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

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.

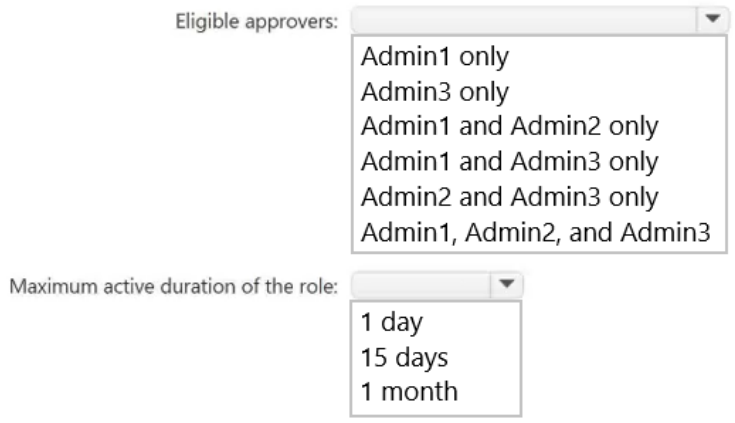
Store objects used for authentication and encryption in Vault1 and ensure that Vault1 regenerates the objects every 30 days, whenever possible.

User1 has requested to use the AI Administrator role.

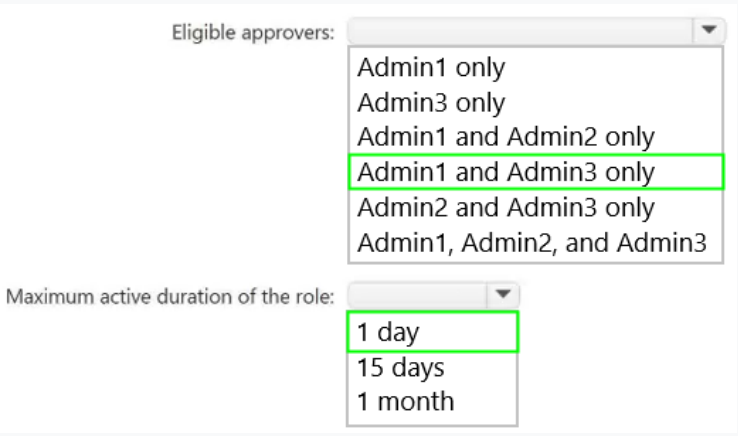
Which approvers can approve the request, and how long will User1 be an AI administrator after the role is approved? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:



Currently there are no comments in this discussion, be the first to comment!

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.

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.

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.	○	○

Suggested 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.	◯	○

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 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

Suggested Answer: *BE*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 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.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

DRAG DROP -

You have a Microsoft Entra tenant.

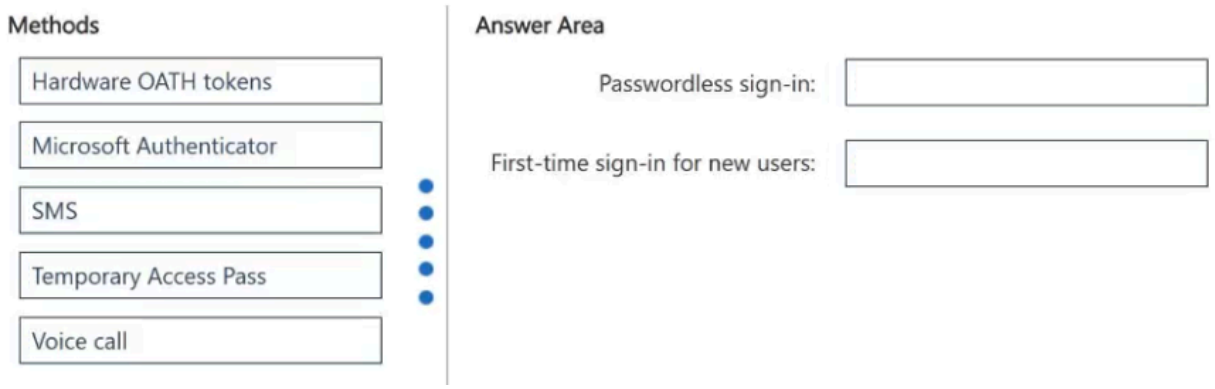
You need to implement passwordless authentication. The solution must meet the following requirements:

Users can sign in without a password by using a mobile device.

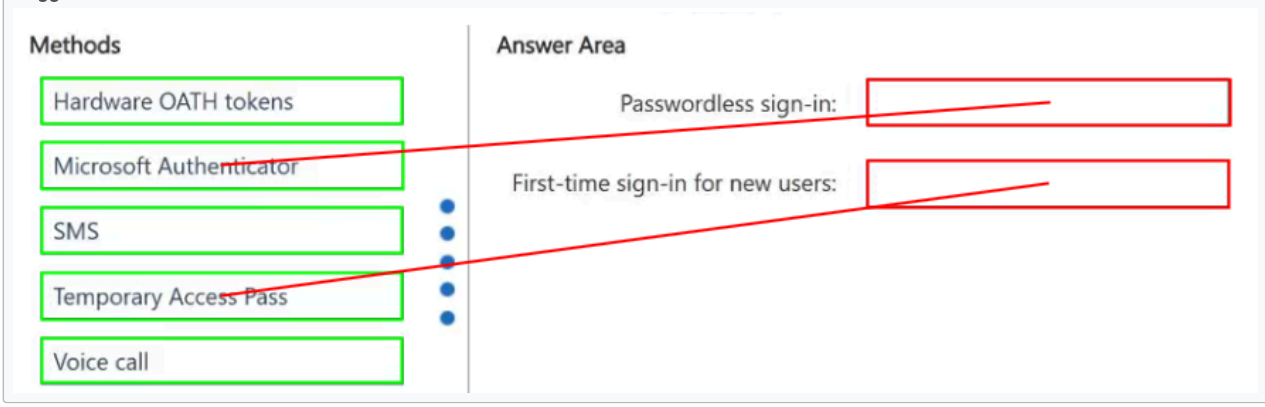
New users that sign in for the first time must use a helpdesk-issued sign-in method that expires.

Which authentication method should you enable for each requirement? To answer, drag the appropriate methods to the correct requirements. Each method 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.



Suggested Answer:



Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

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 scope

D. Owner at the MG1 scope

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

DRAG DROP -

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:

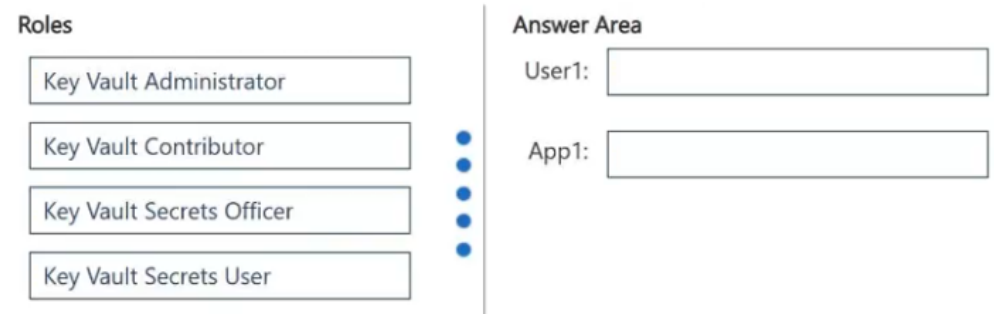
App1 must be able to retrieve secrets from KV1.

User1 must manage the KV1 settings without accessing secret values.

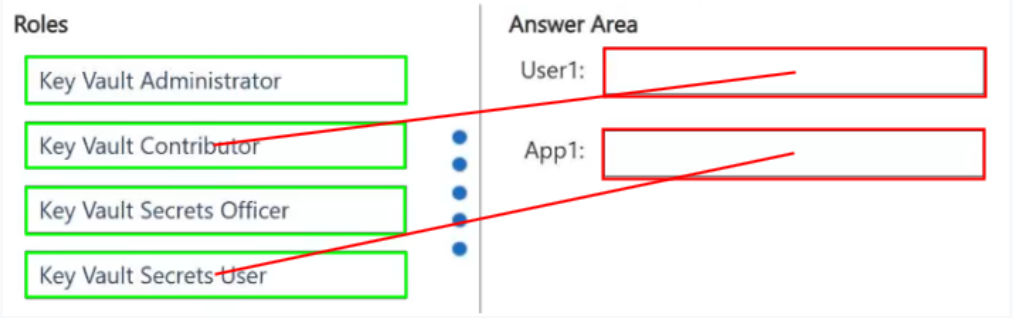
The solution must follow the principle of least privilege.

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.



Suggested Answer:



Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

HOTSPOT -

You have an Azure subscription named Sub1 that contains 50 virtual machines. Sub1 has Microsoft Defender for Cloud enabled.

Sub1 contains an Azure key vault named KV1 and an Azure policy that enforces storing all secrets in KV1.

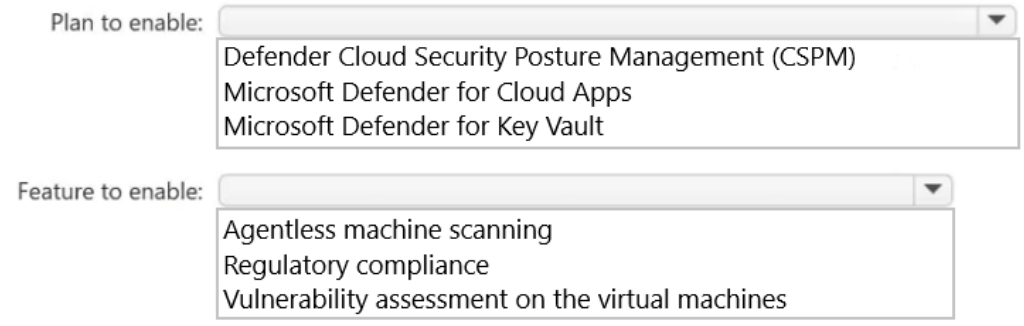
Occasionally, the developers at your company store plaintext tokens and SSH private keys on the virtual machines.

You need to configure Defender for Cloud to detect plaintext secrets on the virtual machines. The solution must minimize administrative changes to the virtual machines.

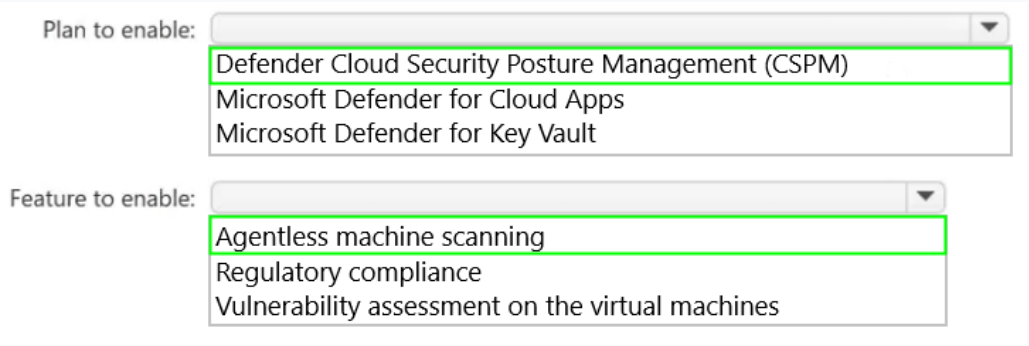
How should you configure Defender for Cloud? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:



Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

HOTSPOT -

You have an Azure subscription.

You need to create and deploy an Azure policy that meets the following requirements:

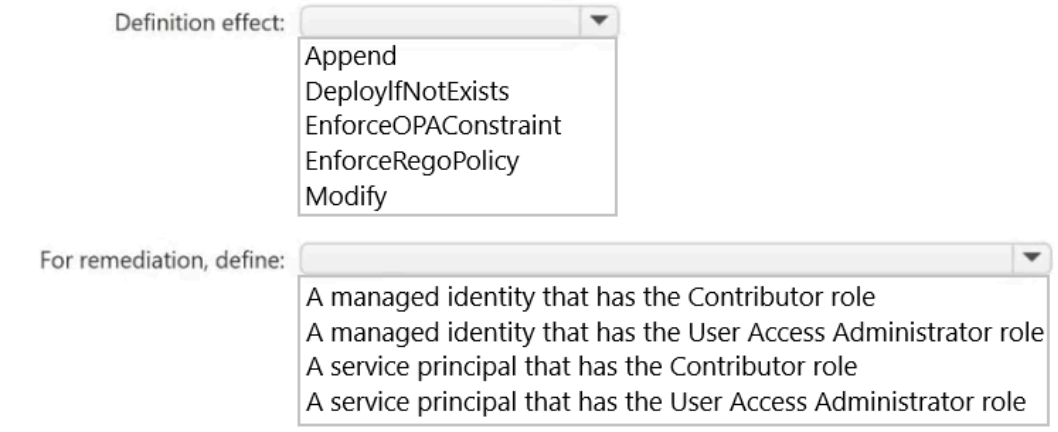
When a new virtual machine is deployed, automatically install a custom security extension.

Trigger an autogenerated remediation task for non-compliant virtual machines to install the extension.

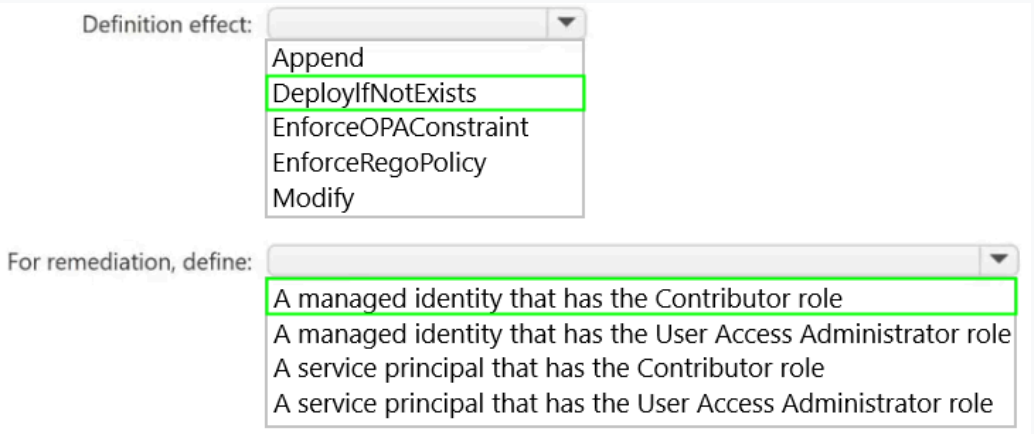
What should you include in the policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:



Currently there are no comments in this discussion, be the first to comment!

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.

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.

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

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.
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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

You have an Azure SQL Database logical server named Server1 that contains multiple databases.
The databases contain legacy SQL authentication logins that must no longer be usable for sign-in but must NOT be removed from the databases.
You need to ensure that SQL authentication is denied for connections.
What should you do?

A. Run create USER ... FROM EXTERNAL PROVIDER on each database.

B. Create a Conditional Access policy.

C. Enable Microsoft Entra-only authentication for Server1.

D. Assign the SQL Server Contributor role to Server1.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

You have an Azure subscription named Sub1 that contains an Azure Database for PostgreSQL instance. Sub1 has Microsoft Defender for Cloud enabled.
You need to configure Microsoft Defender for Databases to minimize costs.
Which Defender plan should you enable?

A. Microsoft Defender for Servers

B. Microsoft Defender for Open-Source Relational Databases

C. Microsoft Defender for SQL Servers on Machines

D. Microsoft Defender for Azure SQL Databases

E. Microsoft Defender for Storage

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

You have an Azure Storage account named storage1 that contains Azure Files shares.
You have an application named App1 that uses a system-assigned managed identity to access the shares.
Administrators access the shares by using storage account keys.
You need to ensure that App1 access the shares without using the storage account keys.
What should you do on storage1?

A. Store the storage account access keys in Azure Key Vault and regenerate them periodically.

B. Set Allow storage account key access to Disabled.

C. Select Default to Microsoft Entra authorization in the Azure portal.

D. Assign the Storage File Data Privileged Reader role to the managed identity of App1.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

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. Application Insights

B. Azure Event Hubs

C. Azure Event Grid

D. Azure Policy

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

DRAG DROP -

You have an Azure virtual network named VNet1 that contains three subnets named Subnet1, Subnet2, and Subnet3. A single network security group (NSG) named NSG1 is associated with all the subnets. You have the following virtual machines:

VM1 on Subnet1 -

VM2 on Subnet2 -

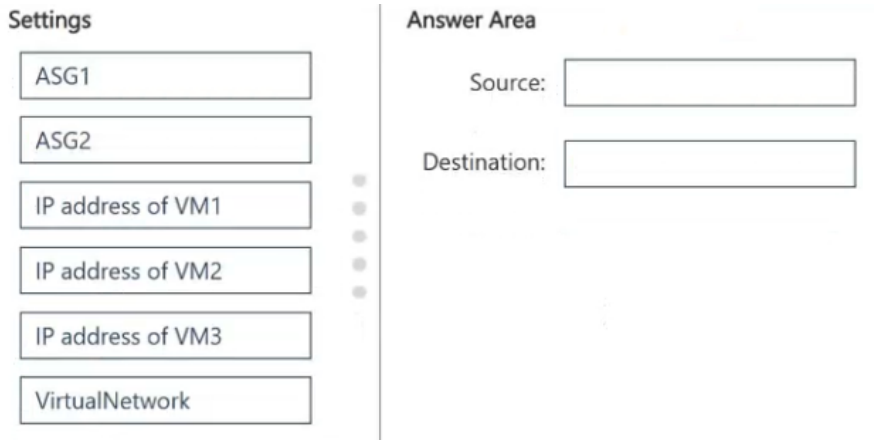
VM3 on Subnet3 -

You create two application security groups named ASG1 and ASG2. VM2 is a member of ASG1, and VM3 is a member of ASG2.

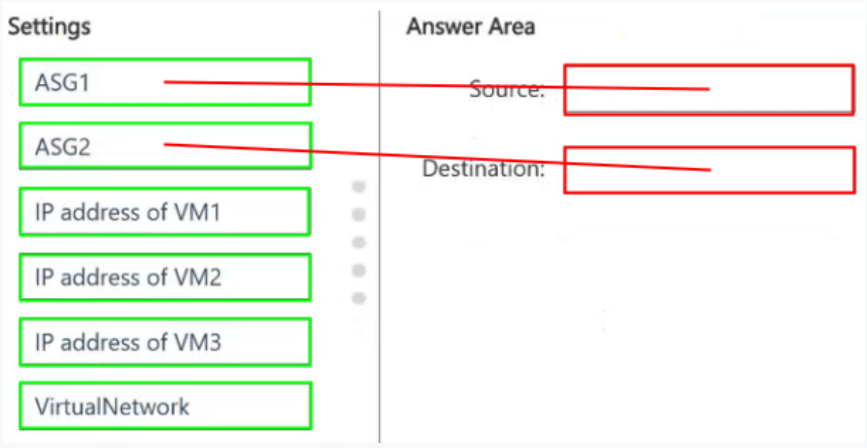
You need to ensure that only VM2 can connect to VM3. The solution must continue to work if the private IP address of VM2 changes.

How should you configure the inbound rule on NSG1? To answer, drag the settings to the correct configurations. Each setting 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.



Suggested Answer:



Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

You have an Azure virtual network that contains 100 virtual machines and an Azure Firewall instance named FW1.
All the traffic from the virtual machines is routed through FW1.
You need to ensure that FW1 allows access to only a URL of updates.contoso.com and blocks all other outbound traffic.
What should you use?

A. an inbound NAT rule

B. an application rule

C. an outbound NAT rule

D. a network rule

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

You use Azure Virtual Network Manager to manage multiple virtual networks in a network group named Group1.
You discover that the virtual machines in Group1 are accessible from the internet by using TCP port 3389.
You need to block inbound TCP 3389 from the internet across all the virtual networks in Group1. The solution must minimize administrative effort.
What should you use?

A. a connectivity configuration

B. a security admin configuration

C. a user-defined route (UDR)

D. a network security group (NSG)

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

You have an Azure subscription.
You need to deploy an Azure virtual WAN to meet the following requirements:
Create three secured virtual hubs located in the East US, West US, and North Europe Azure regions.
Ensure that security rules sync between the regions.
What should you use?

A. Azure Network Function Manager

B. Azure Firewall Manager

C. Azure Virtual Network Manager

D. Azure Front Door

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

You have an Azure Storage account named storage1 that hosts a blob container named container1.
You have an Azure Functions app named app1 that uses a managed identity.
You need to configure app1 to read, write, and delete blobs in container1. The solution must follow the principle of least privilege.
What should you do?

A. Assign the Storage Account Contributor role to the managed identity of app1 at the scope of storage1.

B. Assign the Storage Blob Delegator role to the managed identity of App1 at the scope of container1.

C. Assign the Owner role to the managed identity of App1 at the scope of container1.

D. Assign the Storage Blob Data Contributor role to the managed identity of App1 at the scope of container1.

Suggested Answer: *D*

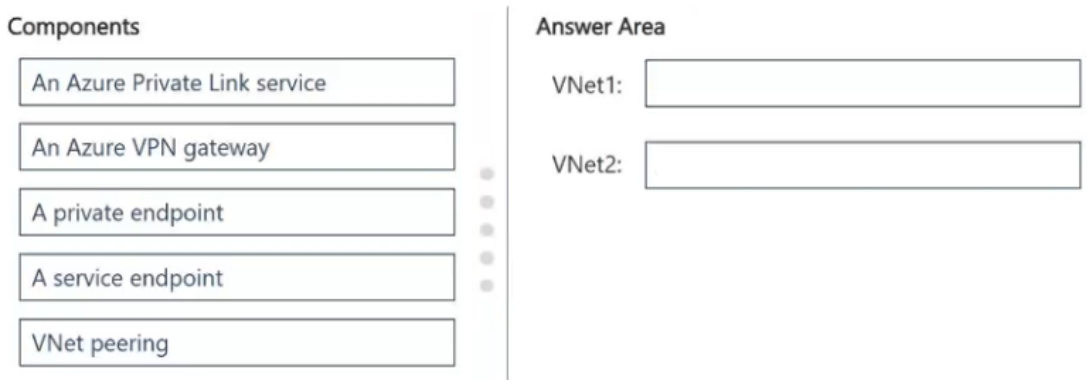
Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

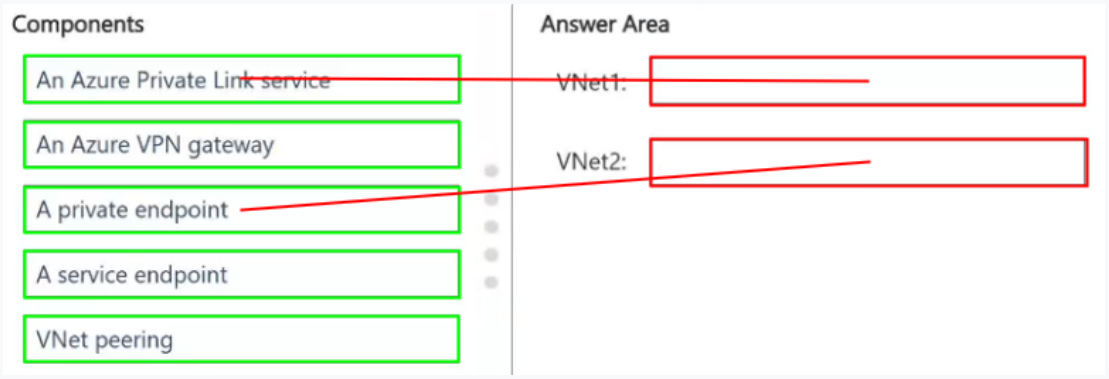
DRAG DROP -
You have an Azure subscription named Sub1 that contains a virtual network named VNet1.
VNet1 contains multiple virtual machines, including two virtual machines named VM1 and VM2.
Sub1 is linked to a Microsoft Entra tenant named contoso.com.

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.



Suggested Answer:



Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

HOTSPOT -

You have an Azure subscription that contains the following resources:

An Azure SQL Database logical server named Server1 that contains a database named DB1

An Azure SQL Managed Instance named Instance1 that contains a database named DB2

You need to configure database auditing. The solution must meet the following requirements:

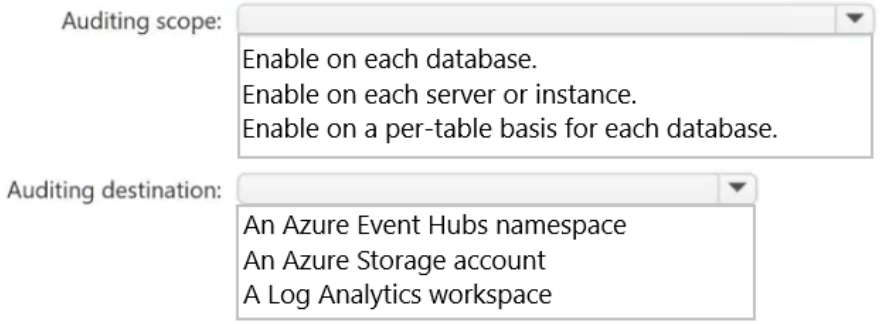
Ensure that audit data is centrally available in a location that supports for KQL queries.

Minimize ongoing administrative effort as additional databases are added.

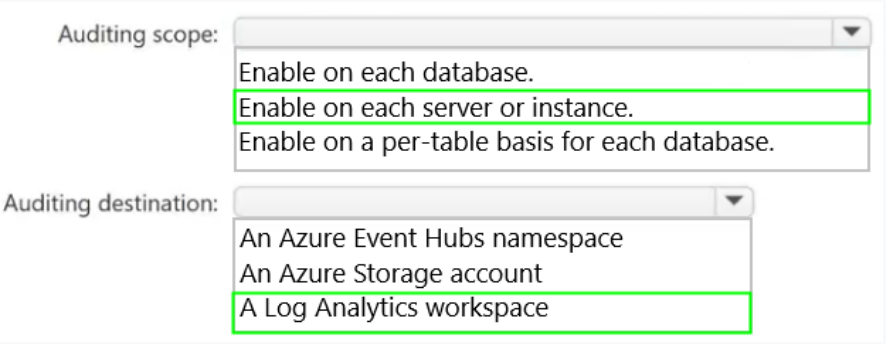
What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:



Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

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 create a user-assigned managed identity, assign the identity to each virtual machine, and then add each managed identity to a role on storage1.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

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 create a private endpoint on storage1.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

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: