Microsoft Certified Azure Security Engineer Associate

Exam AZ-500 Microsoft Azure Security Technologies

Demo Questions

Microsoft Azure

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

AZ-500: Microsoft Azure Security Technologies

Q.1
You have a Azure subscription that contains an Azure Container Registry named Registry1. The subscription uses the Standard use tier of Azure Security Center.
You upload several container images to Register1.
You discover that vulnerability security scans were not performed. You need to ensure that the images are scanned for vulnerabilities when they are uploaded to Registry1.
What should you do?
A. From the Azure portal modify the Pricing tier settings.
B. From Azure CLI, lock the container images.
C. Upload the container images by using AzCopy
D. Push the container images to Registry1 by using Docker

Answer: A

Q.2
You have an Azure resource group that contains 100 virtual machines.
You have an initiative named Initiative1 that contains multiple policy definitions. Initiative1 is assigned to the resource group.
You need to identify which resources do **NOT** match the definitions.
What should you do?
A. From Azure Security Center, view the Regulatory compliance assessment.
B. From the Policy blade of the Azure Active Directory admin center, select **Compliance**.
C. From Azure Security Center, view the Secure Score.
D. From the Policy blade of the Azure Active Directory admin center, select **Assignments**.

Answer: B

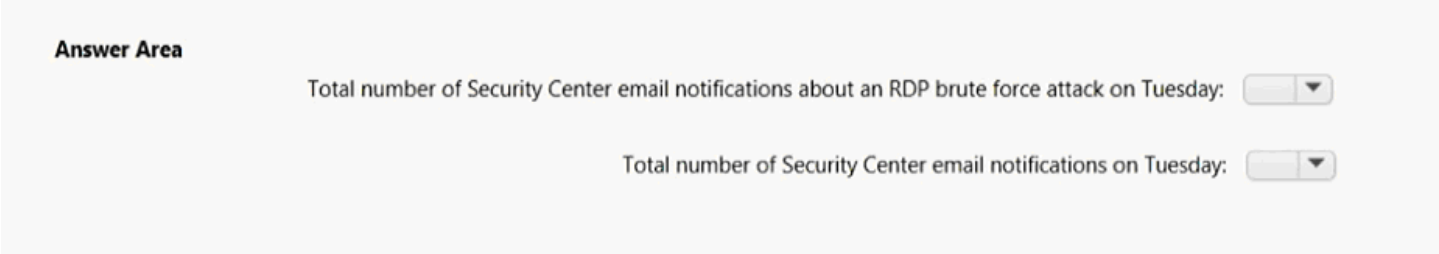
Q.3
You have an Azure environment. You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001:2013 standards. What should you use?
A. Azure Sentinel
B. Microsoft Defender for Identity
C. Azure Active Directory (Azure AD) Identity Protection
D. Azure Security Center

Answer: D

Q.4
On Monday, you configure an email notification in Azure Security Center to notify user1@contoso.com about alerts that have a severity level of Low, Medium, or High.
On Tuesday, Security Center generates the security alerts shown in the following table.

Time	Description	Severity
01:00	Failed RDP brute force attack	Medium
01:01	Successful RDP brute force attack	High
06:10	Suspicious process executed	High
09:00	Malicious SQL activity	High
11:15	Network communication with a malicious machine detected	Low
13:30	Suspicious process executed	High
14:00	Failed RDP brute force attack	Medium
16:01	Successful RDP brute force attack	High
23:20	Possible outgoing spam activity detected	Low
23:25	Modified system binary discovered in dump file	High
23:30	Malicious SQL activity	High

How many email notifications will user1@contoso.com receive on Tuesday?
To answer, select the appropriate options in the answer area. **NOTE:** Each correct selection is worth one point.



Total number of Security Center email notifications about an RDP brute force attack on Tuesday:
A. 1
B. 2
C. 3
D. 4

Total number of Security Center email notifications on Tuesday:
E. 3
F. 4
G. 7
H. 9
I. 11

Answer: D, I

Q.5

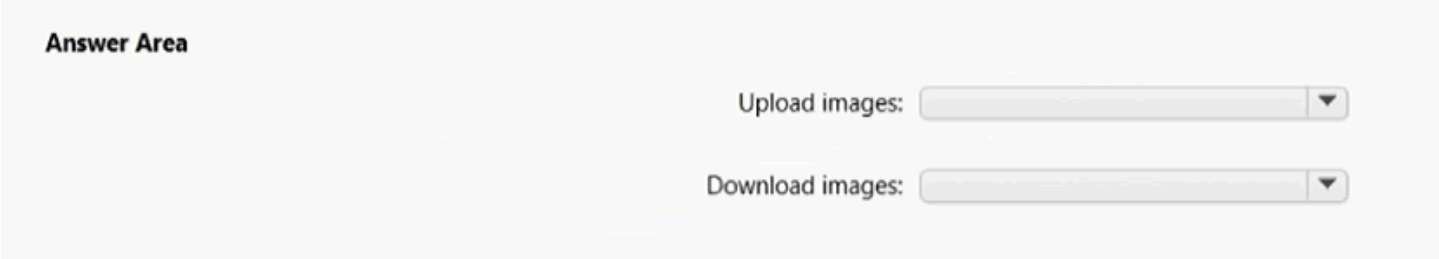
You have an Azure Container Registry named Registry1.

You add role assignments for Registry1 as shown in the following table.

User	Role
User1	AcrPush
User2	AcrPull
User3	AcrimageSigner
User4	Contributor

Which users can upload images to Registry1 and download images from Registry1?

To answer, select the appropriate options in the answer area. **NOTE:** Each correct selection is worth one point.



Upload images:

A. User1 only
B. User1 and User4 only
C. User1, User3, and User4
D. User1, User2, User3, and User4

Download images:

E. User2 only
F. User1 and User2 only
G. User2 and User4 only
H. User1, User2, and User4
I. User1, User2, User3, and User4

Answer: B, H

Q.6

You are troubleshooting a security issue for an Azure Storage account.

You enable Azure Storage Analytics logs and archive it to a storage account.

What should you use to retrieve the diagnostics logs?

A. Azure Storage Explorer
B. Azure Cosmos DB explorer
C. SQL query editor in Azure
D. the Security admin center

Answer: A

Q.7

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	In resource group
cont1	Container instance	RG1
VNET1	Virtual network	RG1
App1	App Service app	RG1
VM1	Virtual machine	RG1
User1	User	**Not applicable**

You create a custom RBAC role in Subscription1 by using the following JSON file.

```
{
  "Name": "Role1",
  "IsCustom": true,
  "Description": "Role1 description",
  "Actions": [
     "*/Read",
     "Microsoft.Compute/*"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/subscriptions/923a419a-4358-40fb-b4a9-b8af43dd0c92/resourceGroups/RG1"
  ]
}
```

You assign Role1 to User1 on RG1.

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
User1 can add VM1 to VNET1.	○	○
User1 can start and stop App1.	○	○
User1 can start and stop cont1.	○	○

User1 can add VM1 to VNET1.

A. Yes

B. No

User1 can start and stop App1.

C. Yes

D. No

User1 can start and stop cont1.

E. Yes

F. No

Answer: A, D, F

Q.8

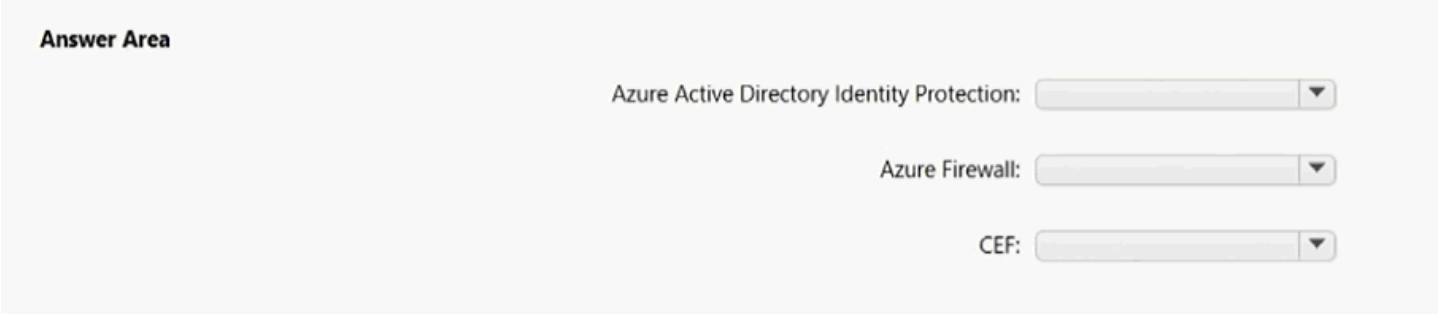
You have an Azure Sentinel workspace that has the following data connectors:

- Azure Active Directory Identity Protection
- Common Event Format (CEF)
- Azure Firewall

You need to ensure that data is being ingested from each connector.

From the Logs query window, which table should you query for each connector?

To answer, selector the appropriate options in the answer area. **NOTE:** Each correct selection is worth one point.



Azure Active Directory Identity Protection:

A. AzureDiagnostics
B. CommonSecurityLog
C. SecurityAlert
D. SecurityEvent
E. Syslog

Azure Firewall:

F. AzureDiagnostics
G. CommonSecurityLog
H. SecurityAlert
I. SecurityEvent
J. Syslog

CEF:

K. AzureDiagnostics
L. CommonSecurityLog
M. SecurityAlert
N. SecurityEvent
O. Syslog

Answer: C, I, O

Q.9

You have an Azure subscription that contains the Azure Active Directory (Azure AD) resource shown in the following table.

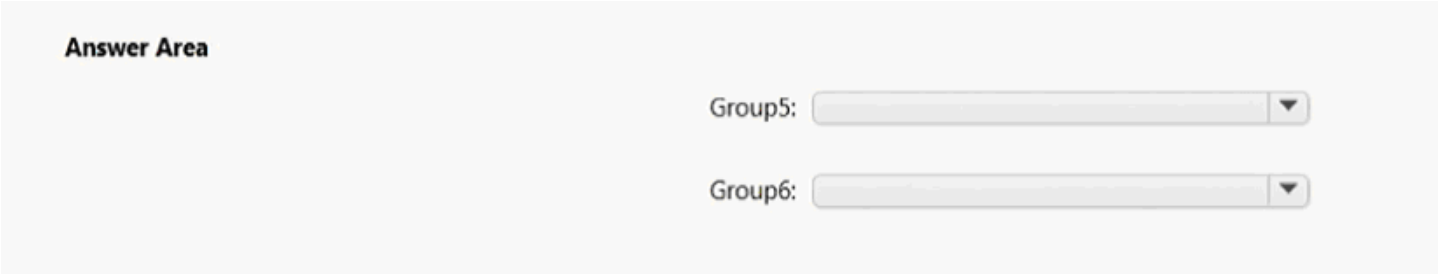
Name	Description
User1	User
Group1	Security group that has a Membership type of Dynamic Device
Managed1	Managed identity
App1	Enterprise application

You create the groups shown in the following table.

Name	Description
Group5	Security group that has a Membership type of Assigned
Group6	Microsoft 365 group that has a Membership type of Assigned

Which resources can you add to Group5 and Group6?

To answer, selector the appropriate options in the answer area. **NOTE:** Each correct selection is worth one point.



Group5:

A. User1 only
B. User1 and Group1 only
C. User1, Group1, and Managed1 only
D. User1, Group1, Managed1, and App1

Group6:

E. User1 only
F. User1 and Group1 only
G. User1, Group1, and Managed1 only
H. User1, Group1, Managed1, and App1

Answer: D, E

Q.10

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com

The tenant contains the users shown in the following table.

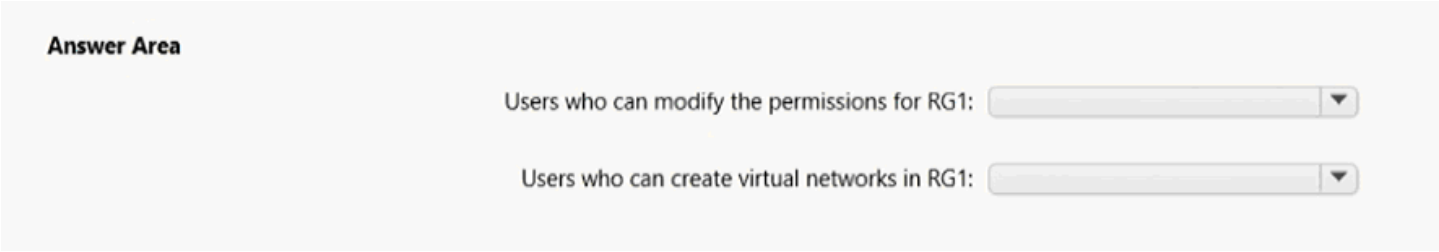
Name	Subscription role	Azure AD user role
User1	Owner	**None**
User2	Contributor	**None**
User3	Security Admin	**None**
User4	**None**	Service administrator

You create a resource group named RG1.

Which users can modify the permissions for RG1 and which users can create virtual networks in RG1?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Users who can modify the permissions for RG1:

A. User1 only
B. User1 and User2 only
C. User1 and User3 only
D. User1, User2, and User3 only
E. User1, User2, User3, and User4

Users who can create virtual networks in RG1:

F. User1 only
G. User1 and User2 only
H. User1 and User3 only
I. User1, User2, and User3 only
J. User1, User2, User3, and User4

Answer: A, G

Q.11
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Subscription role
Admin1	Global administrator
Admin2	Global administrator
Admin3	User administrator

contoso.com contains a group naming policy. The policy has a custom blocked word list rule that includes the word Contoso. Which users can create a group name Contoso Sales in contoso.com?
To answer, select the appropriate options in the answer area. **NOTE:** Each correct selection is worth one point.

Users who can create a security group named Contoso Sales:
A. Admin1 only
B. Admin1 and Admin2 only
C. Admin1 and Admin3 only
D. Admin1, Admin2, and Admin3

Users who can create a Microsoft 365 group named Contoso Sales:
E. Admin1 only
F. Admin1 and Admin2 only
G. Admin1 and Admin3 only
H. Admin1, Admin2, and Admin3

Answer: C, G

Q.12
You have 10 on-premises servers that run Windows Server 2019.
You plan to implement Azure Security Center vulnerability scanning for the servers.
What should you install on the servers first?
A. the Security Events data connector in Azure Sentinel
B. the Microsoft Endpoint Configuration Manager client
C. the Microsoft Defender for Endpoint agent
D. the Azure Arc enabled servers Connected Machine agent

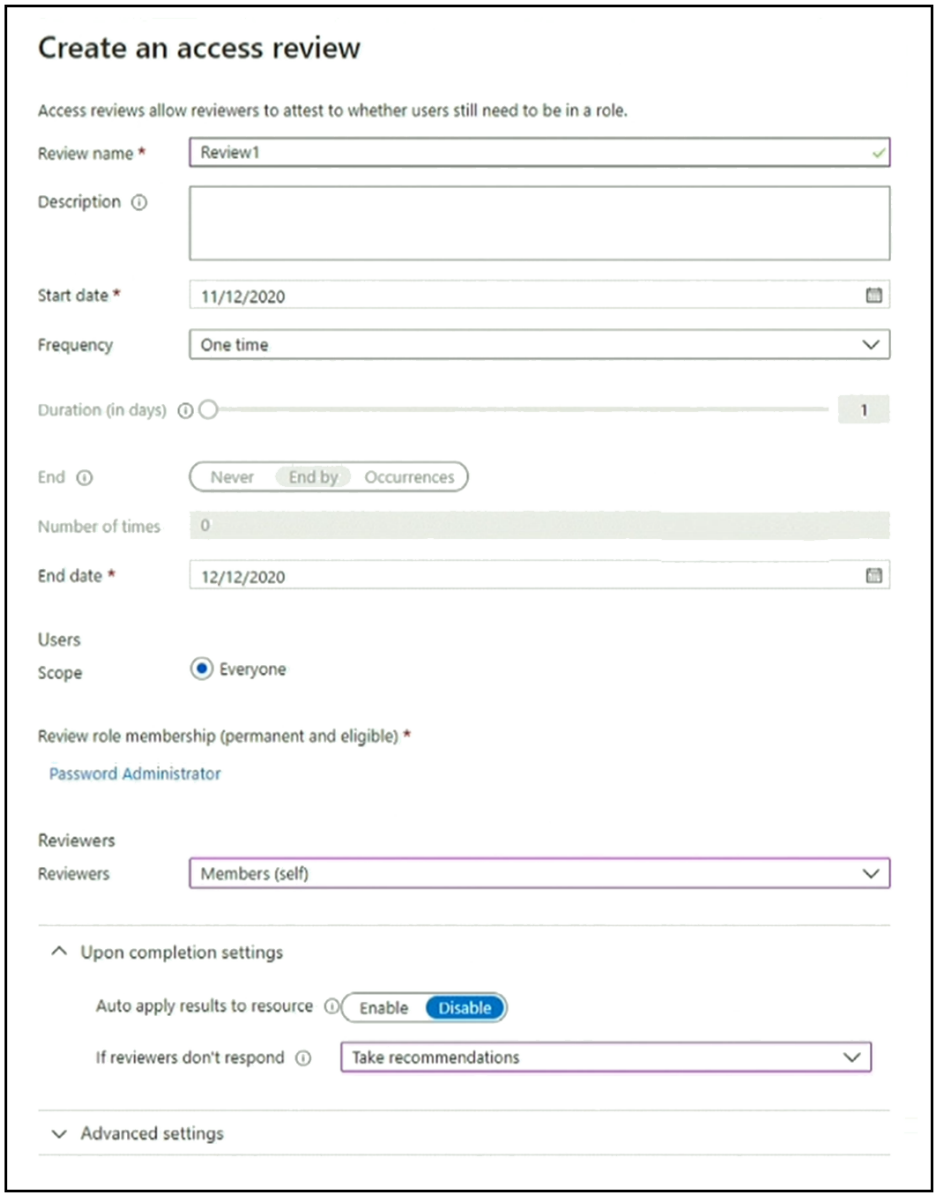
Answer: C

Q.13

You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role	Sign in frequency
User1	Password administrator	Signs in every work day
User2	Password administrator	Signs in bi-weekly
User3	Global administrator, Password administrator	Signs in every month

You configure an access review named Review1 as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Answer Area

User3 can perform Review1 for **[answer choice]**. [ ]

If User2 fails to complete Review1 by December 12, 2020, **[answer choice]**. [ ]

User3 can perform Review1 for [answer choice].

A. User3 only
B. User1 and User2 only
C. User1, User2, and User3

If User2 fail to complete Review1 by December 12, 2020, [answer choice].

D. The Password administrator role will be revoked from User2
E. User2 will retain the Password administrator role
F. User3 will receive a confirmation request

Answer: A, F

Q.14
You have the Azure virtual machines shown in the following table.

Name	Operating system	State
VM1	Windows Server 2012	Running
VM2	Windows Server 2012 R2	Running
VM3	Windows Server 2016	Stopped
VM4	Ubuntu Server 18.04 LTS	Running

For which virtual machine can you enable Update Management?

A. VM2 and VM3 only
B. VM2, VM3, and VM4 only
C. VM1, VM2, and VM3 only
D. VM1, VM2, and VM4 only
E. VM1, VM2, VM3, and VM4

Answer: D

Q.15
Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD). Azure AD Connect is installed on a domain member server named Server1.
You need to ensure that a domain administrator for the adatum.com domain can modify the synchronization options. The solution must use the principle of least privilege. Which Azure AD role should you assign to the domain administrator?

A. User administrator
B. Global administrator
C. Security administrator

Answer: B

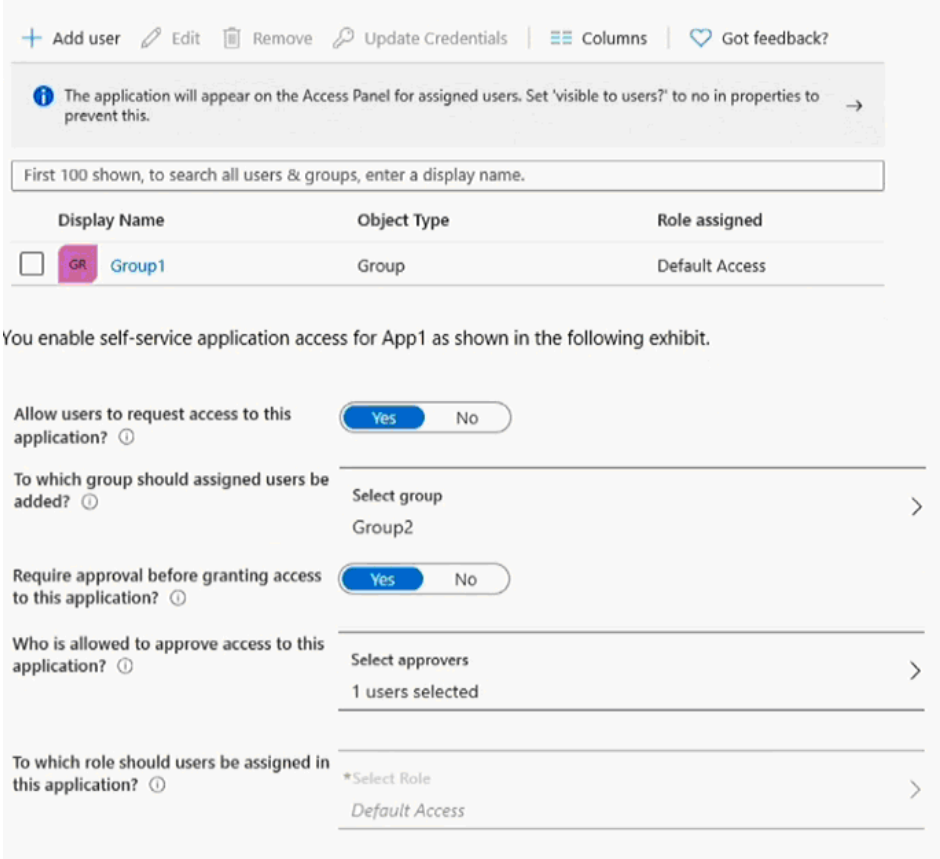
Q.16

You have an Azure Active Directory (Azure AD) tenant that contains the resources shown in the following table.

Name	Type
User1	User
User2	User
Group1	Security group
Group2	Security group
App1	Enterprise application

User2 is the owner of Group2.

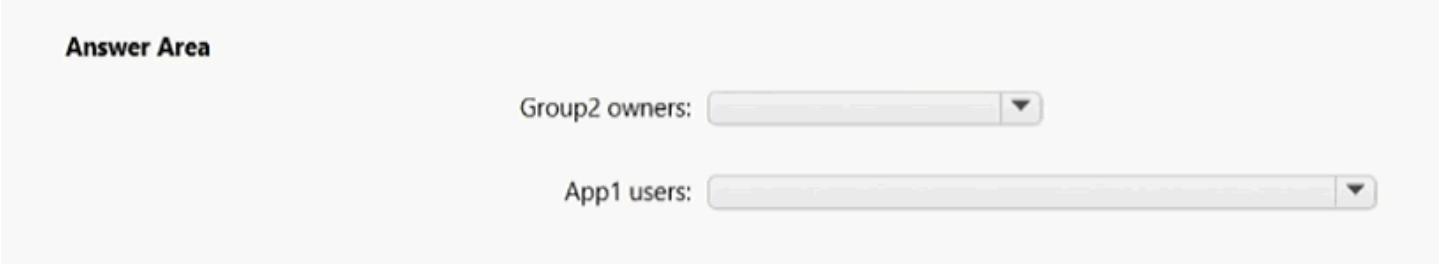
The users and group settings for App1 are configured as shown in the following exhibit.



User3 is configured to approve access to App1.

After you enable self-service application access for App1, who will be configured as the Group2 owner and who will be configured as the App1 users?

To answer, select the appropriate options in the answer area.



Group2 owners:

A. User2 only
B. User3 only
C. User1 and User2 only
D. User2 and User3 only
E. User1, User2, and User3

App1 users:

F. Group1 members only
G. Group2 members only
H. Group1 and Group2 members only
I. Group1 and Group2 members and User1 only
J. Group1 and Group2 members, User1, and User3 only

Answer: A, H

Q.17

You have an Azure Sentinel deployment.

You need to connect a third-party security solution to the deployment. The third-party solution will send Common Event Format (CEF)-formatted messages.

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

NOTE: Each correct selection is worth one point.

Deploy:

A. A Linux server and a Syslog forwarder daemon
B. A Windows server and a Windows Event Forwarding subscription
C. An Azure event hub that has a dedicated namespace

Forward events to Azure Sentinel by using:

D. A Dependency agent
E. An Azure Arc enabled servers Connected Machine agent
F. An Azure Log Analytics agent

Answer: TBC

Q.18

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Enabled
User2	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:

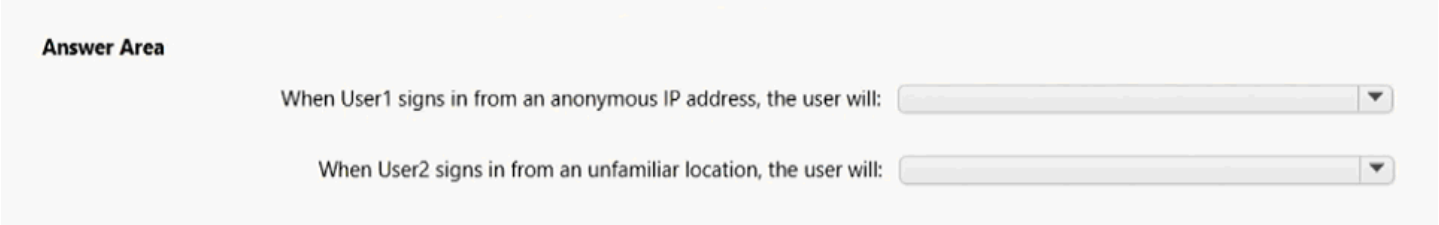
- Assignments: Include Group1, exclude Group2
- Conditions: Sign-in risk level: Low and above
- Access: Allow access, Require multi-factor authentication

You need to identify what occurs when the users sign in to Azure AD.

What should you identify for each user?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



When User1 signs in from an anonymous IP address, the user will:

A. Be blocked
B. Be prompted for MFA
C. Sign in by using a username and password only

When User2 signs in from an unfamiliar locations, the user will:

D. Be blocked
E. Be prompted for MFA
F. Sign in by using a username and password only

Answer: B, D

Q.19

From the Azure portal, you are configuring an Azure Policy.

You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects.

Which effect requires a managed identity for the assignment?

A. **`AuditIfNotExist`**
B. **`Append`**
C. **`DeployIfNotExist`**
D. **`Deny`**

Answer: C

Q.20

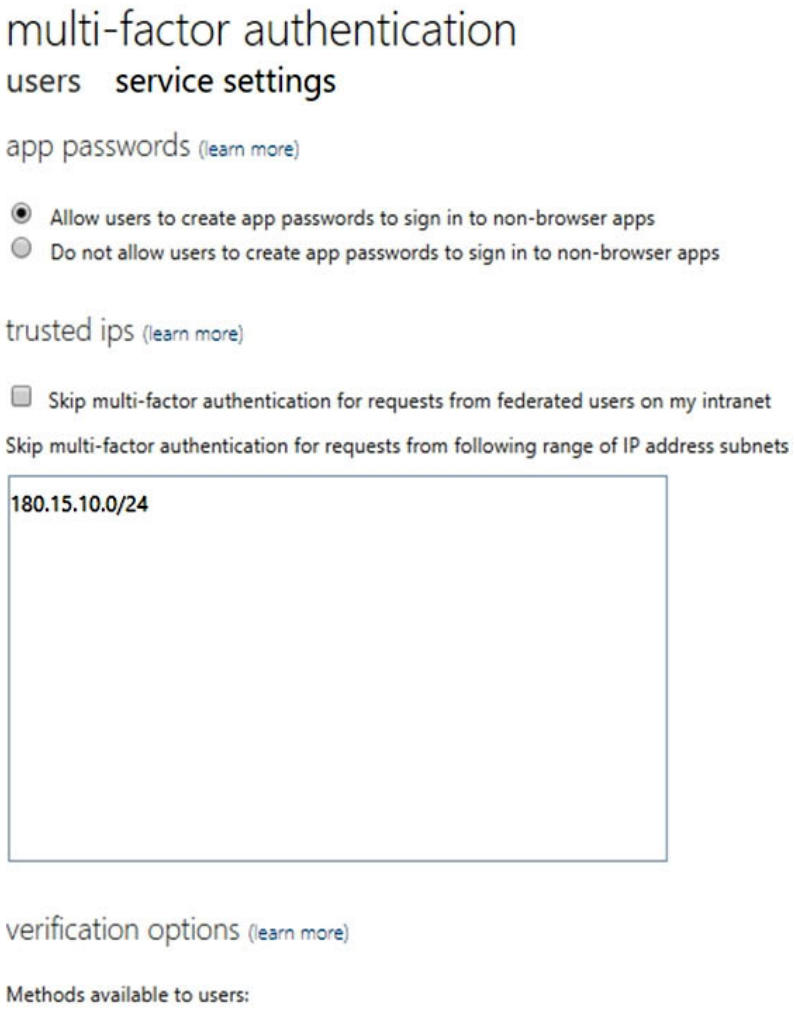
You work at a company named Contoso, Ltd. that has the offices shown in the following table.

Name	IP address space
Boston	180.15.10.0/24
Seattle	132.32.15.0/24

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com. All Contoso.com users have Azure multi-Factor Authentication (MFA) enabled. The tenant contains the users shown in the following table.

Name	User device	Last sign-in	During last sign-in, user selected Don't ask again for 14 days
User1	Device1	June 1	Yes
User2	Device2	June 3	No

The multi-factor authentication settings for Contoso.com are configured as shown in the following exhibit.



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
When User1 signs in to Device1 from the Seattle office on June 10, the user will be prompted for MFA.	○	○
When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA.	○	○
When User1 signs in to new device from the Seattle office on June 7, the user will be prompted for MFA.	○	○

When User1 signs in to Device1 from the Seattle office on June 10, the user will be prompted for MFA.

A. Yes

B. No

When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA.

C. Yes

D. No

When User1 signs in to new device from the Seattle office on June 7, the user will be prompted for MFA.

E. Yes

F. No

Answer: B, C, E

Q.21

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
RG1	Resource group	Used to store virtual machines
RG2	Resource group	Used to store virtual network
ServerAdmin	Security group	Used to manage virtual machines

You need to ensure that ServerAdmins can perform the following tasks:

- Create virtual machines in RG1 only
- Connect the virtual machines to the existing virtual networks in RG2 only

The solution must use the principle of least privilege.

Which two role-based access control (RBAC) roles should you assign to ServerAdmins?

Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. the Network Contributor role for RG1

B. the Network Contributor role for RG2

C. the Virtual Machine Contributor role for RG1

D. the Contributor role for the subscription

E. a custom RBAC role for the subscription

F. a custom BRAC role for RG2

Answer: B, C

Q.22

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	**None**	Disabled
User2	Group1	Disabled
User3	Group1	Enforced

Azure AD Privileged Identify Management (PIM) is used in contoso.com.

In PIM, the Password Administrator role has the following settings:

- Maximum activation duration (hours): 2
- Send email notifying admins of activation: Disable
- Require incident/request ticket number during activation: Disable
- Require Azure Multi-Factor Authentication for activation: Enable
- Require approval to activate this role: Enable
- Selected approver: Group1

You assign users the Password Administrator role as shown in the following table.

Name	Assignment type
User1	**Active**
User2	Eligible
User3	Eligible

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
When User1 signs in, the user is assigned the Password Administrator role automatically.	○	○
User2 can request to activate the Password Administrator role.	○	○
If User3 wants to activate the Password Administrator role, the user can approve their own request.	○	○

When User1 signs in, the user is assigned the Password Administrator role automatically.

A. Yes

B. No

User2 can request to activate the Password Administrator role.

C. Yes

D. No

If User3 wants to activate the Password Administrator role, the user can approve their own request.

E. Yes

F. No

Answer: B, C, F

Q.23

You have the Azure key vaults shown in the following table.

Name	Location	Azure subscription name
KV1	West US	Subscription1
KV2	West US	Subscription1
KV3	East US	Subscription1
KV4	West US	Subscription2
KV5	East US	Subscription2

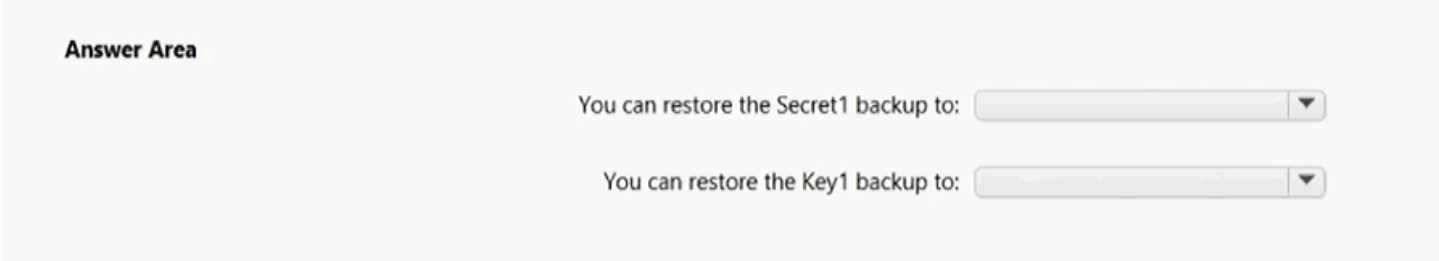
KV1 stores a secret named Secret1 and a key for a managed storage account named Key1.

You back up Secret1 and Key1.

To which key vaults can you restore each backup?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



You can restore the Secret1 backup to:

A. KV1 only
B. KV1 and KV2 only
C. KV1, KV2, and KV3 only
D. KV1, KV2, and KV4 only
E. KV1, KV2, KV3, KV4, and KV5

You can restore the Key1 backup to:

F. KV1 only
G. KV1 and KV2 only
H. KV1, KV2, and KV3 only
I. KV1, KV2, and KV4 only
J. KV1, KV2, KV3, KV4, and KV5

Answer: C, H

Q.24

You have an Azure subscription that contains an Azure key vault named Vault1.

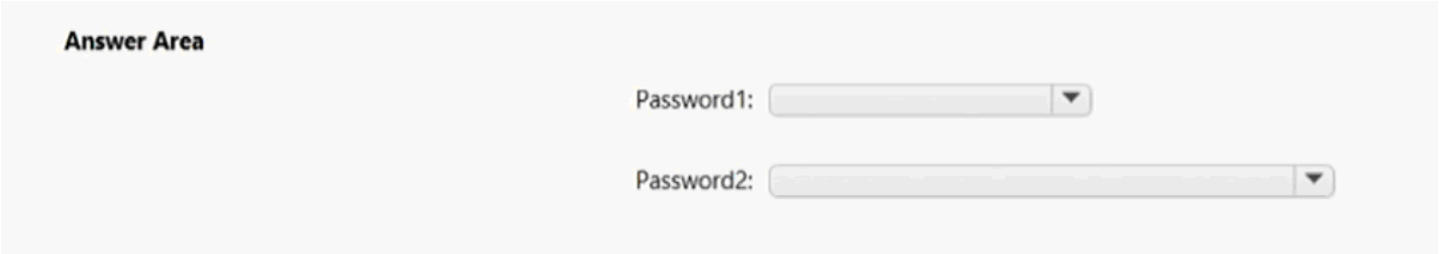
On January1, 2019, Vault1 stores the following secrets. All dates are in the mm/dd/yy format.

```
Enabled     : False
Expires     :
NotBefore   : 5/1/19 12:00:00 AM
Created     : 12/20/18 2:55:00 PM
Updated     : 12/20/18 2:55:00 PM
ContentType :
Tags        :
TagTable    :
VaultName   : vault1
Name        : Password1
Version     :
Id          : https://vault1.vault.azure.net:443/secrets/Password1

Enabled     : True
Expires     : 5/1/19 12:00:00 AM
NotBefore   : 3/1/19 12:00:00 AM
Created     : 12/20/18 3:00:00 PM
Updated     : 12/20/18 3:00:00 PM
ContentType :
Tags        :
TagsTable   :
VaultName   : vault1
Name        : Password2
Version     :
Id          : https://vault1.vault.azure.net:443/secrets/Password2
```

When can each secret be used by an application? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Password1:

A. Never
B. Always
C. Only after May 1, 2019

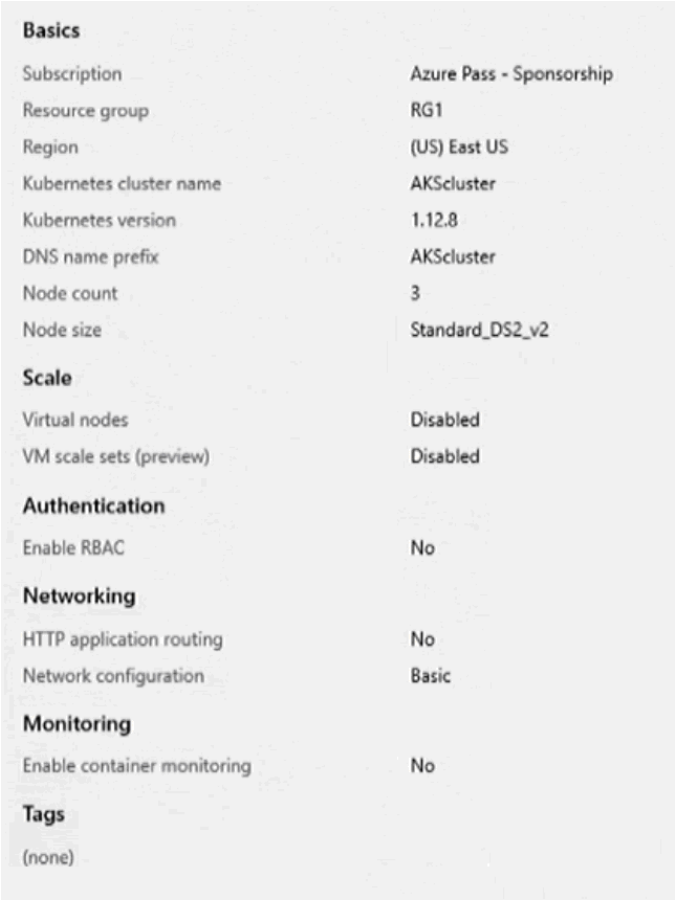
Password2:

D. Never
E. Always
F. Only between March 1, 2019 and May 1, 2019

Answer: A, F

Q.25

You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit.



Basics	
Subscription	Azure Pass - Sponsorship
Resource group	RG1
Region	(US) East US
Kubernetes cluster name	AKScluster
Kubernetes version	1.12.8
DNS name prefix	AKScluster
Node count	3
Node size	Standard_DS2_v2
Scale	
Virtual nodes	Disabled
VM scale sets (preview)	Disabled
Authentication	
Enable RBAC	No
Networking	
HTTP application routing	No
Network configuration	Basic
Monitoring	
Enable container monitoring	No
Tags	
(none)	

You plan to deploy the cluster to production. You disable HTTP application routing.

You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address.

What should you do?

A. Create an AKS Ingress controller.

B. Install the container network interface (CNI) plug-in.

C. Create an Azure Standard Load Balancer.

D. Create an Azure Basic Load Balancer.

Answer: A

Q.26

You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.

You need to use automatically generated service principal for the AKS cluster to authenticate to the Azure Container Registry. What should you create?

A. a secret in Azure Key Vault

B. a role assignment

C. an Azure Active Directory (Azure AD) user

D. an Azure Active Directory (Azure AD) group

Answer: B

Q.27

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Region	Description
HubVNet	East US	HubVNet is a virtual network connected to the on-premises network by using a site-to-site VPN that has BGP route propagation enabled. HubVNet contains subnets named HubVNetSubnet0, AzureFirewallSubnet and GatewaySubnet Virtual network gateway is connected to GatewaySubnet.
SpokeVNet	East US	SpokeVNet is a virtual network connected to HubVNet by using VNet peering. SpokeVNet contains a subnet named SpokeVNetSubnet0

The Azure virtual machines on SpokeVNetSubnet0 can communicate with the computers on the on-premises network.

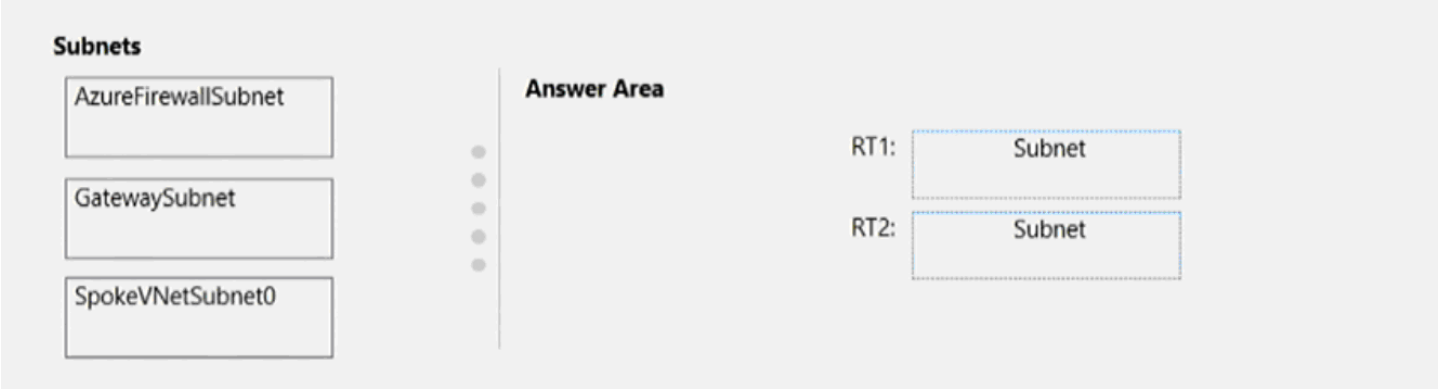
You plan to deploy an Azure firewall to HubVNet.

You create the following two routing tables:

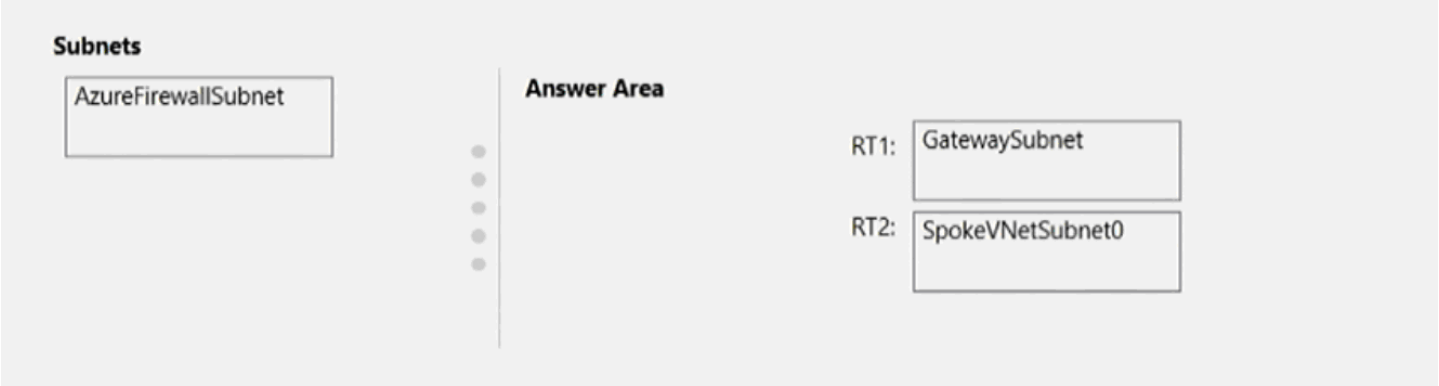
- RT1: Includes a user-defined route that points to the private IP address of the Azure firewall as a next hop address
- RT2: Disables BGP route propagation and defines the private IP address of the Azure firewall as the default gateway.

You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.

To which subnet should you associate each route table? To answer, drag the appropriate subnets to the correct route tables. Each subnet 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.



Answer:



Q.28

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD). The tenant contains the users shown in the following table.

Name	Role	Member of
User1	Security administrator	Group1
User2	Network Contributor	Group2
User3	Key Vault Contributor	Group1, Group2

You have an Azure key vault named Vault1 that has Purge protection set to **Disable**. Vault1 contains the access policies shown in the following table.

Name	Key permission	Secret permission	Certificate permission
Group1	Purge	Purge	Purge
Group2	Select all	Select all	Select all

You create role assignments for Vault1 as shown in the following table.

Name	Role
User1	None
User2	Key Vault Contributor
User3	User Access Administrator

For each of the following statement, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	○	○
User2 can configure firewalls and virtual networks for Vault1.	○	○
User3 can add access policies to Vault1.	○	○

User1 can set Purge protection to Enable for Vault1.

A. Yes

B. No

User2 can configure firewalls and virtual networks for Vault1.

C. Yes

D. No

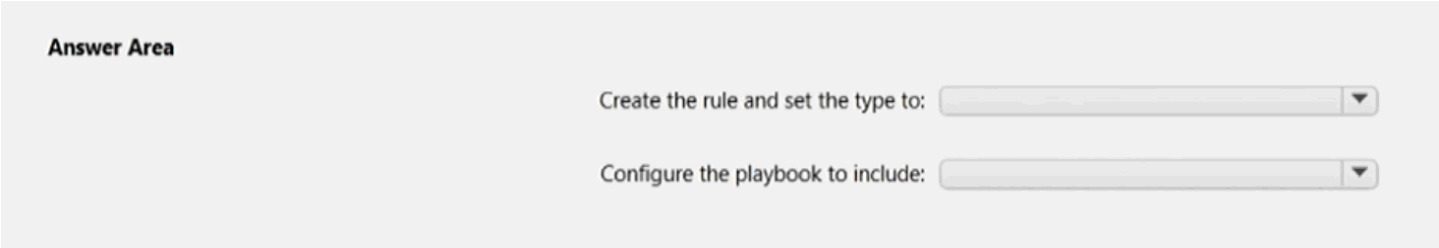
User3 can add access policies to Vault1.

E. Yes

F. No

Answer: B, C, E

Q.29
You have an Azure Sentinel workspace that contains an Azure Active Directory (Azure AD) connector, an Azure Log Analytics query named Query1, and a playbook named Playbook1.
Query1 returns a subnet of security events generated by Azure AD
You plan to create an Azure Sentinel analytic rule based on Query1 that will trigger Playbook1.
You need to ensure that you can add Playbook1 to the new rule.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Create the rule and set the type to:
A. Fusion
B. Microsoft Security incident creation
C. Scheduled

Configure the playbook to include:
D. A managed connector
E. A system-assigned managed identity
F. A trigger
G. Diagnostic settings

Answer: C, F

Q.30
Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com
The company develops an application named App1. App1 is registered in Azure AD.
You need to ensure that App1 can access secrets in Azure Key Vault on behalf of the application users.
What should you configure?
A. a delegated permission without admin consent
B. a delegated permission that requires admin consent
C. a application permission without admin consent
D. a application permission that requires admin consent

Answer: A