Microsoft

SC-500

Implementing End-to-End Security Controls for Cloud and AI Workloads

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.

Latest Version: 6.0

Topic 1, Contoso Ltd.

Company Background
Contoso, Ltd. is a financial analytics company that is modernizing its cloud security architecture in Microsoft Azure. Contoso uses Azure Kubernetes Service, Azure Functions, Azure SQL Database, Azure Storage, Microsoft Defender for Cloud, Microsoft Entra Privileged Identity Management, and Azure Arc to secure production workloads and AI-based services.
Contoso has one Azure subscription named Sub1 that is linked to a Microsoft Entra tenant named contoso.com.
Existing Azure Environment
Subscription and Resource Groups
Sub1 contains the following resource groups:
Resource Group
Purpose
RG-App
Hosts production application workloads
RG-Data
Hosts storage and database services
RG-Security
Hosts monitoring and security resources
RG-AI
Hosts AI and agent-related workloads
Compute Resources
Contoso has the following compute resources:
Resource
Type
Description
AKS1
Azure Kubernetes Service cluster
Hosts production containerized applications
ACR1
Azure Container Registry
Stores container images used by AKS1
Fa1
Azure Function App
Processes production AI transaction events
Fa2

Azure Function App
Runs test and diagnostic jobs only
Fa3
Azure Function App
Processes production security automation events
Server1
On-premises server
Hosts a legacy security processing workload
AKS1 uses a managed identity. A separate user-assigned managed identity named ID1 is used by the deployment automation process.

Data Resources

Contoso has the following data resources:
Resource
Type
Description
SQLServer1
Azure SQL logical server
Hosts production SQL databases
SQLdb1
Azure SQL Database
Stores sensitive application data
storage2
Azure Storage account
Stores AI output files and security processing artifacts

Current Security Configuration

Microsoft Defender for Cloud is enabled for Sub1. Defender Cloud Security Posture Management is also enabled.
Contoso has not yet enabled a Defender workload protection plan for AKS1.
Server1 is not currently connected to Azure. The security team wants Server1 to be visible in Azure for monitoring, compliance, and security operations.

Users and Administrators

The Microsoft Entra tenant contains the following users:
User
Current Role / Responsibility
User1
AI engineering user who requests privileged access when required
Admin1
Security administrator for Sub1 and approved Defender for Cloud delegate
Admin2
General application administrator
Admin3
Privileged Role Administrator for Microsoft Entra roles
Admin4

Helpdesk administrator

Privileged Identity Management Configuration

Contoso uses Microsoft Entra Privileged Identity Management.

The following PIM role settings are configured:

Role	Approval Required	Eligible Approvers	Maximum Active Duration
AI Administrator	Yes	Admin1 and Admin3 only	1 day
Agent ID Developer	Yes	Admin1 only	2 days

Admin3 has permission to manage eligible and active assignments for Microsoft Entra roles.

Admin2 is not configured as an approver for the AI Administrator role.

Planned Changes

Contoso plans to implement the following changes:

Configure AKS1 so that it can pull images from ACR1 without granting unnecessary permissions.

Configure ID1 so that the deployment automation process can modify Azure resources required by the application deployment.

Configure SQLdb1 so that access is controlled by Microsoft Entra authentication and Conditional Access.

Configure storage2 so that selected blobs can use a separate encryption boundary without changing encryption for the entire storage account.

Implement the production Function App security changes only for Function Apps that process production workload data.

Enable the correct Microsoft Defender for Cloud plan to protect applications running on AKS1.

Delegate the Defender for Cloud planned change to the least-privileged administrator.

Configure Server1 so that it can be monitored and managed through Azure security tooling.

Technical Requirements

Contoso has the following technical requirements:

AKS and Container Registry

AKS1 must pull container images from ACR1.

AKS1 must receive only the minimum role required to pull images.

The managed identity ID1 must be able to perform deployment automation tasks that modify Azure resources.

Permissions must follow the principle of least privilege.

Azure SQL Database

SQLdb1 must support Microsoft Entra-based authentication.
Access to SQLdb1 must be controlled by Conditional Access.
SQL authentication must not be used for the planned access model.

Azure Storage

storage2 must support granular encryption for selected application data.
The encryption change must not force all data in storage2 to use the same account-level encryption configuration.
The solution must support future separation of encrypted data by workload.

Azure Functions

Only Function Apps that process production workload data must be included in the implementation.
Fa1 processes production AI transaction events and must be included.
Fa2 is used only for diagnostics and test jobs and must not be included.
Fa3 processes production security automation events and must be included.

Microsoft Defender for Cloud

Applications hosted on AKS1 must be protected by the appropriate Defender for Cloud workload plan.
The Defender for Cloud planned change must be delegated to the user with the least privilege required.

Azure Arc and Monitoring

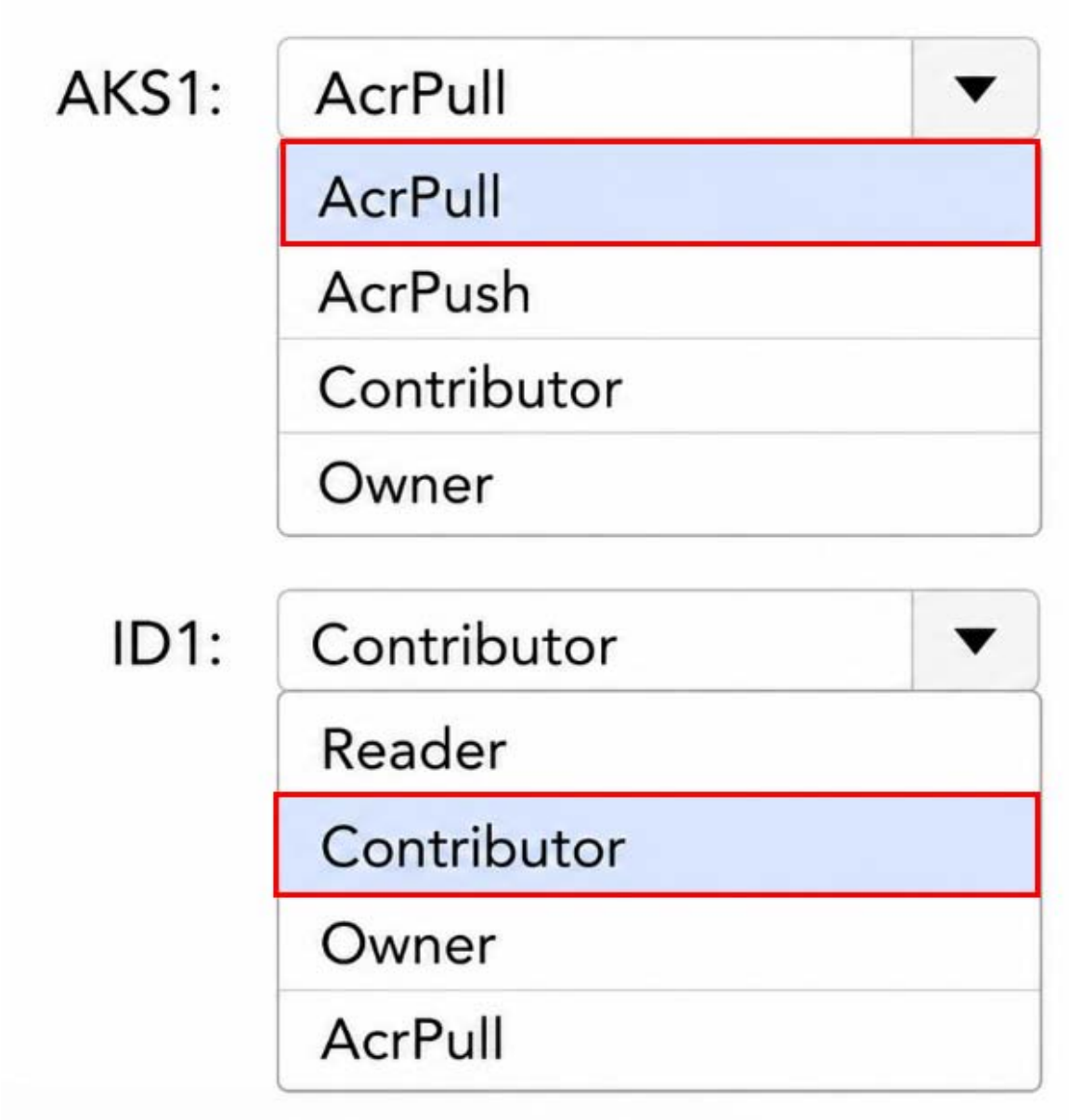
Server1 must be onboarded to Azure.
Security telemetry from Server1 must be collected centrally.
The solution must support security monitoring through Azure-native tooling.

Question: 1

HOTSPOT
You need to configure the AKS1 and ID 1 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.


AKS1:
AcrPull
AcrPull
AcrPush
Contributor
Owner
ID1:
Contributor
Reader
Contributor
Owner
AcrPull

Answer:



Question: 2

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: B, C

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.
==========

Question: 3

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: B

Explanation:
An encryption scope provides a named encryption boundary for blobs and can use Microsoft-managed or customer-managed keys depending on configuration. The planned change refers to storage encryption, and the visible answer set points to a storage2-specific encryption configuration rather than vault purge protection or Azure RBAC. Account-level encryption keys affect the entire account; encryption scopes are the correct more granular storage encryption control. The important exam skill is separating data-plane access, management-plane administration, and network reachability. A storage, database, or firewall setting must be selected because it enforces the exact path requested in the scenario. Distractors often look plausible because they improve security generally, but they do not satisfy the protocol, scope, or automation requirement stated in the question. The result is a direct exam-style

implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > storage encryption; Microsoft Learn > Azure Storage encryption scopes.
==========

Question: 4

You need to implement the function apps to meet the technical requirements.
Which apps should you include in the implementation?

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

Answer: C

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

Question: 5

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.
==========

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/