Passcert

Higher Quality, better service!

Q&A

Http://www.passcert.com

We offer free update service for one year.

Exam : **SC-500**

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

Version : DEMO

1. Topic 1: Contoso Ltd.

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	Role
Admin1	Global Administrator
Admin2	AI Administrator
Admin3	Privileged Role Administrator
User1	*None*

Existing Environment. On-premises environment

The on-premises network contains an Active Directory Domain Services (AD DS) forest that syncs with contoso.com. The forest contains a server named Server1 that runs Windows Server.

Existing Environment. Azure subscription

Sub1 contains the storage accounts shown in the following table.

Name	Azure region	Performance	Premium account type
storage1	West US	Standard	*Not applicable*
storage2	East US	Premium	Block blobs
storage3	East US	Premium	File shares
storage4	East US	Premium	Page blobs

Sub1 contains the virtual networks shown in the following table.

Name	Azure region	Subnet
VNet1	West US	Subnet1, Subnet2
VNet2	East US	Subnet3
VNet3	West US	Subnet4

Sub1 contains the virtual machines shown in the following table.

Name	Connected to	Network security group (NSG)
VM1	Subnet1	NSG1
VM2	Subnet2	NSG2
VM3	Subnet3	NSG3
VM4	Subnet4	NSG4

The network interface of VM1 is associated with an application security group named ASG1.

Sub1 contains the resources shown in the following table.

Name	Azure region	Description
sql1	West US	Azure SQL server
AKS1	East US	Azure Kubernetes Service (AKS) cluster
Vault1	East US	Azure key vault

Vault1 stores the objects shown in the following table.

Name	Type	Status
Key1	Key	Disabled
Secret1	Secret	Enabled
Certificate1	Certificate	Disabled
Certificate2	Certificate	Enabled

Existing Environment. Privileged Identity Management (PIM) configuration

You manage privileged roles by using Privileged Identity Management (PIM).

The PIM role settings are configured as shown in the following table.

Setting	State	
	AI Administrator role	Agent ID Developer role
Activation maximum duration (hours)	1 Day(s)	1 Day(s)
Require approval to activate	Enabled	Disabled
Approvers	None	None
Expire eligible assignments after	1 Month(s)	1 Month(s)
Expire active assignments after	15 Day(s)	15 Day(s)

Existing Environment. Microsoft Sentinel configuration

Contoso has a Microsoft Sentinel workspace that contains the following tables.

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

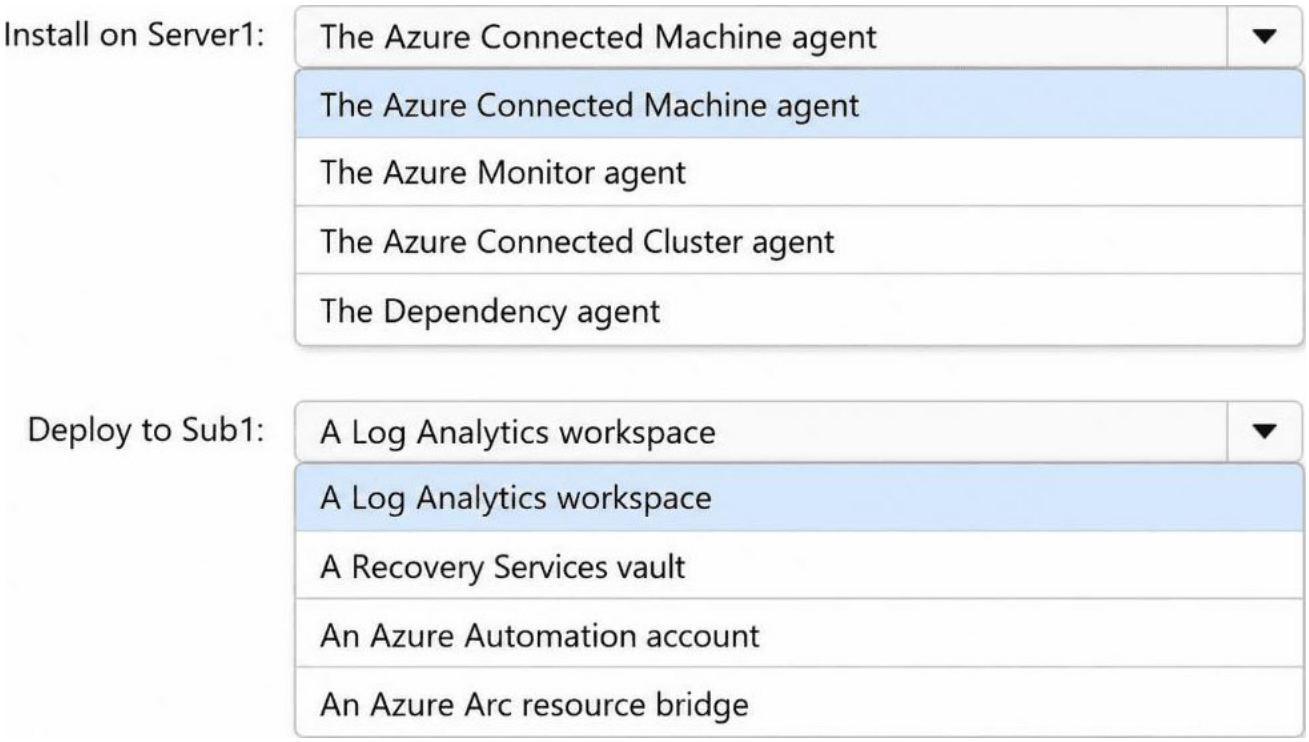
Contoso identifies the following technical requirements:

- Protect Server1 by using file integrity monitoring.
- Protect AKS1 by using Microsoft Defender for Cloud.

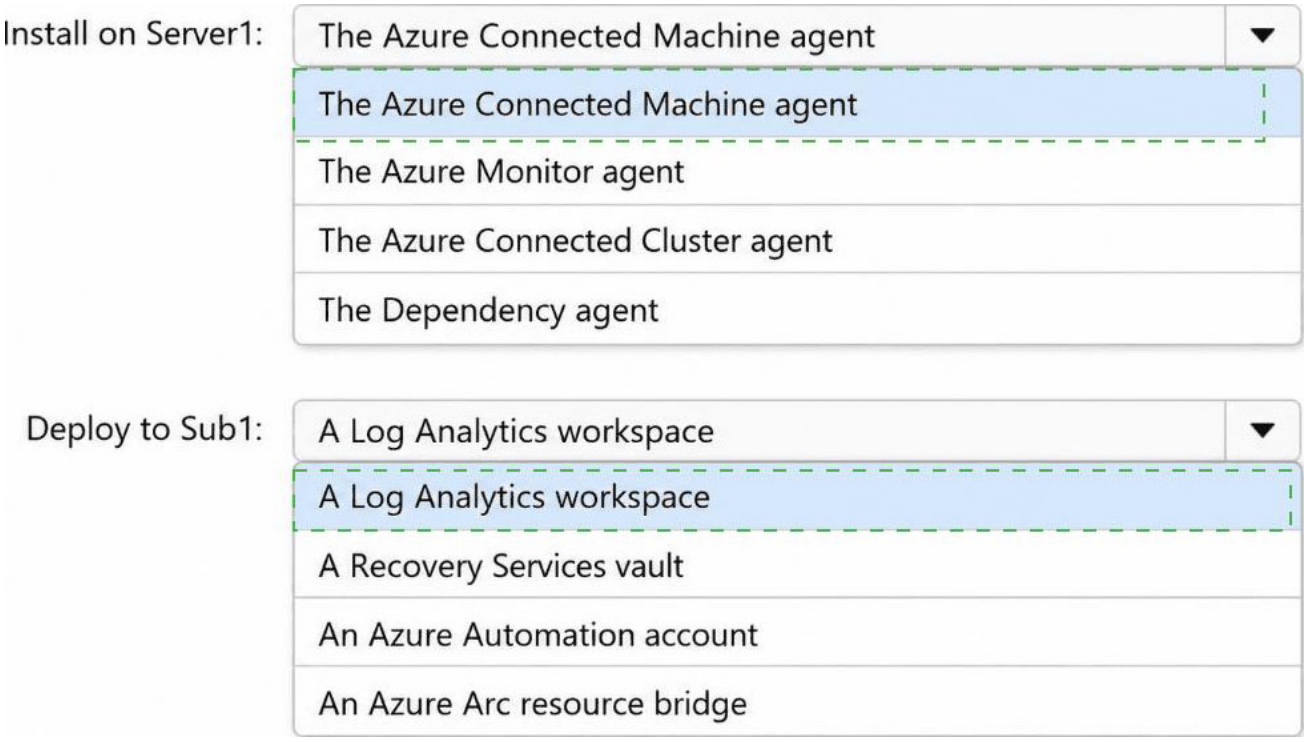
- Configure Microsoft Sentinel to retain data for the maximum supported duration without changing the tier.
- Store objects used for authentication and encryption in Vault1 and ensure that Vault1 regenerates the objects every 30 days, whenever possible.

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.

2.HOTSPOT
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.



Answer:



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.

3.Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.
After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.
You have a Microsoft Sentinel workspace
You have a multi-tier Security Operations Center (SOC) team.
You need to ensure that all new security incidents are assigned immediately to the Tier 1 analysts group and flagged for triage.
Solution: You create a playbook
Does this meet the goal?
A. Yes
B. No
Answer: A
Explanation:
A playbook can automate incident response actions by using a Logic Apps workflow. When designed with the Microsoft Sentinel incident trigger or invoked from an automation rule, it can assign an incident and add a triage flag. Because the proposed solution is a playbook for new incidents, it can meet the goal. The essential point is that the workflow must run when incidents are created and update incident properties. The SC-500 study guide places these tasks under security posture, event collection, Defender CSPM, EASM, Sentinel, and Security Copilot operations. The exam expects the control that minimizes analyst effort while preserving correct permissions and data flow. The selected answer reflects that service boundary and avoids a broader or merely investigative alternative. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Sentinel playbooks; Microsoft Learn > automate incident assignment and tagging.

4.For which storage accounts can you implement the planned changes for storage?
A. storage1, storage2, storage3, and storage4
B. storage1, storage2, and storage4 only
C. storage2 and storage4 only
D. storage1 and storage3 only
E. storage2, storage3, and storage4 only

F. storage1 only
Answer: D
Explanation:
The planned change is to enable Microsoft Entra Kerberos authentication for all supported storage. Microsoft Entra Kerberos authentication is supported for Azure Files SMB shares, so only storage account types that support Azure Files qualify. Microsoft documents Microsoft Entra Kerberos as an identity-based authentication method specifically for Azure file shares over SMB.
From the case:
☞ storage1 — Standard, general-purpose storage: supported. Standard general- purpose v2 accounts support Azure Files in addition to blobs, queues, and tables.
☞ storage2 — Premium Block blobs: not supported because this account type supports Blob Storage, not Azure Files.
☞ storage3 — Premium File shares: supported because this account type is specifically designed for Azure Files.
☞ storage4 — Premium Page blobs: not supported because this account type supports page blobs only.
Therefore, Microsoft Entra Kerberos can be enabled for storage1 and storage3 only.
The account's Azure region does not change this determination. The decisive factor is whether the storage account supports Azure Files SMB, because Microsoft Entra Kerberos authentication is configured through the Azure Files identity-based access settings.

5.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.