DBCLOUD
EXAMS

QUESTIONS & ANSWERS

verified



Technology Provider: Microsoft

Exam: Implementing End-to-End Security Controls for Cloud and AI Workloads - SC-500

Number of questions in the database: 298

Exam Version: NOV.2026

Topic 1

Question #1*Topic 1*

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	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

https://dbcloud.academy/

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)

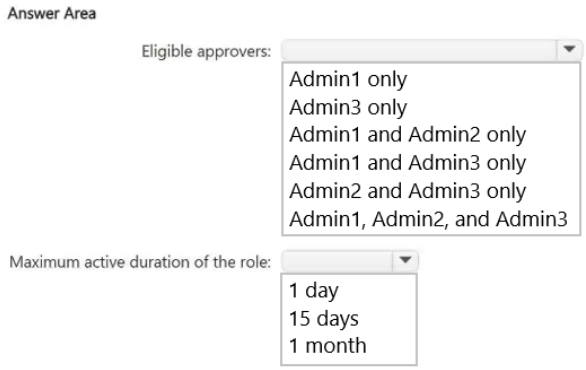
Existing Environment. Microsoft Sentinel configuration
Contoso has a Microsoft Sentinel workspace that contains the following tables.

Name	Tier
DeviceInfo	Analytics
DnsEvents	Analytics

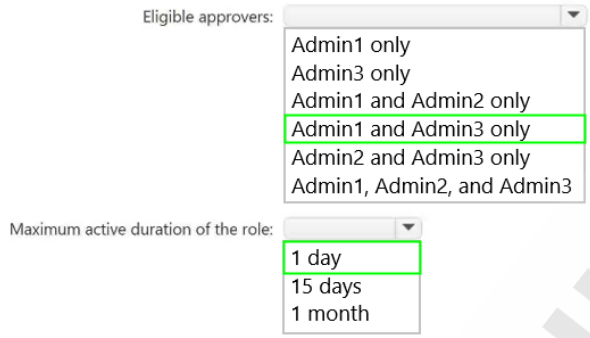
Requirements. Planned changes -
Contoso plans to implement the following changes:
Integrate AKS1 with Vault1.
Enable Microsoft Entra Kerberos authentication for all supported storage.
Configure auditing for sql1 by using the Azure portal and store audit logs in a centralized location.
Requirements. Technical 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.
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.

https://dbcloud.academy/

NOTE: Each correct selection is worth one point.



Correct Answer:



Question #2*Topic 1*

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	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.

https://dbcloud.academy/

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 -

https://dbcloud.academy/

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.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Admin1 must approve requests for the Agent ID Developer role.	○	○
Admin2 can approve requests for the AI Administrator role.	○	○
Admin3 can assign User1 a two-day active assignment for the Agent ID Developer role.	○	○

Correct Answer:

Statements	Yes	No
Admin1 must approve requests for the Agent ID Developer role.	○	◉
Admin2 can approve requests for the AI Administrator role.	○	◉
Admin3 can assign User1 a two-day active assignment for the Agent ID Developer role.	◉	○

https://dbcloud.academy/

Question #3Topic 1

You have an Azure SQL Database logical server named Server1 that contains a database named DB1.

You need to configure authentication for Server1 to meet the following requirements:

SQL authentication cannot be used for any databases on Server1.

The solution must be enforced centrally at the server level.

What should you do?

A. Configure a Microsoft Entra administrator for Server1.

B. Enable a managed identity for Server1.

C. Enable Microsoft Entra-only authentication for Server1.

D. Remove SQL logins from DB1.

Correct Answer: C

Question #4Topic 1

You have a Microsoft Entra tenant that has the following configurations:

User consent for applications is disabled.

Only administrators can grant permissions to applications.

You register an application named App1 that uses delegated Microsoft Graph permissions.

You need to configure App1 to meet the following requirements:

Enable user sign-ins without interactive consent prompts.

Enable App1 to access Microsoft Graph on behalf of the signed-in user.

What should you do?

A. Configure enterprise applications to require user assignment and assign users to App1.

B. Modify the app registration to use application permissions instead of delegated permissions.

C. Add the required delegated Microsoft Graph permissions to the app registration and rely on user consent during sign-in.

D. Grant admin consent to App1 for the required delegated permissions.

Correct Answer: D

https://dbcloud.academy/

Question #5Topic 1

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. Expire active assignments after

B. Require approval to activate

C. Require justification on activation

D. Expire eligible assignments after

E. Activation maximum duration

Correct Answer: BE

Question #6Topic 1

You have two management groups named MG1 and MG2 that contain multiple Azure subscriptions. The subscriptions are linked to a Microsoft Entra tenant.

You have a user named User1 and a global administrator named Admin1.

You are informed that User1 created an Azure subscription named Sub1 under the MG2 management group and is the only owner of the subscription.

You need to ensure that Admin1 can remove the Owner role from User1 for Sub1.

What should you do first?

A. Move Sub1 to MG1.

B. Assign Admin1 the User Access Administrator role for Sub1.

C. Instruct Admin1 to use Privileged Identity Management (PIM) to request the Security Administrator role.

D. Instruct Admin1 to enable Access management for Azure resources.

Correct Answer: D

https://dbcloud.academy/

Question #7Topic 1

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.

Correct Answer: A

Question #8Topic 1

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

Correct Answer: D

https://dbcloud.academy/