers onboarding • 7. Azure Bastion - Application platform security • 1. Web Application Firewall (WAF) • 2. AKS security and Defender for Containers • 3. App Service security controls • 4. Container Registry security • 5. API Management security policies • 6. Azure Functions security - Security for AI workloads • 1. AI Gateway (Azure API Management) • 2. Defender for AI services • 3. Microsoft Copilot and AI risk identification • 4. Microsoft Purview DSPM for AI • 5. Security Copilot agents and monitoring • 6. Entra Agent ID security and access control

Topic 4: Manage and monitor security posture	20–25%	- Microsoft Sentinel • 1. Data connectors (Azure, syslog, CEF) • 2. Custom logs and tables • 3. Automation rules and playbooks • 4. Workspaces and role assignment • 5. Retention policies • 6. Data collection rules and WEF - Microsoft Defender for Cloud • 1. Multi-cloud (AWS/GCP) integration • 2. Defender CSPM risk identification • 3. Compliance frameworks evaluation • 4. Defender Vulnerability Management • 5. Workload protection plans • 6. External Attack Surface Management (EASM) - Security Copilot • 1. Permissions and roles • 2. Plugins and integrations • 3. Workspace configuration • 4. Security Store agents

100% Pass Microsoft Realistic Training SC-500 Kit

Our SC-500 training prep was produced by many experts, and the content was very rich. At the same time, the experts constantly updated the contents of the SC-500 study materials according to the changes in the society. The content of our SC-500 learning guide is definitely the most abundant. Before you go to the exam, our SC-500 exam questions can provide you with the simulating exam environment.

Microsoft Implementing End-to-End Security Controls for Cloud and AI Workloads Sample Questions (Q16-Q21):

NEW QUESTION # 16
You have a Microsoft Entra tenant that uses Microsoft Entra Agent ID.
You have multiple Microsoft Foundry agents that have agent identities assigned.
You discover that one of the identities is flagged as high risk due to unusual sign-in activity.
You need to ensure that agent access to resources is restricted automatically based on risk.
What should you create?

- A. a Conditional Access policy for the identities
- B. a Microsoft Entra role assignment policy
- C. a Privileged Identity Management (PIM) activation policy
- D. an Access review for the identities

Answer: A

Explanation:
To automatically restrict agent access to resources based on risk, you should create a Conditional Access policy for agent identities integrated with Microsoft Entra ID Protection. This monitors and revokes or blocks token issuance when an agent's sign-in is flagged at a high risk level.
Reference:
https://learn.microsoft.com/en-us/entra/id-protection/concept-workload-identity-risk

NEW QUESTION # 17
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. Azure Event Grid
- B. Azure Event Hubs
- C. Azure Policy
- D. Application Insights

Answer: A

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 # 18
Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals.
More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.
After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.
You have a Microsoft Sentinel workspace
You have a multi-tier Security Operations Center (SOC) team.
You need to ensure that all new security incidents are assigned immediately to the Tier 1 analysts group and flagged for triage.
Solution: You create a playbook
Does this meet the goal?

- A. No
- B. Yes

Answer: B

Explanation:
A playbook can automate incident response actions by using a Logic Apps workflow. When designed with the Microsoft Sentinel incident trigger or invoked from an automation rule, it can assign an incident and add a triage flag. Because the proposed solution is a playbook for new incidents, it can meet the goal. The essential point is that the workflow must run when incidents are created and update incident properties. The SC-500 study guide places these tasks under security posture, event collection, Defender CSPM, EASM, Sentinel, and Security Copilot operations. The exam expects the control that minimizes analyst effort while preserving correct permissions and data flow. The selected answer reflects that service boundary and avoids a broader or merely investigative alternative. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege.
Official Microsoft source/topic: SC-500 Study Guide > Sentinel playbooks; Microsoft Learn > automate incident assignment and tagging.

NEW QUESTION # 19
You have an Azure subscription named Sub1 that contains a resource group named RG1.
RG1 contains a virtual network named VNet1 and a storage account named storage1. Several engineers are assigned the Owner role for Sub1.
You need to prevent updates to and deletions from VNet1. The solution must ensure that engineers can continue updating other resources in RG1.
Which lock should you apply?

- A. a Read-only resource lock at the RG1 scope
- B. a Delete resource lock at the VNet1 scope

- C. a Delete resource lock at the RG1 scope
- D. a Read-only resource lock at the VNet1 scope

Answer: D

Explanation:
You should use a ReadOnly (also known as Read-only) lock applied directly to the virtual network resource.
Prevents Updates and Deletions: A ReadOnly lock strictly prevents any updates, modifications, or deletions to the resource it is applied to. It forces authorized users (even those with the Owner role) into a "look, but don't touch" state for that specific resource.
Preserves Scope Hierarchy: By applying the lock directly to the virtual network rather than the entire resource group, the lock's restrictions are isolated to just the VNet.
Allows Work on Other Resources: Because the lock is not applied at the resource group level, the selected subscription owners can continue to freely update and modify other resources within the group, such as the storage account.
Reference:
https://learn.microsoft.com/en-us/answers/questions/1465614/safeguarding-your-azure-resources-resource-group-l

NEW QUESTION # 20
Case Study 2 - Fabrikam, Inc.
Overview
Fabrikam, Inc. is a consulting company. The company has a main office in New York City and branch offices in Amsterdam and Singapore.
Existing Environment. Network environment
The on-premises network contains a datacenter in each office.
Existing Environment. Cloud environment
Fabrikam has two Azure subscriptions named Sub1 and Sub2 and a Microsoft 365 subscription that includes Microsoft 365 E5 licenses.
All the subscriptions are linked to a Microsoft Entra tenant named fabrikam.com that contains the identities shown in the following table.

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

The tenant contains the groups shown in the following table.

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

All devices are enrolled in Microsoft Intune.

Existing Environment. Sub1 Resources

Sub1 contains a resource group named RG1 that contains the resources shown in the following table.

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

SQLServer1 uses Microsoft SQL Server authentication.

Sub1 has an Azure Web Application Firewall (WAF) named WAF1 that has the following types of rule sets:

- Bot Manager 1.1
- Azure-managed Default Rule Set (DRS)

Sub1 has the following compliance standards assigned in Microsoft Defender for Cloud:

- NIST SP 800-53 Rev. 4
- Microsoft cloud security benchmark (MCSB)
- System and Organization Controls (SOC) 2 Type 2

Existing Environment. Sub2 Resources

Sub2 contains a resource group named RG2.

Planned Changes and Requirements. Planned Changes

Fabrikam plans to implement the following changes:

- Deploy the following key vaults to RG1:

AKV2 in the West Europe Azure region

AKV3 in the Central US Azure region

AKV4 in the East US Azure region

- Deploy the following key vaults to RG2:

AKV5 in the East US region

- Configure VM1 to read data from storage1.
- Create function apps that have the following hosting plans:

Fa1: Flex Consumption hosting plan

Fa2: Consumption hosting plan

Fa3: Dedicated hosting plan

- For WAF1, implement rate limiting rules based on the request location.

- Enable the NIST SP 800-53 Rev. 5 compliance standard in Defender for Cloud.
- Create a new storage account named storage2 that supports Azure Table storage.
- Enforce multifactor authentication (MFA) when database administrators access SQLdb1.
- Implement ExpressRoute circuits to the on-premises network as shown in the following table.

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

- For RG1, create a new Privileged Identity Management (PIM) eligible role assignment that assigns the Contributor role to supported groups.

Planned Changes and Requirements. Technical Requirements

Fabrikam has the following technical requirements:

- If VM1 is deleted, the permissions for VM1 must be removed automatically.
- The AKS1 managed identity must only be able to pull images from Registry1.
- The ID1 managed identity must be able to push images to and pull images from Registry1.
- All the data in the storage accounts must be encrypted by using Fabrikam-managed keys.
- All outbound traffic from the function apps to the on-premises network must use ExpressRoute circuits.
- ExpressRoute connectivity between the on-premises network and the Azure environment must be encrypted by using Layer 2 or Layer 3 encryption.

Hotspot Question

You need to configure the AKS1 and ID1 managed identities to meet the technical requirements.

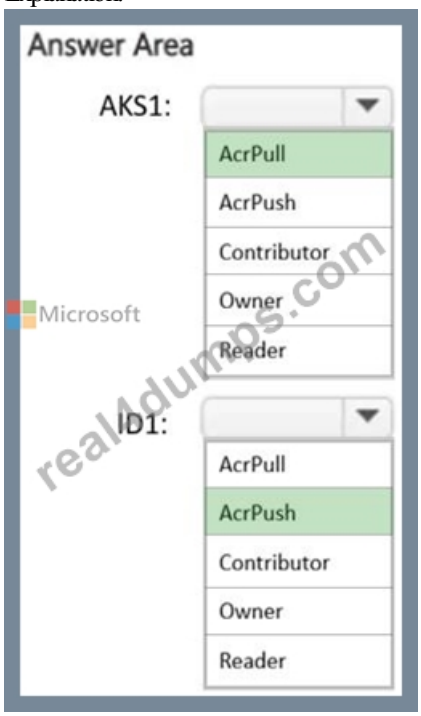
The solution must follow the principle of least privilege.

Which role should you assign to each identity? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:



Explanation:
Box 1: AcrPull
Scenario:
AKS1 is an Azure Kubernetes Service (AKS) cluster in East US.
The AKS1 managed identity must only be able to pull images from Registry1.
Registry1 is an Azure container registry in East US.
To allow the Azure Kubernetes Service (AKS) managed identity (specifically the kubelet identity) to only pull images from an Azure Container Registry (ACR), you must assign the AcrPull role.
Box 2: AcrPush

The ID1 managed identity must be able to push images to and pull images from Registry1.
To allow a managed identity to both push images to and pull images from an Azure Container Registry (ACR), you must assign it the AcrPush built-in role.
Reference:
https://learn.microsoft.com/en-us/azure/aks/pre-created-kubelet-managed-identity?pivots=azure-cli

NEW QUESTION # 21
.....