**Microsoft.AZ-500.vNov-2024.by.Dien.122q**

Number: AZ-500
Passing Score: 800
Time Limit: 120
File Version: 16.0

# Exam Code: AZ-500
# Exam Name: Microsoft Azure Security Technologies

**01 - Implement platform protection**

This is a case study.

Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

General Overview

Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.

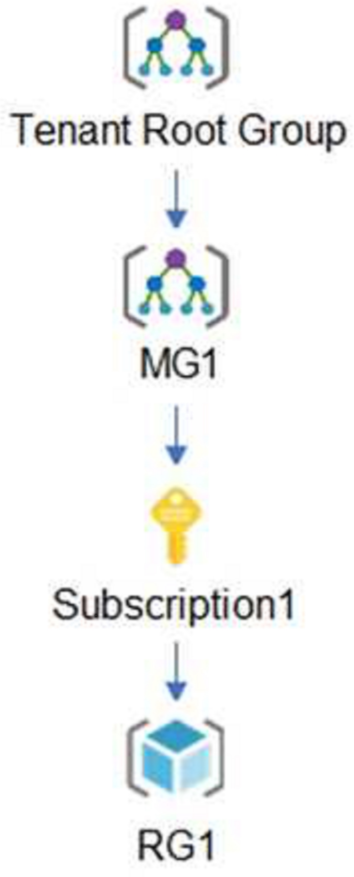
Existing Environment

Network Environment

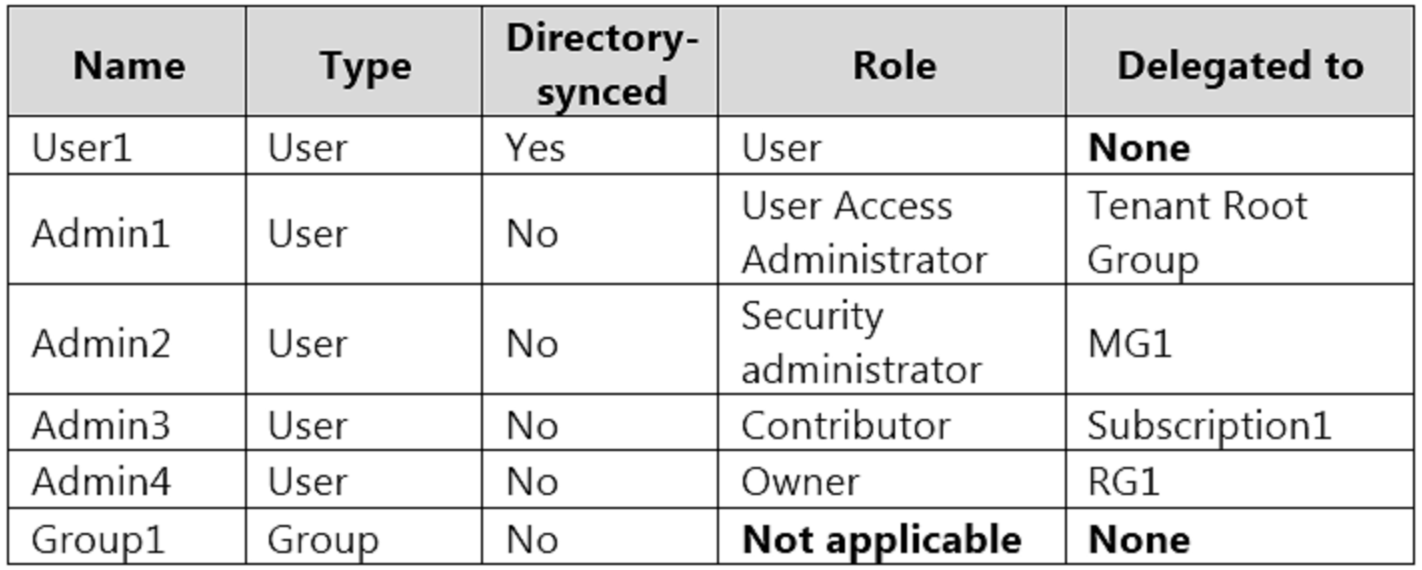
Fabrikam has a Microsoft 365 subscription and an Azure subscription named subscription1.

The network contains an on-premises Active Directory domain named Fabrikam.com. The domain contains two organizational units (OUs) named OU1 and OU2. Azure AD Connect cloud sync syncs only OU1.

The Azure resources hierarchy is shown in the following exhibit.

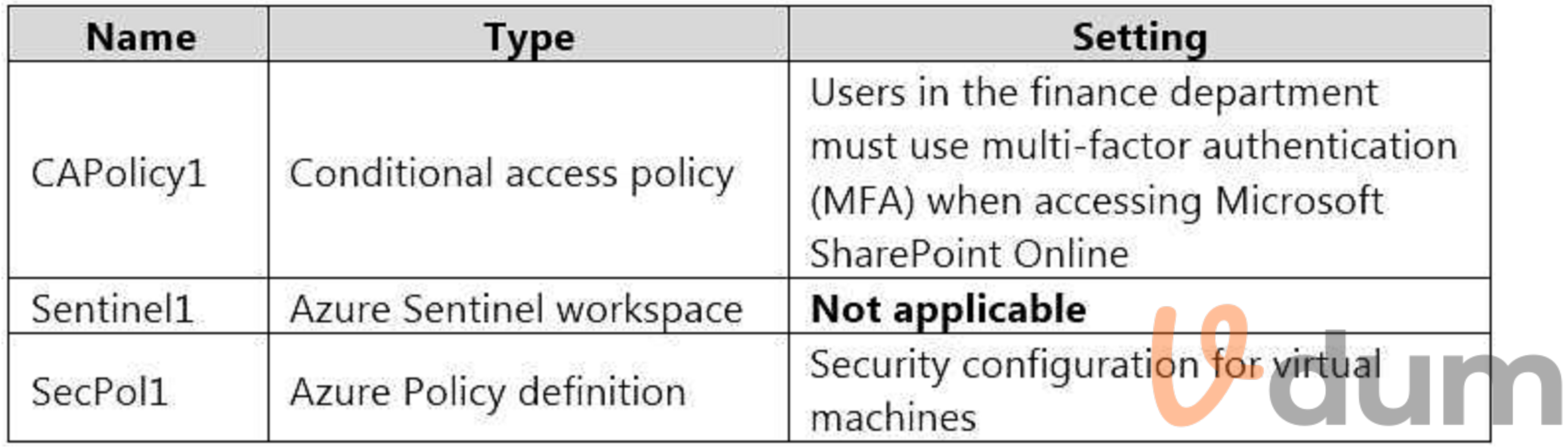


The Azure Active Directory (Azure AD) tenant contains the users shown in the following table.



| Name | Type | Directory-synced | Role | Delegated to |
|---|---|---|---|---|
| User1 | User | Yes | User | **None** |
| Admin1 | User | No | User Access Administrator | Tenant Root Group |
| Admin2 | User | No | Security administrator | MG1 |
| Admin3 | User | No | Contributor | Subscription1 |
| Admin4 | User | No | Owner | RG1 |
| Group1 | Group | No | **Not applicable** | **None** |

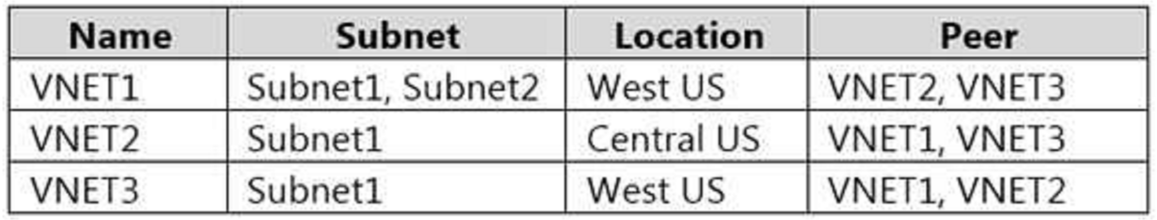
Azure AD contains the resources shown in the following table.



| Name | Type | Setting |
|---|---|---|
| CAPolicy1 | Conditional access policy | Users in the finance department must use multi-factor authentication (MFA) when accessing Microsoft SharePoint Online |
| Sentinel1 | Azure Sentinel workspace | **Not applicable** |
| SecPol1 | Azure Policy definition | Security configuration for virtual machines |

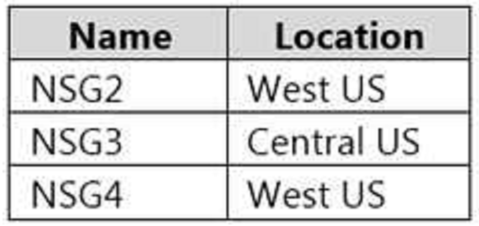
Subscription1 Resources

Subscription1 contains the virtual networks shown in the following table.



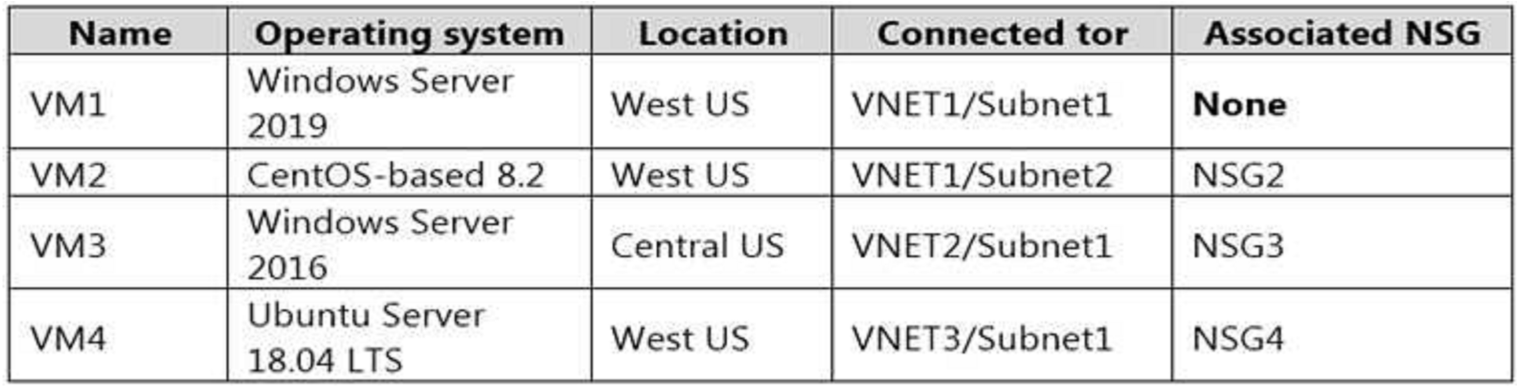
| Name | Subnet | Location | Peer |
|---|---|---|---|
| VNET1 | Subnet1, Subnet2 | West US | VNET2, VNET3 |
| VNET2 | Subnet1 | Central US | VNET1, VNET3 |
| VNET3 | Subnet1 | West US | VNET1, VNET2 |

Subscription1 contains the network security groups (NSGs) shown in the following table.



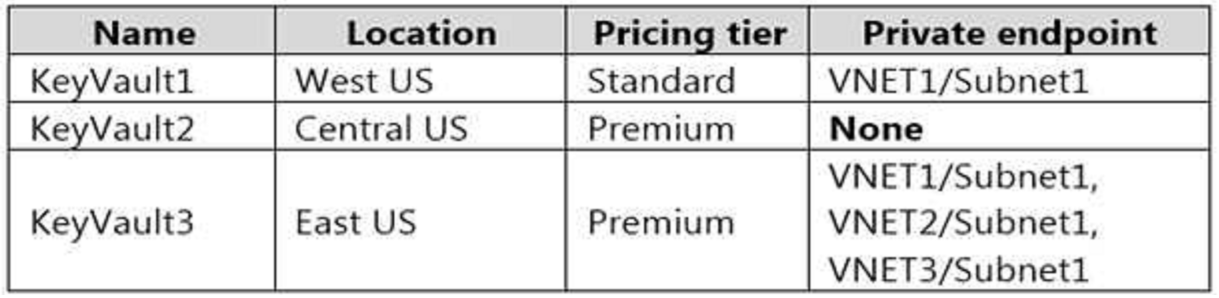
| Name | Location |
|---|---|
| NSG2 | West US |
| NSG3 | Central US |
| NSG4 | West US |

Subscription1 contains the virtual machines shown in the following table.



| Name | Operating system | Location | Connected tor | Associated NSG |
|---|---|---|---|---|
| VM1 | Windows Server 2019 | West US | VNET1/Subnet1 | **None** |
| VM2 | CentOS-based 8.2 | West US | VNET1/Subnet2 | NSG2 |
| VM3 | Windows Server 2016 | Central US | VNET2/Subnet1 | NSG3 |
| VM4 | Ubuntu Server 18.04 LTS | West US | VNET3/Subnet1 | NSG4 |

Subscription1 contains the Azure key vaults shown in the following table.



| Name | Location | Pricing tier | Private endpoint |
|---|---|---|---|
| KeyVault1 | West US | Standard | VNET1/Subnet1 |
| KeyVault2 | Central US | Premium | **None** |
| KeyVault3 | East US | Premium | VNET1/Subnet1,<br>VNET2/Subnet1,<br>VNET3/Subnet1 |

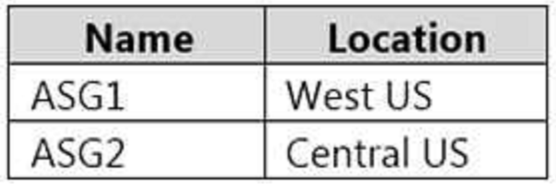
Subscription1 contains a storage account named storage1 in the West US Azure region.

Planned Changes and Requirements

Planned Changes

Fabrikam plans to implement the following changes:

Create two application security groups as shown in the following table.



| Name | Location |
|---|---|
| ASG1 | West US |
| ASG2 | Central US |

Associate the network interface of VM1 to ASG1.

Deploy SecPol1 by using Azure Security Center.

Deploy a third-party app named App1. A version of App1 exists for all available operating systems.

Create a resource group named RG2.

Sync OU2 to Azure AD.

Add User1 to Group1.

Technical Requirements

Fabrikam identifies the following technical requirements:

The finance department users must reauthenticate after three hours when they access SharePoint Online. Storage1 must be encrypted by using customer-managed keys and automatic key rotation.

From Sentinel1, you must ensure that the following notebooks can be launched:

- Entity Explorer – Account
- Entity Explorer – Windows Host
- Guided Investigation Process Alerts

VM1, VM2, and VM3 must be encrypted by using Azure Disk Encryption.

Just in time (JIT) VM access for VM1, VM2, and VM3 must be enabled.

App1 must use a secure connection string stored in KeyVault1.

KeyVault1 traffic must NOT travel over the internet.

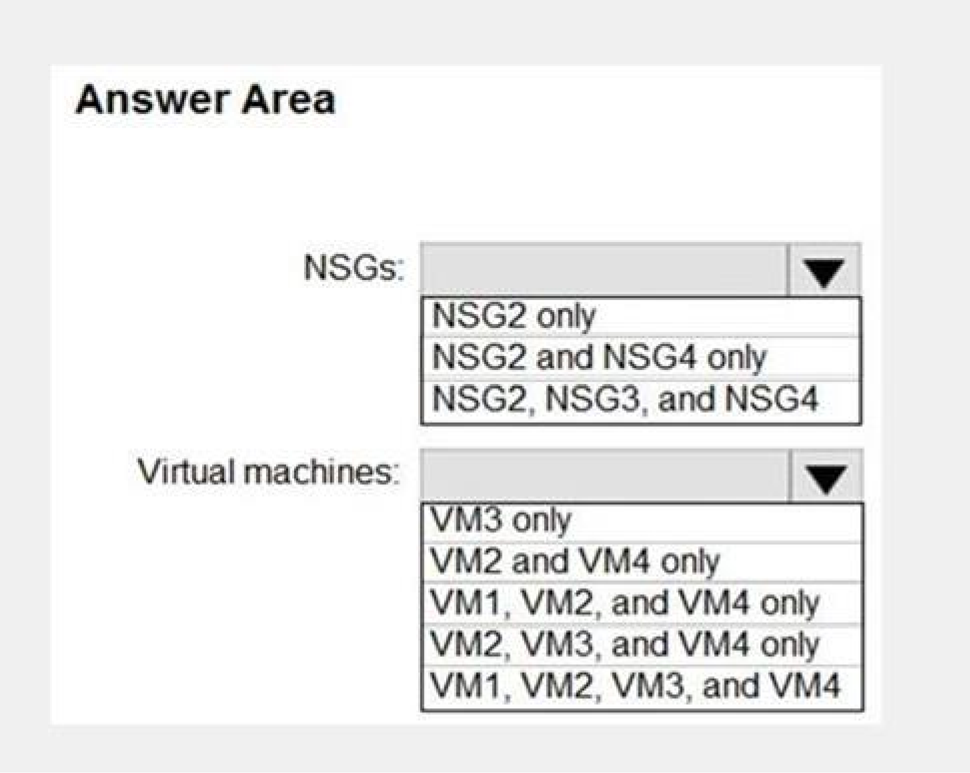
**QUESTION 1**

HOTSPOT

You implement the planned changes for ASG1 and ASG2.

In which NSGs can you use ASG1, and the network interfaces of which virtual machines can you assign to ASG2?

**Hot Area:**



Answer Area

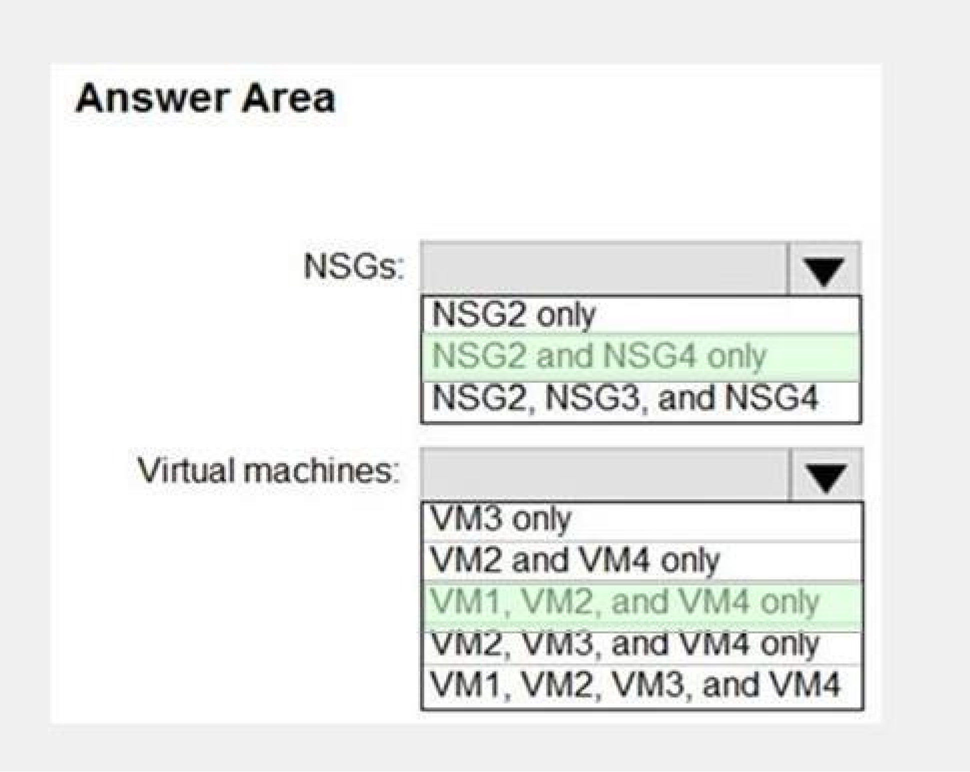
NSGs: ▼

NSG2 only
NSG2 and NSG4 only
NSG2, NSG3, and NSG4

Virtual machines: ▼

VM3 only
VM2 and VM4 only
VM1, VM2, and VM4 only
VM2, VM3, and VM4 only
VM1, VM2, VM3, and VM4

**Answer Area:**



Answer Area

NSGs: ▼

NSG2 only
[✓ NSG2 and NSG4 only]
NSG2, NSG3, and NSG4

Virtual machines: ▼

VM3 only
VM2 and VM4 only
[✓ VM1, VM2, and VM4 only]
VM2, VM3, and VM4 only
VM1, VM2, VM3, and VM4

**Section:**
**Explanation:**

**QUESTION 2**
You plan to implement JIT VM access.
Which virtual machines will be supported?

A. VM2, VM3, and VM4 only

B. VM1, VM2, VM3, and VM4

C. VM1 and VM3 only

D. VM1 only

**Correct Answer: C**
**Section:**

**QUESTION 3**

You plan to configure Azure Disk Encryption for VM4.
Which key vault can you use to store the encryption key?

A. KeyVault1

B. KeyVault2

C. KeyVault3

**Correct Answer: A**
**Section:**
**Explanation:**
The key vault needs to be in the same subscription and same region as the VM.
VM4 is in West US. KeyVault1 is the only key vault in the same region as the VM.
Reference: https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault

**QUESTION 4**

You need to encrypt storage1 to meet the technical requirements.
Which key vaults can you use?

A. KeyVault2 and KeyVault3 only

B. KeyVault1 only

C. KeyVault1 and KeyVault3 only

D. KeyVault1, KeyVault2, and KeyVault3

**Correct Answer: A**
**Section:**
**Explanation:**

**02 - Implement platform protection**

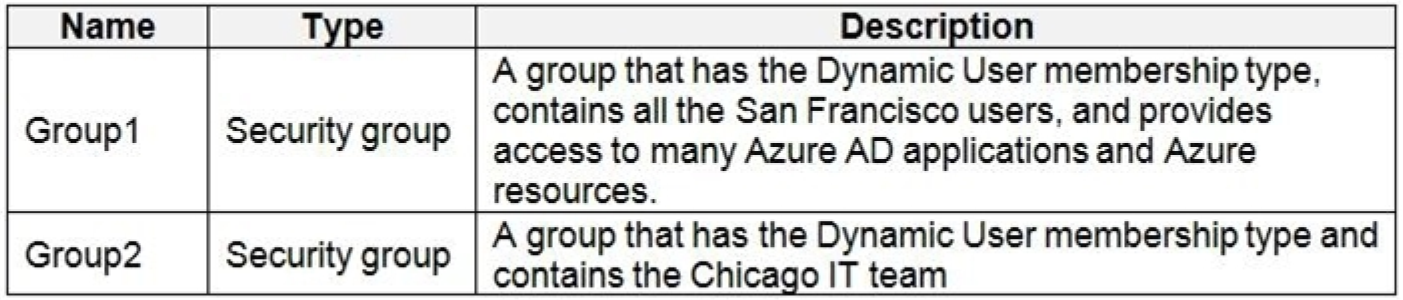
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview
Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

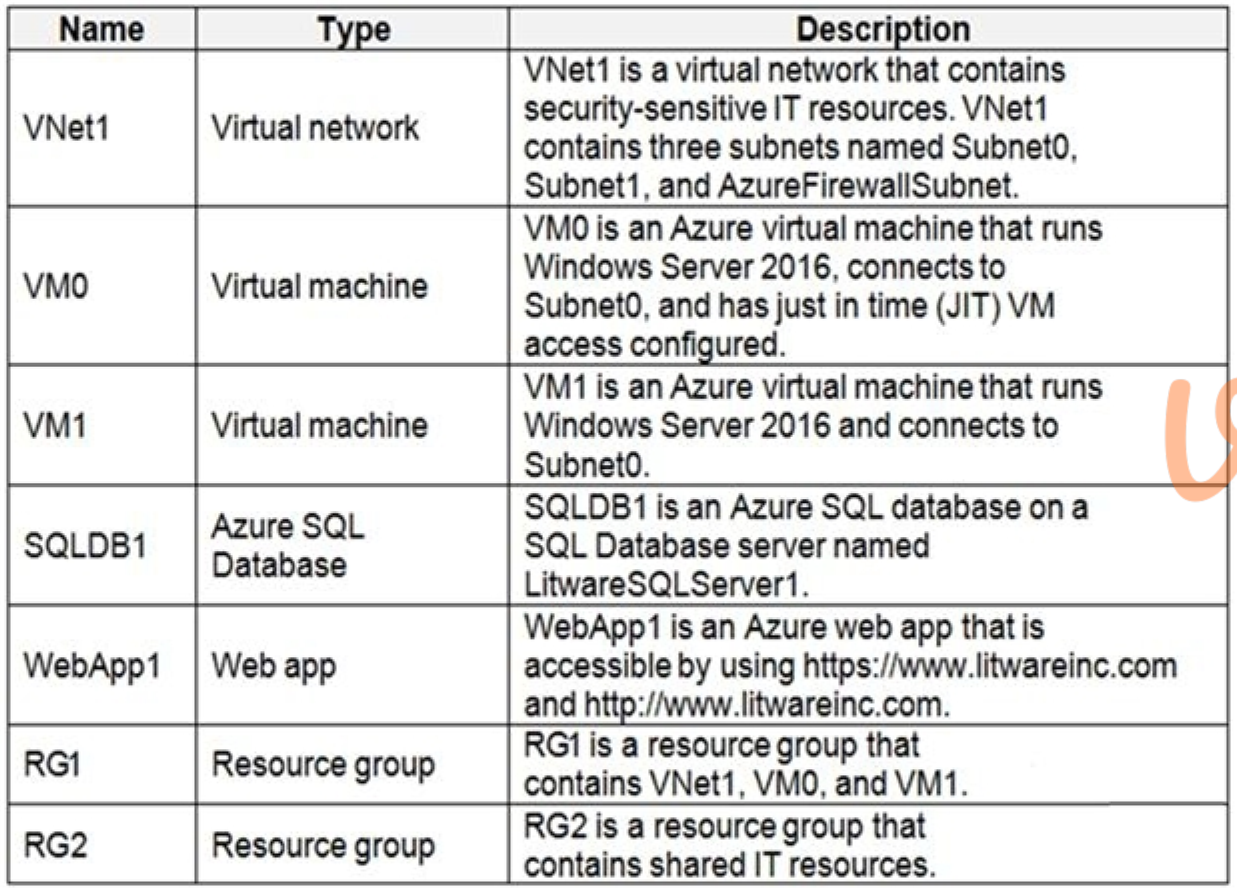
Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.



| Name | Type | Description |
|---|---|---|
| Group1 | Security group | A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources. |
| Group2 | Security group | A group that has the Dynamic User membership type and contains the Chicago IT team |

The Azure subscription contains the objects shown in the following table.



| Name | Type | Description |
|---|---|---|
| VNet1 | Virtual network | VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet. |
| VM0 | Virtual machine | VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured. |
| VM1 | Virtual machine | VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0. |
| SQLDB1 | Azure SQL Database | SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1. |
| WebApp1 | Web app | WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com. |
| RG1 | Resource group | RG1 is a resource group that contains VNet1, VM0, and VM1. |
| RG2 | Resource group | RG2 is a resource group that contains shared IT resources. |

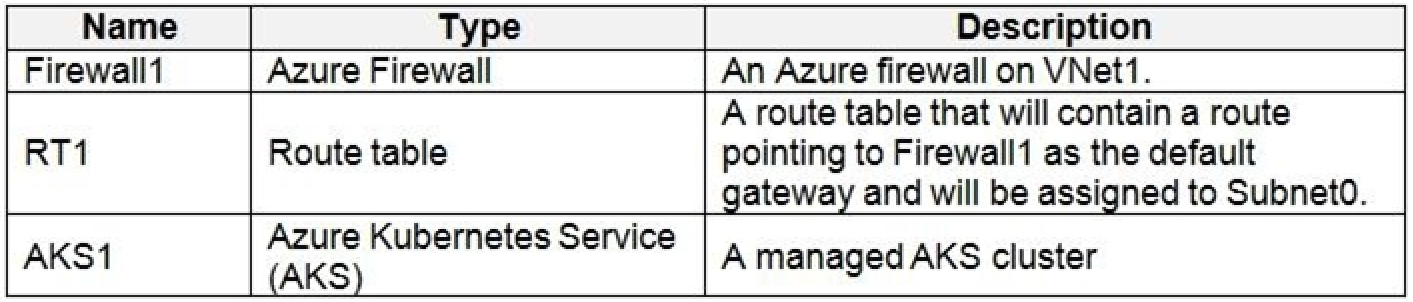
Identity and Access Requirements

Azure Security Center is set to the Standard tier.

Requirements

Planned Changes

Litware plans to deploy the Azure resources shown in the following table.



| Name | Type | Description |
|---|---|---|
| Firewall1 | Azure Firewall | An Azure firewall on VNet1. |
| RT1 | Route table | A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0. |
| AKS1 | Azure Kubernetes Service (AKS) | A managed AKS cluster |

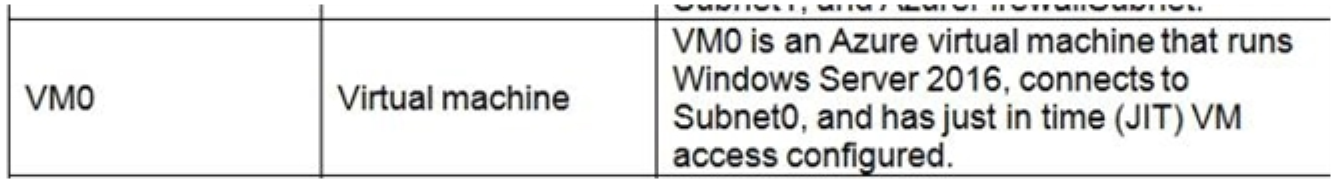
Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.
The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment. Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.
Platform Protection Requirements
Litware identifies the following platform protection requirements:
Microsoft Antimalware must be installed on the virtual machines in RG1.
The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.
Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access. A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.
Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center. Data and Application Requirements
Litware identifies the following data and applications requirements:
The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.
WebApp1 must enforce mutual authentication.
General Requirements
Litware identifies the following general requirements:
Whenever possible, administrative effort must be minimized.
Whenever possible, use of automation must be maximized.

**QUESTION 1**
You need to ensure that users can access VM0. The solution must meet the platform protection requirements. What should you do?

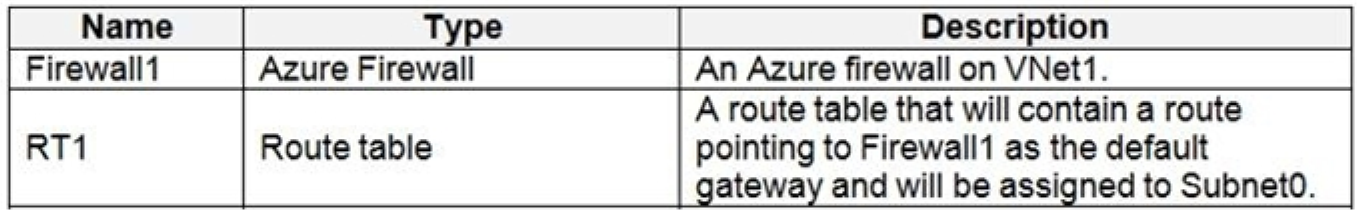
A. Move VM0 to Subnet1.
B. On Firewall, configure a network traffic filtering rule.
C. Assign RT1 to AzureFirewallSubnet.
D. On Firewall, configure a DNAT rule.

**Correct Answer: A**
**Section:**
**Explanation:**
Azure Firewall has the following known issue:
Conflict with Azure Security Center (ASC) Just-in-Time (JIT) feature.
If a virtual machine is accessed using JIT, and is in a subnet with a user-defined route that points to Azure Firewall as a default gateway, ASC JIT doesn't work. This is a result of asymmetric routing – a packet comes in via the virtual machine public IP (JIT opened the access), but the return path is via the firewall, which drops the packet because there is no established session on the firewall.
Solution: To work around this issue, place the JIT virtual machines on a separate subnet that doesn't have a user-defined route to the firewall.
Scenario:



| | | |
|---|---|---|
| | | Subnet1, and AzureFirewallSubnet. |
| VM0 | Virtual machine | VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured. |

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.



| Name | Type | Description |
|---|---|---|
| Firewall1 | Azure Firewall | An Azure firewall on VNet1. |
| RT1 | Route table | A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0. |

References:
https://docs.microsoft.com/en-us/azure/firewall/overview

**QUESTION 2**

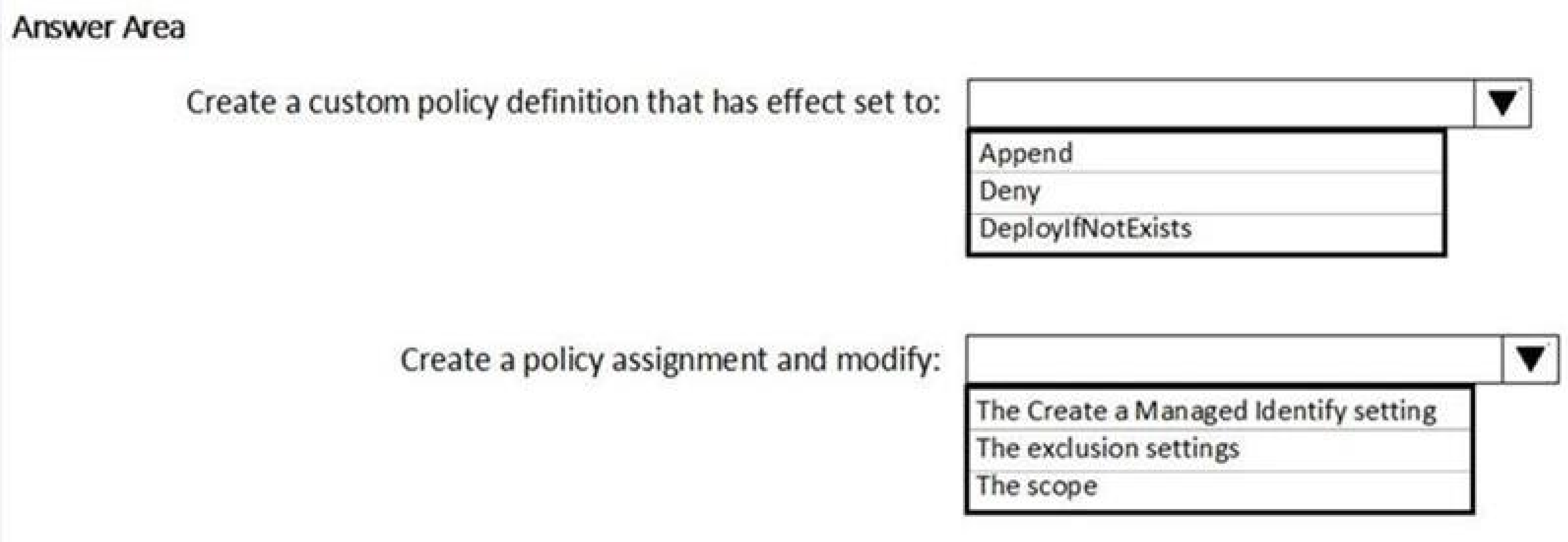
HOTSPOT

You need to deploy Microsoft Antimalware to meet the platform protection requirements.

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

NOTE: Each correct selection is worth one point.

**Hot Area:**



Answer Area

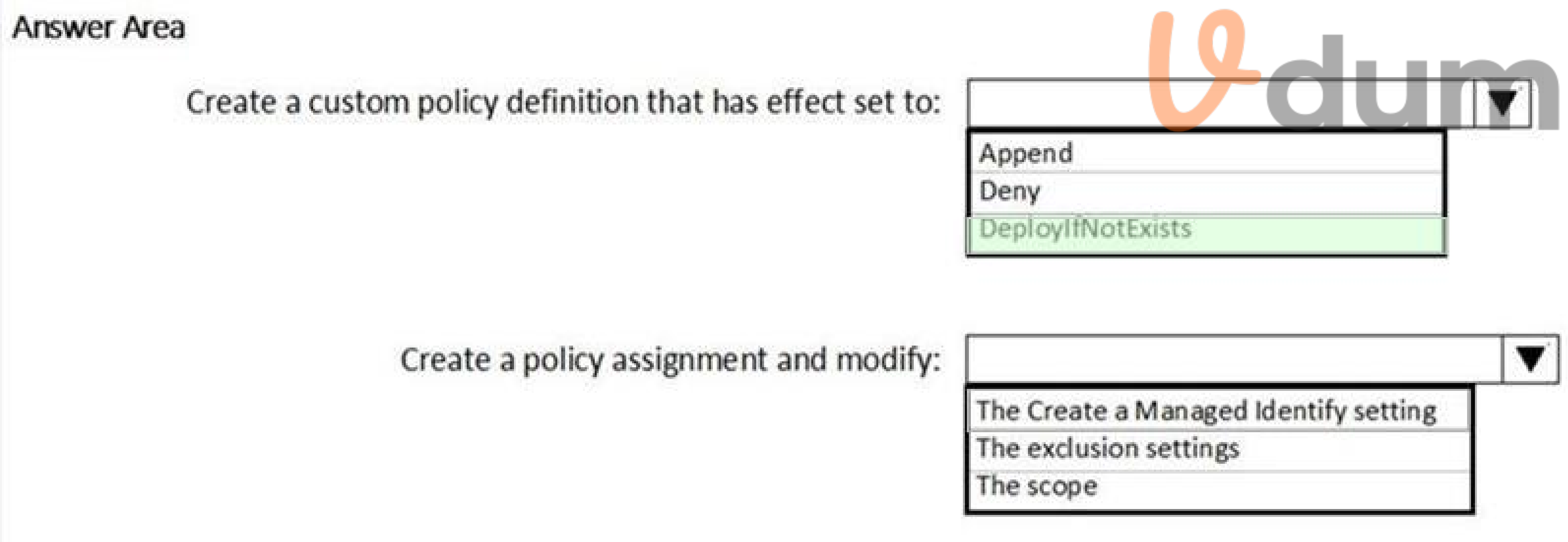
Create a custom policy definition that has effect set to:

- Append
- Deny
- DeployIfNotExists

Create a policy assignment and modify:

- The Create a Managed Identify setting
- The exclusion settings
- The scope

**Answer Area:**



Answer Area

Create a custom policy definition that has effect set to:

- Append
- Deny
- [✓ DeployIfNotExists]

Create a policy assignment and modify:

- The Create a Managed Identify setting
- The exclusion settings
- The scope

**Section:**

**Explanation:**

Scenario: Microsoft Antimalware must be installed on the virtual machines in RG1.

RG1 is a resource group that contains Vnet1, VM0, and VM1.

Box 1: DeployIfNotExists

DeployIfNotExists executes a template deployment when the condition is met.

Azure policy definition Antimalware

Incorrect Answers:

Append:

Append is used to add additional fields to the requested resource during creation or update. A common example is adding tags on resources such as costCenter or specifying allowed IPs for a storage resource.

Deny:

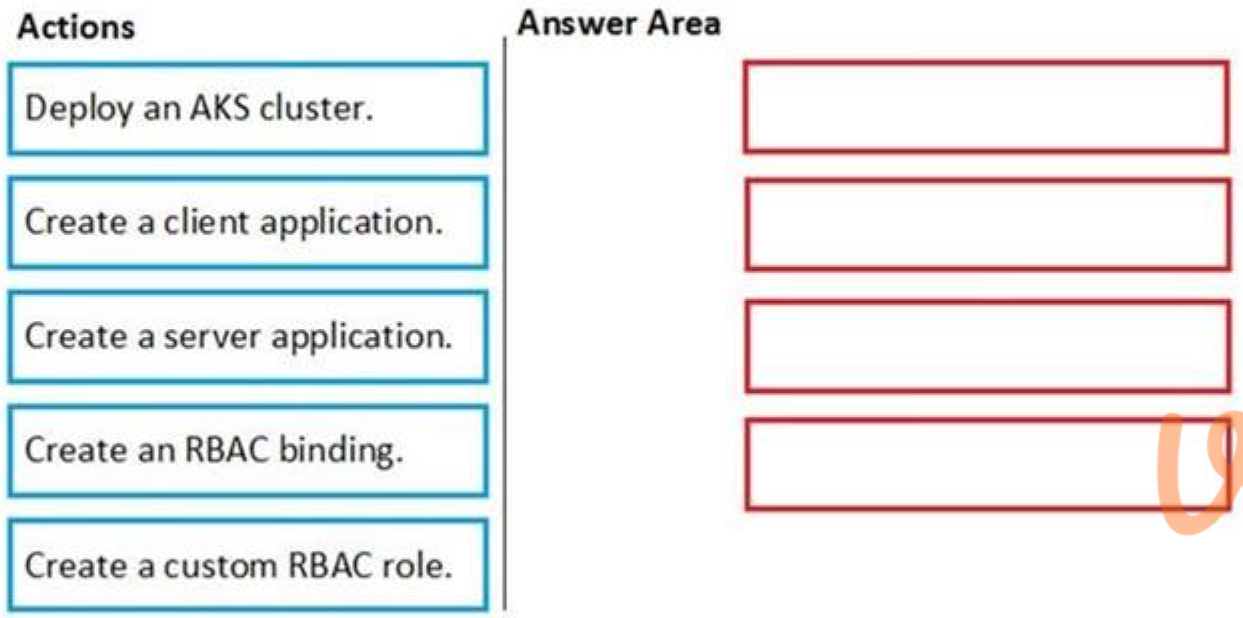
Deny is used to prevent a resource request that doesn't match defined standards through a policy definition and fails the request.

Box 2: The Create a Managed Identity setting

When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity. Azure Policy creates a managed identity for each assignment, but must have details about what roles to grant the managed identity.
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

**QUESTION 3**
DRAG DROP
You need to deploy AKS1 to meet the platform protection requirements.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

**Select and Place:**

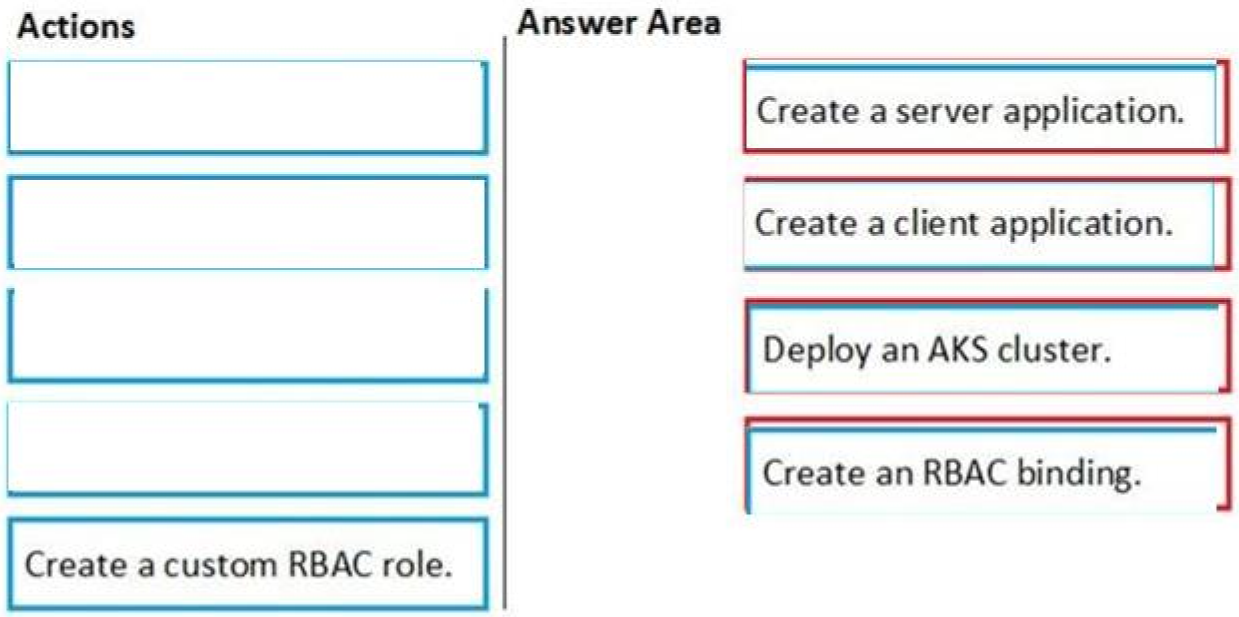


Actions

- Deploy an AKS cluster.
- Create a client application.
- Create a server application.
- Create an RBAC binding.
- Create a custom RBAC role.

Answer Area

**Correct Answer:**



Actions

- Create a custom RBAC role.

Answer Area

- Create a server application.
- Create a client application.
- Deploy an AKS cluster.
- Create an RBAC binding.

**Section:**
**Explanation:**
Scenario: Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.

Litewire plans to deploy AKS1, which is a managed AKS (Azure Kubernetes Services) cluster.

Step 1: Create a server application

To provide Azure AD authentication for an AKS cluster, two Azure AD applications are created. The first application is a server component that provides user authentication.

Step 2: Create a client application

The second application is a client component that's used when you're prompted by the CLI for authentication. This client application uses the server application for the actual authentication of the credentials provided by the client.

Step 3: Deploy an AKS cluster.

Use the az group create command to create a resource group for the AKS cluster.

Use the az aks create command to deploy the AKS cluster.

Step 4: Create an RBAC binding.

Before you use an Azure Active Directory account with an AKS cluster, you must create role-binding or cluster role-binding. Roles define the permissions to grant, and bindings apply them to desired users. These assignments can be applied to a given namespace, or across the entire cluster.

Reference:

https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration

**03 - Implement platform protection**

Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

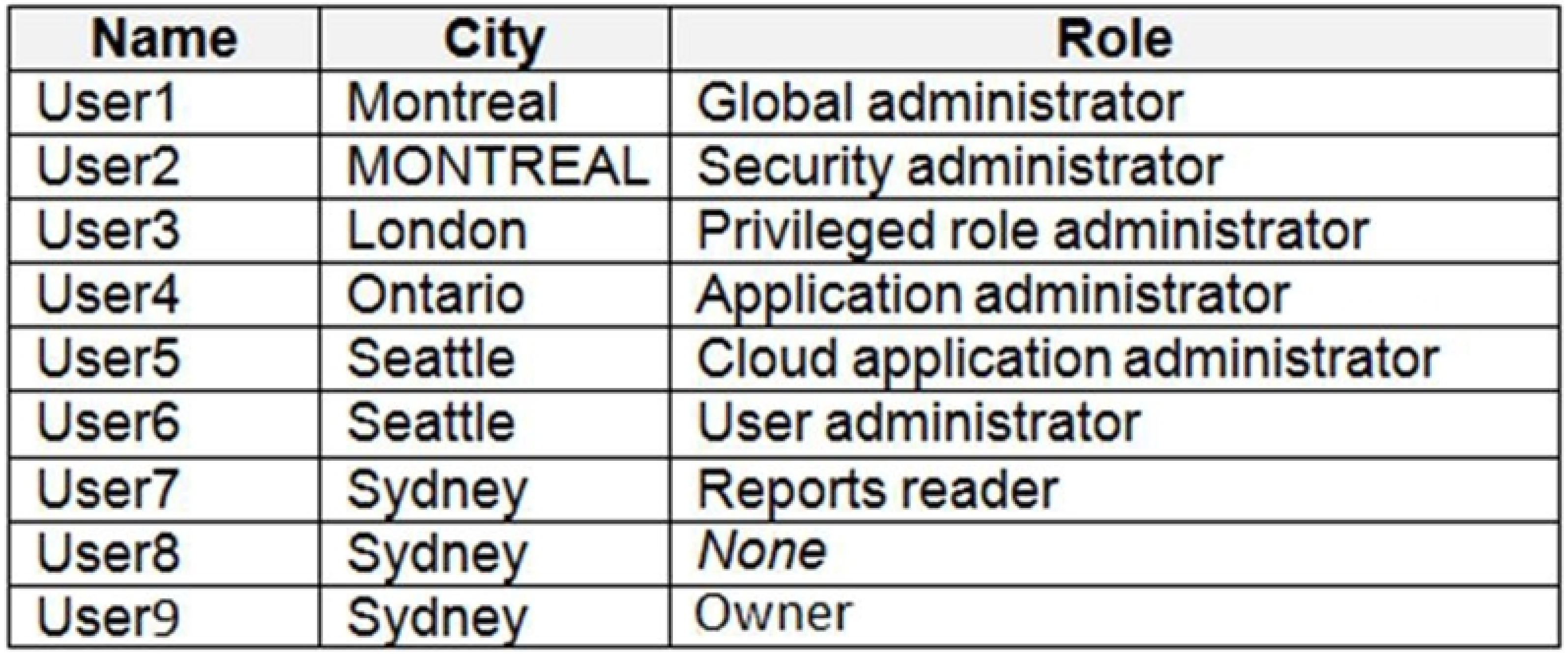
The company hosts its entire server infrastructure in Azure.

Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

Existing Environment

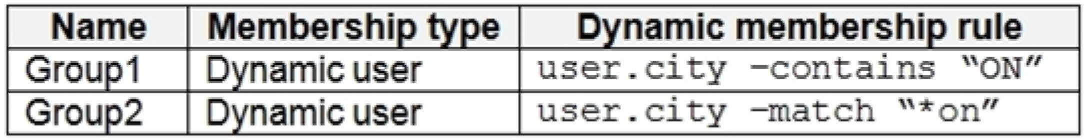
Azure AD

Contoso.com contains the users shown in the following table.



| Name | City | Role |
|---|---|---|
| User1 | Montreal | Global administrator |
| User2 | MONTREAL | Security administrator |
| User3 | London | Privileged role administrator |
| User4 | Ontario | Application administrator |
| User5 | Seattle | Cloud application administrator |
| User6 | Seattle | User administrator |
| User7 | Sydney | Reports reader |
| User8 | Sydney | *None* |
| User9 | Sydney | Owner |

Contoso.com contains the security groups shown in the following table.

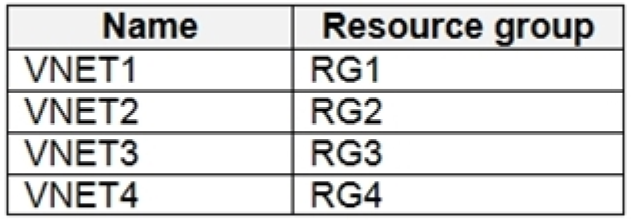


| Name | Membership type | Dynamic membership rule |
|---|---|---|
| Group1 | Dynamic user | `user.city -contains “ON”` |
| Group2 | Dynamic user | `user.city -match “*on”` |

Sub1

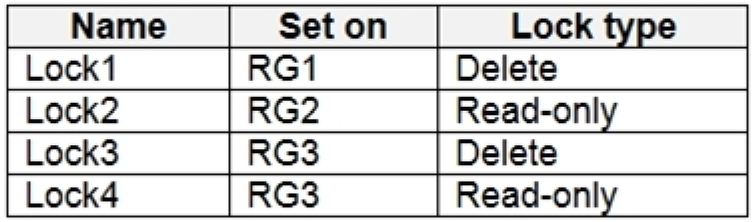
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.



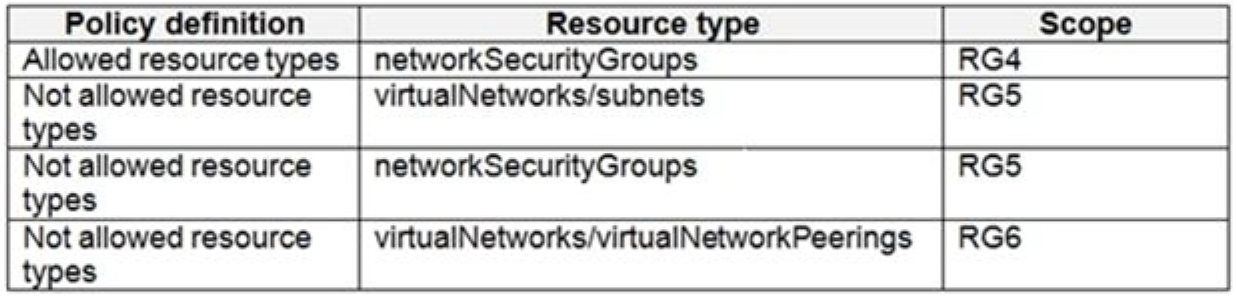
| Name | Resource group |
|---|---|
| VNET1 | RG1 |
| VNET2 | RG2 |
| VNET3 | RG3 |
| VNET4 | RG4 |

Sub1 contains the locks shown in the following table.



| Name | Set on | Lock type |
|---|---|---|
| Lock1 | RG1 | Delete |
| Lock2 | RG2 | Read-only |
| Lock3 | RG3 | Delete |
| Lock4 | RG3 | Read-only |

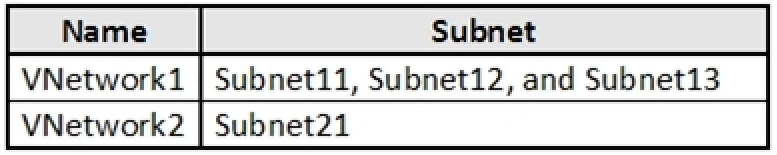
Sub1 contains the Azure policies shown in the following table.



| Policy definition | Resource type | Scope |
|---|---|---|
| Allowed resource types | networkSecurityGroups | RG4 |
| Not allowed resource types | virtualNetworks/subnets | RG5 |
| Not allowed resource types | networkSecurityGroups | RG5 |
| Not allowed resource types | virtualNetworks/virtualNetworkPeerings | RG6 |

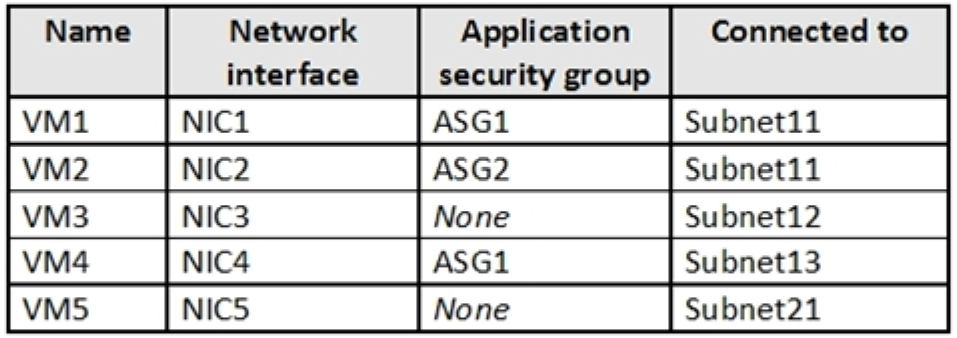
Sub2

Sub2 contains the virtual networks shown in the following table.



| Name | Subnet |
|---|---|
| VNetwork1 | Subnet11, Subnet12, and Subnet13 |
| VNetwork2 | Subnet21 |

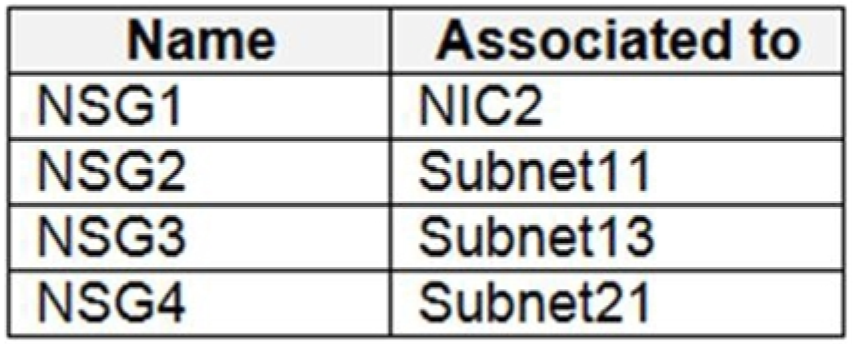
Sub2 contains the virtual machines shown in the following table.



| Name | Network interface | Application security group | Connected to |
|---|---|---|---|
| VM1 | NIC1 | ASG1 | Subnet11 |
| VM2 | NIC2 | ASG2 | Subnet11 |
| VM3 | NIC3 | *None* | Subnet12 |
| VM4 | NIC4 | ASG1 | Subnet13 |
| VM5 | NIC5 | *None* | Subnet21 |

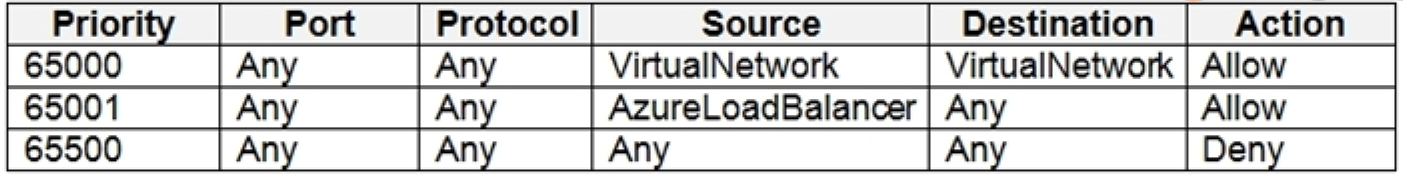
All virtual machines have public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

Sub2 contains the network security groups (NSGs) shown in the following table.



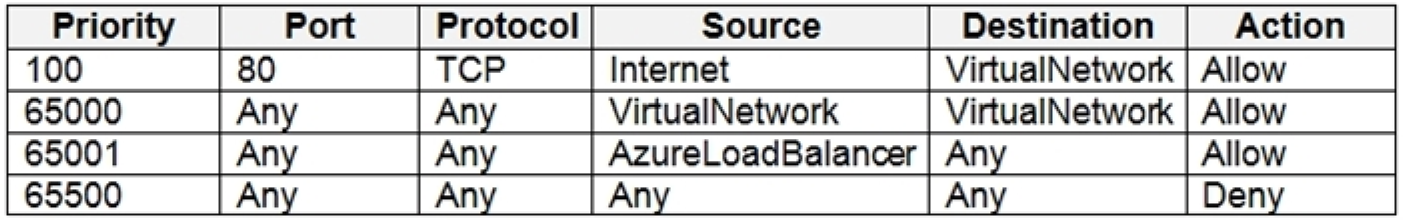
| Name | Associated to |
|---|---|
| NSG1 | NIC2 |
| NSG2 | Subnet11 |
| NSG3 | Subnet13 |
| NSG4 | Subnet21 |

NSG1 has the inbound security rules shown in the following table.



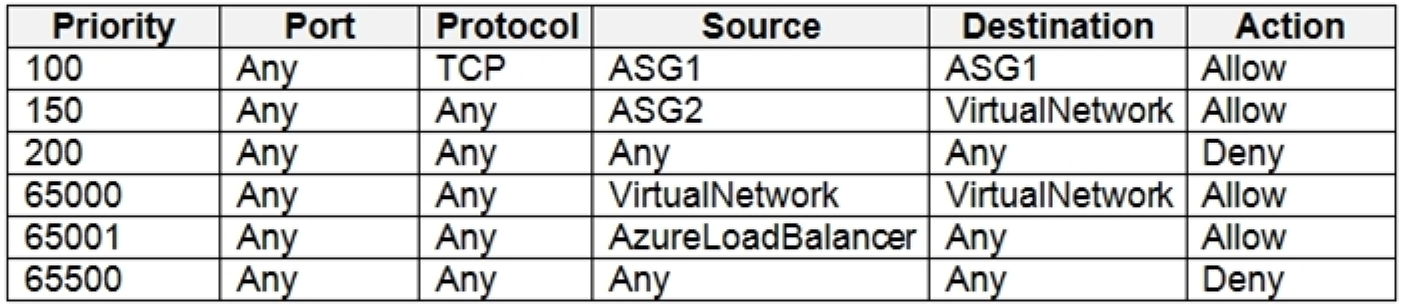
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

NSG2 has the inbound security rules shown in the following table.



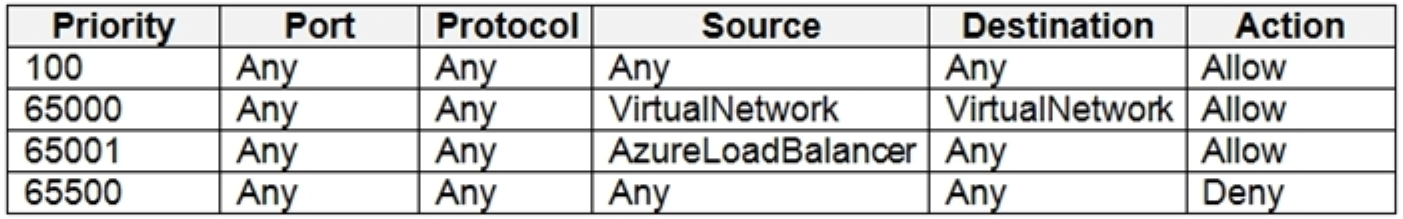
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 100 | 80 | TCP | Internet | VirtualNetwork | Allow |
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

NSG3 has the inbound security rules shown in the following table.



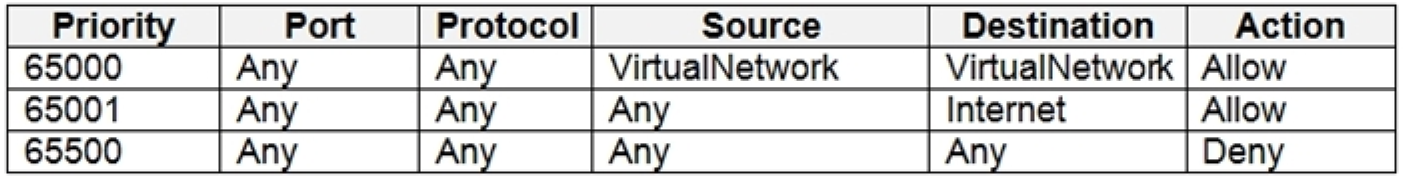
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 100 | Any | TCP | ASG1 | ASG1 | Allow |
| 150 | Any | Any | ASG2 | VirtualNetwork | Allow |
| 200 | Any | Any | Any | Any | Deny |
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

NSG4 has the inbound security rules shown in the following table.



| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 100 | Any | Any | Any | Any | Allow |
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

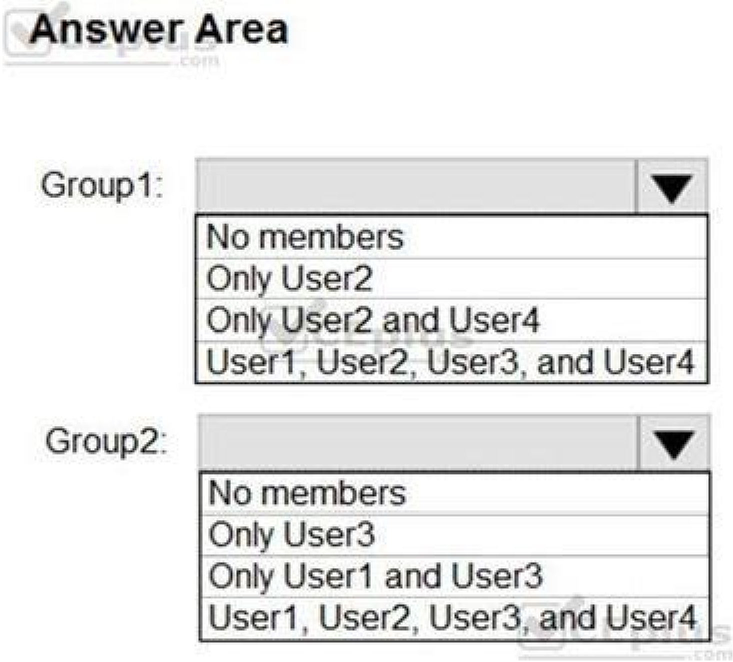


| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | Any | Internet | Allow |
| 65500 | Any | Any | Any | Any | Deny |

Technical requirements
Contoso identifies the following technical requirements:
Deploy Azure Firewall to VNetwork1 in Sub2.
Register an application named App2 in contoso.com.
Whenever possible, use the principle of least privilege.
Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

**QUESTION 1**
HOTSPOT
What is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Hot Area:**

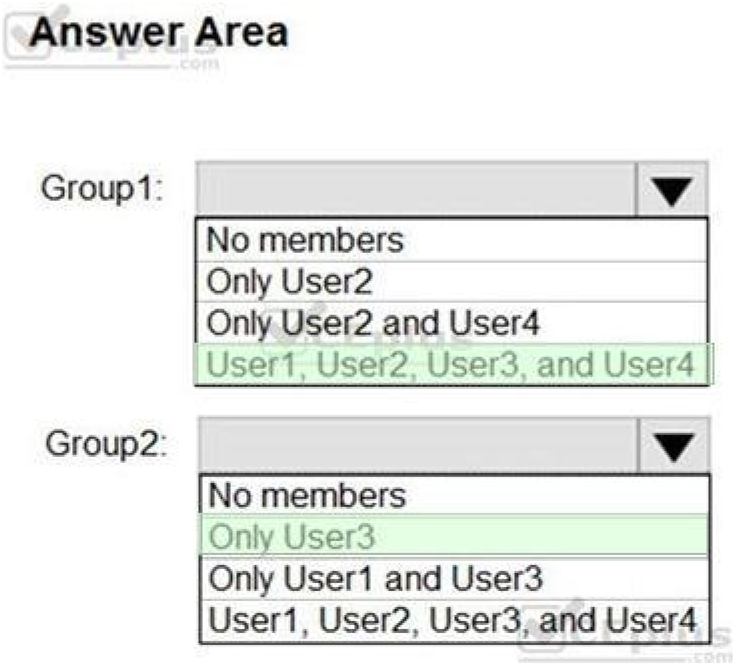


Answer Area

Group1:
- No members
- Only User2
- Only User2 and User4
- User1, User2, User3, and User4

Group2:
- No members
- Only User3
- Only User1 and User3
- User1, User2, User3, and User4

**Answer Area:**



Answer Area

Group1:

- No members
- Only User2
- Only User2 and User4
- [✓ User1, User2, User3, and User4]

Group2:

- No members
- [✓ Only User3]
- Only User1 and User3
- User1, User2, User3, and User4

**Section:**

**Explanation:**

Box 1: User1, User2, User3, User4

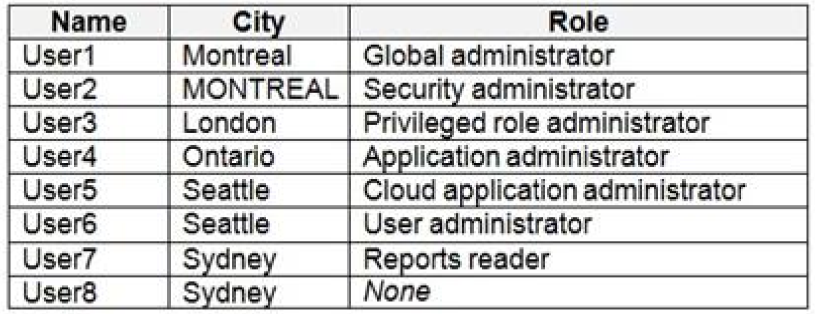
Contains "ON" is true for Montreal (User1), MONTREAL (User2), London (User 3), and Ontario (User4) as string and regex operations are not case sensitive.

Box 2: Only User3

Match "*on" is only true for London (User3).

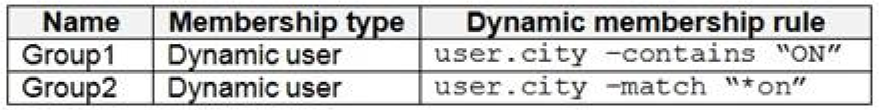
Scenario:

Contoso.com contains the users shown in the following table.



| Name | City | Role |
|---|---|---|
| User1 | Montreal | Global administrator |
| User2 | MONTREAL | Security administrator |
| User3 | London | Privileged role administrator |
| User4 | Ontario | Application administrator |
| User5 | Seattle | Cloud application administrator |
| User6 | Seattle | User administrator |
| User7 | Sydney | Reports reader |
| User8 | Sydney | *None* |

Contoso.com contains the security groups shown in the following table.



| Name | Membership type | Dynamic membership rule |
|---|---|---|
| Group1 | Dynamic user | `user.city -contains "ON"` |
| Group2 | Dynamic user | `user.city -match "*on"` |

References:

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership

**QUESTION 2**

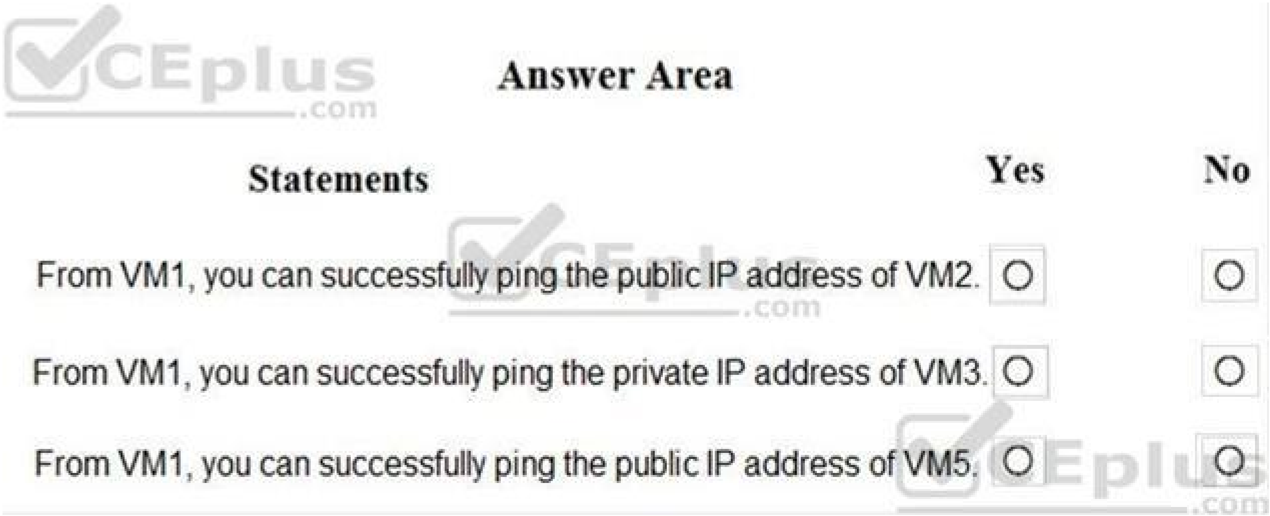
HOTSPOT

You are evaluating the security of the network communication between the virtual machines in Sub2.

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

NOTE: Each correct selection is worth one point.

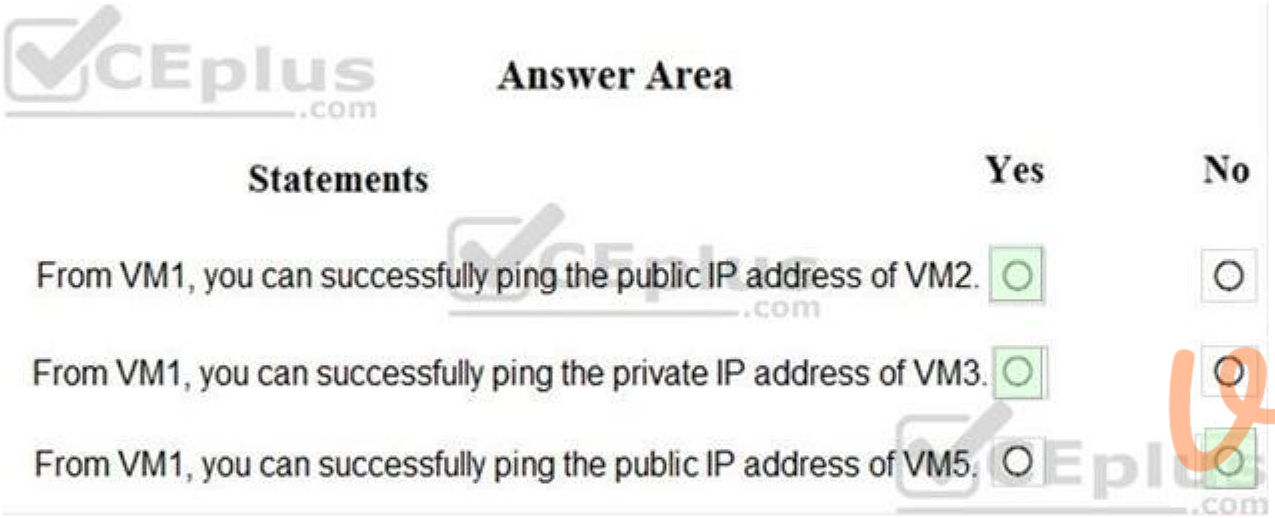
**Hot Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| From VM1, you can successfully ping the public IP address of VM2. | ○ | ○ |
| From VM1, you can successfully ping the private IP address of VM3. | ○ | ○ |
| From VM1, you can successfully ping the public IP address of VM5. | ○ | ○ |

**Answer Area:**



Answer Area

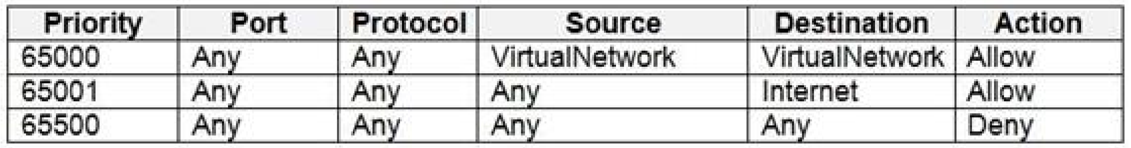
| Statements | Yes | No |
|---|---|---|
| From VM1, you can successfully ping the public IP address of VM2. | ● | ○ |
| From VM1, you can successfully ping the private IP address of VM3. | ● | ○ |
| From VM1, you can successfully ping the public IP address of VM5. | ○ | ● |

**Section:**

**Explanation:**

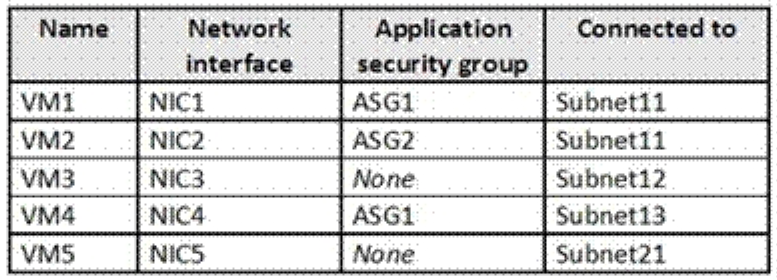
Box 1: Yes. All traffic is allowed out to the Internet so you can ping the public IP.

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

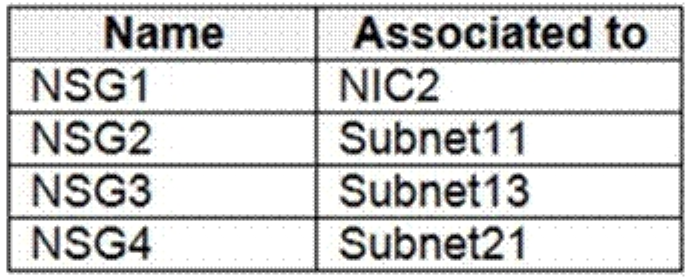


| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | Any | Internet | Allow |
| 65500 | Any | Any | Any | Any | Deny |

Box 2: Yes. VM3 is on Subnet12. There is no NSG attached to Subnet12 so the traffic will be allowed by default.



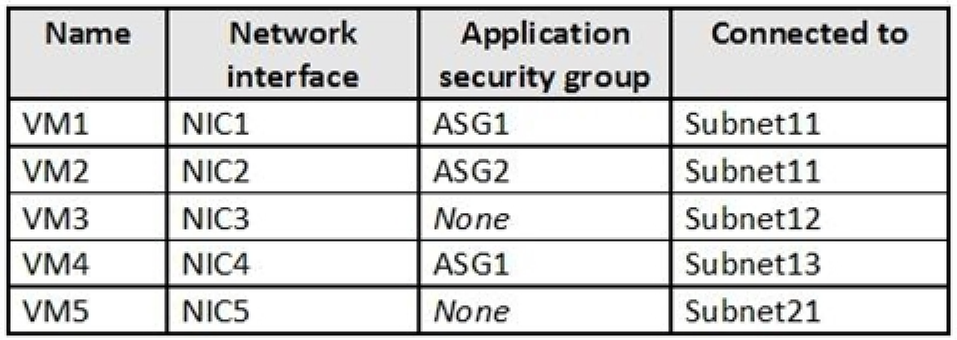
| Name | Network interface | Application security group | Connected to |
|---|---|---|---|
| VM1 | NIC1 | ASG1 | Subnet11 |
| VM2 | NIC2 | ASG2 | Subnet11 |
| VM3 | NIC3 | *None* | Subnet12 |
| VM4 | NIC4 | ASG1 | Subnet13 |
| VM5 | NIC5 | *None* | Subnet21 |



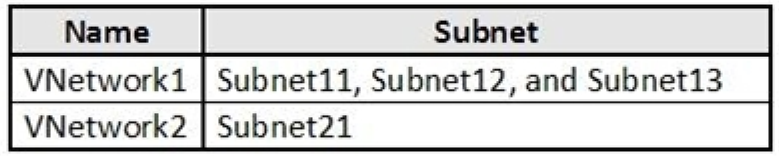
| Name | Associated to |
|---|---|
| NSG1 | NIC2 |
| NSG2 | Subnet11 |
| NSG3 | Subnet13 |
| NSG4 | Subnet21 |

Box 3: No (because VM5 is in a separate VNet).

Note: Sub2 contains the virtual machines shown in the following table.



| Name | Network interface | Application security group | Connected to |
|---|---|---|---|
| VM1 | NIC1 | ASG1 | Subnet11 |
| VM2 | NIC2 | ASG2 | Subnet11 |
| VM3 | NIC3 | *None* | Subnet12 |
| VM4 | NIC4 | ASG1 | Subnet13 |
| VM5 | NIC5 | *None* | Subnet21 |



| Name | Subnet |
|---|---|
| VNetwork1 | Subnet11, Subnet12, and Subnet13 |
| VNetwork2 | Subnet21 |

**QUESTION 3**

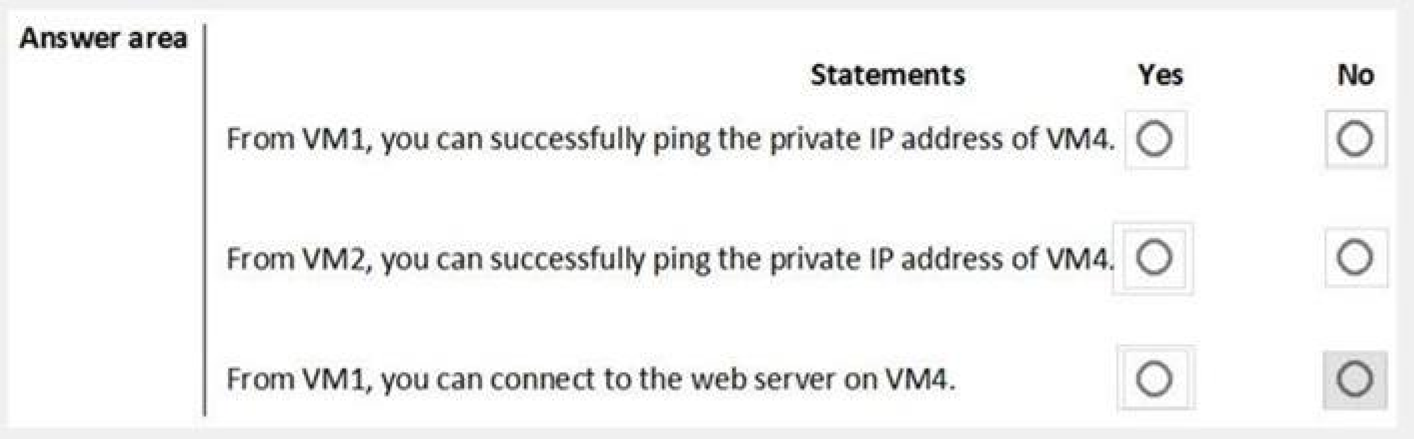
HOTSPOT

You are evaluating the effect of the application security groups on the network communication between the virtual machines in Sub2.

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

NOTE: Each correct selection is worth one point.

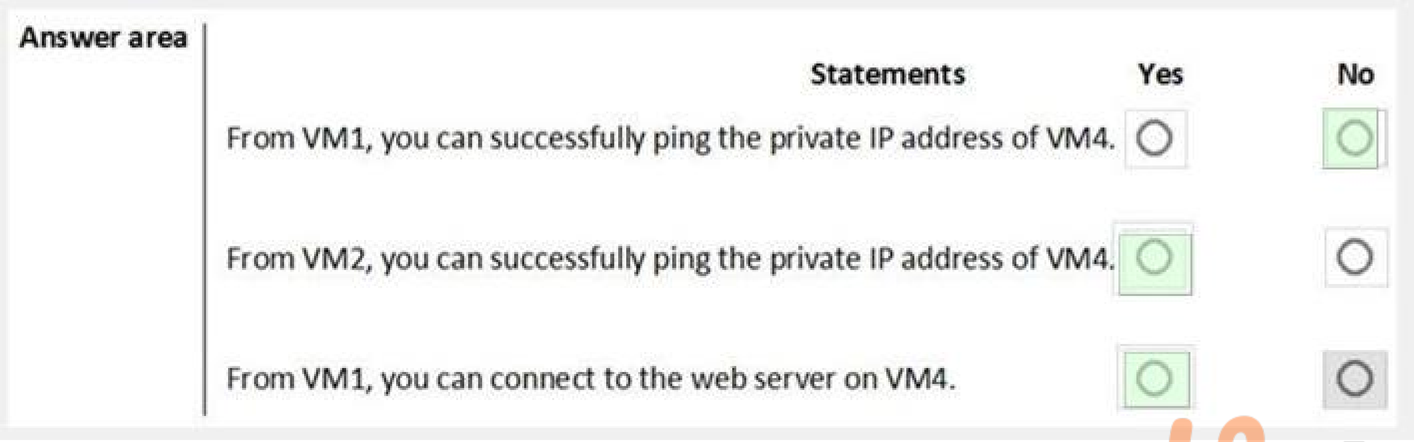
**Hot Area:**



Answer area

| Statements | Yes | No |
|---|---|---|
| From VM1, you can successfully ping the private IP address of VM4. | ○ | ○ |
| From VM2, you can successfully ping the private IP address of VM4. | ○ | ○ |
| From VM1, you can connect to the web server on VM4. | ○ | ○ |

**Answer Area:**



Answer area

| Statements | Yes | No |
|---|---|---|
| From VM1, you can successfully ping the private IP address of VM4. | ○ | [✓ ○] |
| From VM2, you can successfully ping the private IP address of VM4. | [✓ ○] | ○ |
| From VM1, you can connect to the web server on VM4. | [✓ ○] | ○ |

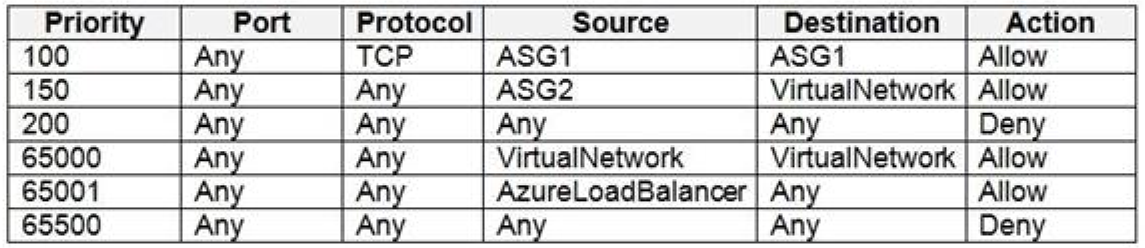
**Section:**

**Explanation:**

Box 1: No. VM4 is in Subnet13 which has NSG3 attached to it.

VM1 is in ASG1. NSG3 would only allow ICMP pings from ASG2 but not ASG1. Only TCP traffic is allowed from ASG1.

NSG3 has the inbound security rules shown in the following table.



| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 100 | Any | TCP | ASG1 | ASG1 | Allow |
| 150 | Any | Any | ASG2 | VirtualNetwork | Allow |
| 200 | Any | Any | Any | Any | Deny |
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

Box 2: Yes.

VM2 is in ASG2. Any protocol is allowed from ASG2 so ICMP ping would be allowed.

Box3. VM1 is in ASG1. TCP traffic is allowed from ASG1 so VM1 could connect to the web server as connections to the web server would be on ports TCP 80 or TCP 443.

**QUESTION 4**

You need to meet the technical requirements for VNetwork1.

What should you do first?

A. Create a new subnet on VNetwork1.

B. Remove the NSGs from Subnet11 and Subnet13.

C. Associate an NSG to Subnet12.

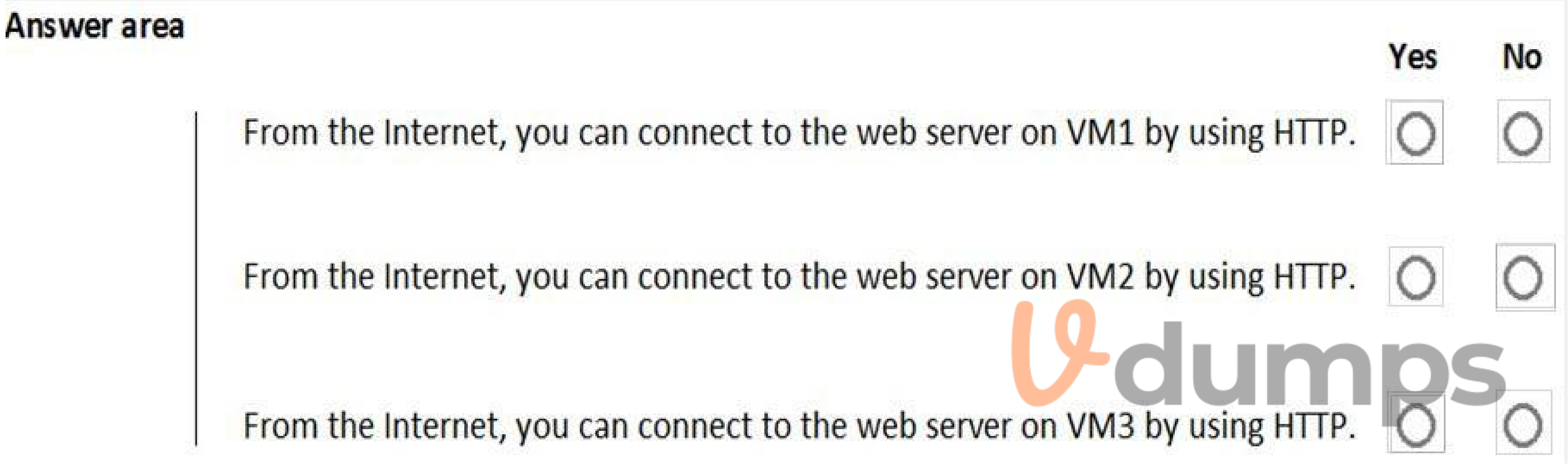
D. Configure DDoS protection for VNetwork1.

**Correct Answer: A**

**Section:**
**Explanation:**
From scenario: Deploy Azure Firewall to VNetwork1 in Sub2.
Azure firewall needs a dedicated subnet named AzureFirewallSubnet.
References:
https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal

**QUESTION 5**
HOTSPOT
You are evaluating the security of VM1, VM2, and VM3 in Sub2.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

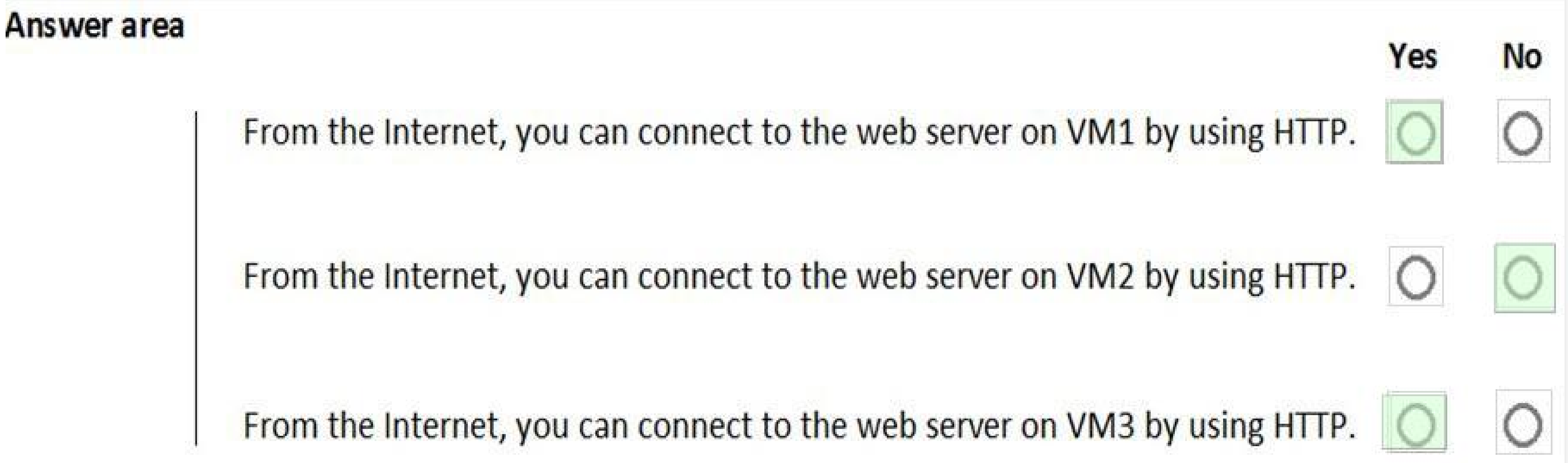
**Hot Area:**



Answer area

| | Yes | No |
|---|---|---|
| From the Internet, you can connect to the web server on VM1 by using HTTP. | ○ | ○ |
| From the Internet, you can connect to the web server on VM2 by using HTTP. | ○ | ○ |
| From the Internet, you can connect to the web server on VM3 by using HTTP. | ○ | ○ |

**Answer Area:**



Answer area

| | Yes | No |
|---|---|---|
| From the Internet, you can connect to the web server on VM1 by using HTTP. | [✓ ○] | ○ |
| From the Internet, you can connect to the web server on VM2 by using HTTP. | ○ | [✓ ○] |
| From the Internet, you can connect to the web server on VM3 by using HTTP. | [✓ ○] | ○ |

**Section:**
**Explanation:**
VM1: Yes. NSG2 applies to VM1 and this allows inbound traffic on port 80.
VM2: No. NSG2 and NSG1 apply to VM2. NSG2 allows the inbound traffic on port 80 but NSG1 does not allow it. VM3: Yes. There are no NSGs applying to VM3 so all ports will be open.

**01 - Manage identity and access**

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Overview

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

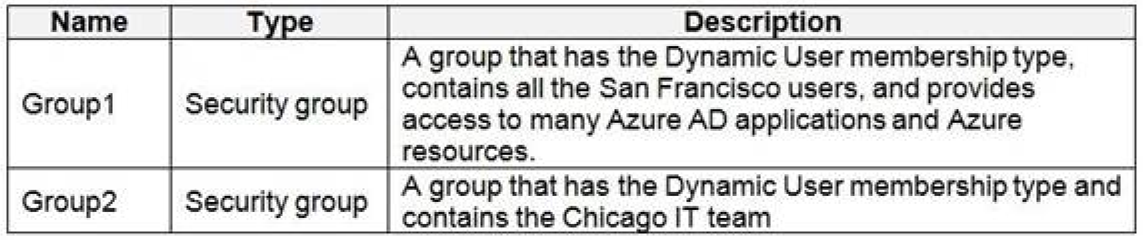
Existing Environment

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD

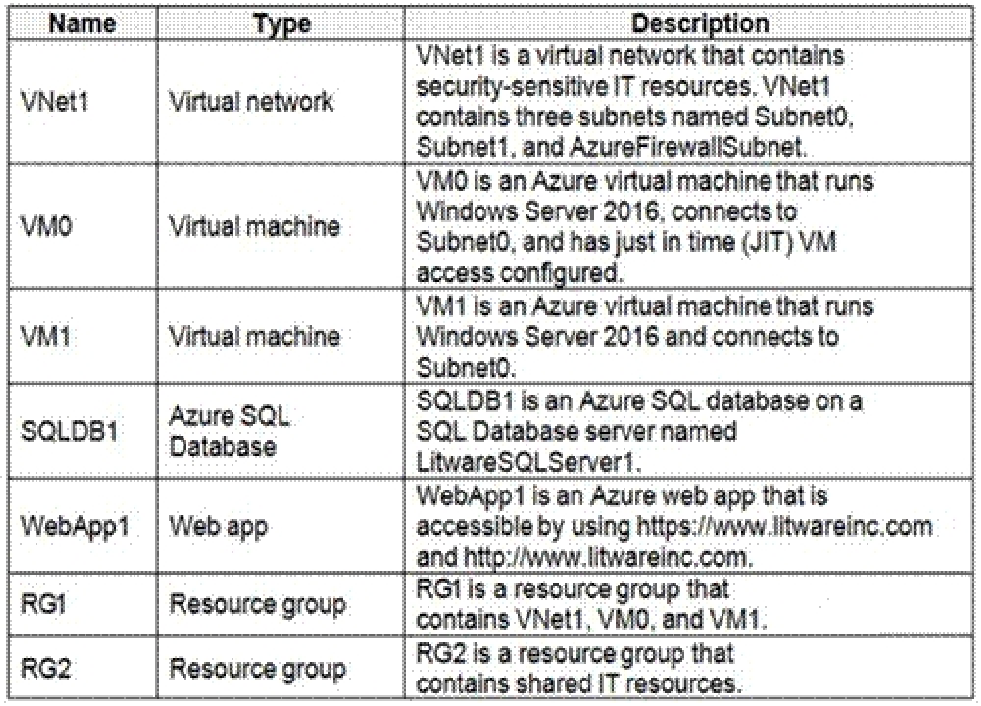
Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.



| Name | Type | Description |
|---|---|---|
| Group1 | Security group | A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources. |
| Group2 | Security group | A group that has the Dynamic User membership type and contains the Chicago IT team |

The Azure subscription contains the objects shown in the following table.



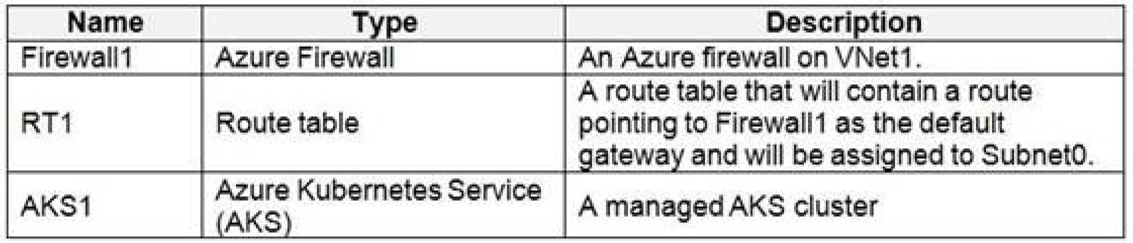
| Name | Type | Description |
|---|---|---|
| VNet1 | Virtual network | VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet. |
| VM0 | Virtual machine | VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured. |
| VM1 | Virtual machine | VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0. |
| SQLDB1 | Azure SQL Database | SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1. |
| WebApp1 | Web app | WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com. |
| RG1 | Resource group | RG1 is a resource group that contains VNet1, VM0, and VM1. |
| RG2 | Resource group | RG2 is a resource group that contains shared IT resources. |

Azure Security Center is set to the Standard tier.

Requirements

Planned Changes

Litware plans to deploy the Azure resources shown in the following table.



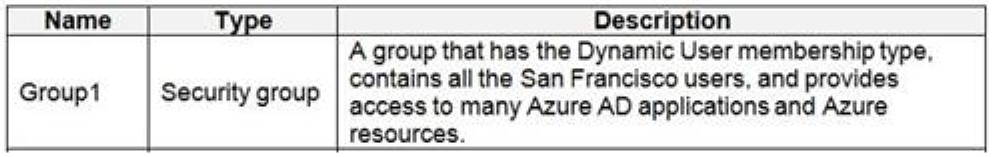
| Name | Type | Description |
|---|---|---|
| Firewall1 | Azure Firewall | An Azure firewall on VNet1. |
| RT1 | Route table | A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0. |
| AKS1 | Azure Kubernetes Service (AKS) | A managed AKS cluster |

Identity and Access Requirements
Litware identifies the following identity and access requirements:
All San Francisco users and their devices must be members of Group1.
The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment.
Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.
Platform Protection Requirements
Litware identifies the following platform protection requirements:
Microsoft Antimalware must be installed on the virtual machines in RG1.
The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.
Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.
A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.
Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center.
Data and Application Requirements
Litware identifies the following data and applications requirements:
The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.
WebApp1 must enforce mutual authentication.
General Requirements
Litware identifies the following general requirements:
Whenever possible, administrative effort must be minimized.
Whenever possible, use of automation must be maximized.

**QUESTION 1**
You need to meet the identity and access requirements for Group1.
What should you do?

A. Add a membership rule to Group1.
B. Delete Group1. Create a new group named Group1 that has a membership type of Microsoft 365. Add users and devices to the group.
C. Modify the membership rule of Group1.
D. Change the membership type of Group1 to Assigned. Create two groups that have dynamic memberships. Add the new groups to Group1.

**Correct Answer: D**
**Section:**
**Explanation:**
When you create dynamic groups, they can either contain users or devices. Hence here we need to create two separate dynamic groups and assign those groups to an Assigned group. Incorrect Answers:
A, C: You can create a dynamic group for devices or for users, but you can't create a rule that contains both users and devices.
D: For assigned group you can only add individual members.
Scenario:
Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1.
The tenant currently contain this group:



| Name | Type | Description |
|---|---|---|
| Group1 | Security group | A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources. |

References:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal

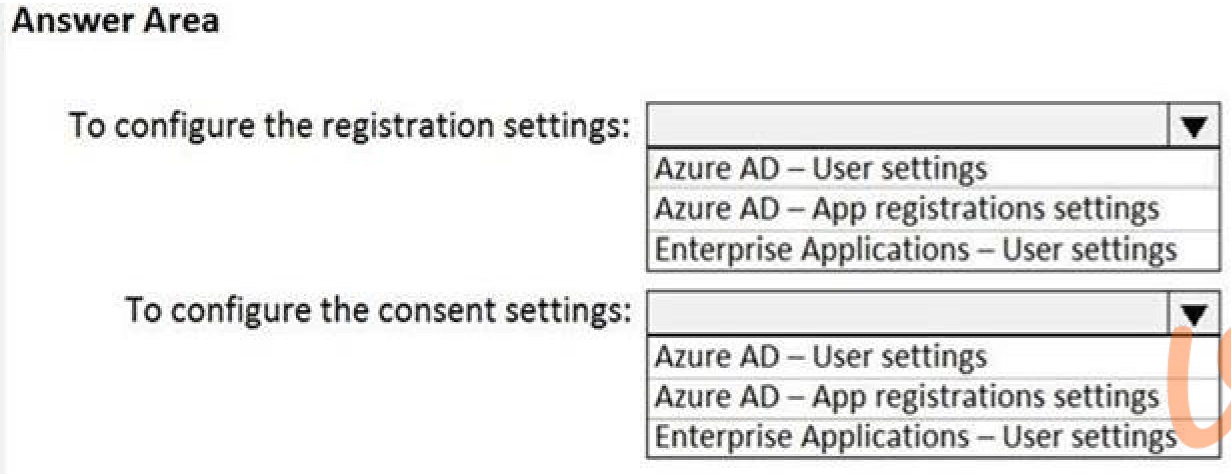
**QUESTION 2**

HOTSPOT

You need to ensure that the Azure AD application registration and consent configurations meet the identity and access requirements. What should you use in the Azure portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Hot Area:**

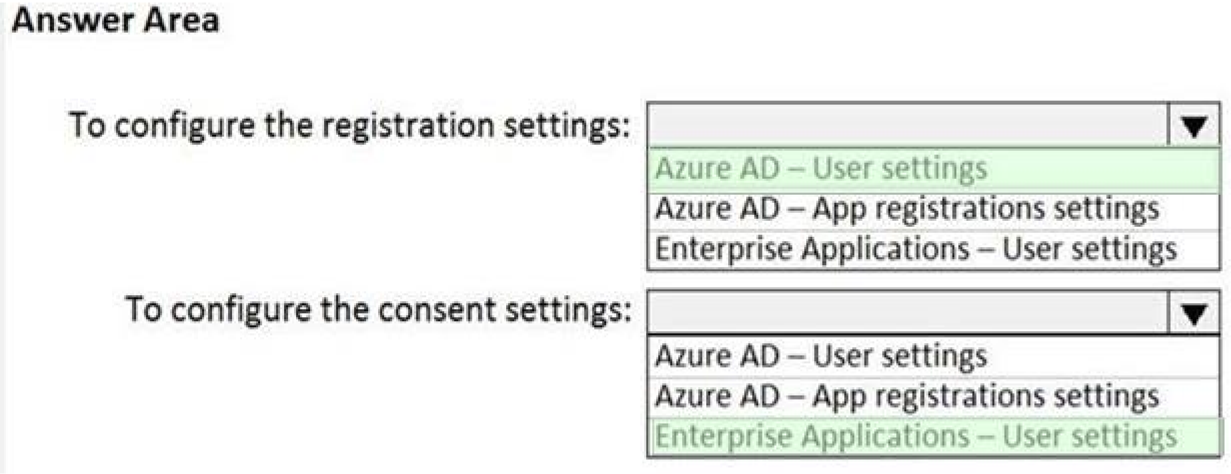


Answer Area

To configure the registration settings:
- Azure AD – User settings
- Azure AD – App registrations settings
- Enterprise Applications – User settings

To configure the consent settings:
- Azure AD – User settings
- Azure AD – App registrations settings
- Enterprise Applications – User settings

**Answer Area:**



Answer Area

To configure the registration settings:
- [✓ Azure AD – User settings]
- Azure AD – App registrations settings
- Enterprise Applications – User settings

To configure the consent settings:
- Azure AD – User settings
- Azure AD – App registrations settings
- [✓ Enterprise Applications – User settings]

**Section:**

**Explanation:**

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent

**02 - Manage identity and access**

Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

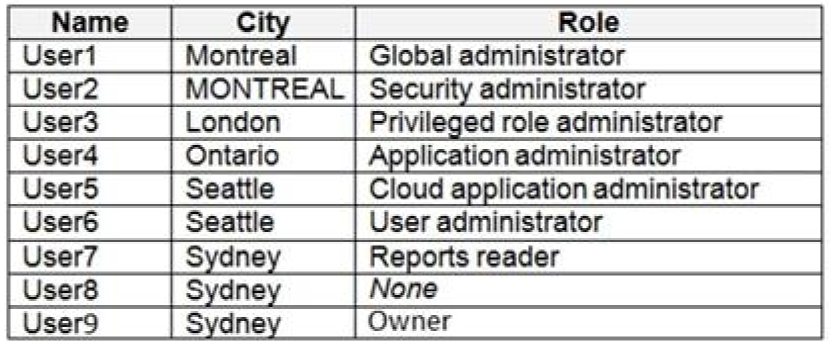
The company hosts its entire server infrastructure in Azure.

Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

Existing Environment

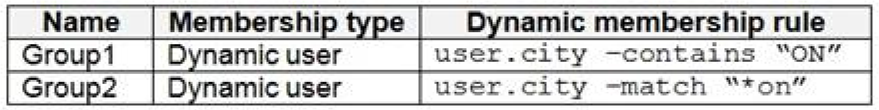
Azure AD

Contoso.com contains the users shown in the following table.



| Name | City | Role |
|---|---|---|
| User1 | Montreal | Global administrator |
| User2 | MONTREAL | Security administrator |
| User3 | London | Privileged role administrator |
| User4 | Ontario | Application administrator |
| User5 | Seattle | Cloud application administrator |
| User6 | Seattle | User administrator |
| User7 | Sydney | Reports reader |
| User8 | Sydney | *None* |
| User9 | Sydney | Owner |

Contoso.com contains the security groups shown in the following table.

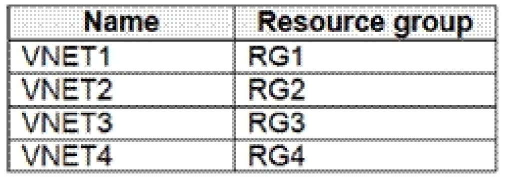


| Name | Membership type | Dynamic membership rule |
|---|---|---|
| Group1 | Dynamic user | `user.city -contains "ON"` |
| Group2 | Dynamic user | `user.city -match "*on"` |

Sub1

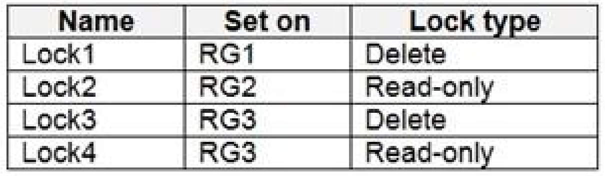
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.



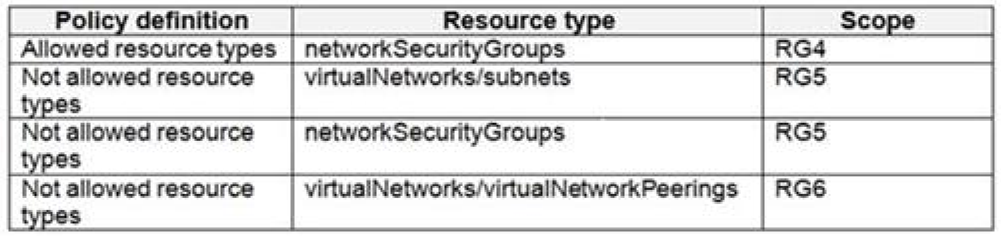
| Name | Resource group |
|---|---|
| VNET1 | RG1 |
| VNET2 | RG2 |
| VNET3 | RG3 |
| VNET4 | RG4 |

Sub1 contains the locks shown in the following table.



| Name | Set on | Lock type |
|---|---|---|
| Lock1 | RG1 | Delete |
| Lock2 | RG2 | Read-only |
| Lock3 | RG3 | Delete |
| Lock4 | RG3 | Read-only |

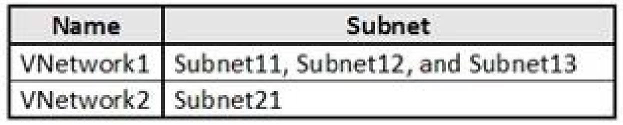
Sub1 contains the Azure policies shown in the following table.



| Policy definition | Resource type | Scope |
|---|---|---|
| Allowed resource types | networkSecurityGroups | RG4 |
| Not allowed resource types | virtualNetworks/subnets | RG5 |
| Not allowed resource types | networkSecurityGroups | RG5 |
| Not allowed resource types | virtualNetworks/virtualNetworkPeerings | RG6 |

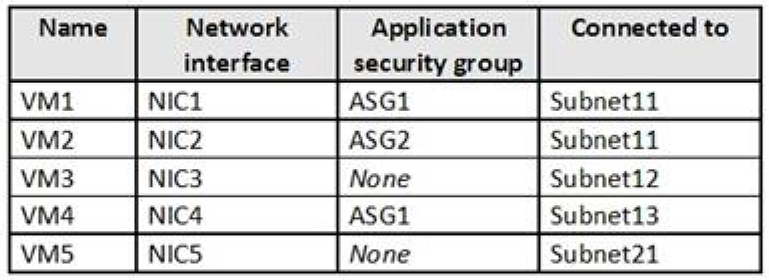
Sub2

Sub2 contains the virtual networks shown in the following table.



| Name | Subnet |
|---|---|
| VNetwork1 | Subnet11, Subnet12, and Subnet13 |
| VNetwork2 | Subnet21 |

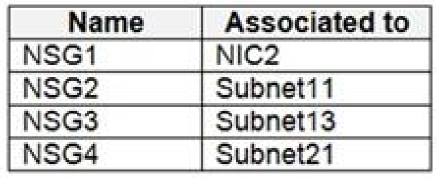
Sub2 contains the virtual machines shown in the following table.



| Name | Network interface | Application security group | Connected to |
|---|---|---|---|
| VM1 | NIC1 | ASG1 | Subnet11 |
| VM2 | NIC2 | ASG2 | Subnet11 |
| VM3 | NIC3 | *None* | Subnet12 |
| VM4 | NIC4 | ASG1 | Subnet13 |
| VM5 | NIC5 | *None* | Subnet21 |

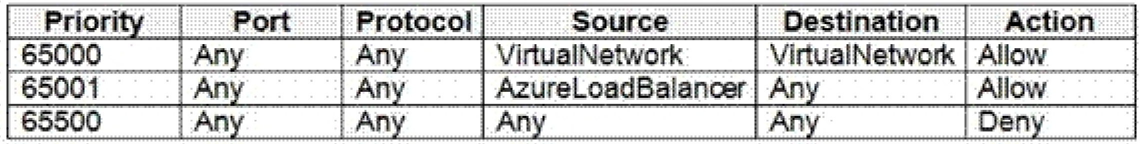
All virtual machines have public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

Sub2 contains the network security groups (NSGs) shown in the following table.



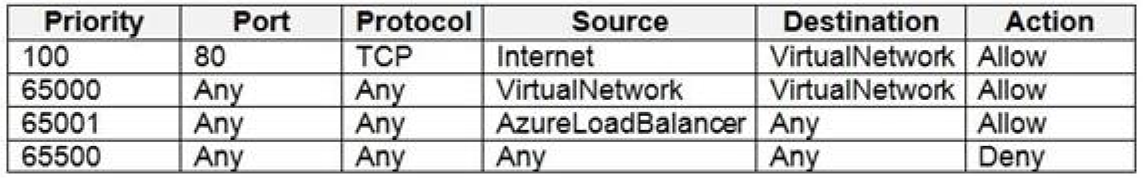
| Name | Associated to |
|---|---|
| NSG1 | NIC2 |
| NSG2 | Subnet11 |
| NSG3 | Subnet13 |
| NSG4 | Subnet21 |

NSG1 has the inbound security rules shown in the following table.



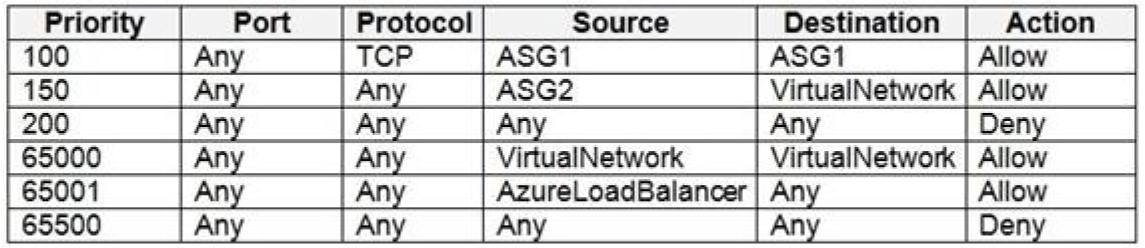
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

NSG2 has the inbound security rules shown in the following table.



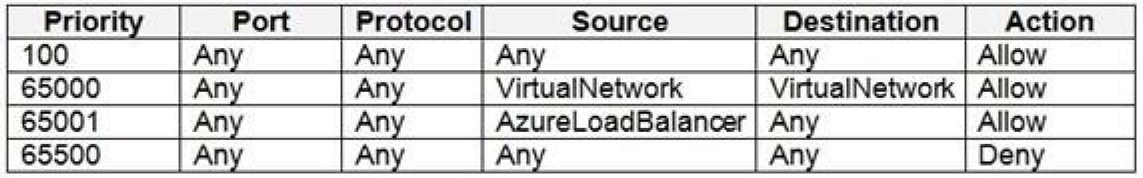
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 100 | 80 | TCP | Internet | VirtualNetwork | Allow |
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

NSG3 has the inbound security rules shown in the following table.



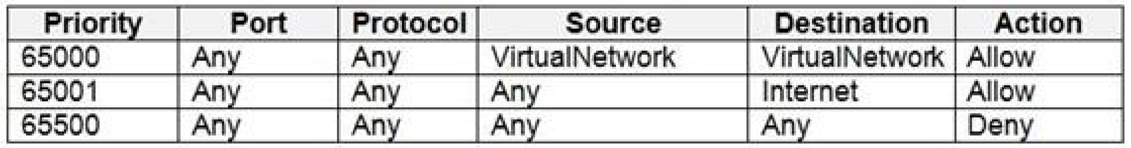
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 100 | Any | TCP | ASG1 | ASG1 | Allow |
| 150 | Any | Any | ASG2 | VirtualNetwork | Allow |
| 200 | Any | Any | Any | Any | Deny |
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

NSG4 has the inbound security rules shown in the following table.



| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 100 | Any | Any | Any | Any | Allow |
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.



| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | Any | Internet | Allow |
| 65500 | Any | Any | Any | Any | Deny |

Technical requirements

Contoso identifies the following technical requirements:

Deploy Azure Firewall to VNetwork1 in Sub2.

Register an application named App2 in contoso.com.

Whenever possible, use the principle of least privilege.
Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

**QUESTION 1**

You need to ensure that User2 can implement PIM.
What should you do first?

A. Assign User2 the Global administrator role.

B. Configure authentication methods for contoso.com.

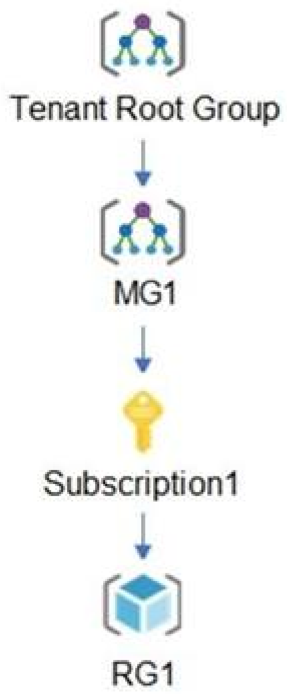
C. Configure the identity secure score for contoso.com.

D. Enable multi-factor authentication (MFA) for User2.

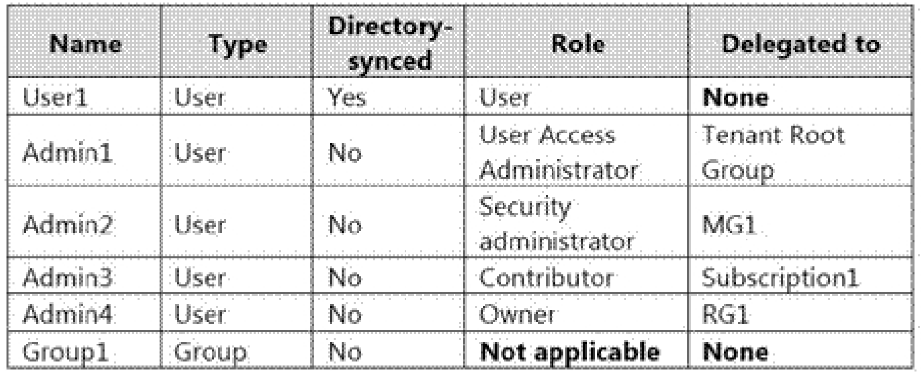
**Correct Answer: A**
**Section:**
**Explanation:**
To start using PIM in your directory, you must first enable PIM.
1. Sign in to the Azure portal as a Global Administrator of your directory.
You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory. Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com
References:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started

**03 - Manage identity and access**

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
General Overview
Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.
Existing Environment
Network Environment
Fabrikam has a Microsoft 365 subscription and an Azure subscription named subscription1.
The network contains an on-premises Active Directory domain named Fabrikam.com. The domain contains two organizational units (OUs) named OU1 and OU2. Azure AD Connect cloud sync syncs only OU1.
The Azure resources hierarchy is shown in the following exhibit.

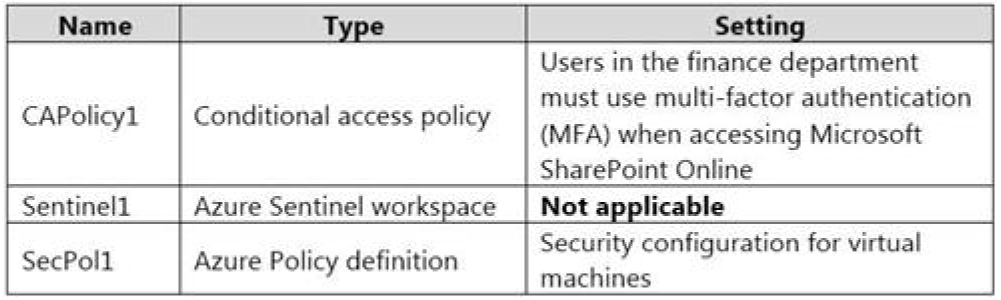


The Azure Active Directory (Azure AD) tenant contains the users shown in the following table.



| Name | Type | Directory-synced | Role | Delegated to |
|---|---|---|---|---|
| User1 | User | Yes | User | **None** |
| Admin1 | User | No | User Access Administrator | Tenant Root Group |
| Admin2 | User | No | Security administrator | MG1 |
| Admin3 | User | No | Contributor | Subscription1 |
| Admin4 | User | No | Owner | RG1 |
| Group1 | Group | No | **Not applicable** | **None** |

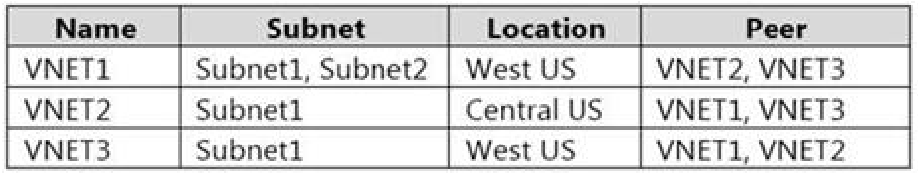
Azure AD contains the resources shown in the following table.



| Name | Type | Setting |
|---|---|---|
| CAPolicy1 | Conditional access policy | Users in the finance department must use multi-factor authentication (MFA) when accessing Microsoft SharePoint Online |
| Sentinel1 | Azure Sentinel workspace | **Not applicable** |
| SecPol1 | Azure Policy definition | Security configuration for virtual machines |

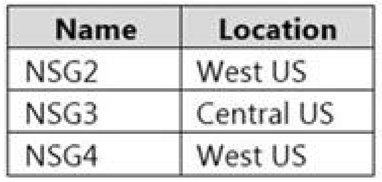
Subscription1 Resources

Subscription1 contains the virtual networks shown in the following table.



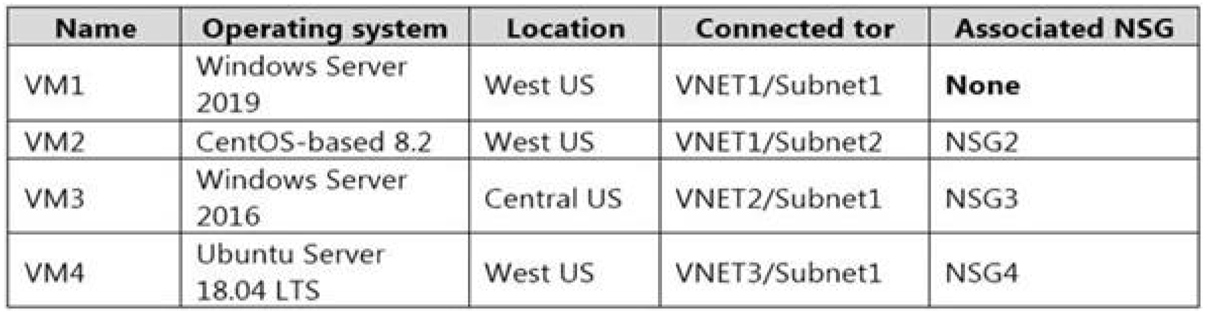
| Name | Subnet | Location | Peer |
|---|---|---|---|
| VNET1 | Subnet1, Subnet2 | West US | VNET2, VNET3 |
| VNET2 | Subnet1 | Central US | VNET1, VNET3 |
| VNET3 | Subnet1 | West US | VNET1, VNET2 |

Subscription1 contains the network security groups (NSGs) shown in the following table.



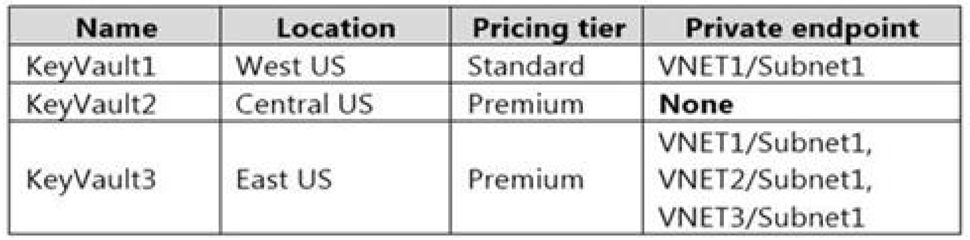
| Name | Location |
|---|---|
| NSG2 | West US |
| NSG3 | Central US |
| NSG4 | West US |

Subscription1 contains the virtual machines shown in the following table.



| Name | Operating system | Location | Connected tor | Associated NSG |
|---|---|---|---|---|
| VM1 | Windows Server 2019 | West US | VNET1/Subnet1 | **None** |
| VM2 | CentOS-based 8.2 | West US | VNET1/Subnet2 | NSG2 |
| VM3 | Windows Server 2016 | Central US | VNET2/Subnet1 | NSG3 |
| VM4 | Ubuntu Server 18.04 LTS | West US | VNET3/Subnet1 | NSG4 |

Subscription1 contains the Azure key vaults shown in the following table.



| Name | Location | Pricing tier | Private endpoint |
|---|---|---|---|
| KeyVault1 | West US | Standard | VNET1/Subnet1 |
| KeyVault2 | Central US | Premium | **None** |
| KeyVault3 | East US | Premium | VNET1/Subnet1,<br>VNET2/Subnet1,<br>VNET3/Subnet1 |

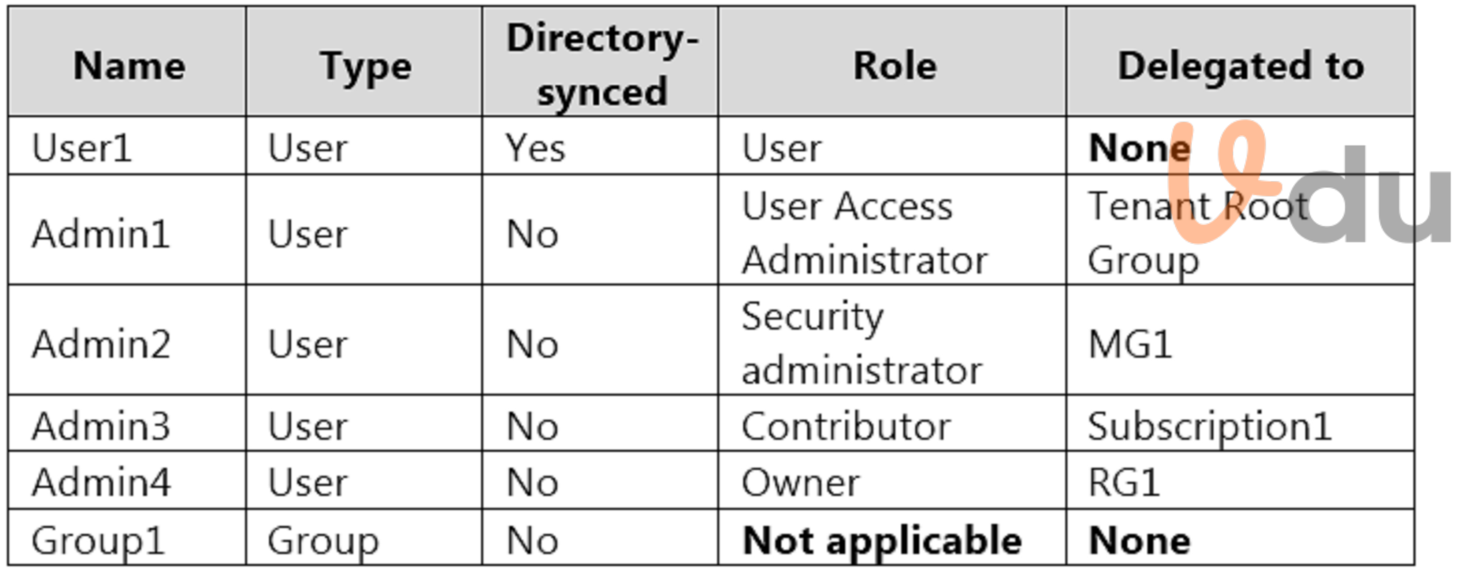
Subscription1 contains a storage account named storage1 in the West US Azure region.

Planned Changes and Requirements

Planned Changes

Fabrikam plans to implement the following changes:

Create two application security groups as shown in the following table.



| Name | Type | Directory-synced | Role | Delegated to |
|---|---|---|---|---|
| User1 | User | Yes | User | **None** |
| Admin1 | User | No | User Access Administrator | Tenant Root Group |
| Admin2 | User | No | Security administrator | MG1 |
| Admin3 | User | No | Contributor | Subscription1 |
| Admin4 | User | No | Owner | RG1 |
| Group1 | Group | No | **Not applicable** | **None** |

Associate the network interface of VM1 to ASG1.

Deploy SecPol1 by using Azure Security Center.

Deploy a third-party app named App1. A version of App1 exists for all available operating systems.

Create a resource group named RG2.

Sync OU2 to Azure AD.

Add User1 to Group1.

Technical Requirements

Fabrikam identifies the following technical requirements:

The finance department users must reauthenticate after three hours when they access SharePoint Online. Storage1 must be encrypted by using customer-managed keys and automatic key rotation.

From Sentinel1, you must ensure that the following notebooks can be launched:

- Entity Explorer – Account
- Entity Explorer – Windows Host
- Guided Investigation Process Alerts

VM1, VM2, and VM3 must be encrypted by using Azure Disk Encryption.

Just in time (JIT) VM access for VM1, VM2, and VM3 must be enabled.

App1 must use a secure connection string stored in KeyVault1.

KeyVault1 traffic must NOT travel over the internet.

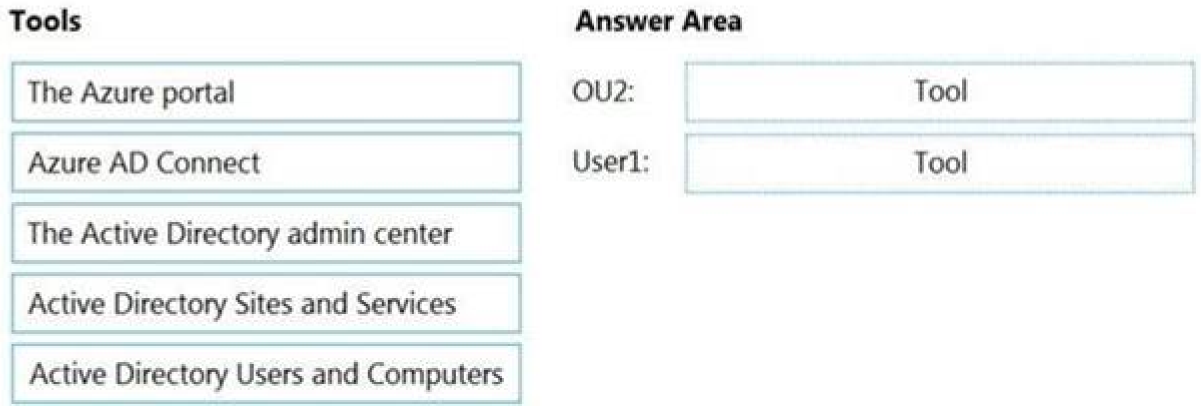
**QUESTION 1**

DRAG DROP

You need to perform the planned changes for OU2 and User1.

Which tools should you use? To answer, drag the appropriate tools to the correct resources. Each tool 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.

**Select and Place:**



**Tools**

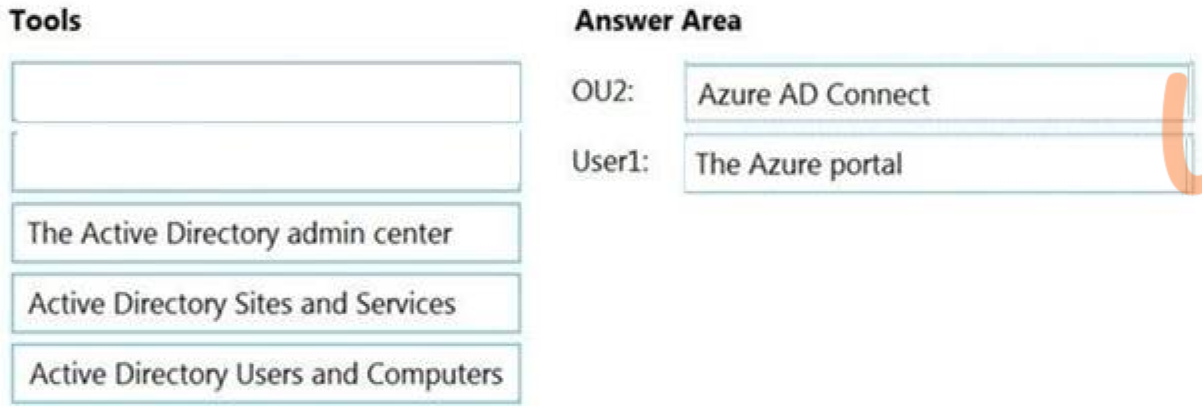
- The Azure portal
- Azure AD Connect
- The Active Directory admin center
- Active Directory Sites and Services
- Active Directory Users and Computers

**Answer Area**

OU2: Tool

User1: Tool

**Correct Answer:**



**Tools**

- The Active Directory admin center
- Active Directory Sites and Services
- Active Directory Users and Computers

**Answer Area**

OU2: Azure AD Connect

User1: The Azure portal

**Section:**

**Explanation:**

**QUESTION 2**

You need to meet the technical requirements for the finance department users.

Which CAPolicy1 settings should you modify?

A. Cloud apps or actions

B. Conditions

C. Grant

D. Session

**Correct Answer: D**

**Section:**

**Explanation:**

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime

**QUESTION 3**

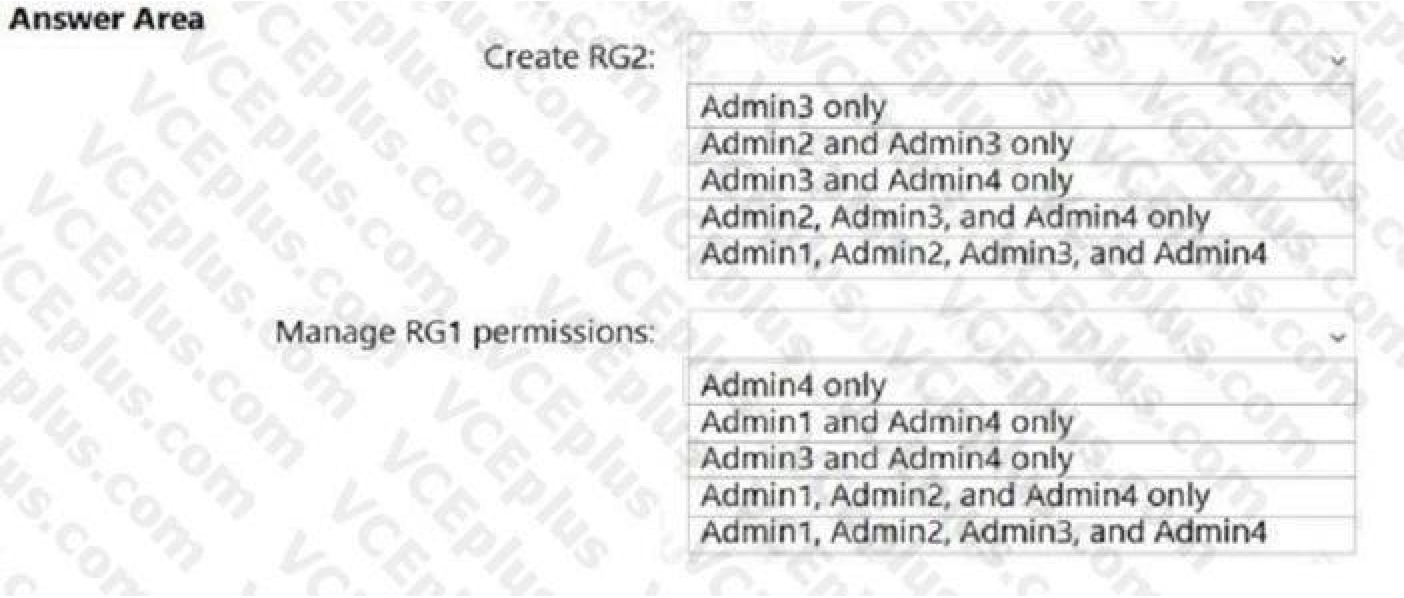
HOTSPOT

You need to delegate the creation of RG2 and the management of permissions for RG1.

Which users can perform each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Hot Area:**

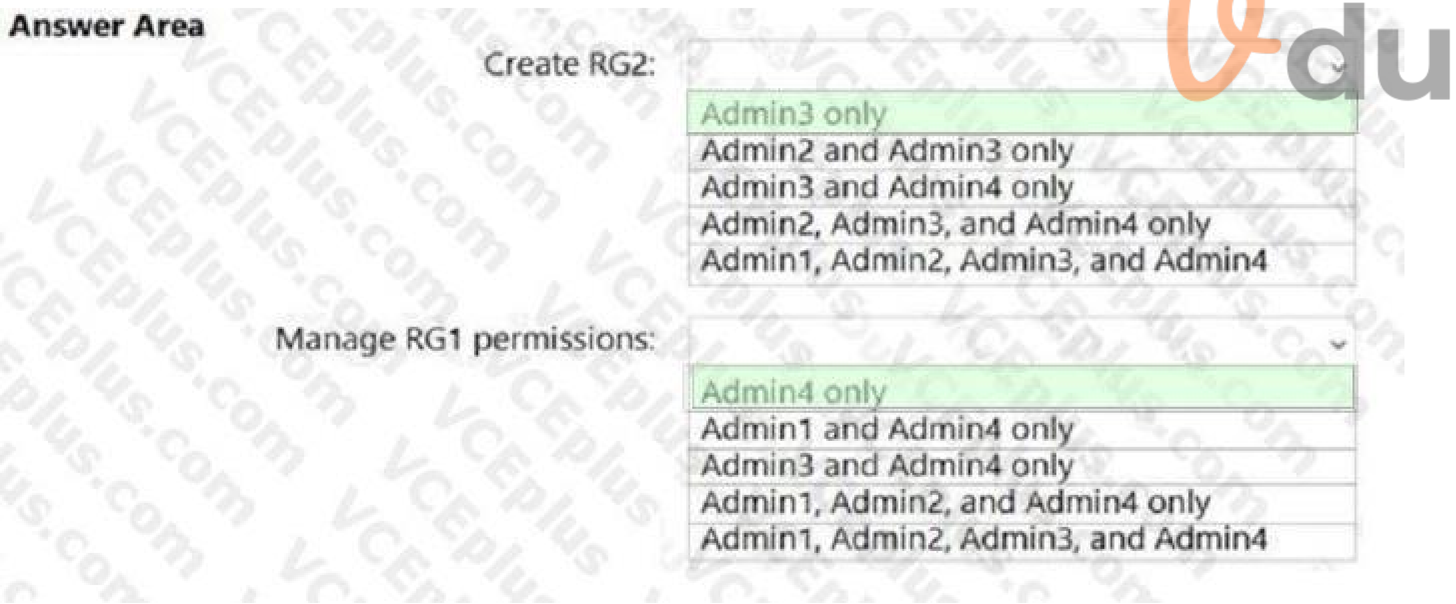


**Answer Area**

Create RG2:
- Admin3 only
- Admin2 and Admin3 only
- Admin3 and Admin4 only
- Admin2, Admin3, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4

Manage RG1 permissions:
- Admin4 only
- Admin1 and Admin4 only
- Admin3 and Admin4 only
- Admin1, Admin2, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4

**Answer Area:**



**Answer Area**

Create RG2:
- [✓ Admin3 only]
- Admin2 and Admin3 only
- Admin3 and Admin4 only
- Admin2, Admin3, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4

Manage RG1 permissions:
- [✓ Admin4 only]
- Admin1 and Admin4 only
- Admin3 and Admin4 only
- Admin1, Admin2, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4

**Section:**

**Explanation:**

Box 1: Admin3 only

The Contributor role has the necessary write permissions to create the resource group.

Box 2: Admin4 only

You need Owner level access to be able to manage permissions. The Contributor role can do most things but cannot modify permissions on existing objects.

**01 - Manage security operations**

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

General Overview

Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.

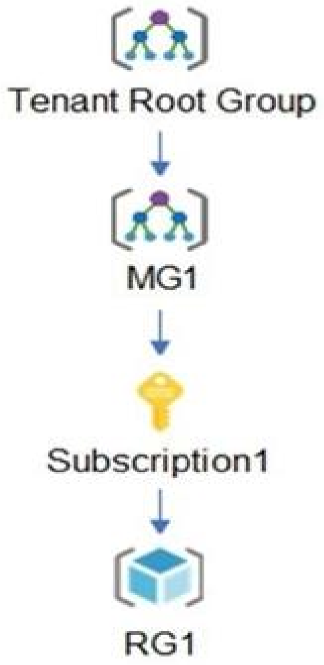
Existing Environment

Network Environment

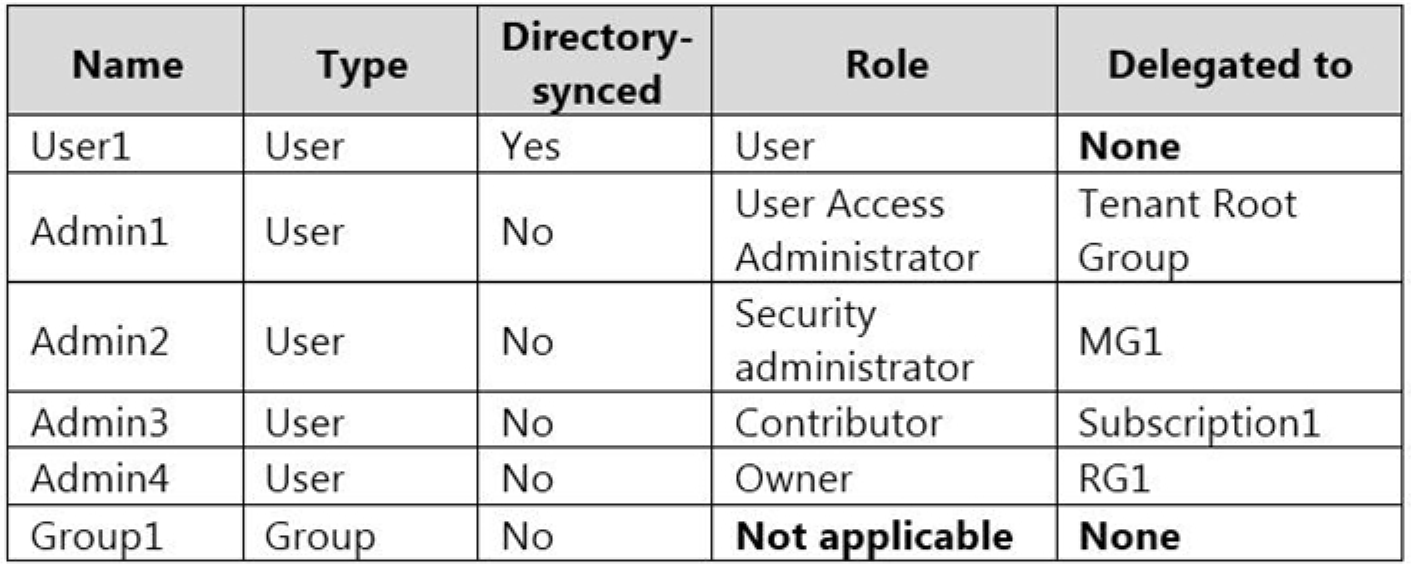
Fabrikam has a Microsoft 365 subscription and an Azure subscription named subscription1.

The network contains an on-premises Active Directory domain named Fabrikam.com. The domain contains two organizational units (OUs) named OU1 and OU2. Azure AD Connect cloud sync syncs only OU1.

The Azure resources hierarchy is shown in the following exhibit.

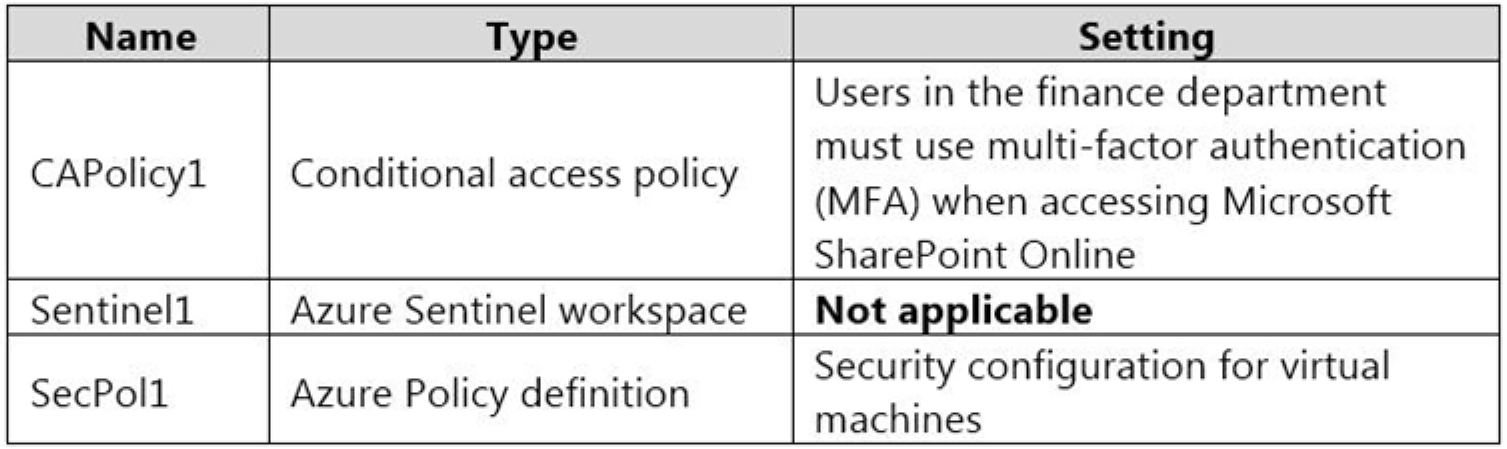


The Azure Active Directory (Azure AD) tenant contains the users shown in the following table.



| Name | Type | Directory-synced | Role | Delegated to |
|---|---|---|---|---|
| User1 | User | Yes | User | **None** |
| Admin1 | User | No | User Access Administrator | Tenant Root Group |
| Admin2 | User | No | Security administrator | MG1 |
| Admin3 | User | No | Contributor | Subscription1 |
| Admin4 | User | No | Owner | RG1 |
| Group1 | Group | No | **Not applicable** | **None** |

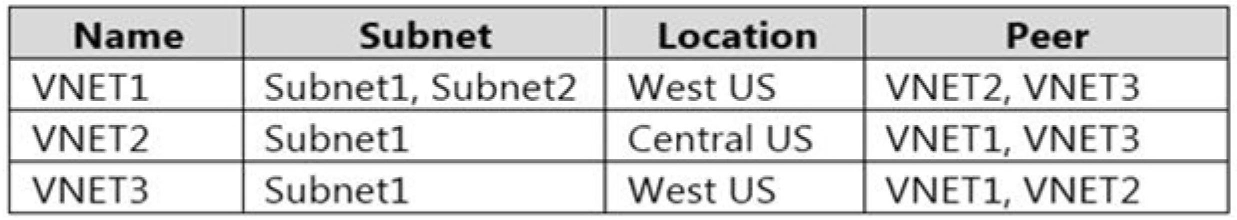
Azure AD contains the resources shown in the following table.



| Name | Type | Setting |
|---|---|---|
| CAPolicy1 | Conditional access policy | Users in the finance department must use multi-factor authentication (MFA) when accessing Microsoft SharePoint Online |
| Sentinel1 | Azure Sentinel workspace | **Not applicable** |
| SecPol1 | Azure Policy definition | Security configuration for virtual machines |

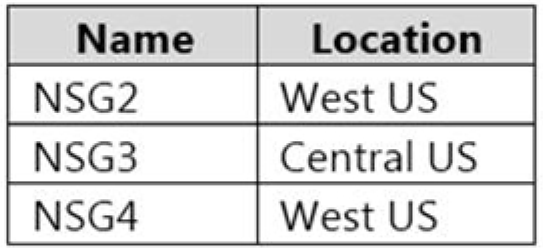
Subscription1 Resources

Subscription1 contains the virtual networks shown in the following table.



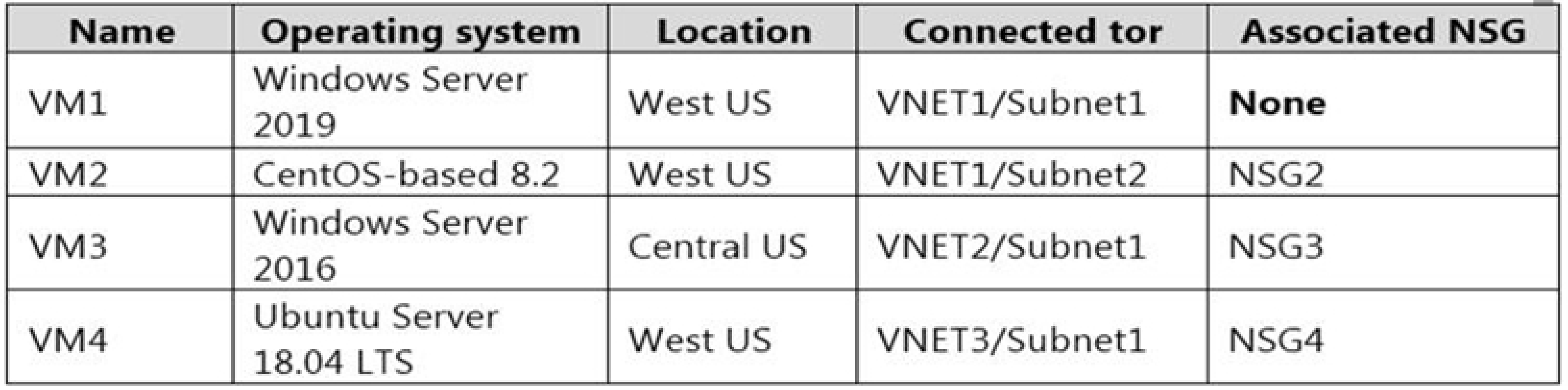
| Name | Subnet | Location | Peer |
|---|---|---|---|
| VNET1 | Subnet1, Subnet2 | West US | VNET2, VNET3 |
| VNET2 | Subnet1 | Central US | VNET1, VNET3 |
| VNET3 | Subnet1 | West US | VNET1, VNET2 |

Subscription1 contains the network security groups (NSGs) shown in the following table.



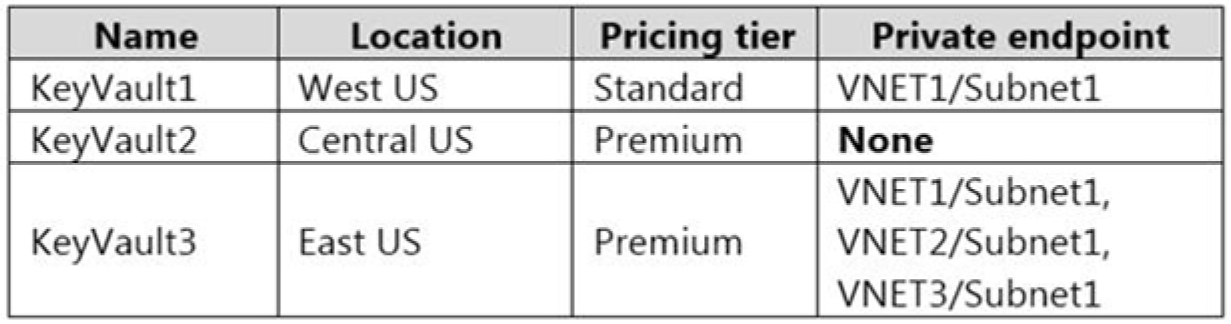
| Name | Location |
|---|---|
| NSG2 | West US |
| NSG3 | Central US |
| NSG4 | West US |

Subscription1 contains the virtual machines shown in the following table.



| Name | Operating system | Location | Connected tor | Associated NSG |
|---|---|---|---|---|
| VM1 | Windows Server 2019 | West US | VNET1/Subnet1 | **None** |
| VM2 | CentOS-based 8.2 | West US | VNET1/Subnet2 | NSG2 |
| VM3 | Windows Server 2016 | Central US | VNET2/Subnet1 | NSG3 |
| VM4 | Ubuntu Server 18.04 LTS | West US | VNET3/Subnet1 | NSG4 |

Subscription1 contains the Azure key vaults shown in the following table.



| Name | Location | Pricing tier | Private endpoint |
|---|---|---|---|
| KeyVault1 | West US | Standard | VNET1/Subnet1 |
| KeyVault2 | Central US | Premium | **None** |
| KeyVault3 | East US | Premium | VNET1/Subnet1,<br>VNET2/Subnet1,<br>VNET3/Subnet1 |

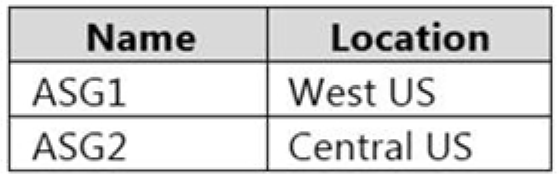
Subscription1 contains a storage account named storage1 in the West US Azure region.

Planned Changes and Requirements

Planned Changes

Fabrikam plans to implement the following changes:

Create two application security groups as shown in the following table.

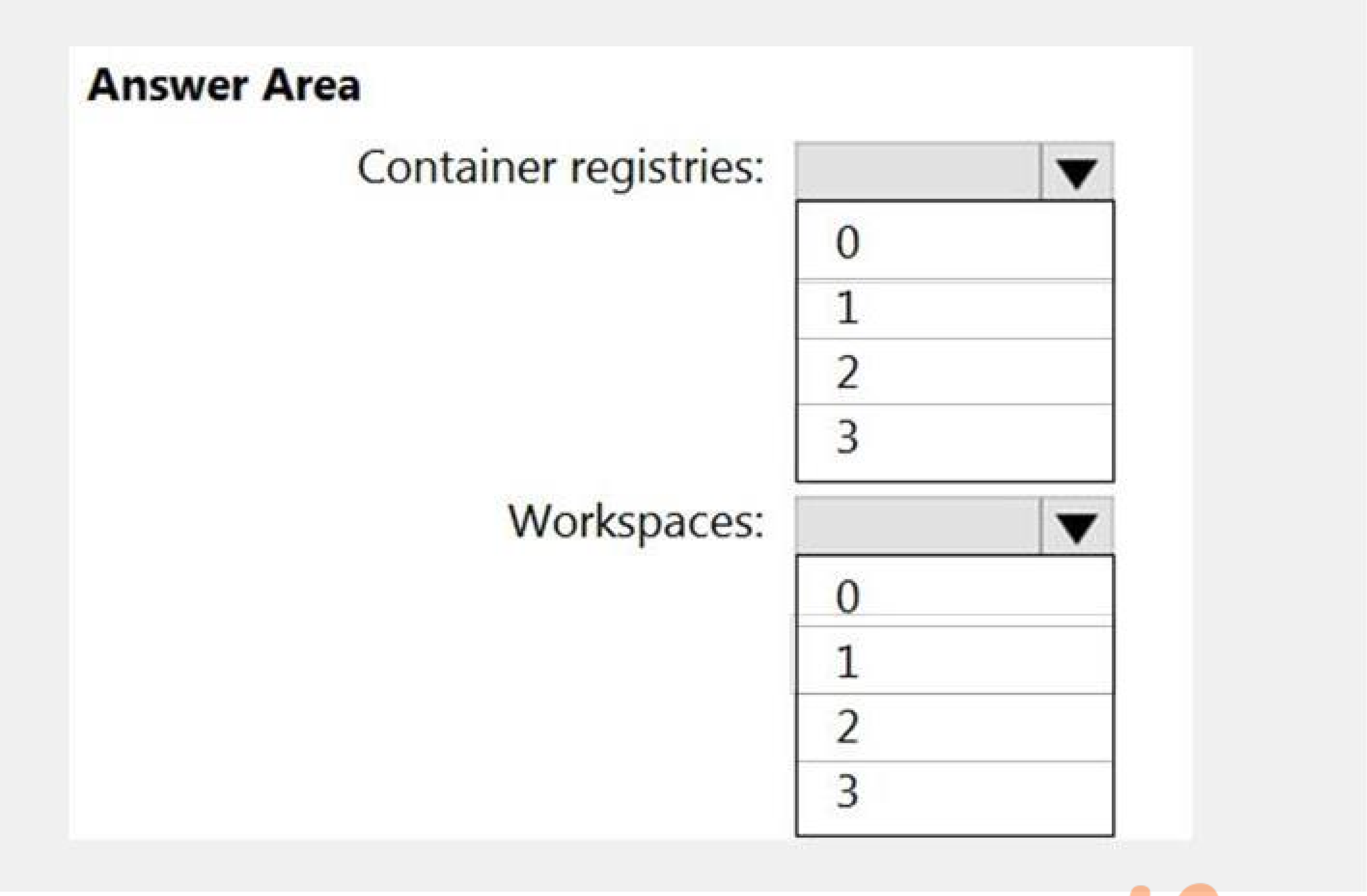


| Name | Location |
|---|---|
| ASG1 | West US |
| ASG2 | Central US |

Associate the network interface of VM1 to ASG1.
Deploy SecPol1 by using Azure Security Center.
Deploy a third-party app named App1. A version of App1 exists for all available operating systems.
Create a resource group named RG2.
Sync OU2 to Azure AD.
Add User1 to Group1.
Technical Requirements
Fabrikam identifies the following technical requirements:
The finance department users must reauthenticate after three hours when they access SharePoint Online. Storage1 must be encrypted by using customer-managed keys and automatic key rotation.
From Sentinel1, you must ensure that the following notebooks can be launched:
- Entity Explorer – Account
- Entity Explorer – Windows Host
- Guided Investigation Process Alerts
VM1, VM2, and VM3 must be encrypted by using Azure Disk Encryption.
Just in time (JIT) VM access for VM1, VM2, and VM3 must be enabled.
App1 must use a secure connection string stored in KeyVault1.
KeyVault1 traffic must NOT travel over the internet.

**QUESTION 1**
HOTSPOT
You need to configure support for Azure Sentinel notebooks to meet the technical requirements.
What is the minimum number of Azure container registries and Azure Machine Learning workspaces required?

**Hot Area:**

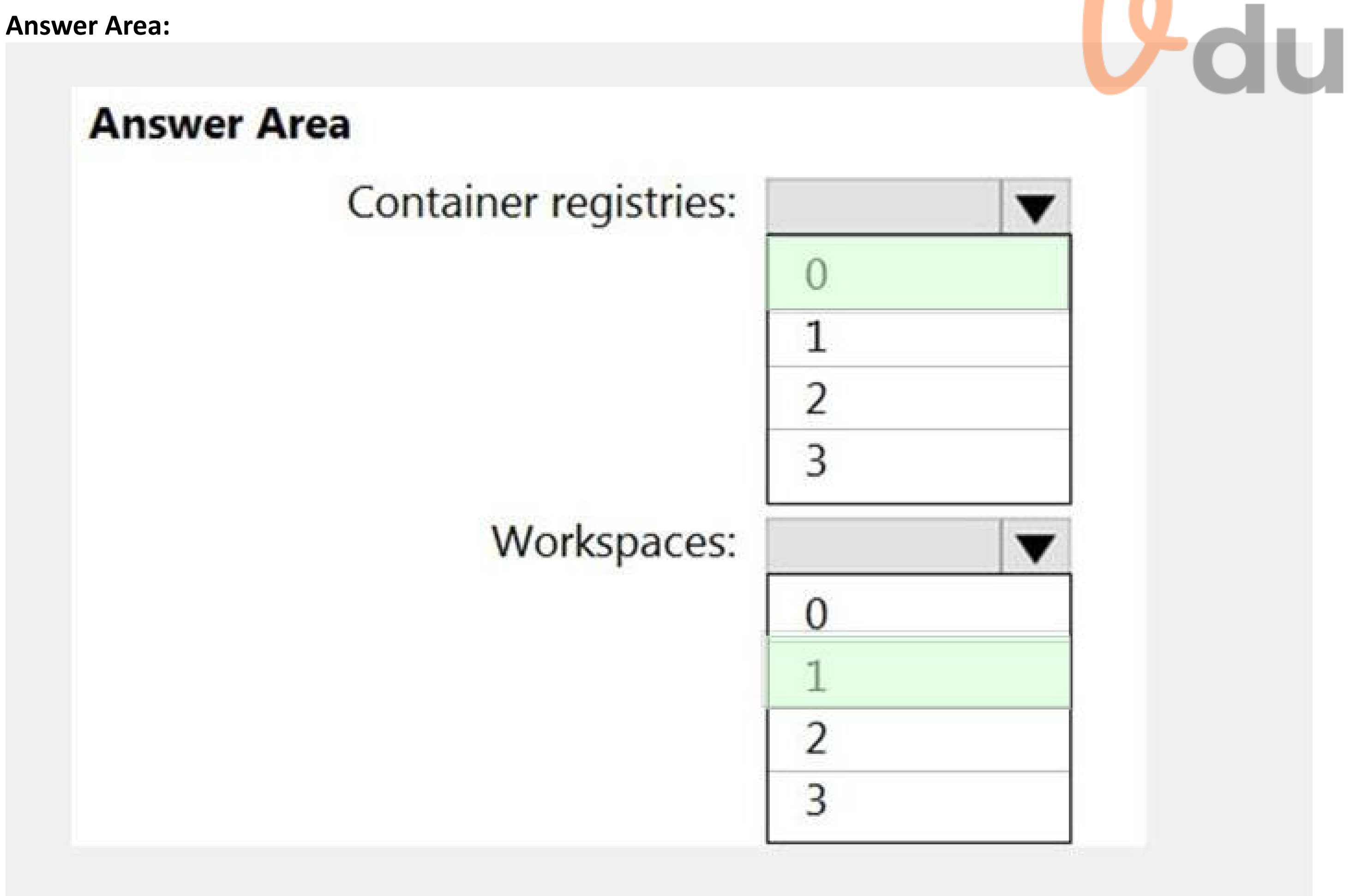


**Answer Area**

Container registries:
- 0
- 1
- 2
- 3

Workspaces:
- 0
- 1
- 2
- 3

**Answer Area:**



**Answer Area**

Container registries:
- [✓ 0]
- 1
- 2
- 3

Workspaces:
- 0
- [✓ 1]
- 2
- 3

**Section:**

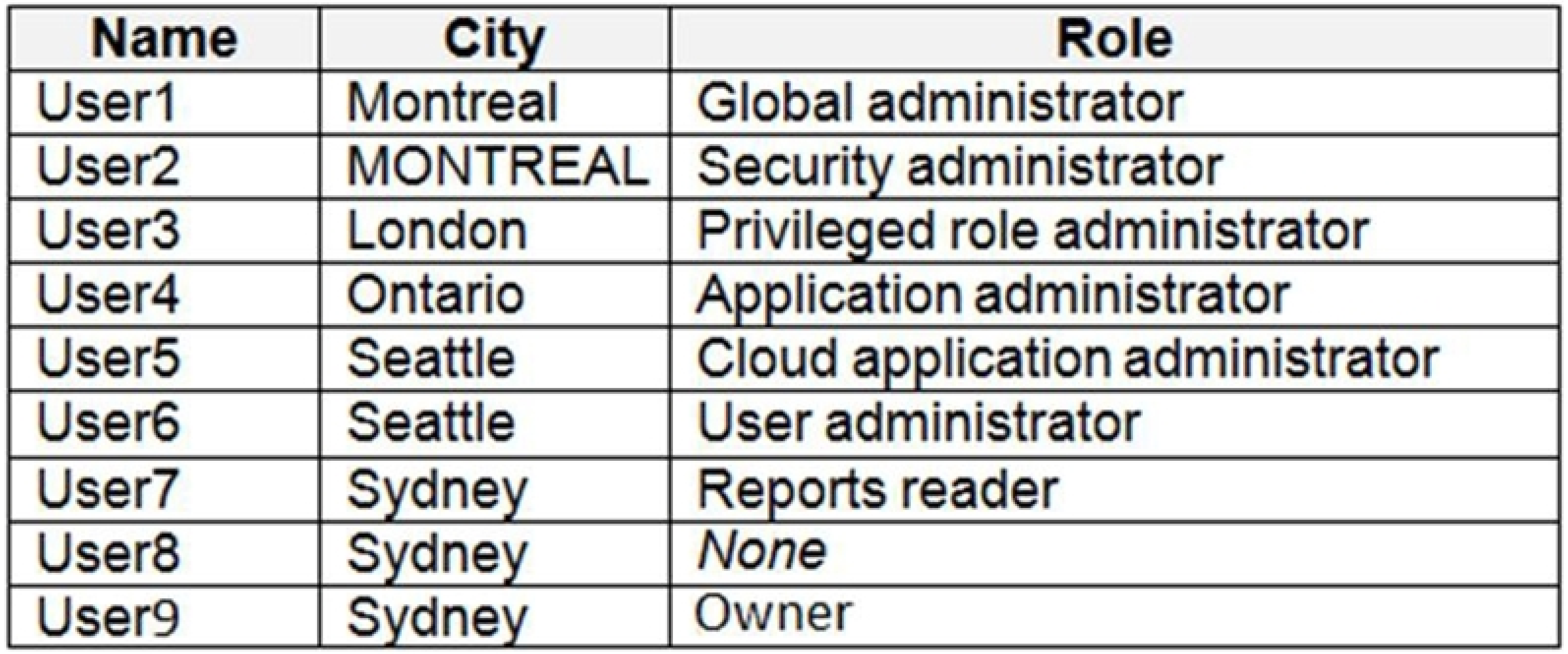
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

**QUESTION 2**
From Azure Security Center, you need to deploy SecPol1.
What should you do first?

A. Enable Azure Defender.
B. Create an Azure Management group.
C. Create an initiative.
D. Configure continuous export.

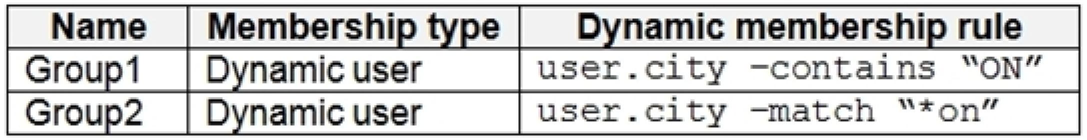
**Correct Answer: C**
**Section:**
**Explanation:**
Reference:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/security-center/custom-security-policies.md
https://zimmergren.net/create-custom-security-center-recommendation-with-azure-policy/

**02 - Manage security operations**
Case Study
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview
Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.
The company hosts its entire server infrastructure in Azure.
Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
Existing Environment
Azure AD
Contoso.com contains the users shown in the following table.



| Name | City | Role |
|---|---|---|
| User1 | Montreal | Global administrator |
| User2 | MONTREAL | Security administrator |
| User3 | London | Privileged role administrator |
| User4 | Ontario | Application administrator |
| User5 | Seattle | Cloud application administrator |
| User6 | Seattle | User administrator |
| User7 | Sydney | Reports reader |
| User8 | Sydney | *None* |
| User9 | Sydney | Owner |

Contoso.com contains the security groups shown in the following table.

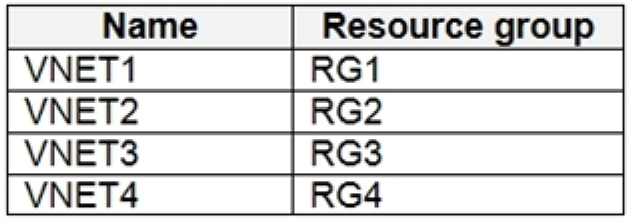


| Name | Membership type | Dynamic membership rule |
|---|---|---|
| Group1 | Dynamic user | `user.city –contains “ON”` |
| Group2 | Dynamic user | `user.city –match “*on”` |

Sub1

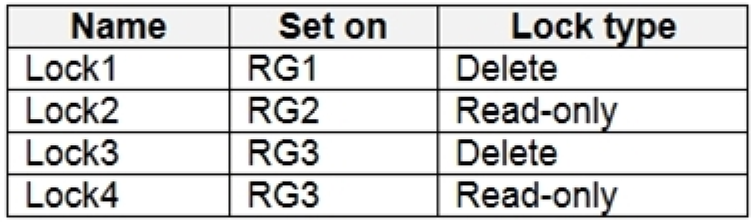
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.



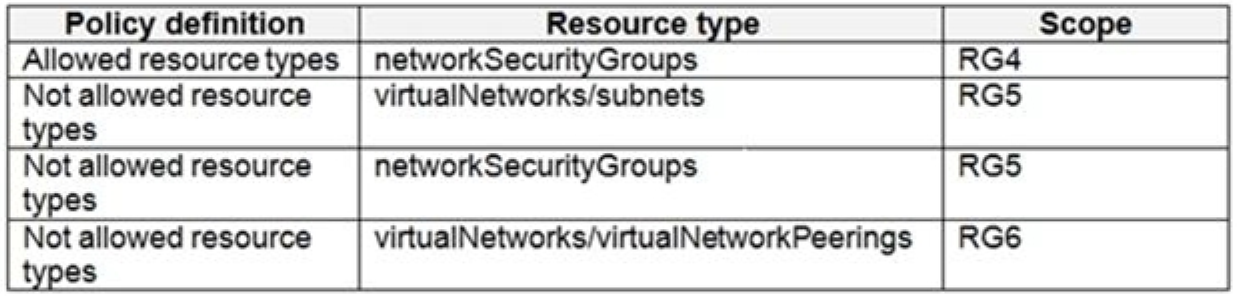
| Name | Resource group |
|---|---|
| VNET1 | RG1 |
| VNET2 | RG2 |
| VNET3 | RG3 |
| VNET4 | RG4 |

Sub1 contains the locks shown in the following table.



| Name | Set on | Lock type |
|---|---|---|
| Lock1 | RG1 | Delete |
| Lock2 | RG2 | Read-only |
| Lock3 | RG3 | Delete |
| Lock4 | RG3 | Read-only |

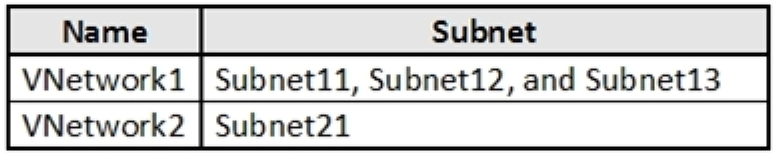
Sub1 contains the Azure policies shown in the following table.



| Policy definition | Resource type | Scope |
|---|---|---|
| Allowed resource types | networkSecurityGroups | RG4 |
| Not allowed resource types | virtualNetworks/subnets | RG5 |
| Not allowed resource types | networkSecurityGroups | RG5 |
| Not allowed resource types | virtualNetworks/virtualNetworkPeerings | RG6 |

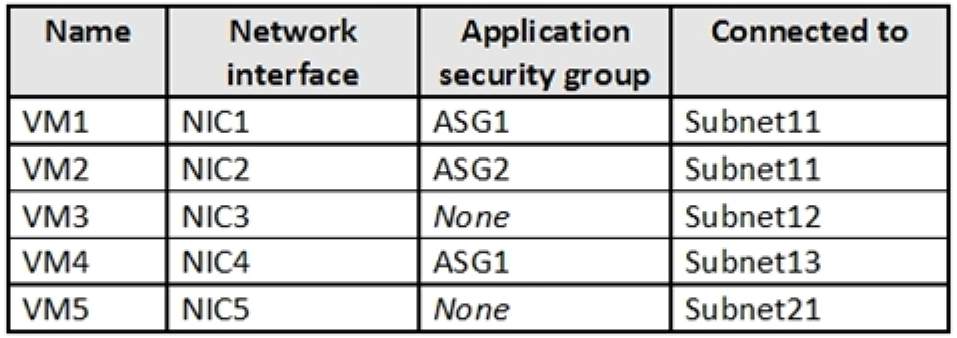
Sub2

Sub2 contains the virtual networks shown in the following table.



| Name | Subnet |
|---|---|
| VNetwork1 | Subnet11, Subnet12, and Subnet13 |
| VNetwork2 | Subnet21 |

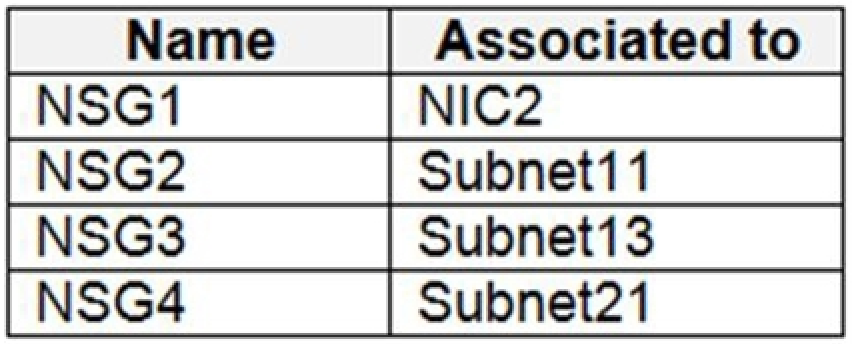
Sub2 contains the virtual machines shown in the following table.



| Name | Network interface | Application security group | Connected to |
|---|---|---|---|
| VM1 | NIC1 | ASG1 | Subnet11 |
| VM2 | NIC2 | ASG2 | Subnet11 |
| VM3 | NIC3 | *None* | Subnet12 |
| VM4 | NIC4 | ASG1 | Subnet13 |
| VM5 | NIC5 | *None* | Subnet21 |

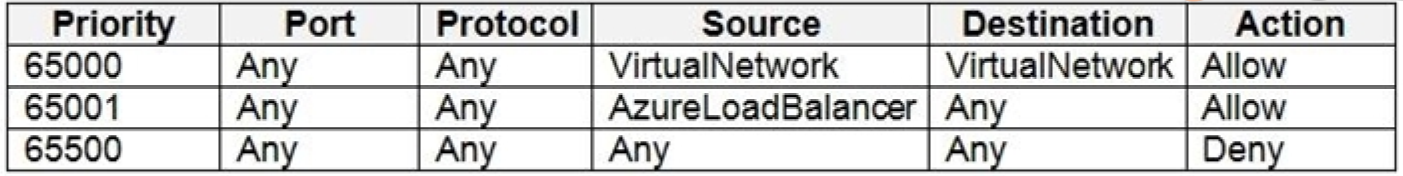
All virtual machines have public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

Sub2 contains the network security groups (NSGs) shown in the following table.



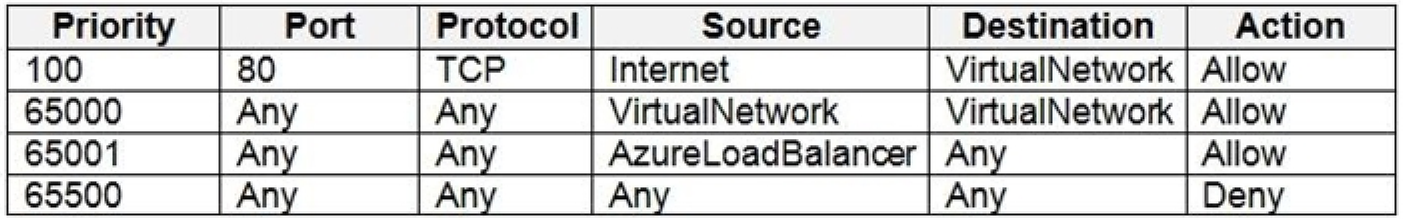
| Name | Associated to |
|---|---|
| NSG1 | NIC2 |
| NSG2 | Subnet11 |
| NSG3 | Subnet13 |
| NSG4 | Subnet21 |

NSG1 has the inbound security rules shown in the following table.



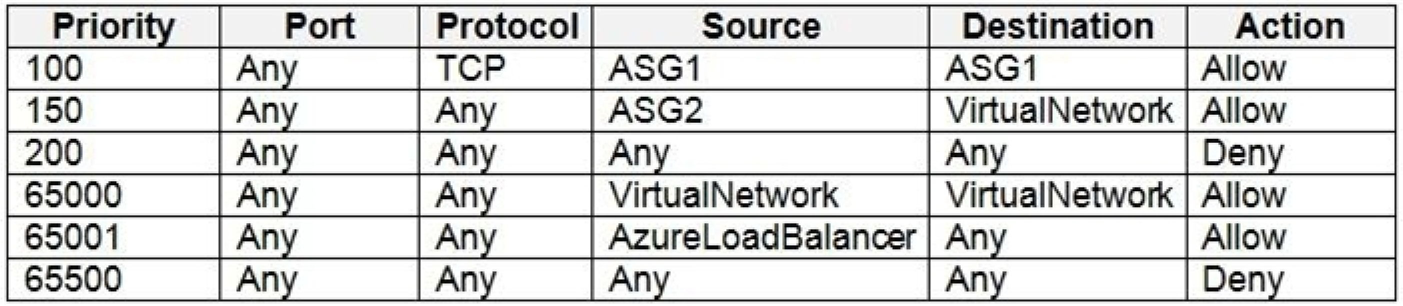
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

NSG2 has the inbound security rules shown in the following table.



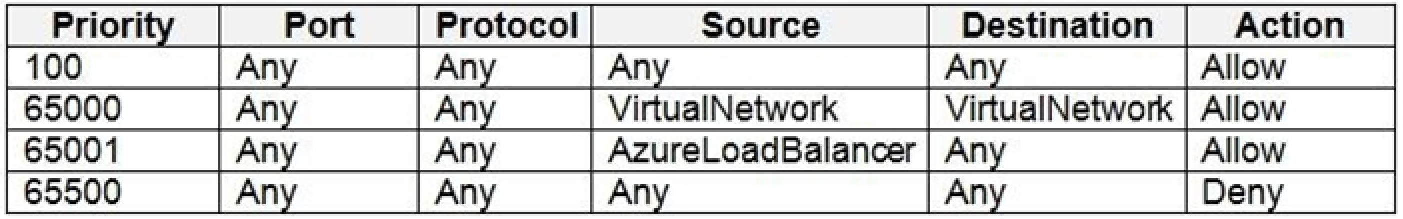
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 100 | 80 | TCP | Internet | VirtualNetwork | Allow |
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

NSG3 has the inbound security rules shown in the following table.



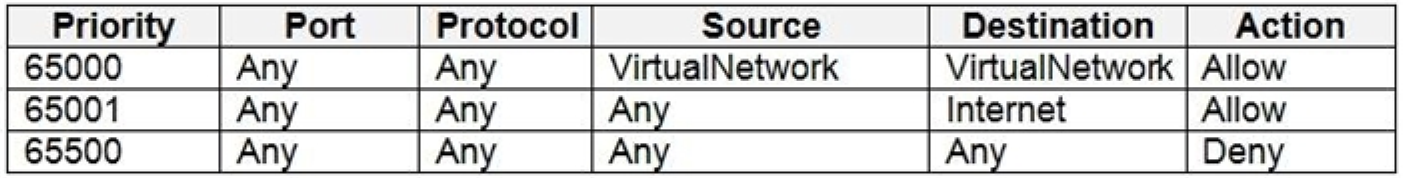
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 100 | Any | TCP | ASG1 | ASG1 | Allow |
| 150 | Any | Any | ASG2 | VirtualNetwork | Allow |
| 200 | Any | Any | Any | Any | Deny |
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

NSG4 has the inbound security rules shown in the following table.



| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 100 | Any | Any | Any | Any | Allow |
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.



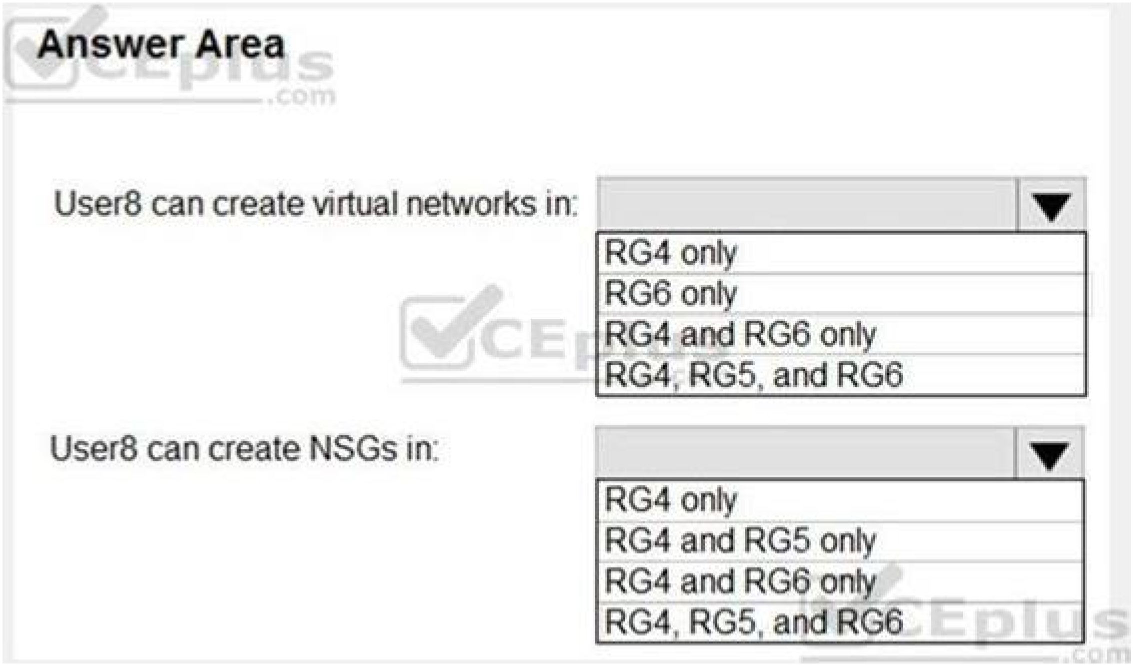
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | Any | Internet | Allow |
| 65500 | Any | Any | Any | Any | Deny |

Technical requirements
Contoso identifies the following technical requirements:
Deploy Azure Firewall to VNetwork1 in Sub2.
Register an application named App2 in contoso.com.
Whenever possible, use the principle of least privilege.
Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

**QUESTION 1**

You assign User8 the Owner role for RG4, RG5, and RG6.In which resource groups can User8 create virtual networks and NSGs? You must be able to connect virtual machines to deployed virtual networks. To answer, select the appropriate options in the answer area.NOTE: Each correct selection is worth one point.

**Hot Area:**

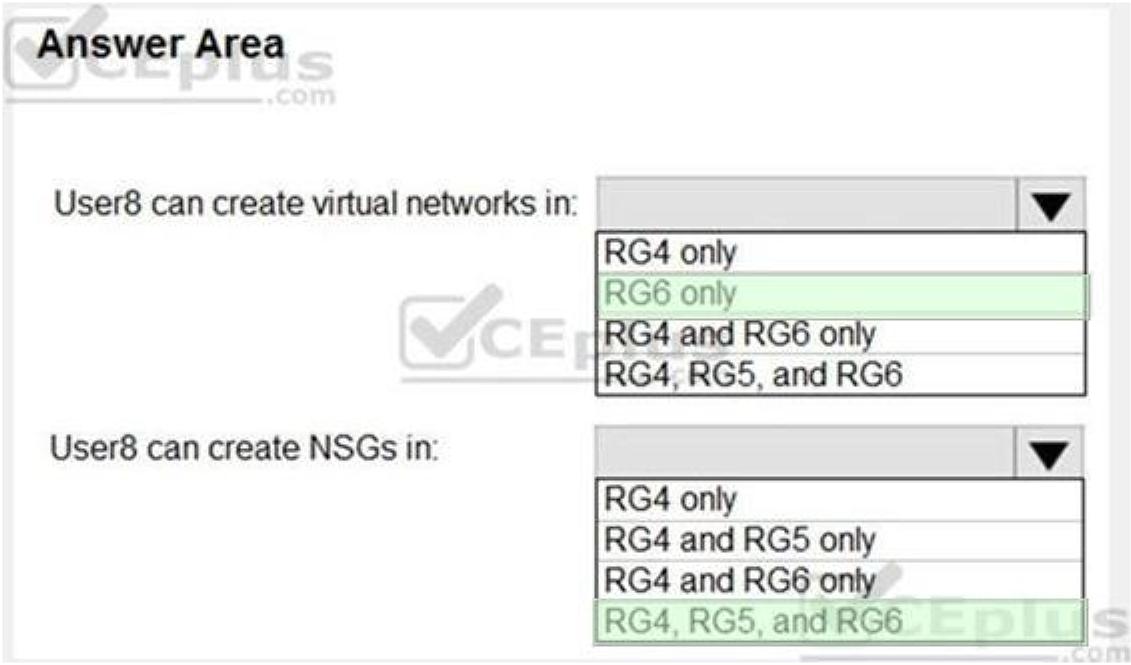


Answer Area

User8 can create virtual networks in:

User8 can create NSGs in:

**Answer Area:**



Answer Area

User8 can create virtual networks in:

- RG4 only
- [✓ RG6 only]
- RG4 and RG6 only
- RG4, RG5, and RG6

User8 can create NSGs in:

- RG4 only
- RG4 and RG5 only
- RG4 and RG6 only
- [✓ RG4, RG5, and RG6]

**Section:**
**Explanation:**

Box 1: RG6 only

The policy does not allow the creation of virtual networks/subnets in RG5. Only NSGs can be created in RG4.B

Box 2: Rg4,Rg5, and Rg6

Scenario:

Contoso has two Azure subscriptions named Sub1 and Sub2.

Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

You assign User8 the Owner role for RG4, RG5, and RG6

User8 city Sidney, Role:None

Note: A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager).

References:

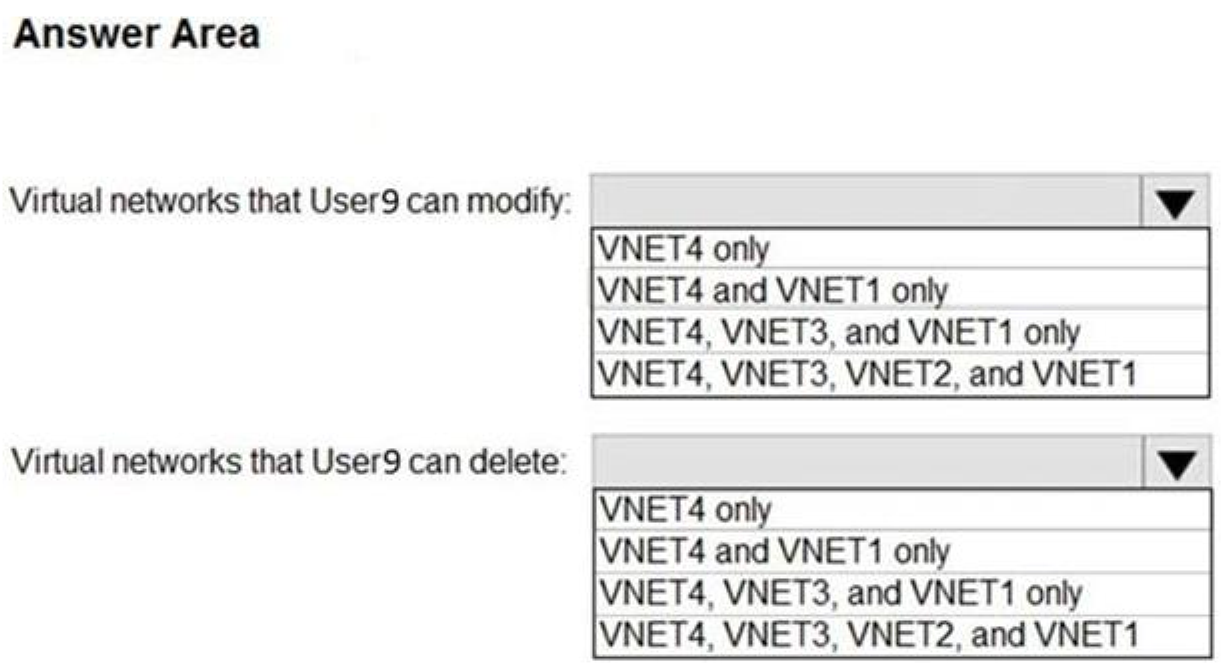
https://docs.microsoft.com/en-us/azure/governance/policy/overview

**QUESTION 2**

Which virtual networks in Sub1 can User9 modify and delete in their current state? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Hot Area:**



Answer Area

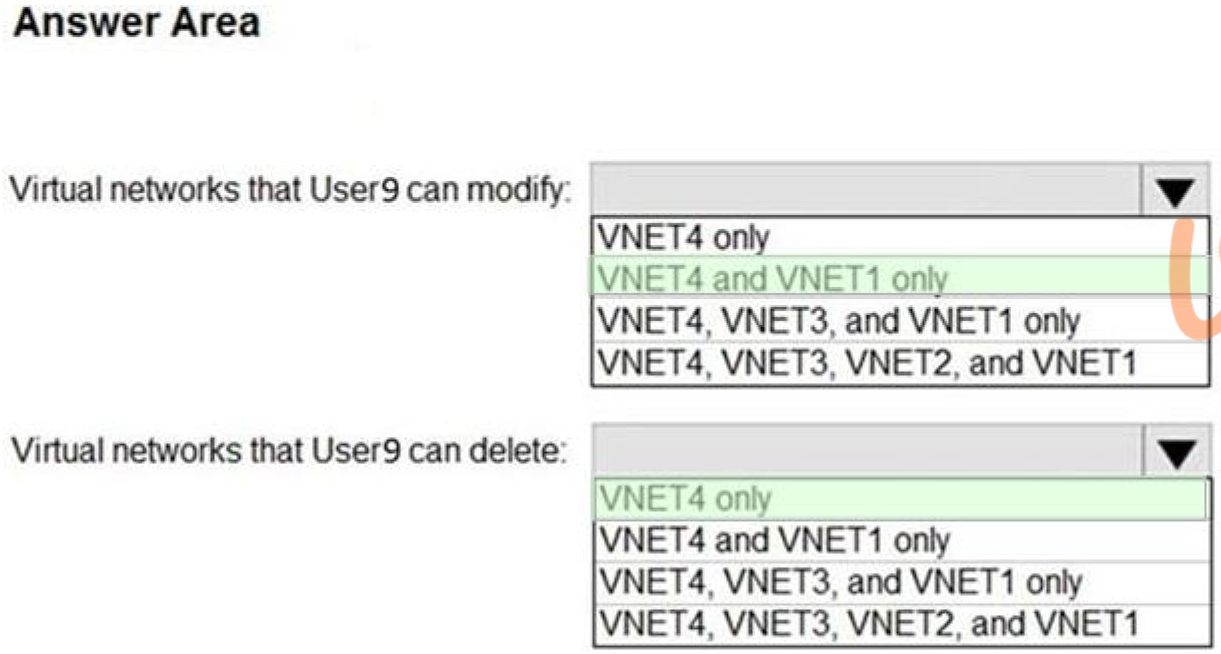
Virtual networks that User9 can modify:

- VNET4 only
- VNET4 and VNET1 only
- VNET4, VNET3, and VNET1 only
- VNET4, VNET3, VNET2, and VNET1

Virtual networks that User9 can delete:

- VNET4 only
- VNET4 and VNET1 only
- VNET4, VNET3, and VNET1 only
- VNET4, VNET3, VNET2, and VNET1

**Answer Area:**



Answer Area

Virtual networks that User9 can modify:

- VNET4 only
- [✓ VNET4 and VNET1 only]
- VNET4, VNET3, and VNET1 only
- VNET4, VNET3, VNET2, and VNET1

Virtual networks that User9 can delete:

- [✓ VNET4 only]
- VNET4 and VNET1 only
- VNET4, VNET3, and VNET1 only
- VNET4, VNET3, VNET2, and VNET1

**Section:**

**Explanation:**

Box 1: VNET4 and VNET1 only

RG1 has only Delete lock, while there are no locks on RG4.

RG2 and RG3 both have Read-only locks.

Box 2: VNET4 only

There are no locks on RG4, while the other resource groups have either Delete or Read-only locks.

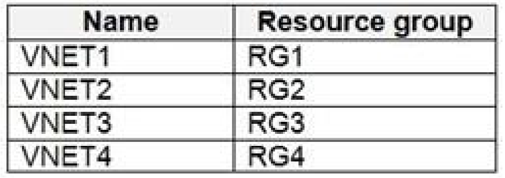
Note: As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.

CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource. ReadOnly means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Scenario:

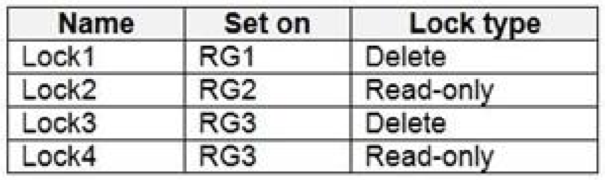
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.



| Name | Resource group |
|---|---|
| VNET1 | RG1 |
| VNET2 | RG2 |
| VNET3 | RG3 |
| VNET4 | RG4 |

Sub1 contains the locks shown in the following table.



| Name | Set on | Lock type |
|---|---|---|
| Lock1 | RG1 | Delete |
| Lock2 | RG2 | Read-only |
| Lock3 | RG3 | Delete |
| Lock4 | RG3 | Read-only |

Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

**03 - Manage security operations**

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

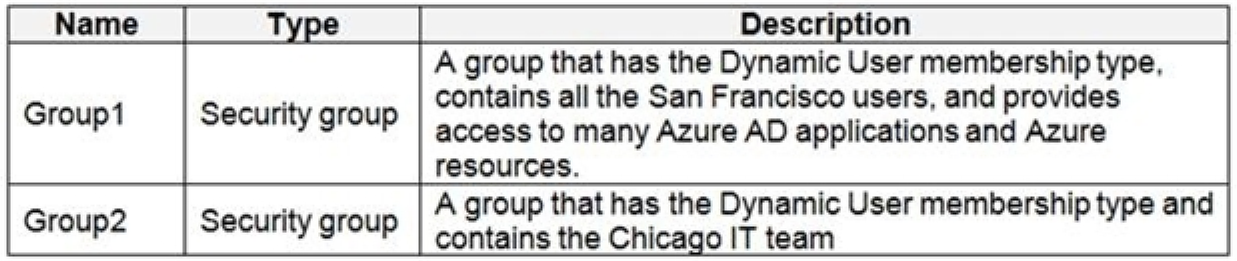
Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

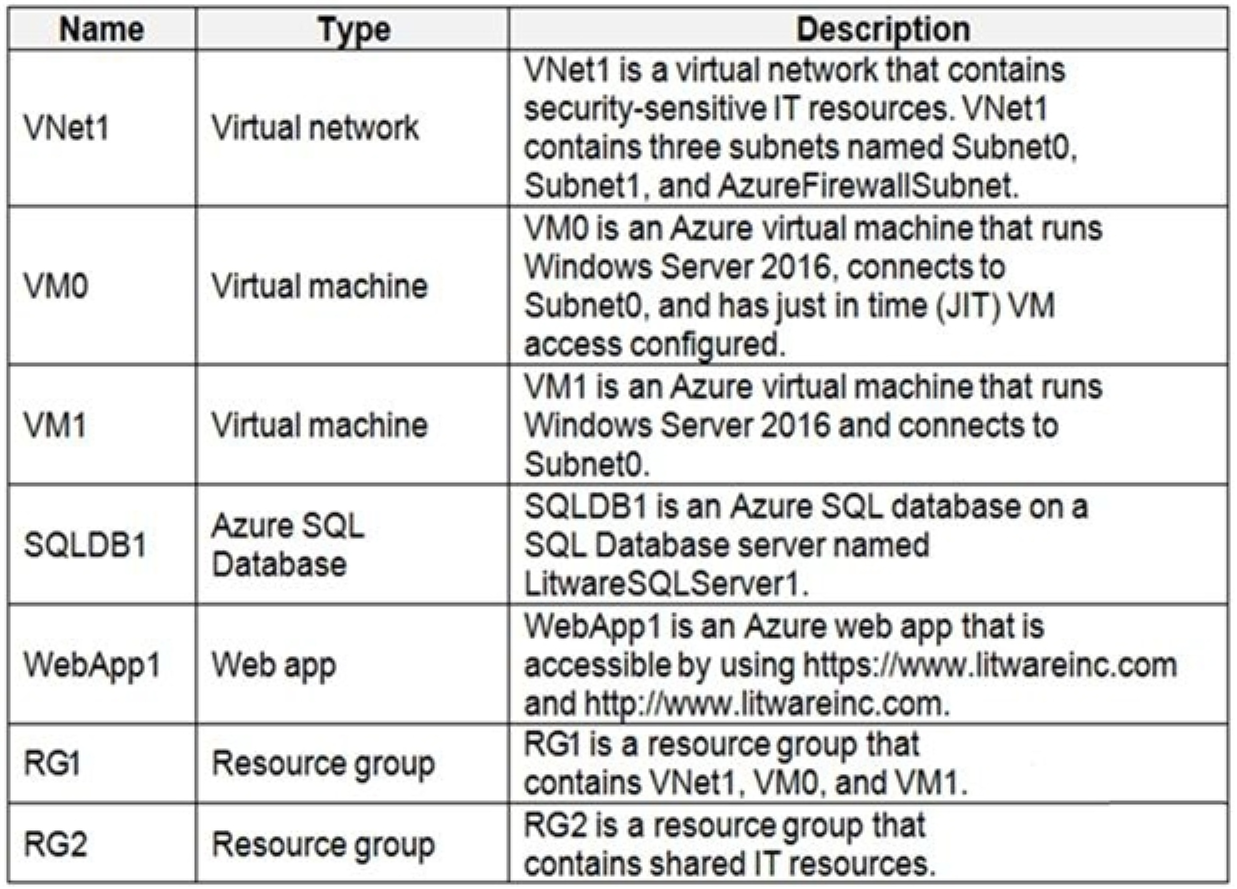
Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.



| Name | Type | Description |
|---|---|---|
| Group1 | Security group | A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources. |
| Group2 | Security group | A group that has the Dynamic User membership type and contains the Chicago IT team |

The Azure subscription contains the objects shown in the following table.



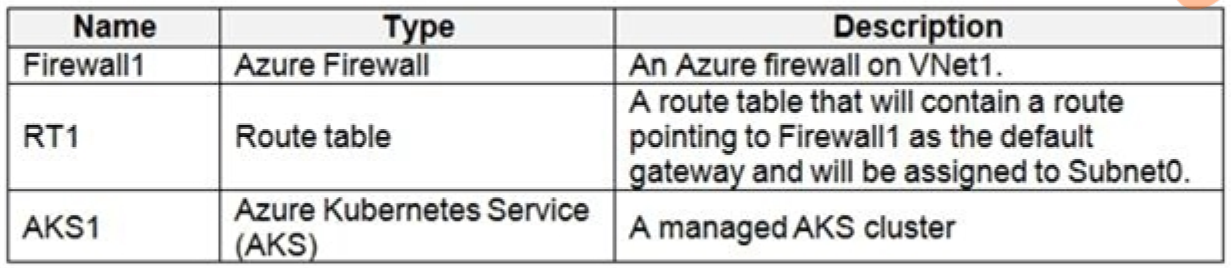
| Name | Type | Description |
|---|---|---|
| VNet1 | Virtual network | VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet. |
| VM0 | Virtual machine | VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured. |
| VM1 | Virtual machine | VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0. |
| SQLDB1 | Azure SQL Database | SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1. |
| WebApp1 | Web app | WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com. |
| RG1 | Resource group | RG1 is a resource group that contains VNet1, VM0, and VM1. |
| RG2 | Resource group | RG2 is a resource group that contains shared IT resources. |

Azure Security Center is set to the Standard tier.

Requirements

Planned Changes

Litware plans to deploy the Azure resources shown in the following table.



| Name | Type | Description |
|---|---|---|
| Firewall1 | Azure Firewall | An Azure firewall on VNet1. |
| RT1 | Route table | A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0. |
| AKS1 | Azure Kubernetes Service (AKS) | A managed AKS cluster |

Identity and Access Requirements

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.

The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment. Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

Platform Protection Requirements

Litware identifies the following platform protection requirements:

Microsoft Antimalware must be installed on the virtual machines in RG1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access. A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.

Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center. Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

WebApp1 must enforce mutual authentication.

General Requirements

Litware identifies the following general requirements:
Whenever possible, administrative effort must be minimized.
Whenever possible, use of automation must be maximized.

**QUESTION 1**
You need to ensure that you can meet the security operations requirements. What should you do first?

A. Turn on Auto Provisioning in Security Center.
B. Integrate Security Center and Microsoft Cloud App Security.
C. Upgrade the pricing tier of Security Center to Standard.
D. Modify the Security Center workspace configuration.

**Correct Answer: C**
**Section:**
**Explanation:**
The Standard tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The Standard tier also adds advanced threat detection capabilities, which uses built-in behavioral analytics and machine learning to identify attacks and zero-days exploits, access and application controls to reduce exposure to network attacks and malware, and more.
Scenario: Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing

**01 - Secure data and applications**

**QUESTION 1**
You need to recommend which virtual machines to use to host App1. The solution must meet the technical requirements for KeyVault1.
Which virtual machines should you use?

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

**Correct Answer: D**
**Section:**
**Explanation:**

**02 - Secure data and applications**
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Overview

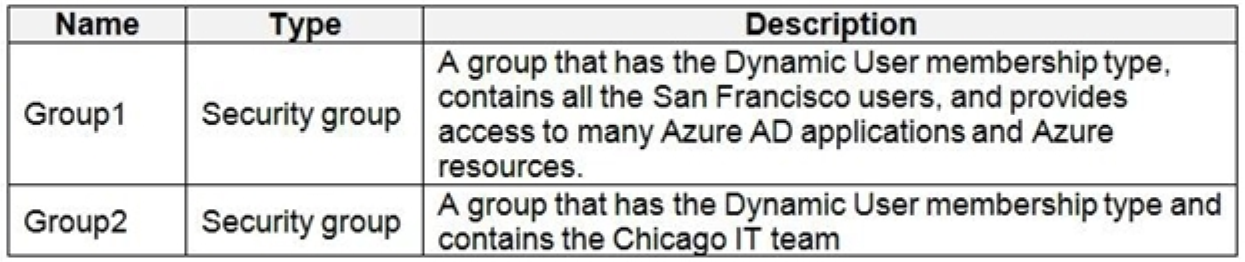
Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

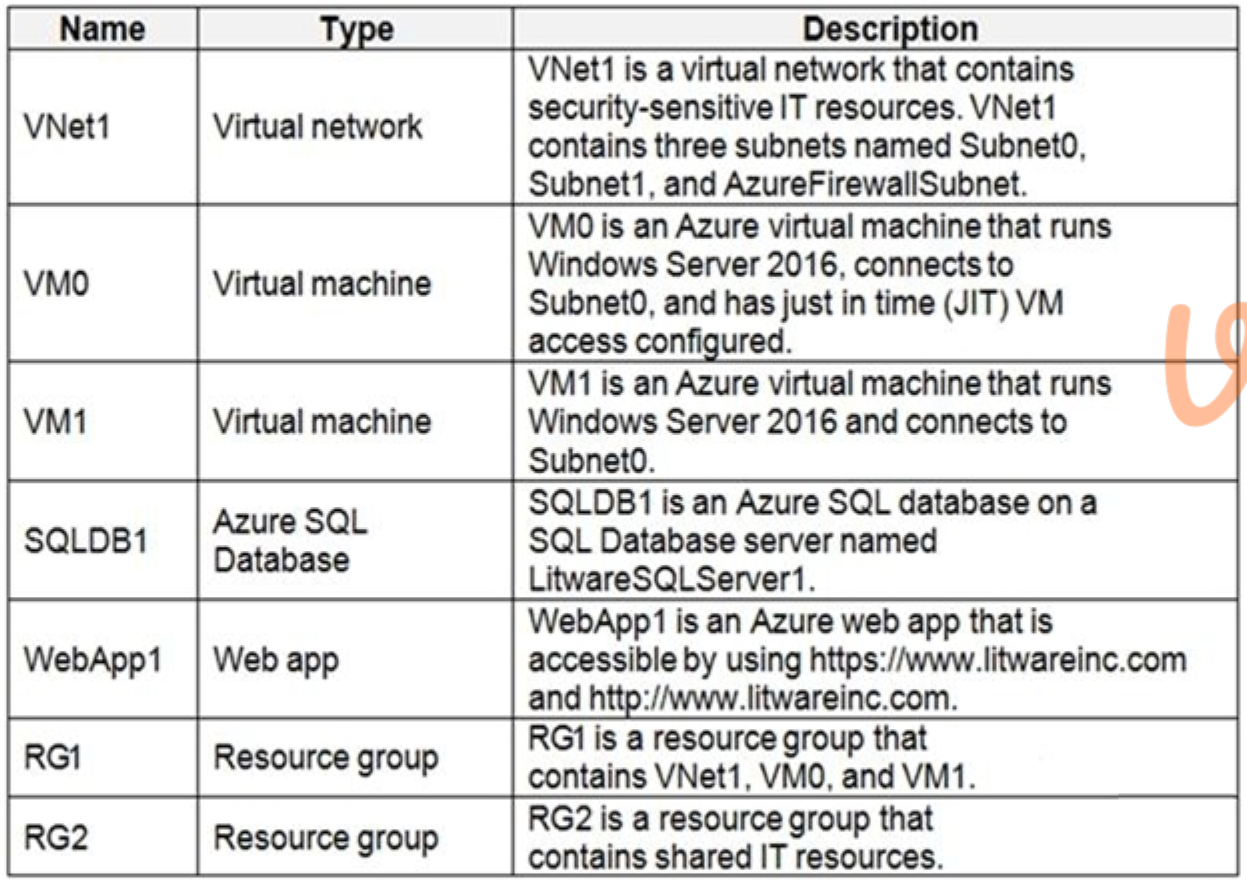
Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.



| Name | Type | Description |
|---|---|---|
| Group1 | Security group | A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources. |
| Group2 | Security group | A group that has the Dynamic User membership type and contains the Chicago IT team |

The Azure subscription contains the objects shown in the following table.



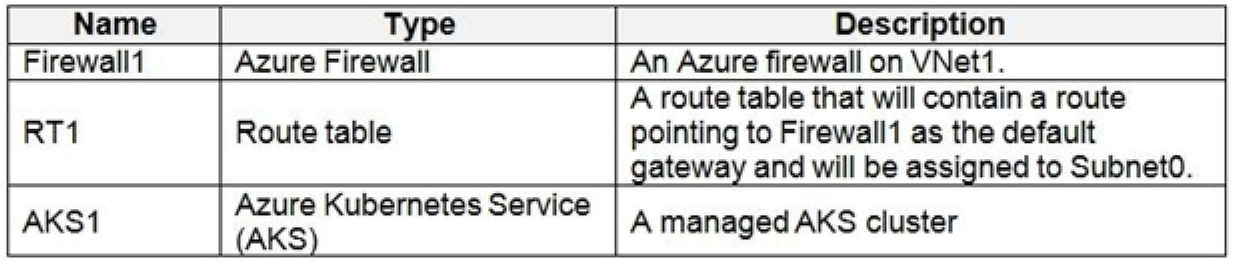
| Name | Type | Description |
|---|---|---|
| VNet1 | Virtual network | VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet. |
| VM0 | Virtual machine | VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured. |
| VM1 | Virtual machine | VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0. |
| SQLDB1 | Azure SQL Database | SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1. |
| WebApp1 | Web app | WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com. |
| RG1 | Resource group | RG1 is a resource group that contains VNet1, VM0, and VM1. |
| RG2 | Resource group | RG2 is a resource group that contains shared IT resources. |

Azure Security Center is set to the Standard tier.

Requirements

Planned Changes

Litware plans to deploy the Azure resources shown in the following table.



| Name | Type | Description |
|---|---|---|
| Firewall1 | Azure Firewall | An Azure firewall on VNet1. |
| RT1 | Route table | A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0. |
| AKS1 | Azure Kubernetes Service (AKS) | A managed AKS cluster |

Identity and Access Requirements

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.
The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment. Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.
Platform Protection Requirements
Litware identifies the following platform protection requirements:
Microsoft Antimalware must be installed on the virtual machines in RG1.
The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.
Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access. A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.
Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center. Data and Application Requirements
Litware identifies the following data and applications requirements:
The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.
WebApp1 must enforce mutual authentication.
General Requirements
Litware identifies the following general requirements:
Whenever possible, administrative effort must be minimized.
Whenever possible, use of automation must be maximized.

**QUESTION 1**

You need to configure WebApp1 to meet the data and application requirements.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Upload a public certificate.
B. Turn on the HTTPS Only protocol setting.
C. Set the Minimum TLS Version protocol setting to 1.2.
D. Change the pricing tier of the App Service plan.
E. Turn on the Incoming client certificates protocol setting.

**Correct Answer: A, C**
**Section:**
**Explanation:**
A: To configure Certificates for use in Azure Websites Applications you need to upload a public Certificate.
C: Over time, multiple versions of TLS have been released to mitigate different vulnerabilities. TLS 1.2 is the most current version available for apps running on Azure App Service.
Incorrect Answers:
B: We need support the http url as well.
Note:

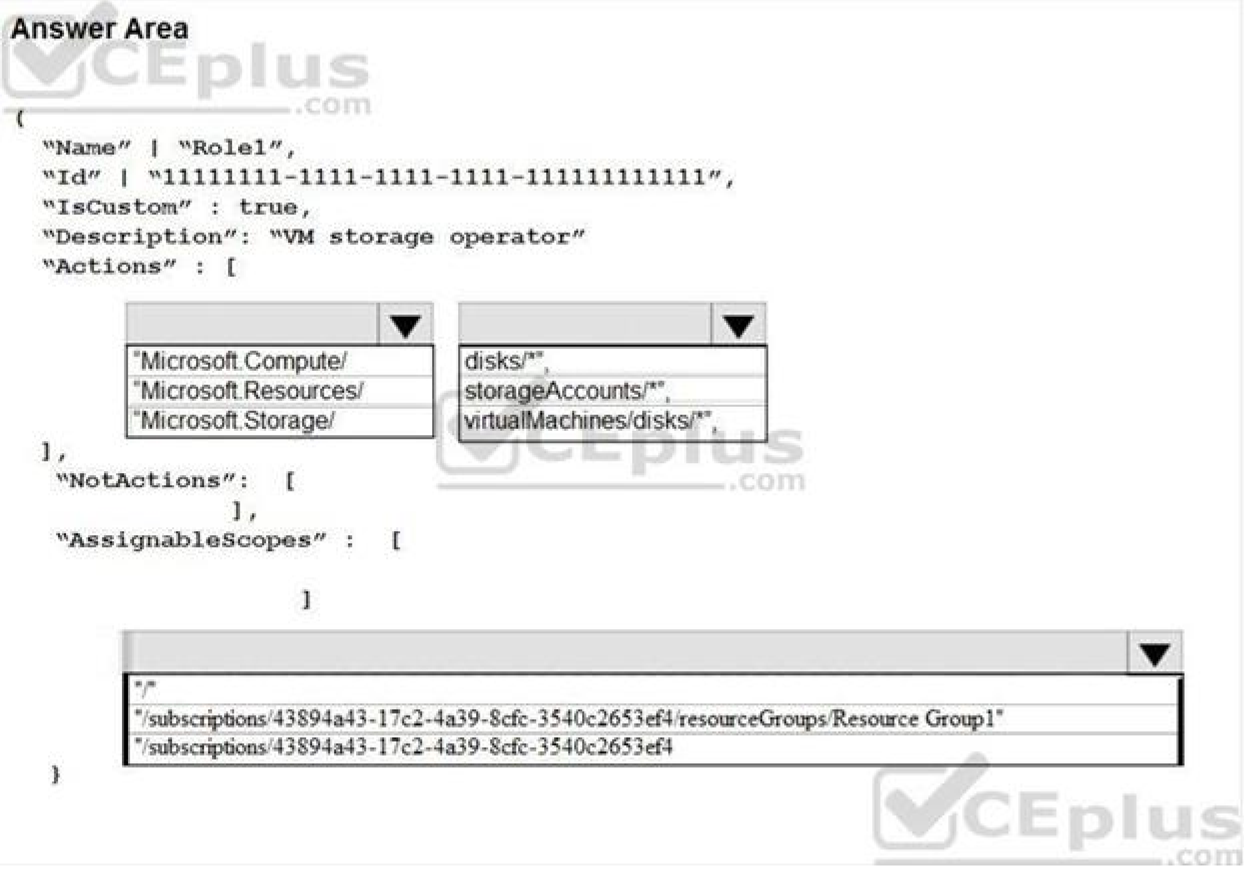
WebApp1 is an Azure web app that is accessible by using https://litwareinc.com and http://www.litwareinc.com.

References:
https://docs.microsoft.com/en-us/azure/app-service/app-service-web-configure-tls-mutual-auth
https://azure.microsoft.com/en-us/updates/app-service-and-functions-hosted-apps-can-now-update-tls-versions/

**QUESTION 2**

HOTSPOT
You need to create Role1 to meet the platform protection requirements.
How should you complete the role definition of Role1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Hot Area:**



Answer Area

```
{
  "Name" | "Role1",
  "Id" | "11111111-1111-1111-1111-111111111111",
  "IsCustom" : true,
  "Description": "VM storage operator"
  "Actions" : [
```

- "Microsoft.Compute/
- "Microsoft.Resources/
- "Microsoft.Storage/

- disks/*",
- storageAccounts/*",
- virtualMachines/disks/*",

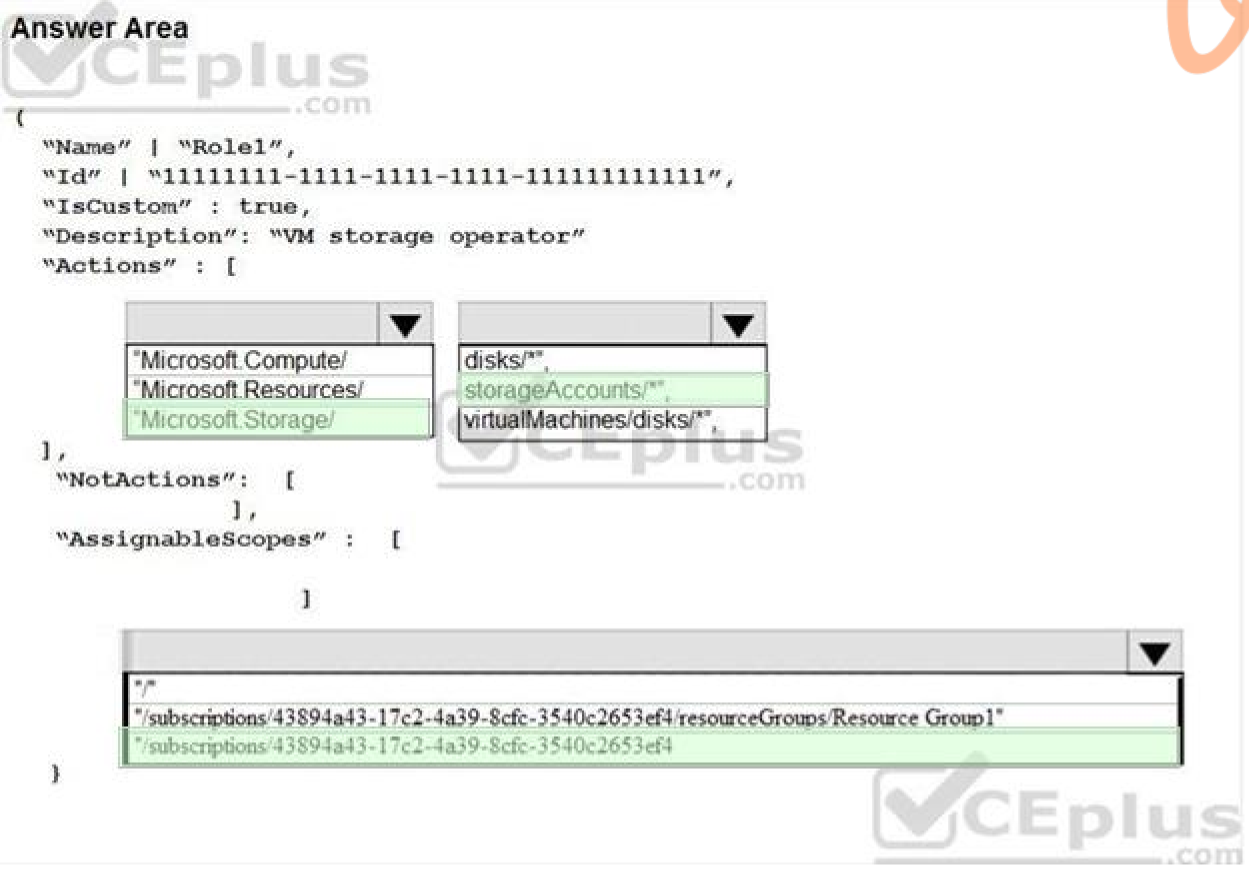
```
  ],
   "NotActions":  [
                ],
   "AssignableScopes" :  [

                     ]
```

- "/*
- "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1"
- "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4

```
 }
```

**Answer Area:**



Answer Area

```
{
  "Name" | "Role1",
  "Id" | "11111111-1111-1111-1111-111111111111",
  "IsCustom" : true,
  "Description": "VM storage operator"
  "Actions" : [
```

- "Microsoft.Compute/
- "Microsoft.Resources/
- "Microsoft.Storage/

- disks/*",
- storageAccounts/*",
- virtualMachines/disks/*",

```
  ],
   "NotActions":  [
                ],
   "AssignableScopes" :  [

                     ]
```

- "/*
- "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1"
- "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4

```
 }
```

**Section:**

**Explanation:**

Scenario: A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.

Azure RBAC template managed disks "Microsoft.Storage/"
Reference:
https://blogs.msdn.microsoft.com/azureedu/2017/02/11/new-managed-disk-storage-option-for-your-azure-vms/
https://blogs.msdn.microsoft.com/azure4fun/2016/10/21/custom-azure-rbac-roles-and-how-to-extend-existing-role-definitions-scope/

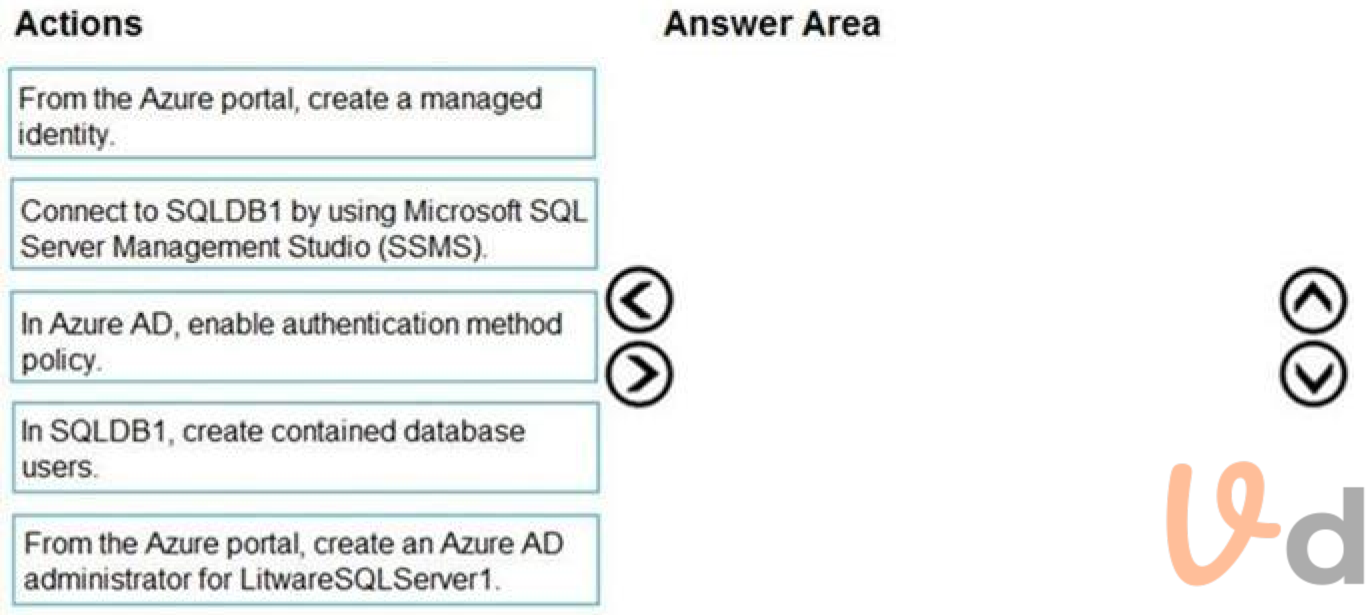
**QUESTION 3**

DRAG DROP

You need to configure SQLDB1 to meet the data and application requirements.

Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

**Select and Place:**

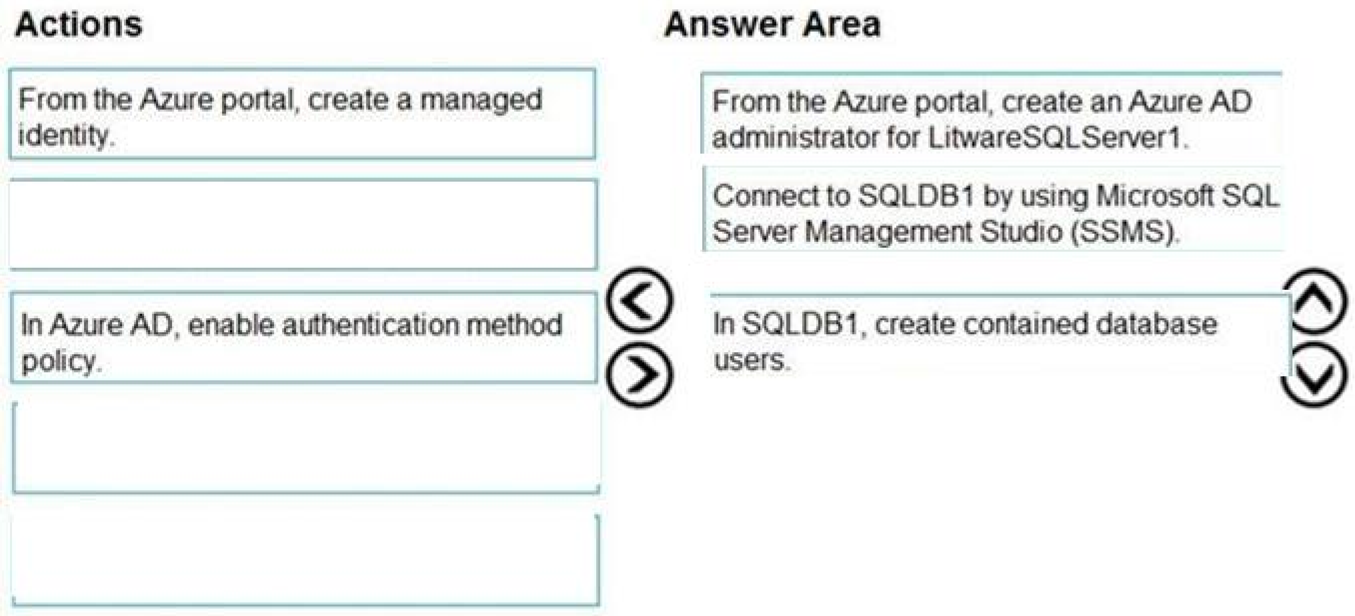


Actions

- From the Azure portal, create a managed identity.
- Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS).
- In Azure AD, enable authentication method policy.
- In SQLDB1, create contained database users.
- From the Azure portal, create an Azure AD administrator for LitwareSQLServer1.

Answer Area

**Correct Answer:**



Actions

- From the Azure portal, create a managed identity.
- In Azure AD, enable authentication method policy.

Answer Area

- From the Azure portal, create an Azure AD administrator for LitwareSQLServer1.
- Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS).
- In SQLDB1, create contained database users.

**Section:**

**Explanation:**

Reference:
https://docs.microsoft.com/en-gb/azure/azure-sql/database/authentication-aad-overview

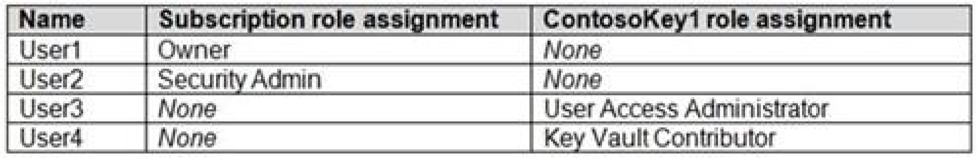
**03 - Secure data and applications**

**QUESTION 1**

HOTSPOT

You have an Azure subscription that contains an Azure key vault named ContosoKey1.

You create users and assign them roles as shown in the following table.



| Name | Subscription role assignment | ContosoKey1 role assignment |
|---|---|---|
| User1 | Owner | *None* |
| User2 | Security Admin | *None* |
| User3 | *None* | User Access Administrator |
| User4 | *None* | Key Vault Contributor |

You need to identify which users can perform the following actions:

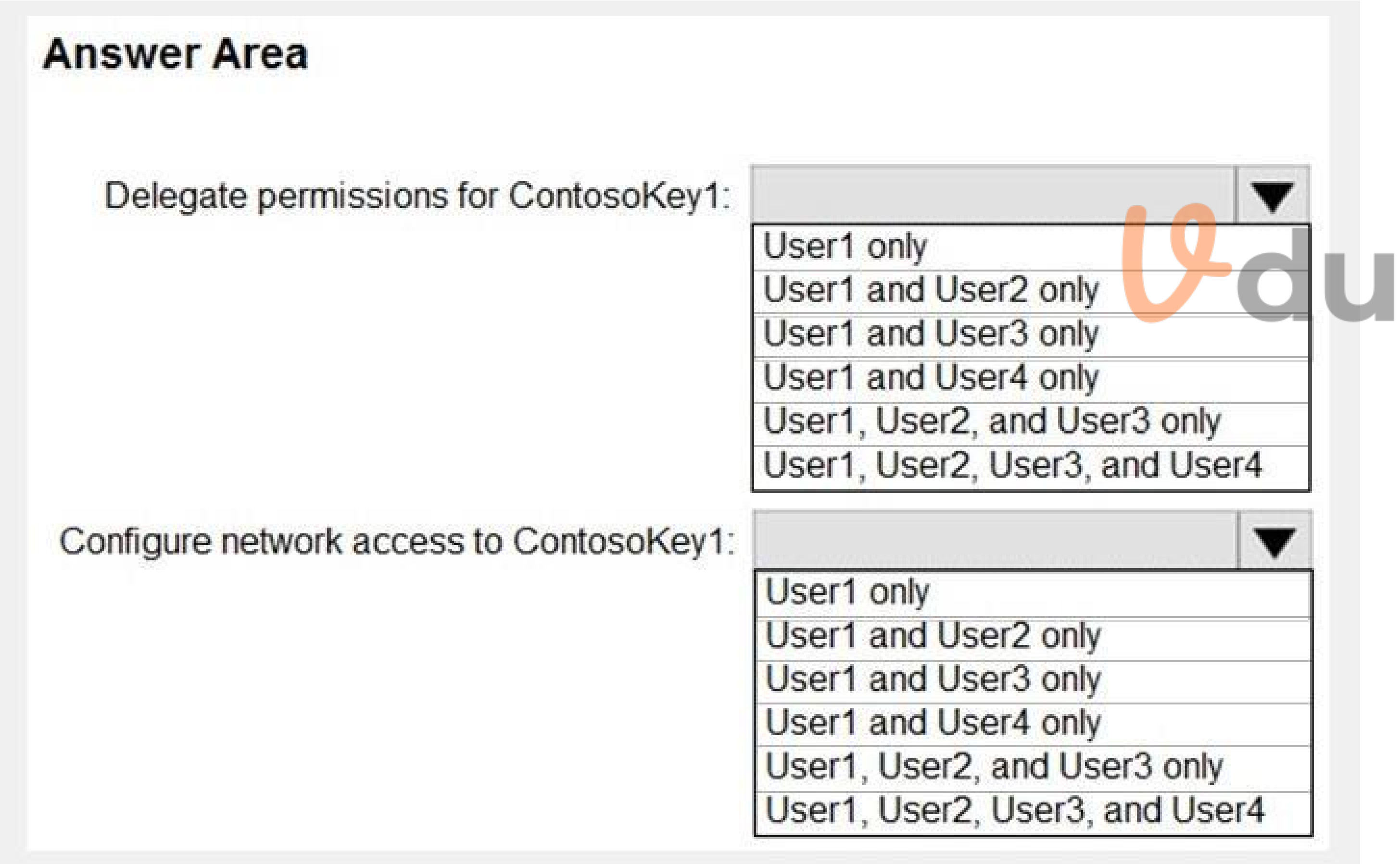
Delegate permissions for ContsosKey1.

Configure network access to ContosoKey1.

Which users should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Hot Area:**



**Answer Area**

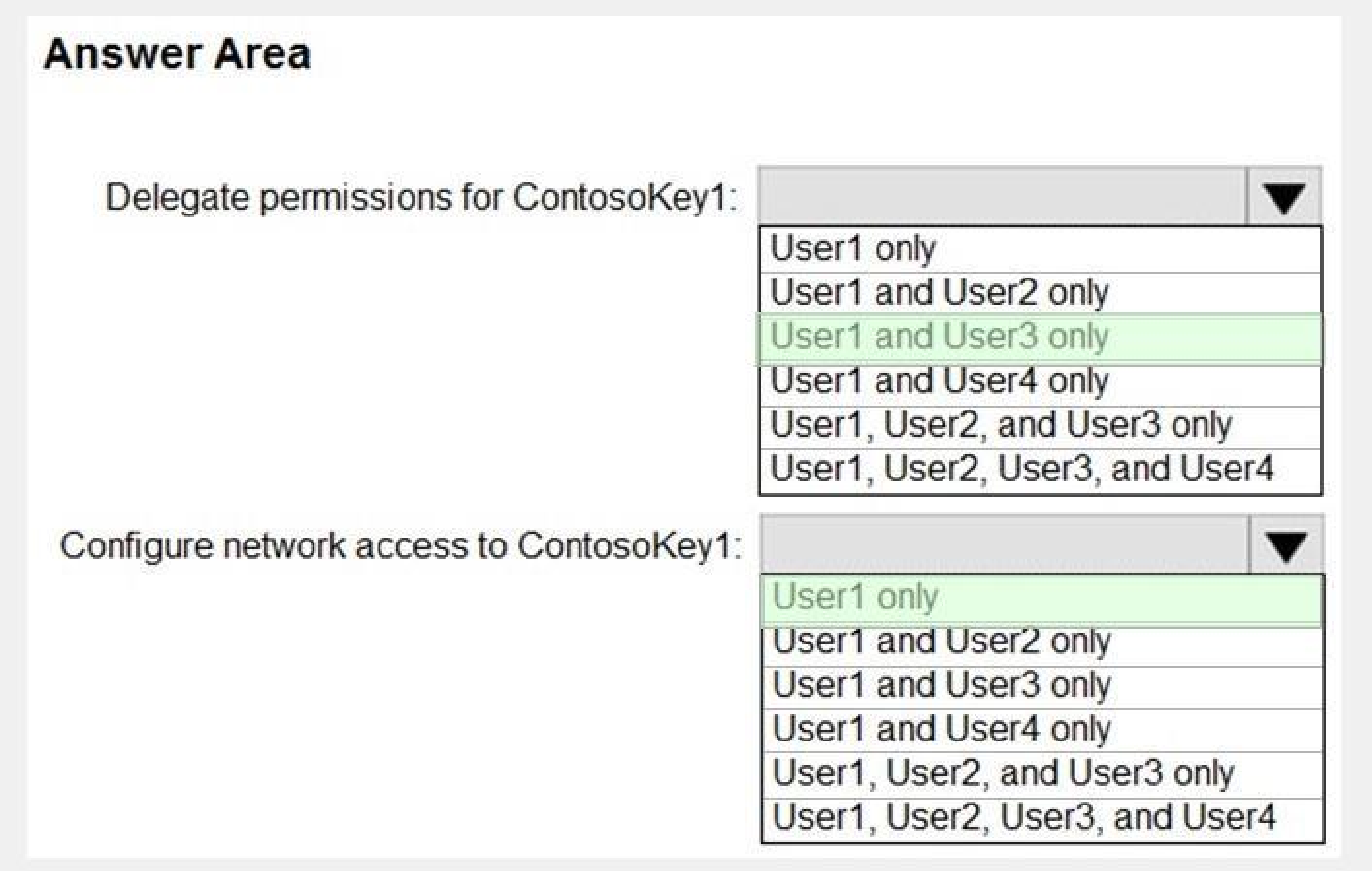
Delegate permissions for ContosoKey1:

- User1 only
- User1 and User2 only
- User1 and User3 only
- User1 and User4 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

Configure network access to ContosoKey1:

- User1 only
- User1 and User2 only
- User1 and User3 only
- User1 and User4 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

**Answer Area:**



Answer Area

Delegate permissions for ContosoKey1: ▼

- User1 only
- User1 and User2 only
- [✓ User1 and User3 only]
- User1 and User4 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

Configure network access to ContosoKey1: ▼

- [✓ User1 only]
- User1 and User2 only
- User1 and User3 only
- User1 and User4 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-gb/azure/key-vault/general/rbac-guide

**QUESTION 2**
You have an Azure subscription that contains four Azure SQL managed instances.
You need to evaluate the vulnerability of the managed instances to SQL injection attacks.
What should you do first?

A. Create an Azure Sentinel workspace.

B. Enable Advanced Data Security.

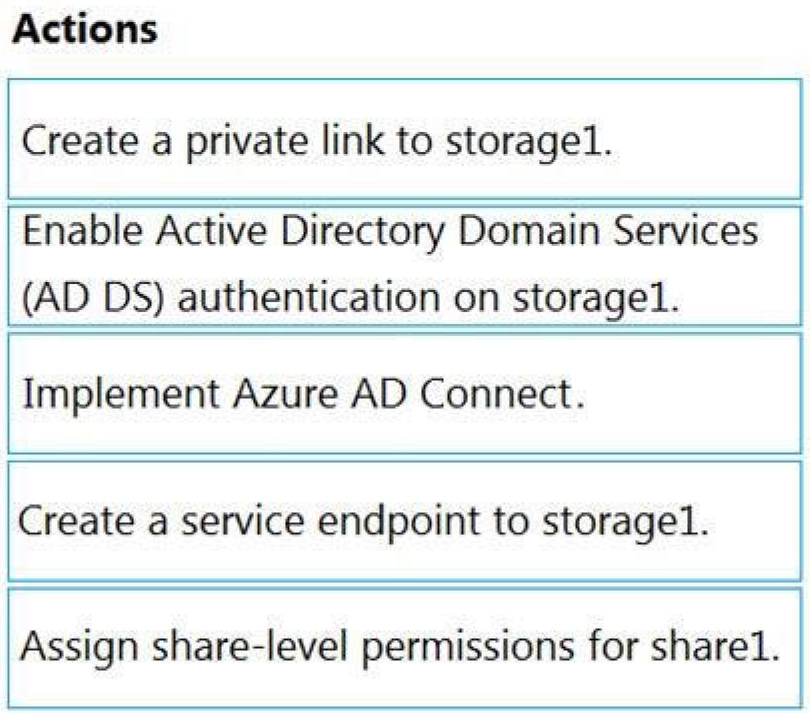
C. Add the SQL Health Check solution to Azure Monitor.

D. Create an Azure Advanced Threat Protection (ATP) instance.

**Correct Answer: B**
**Section:**

**QUESTION 3**
DRAG DROP
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains a user named User1.
You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains an Azure Storage account named storage1. Storage1 contains an Azure file share named share1.
Currently, the domain and the tenant are not integrated.
You need to ensure that User1 can access share1 by using his domain credentials.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

**Select and Place:**



**Actions**

Create a private link to storage1.

Enable Active Directory Domain Services (AD DS) authentication on storage1.

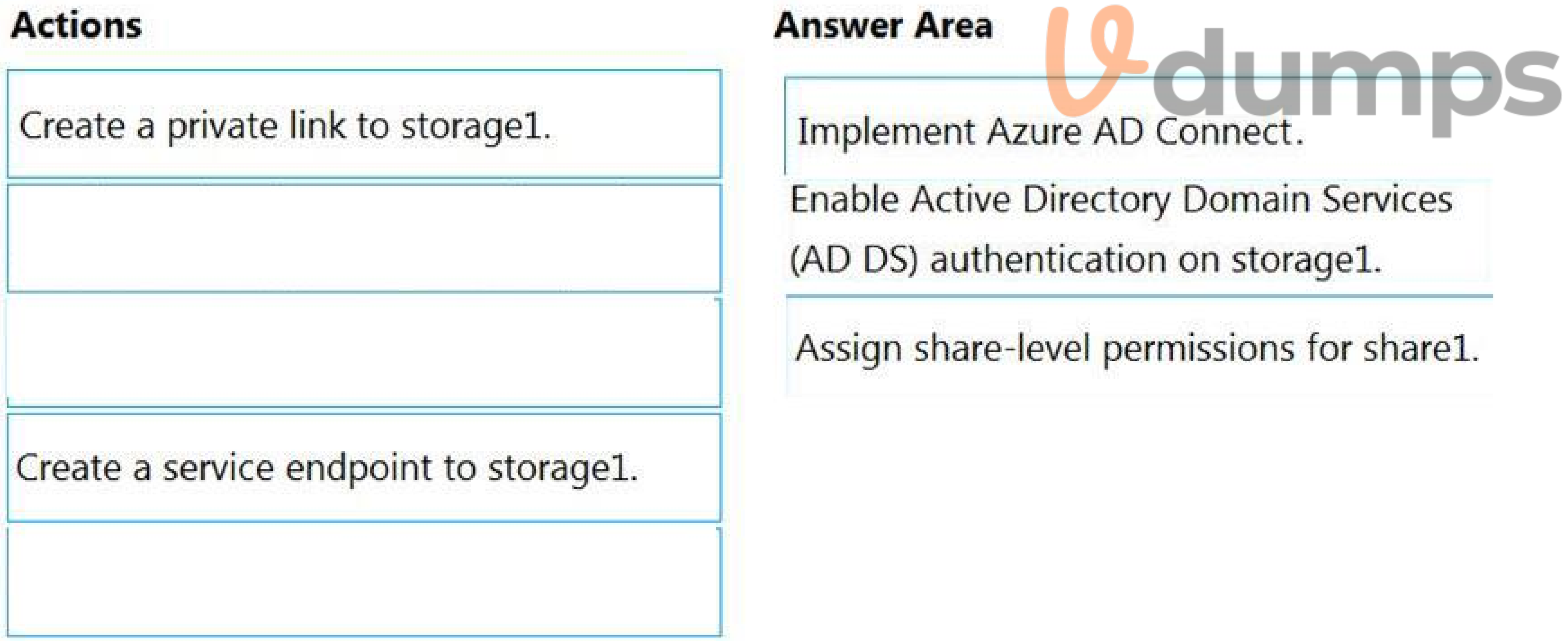
Implement Azure AD Connect.

Create a service endpoint to storage1.

Assign share-level permissions for share1.

**Answer Area**

**Correct Answer:**



**Actions**

Create a private link to storage1.

Create a service endpoint to storage1.

**Answer Area**

Implement Azure AD Connect.

Enable Active Directory Domain Services (AD DS) authentication on storage1.

Assign share-level permissions for share1.

**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-enable

**QUESTION 4**

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. an application permission without admin consent
B. a delegated permission without admin consent
C. a delegated permission that requires admin consent
D. an application permission that requires admin consent

**Correct Answer: B**
**Section:**
**Explanation:**
Delegated permissions - Your client application needs to access the web API as the signed-in user, but with access limited by the selected permission. This type of permission can be granted by a user unless the permission requires administrator consent.
Incorrect Answers:
A, D: Application permissions - Your client application needs to access the web API directly as itself (no user context). This type of permission requires administrator consent and is also not available for public (desktop and mobile) client applications.
References: https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis

**QUESTION 5**
Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory Azure (Azure AD) tenant named contoso.com. The company develops a mobile application named App1. App1 uses the OAuth 2 implicit grant type to acquire Azure AD access tokens. You need to register App1 in Azure AD.
What information should you obtain from the developer to register the application?

A. a redirect URI
B. a reply URL
C. a key
D. an application ID

**Correct Answer: A**
**Section:**
**Explanation:**
For Native Applications you need to provide a Redirect URI, which Azure AD will use to return token responses. References: https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code

**QUESTION 6**
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

**Correct Answer: C**
**Section:**
**Explanation:**
When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity. References: https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources

**QUESTION 7**
You have an Azure subscription that contains an Azure key vault named Vault1.
In Vault1, you create a secret named Secret1.

An application developer registers an application in Azure Active Directory (Azure AD).
You need to ensure that the application can use Secret1.
What should you do?

A. In Azure AD, create a role.
B. In Azure Key Vault, create a key.
C. In Azure Key Vault, create an access policy.
D. In Azure AD, enable Azure AD Application Proxy.

**Correct Answer: A**
**Section:**
**Explanation:**
Azure Key Vault provides a way to securely store credentials and other keys and secrets, but your code needs to authenticate to Key Vault to retrieve them. Managed identities for Azure resources overview makes solving this problem simpler, by giving Azure services an automatically managed identity in Azure Active Directory (Azure AD). You can use this identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without having any credentials in your code. Example: How a system-assigned managed identity works with an Azure VM
After the VM has an identity, use the service principal information to grant the VM access to Azure resources. To call Azure Resource Manager, use role-based access control (RBAC) in Azure AD to assign the appropriate role to the VM service principal. To call Key Vault, grant your code access to the specific secret or key in Key Vault. References: https://docs.microsoft.com/en-us/azure/key-vault/quick-create-net https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

**QUESTION 8**
You have an Azure SQL database.
You implement Always Encrypted.
You need to ensure that application developers can retrieve and decrypt data in the database.
Which two pieces of information should you provide to the developers? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. a stored access policy
B. a shared access signature (SAS)
C. the column encryption key
D. user credentials
E. the column master key

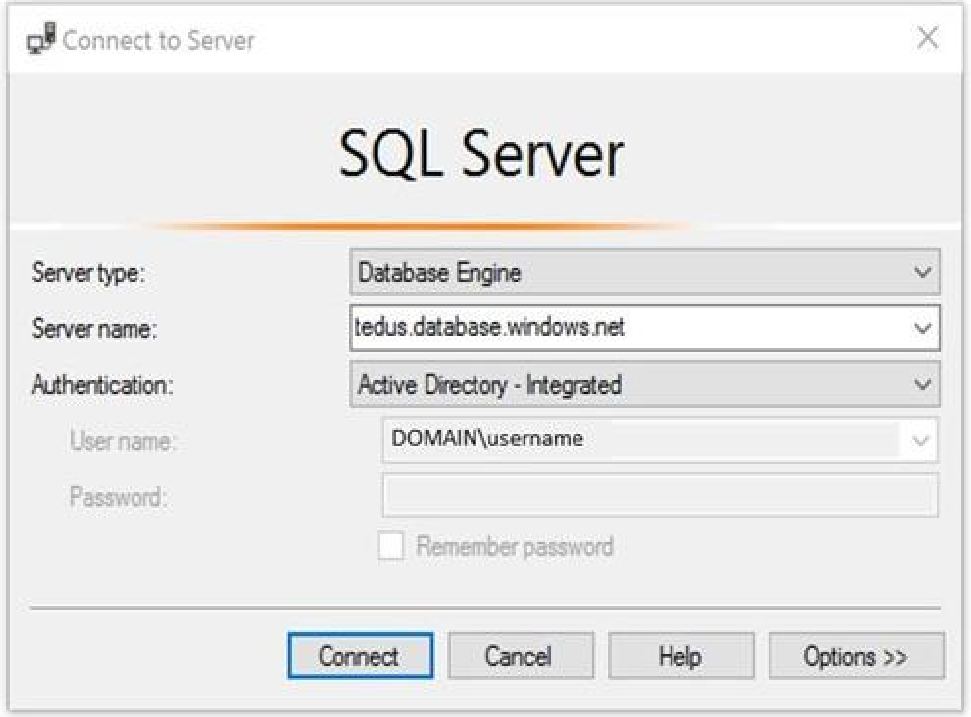
**Correct Answer: C, E**
**Section:**
**Explanation:**
Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.
References: https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine

**QUESTION 9**
You have a hybrid configuration of Azure Active Directory (Azure AD).
All users have computers that run Windows 10 and are hybrid Azure AD joined.
You have an Azure SQL database that is configured to support Azure AD authentication.
Database developers must connect to the SQL database by using Microsoft SQL Server Management Studio (SSMS) and authenticate by using their on-premises Active Directory account. You need to tell the developers which authentication method to use to connect to the SQL database from SSMS. The solution must minimize authentication prompts. Which authentication method should you instruct the developers to use?

A. SQL Login
B. Active Directory - Universal with MFA support
C. Active Directory - Integrated

D. Active Directory - Password

**Correct Answer: C**
**Section:**
**Explanation:**
Azure AD can be the initial Azure AD managed domain. Azure AD can also be an on-premises Active Directory Domain Services that is federated with the Azure AD.
Using an Azure AD identity to connect using SSMS or SSDT
The following procedures show you how to connect to a SQL database with an Azure AD identity using SQL Server Management Studio or SQL Server Database Tools.
Active Directory integrated authentication
Use this method if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.
1. Start Management Studio or Data Tools and in the Connect to Server (or Connect to Database Engine) dialog box, in the Authentication box, select Active Directory - Integrated. No password is needed or can be entered because your existing credentials will be presented for the connection.


Connect to Server

SQL Server

Server type: Database Engine
Server name: tedus.database.windows.net
Authentication: Active Directory - Integrated
User name: DOMAIN\username
Password:
□ Remember password

2. Select the Options button, and on the Connection Properties page, in the Connect to database box, type the name of the user database you want to connect to. (The AD domain name or tenant ID" option is only supported for Universal with MFA connection options, otherwise it is greyed out.)
References:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/sql-database/sql-database-aad-authentication-configure.md

**QUESTION 10**
You have an Azure SQL Database server named SQL1.
You plan to turn on Advanced Threat Protection for SQL1 to detect all threat detection types.
Which action will Advanced Threat Protection detect as a threat?

A. A user updates more than 50 percent of the records in a table.
B. A user attempts to sign as select * from table1.
C. A user is added to the db_owner database role.
D. A user deletes more than 100 records from the same table.

**Correct Answer: B**
**Section:**
**Explanation:**
Advanced Threat Protection can detect potential SQL injections: This alert is triggered when an active exploit happens against an identified application vulnerability to SQL injection. This means the attacker is trying to inject

malicious SQL statements using the vulnerable application code or stored procedures.
References: https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview

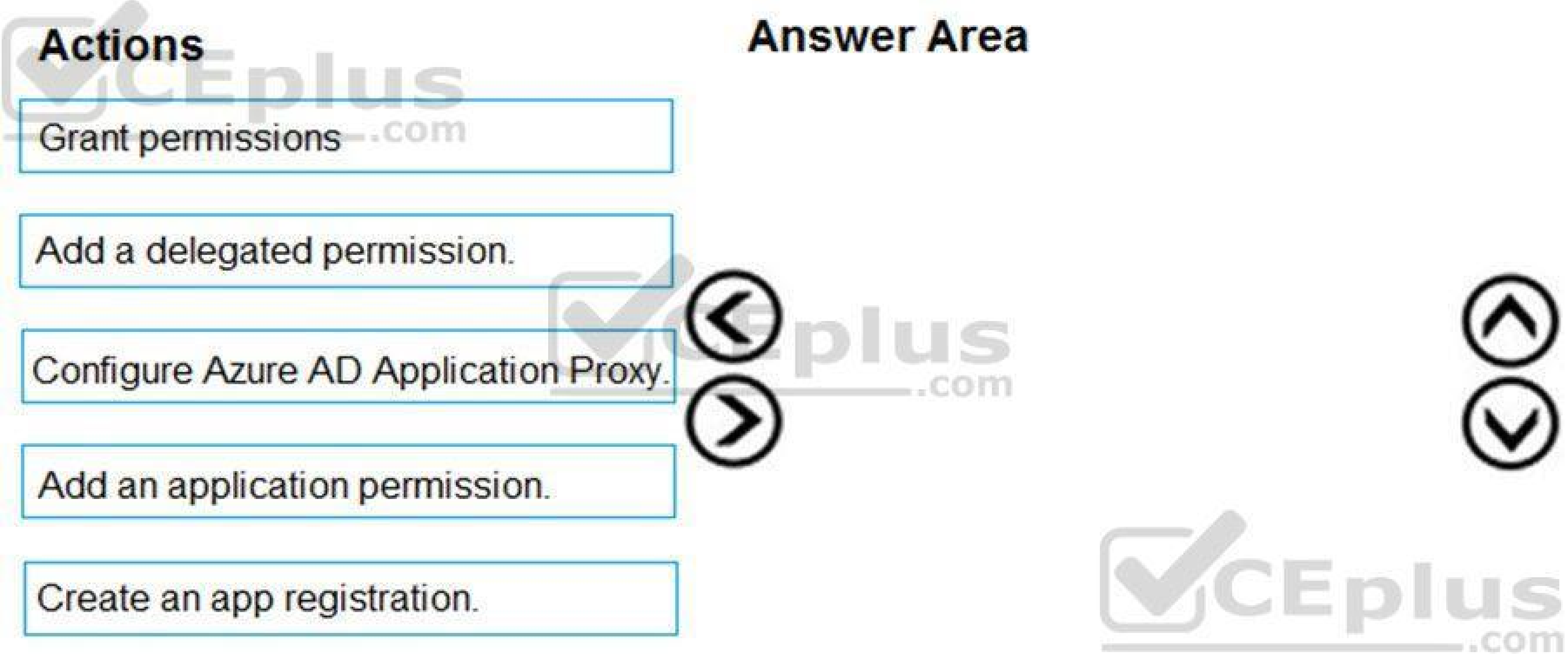
**QUESTION 11**
Your company uses Azure DevOps.
You need to recommend a method to validate whether the code meets the company's quality standards and code review standards. What should you recommend implementing in Azure DevOps?

A. branch folders
B. branch permissions
C. branch policies
D. branch locking

**Correct Answer: C**
**Section:**
**Explanation:**
Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards. References:
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&viewFallbackFrom=vsts

**QUESTION 12**
DRAG DROP
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.
The company is developing an application named App1. App1 will run as a service on server that runs Windows Server 2016. App1 will authenticate to contoso.com and access Microsoft Graph to read directory data.
You need to delegate the minimum required permissions to App1.
Which three actions should you perform in sequence from the Azure portal? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

**Select and Place:**



Actions

Grant permissions

Add a delegated permission.

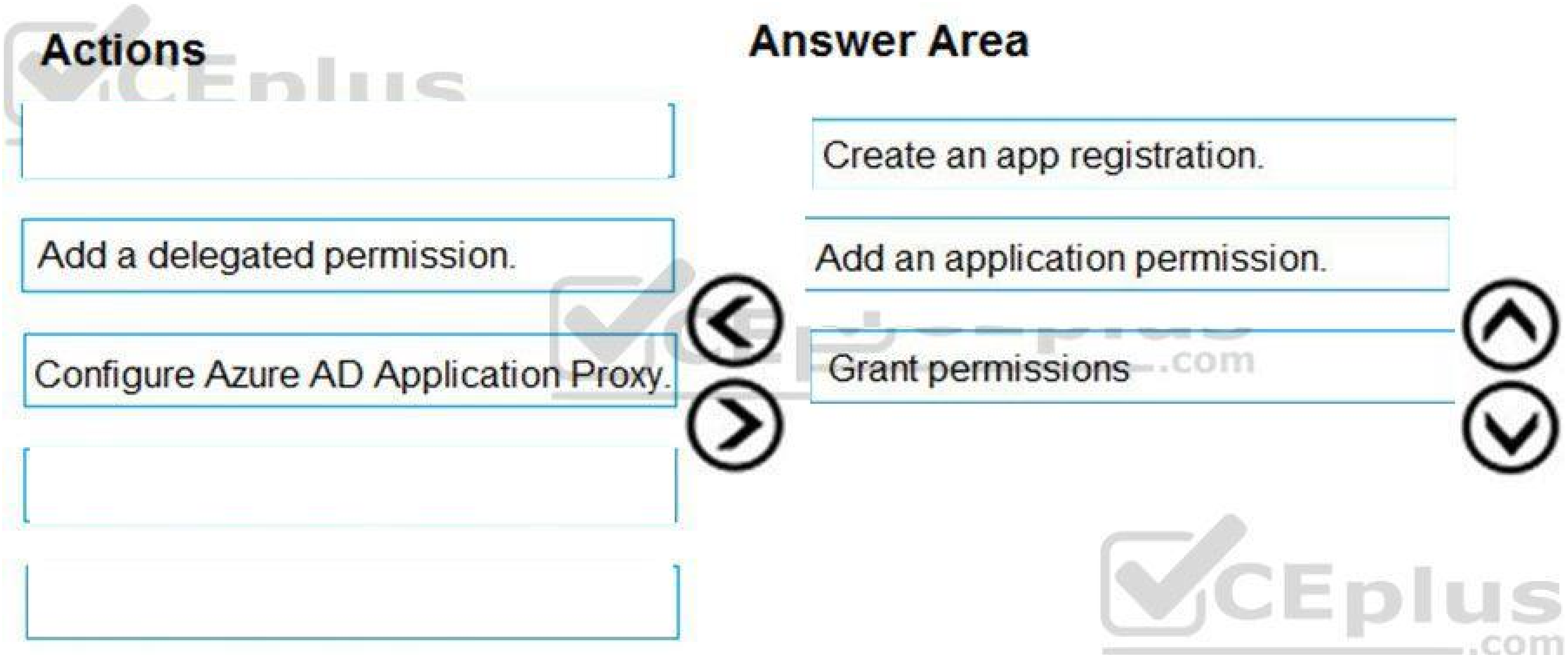
Configure Azure AD Application Proxy.

Add an application permission.

Create an app registration.

Answer Area

**Correct Answer:**



Actions

Add a delegated permission.

Configure Azure AD Application Proxy.

Answer Area

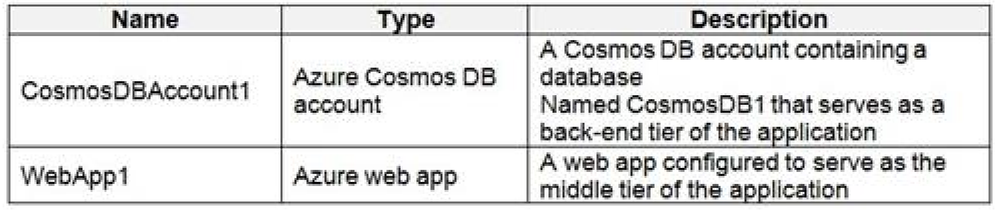
Create an app registration.

Add an application permission.

Grant permissions

**Section:**
**Explanation:**
Step 1: Create an app registration
First the application must be created/registered.
Step 2: Add an application permission
Application permissions are used by apps that run without a signed-in user present.
Step 3: Grant permissions
Incorrect Answers:
Delegated permission
Delegated permissions are used by apps that have a signed-in user present.
Application Proxy:
Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications.
References:
https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-permissions-and-consent

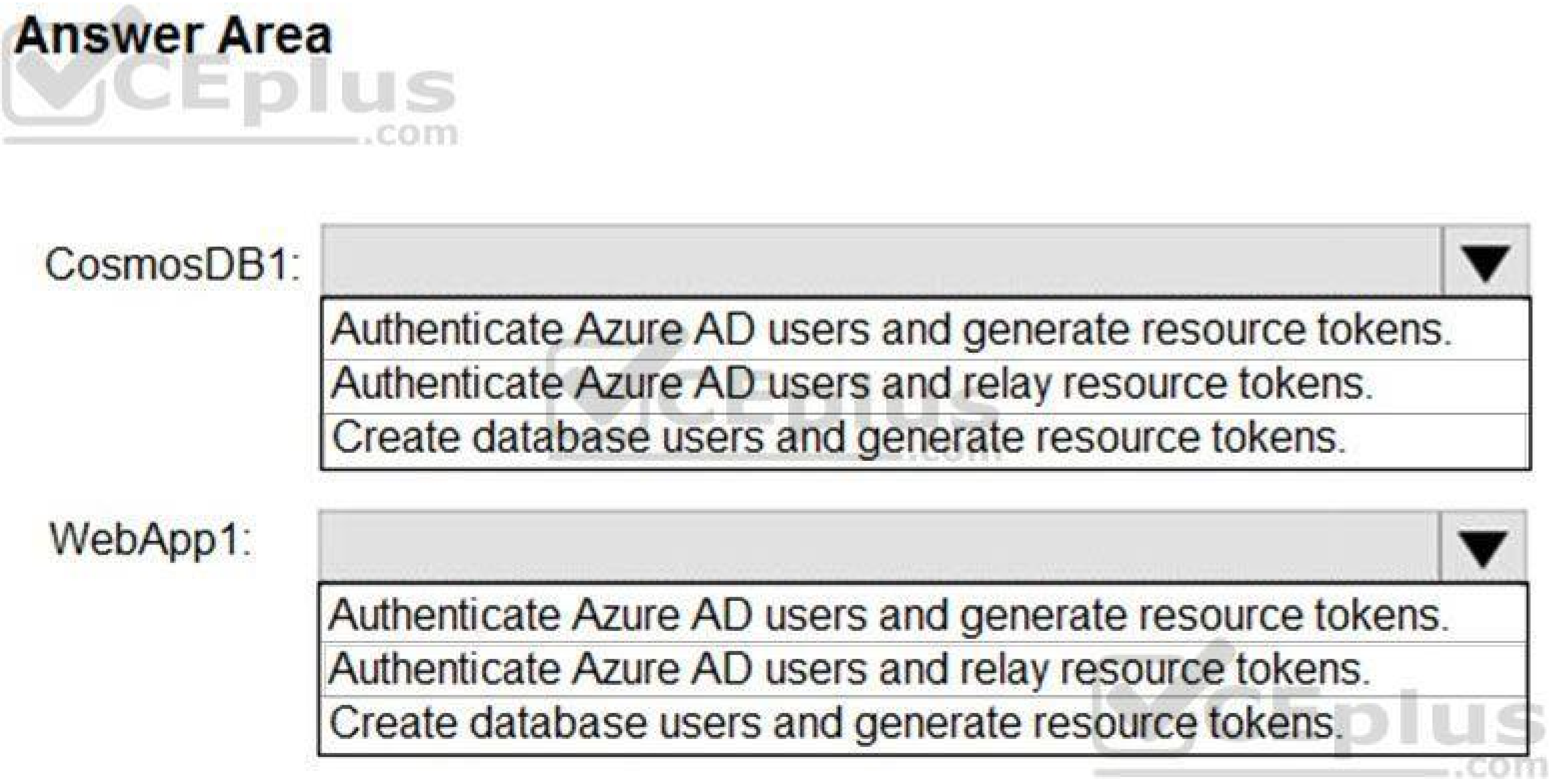
**QUESTION 13**
HOTSPOT
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
You plan to implement an application that will consist of the resources shown in the following table.



| Name | Type | Description |
|---|---|---|
| CosmosDBAccount1 | Azure Cosmos DB account | A Cosmos DB account containing a database<br>Named CosmosDB1 that serves as a back-end tier of the application |
| WebApp1 | Azure web app | A web app configured to serve as the middle tier of the application |

Users will authenticate by using their Azure AD user account and access the Cosmos DB account by using resource tokens.
You need to identify which tasks will be implemented in CosmosDB1 and WebApp1.
Which task should you identify for each resource? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**



Answer Area

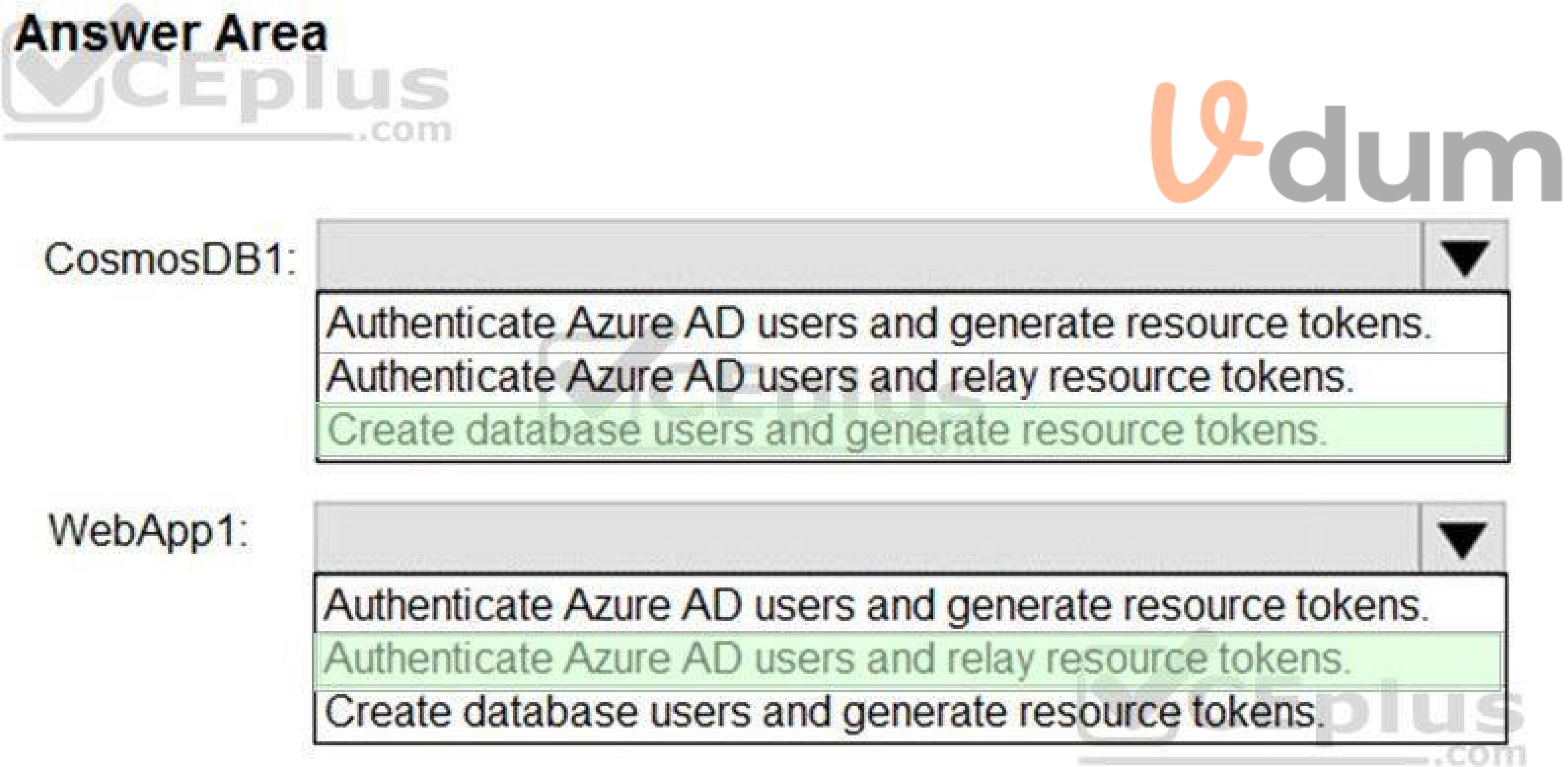
CosmosDB1:

- Authenticate Azure AD users and generate resource tokens.
- Authenticate Azure AD users and relay resource tokens.
- Create database users and generate resource tokens.

WebApp1:

- Authenticate Azure AD users and generate resource tokens.
- Authenticate Azure AD users and relay resource tokens.
- Create database users and generate resource tokens.

**Answer Area:**



Answer Area

CosmosDB1:

- Authenticate Azure AD users and generate resource tokens.
- Authenticate Azure AD users and relay resource tokens.
- [✓ Create database users and generate resource tokens.]

WebApp1:

- Authenticate Azure AD users and generate resource tokens.
- [✓ Authenticate Azure AD users and relay resource tokens.]
- Create database users and generate resource tokens.

**Section:**

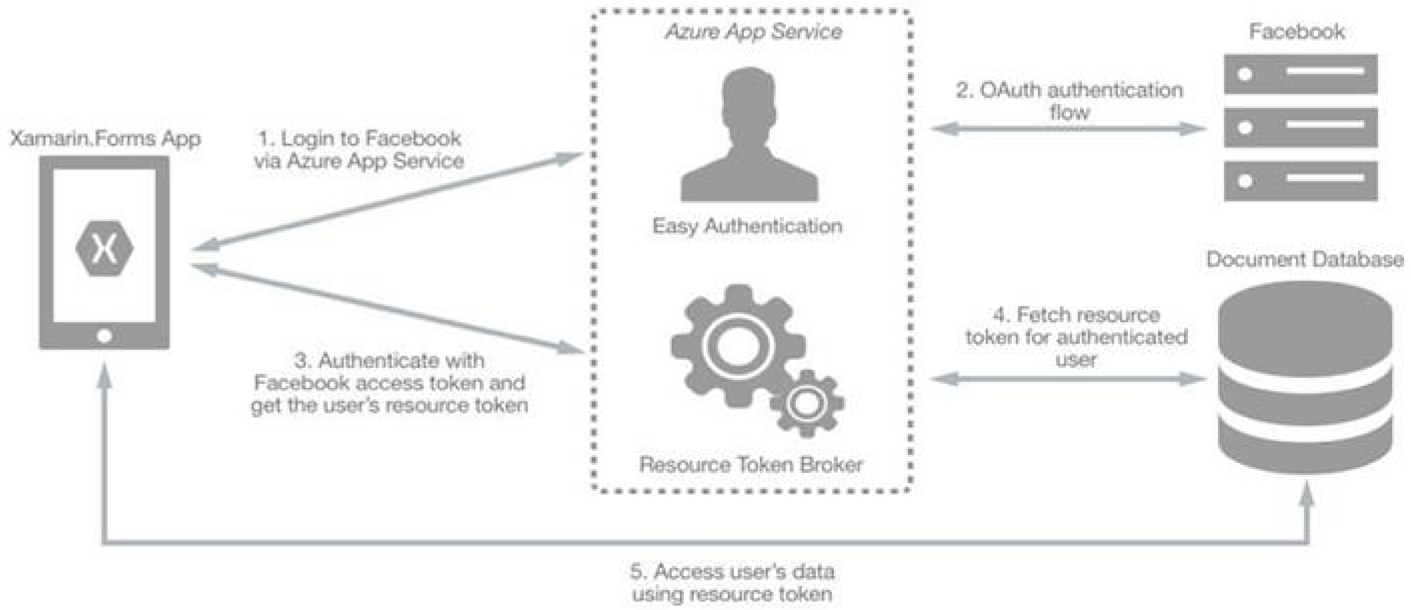
**Explanation:**

CosmosDB1: Create database users and generate resource tokens.

Azure Cosmos DB resource tokens provide a safe mechanism for allowing clients to read, write, and delete specific resources in an Azure Cosmos DB account according to the granted permissions.

WebApp1: Authenticate Azure AD users and relay resource tokens

A typical approach to requesting, generating, and delivering resource tokens to a mobile application is to use a resource token broker. The following diagram shows a high-level overview of how the sample application uses a resource token broker to manage access to the document database data:


Azure App Service
Xamarin.Forms App
1. Login to Facebook via Azure App Service
Easy Authentication
2. OAuth authentication flow
Facebook
Document Database
4. Fetch resource token for authenticated user
3. Authenticate with Facebook access token and get the user's resource token
Resource Token Broker
5. Access user's data using resource token

References:
https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication

**QUESTION 14**

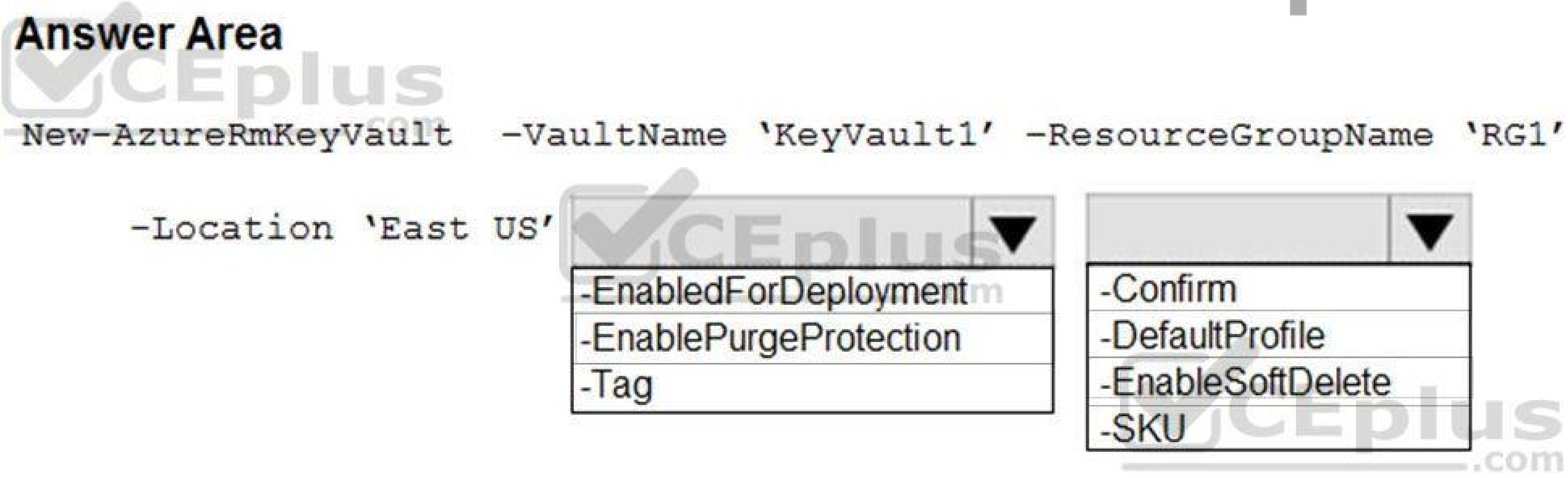
HOTSPOT

You need to create an Azure key vault. The solution must ensure that any object deleted from the key vault be retained for 90 days.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Hot Area:**



Answer Area

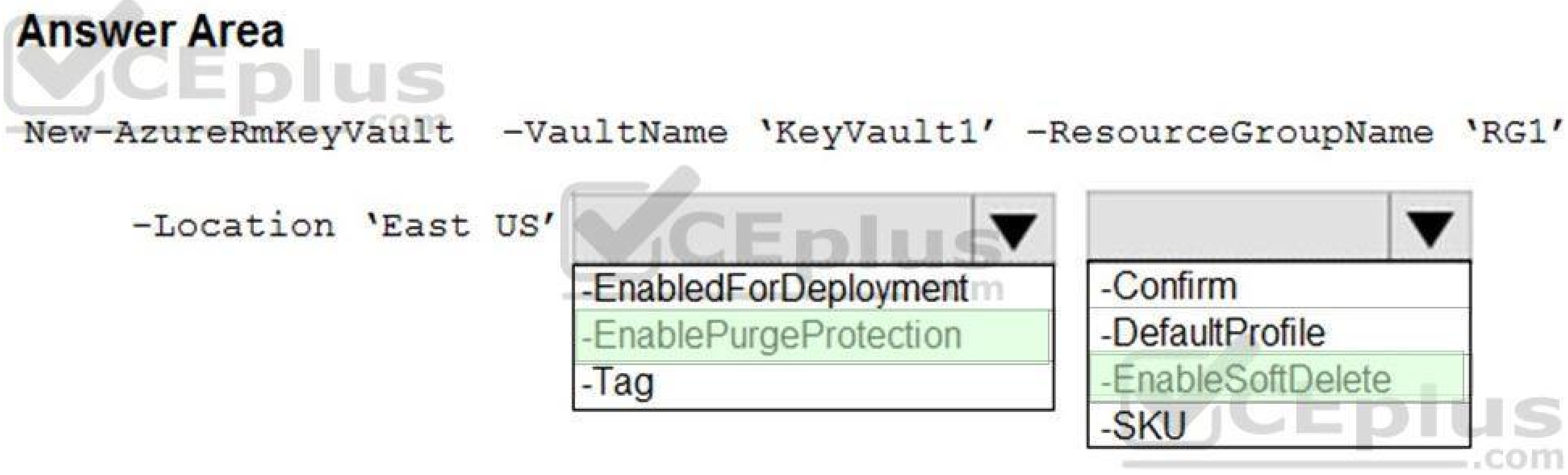
```
New-AzureRmKeyVault  -VaultName 'KeyVault1' -ResourceGroupName 'RG1'

    -Location 'East US'  [ ▼ ]  [ ▼ ]
```

- -EnabledForDeployment
- -EnablePurgeProtection
- -Tag

- -Confirm
- -DefaultProfile
- -EnableSoftDelete
- -SKU

**Answer Area:**



Answer Area

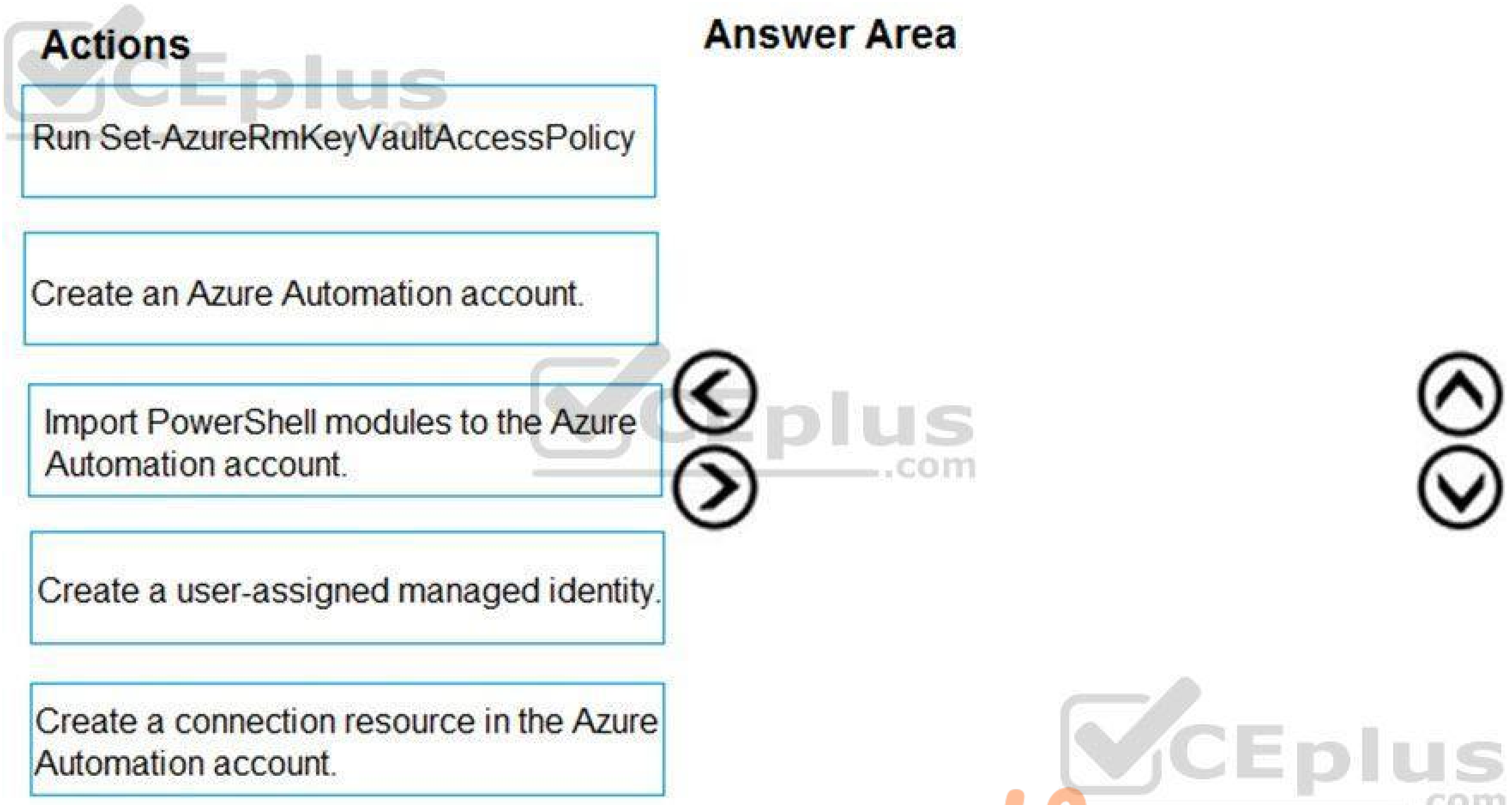
```
New-AzureRmKeyVault  -VaultName 'KeyVault1' -ResourceGroupName 'RG1'

     -Location 'East US'
```

**Section:**
**Explanation:**
Box 1: -EnablePurgeProtection
If specified, protection against immediate deletion is enabled for this vault; requires soft delete to be enabled as well.
Box 2: -EnableSoftDelete
Specifies that the soft-delete functionality is enabled for this key vault. When soft-delete is enabled, for a grace period, you can recover this key vault and its contents after it is deleted.
References:
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault

**QUESTION 15**
DRAG DROP
You have an Azure subscription named Sub1 that contains an Azure Storage account named Contosostorage1 and an Azure key vault named Contosokeyvault1.
You plan to create an Azure Automation runbook that will rotate the keys of Contosostorage1 and store them in Contosokeyvault1.
You need to implement prerequisites to ensure that you can implement the runbook.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

**Select and Place:**



Actions

Run Set-AzureRmKeyVaultAccessPolicy

Create an Azure Automation account.

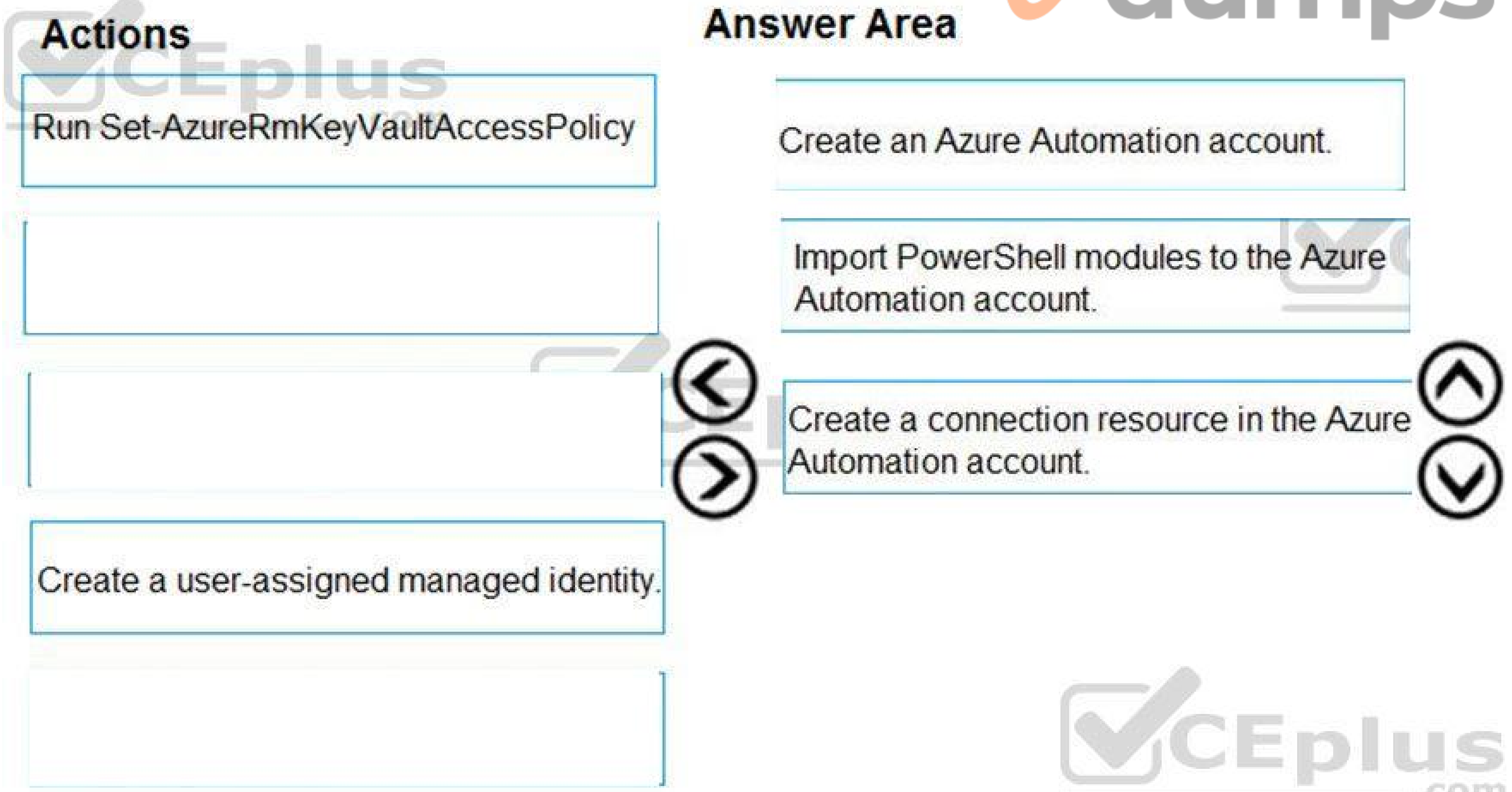
Import PowerShell modules to the Azure Automation account.

Create a user-assigned managed identity.

Create a connection resource in the Azure Automation account.

Answer Area

**Correct Answer:**



Actions

Run Set-AzureRmKeyVaultAccessPolicy

Create a user-assigned managed identity.

Answer Area

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

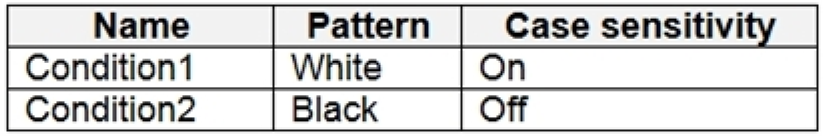
Create a connection resource in the Azure Automation account.

**Section:**
**Explanation:**
Step 1: Create an Azure Automation account
Runbooks live within the Azure Automation account and can execute PowerShell scripts.
Step 2: Import PowerShell modules to the Azure Automation account
Under ‘Assets’ from the Azure Automation account Resources section select ‘to add in Modules to the runbook. To execute key vault cmdlets in the runbook, we need to add AzureRM.profile and AzureRM.key vault.
Step 3: Create a connection resource in the Azure Automation account
You can use the sample code below, taken from the AzureAutomationTutorialScript example runbook, to authenticate using the Run As account to manage Resource Manager resources with your runbooks. The AzureRunAsConnection is a connection asset automatically created when we created ‘run as accounts’ above. This can be found under Assets -> Connections. After the authentication code, run the same code above to get all the keys from the vault.

```
$connectionName = "AzureRunAsConnection"
try
{
# Get the connection "AzureRunAsConnection "
$servicePrincipalConnection=Get-AutomationConnection -Name $connectionName
"Logging in to Azure..."
Add-AzureRmAccount `
-ServicePrincipal `
-TenantId $servicePrincipalConnection.TenantId `
-ApplicationId $servicePrincipalConnection.ApplicationId `
-CertificateThumbprint $servicePrincipalConnection.CertificateThumbprint
}
```

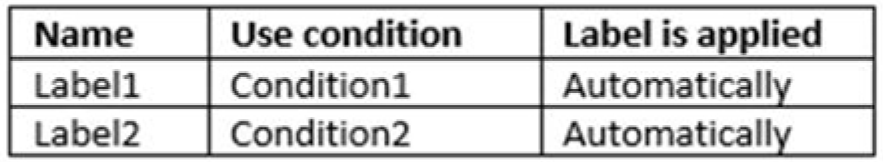
References:
https://www.rahulpnath.com/blog/accessing-azure-key-vault-from-azure-runbook/

**QUESTION 16**
HOTSPOT
You have the Azure Information Protection conditions shown in the following table.



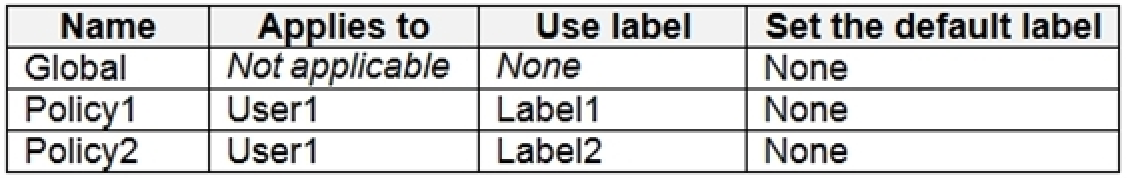
| Name | Pattern | Case sensitivity |
|---|---|---|
| Condition1 | White | On |
| Condition2 | Black | Off |

You have the Azure Information Protection labels shown in the following table.



| Name | Use condition | Label is applied |
|---|---|---|
| Label1 | Condition1 | Automatically |
| Label2 | Condition2 | Automatically |

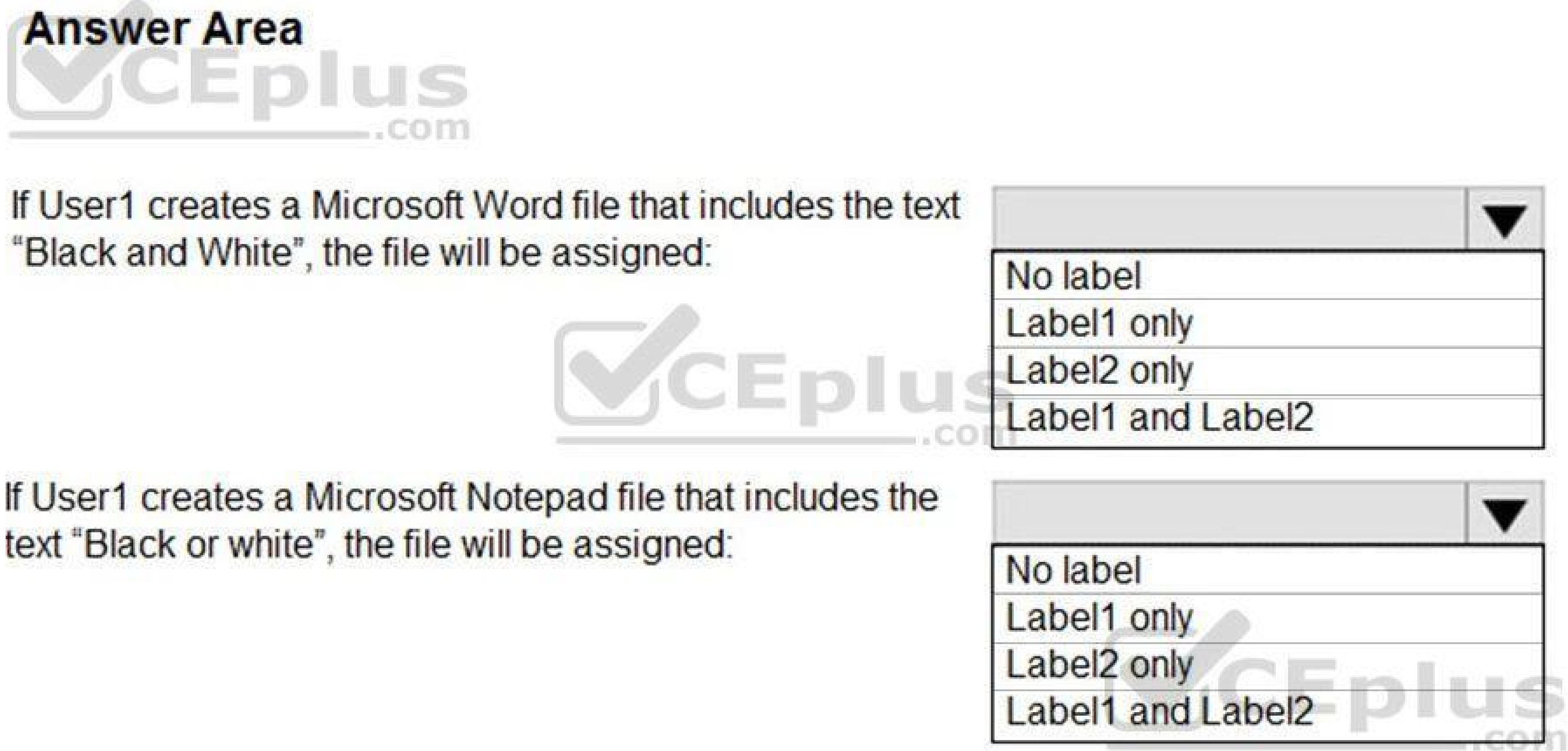
You have the Azure Information Protection policies shown in the following table.



| Name | Applies to | Use label | Set the default label |
|---|---|---|---|
| Global | *Not applicable* | *None* | None |
| Policy1 | User1 | Label1 | None |
| Policy2 | User1 | Label2 | None |

You need to identify how Azure Information Protection will label files.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**



Answer Area

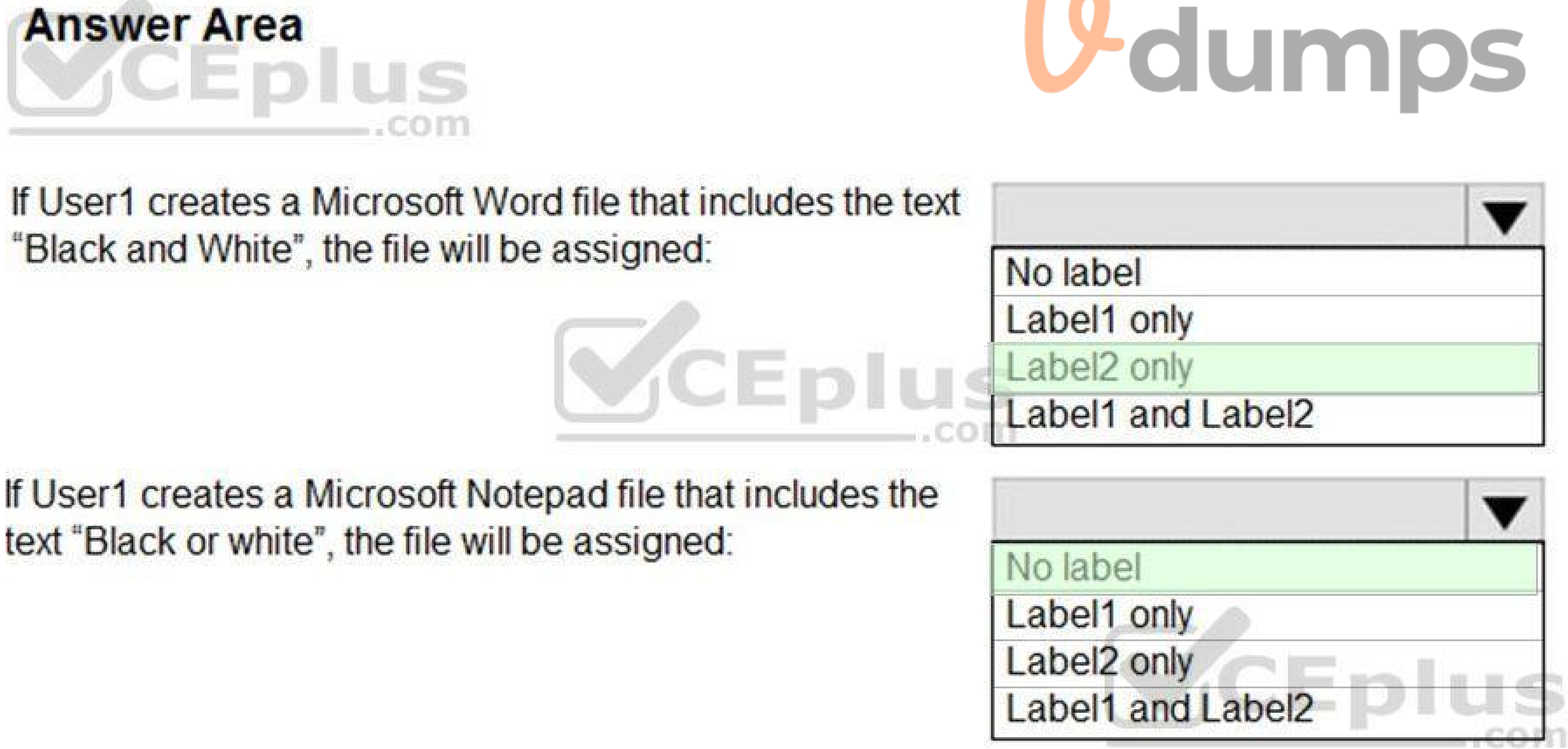
If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

- No label
- Label1 only
- Label2 only
- Label1 and Label2

If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:

- No label
- Label1 only
- Label2 only
- Label1 and Label2

**Answer Area:**



Answer Area

If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

- No label
- Label1 only
- [✓ Label2 only]
- Label1 and Label2

If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:

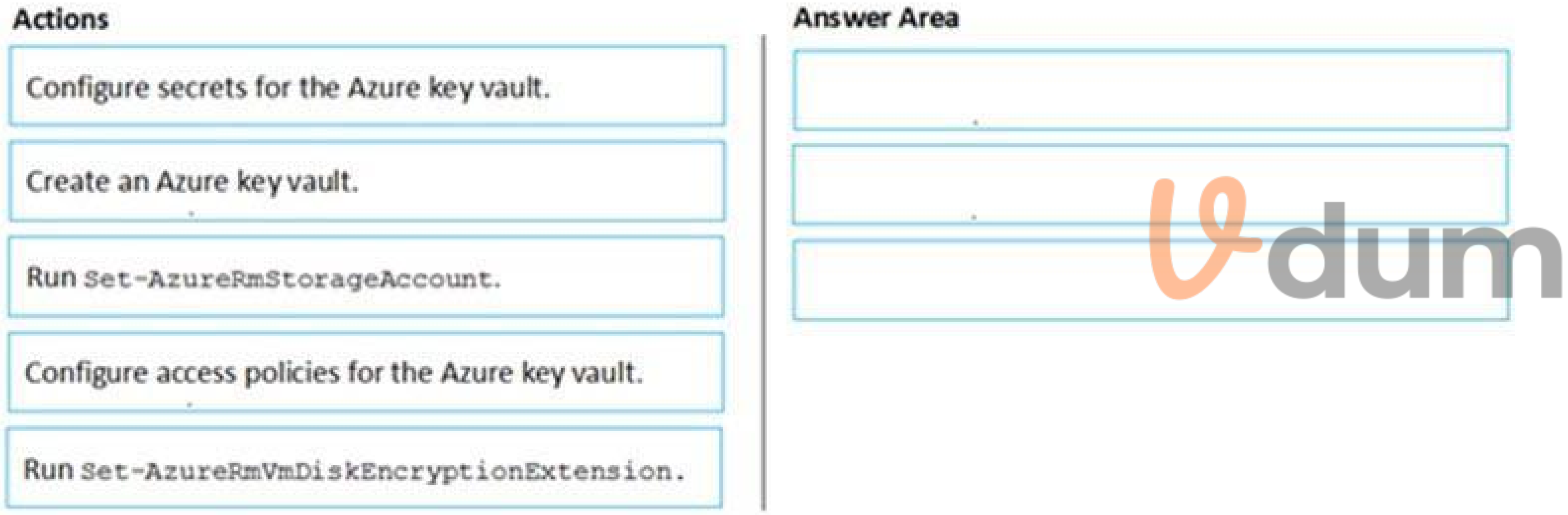
- [✓ No label]
- Label1 only
- Label2 only
- Label1 and Label2

**Section:**
**Explanation:**
Box 1: Label 2 only
How multiple conditions are evaluated when they apply to more than one label

1. The labels are ordered for evaluation, according to their position that you specify in the policy: The label positioned first has the lowest position (least sensitive) and the label positioned last has the highest position (most sensitive).
2. The most sensitive label is applied.
3. The last sublabel is applied.
Box 2: No Label
Automatic classification applies to Word, Excel, and PowerPoint when documents are saved, and apply to Outlook when emails are sent. Automatic classification does not apply to Microsoft Notepad. References: https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

**QUESTION 17**
DRAG DROP
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Subscription named Sub1. Sub1 contains an Azure virtual machine named VM1 that runs Windows Server 2016.
You need to encrypt VM1 disks by using Azure Disk Encryption.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

**Select and Place:**



Actions

Configure secrets for the Azure key vault.

Create an Azure key vault.

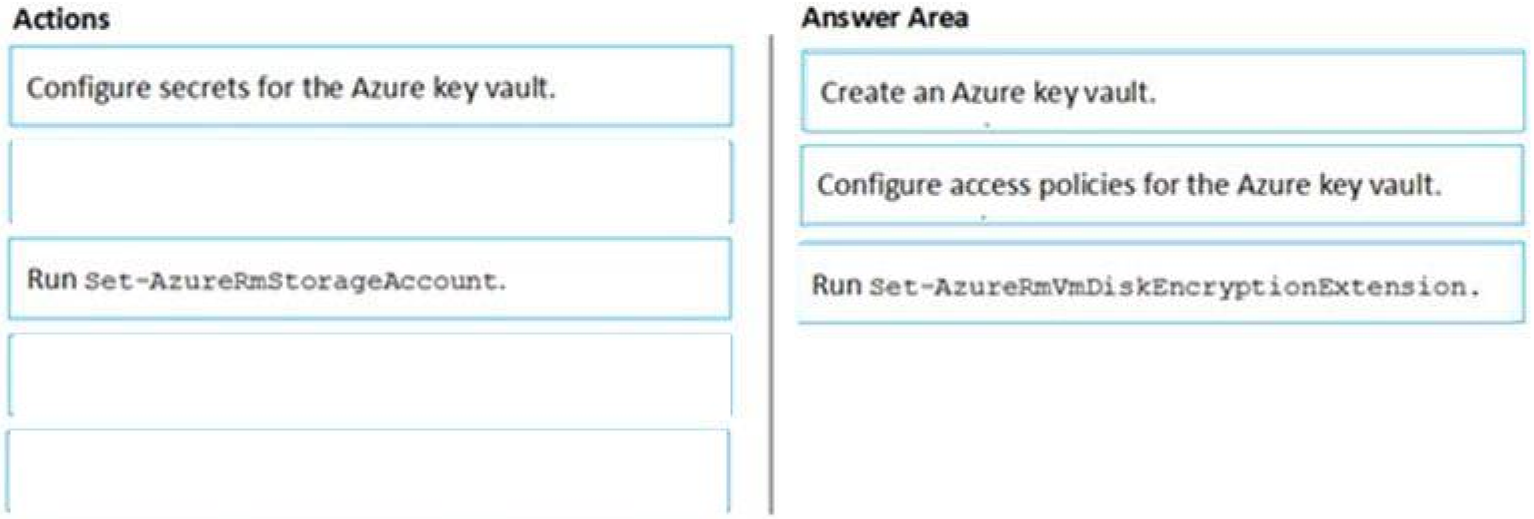
Run `Set-AzureRmStorageAccount.`

Configure access policies for the Azure key vault.

Run `Set-AzureRmVmDiskEncryptionExtension.`

Answer Area

**Correct Answer:**



Actions

Configure secrets for the Azure key vault.

Run `Set-AzureRmStorageAccount.`

Answer Area

Create an Azure key vault.

Configure access policies for the Azure key vault.

Run `Set-AzureRmVmDiskEncryptionExtension.`

**Section:**
**Explanation:**

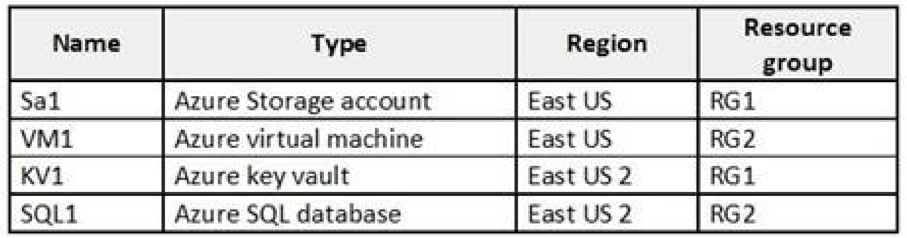
References:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/encrypt-disks

**QUESTION 18**
You have an Azure subscription that contains a virtual machine named VM1.
You create an Azure key vault that has the following configurations:
Name: Vault5
Region: West US
Resource group: RG1
You need to use Vault5 to enable Azure Disk Encryption on VM1. The solution must support backing up VM1 by using Azure Backup.
Which key vault settings should you configure?

A. Access policies
B. Secrets
C. Keys
D. Locks

**Correct Answer: A**
**Section:**
**Explanation:**
References:
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

**QUESTION 19**
You have an Azure subscription named Sub1 that contains the resources shown in the following table.



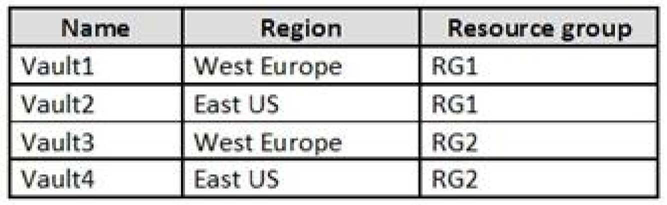
| Name | Type | Region | Resource group |
|---|---|---|---|
| Sa1 | Azure Storage account | East US | RG1 |
| VM1 | Azure virtual machine | East US | RG2 |
| KV1 | Azure key vault | East US 2 | RG1 |
| SQL1 | Azure SQL database | East US 2 | RG2 |

You need to ensure that you can provide VM1 with secure access to a database on SQL1 by using a contained database user.
What should you do?

A. Enable a managed service identity on VM1.
B. Create a secret in KV1.
C. Configure a service endpoint on SQL1.
D. Create a key in KV1.

**Correct Answer: B**
**Section:**
**Explanation:**
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure- resources/tutorial-windows-vm-access-sql

**QUESTION 20**
You have an Azure subscription named Sub1 that contains the Azure key vaults shown in the following table:



| Name | Region | Resource group |
|---|---|---|
| Vault1 | West Europe | RG1 |
| Vault2 | East US | RG1 |
| Vault3 | West Europe | RG2 |
| Vault4 | East US | RG2 |

In Sub1, you create a virtual machine that has the following configurations:
Name: VM1
Size: DS2v2
Resource group: RG1
Region: West Europe
Operating system: Windows Server 2016
You plan to enable Azure Disk Encryption on VM1.
In which key vaults can you store the encryption key for VM1?

A. Vault1 or Vault3 only

B. Vault1, Vault2, Vault3, or Vault4

C. Vault1 only

D. Vault1 or Vault2 only

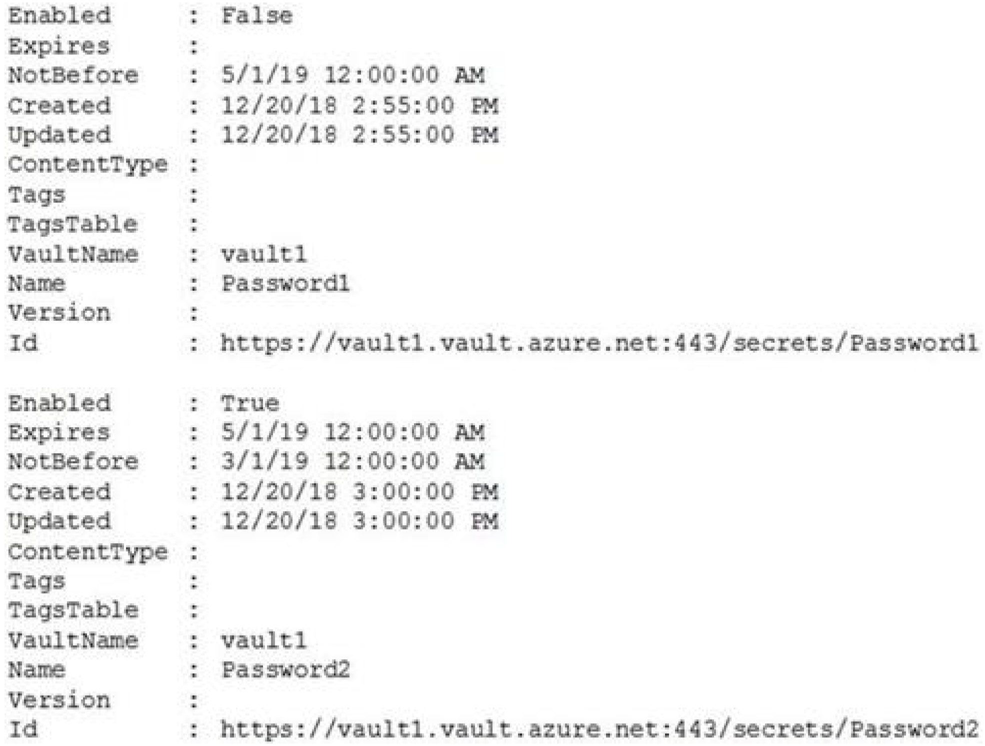
**Correct Answer: C**
**Section:**
**Explanation:**

**QUESTION 21**

HOTSPOT

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

On January 1, 2019, Vault1 stores the following secrets.

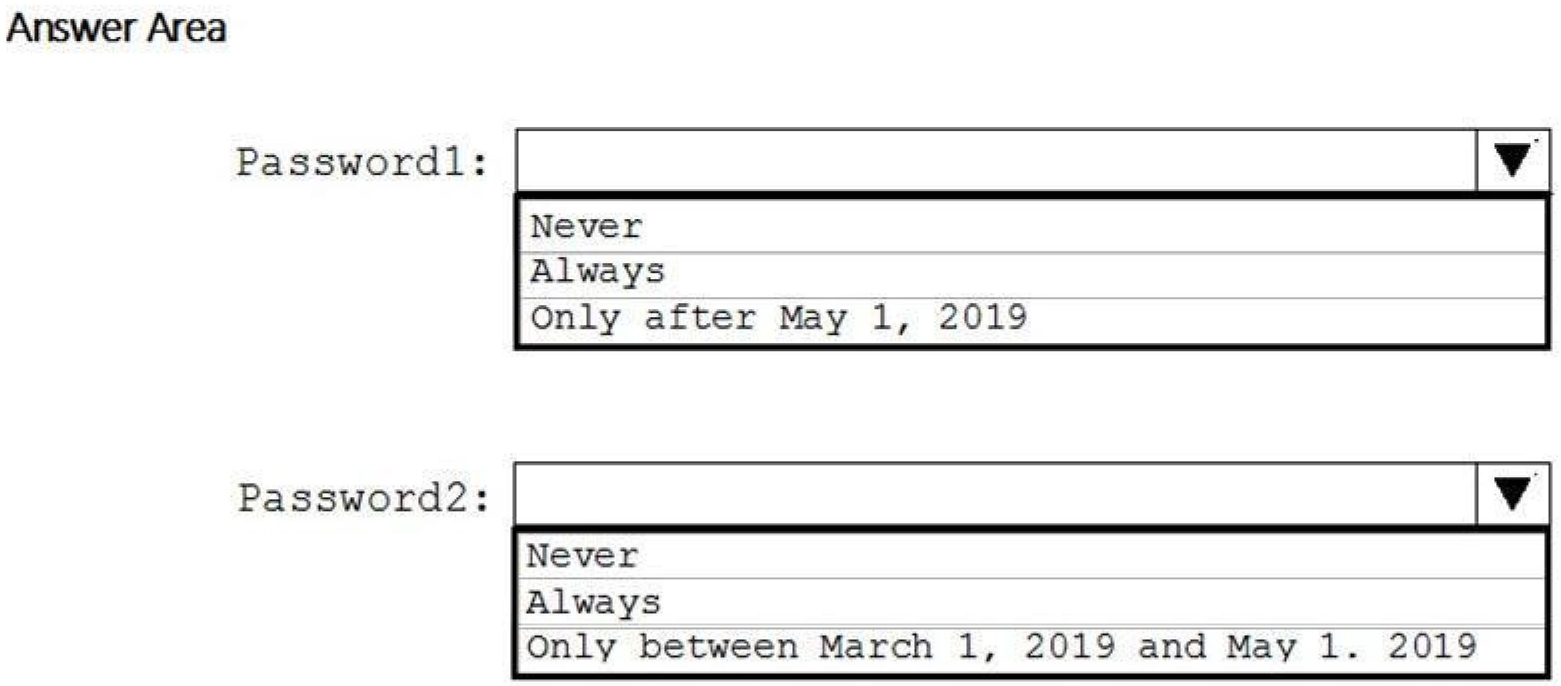


```
Enabled     : False
Expires     :
NotBefore   : 5/1/19 12:00:00 AM
Created     : 12/20/18 2:55:00 PM
Updated     : 12/20/18 2:55:00 PM
ContentType :
Tags        :
TagsTable   :
VaultName   : vault1
Name        : Password1
Version     :
Id          : https://vault1.vault.azure.net:443/secrets/Password1

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.

**Hot Area:**



Answer Area

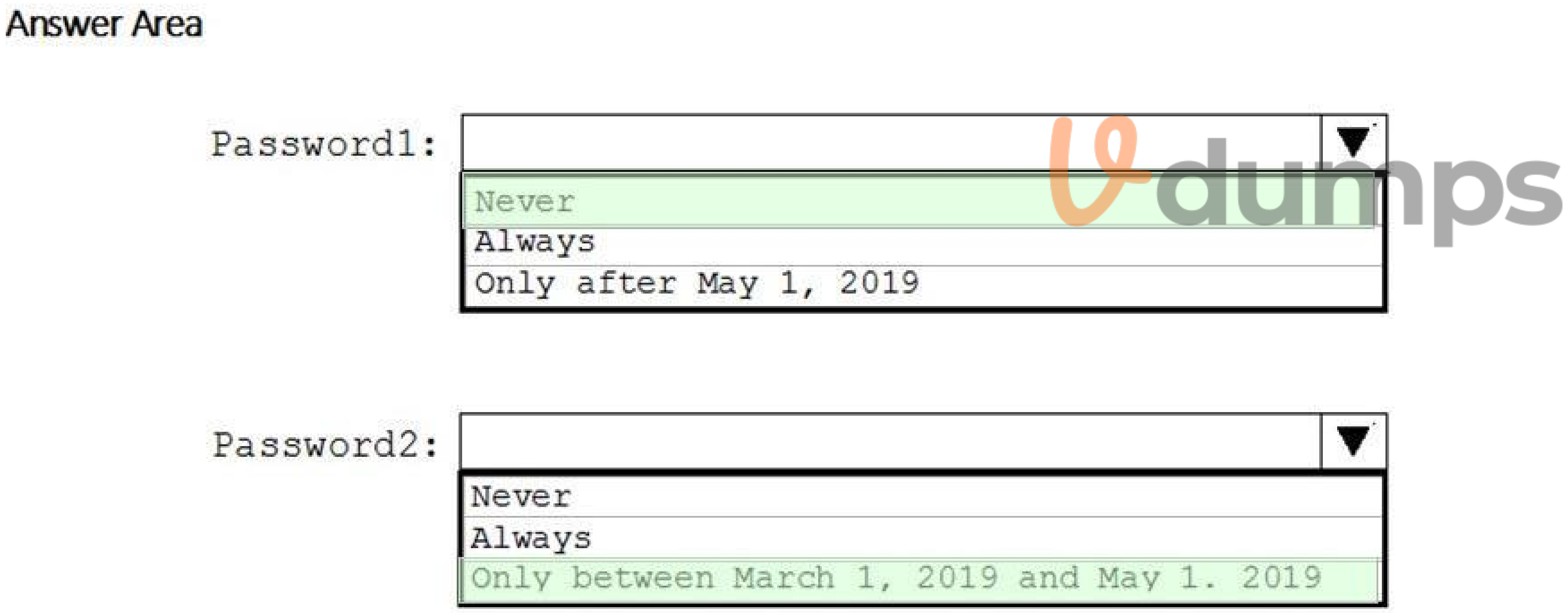
Password1:

Never
Always
Only after May 1, 2019

Password2:

Never
Always
Only between March 1, 2019 and May 1. 2019

**Answer Area:**



Answer Area

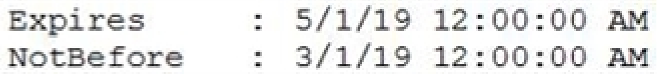
Password1:

[✓ Never]
Always
Only after May 1, 2019

Password2:

Never
Always
[✓ Only between March 1, 2019 and May 1. 2019]

**Section:**
**Explanation:**
Box 1: Never
Password1 is disabled.
Box 2: Only between March 1, 2019 and May 1,
Password2:



```
Expires      : 5/1/19 12:00:00 AM
NotBefore    : 3/1/19 12:00:00 AM
```

Reference:
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurekeyvaultsecretattribute

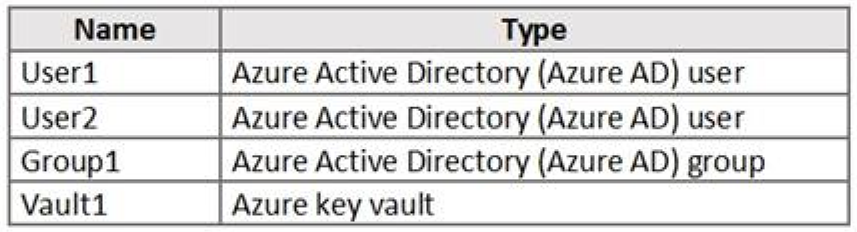
**QUESTION 22**

You have an Azure web app named webapp1.
You need to configure continuous deployment for webapp1 by using an Azure Repo.
What should you create first?

A. an Azure Application Insights service
B. an Azure DevOps organizations
C. an Azure Storage account
D. an Azure DevTest Labs lab

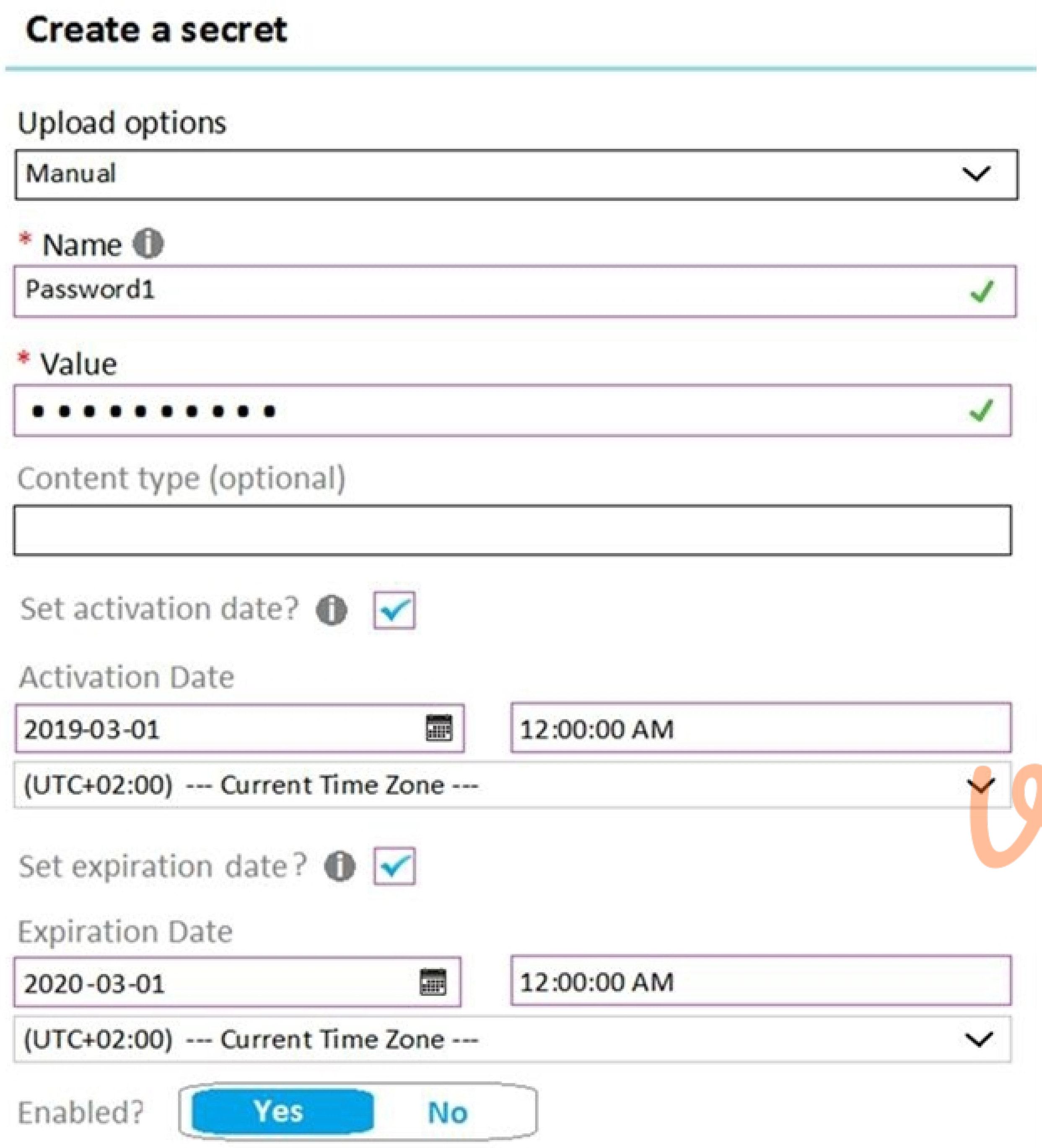
**Correct Answer: B**
**Section:**
**Explanation:**
To use Azure Repos, make sure your Azure DevOps organization is linked to your Azure subscription.
Reference:
https://docs.microsoft.com/en-us/azure/app-service/deploy-continuous-deployment

**QUESTION 23**
HOTSPOT
You have an Azure subscription that contains the resources shown in the following table.



| Name | Type |
|---|---|
| User1 | Azure Active Directory (Azure AD) user |
| User2 | Azure Active Directory (Azure AD) user |
| Group1 | Azure Active Directory (Azure AD) group |
| Vault1 | Azure key vault |

User1 is a member of Group1. Group1 and User2 are assigned the Key Vault Contributor role for Vault1.
On January 1, 2019, you create a secret in Vault1. The secret is configured as shown in the exhibit. (Click the Exhibit tab.)



Create a secret

Upload options
Manual

* Name
Password1 ✓

* Value
●●●●●●●●●● ✓

Content type (optional)

Set activation date? ☑

Activation Date
2019-03-01 | 12:00:00 AM
(UTC+02:00) --- Current Time Zone ---

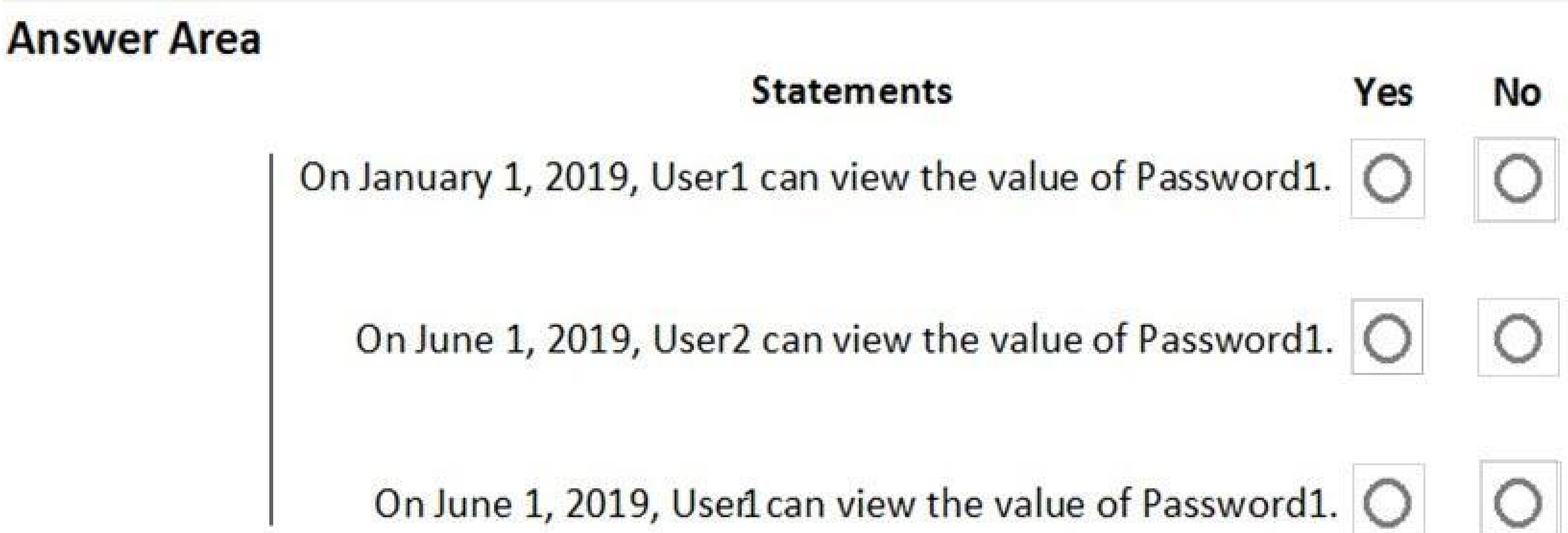
Set expiration date? ☑

Expiration Date
2020-03-01 | 12:00:00 AM
(UTC+02:00) --- Current Time Zone ---

Enabled? [✓ Yes] No

User2 is assigned an access policy to Vault1. The policy has the following configurations:
Key Management Operations: Get, List, and Restore
Cryptographic Operations: Decrypt and Unwrap Key
Secret Management Operations: Get, List, and Restore
Group1 is assigned an access policy to Vault1. The policy has the following configurations:
Key Management Operations: Get and Recover
Secret Management Operations: List, Backup, and Recover
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

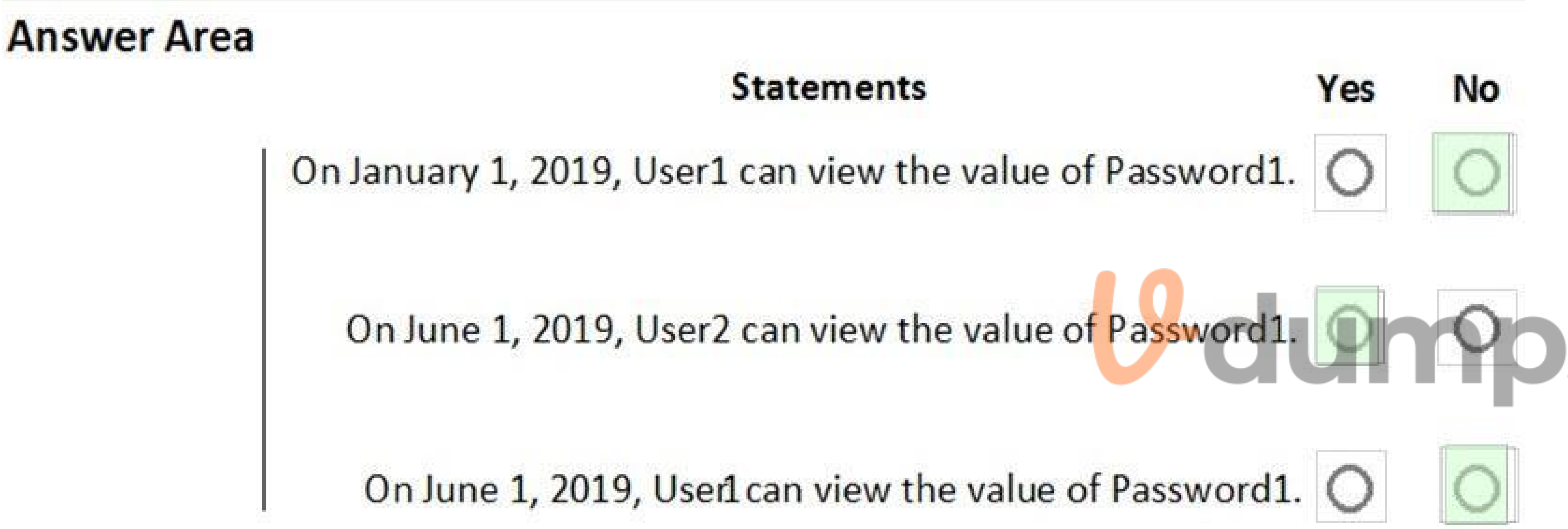
**Hot Area:**



## Answer Area

| Statements | Yes | No |
|---|---|---|
| On January 1, 2019, User1 can view the value of Password1. | ○ | ○ |
| On June 1, 2019, User2 can view the value of Password1. | ○ | ○ |
| On June 1, 2019, User1 can view the value of Password1. | ○ | ○ |

**Answer Area:**

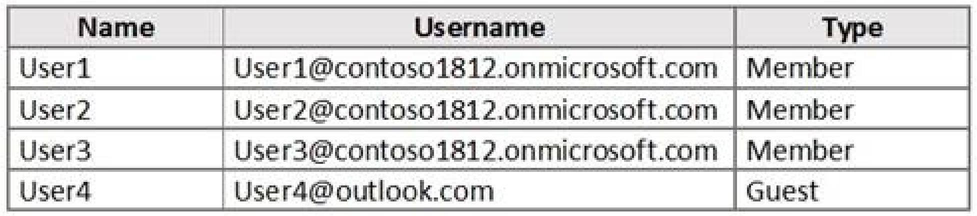


## Answer Area

| Statements | Yes | No |
|---|---|---|
| On January 1, 2019, User1 can view the value of Password1. | ○ | [✓ ○] |
| On June 1, 2019, User2 can view the value of Password1. | [✓ ○] | ○ |
| On June 1, 2019, User1 can view the value of Password1. | ○ | [✓ ○] |

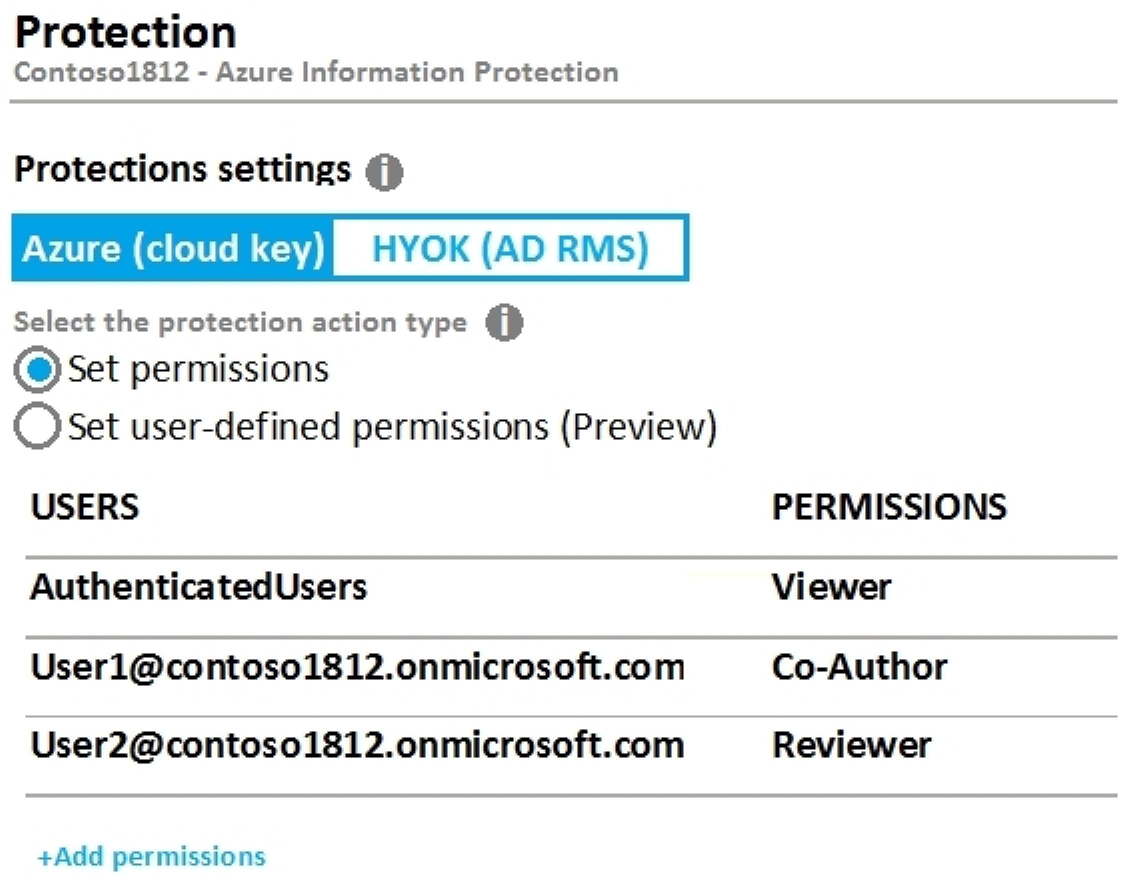
**Section:**
**Explanation:**

**QUESTION 24**
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant named contoso1812.onmicrosoft.com that contains the users shown in the following table.



| Name | Username | Type |
|---|---|---|
| User1 | User1@contoso1812.onmicrosoft.com | Member |
| User2 | User2@contoso1812.onmicrosoft.com | Member |
| User3 | User3@contoso1812.onmicrosoft.com | Member |
| User4 | User4@outlook.com | Guest |

You create an Azure Information Protection label named Label1. The Protection settings for Label1 are configured as shown in the exhibit. (Click the Exhibit tab.)



Protection

Contoso1812 - Azure Information Protection

Protections settings

Select the protection action type

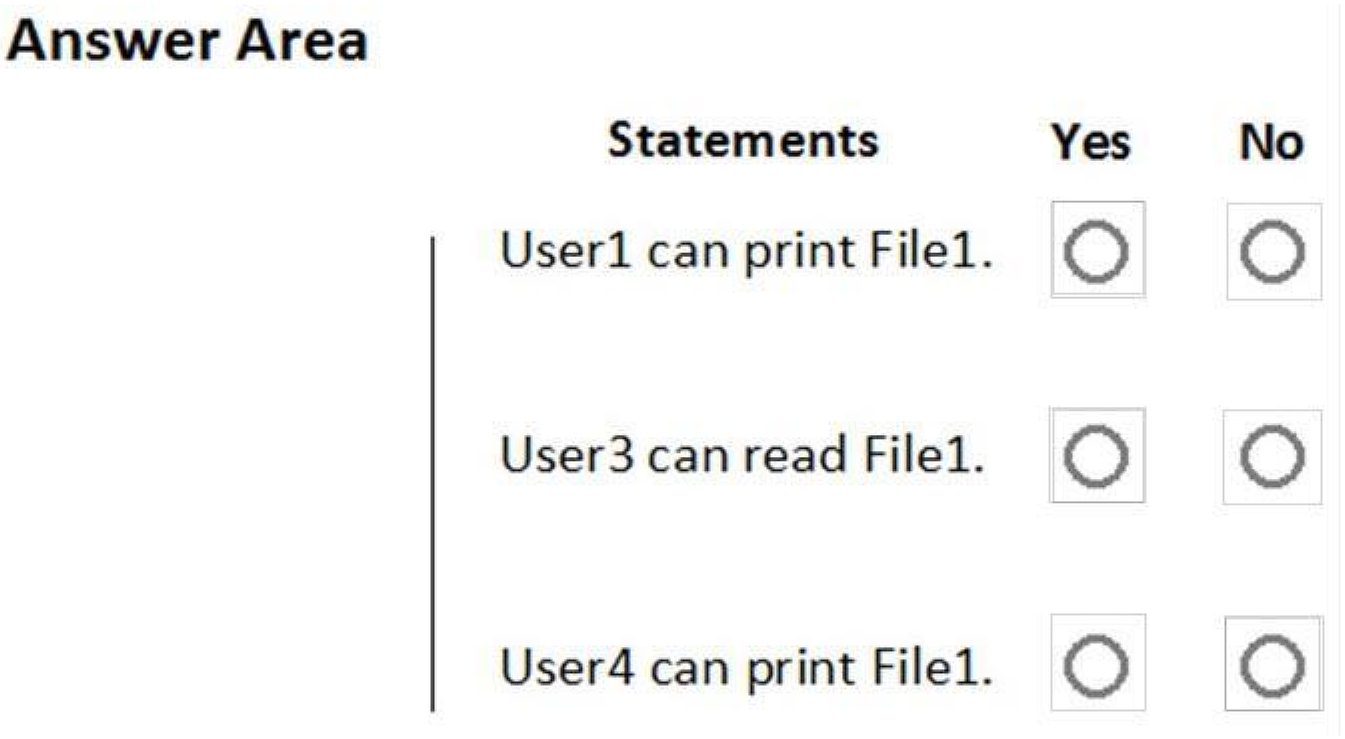
● Set permissions

○ Set user-defined permissions (Preview)

| USERS | PERMISSIONS |
|---|---|
| AuthenticatedUsers | Viewer |
| User1@contoso1812.onmicrosoft.com | Co-Author |
| User2@contoso1812.onmicrosoft.com | Reviewer |

Label1 is applied to a file named File1.
For each of the following statements, select Yes if the statement is true, Otherwise, select No.
NOTE: Each correct selection is worth one point.

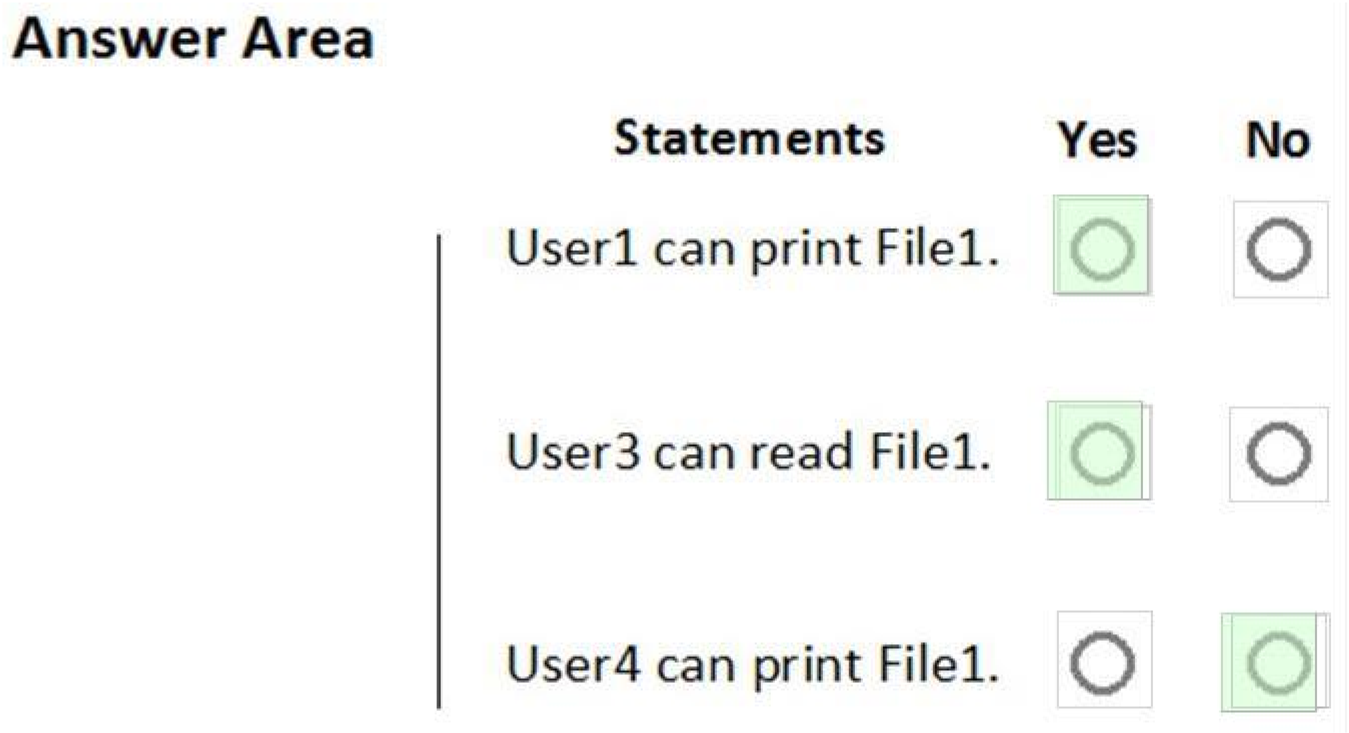
**Hot Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| User1 can print File1. | ○ | ○ |
| User3 can read File1. | ○ | ○ |
| User4 can print File1. | ○ | ○ |

**Answer Area:**



## Answer Area

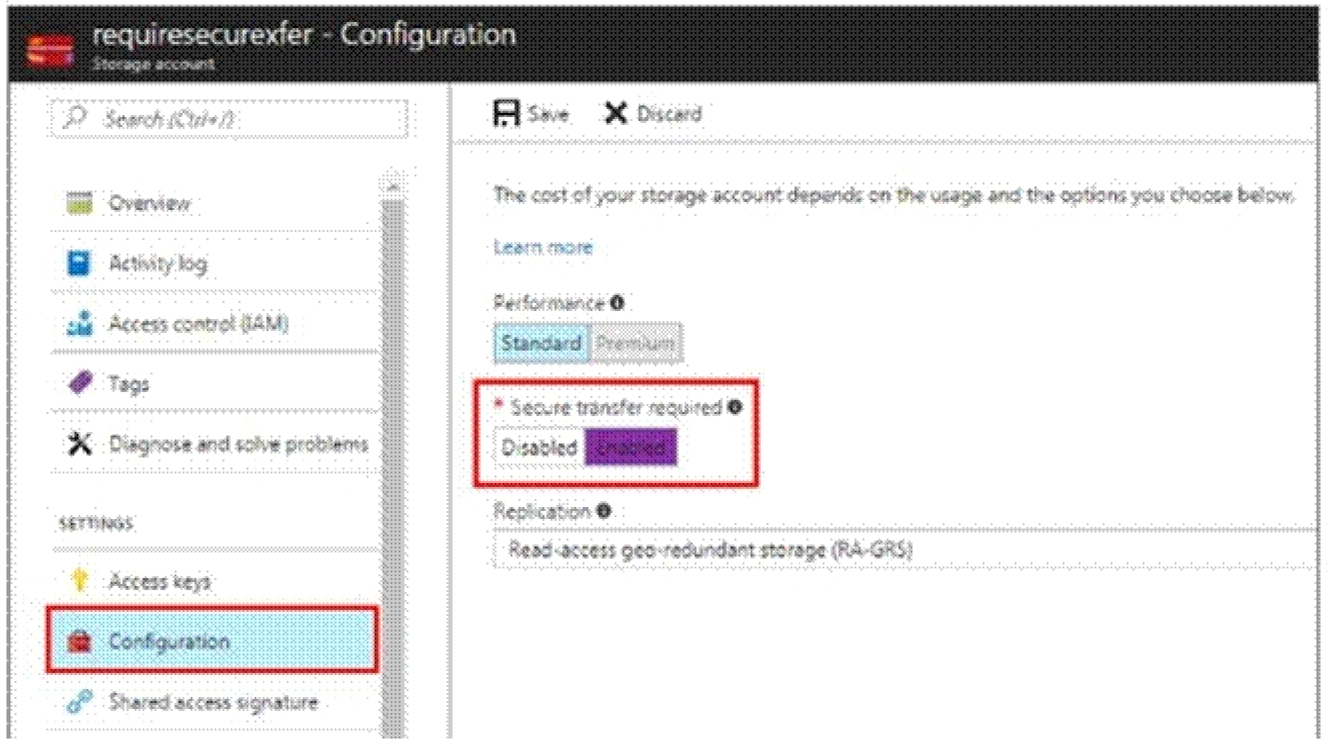
| Statements | Yes | No |
|---|---|---|
| User1 can print File1. | [✓ ○] | ○ |
| User3 can read File1. | [✓ ○] | ○ |
| User4 can print File1. | ○ | [✓ ○] |

**Section:**
**Explanation:**

**QUESTION 25**
SIMULATION
You need to prevent HTTP connections to the rg1lod10598168n1 Azure Storage account.
To complete this task, sign in to the Azure portal.

A. Explanation

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
The "Secure transfer required" feature is now supported in Azure Storage account. This feature enhances the security of your storage account by enforcing all requests to your account through a secure connection. This feature is disabled by default.
1. In Azure Portal select you Azure Storage account rg1lod10598168n1.
2. Select Configuration, and Secure Transfer required.



The cost of your storage account depends on the usage and the options you choose below.

Learn more

Performance: Standard | Premium

* Secure transfer required: Disabled | Enabled

Replication: Read-access geo-redundant storage (RA-GRS)

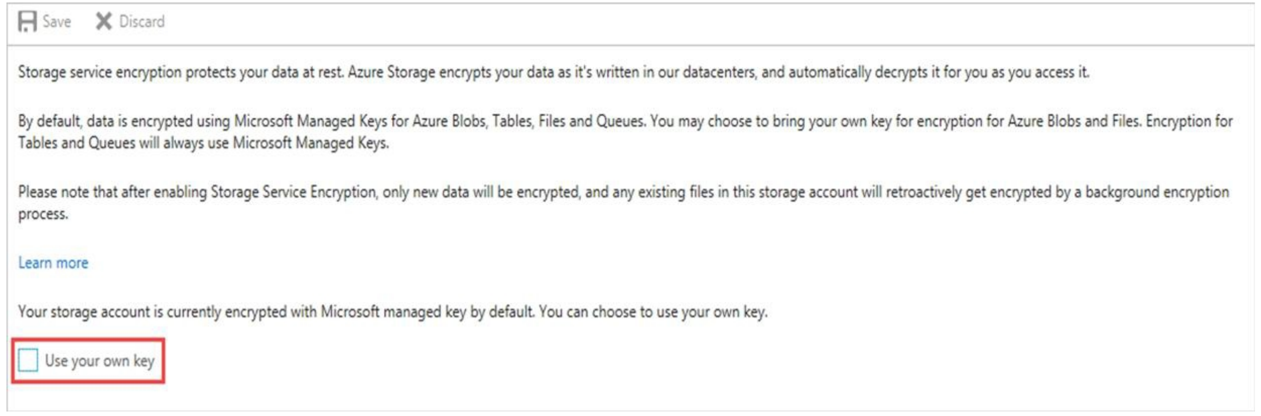
Reference:
https://techcommunity.microsoft.com/t5/Azure/quot-Secure-transfer-required-quot-is-available-in-Azure-Storage/m-p/82475

**QUESTION 26**

SIMULATION
You need to ensure that the rg1lod10598168n1 Azure Storage account is encrypted by using a key stored in the KeyVault10598168 Azure key vault.
To complete this task, sign in to the Azure portal.

A. Explanation

**Correct Answer: A**
**Section:**
**Explanation:**
Step 1: To enable customer-managed keys in the Azure portal, follow these steps:
1. Navigate to your storage account rg1lod10598168n1
2. On the Settings blade for the storage account, click Encryption. Select the Use your own key option, as shown in the following figure.



Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data is encrypted using Microsoft Managed Keys for Azure Blobs, Tables, Files and Queues. You may choose to bring your own key for encryption for Azure Blobs and Files. Encryption for Tables and Queues will always use Microsoft Managed Keys.

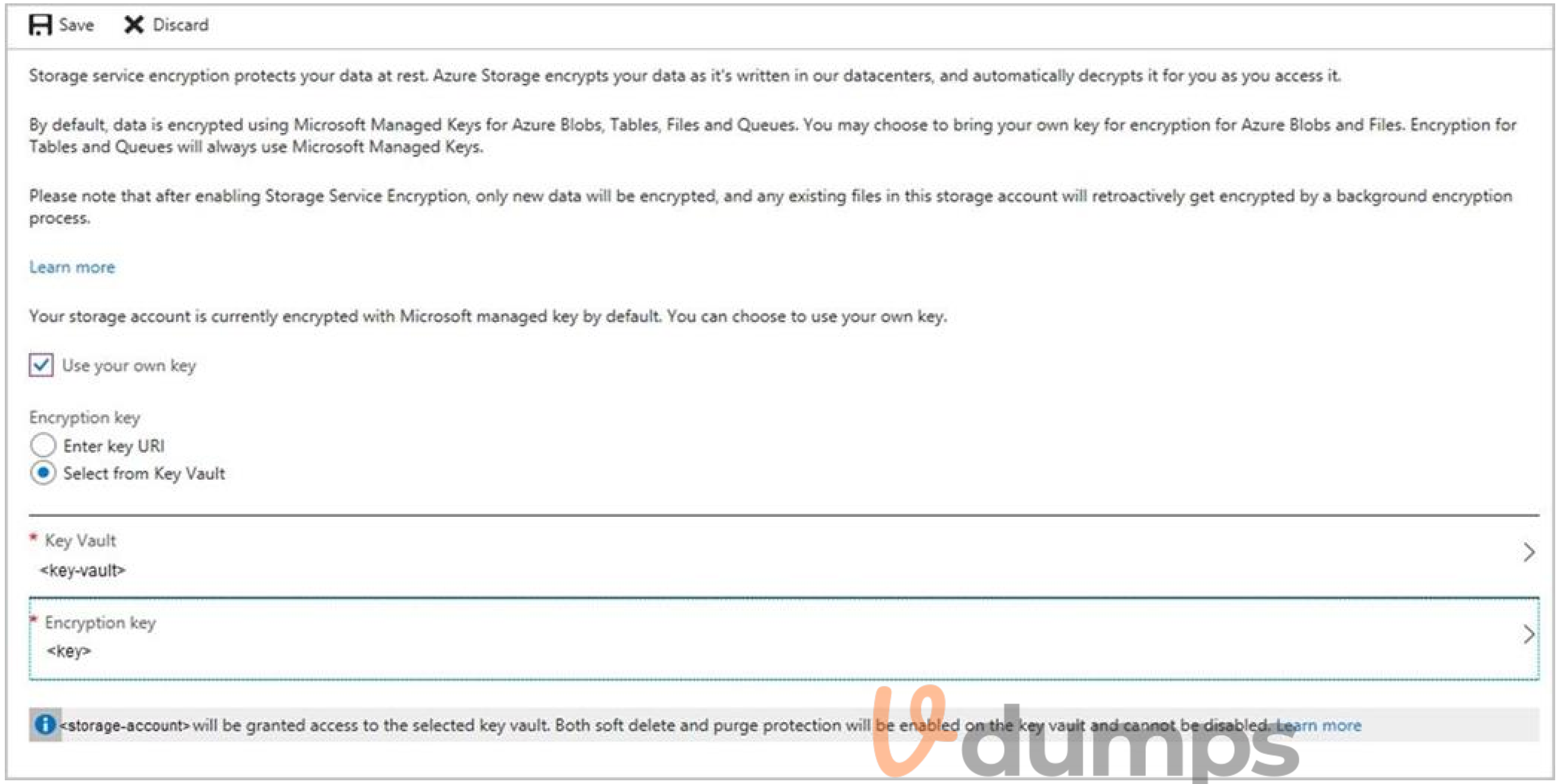
Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

Learn more

Your storage account is currently encrypted with Microsoft managed key by default. You can choose to use your own key.

□ Use your own key

Step 2: Specify a key from a key vault
To specify a key from a key vault, first make sure that you have a key vault that contains a key. To specify a key from a key vault, follow these steps:
4. Choose the Select from Key Vault option.
5. Choose the key vault KeyVault10598168 containing the key you want to use.
6. Choose the key from the key vault.



Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data is encrypted using Microsoft Managed Keys for Azure Blobs, Tables, Files and Queues. You may choose to bring your own key for encryption for Azure Blobs and Files. Encryption for Tables and Queues will always use Microsoft Managed Keys.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

Learn more

Your storage account is currently encrypted with Microsoft managed key by default. You can choose to use your own key.

☑ Use your own key

Encryption key
○ Enter key URI
● Select from Key Vault

* Key Vault
<key-vault>

* Encryption key
<key>

<storage-account> will be granted access to the selected key vault. Both soft delete and purge protection will be enabled on the key vault and cannot be disabled. Learn more

Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-encryption-keys-portal

**QUESTION 27**
You have a web app named WebApp1.
You create a web application firewall (WAF) policy named WAF1.
You need to protect WebApp1 by using WAF1.
What should you do first?

A. Deploy an Azure Front Door.
B. Add an extension to WebApp1.
C. Deploy Azure Firewall.

**Correct Answer: A**
**Section:**
**Explanation:**
References:
https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door

**QUESTION 28**
SIMULATION
You need to configure a weekly backup of an Azure SQL database named Homepage. The backup must be retained for eight weeks.
To complete this task, sign in to the Azure portal.

A. Explanation

**Correct Answer: A**
**Section:**
**Explanation:**
You need to configure the backup policy for the Azure SQL database.
1. In the Azure portal, type Azure SQL Database in the search box, select Azure SQL Database from the search results then select Homepage. Alternatively, browse to Azure SQL Database in the left navigation pane.
2. Select the server hosting the Homepage database and click on Manage backups.
3. Click on Configure policies.
4. Ensure that the Weekly Backups option is ticked.
5. Configure the How long would you like weekly backups to be retained option to 8 weeks.
6. Click Apply to save the changes.

**QUESTION 29**
SIMULATION
You need to ensure that when administrators deploy resources by using an Azure Resource Manager template, the deployment can access secrets in an Azure key vault named KV11597200.
To complete this task, sign in to the Azure portal.

A. Explanation

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
You need to configure an option in the Advanced Access Policy of the key vault.
1. In the Azure portal, type Azure Key Vault in the search box, select Azure Key Vault from the search results then select the key vault named KV11597200. Alternatively, browse to Azure Key Vault in the left navigation pane.
2. In the properties of the key vault, click on Advanced Access Policies.
3. Tick the checkbox labelled Enable access to Azure Resource Manager for template deployment.
4. Click Save to save the changes.

**QUESTION 30**
SIMULATION
You need to ensure that connections through an Azure Application Gateway named Homepage-AGW are inspected for malicious requests.
To complete this task, sign in to the Azure portal.
You do not need to wait for the task to complete.

A. Explanation

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
You need to enable the Web Application Firewall on the Application Gateway.
1. In the Azure portal, type Application gateways in the search box, select Application gateways from the search results then select the gateway named Homepage-AGW. Alternatively, browse to Application Gateways in the left navigation pane.
2. In the properties of the application gateway, click on Web application firewall.
3. For the Tier setting, select WAF V2.

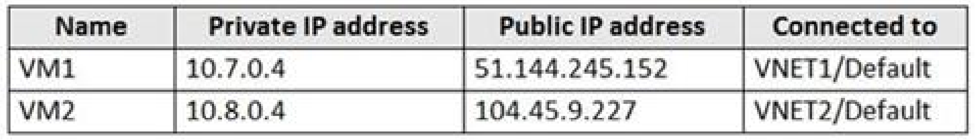
4. In the Firewall status section, click the slider to switch to Enabled.
5. In the Firewall mode section, click the slider to switch to Prevention.
6. Click Save to save the changes.

**QUESTION 31**
SIMULATION
You need to create a web app named Intranet11597200 and enable users to authenticate to the web app by using Azure Active Directory (Azure AD).
To complete this task, sign in to the Azure portal.

A. Explanation

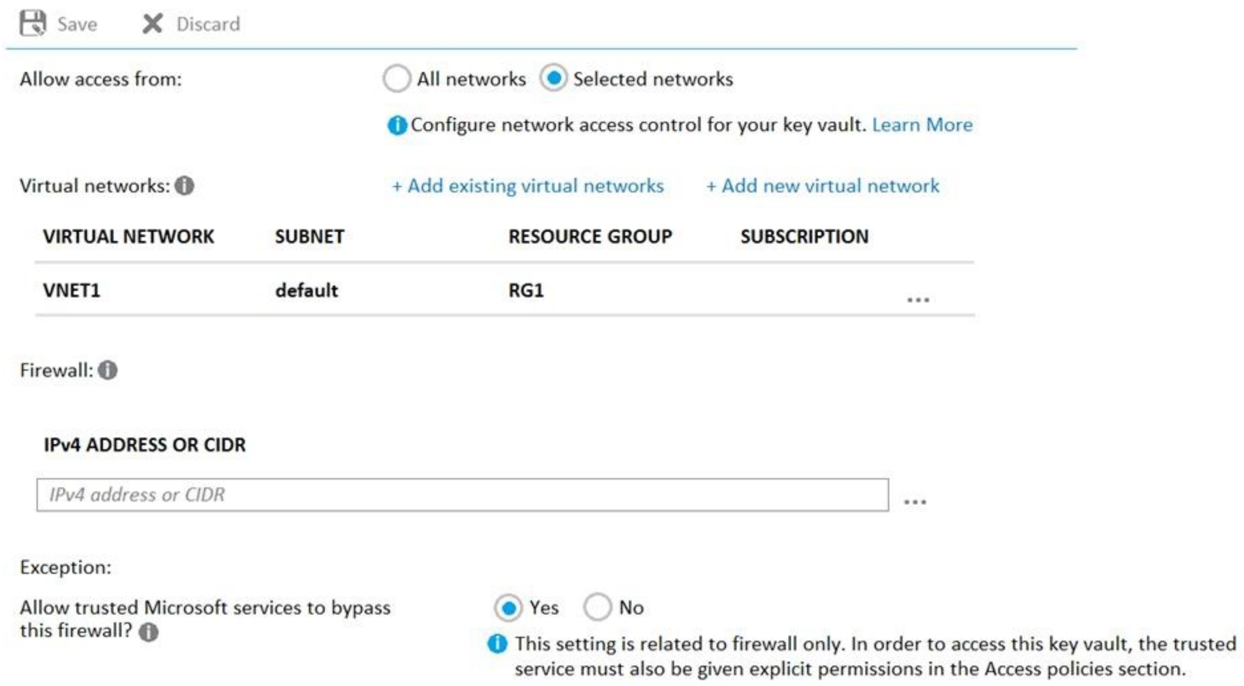
**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
1. In the Azure portal, type App services in the search box and select App services from the search results. 2. Click the Create app service button to create a new app service.
3. In the Resource Group section, click the Create new link to create a new resource group.
4. Give the resource group a name such as Intranet11597200RG and click OK.
5. In the Instance Details section, enter Intranet11597200 in the Name field.
6. In the Runtime stack field, select any runtime stack such as .NET Core 3.1.
7. Click the Review + create button.
8. Click the Create button to create the web app.
9. Click the Go to resource button to open the properties of the new web app.
10. In the Settings section, click on Authentication / Authorization.
11. Click the App Service Authentication slider to set it to On.
12. In the Action to take when request is not authentication box, select Log in with Azure Active Directory. 13. Click Save to save the changes.

**QUESTION 32**
HOTSPOT
You have an Azure subscription that contains an Azure key vault named KeyVault1 and the virtual machines shown in the following table.



| Name | Private IP address | Public IP address | Connected to |
|---|---|---|---|
| VM1 | 10.7.0.4 | 51.144.245.152 | VNET1/Default |
| VM2 | 10.8.0.4 | 104.45.9.227 | VNET2/Default |

You set the Key Vault access policy to Enable access to Azure Disk Encryption for volume encryption.
KeyVault1 is configured as shown in the following exhibit.



Allow access from: ○ All networks ● Selected networks

Configure network access control for your key vault. Learn More

Virtual networks: + Add existing virtual networks + Add new virtual network

| VIRTUAL NETWORK | SUBNET | RESOURCE GROUP | SUBSCRIPTION |
|---|---|---|---|
| VNET1 | default | RG1 | ... |

Firewall:

IPv4 ADDRESS OR CIDR

IPv4 address or CIDR ...

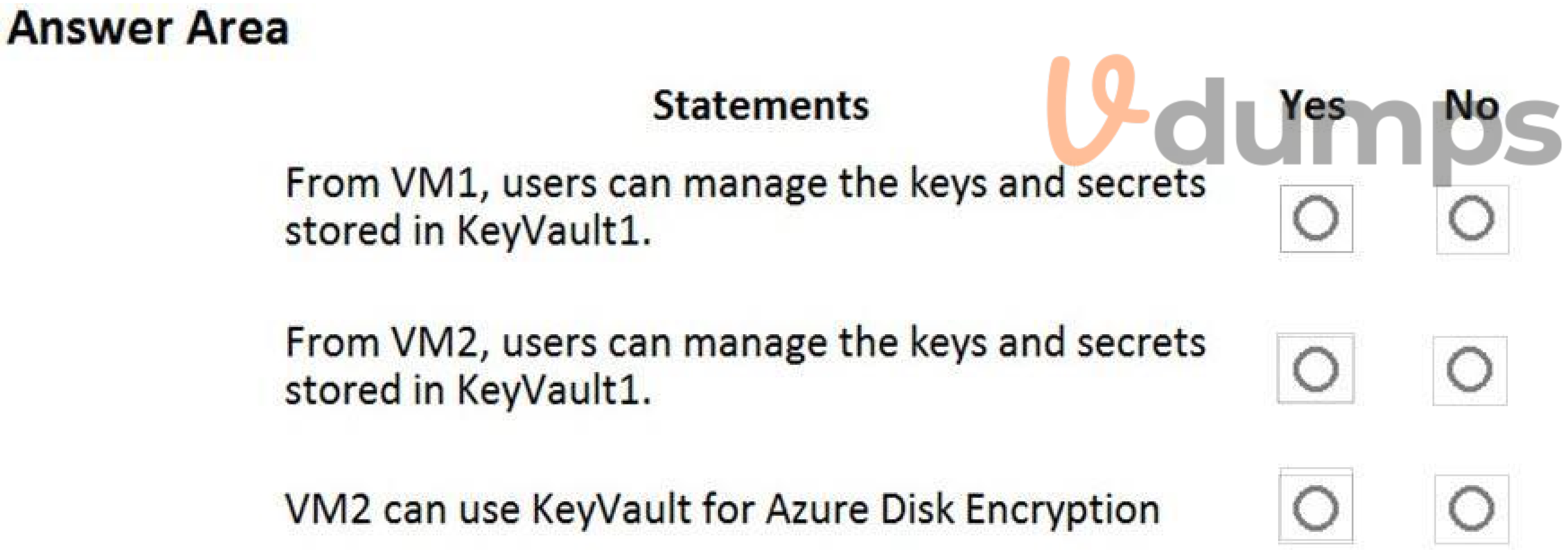
Exception:

Allow trusted Microsoft services to bypass this firewall? ● Yes ○ No

This setting is related to firewall only. In order to access this key vault, the trusted service must also be given explicit permissions in the Access policies section.

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

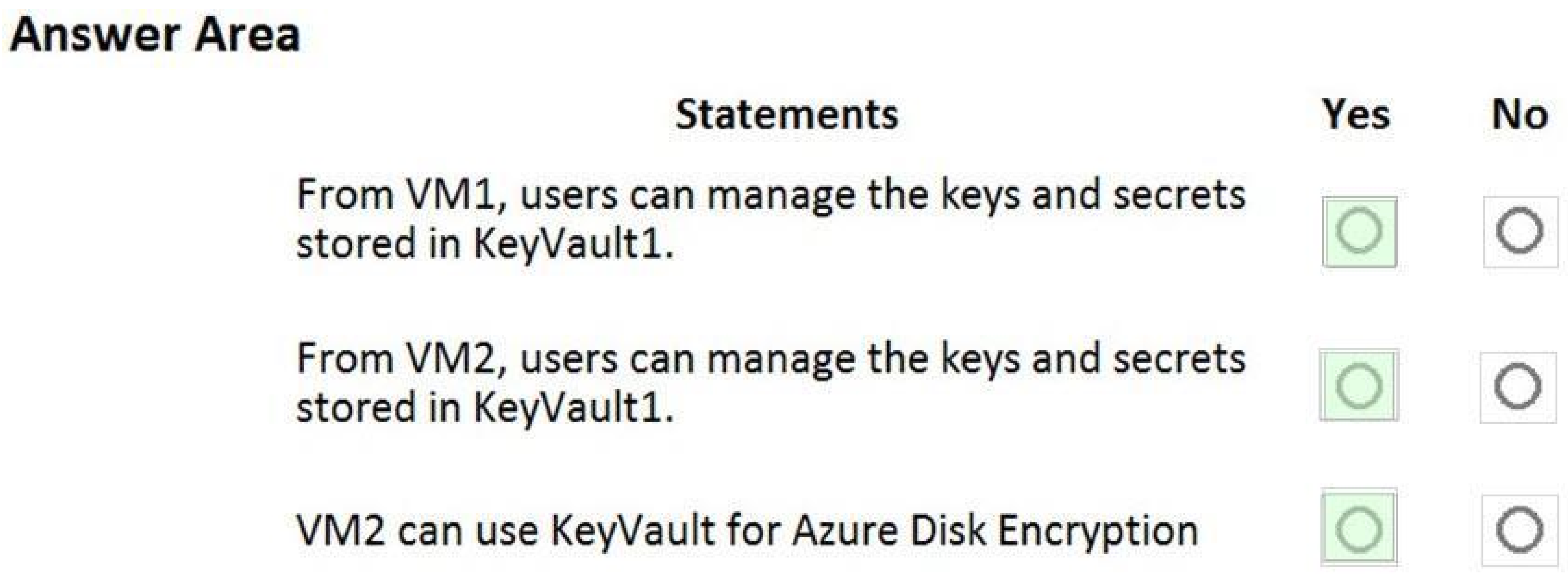
**Hot Area:**



## Answer Area

| Statements | Yes | No |
|---|---|---|
| From VM1, users can manage the keys and secrets stored in KeyVault1. | ○ | ○ |
| From VM2, users can manage the keys and secrets stored in KeyVault1. | ○ | ○ |
| VM2 can use KeyVault for Azure Disk Encryption | ○ | ○ |

**Answer Area:**



## Answer Area

| Statements | Yes | No |
|---|---|---|
| From VM1, users can manage the keys and secrets stored in KeyVault1. | [✓ ○] | ○ |
| From VM2, users can manage the keys and secrets stored in KeyVault1. | [✓ ○] | ○ |
| VM2 can use KeyVault for Azure Disk Encryption | [✓ ○] | ○ |

**Section:**
**Explanation:**

**QUESTION 33**
You have an Azure web app named WebApp1.
You upload a certificate to WebApp1.
You need to make the certificate accessible to the app code of WebApp1.
What should you do?

A. Add a user-assigned managed identity to WebApp1.
B. Add an app setting to the WebApp1 configuration.
C. Enable system-assigned managed identity for the WebApp1.
D. Configure the TLS/SSL binding for WebApp1.

**Correct Answer: B**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate-in-code

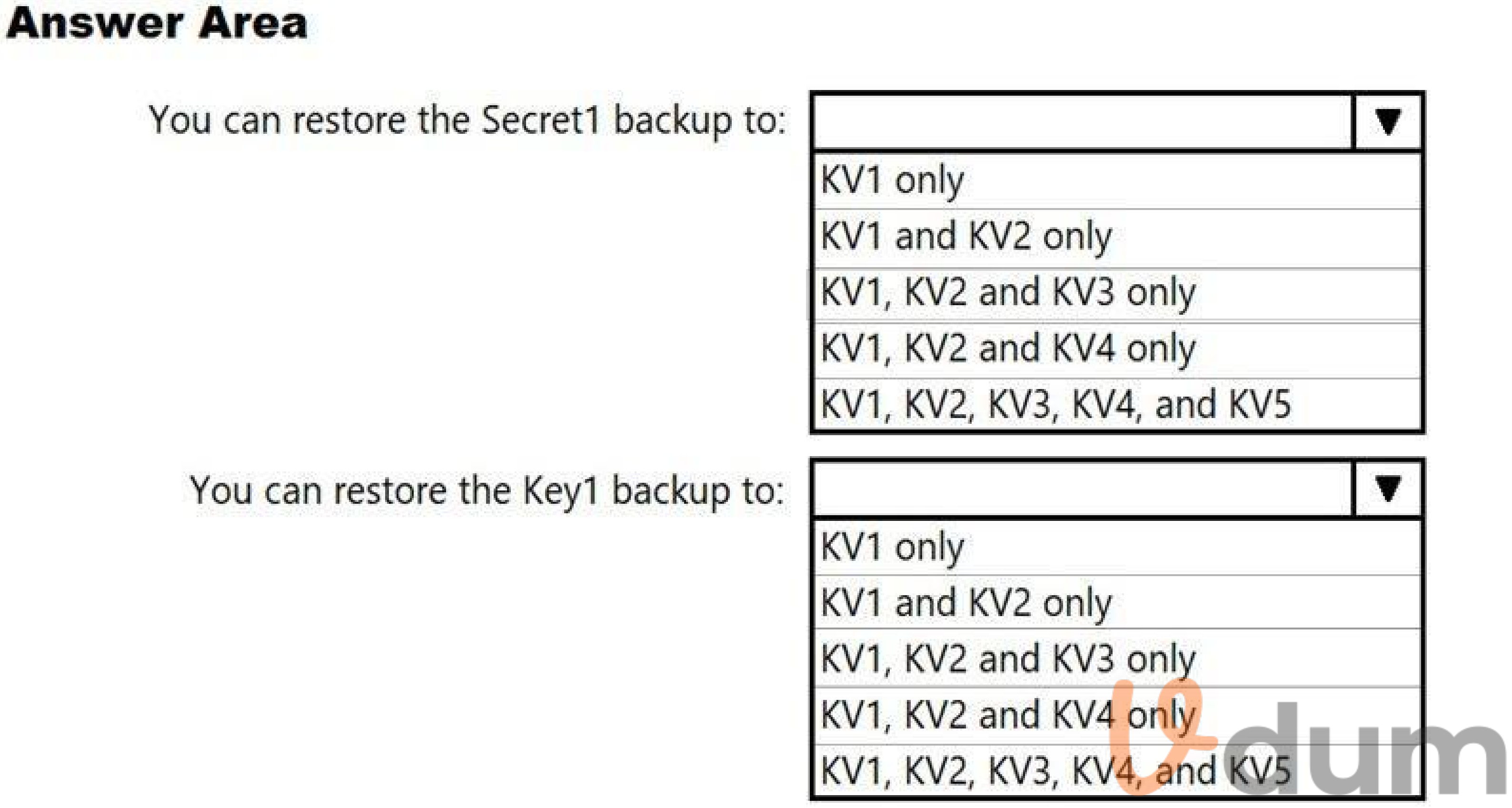
**QUESTION 34**
HOTSPOT
You have the Azure key vaults shown in the following table.

| 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.

**Hot Area:**



**Answer Area**

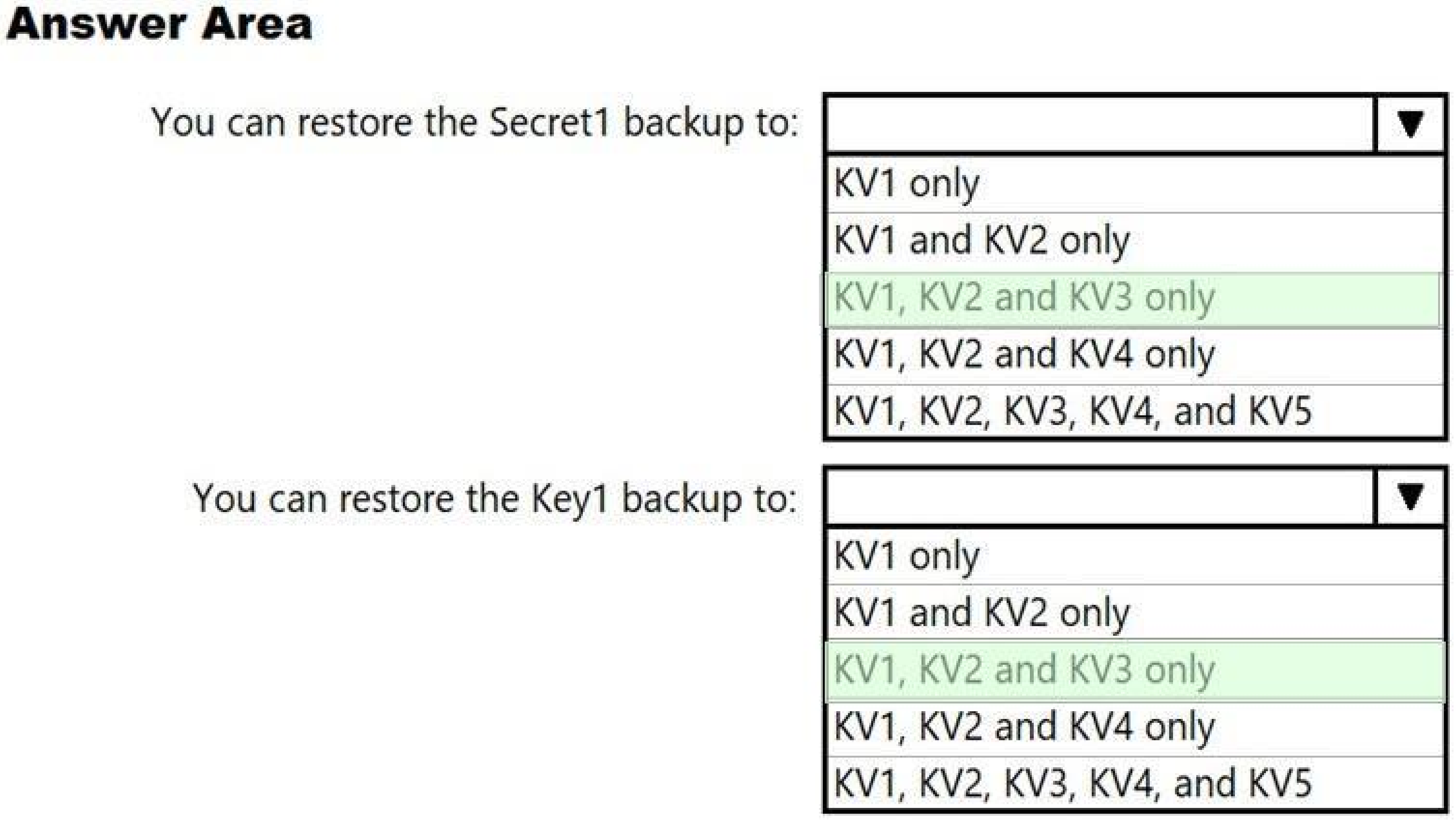
You can restore the Secret1 backup to: ▼

KV1 only
KV1 and KV2 only
KV1, KV2 and KV3 only
KV1, KV2 and KV4 only
KV1, KV2, KV3, KV4, and KV5

You can restore the Key1 backup to: ▼

KV1 only
KV1 and KV2 only
KV1, KV2 and KV3 only
KV1, KV2 and KV4 only
KV1, KV2, KV3, KV4, and KV5

**Answer Area:**



**Answer Area**

You can restore the Secret1 backup to: ▼

KV1 only
KV1 and KV2 only
[✓ KV1, KV2 and KV3 only]
KV1, KV2 and KV4 only
KV1, KV2, KV3, KV4, and KV5

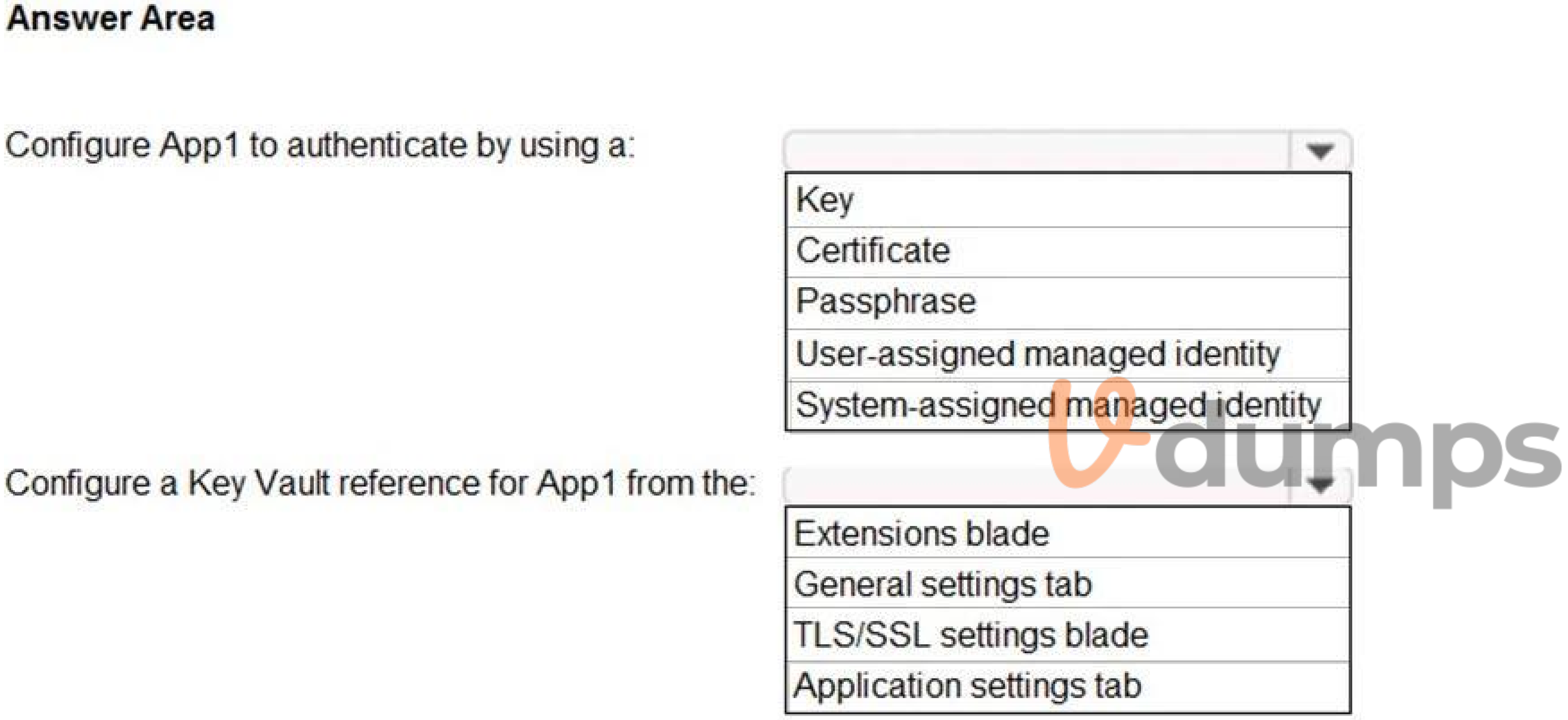
You can restore the Key1 backup to: ▼

KV1 only
KV1 and KV2 only
[✓ KV1, KV2 and KV3 only]
KV1, KV2 and KV4 only
KV1, KV2, KV3, KV4, and KV5

**Section:**
**Explanation:**
The backups can only be restored to key vaults in the same subscription and same geography. You can restore to a different region in the same geography.

**QUESTION 35**
HOTSPOT
You have an Azure subscription that contains a web app named App1 and an Azure key vault named Vault1.
You need to configure App1 to store and access the secrets in Vault1.
How should you configure App1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**



**Answer Area**

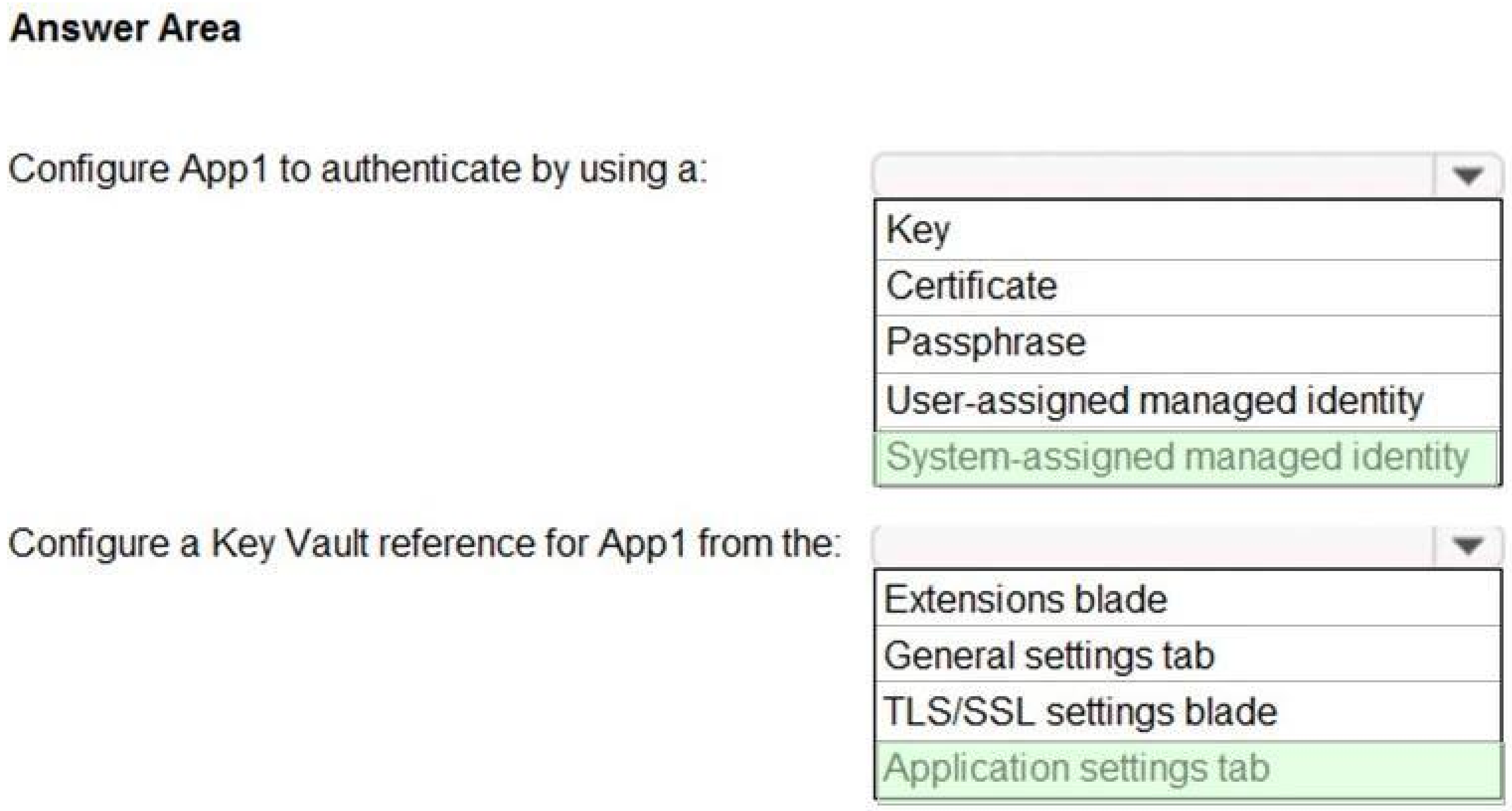
Configure App1 to authenticate by using a:

- Key
- Certificate
- Passphrase
- User-assigned managed identity
- System-assigned managed identity

Configure a Key Vault reference for App1 from the:

- Extensions blade
- General settings tab
- TLS/SSL settings blade
- Application settings tab

**Answer Area:**



## Answer Area

Configure App1 to authenticate by using a:

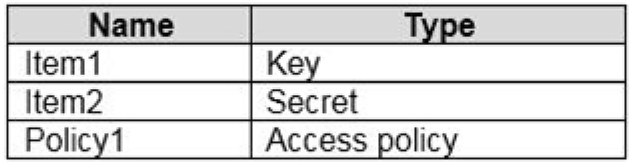
- Key
- Certificate
- Passphrase
- User-assigned managed identity
- [✓ System-assigned managed identity]

Configure a Key Vault reference for App1 from the:

- Extensions blade
- General settings tab
- TLS/SSL settings blade
- [✓ Application settings tab]

**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet

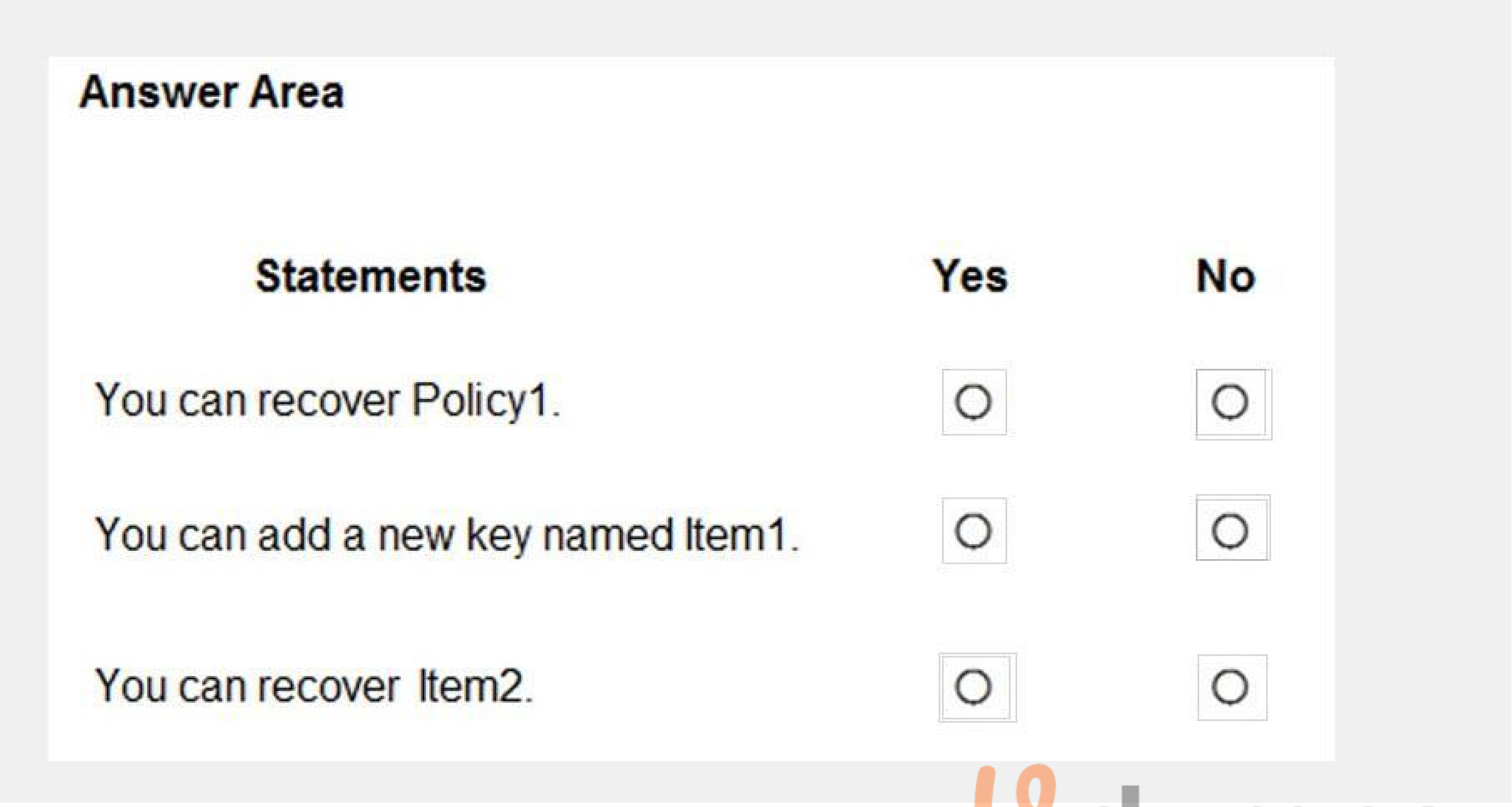
**QUESTION 36**
HOTSPOT
You have an Azure key vault named KeyVault1 that contains the items shown in the following table.



| Name | Type |
|---|---|
| Item1 | Key |
| Item2 | Secret |
| Policy1 | Access policy |

In KeyVault1, the following events occur in sequence:
Item1 is deleted.
Item2 and Policy1 are deleted.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

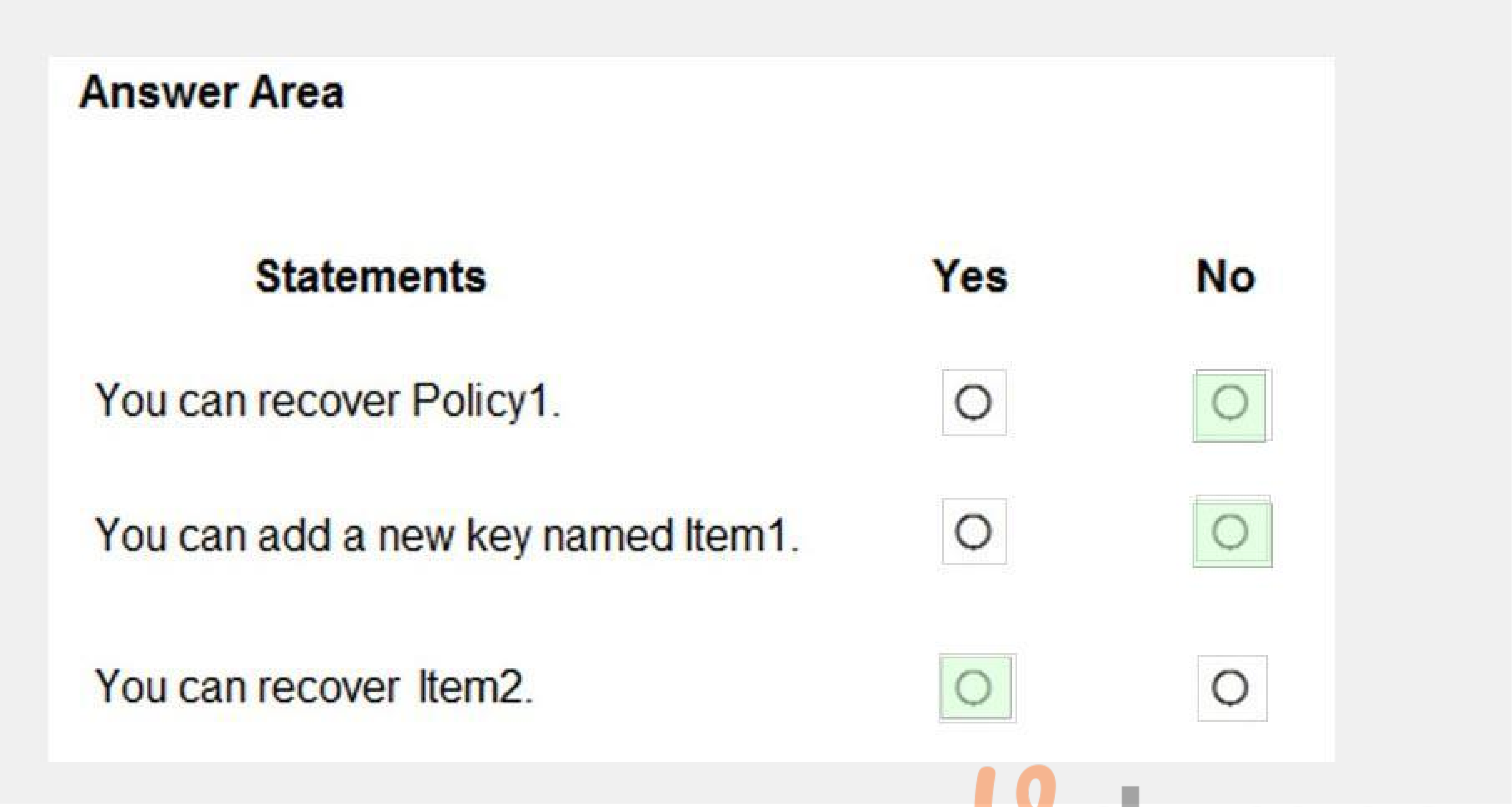
**Hot Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| You can recover Policy1. | ○ | ○ |
| You can add a new key named Item1. | ○ | ○ |
| You can recover Item2. | ○ | ○ |

**Answer Area:**



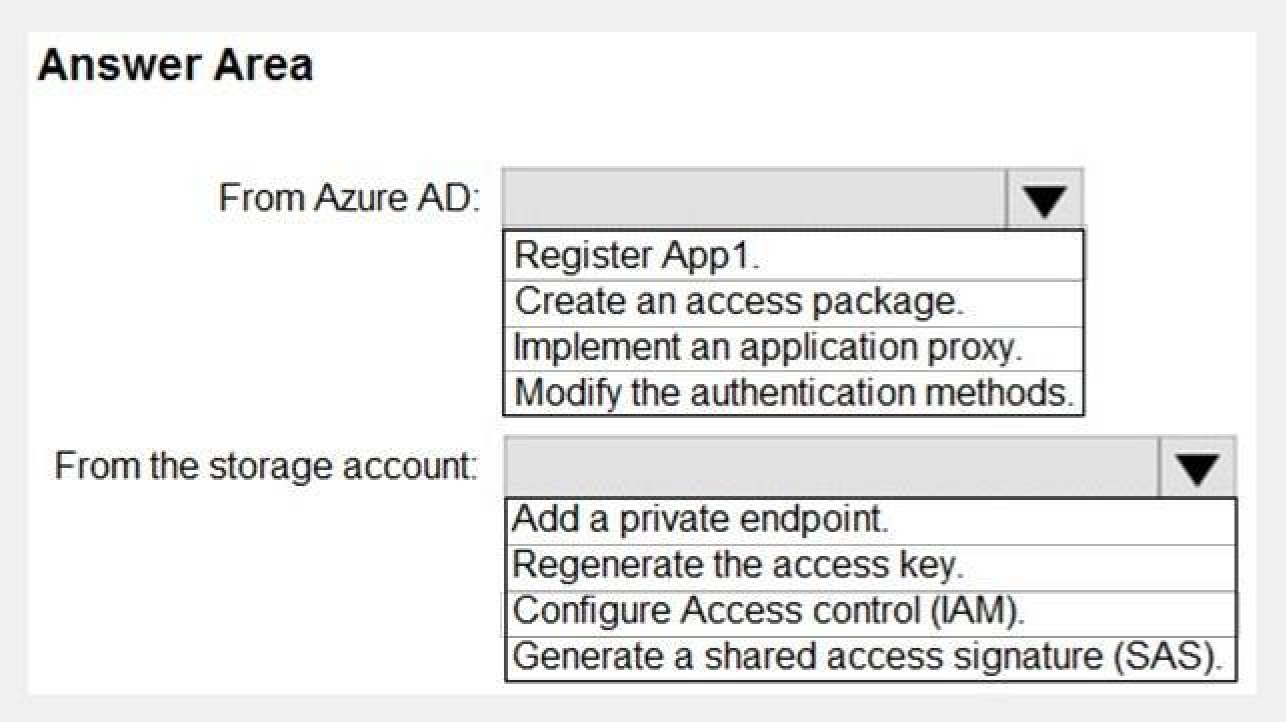
Answer Area

| Statements | Yes | No |
|---|---|---|
| You can recover Policy1. | ○ | [✓ ○] |
| You can add a new key named Item1. | ○ | [✓ ○] |
| You can recover Item2. | [✓ ○] | ○ |

**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview

**QUESTION 37**
HOTSPOT
You have an Azure Storage account that contains a blob container named container1 and a client application named App1.
You need to enable App1 access to container1 by using Azure Active Directory (Azure AD) authentication.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**



Answer Area

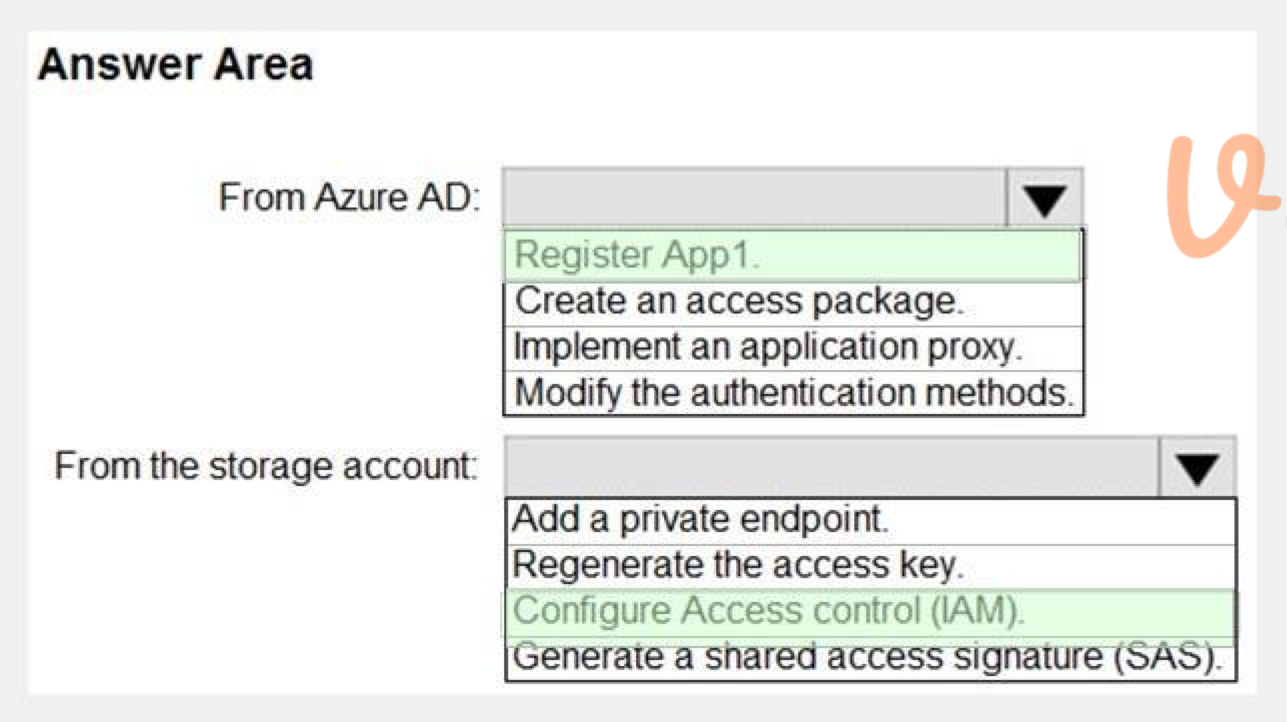
From Azure AD:

- Register App1.
- Create an access package.
- Implement an application proxy.
- Modify the authentication methods.

From the storage account:

- Add a private endpoint.
- Regenerate the access key.
- Configure Access control (IAM).
- Generate a shared access signature (SAS).

**Answer Area:**



Answer Area

From Azure AD:

- [✓ Register App1.]
- Create an access package.
- Implement an application proxy.
- Modify the authentication methods.

From the storage account:

- Add a private endpoint.
- Regenerate the access key.
- [✓ Configure Access control (IAM).]
- Generate a shared access signature (SAS).

**Section:**

**Explanation:**

Reference:

https://azure.microsoft.com/en-in/blog/announcing-the-preview-of-aad-authentication-for-storage/

https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/storage/common/storage-auth-aad-rbac-portal.md

**QUESTION 38**

You have an Azure subscription that contains an Azure SQL database named sql1.

You plan to audit sql1.

You need to configure the audit log destination. The solution must meet the following requirements:

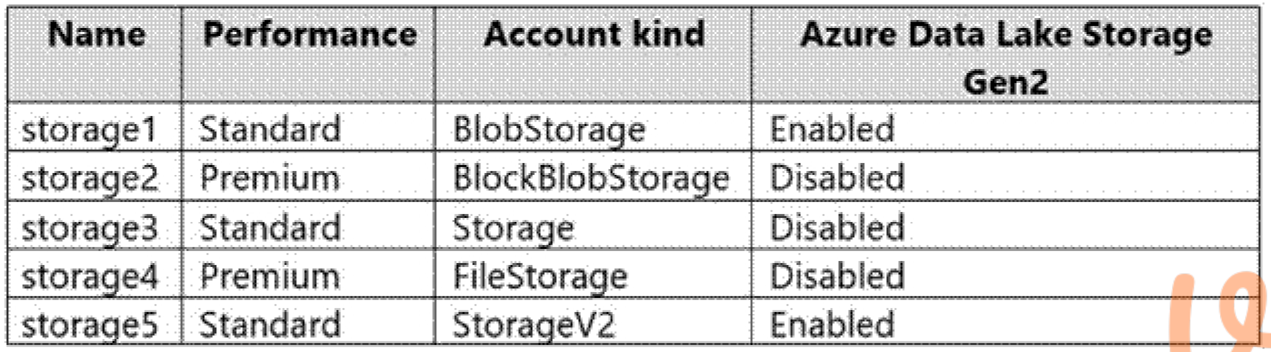
Support querying events by using the Kusto query language.

Minimize administrative effort.
What should you configure?

A. an event hub
B. a storage account
C. a Log Analytics workspace

**Correct Answer: C**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-log-analytics-wizard

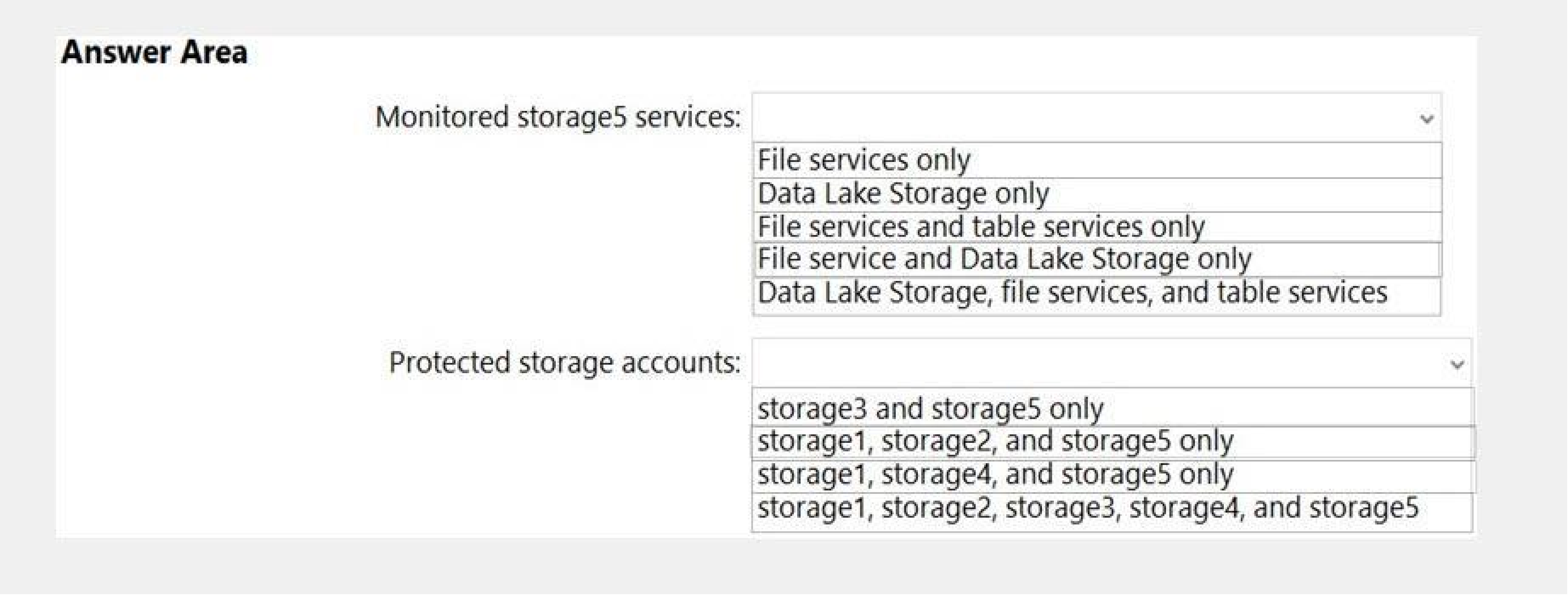
**QUESTION 39**
HOTSPOT
You have an Azure subscription that contains the storage accounts shown in the following table.



| Name | Performance | Account kind | Azure Data Lake Storage Gen2 |
|---|---|---|---|
| storage1 | Standard | BlobStorage | Enabled |
| storage2 | Premium | BlockBlobStorage | Disabled |
| storage3 | Standard | Storage | Disabled |
| storage4 | Premium | FileStorage | Disabled |
| storage5 | Standard | StorageV2 | Enabled |

You enable Azure Defender for Storage.
Which storage services of storage5 are monitored by Azure Defender for Storage, and which storage accounts are protected by Azure Defender for Storage? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**

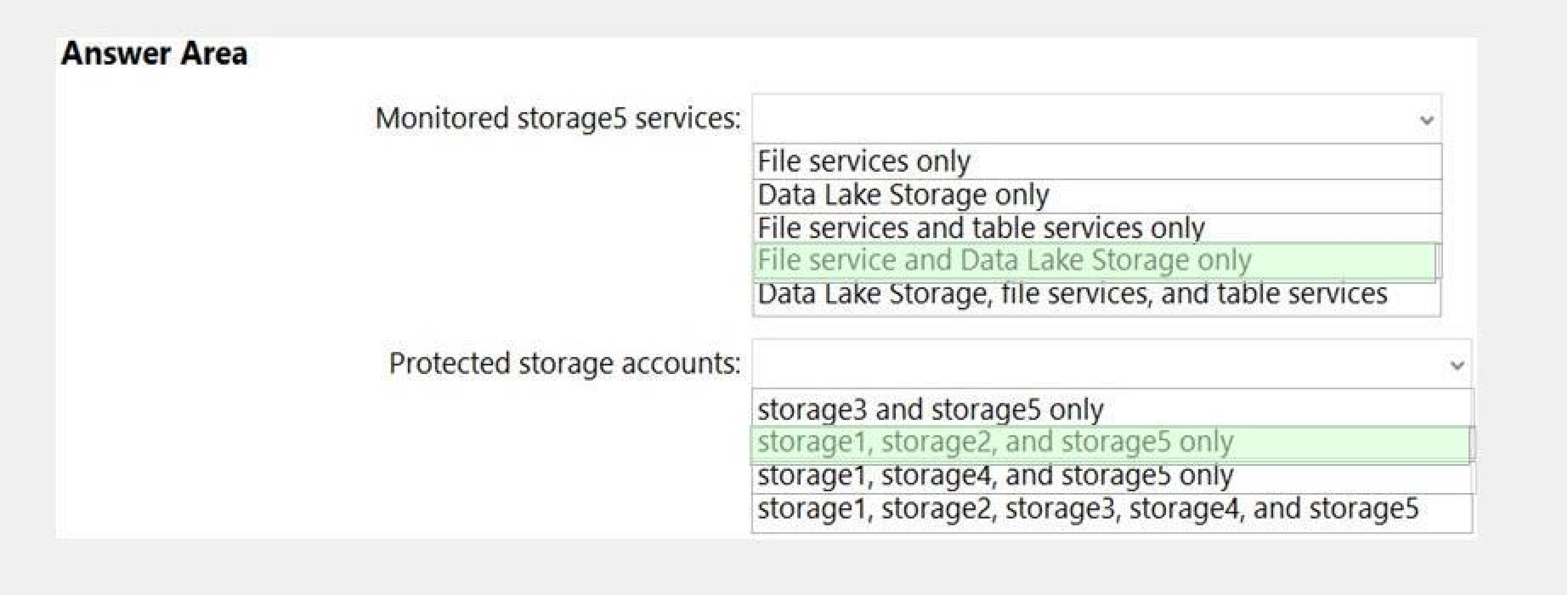


Answer Area

Monitored storage5 services:
- File services only
- Data Lake Storage only
- File services and table services only
- File service and Data Lake Storage only
- Data Lake Storage, file services, and table services

Protected storage accounts:
- storage3 and storage5 only
- storage1, storage2, and storage5 only
- storage1, storage4, and storage5 only
- storage1, storage2, storage3, storage4, and storage5

**Answer Area:**



**Answer Area**

Monitored storage5 services:

- File services only
- Data Lake Storage only
- File services and table services only
- [✓ File service and Data Lake Storage only]
- Data Lake Storage, file services, and table services

Protected storage accounts:

- storage3 and storage5 only
- [✓ storage1, storage2, and storage5 only]
- storage1, storage4, and storage5 only
- storage1, storage2, storage3, storage4, and storage5

**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/azure-defender-storage-configure?tabs=azure-security-center

**QUESTION 40**
You have an Azure subscription that contains as Azure key vault and an Azure Storage account. The key vault contains customer-managed keys. The storage account is configured to use the customer-managed keys stored in the key vault.
You plan to store data in Azure by using the following services:
Azure Files
Azure Blob storage
Azure Log Analytics
Azure Table storage
Azure Queue storage
Which two services support data encryption by using the keys stored in the key vault? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

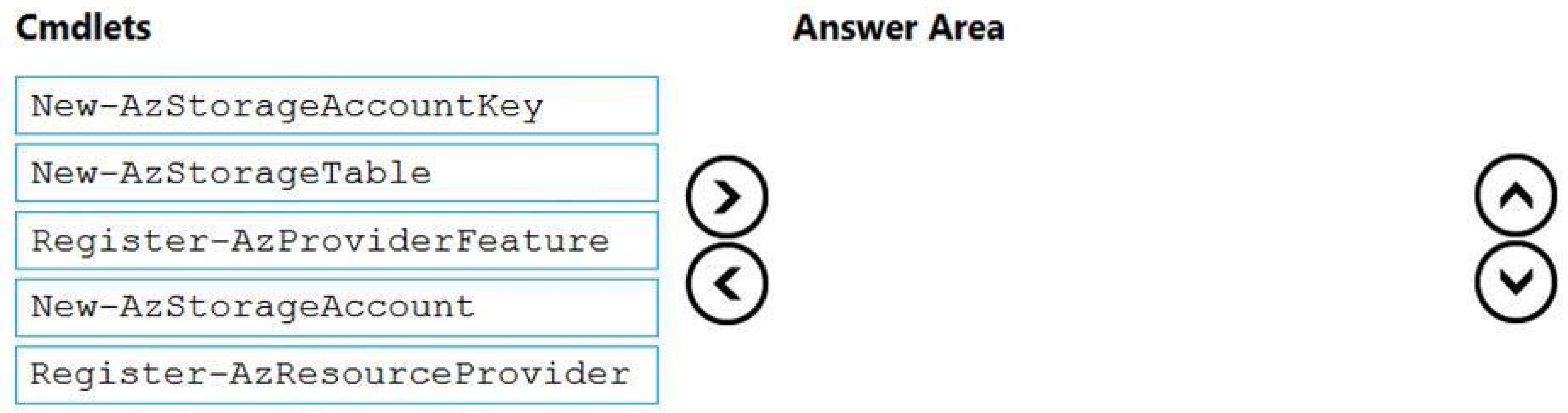
A. Table storage
B. Azure Files
C. Blob storage
D. Queue storage

**Correct Answer: B, C**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption

**QUESTION 41**
DRAG DROP
You have an Azure subscription.

You plan to create a storage account.
You need to use customer-managed keys to encrypt the tables in the storage account.
From Azure Cloud Shell, which three cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.

**Select and Place:**

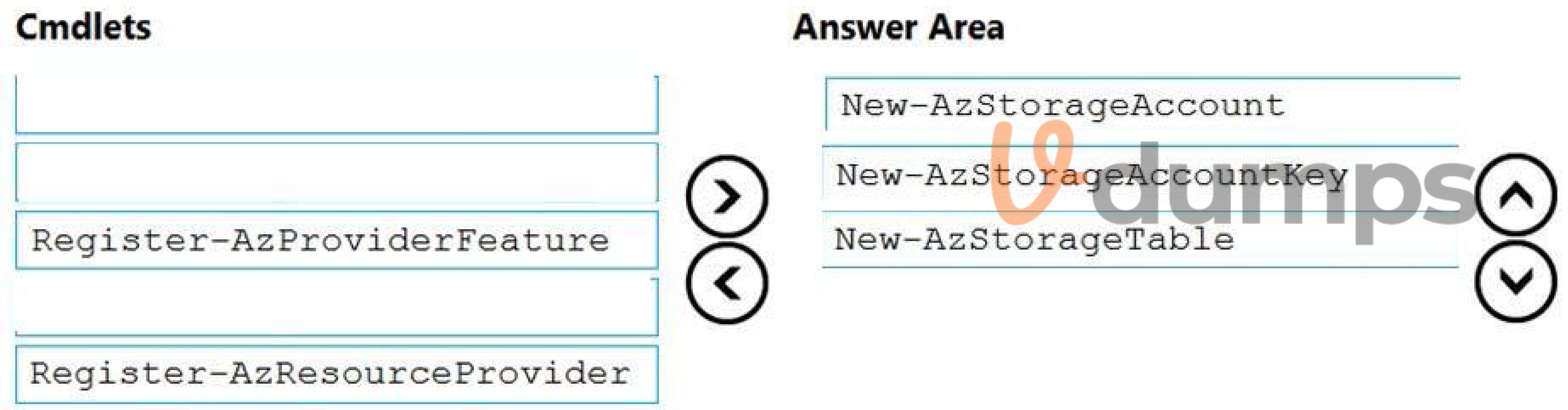


**Cmdlets**

New-AzStorageAccountKey
New-AzStorageTable
Register-AzProviderFeature
New-AzStorageAccount
Register-AzResourceProvider

**Answer Area**

**Correct Answer:**



**Cmdlets**

Register-AzProviderFeature
Register-AzResourceProvider

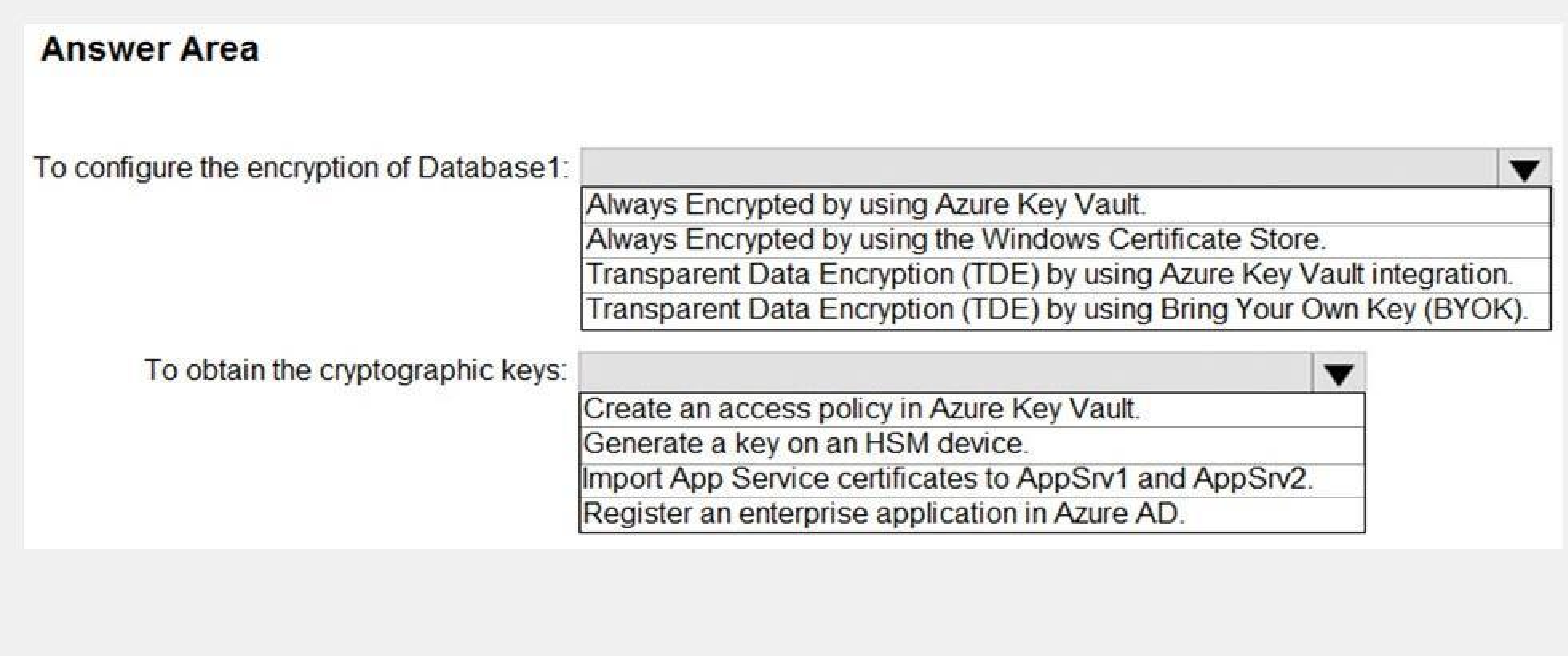
**Answer Area**

New-AzStorageAccount
New-AzStorageAccountKey
New-AzStorageTable

**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-key-vault?tabs=powershell

**QUESTION 42**
HOTSPOT
You have an Azure subscription that contains the following resources:
An Azure key vault
An Azure SQL database named Database1
Two Azure App Service web apps named AppSrv1 and AppSrv2 that are configured to use system-assigned managed identities and access Database1
You need to implement an encryption solution for Database1 that meets the following requirements:
The data in a column named Discount in Database1 must be encrypted so that only AppSrv1 can decrypt the data. AppSrv1 and AppSrv2 must be authorized by using managed identities to obtain cryptographic keys.
How should you configure the encryption settings for Database1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**



Answer Area

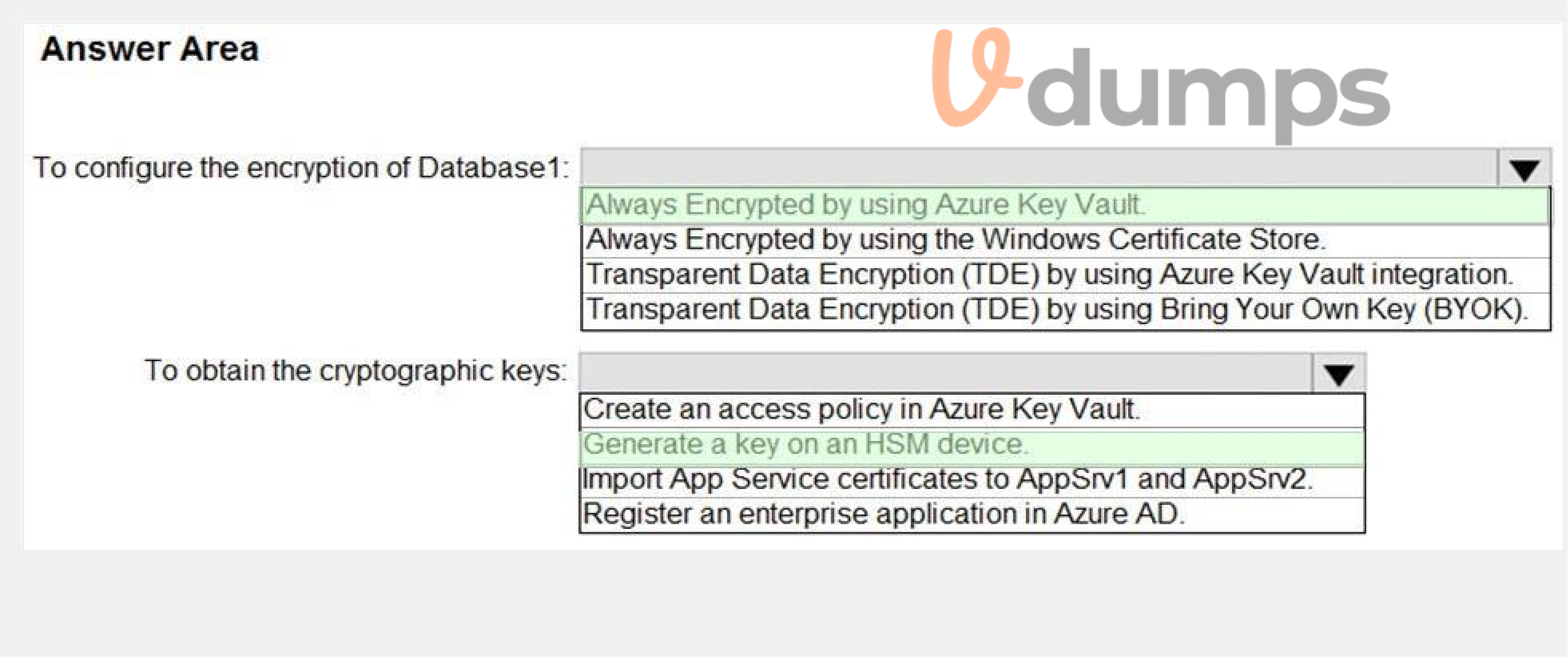
To configure the encryption of Database1:

- Always Encrypted by using Azure Key Vault.
- Always Encrypted by using the Windows Certificate Store.
- Transparent Data Encryption (TDE) by using Azure Key Vault integration.
- Transparent Data Encryption (TDE) by using Bring Your Own Key (BYOK).

To obtain the cryptographic keys:

- Create an access policy in Azure Key Vault.
- Generate a key on an HSM device.
- Import App Service certificates to AppSrv1 and AppSrv2.
- Register an enterprise application in Azure AD.

**Answer Area:**



Answer Area

To configure the encryption of Database1:

- [✓ Always Encrypted by using Azure Key Vault.]
- Always Encrypted by using the Windows Certificate Store.
- Transparent Data Encryption (TDE) by using Azure Key Vault integration.
- Transparent Data Encryption (TDE) by using Bring Your Own Key (BYOK).

To obtain the cryptographic keys:

- Create an access policy in Azure Key Vault.
- [✓ Generate a key on an HSM device.]
- Import App Service certificates to AppSrv1 and AppSrv2.
- Register an enterprise application in Azure AD.

**Section:**

**Explanation:**

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/always-encrypted-azure-key-vault-configure?tabs=azure-powershell

**QUESTION 43**

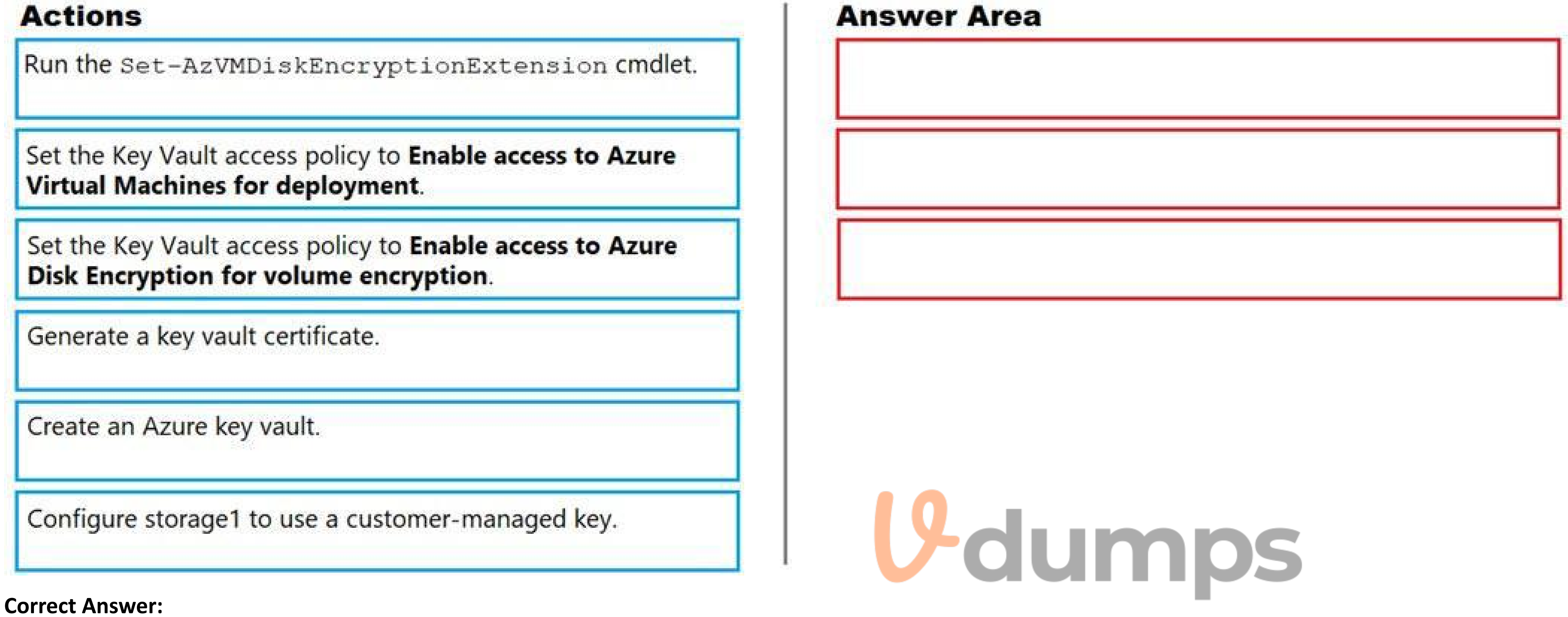
DRAG DROP

You have an Azure Storage account named storage1 and an Azure virtual machine named VM1. VM1 has a premium SSD managed disk.

You need to enable Azure Disk Encryption for VM1.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange then in the correct order.

**Select and Place:**

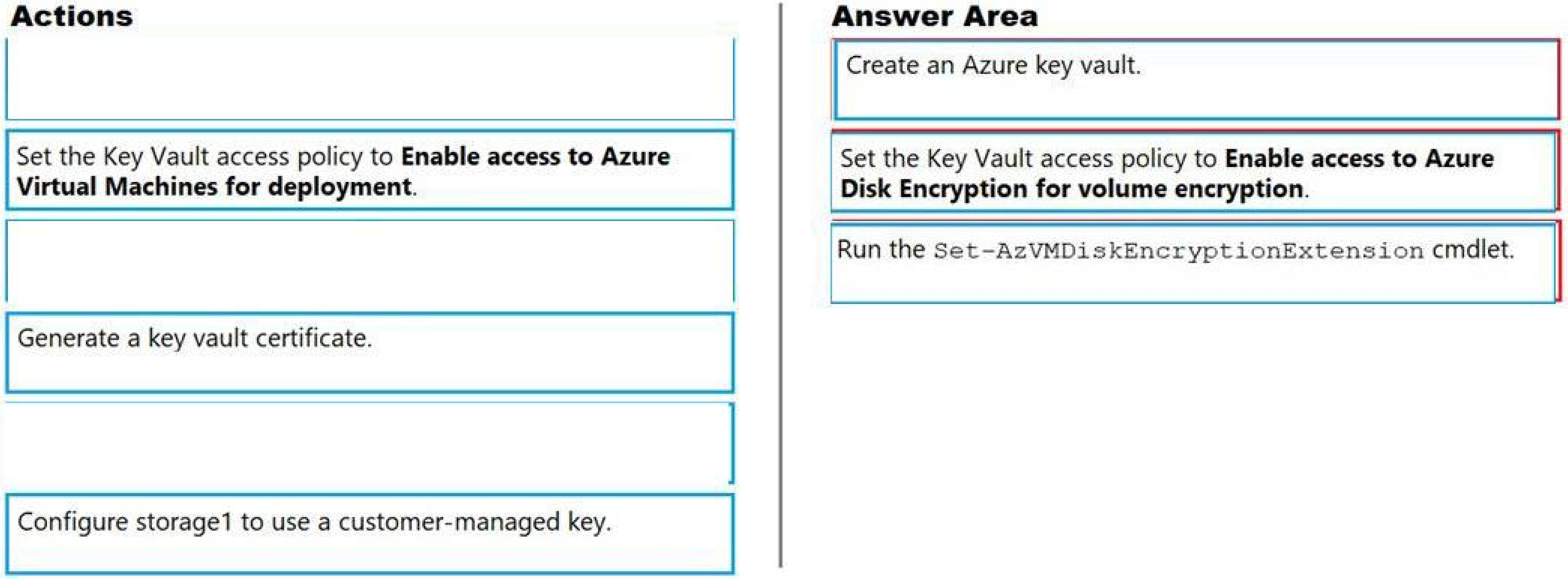


**Actions**

- Run the `Set-AzVMDiskEncryptionExtension` cmdlet.
- Set the Key Vault access policy to **Enable access to Azure Virtual Machines for deployment**.
- Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption**.
- Generate a key vault certificate.
- Create an Azure key vault.
- Configure storage1 to use a customer-managed key.

**Answer Area**

**Correct Answer:**



**Actions**

- Set the Key Vault access policy to **Enable access to Azure Virtual Machines for deployment**.
- Generate a key vault certificate.
- Configure storage1 to use a customer-managed key.

**Answer Area**

- Create an Azure key vault.
- Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption**.
- Run the `Set-AzVMDiskEncryptionExtension` cmdlet.

**Section:**

**Explanation:**

Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault

**QUESTION 44**

SIMULATION

You need to enable Advanced Data Security for the SQLdb1 Azure SQL database. The solution must ensure that Azure Advanced Threat Protection (ATP) alerts are sent to User1@contoso.com.
To complete this task, sign in to the Azure portal and modify the Azure resources.

A. Explanation

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
1. In the Azure portal, type SQL in the search box, select SQL databases from the search results then select SQLdb1. Alternatively, browse to SQL databases in the left navigation pane.
2. In the properties of SQLdb1, scroll down to the Security section and select Advanced data security.
3. Click on the Settings icon.
4. Tick the Enable Advanced Data Security at the database level checkbox.
5. Click Yes at the confirmation prompt.
6. In the Storage account select a storage account if one isn't selected by default.
7. Under Advanced Threat Protection Settings, enter User1@contoso.com in the Send alerts to box.
8. Click the Save button to save the changes.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/advanced-data-security

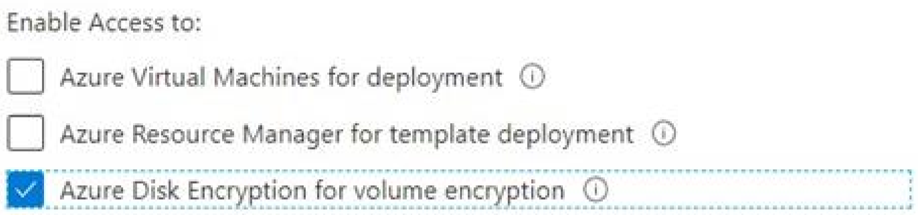
**QUESTION 45**

SIMULATION

You plan to use Azure Disk Encryption for several virtual machine disks.
You need to ensure that Azure Disk Encryption can retrieve secrets from the KeyVault11641655 Azure key vault. To complete this task, sign in to the Azure portal and modify the Azure resources.

A. Explanation

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
1. In the Azure portal, type Key Vaults in the search box, select Key Vaults from the search results then select KeyVault11641655. Alternatively, browse to Key Vaults in the left navigation pane.
2. In the Key Vault properties, scroll down to the Settings section and select Access Policies.
3. Select the Azure Disk Encryption for volume encryption



Enable Access to:

☐ Azure Virtual Machines for deployment ⓘ

☐ Azure Resource Manager for template deployment ⓘ

☑ Azure Disk Encryption for volume encryption ⓘ

4. Click Save to save the changes.

**QUESTION 46**
SIMULATION
You need to ensure that User2-11641655 has all the key permissions for KeyVault11641655.
To complete this task, sign in to the Azure portal and modify the Azure resources.

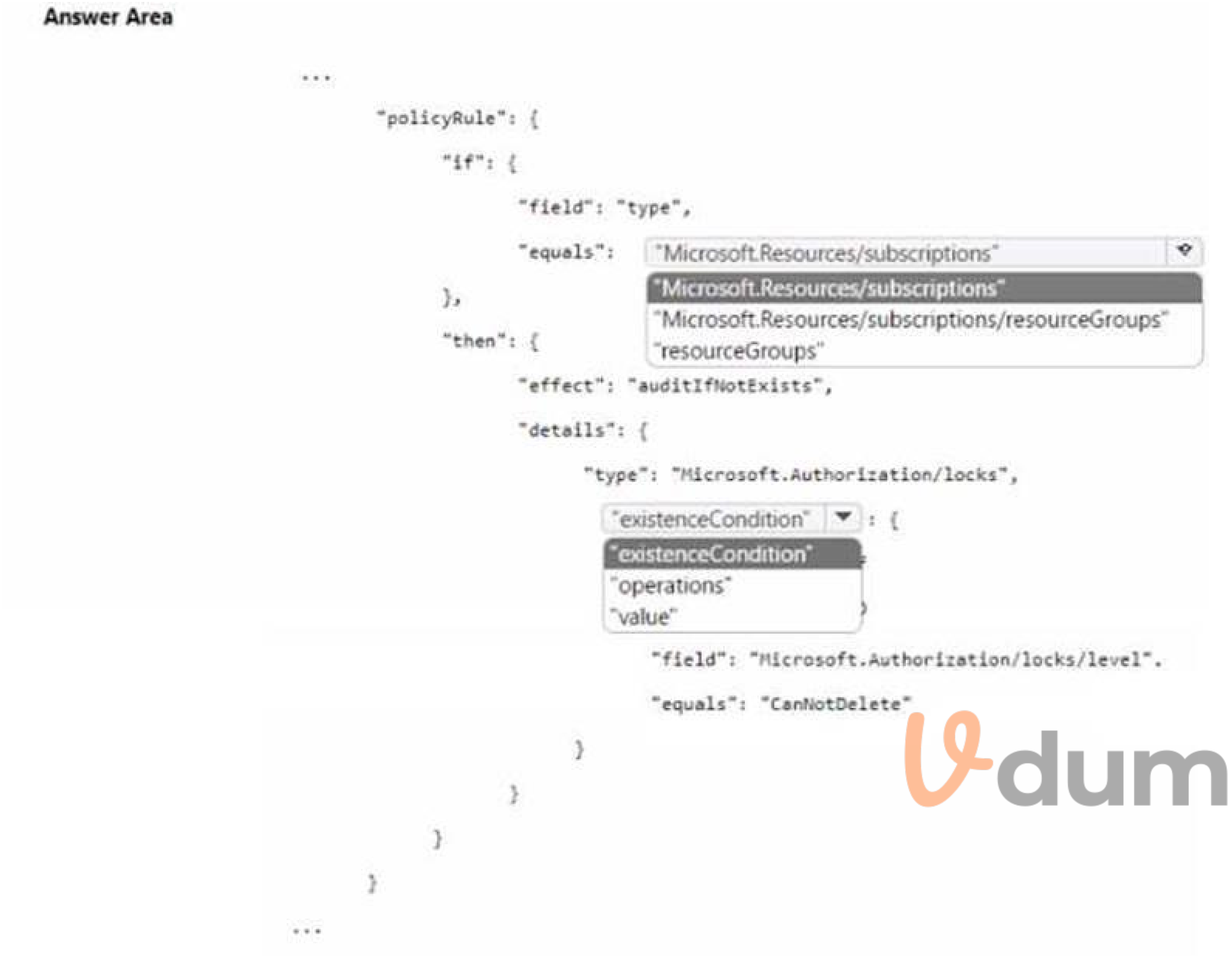
A. Explanation

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
You need to assign the user the Key Vault Secrets Officer role.
1. In the Azure portal, type Key Vaults in the search box, select Key Vaults from the search results then select KeyVault11641655. Alternatively, browse to Key Vaults in the left navigation pane.
2. In the key vault properties, select Access control (IAM).
3. In the Add a role assignment section, click the Add button.
4. In the Role box, select the Key Vault Secrets Officer role from the drop-down list.
5. In the Select box, start typing User2-11641655 and select User2-11641655 from the search results.
6. Click the Save button to save the changes.

**Exam M**

**QUESTION 1**
HOTSPOT
You plan to deploy a custom policy initiative for Microsoft Defender for Cloud.
You need to identify all the resource groups that have a Delete lock.
How should you complete the policy definition? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**



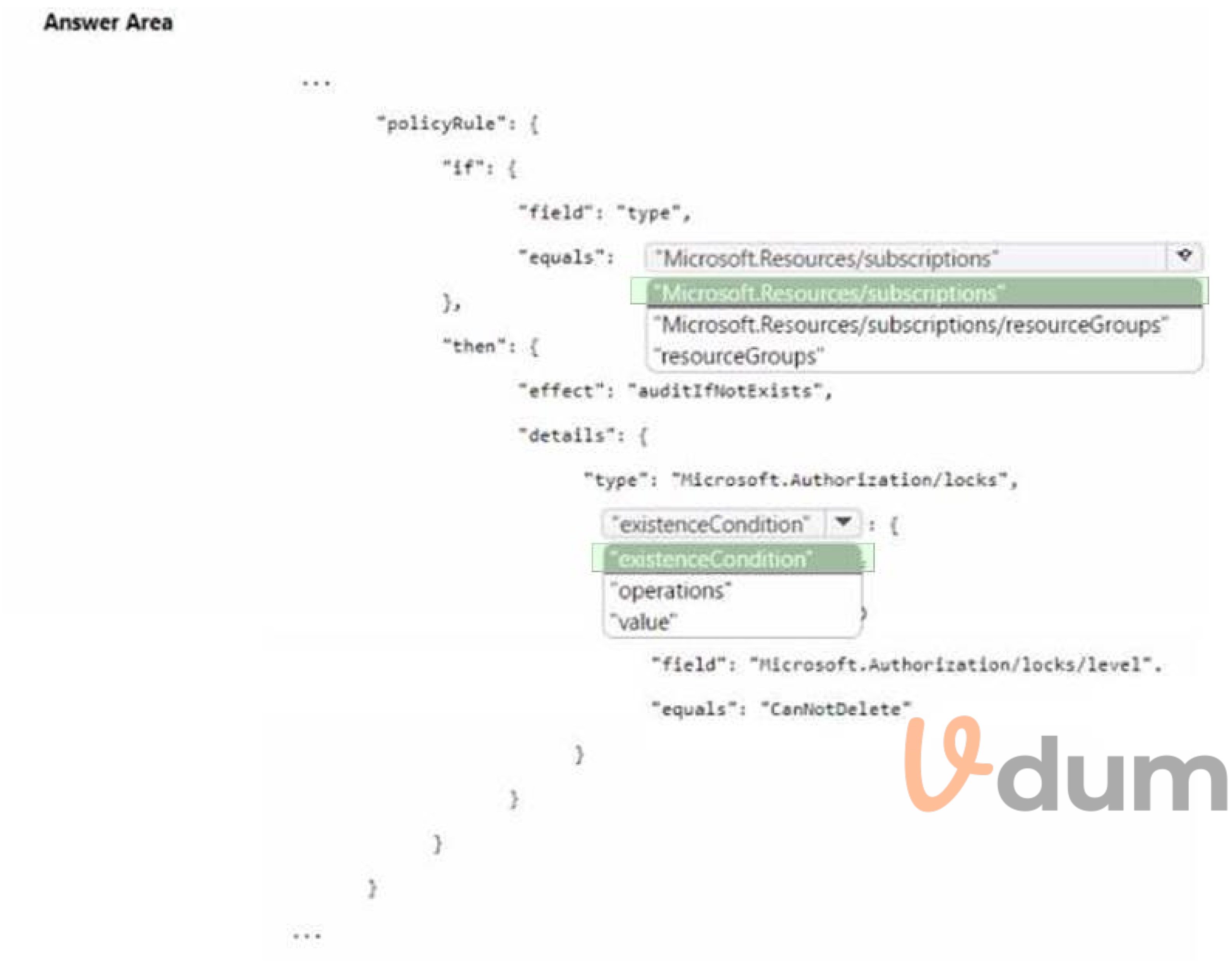
Answer Area

```
...
    "policyRule": {
        "if": {
            "field": "type",
            "equals":  "Microsoft.Resources/subscriptions"
        },
        "then": {
            "effect": "auditIfNotExists",
            "details": {
                "type": "Microsoft.Authorization/locks",
                "existenceCondition" : {
                    "field": "Microsoft.Authorization/locks/level",
                    "equals": "CanNotDelete"
                }
            }
        }
    }
...
```

"Microsoft.Resources/subscriptions"
"Microsoft.Resources/subscriptions/resourceGroups"
"resourceGroups"
"existenceCondition"
"operations"
"value"

Answer Area:

Answer Area



```
...
    "policyRule": {
        "if": {
            "field": "type",
            "equals":  "Microsoft.Resources/subscriptions"
        },
        "then": {
            "effect": "auditIfNotExists",
            "details": {
                "type": "Microsoft.Authorization/locks",
                "existenceCondition" : {
                    "field": "Microsoft.Authorization/locks/level",
                    "equals": "CanNotDelete"
                }
            }
        }
    }
...
```

"Microsoft.Resources/subscriptions"
"Microsoft.Resources/subscriptions"
"Microsoft.Resources/subscriptions/resourceGroups"
"resourceGroups"
"existenceCondition"
"existenceCondition"
"operations"
"value"

**Section:**
**Explanation:**

**QUESTION 2**

You have an Azure AD tenant that contains the users shown in the following table.

| Name | Description |
|---|---|
| User1 | Uses app password authentication for the Mail and Calendar app in Windows 10 |
| User2 | Uses Outlook on the web |

You need to ensure that the users cannot create app passwords. The solution must ensure that User1 can continue to use the Mail and Calendar app.
What should you do?

A. Assign User! the Authentication Policy Administrator role.
B. Enable Azure AD Password Protection.
C. Configure a multi-factor authentication (MFA) registration policy.
D. Create a new app registration.

**Correct Answer: C**
**Section:**

**QUESTION 3**
You have an Azure subscription that uses Microsoft Defender for Cloud.
You have an Amazon Web Services (AWS) account.
You need to ensure that when you deploy a new AWS Elastic Compute Cloud (EC2) instance, the Microsoft Defender for Servers agent installs automatically.
What should you configure first?

A. the log Analytics agent
B. the Azure Monitor agent
C. the native cloud connector
D. the classic cloud connector

**Correct Answer: A**
**Section:**

**QUESTION 4**
You have an Azure subscription.
You plan to map an online infrastructure and perform vulnerability scanning for the following:
• ASNs
• Hostnames
• IP addresses
• SSL certificates
What should you use?

A. Microsoft Defender for Cloud
B. Microsoft Defender for Identity
C. Microsoft Defender for Endpoint
D. Microsoft Defender External Attack Surface Management (Defender EASM)

**Correct Answer: D**
**Section:**

**QUESTION 5**
You have an Azure subscription.
You plan to create a workflow automation in Azure Security Center that will automatically remediate a security vulnerability. What should you create first?

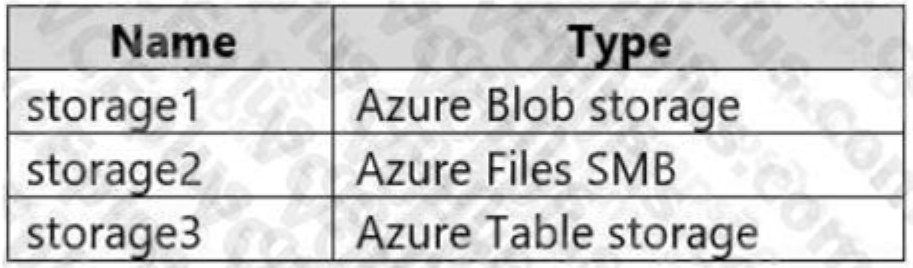
A. an automation account
B. a managed identity
C. an Azure logic app
D. an Azure function app
E. an alert rule

**Correct Answer: C**
**Section:**
**Explanation:**
Reference: https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

**QUESTION 6**

HOTSPOT

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



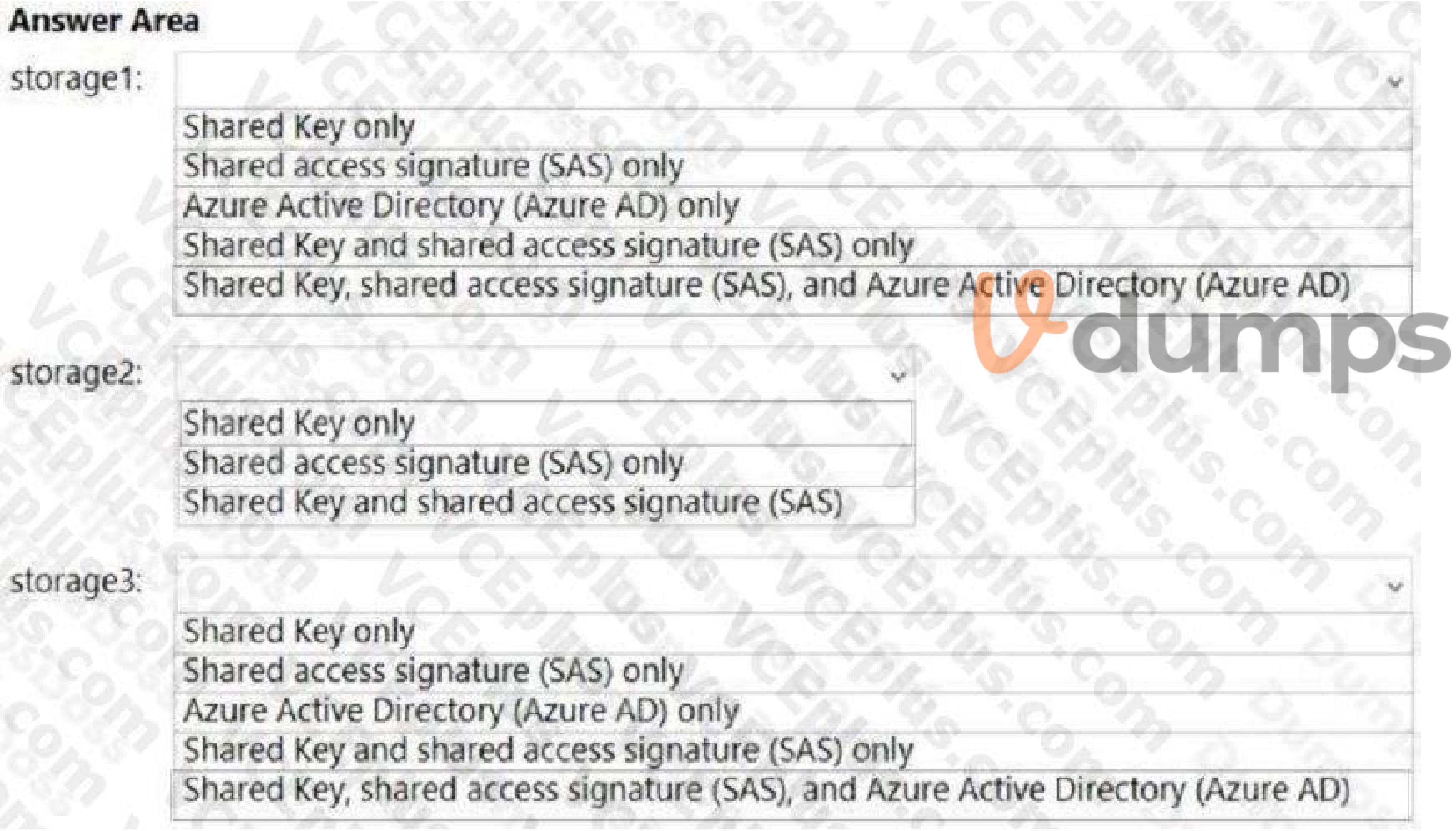
| Name | Type |
|---|---|
| storage1 | Azure Blob storage |
| storage2 | Azure Files SMB |
| storage3 | Azure Table storage |

You need to configure authorization access.

Which authorization types can you use for each storage account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Hot Area:**



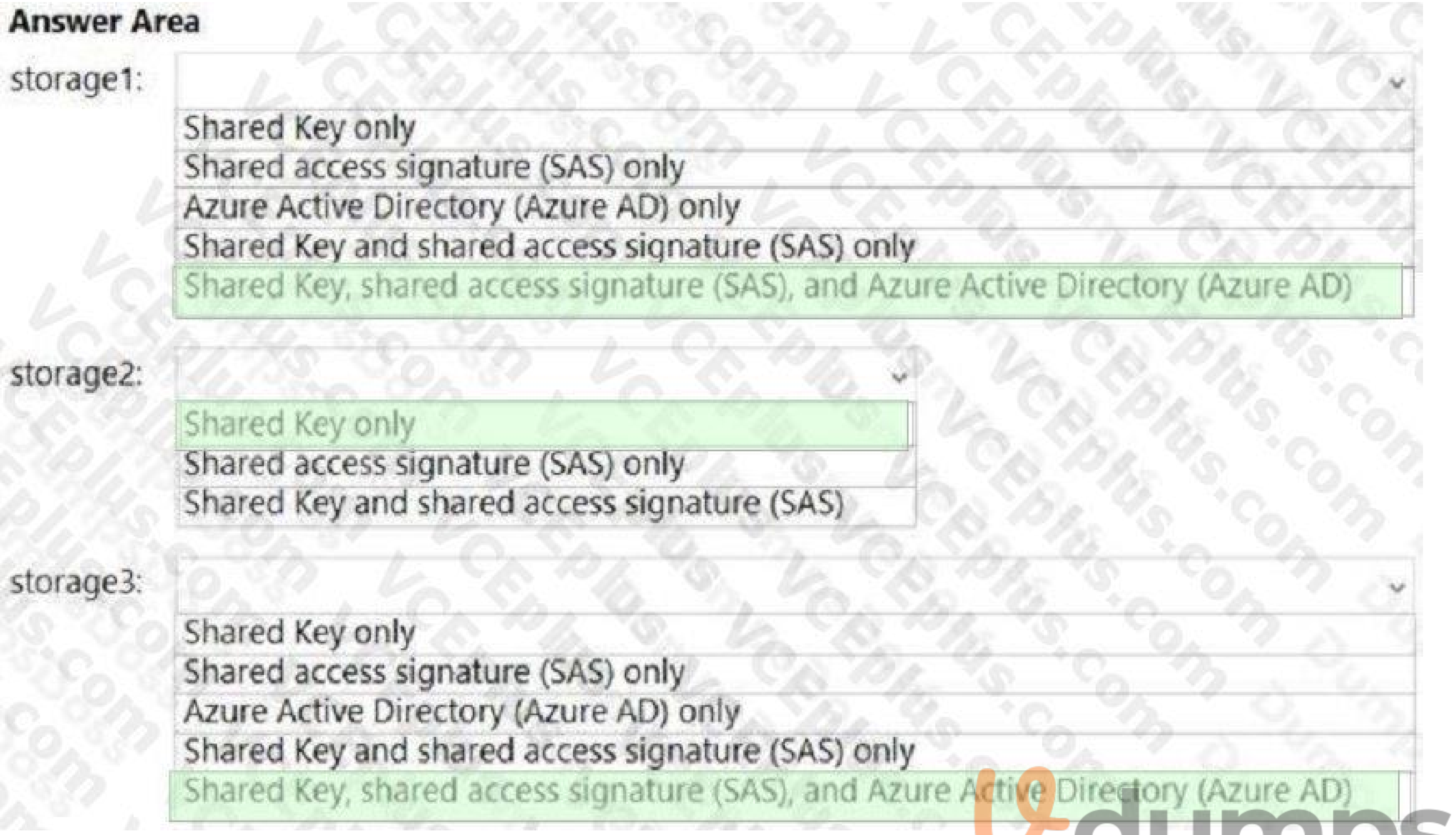
**Answer Area**

storage1:
- Shared Key only
- Shared access signature (SAS) only
- Azure Active Directory (Azure AD) only
- Shared Key and shared access signature (SAS) only
- Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

storage2:
- Shared Key only
- Shared access signature (SAS) only
- Shared Key and shared access signature (SAS)

storage3:
- Shared Key only
- Shared access signature (SAS) only
- Azure Active Directory (Azure AD) only
- Shared Key and shared access signature (SAS) only
- Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

**Answer Area:**



**Answer Area**

storage1:

- Shared Key only
- Shared access signature (SAS) only
- Azure Active Directory (Azure AD) only
- Shared Key and shared access signature (SAS) only
- [✓ Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)]

storage2:

- [✓ Shared Key only]
- Shared access signature (SAS) only
- Shared Key and shared access signature (SAS)

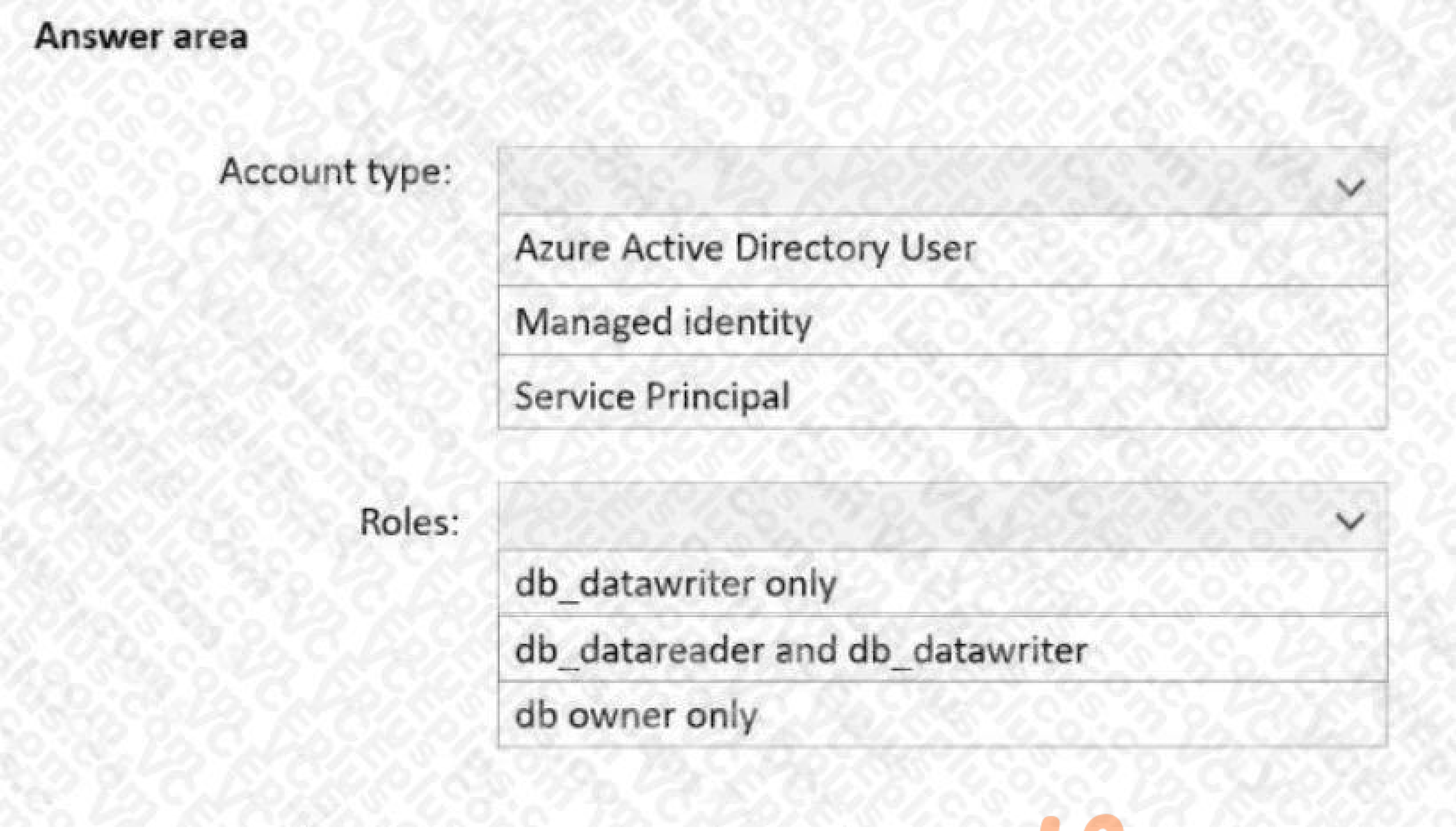
storage3:

- Shared Key only
- Shared access signature (SAS) only
- Azure Active Directory (Azure AD) only
- Shared Key and shared access signature (SAS) only
- [✓ Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)]

**Section:**
**Explanation:**
Reference: https://docs.microsoft.com/en-us/azure/storage/common/authorize-data-access 0CB84EF020870C137158A568970423A4

**QUESTION 7**
HOTSPOT
You have an Azure subscription that contains an Azure SQL database named SQL1.
You plan to deploy a web app named App1.
You need to provide App1 with read and write access to SQL1. The solution must meet the following requirements:
Provide App1 with access to SQL1 without storing a password.
Use the principle of least privilege. Minimize administrative effort.
Which type of account should App1 use to access SQL1, and which database roles should you assign to App1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**



**Answer area**

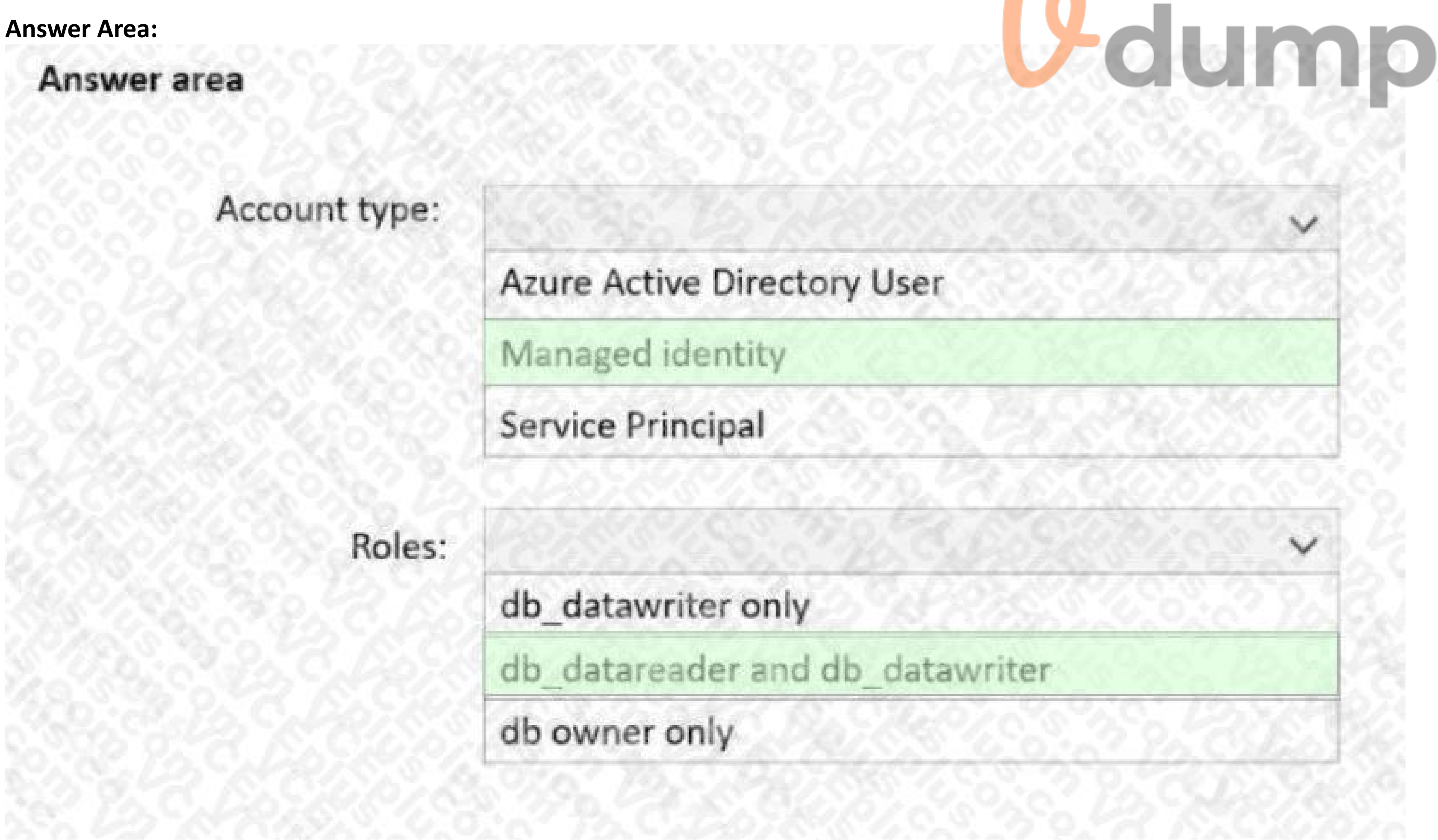
Account type:

- Azure Active Directory User
- Managed identity
- Service Principal

Roles:

- db_datawriter only
- db_datareader and db_datawriter
- db owner only

**Answer Area:**



**Answer area**

Account type:

- Azure Active Directory User
- [✓ Managed identity]
- Service Principal

Roles:

- db_datawriter only
- [✓ db_datareader and db_datawriter]
- db owner only

**Section:**

**Explanation:**
https://docs.microsoft.com/en-us/azure/app-service/tutorial-connect-msi-sql-database?tabs=windowsclient%2Cdotnet

**QUESTION 8**

HOTSPOT

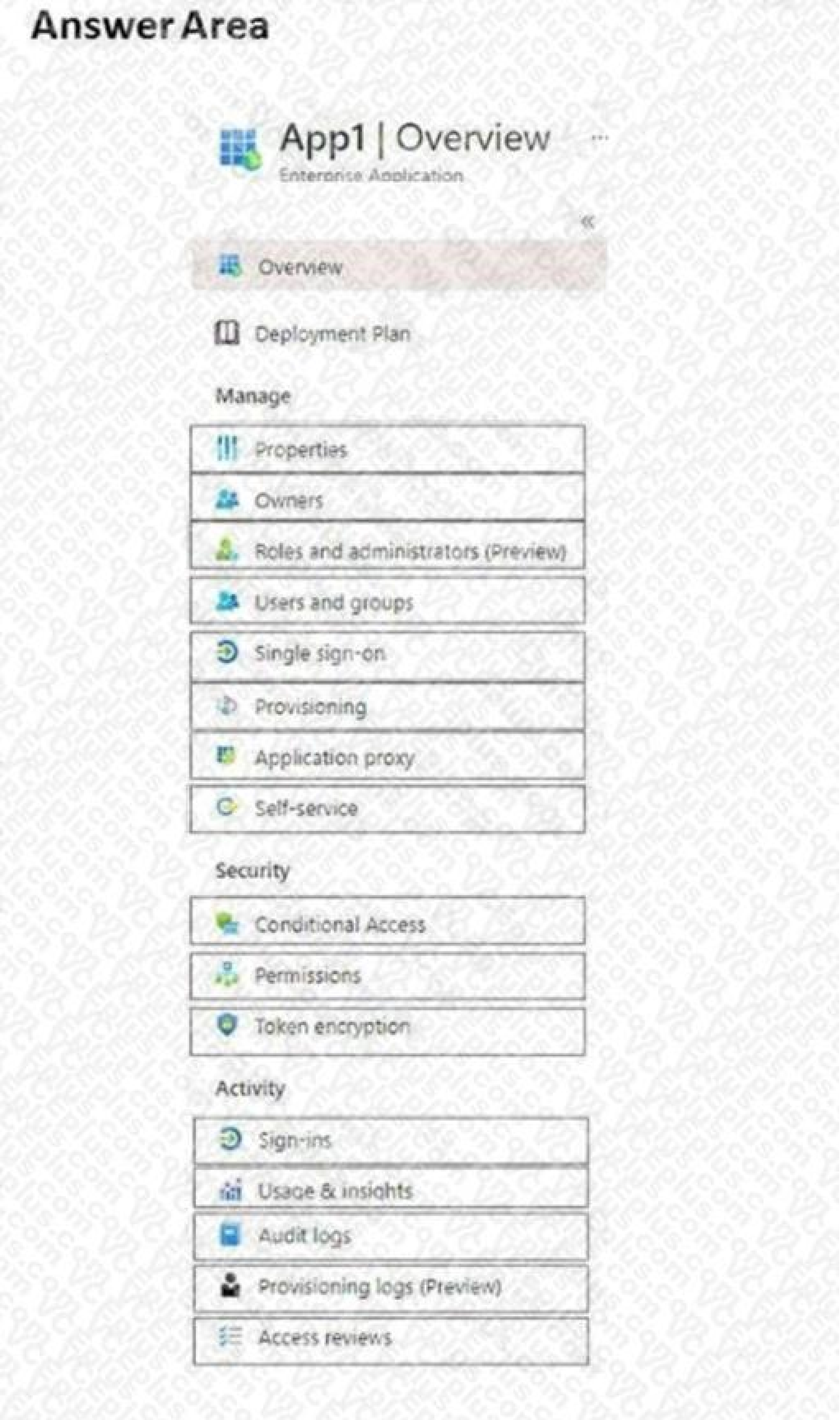
You have an Azure Active Directory (Azure AD) tenant that contains two users named User1 and User2 and a registered app named App1. You create an app-specific role named Role1.

You need to assign Role1 to User1 and enable User2 to request access to App1.

Which two settings should you modify? To answer, select the appropriate settings in the answer area. NOTE: Each correct selection is worth one point.

**Hot Area:**

Answer Area

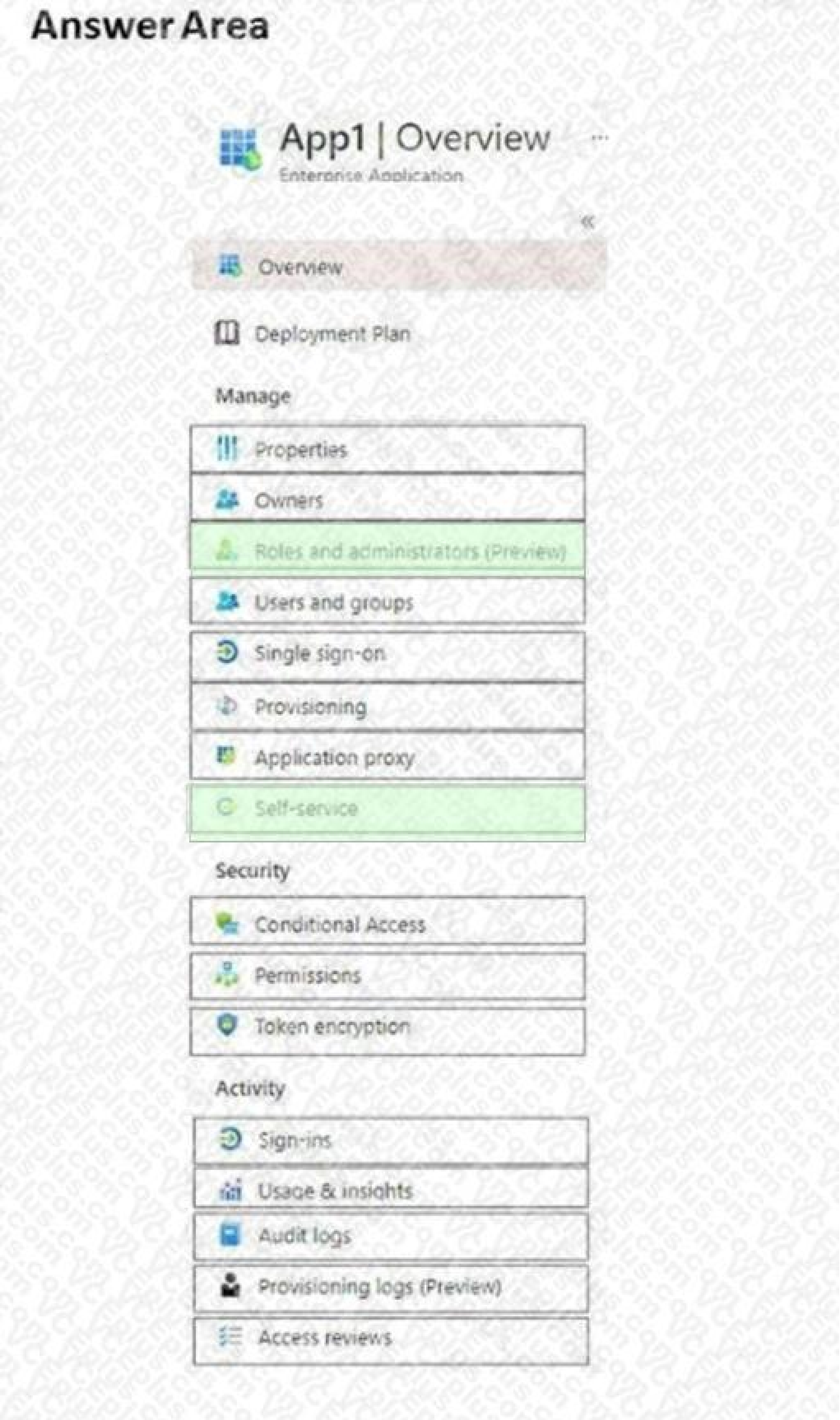


App1 | Overview

Enterprise Application

**Answer Area:**

Answer Area



App1 | Overview ...
Enterprise Application

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Preview)

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-ins

Usage & insights

Audit logs

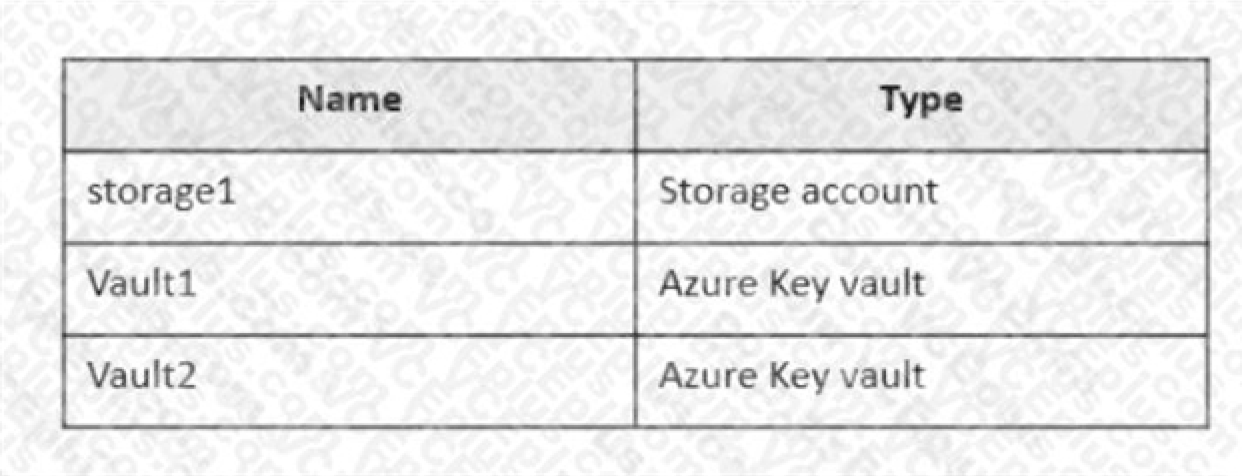
Provisioning logs (Preview)

Access reviews

**Section:**
**Explanation:**
Box 1: Roles and administrators
Here you will find Role1 and be able to assign User1 to the role.
Box 2: Self Service
Under Self Service, there is an option to "Allow users to request access to this application".

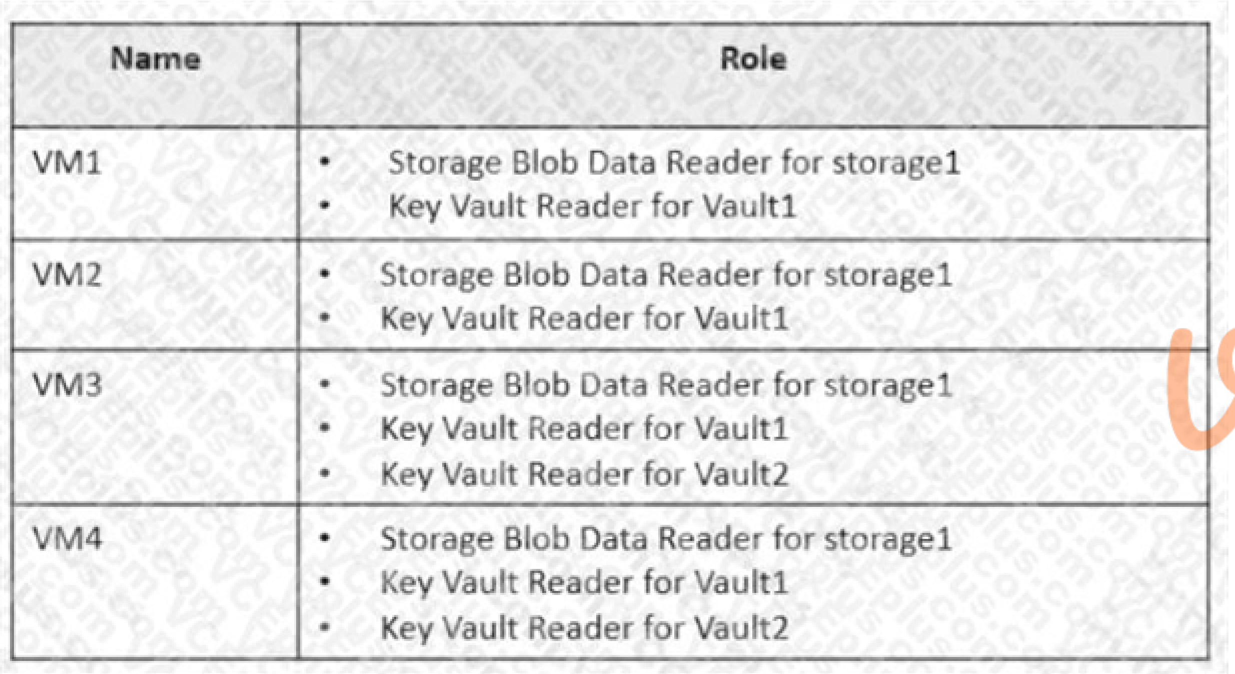
**QUESTION 9**

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



| Name | Type |
|---|---|
| storage1 | Storage account |
| Vault1 | Azure Key vault |
| Vault2 | Azure Key vault |

You plan to deploy the virtual machines shown in the following table.



| Name | Role |
|---|---|
| VM1 | • Storage Blob Data Reader for storage1<br>• Key Vault Reader for Vault1 |
| VM2 | • Storage Blob Data Reader for storage1<br>• Key Vault Reader for Vault1 |
| VM3 | • Storage Blob Data Reader for storage1<br>• Key Vault Reader for Vault1<br>• Key Vault Reader for Vault2 |
| VM4 | • Storage Blob Data Reader for storage1<br>• Key Vault Reader for Vault1<br>• Key Vault Reader for Vault2 |

You need to assign managed identities to the virtual machines. The solution must meet the following requirements:

Assign each virtual machine the required roles. Use the principle of least privilege.

What is the minimum number of managed identities required?

A. 1

B. 2

C. 3

D. 4

**Correct Answer: B**

**Section:**

**Explanation:**

We have two different sets of required permissions. VM1 and VM2 have the same permission requirements. VM3 and VM4 have the same permission requirements.

A user-assigned managed identity can be assigned to one or many resources. By using user-assigned managed identities, we can create just two managed identities: one with the permission requirements for VM1 and VM2 and the other with the permission requirements for VM3 and VM4.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

**QUESTION 10**

SIMULATION

You need to ensure that a user named user2-12345678 can manage the properties of the virtual machines in the RG1lod12345678 resource group. The solution must use the principle of least privilege.

To complete this task, sign in to the Azure portal.

A. Explanation

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

1. Sign in to the Azure portal.
2. Browse to Resource Groups.
3. Select the RG1lod12345678 resource group.
4. Select Access control (IAM).
5. Select Add > role assignment.
6. Select Virtual Machine Contributor (you can filter the list of available roles by typing 'virtual' in the search box) then click Next.
7. Select the +Select members option and select user2-12345678 then click the Select button.
8. Click the Review + assign button twice.

Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal?tabs=current

**QUESTION 11**

SIMULATION

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password. place your cursor in the Enter password box and click on the password below. Azure Username: Userl -28681041@ExamUsers.com

Azure Password: GpOAe4@lDg

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab. The following information is for technical support purposes only:

Lab Instance: 28681041

Task 10

You need to create a new Azure AD directory named 28681041.onmicrosoft.com. The new directory must contain a new user named user1@28681041.onmicrosoft.com.

A. Explanation

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

The first step is to create the Azure Active Directory tenant.

To create a new Azure AD directory named 28681041.onmicrosoft.com that contains a new user named user1@28681041.onmicrosoft.com, you can follow these steps:

In the Azure portal, search for and select Azure Active Directory.

In the left pane, select Domains.

Select Add domain.

In the Add a custom domain pane, enter the following information:

Domain name: Enter the domain name you want to use. For example, 28681041.onmicrosoft.com.

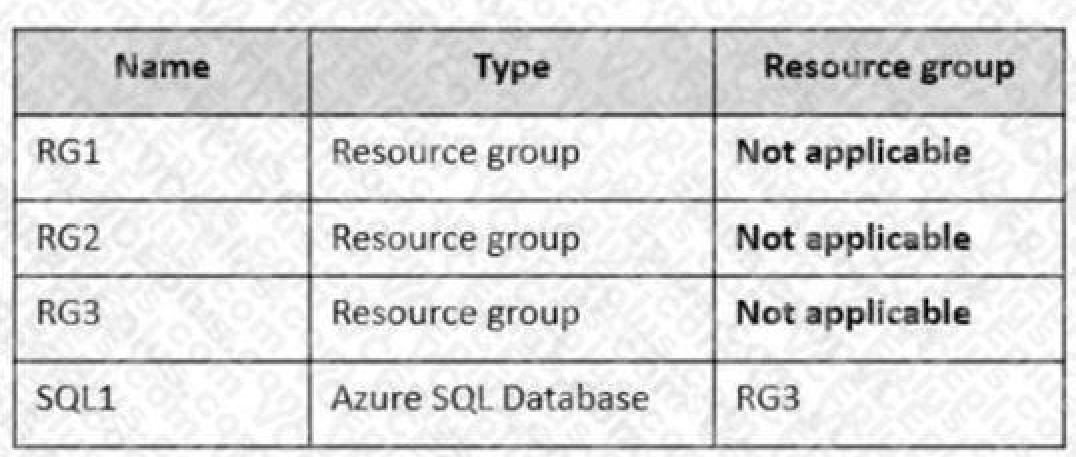
Add domain: Select Add domain.

In the left pane, select Users.
Select New user.
In the New user pane, enter the following information:
User name: Enter the user name you want to use. For example, user1@28681041.onmicrosoft.com.
Name: Enter the name of the user.
Password: Enter a password for the user.
Groups: Select the groups you want the user to be a member of.
Select Create.
You can find more information on these topics in the following Microsoft documentation:
Add a custom domain name to Azure Active Directory
Create a new user in your organization - Azure Active Directory
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory

**QUESTION 12**

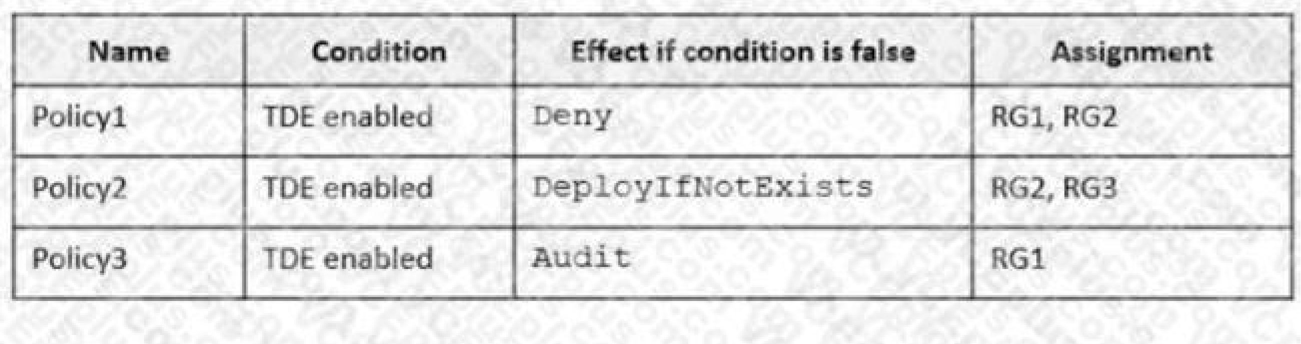
HOTSPOT

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



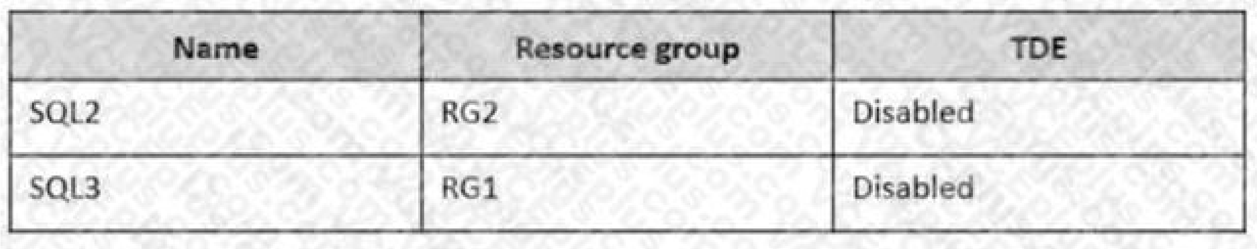
| Name | Type | Resource group |
|---|---|---|
| RG1 | Resource group | **Not applicable** |
| RG2 | Resource group | **Not applicable** |
| RG3 | Resource group | **Not applicable** |
| SQL1 | Azure SQL Database | RG3 |

Transparent Data Encryption (TDE) is disabled on SQL1.
You assign policies to the resource groups as shown in the following table.



| Name | Condition | Effect if condition is false | Assignment |
|---|---|---|---|
| Policy1 | TDE enabled | `Deny` | RG1, RG2 |
| Policy2 | TDE enabled | `DeployIfNotExists` | RG2, RG3 |
| Policy3 | TDE enabled | `Audit` | RG1 |

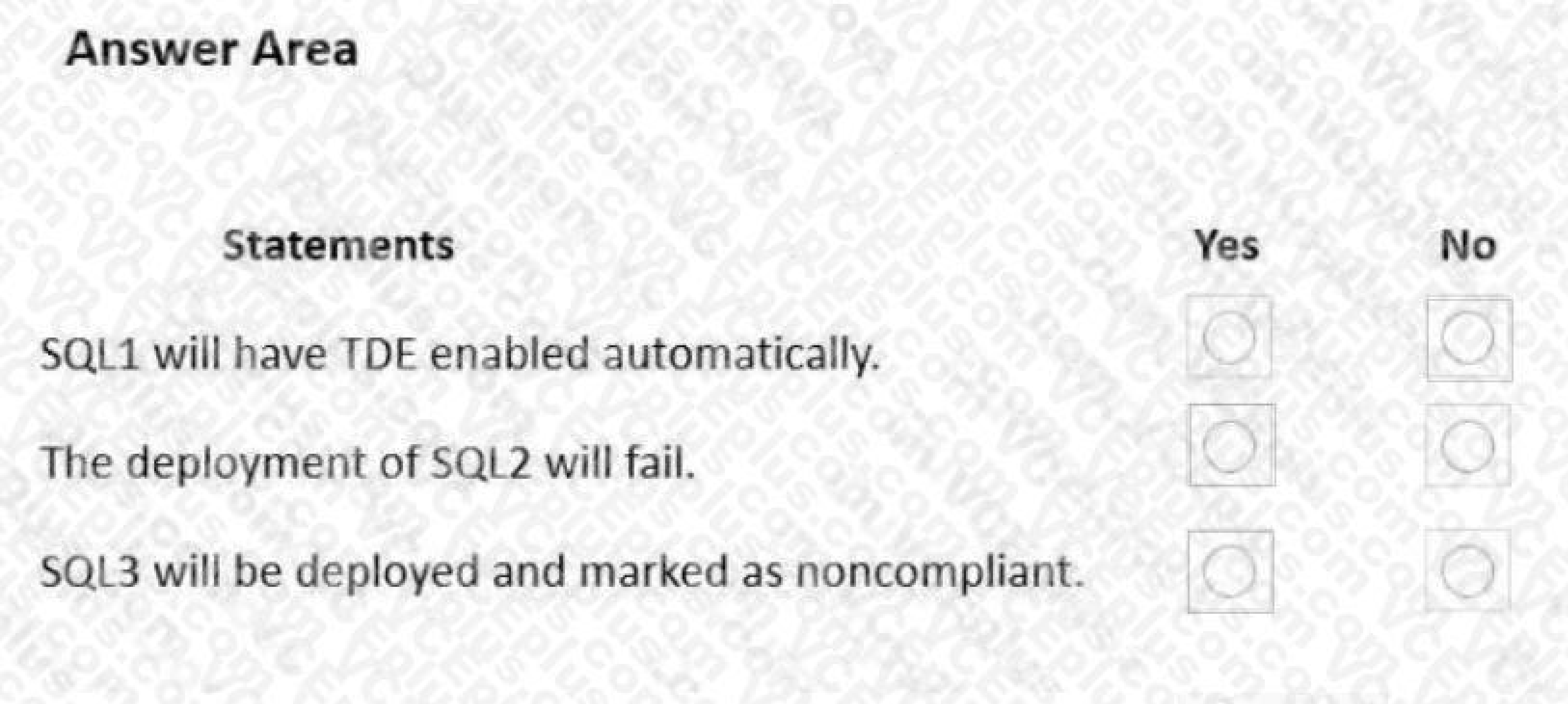
You plan to deploy Azure SQL databases by using an Azure Resource Manager (ARM) template. The databases will be configured as shown in the following table.



| Name | Resource group | TDE |
|---|---|---|
| SQL2 | RG2 | Disabled |
| SQL3 | RG1 | Disabled |

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

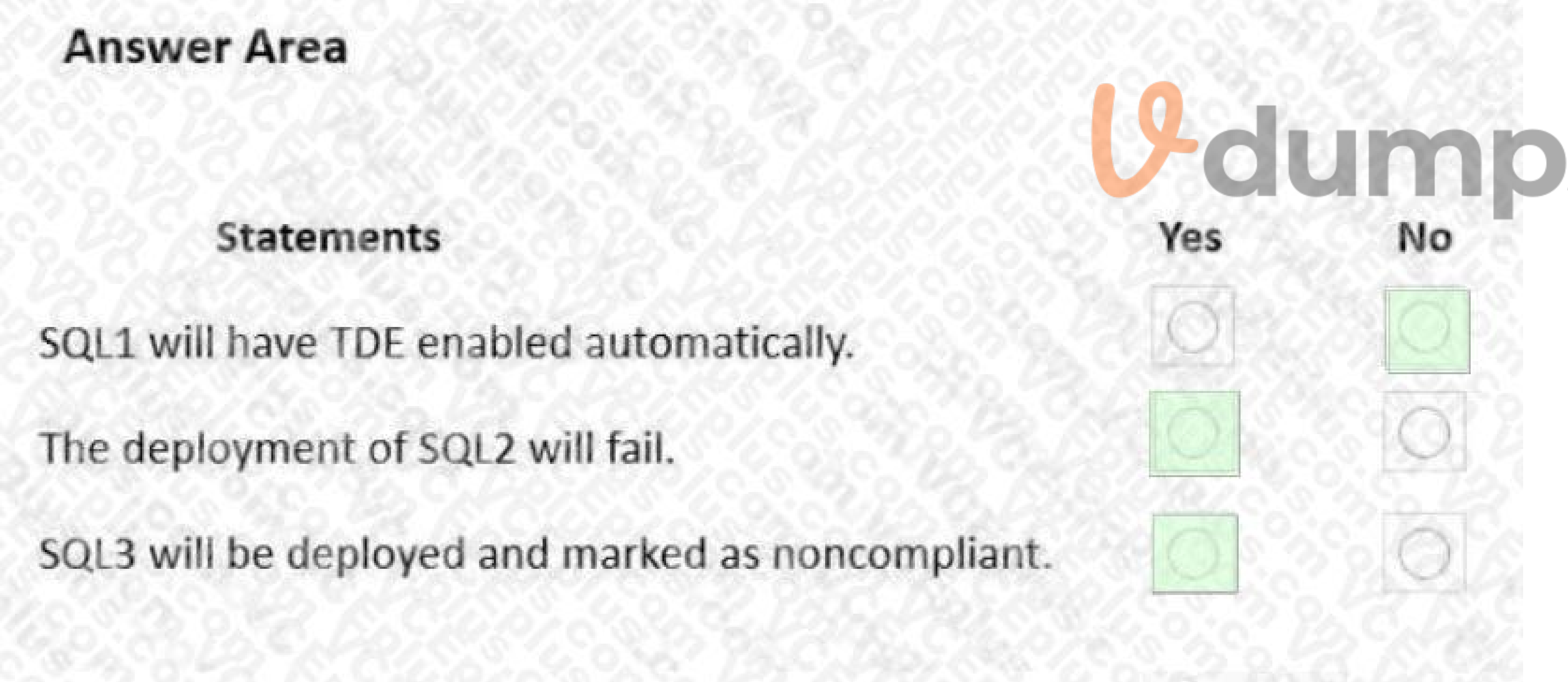
**Hot Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| SQL1 will have TDE enabled automatically. | ○ | ○ |
| The deployment of SQL2 will fail. | ○ | ○ |
| SQL3 will be deployed and marked as noncompliant. | ○ | ○ |

**Answer Area:**

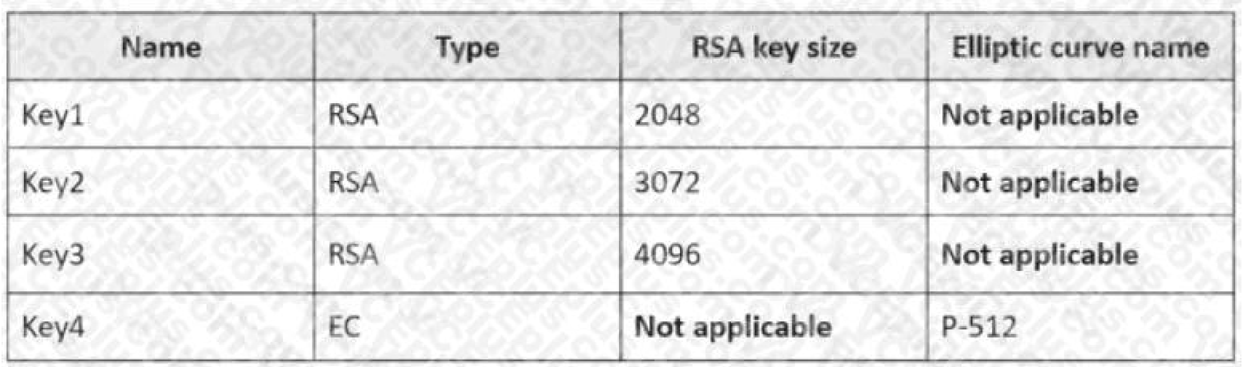


Answer Area

| Statements | Yes | No |
|---|---|---|
| SQL1 will have TDE enabled automatically. | ○ | ● |
| The deployment of SQL2 will fail. | ● | ○ |
| SQL3 will be deployed and marked as noncompliant. | ● | ○ |

**Section:**
**Explanation:**
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

**QUESTION 13**
You have an Azure subscription that contains an Azure SQL database named SQL1 and an Azure key vault namedKeyVault1. KeyVault1 stores the keys shown in the following table. You need to configure Transparent Data Encryption (TDE). TDE will use a customer-managed key for SQL1.



| Name | Type | RSA key size | Elliptic curve name |
|---|---|---|---|
| Key1 | RSA | 2048 | Not applicable |
| Key2 | RSA | 3072 | Not applicable |
| Key3 | RSA | 4096 | Not applicable |
| Key4 | EC | Not applicable | P-512 |

Which keys can you use?

A. Key2 only
B. Key1 only
C. Key2 and Key3 only
D. Key1, Key2, Key3, and Key4
E. Key1 and Key2 only

**Correct Answer: E**
**Section:**
**Explanation:**
The key must be an asymmetric, RSA or RSA HSM key. The supported key lengths are 2048-bit and 3072-bit.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-overview

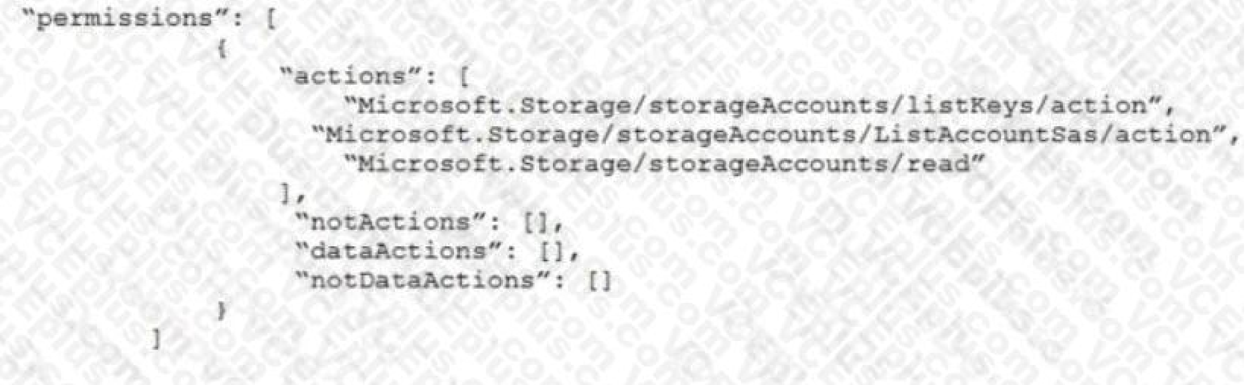
**QUESTION 14**
SIMULATION
You need to create a web app named Intranet12345678 and enable users to authenticate to the web app by using Azure Active Directory (Azure AD). To complete this task, sign in to the Azure portal.

A. Explanation

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
1. In the Azure portal, type App services in the search box and select App services from the search results. 2. Click the Create app service button to create a new app service.
3. In the Resource Group section, click the Create new link to create a new resource group.
4. Give the resource group a name such as Intranet12345678RG and click OK.
5. In the Instance Details section, enter Intranet12345678 in the Name field.
6. In the Runtime stack field, select any runtime stack such as .NET Core 3.1.
7. Click the Review + create button.
8. Click the Create button to create the web app.
9. Click the Go to resource button to open the properties of the new web app.
10.In the Settings section, click on Authentication / Authorization.
11.Click the App Service Authentication slider to set it to On.
12.In the Action to take when request is not authentication box, select Log in with Azure Active Directory. 13.Click Save to save the changes.

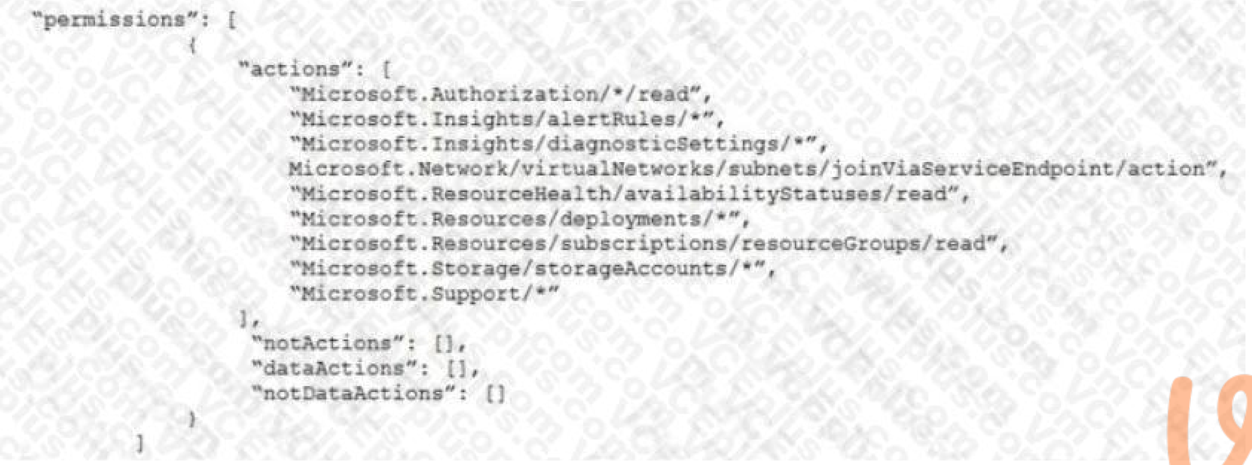
**QUESTION 15**
HOTSPOT

You have an Azure subscription that contains a resource group named RG1. RG1 contains a storage account named storage1.
You have two custom Azure roles named Role1 and Role2 that are scoped to RG1.
The permissions for Role1 are shown in the following JSON code.



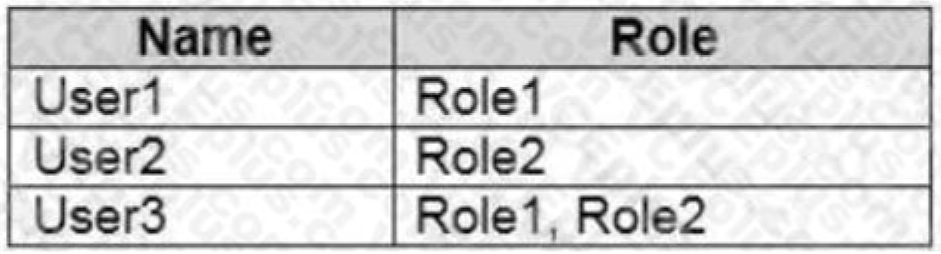
```
"permissions": [
            {
                "actions": [
                    "Microsoft.Storage/storageAccounts/listKeys/action",
                  "Microsoft.Storage/storageAccounts/ListAccountSas/action",
                    "Microsoft.Storage/storageAccounts/read"
                ],
                 "notActions": [],
                 "dataActions": [],
                 "notDataActions": []
            }
        ]
```

The permissions for Role2 are shown in the following JSON code.



```
"permissions": [
            {
                "actions": [
                    "Microsoft.Authorization/*/read",
                    "Microsoft.Insights/alertRules/*",
                    "Microsoft.Insights/diagnosticSettings/*",
                    Microsoft.Network/virtualNetworks/subnets/joinViaServiceEndpoint/action",
                    "Microsoft.ResourceHealth/availabilityStatuses/read",
                    "Microsoft.Resources/deployments/*",
                    "Microsoft.Resources/subscriptions/resourceGroups/read",
                    "Microsoft.Storage/storageAccounts/*",
                    "Microsoft.Support/*"
                ],
                 "notActions": [],
                 "dataActions": [],
                 "notDataActions": []
            }
        ]
```

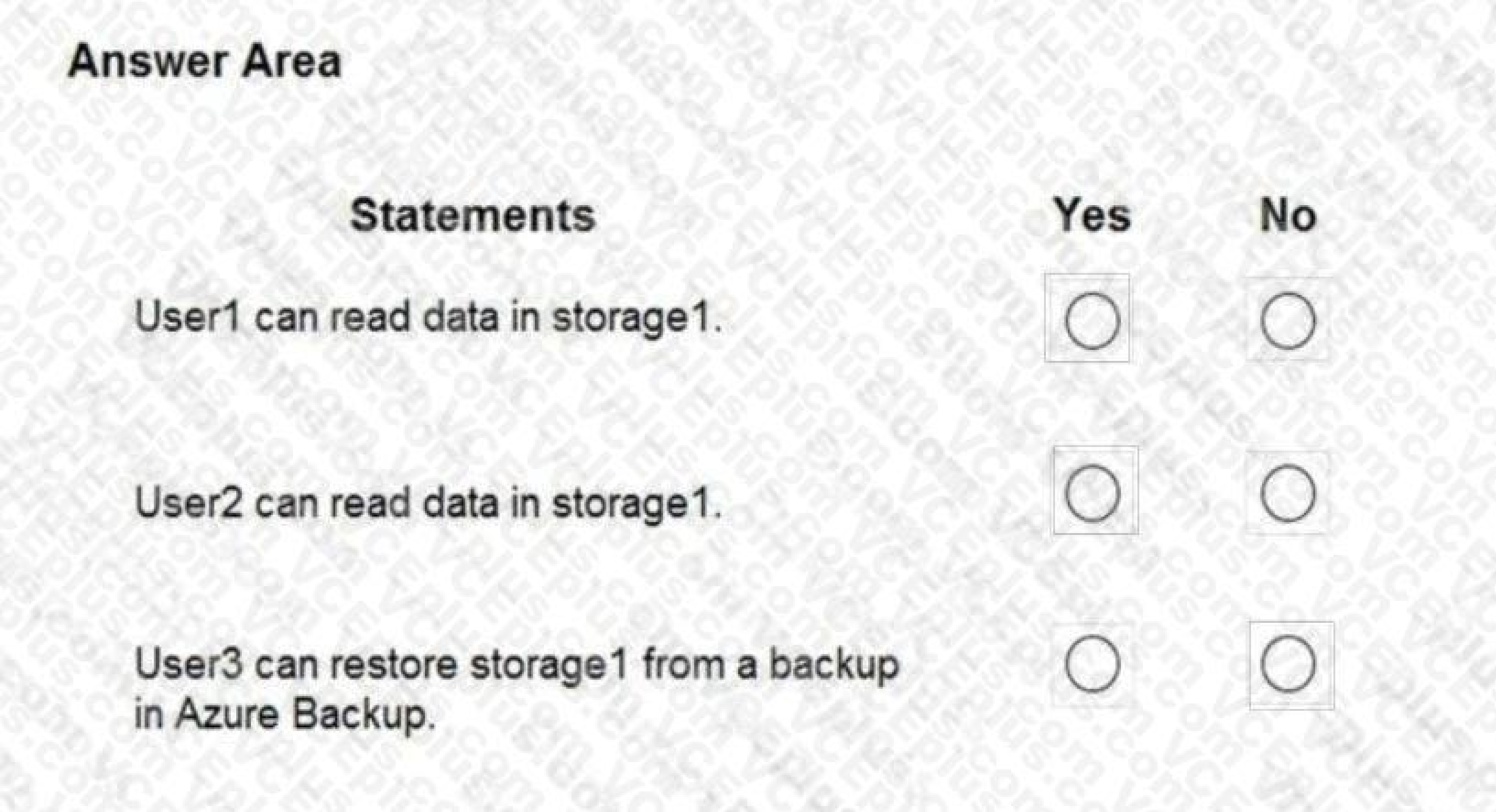
You assign the roles to the users shown in the following table.



| Name | Role |
|---|---|
| User1 | Role1 |
| User2 | Role2 |
| User3 | Role1, Role2 |

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

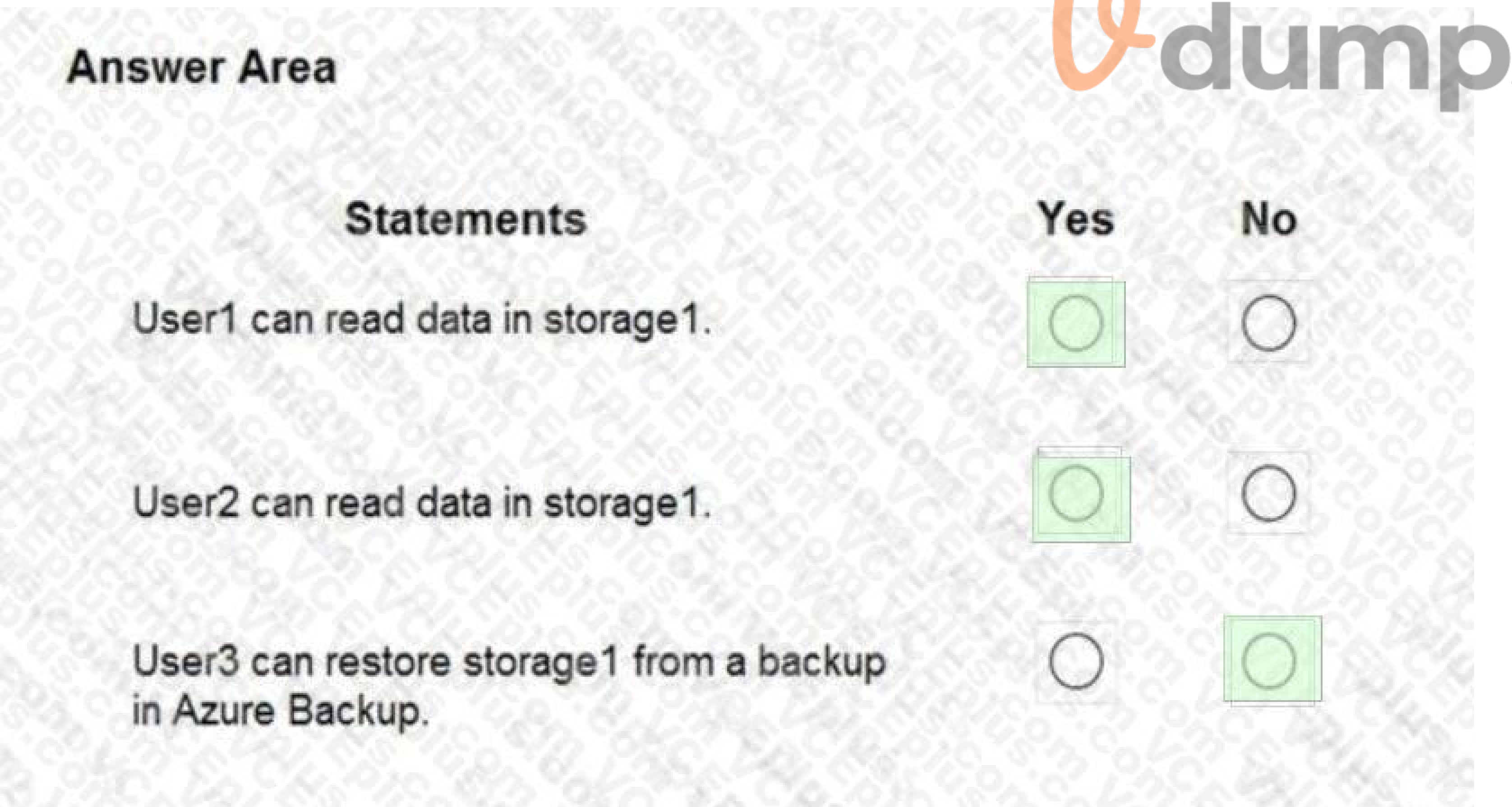
**Hot Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| User1 can read data in storage1. | ○ | ○ |
| User2 can read data in storage1. | ○ | ○ |
| User3 can restore storage1 from a backup in Azure Backup. | ○ | ○ |

**Answer Area:**



Answer Area

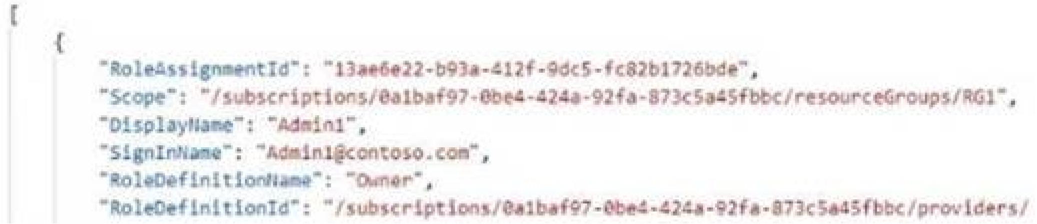
| Statements | Yes | No |
|---|---|---|
| User1 can read data in storage1. | [✓ ○] | ○ |
| User2 can read data in storage1. | [✓ ○] | ○ |
| User3 can restore storage1 from a backup in Azure Backup. | ○ | [✓ ○] |

**Section:**
**Explanation:**
Reference: https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

**QUESTION 16**

HOTSPOT

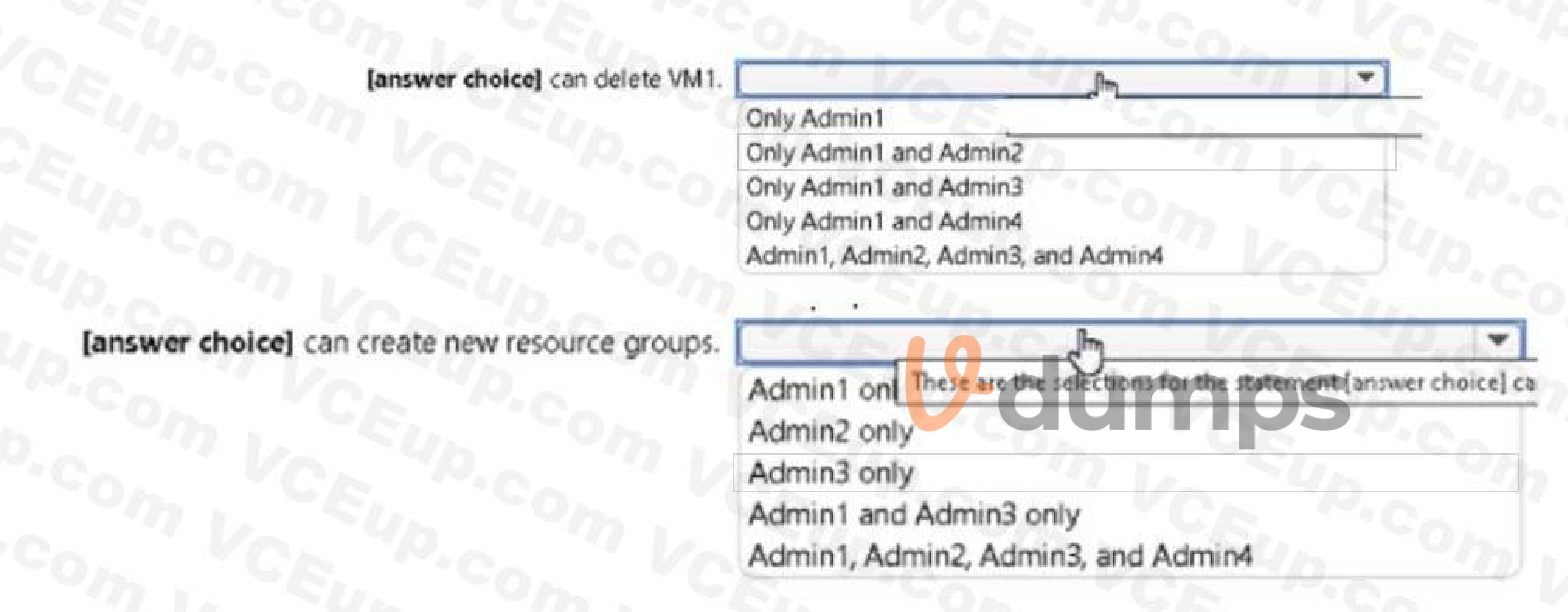
You have the role assignments shown in the following exhibit.



```
[
    {
        "RoleAssignmentId": "13ae6e22-b93a-412f-9dc5-fc82b1726bde",
        "Scope": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/resourceGroups/RG1",
        "DisplayName": "Admin1",
        "SignInName": "Admin1@contoso.com",
        "RoleDefinitionName": "Owner",
        "RoleDefinitionId": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/providers/
```

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.

**Hot Area:**



**[answer choice]** can delete VM1.

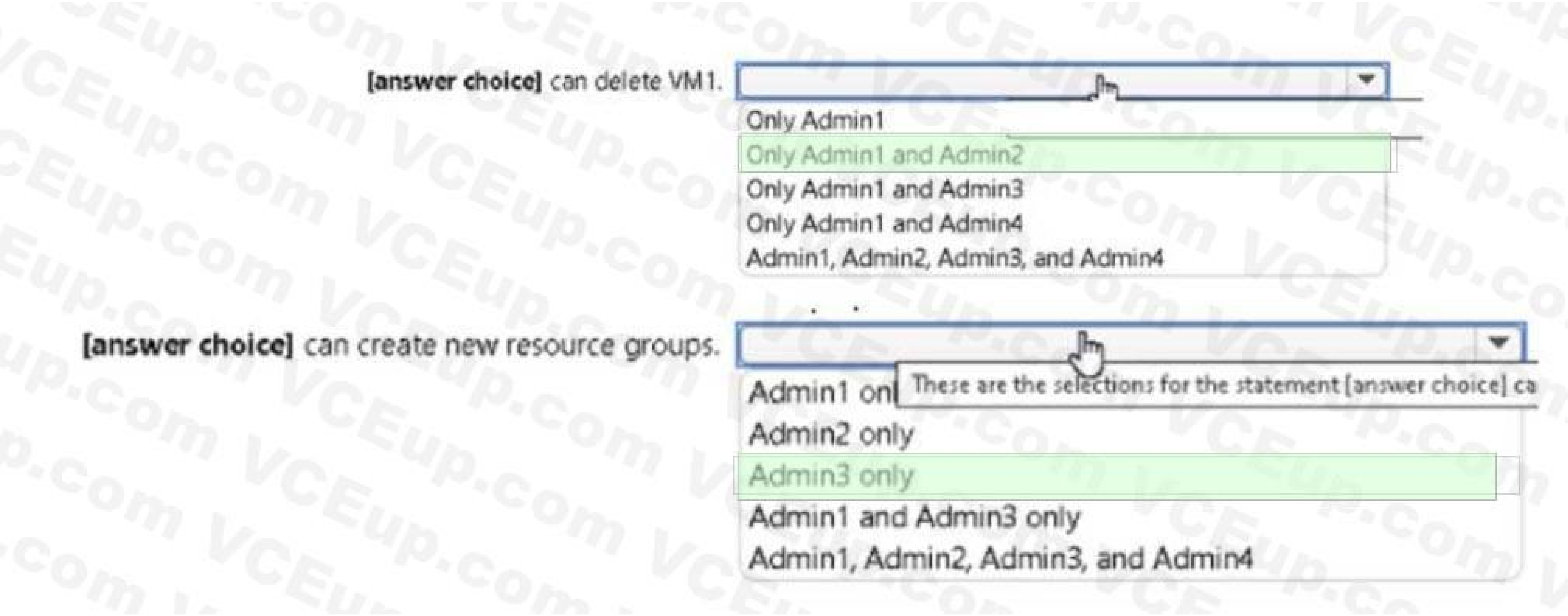
- Only Admin1
- Only Admin1 and Admin2
- Only Admin1 and Admin3
- Only Admin1 and Admin4
- Admin1, Admin2, Admin3, and Admin4

**[answer choice]** can create new resource groups.

- Admin1 onl
- Admin2 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

These are the selections for the statement [answer choice] ca

**Answer Area:**



[answer choice] can delete VM1.

- Only Admin1
- [✓ Only Admin1 and Admin2]
- Only Admin1 and Admin3
- Only Admin1 and Admin4
- Admin1, Admin2, Admin3, and Admin4

[answer choice] can create new resource groups.

These are the selections for the statement [answer choice] ca

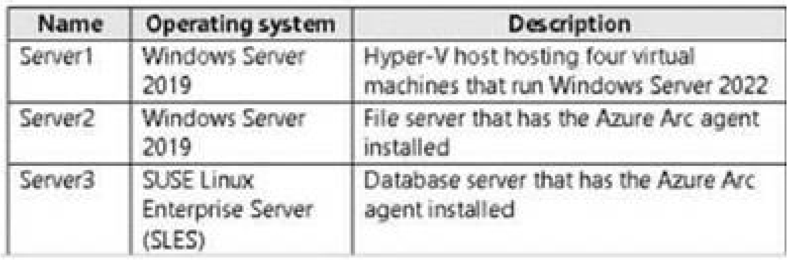
- Admin1 onl
- Admin2 only
- [✓ Admin3 only]
- Admin1 and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

**Section:**
**Explanation:**

**QUESTION 17**

HOTSPOT

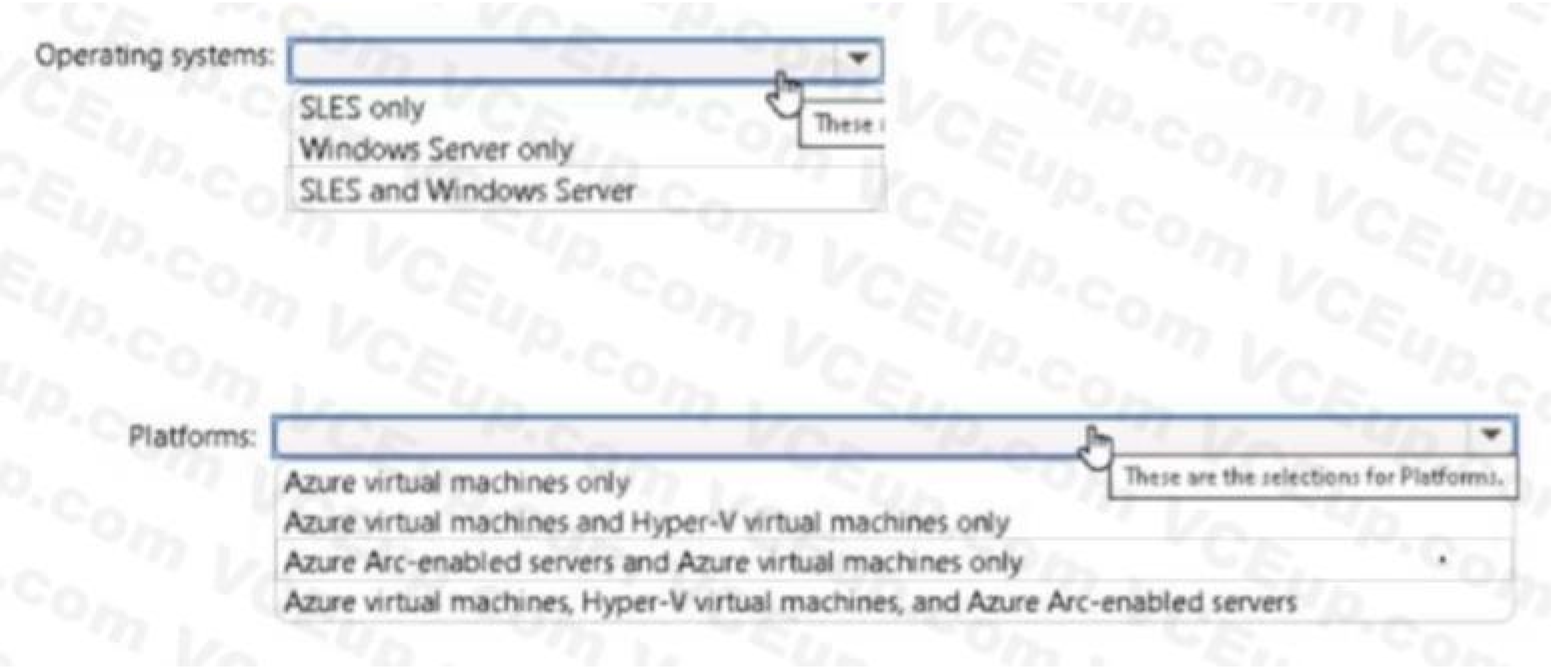
Your on-premises network contains the servers shown in the following table.



| Name | Operating system | Description |
|---|---|---|
| Server1 | Windows Server 2019 | Hyper-V host hosting four virtual machines that run Windows Server 2022 |
| Server2 | Windows Server 2019 | File server that has the Azure Arc agent installed |
| Server3 | SUSE Linux Enterprise Server (SLES) | Database server that has the Azure Arc agent installed |

You have an Azure subscription that contains multiple virtual machines that run either Windows Server 2019 or SLES. You plan to implement adaptive application controls in Microsoft Defender for Cloud. Which operating systems and platforms can you monitor? To answer, select the appropriate
options in the answer area.

**Hot Area:**



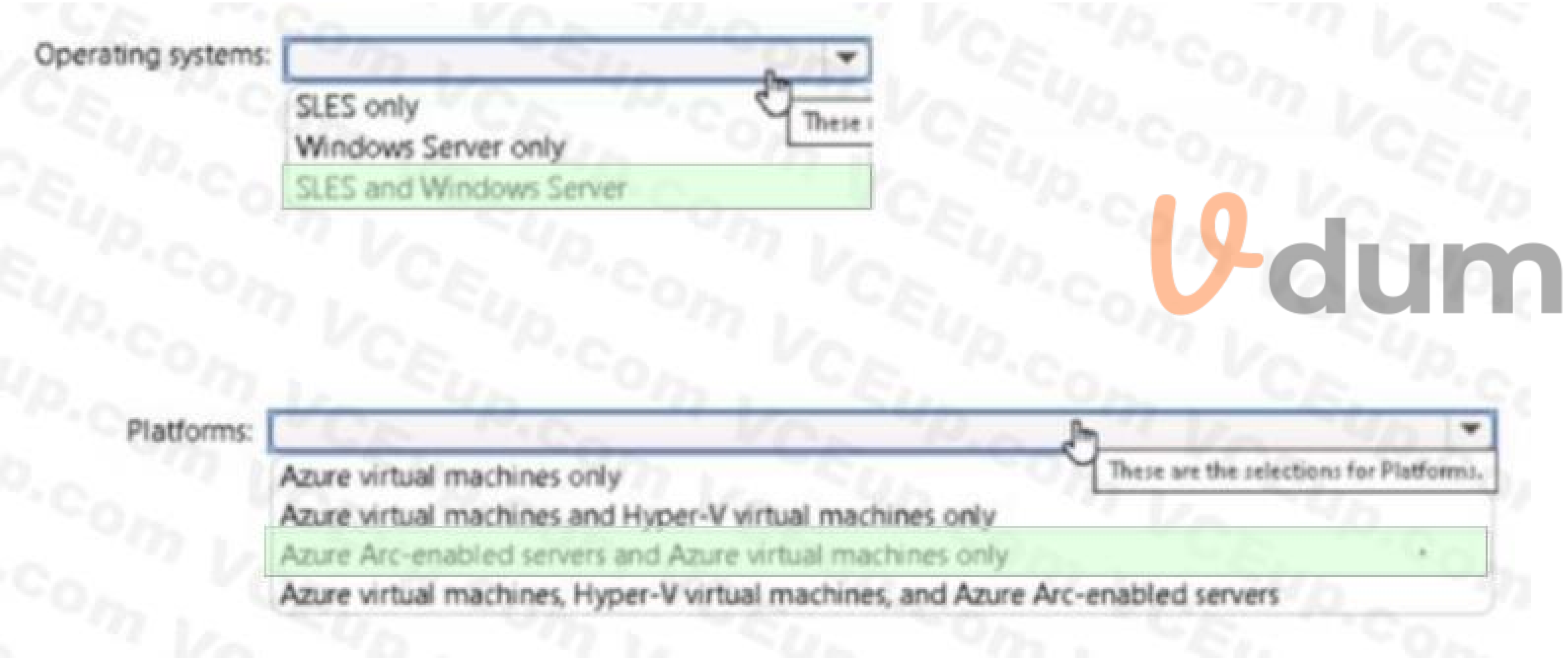
Operating systems:

- SLES only
- Windows Server only
- SLES and Windows Server

Platforms:

- Azure virtual machines only
- Azure virtual machines and Hyper-V virtual machines only
- Azure Arc-enabled servers and Azure virtual machines only
- Azure virtual machines, Hyper-V virtual machines, and Azure Arc-enabled servers

**Answer Area:**



Operating systems:

- SLES only
- Windows Server only
- [✓ SLES and Windows Server]

Platforms:

- Azure virtual machines only
- Azure virtual machines and Hyper-V virtual machines only
- [✓ Azure Arc-enabled servers and Azure virtual machines only]
- Azure virtual machines, Hyper-V virtual machines, and Azure Arc-enabled servers

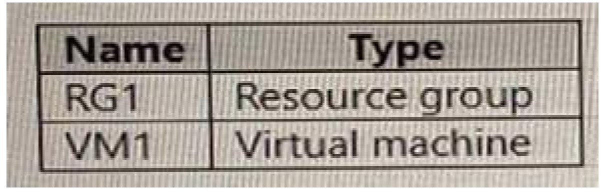
**Section:**

**Explanation:**

**QUESTION 18**

HOTSPOT

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



| Name | Type |
|---|---|
| RG1 | Resource group |
| VM1 | Virtual machine |

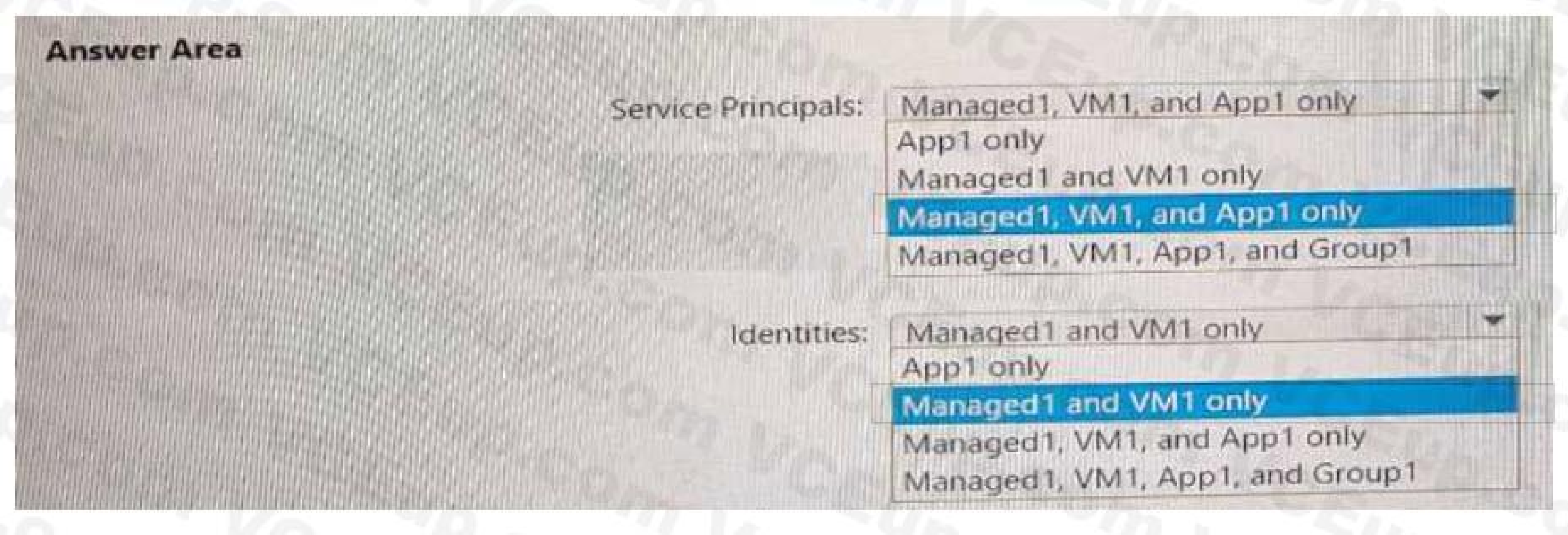
You perform the following tasks:

Create a managed identity named Managed1.

Create a Microsoft 365 group named Group1.

You need to identify which service principals were created and which identities can be assigned the Reader role for RG1. What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Hot Area:**



Answer Area

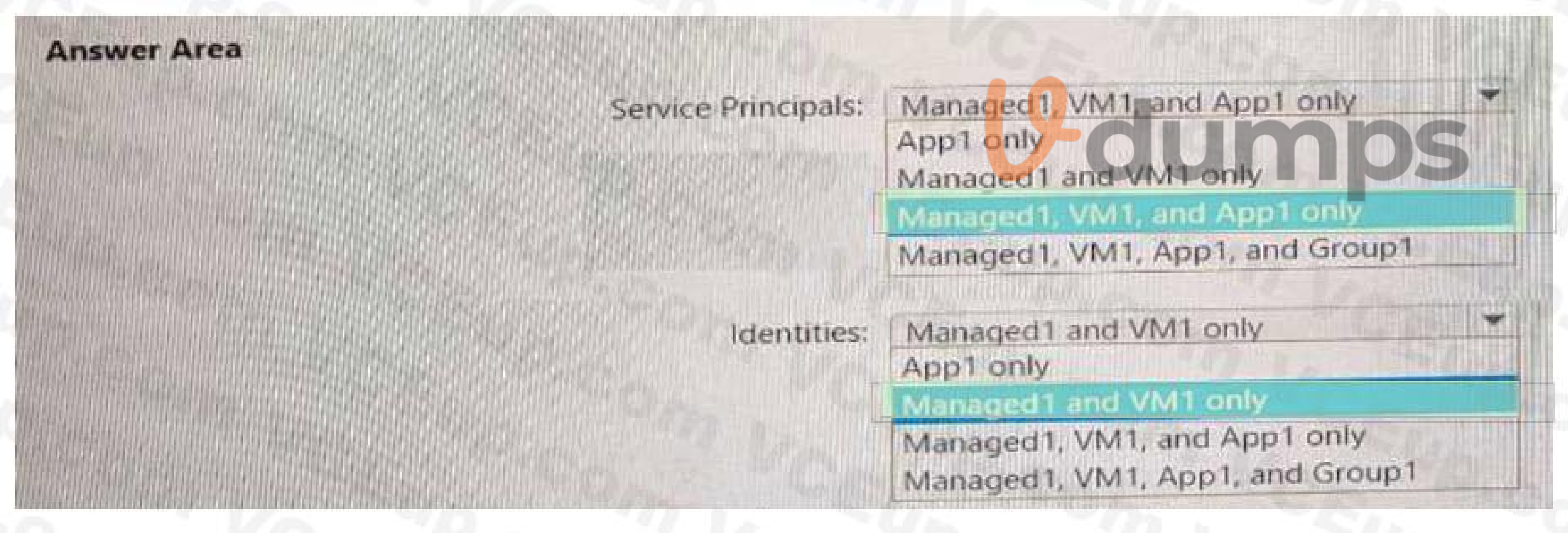
Service Principals: Managed1, VM1, and App1 only

- App1 only
- Managed1 and VM1 only
- [✓ Managed1, VM1, and App1 only]
- Managed1, VM1, App1, and Group1

Identities: Managed1 and VM1 only

- App1 only
- [✓ Managed1 and VM1 only]
- Managed1, VM1, and App1 only
- Managed1, VM1, App1, and Group1

**Answer Area:**



Answer Area

Service Principals: Managed1, VM1, and App1 only

- App1 only
- Managed1 and VM1 only
- [✓ Managed1, VM1, and App1 only]
- Managed1, VM1, App1, and Group1

Identities: Managed1 and VM1 only

- App1 only
- [✓ Managed1 and VM1 only]
- Managed1, VM1, and App1 only
- Managed1, VM1, App1, and Group1

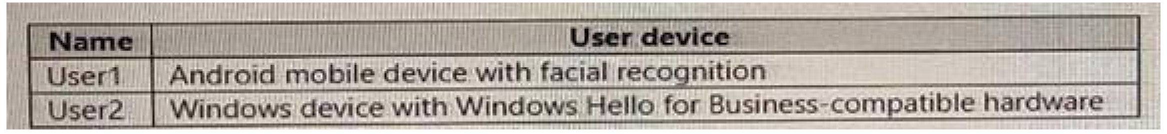
**Section:**

**Explanation:**

**QUESTION 19**

DRAG DROP

You have an Azure AD tenant that contains the users shown in the following table.



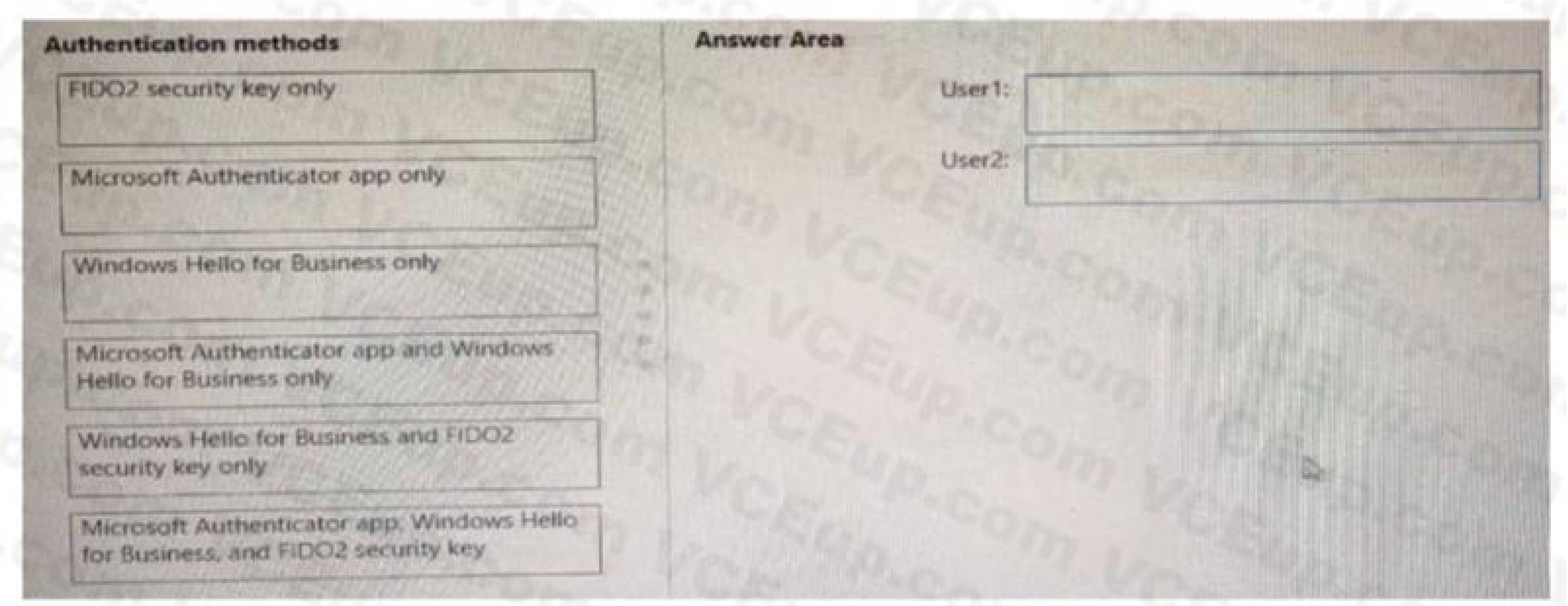
| Name | User device |
|---|---|
| User1 | Android mobile device with facial recognition |
| User2 | Windows device with Windows Hello for Business-compatible hardware |

You enable passwordless authentication for the tenant.

Which authentication method can each user use for passwordless authentication? To answer, drag the appropriate authentication methods to the correct users. Each authentication 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.

**Select and Place:**



**Authentication methods**

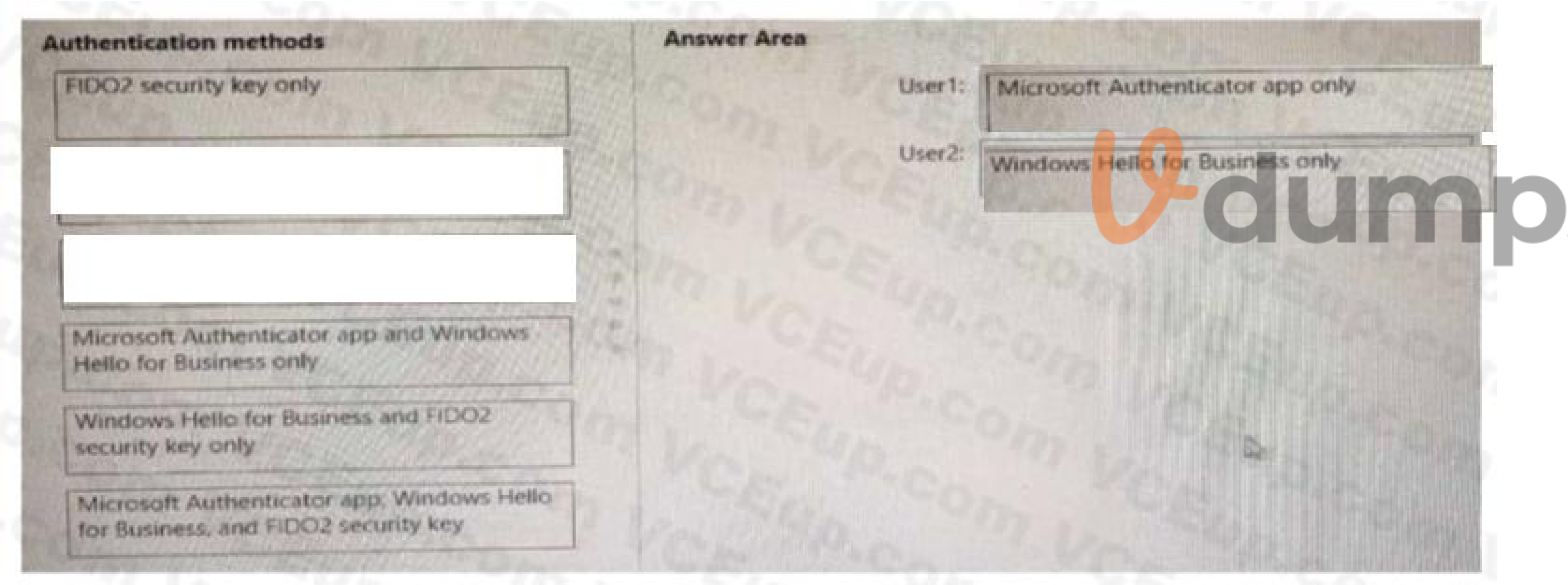
- FIDO2 security key only
- Microsoft Authenticator app only
- Windows Hello for Business only
- Microsoft Authenticator app and Windows Hello for Business only
- Windows Hello for Business and FIDO2 security key only
- Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key

**Answer Area**

User1:

User2:

**Correct Answer:**



**Authentication methods**

- FIDO2 security key only
- Microsoft Authenticator app and Windows Hello for Business only
- Windows Hello for Business and FIDO2 security key only
- Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key

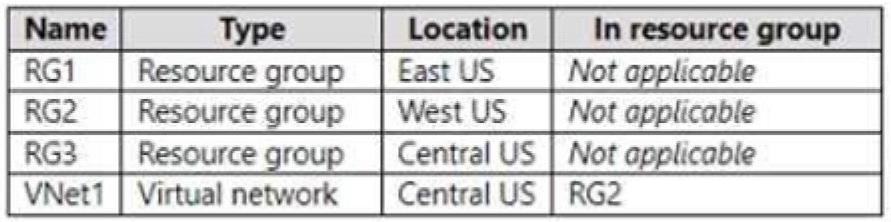
**Answer Area**

User1: Microsoft Authenticator app only

User2: Windows Hello for Business only

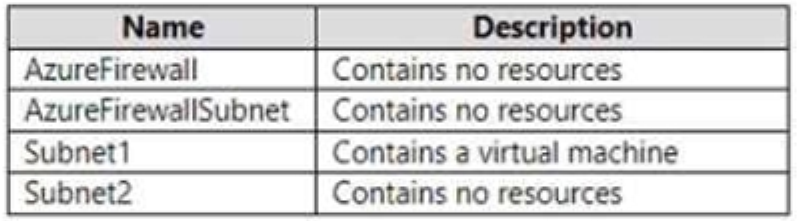
**Section:**
**Explanation:**

**QUESTION 20**
HOTSPOT
You have an Azure subscription that contains the resources shown in the following table.



| Name | Type | Location | In resource group |
|---|---|---|---|
| RG1 | Resource group | East US | *Not applicable* |
| RG2 | Resource group | West US | *Not applicable* |
| RG3 | Resource group | Central US | *Not applicable* |
| VNet1 | Virtual network | Central US | RG2 |

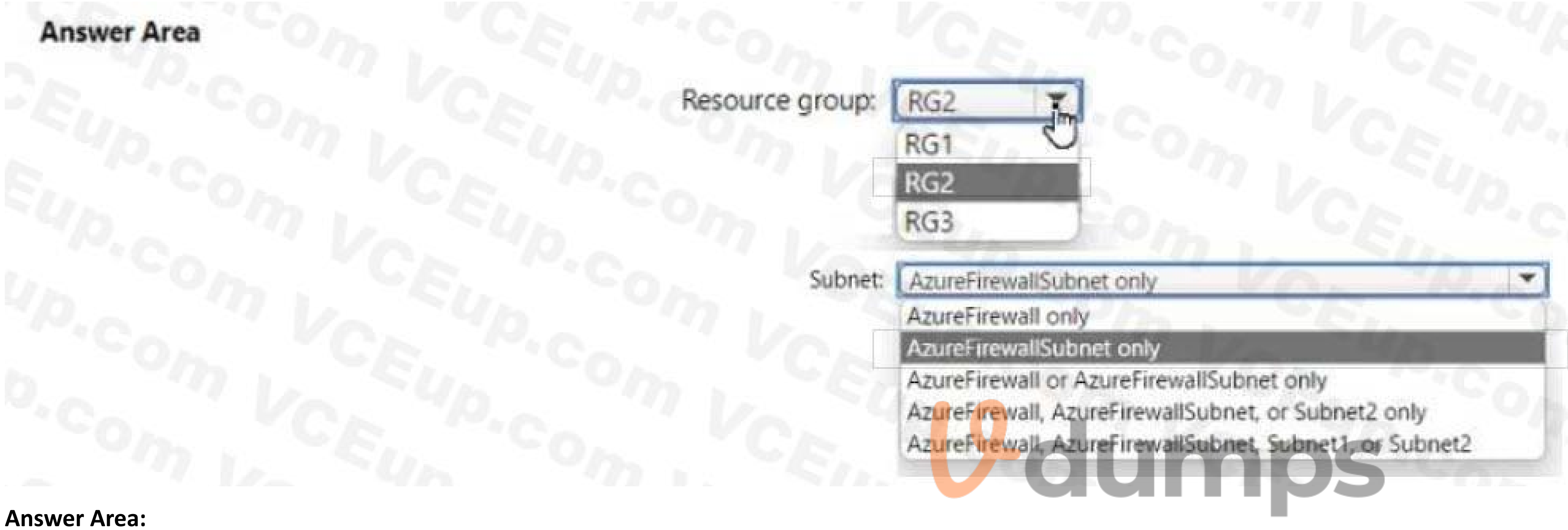
VNet1 contains the subnets shown in the following table.



| Name | Description |
|---|---|
| AzureFirewall | Contains no resources |
| AzureFirewallSubnet | Contains no resources |
| Subnet1 | Contains a virtual machine |
| Subnet2 | Contains no resources |

You plan to use the Azure portal to deploy an Azure firewall named AzFW1 to VNet1.
Which resource group and subnet can you use to deploy AzFW1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Hot Area:**



Answer Area

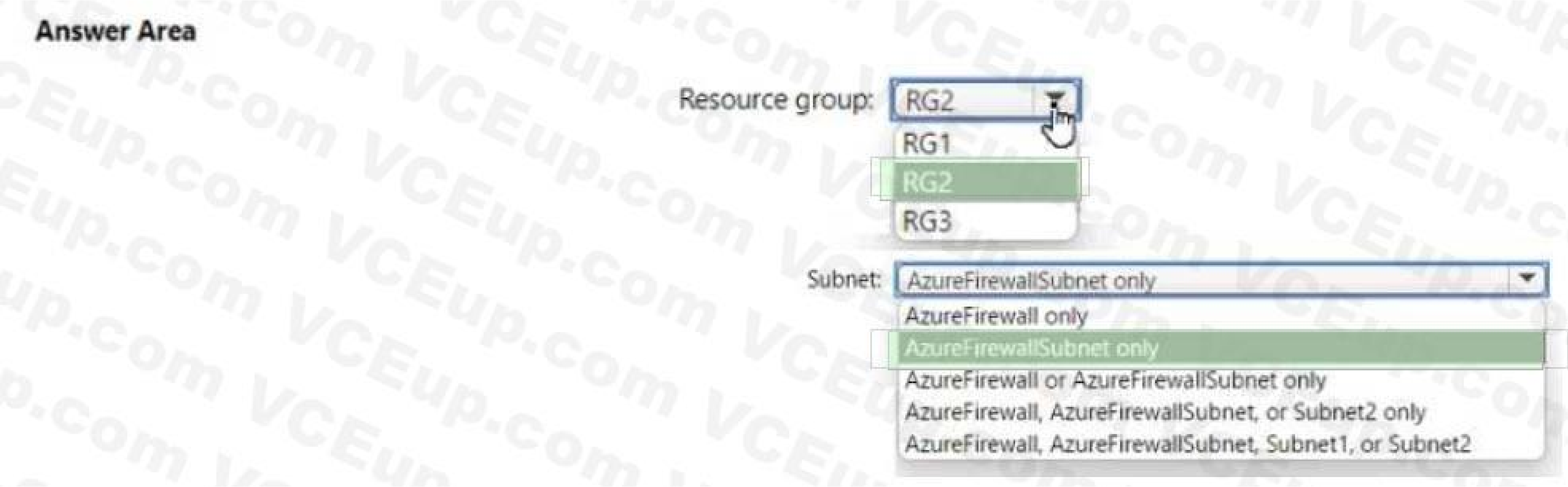
Resource group: RG2

- RG1
- RG2
- RG3

Subnet: AzureFirewallSubnet only

- AzureFirewall only
- AzureFirewallSubnet only
- AzureFirewall or AzureFirewallSubnet only
- AzureFirewall, AzureFirewallSubnet, or Subnet2 only
- AzureFirewall, AzureFirewallSubnet, Subnet1, or Subnet2

**Answer Area:**



Answer Area

Resource group: RG2

- RG1
- [✓ RG2]
- RG3

Subnet: AzureFirewallSubnet only

- AzureFirewall only
- [✓ AzureFirewallSubnet only]
- AzureFirewall or AzureFirewallSubnet only
- AzureFirewall, AzureFirewallSubnet, or Subnet2 only
- AzureFirewall, AzureFirewallSubnet, Subnet1, or Subnet2

**Section:**
**Explanation:**

**QUESTION 21**
DRAG DROP
You have an Azure subscription that contains an Azure web app named Appl.

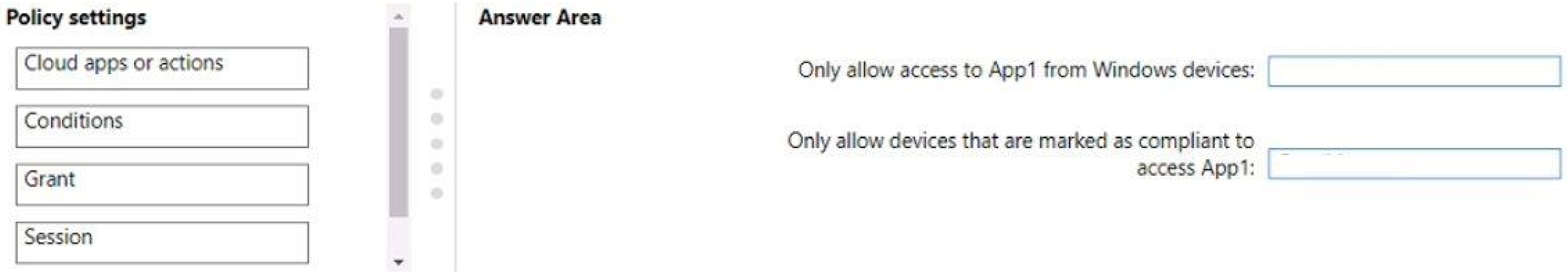
You plan to configure a Conditional Access policy for App1. The solution must meet the following requirements:

- Only allow access to App1 from Windows devices.
- Only allow devices that are marked as compliant to access App1.

Which Conditional Access policy settings should you configure? To answer, drag the appropriate settings to the correct requirements. 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.

**Select and Place:**



**Policy settings**

Cloud apps or actions

Conditions

Grant

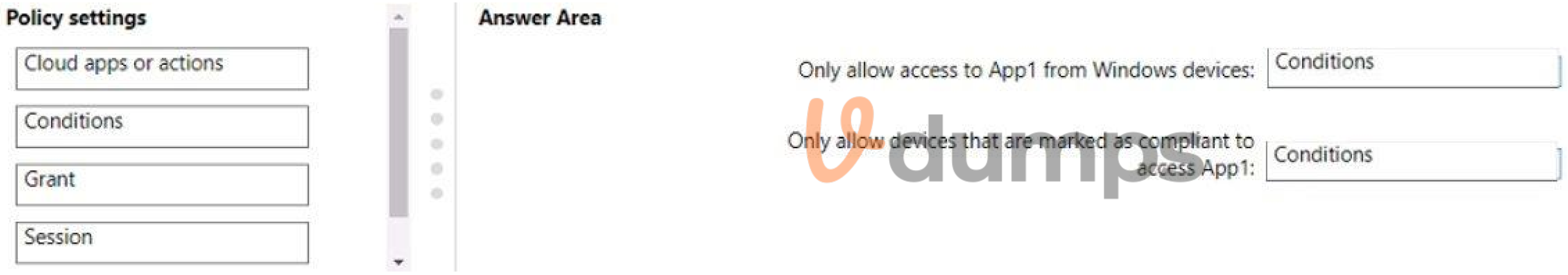
Session

**Answer Area**

Only allow access to App1 from Windows devices:

Only allow devices that are marked as compliant to access App1:

**Correct Answer:**



**Policy settings**

Cloud apps or actions

Conditions

Grant

Session

**Answer Area**

Only allow access to App1 from Windows devices: Conditions

Only allow devices that are marked as compliant to access App1: Conditions

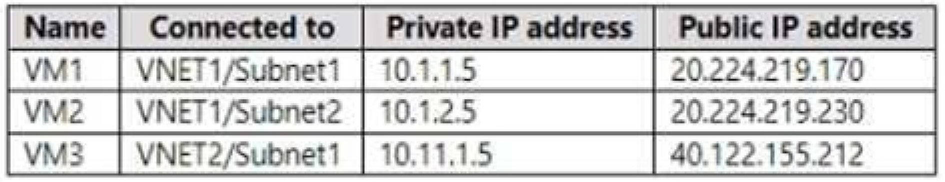
**Section:**

**Explanation:**

**QUESTION 22**

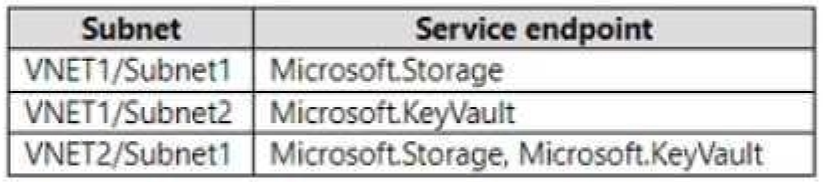
HOTSPOT

You have an Azure subscription that is linked to an Azure AD tenant and contains the virtual machines shown in the following table.



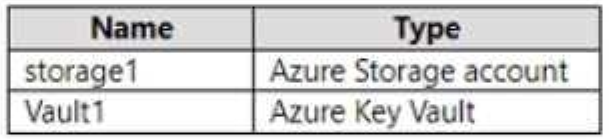
| Name | Connected to | Private IP address | Public IP address |
|---|---|---|---|
| VM1 | VNET1/Subnet1 | 10.1.1.5 | 20.224.219.170 |
| VM2 | VNET1/Subnet2 | 10.1.2.5 | 20.224.219.230 |
| VM3 | VNET2/Subnet1 | 10.11.1.5 | 40.122.155.212 |

The subnets of the virtual networks have the service endpoints shown in the following table.



| Subnet | Service endpoint |
|---|---|
| VNET1/Subnet1 | Microsoft.Storage |
| VNET1/Subnet2 | Microsoft.KeyVault |
| VNET2/Subnet1 | Microsoft.Storage, Microsoft.KeyVault |

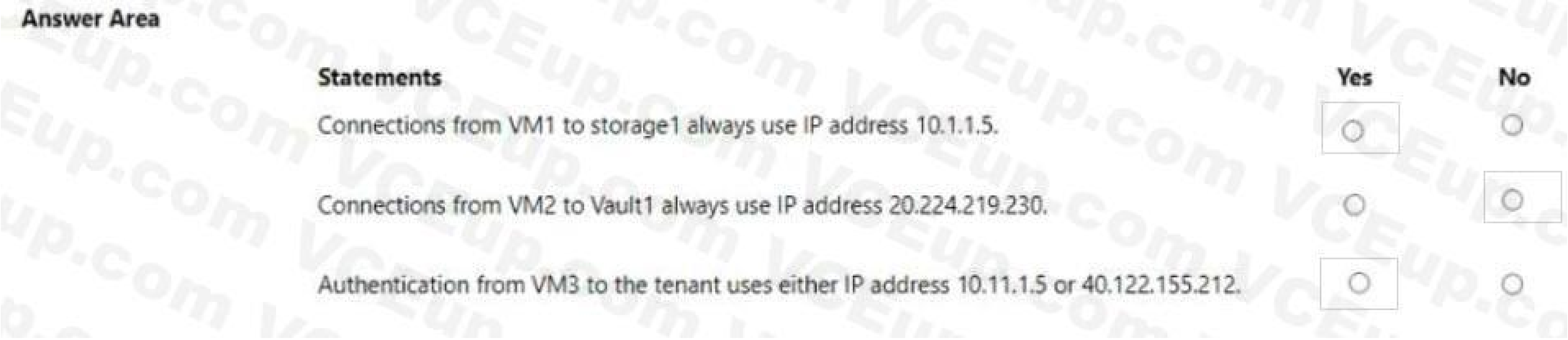
You create the resources shown in the following table.



| Name | Type |
|---|---|
| storage1 | Azure Storage account |
| Vault1 | Azure Key Vault |

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

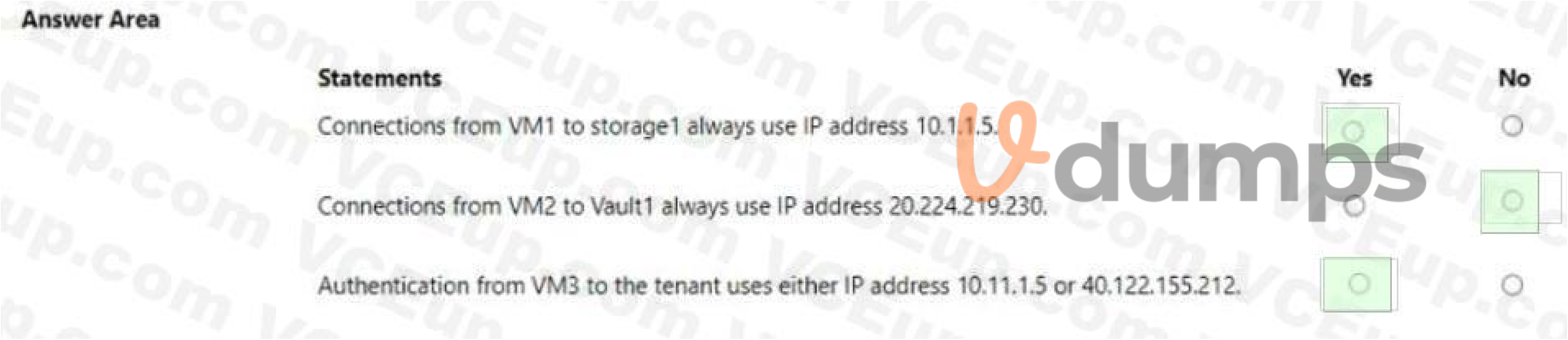
**Hot Area:**



**Answer Area**

| Statements | Yes | No |
|---|---|---|
| Connections from VM1 to storage1 always use IP address 10.1.1.5. | ○ | ○ |
| Connections from VM2 to Vault1 always use IP address 20.224.219.230. | ○ | ○ |
| Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212. | ○ | ○ |

**Answer Area:**



**Answer Area**

| Statements | Yes | No |
|---|---|---|
| Connections from VM1 to storage1 always use IP address 10.1.1.5. | ● | ○ |
| Connections from VM2 to Vault1 always use IP address 20.224.219.230. | ○ | ● |
| Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212. | ● | ○ |

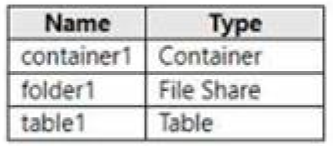
**Section:**

**Explanation:**

**QUESTION 23**

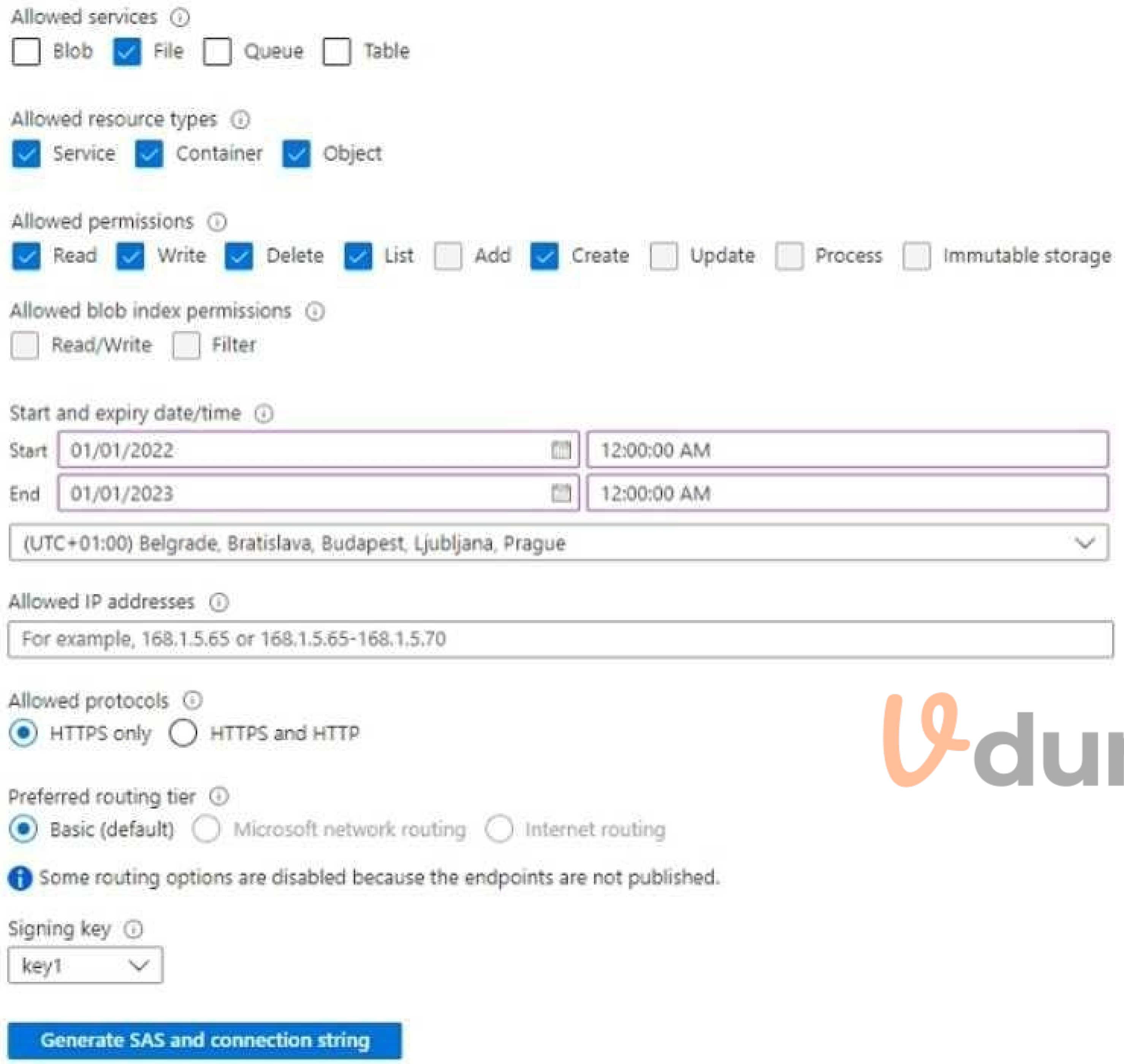
HOTSPOT

You have an Azure subscription that contains a user named User1 and a storage account named storage1. The storage1 account contains the resources shown in the following table.



| Name | Type |
|---|---|
| container1 | Container |
| folder1 | File Share |
| table1 | Table |

In storage1, you create a shared access signature (SAS) named SAS1 as shown in the following exhibit.



Allowed services ⓘ

☐ Blob ☑ File ☐ Queue ☐ Table

Allowed resource types ⓘ

☑ Service ☑ Container ☑ Object

Allowed permissions ⓘ

☑ Read ☑ Write ☑ Delete ☑ List ☐ Add ☑ Create ☐ Update ☐ Process ☐ Immutable storage

Allowed blob index permissions ⓘ

☐ Read/Write ☐ Filter

Start and expiry date/time ⓘ

Start 01/01/2022 12:00:00 AM

End 01/01/2023 12:00:00 AM

(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

Allowed IP addresses ⓘ

For example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols ⓘ

● HTTPS only ○ HTTPS and HTTP

Preferred routing tier ⓘ

● Basic (default) ○ Microsoft network routing ○ Internet routing

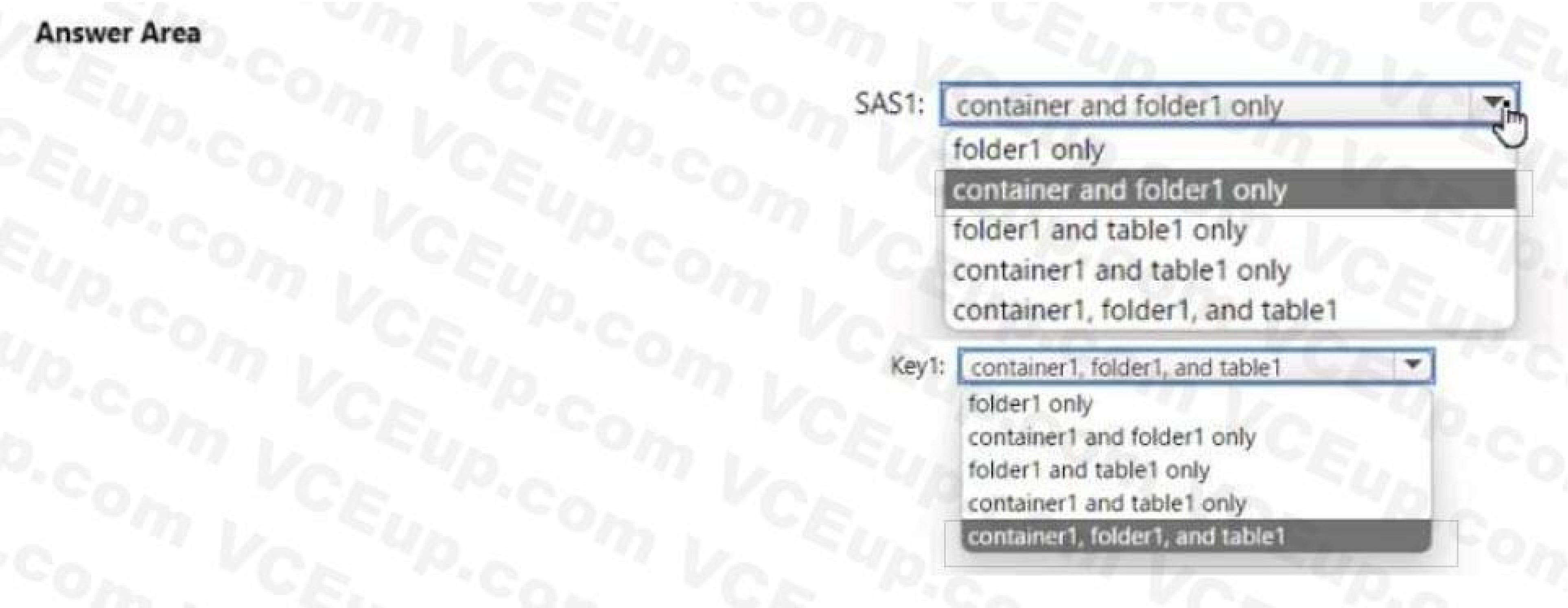
ⓘ Some routing options are disabled because the endpoints are not published.

Signing key ⓘ

key1

To which resources can User! write on July 1, 2022 by using SAS1 and key 1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Hot Area:**



Answer Area

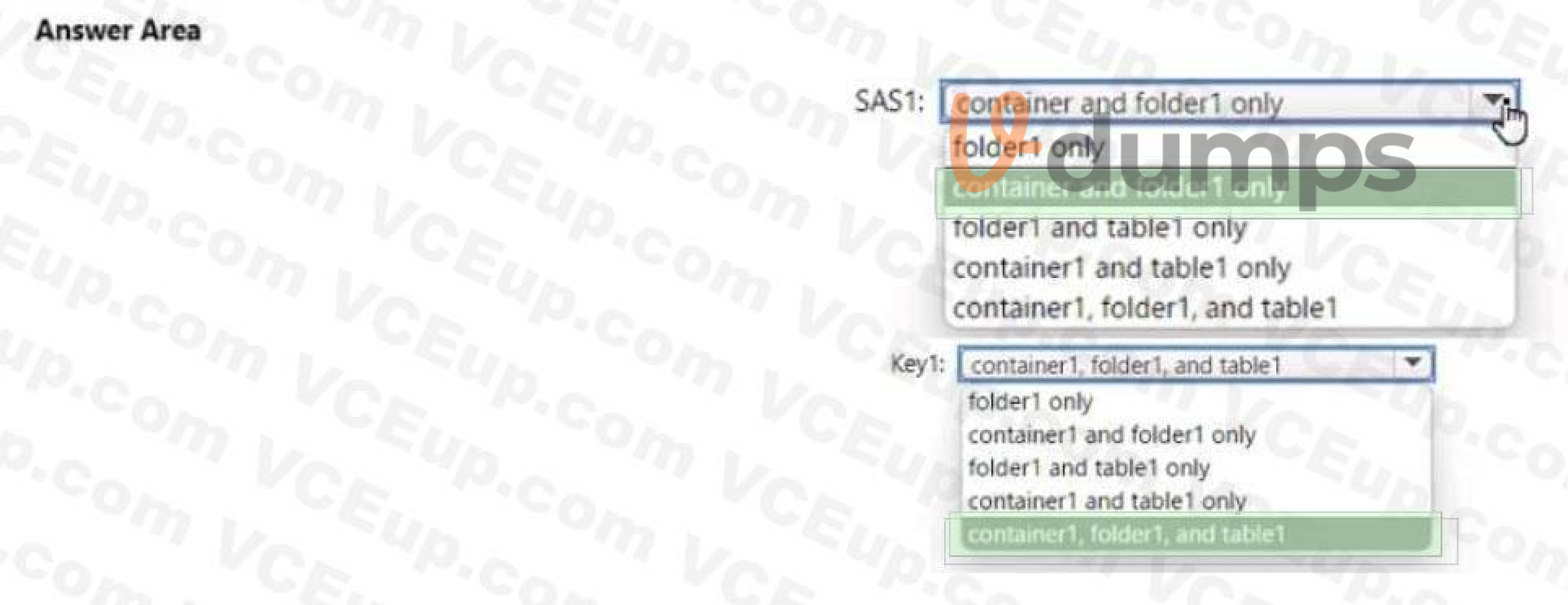
SAS1: container and folder1 only

- folder1 only
- container and folder1 only
- folder1 and table1 only
- container1 and table1 only
- container1, folder1, and table1

Key1: container1, folder1, and table1

- folder1 only
- container1 and folder1 only
- folder1 and table1 only
- container1 and table1 only
- container1, folder1, and table1

**Answer Area:**



Answer Area

SAS1: container and folder1 only

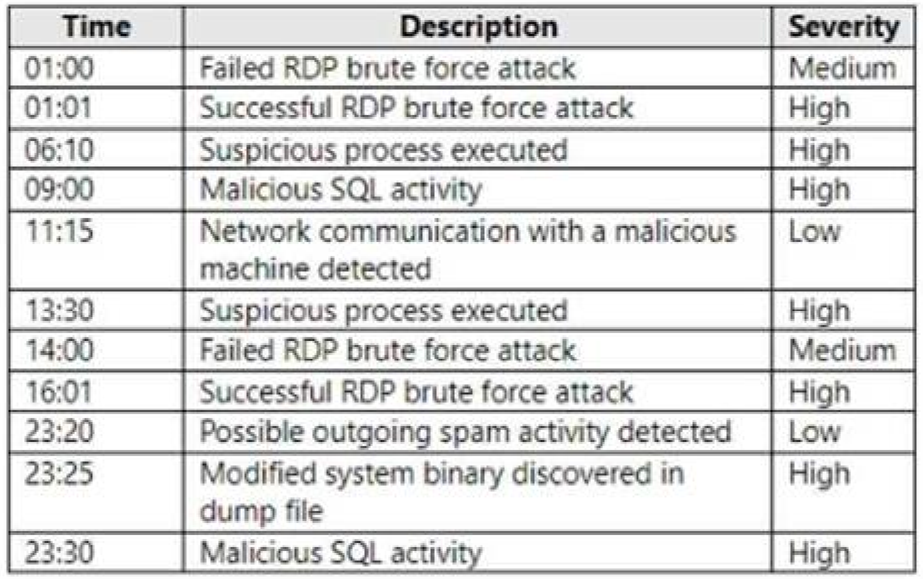
- folder1 only
- container and folder1 only
- folder1 and table1 only
- container1 and table1 only
- container1, folder1, and table1

Key1: container1, folder1, and table1

- folder1 only
- container1 and folder1 only
- folder1 and table1 only
- container1 and table1 only
- container1, folder1, and table1

**Section:**
**Explanation:**

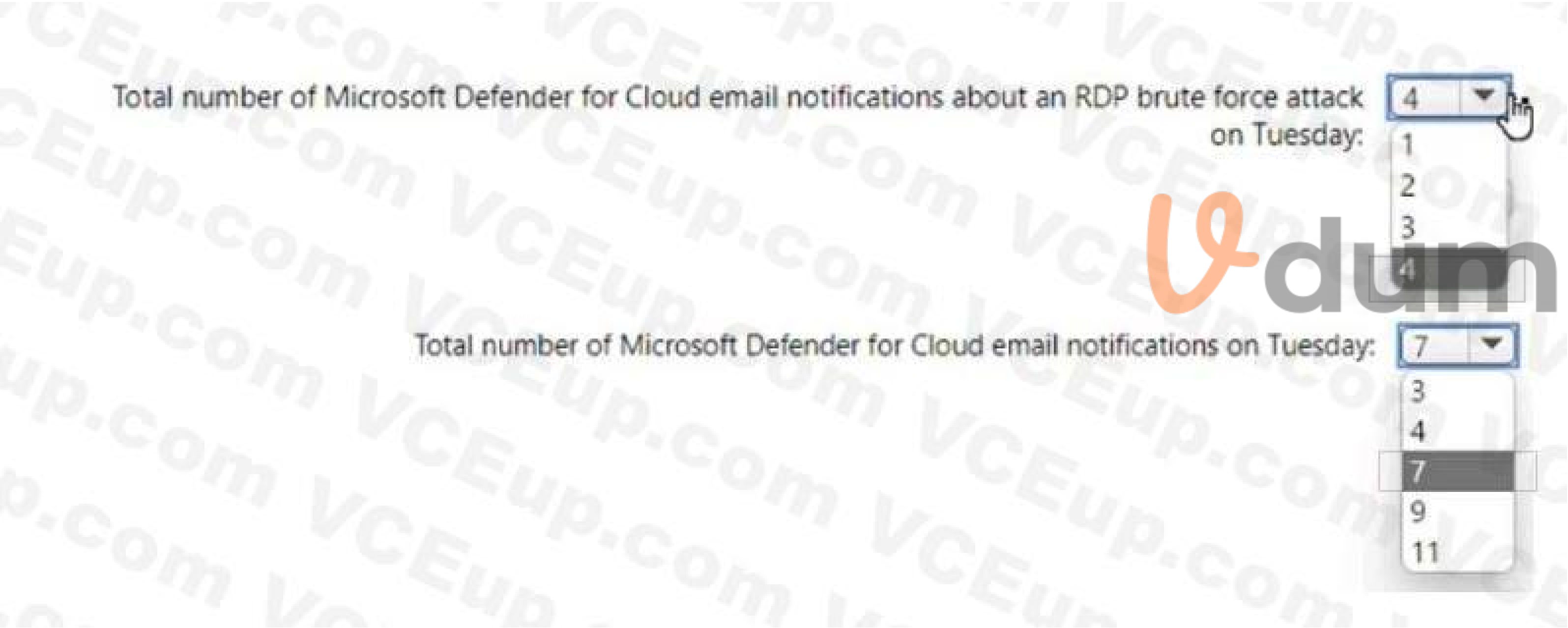
**QUESTION 24**
HOTSPOT
On Monday, you configure an email notification in Microsoft Defender for Cloud to notify user1 @contoso.com about alerts that have a severity level of Low, Medium, or High. On Tuesday, Microsoft Defender for Cloud generates the security alerts shown in the following table.



| 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.

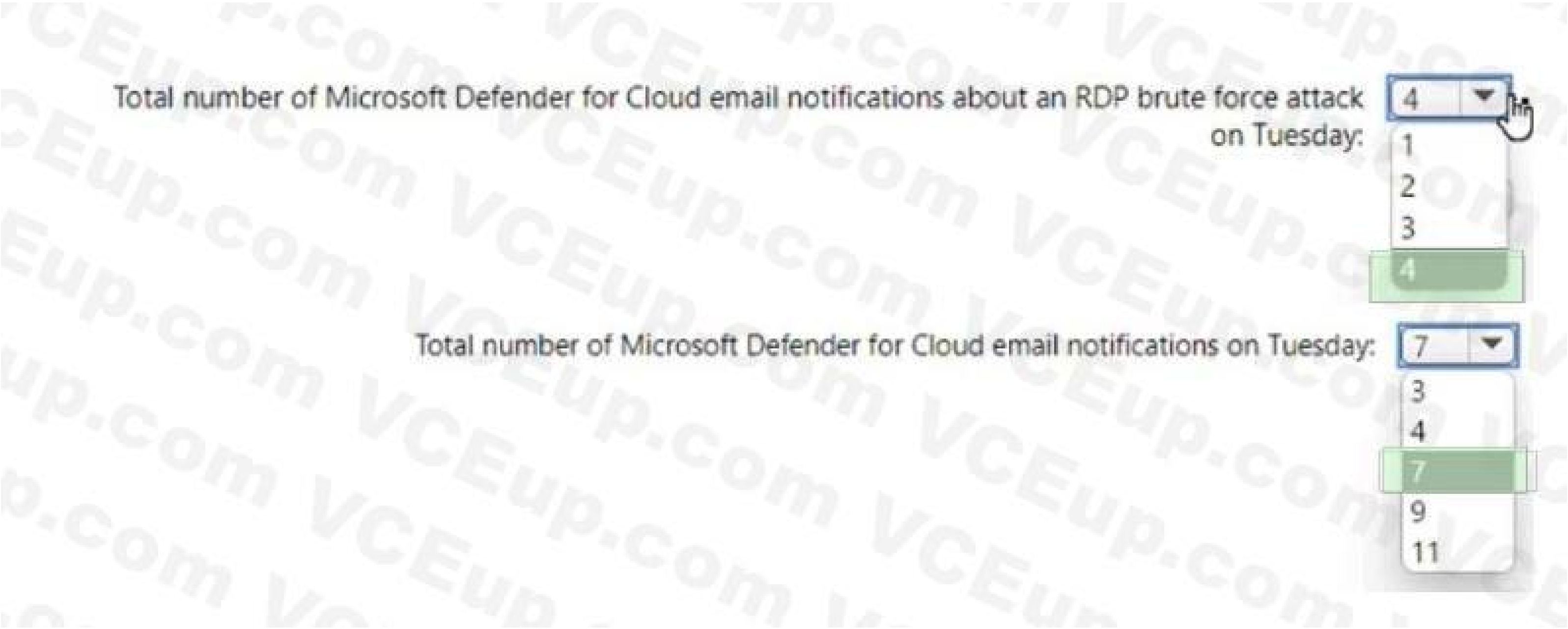
**Hot Area:**



Total number of Microsoft Defender for Cloud email notifications about an RDP brute force attack on Tuesday: 4

Total number of Microsoft Defender for Cloud email notifications on Tuesday: 7

**Answer Area:**



Total number of Microsoft Defender for Cloud email notifications about an RDP brute force attack on Tuesday: 4

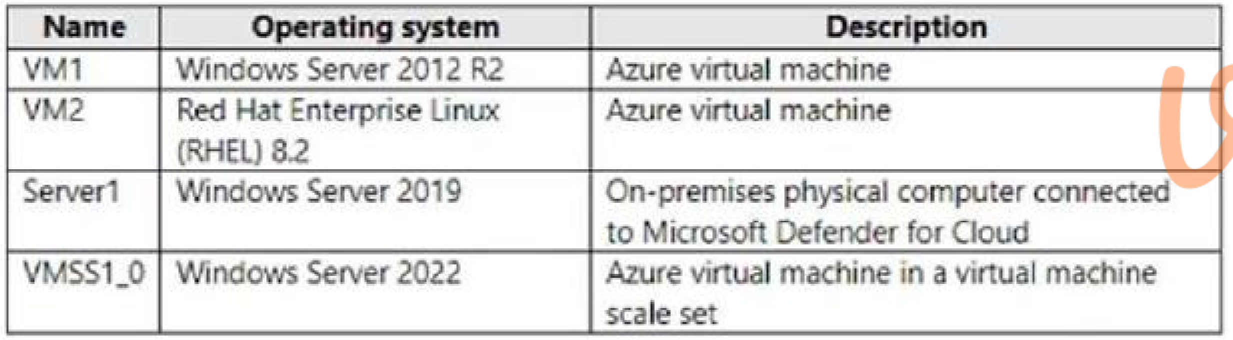
1
2
3
4

Total number of Microsoft Defender for Cloud email notifications on Tuesday: 7

3
4
7
9
11

**Section:**
**Explanation:**

**QUESTION 25**
You have an Azure subscription and the computers shown in the following table.



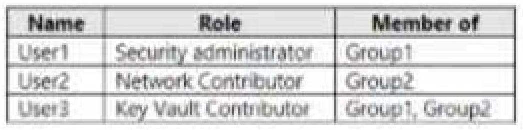
| Name | Operating system | Description |
|---|---|---|
| VM1 | Windows Server 2012 R2 | Azure virtual machine |
| VM2 | Red Hat Enterprise Linux (RHEL) 8.2 | Azure virtual machine |
| Server1 | Windows Server 2019 | On-premises physical computer connected to Microsoft Defender for Cloud |
| VMSS1_0 | Windows Server 2022 | Azure virtual machine in a virtual machine scale set |

You need to perform a vulnerability scan of the computers by using Microsoft Defender for Cloud.
Which computers can you scan?

A. VM1 only
B. VM1 and VM2 only
C. Server1 and VMSS1.0 only
D. VM1, VM2, and Server1 only
E. VM1, VM2, Server1, and VMSS1.0

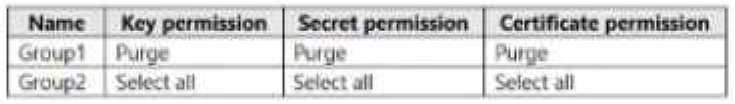
**Correct Answer: A**
**Section:**

**QUESTION 26**
HOTSPOT
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.



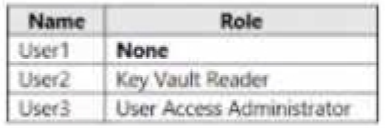
| Name | Role | Member of |
|---|---|---|
| User1 | Security administrator | Group1 |
| User2 | Network Contributor | Group2 |
| User3 | Key Vault Contributor | Group1, Group2 |

You have an Azure key vault named Vault1 that has Purge protection set to Disabled. 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 |

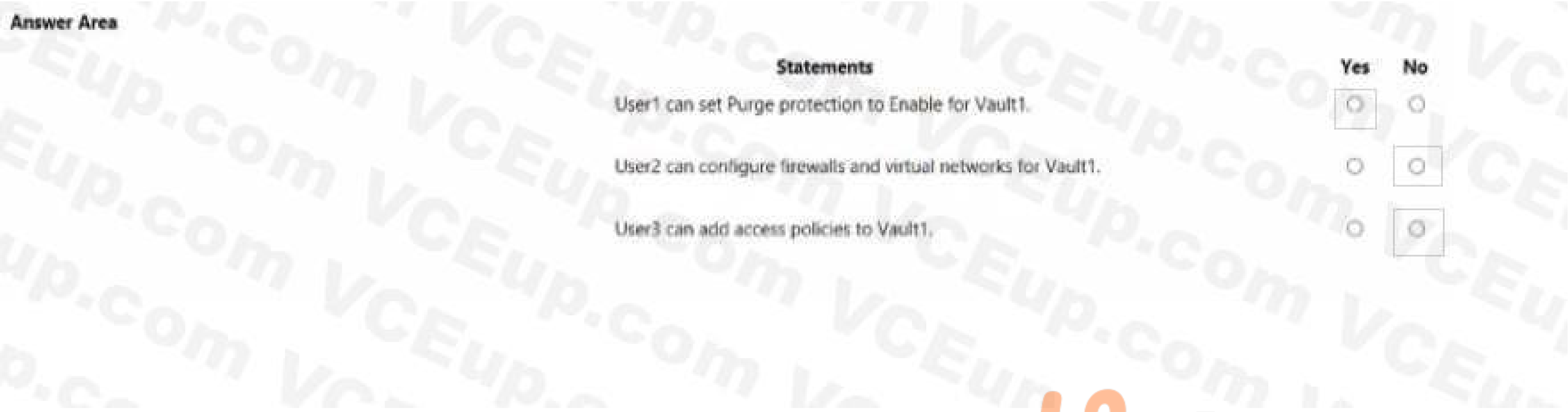
You create role assignments for Vault1 as shown in the following table.



| Name | Role |
|---|---|
| User1 | None |
| User2 | Key Vault Reader |
| User3 | User Access Administrator |

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

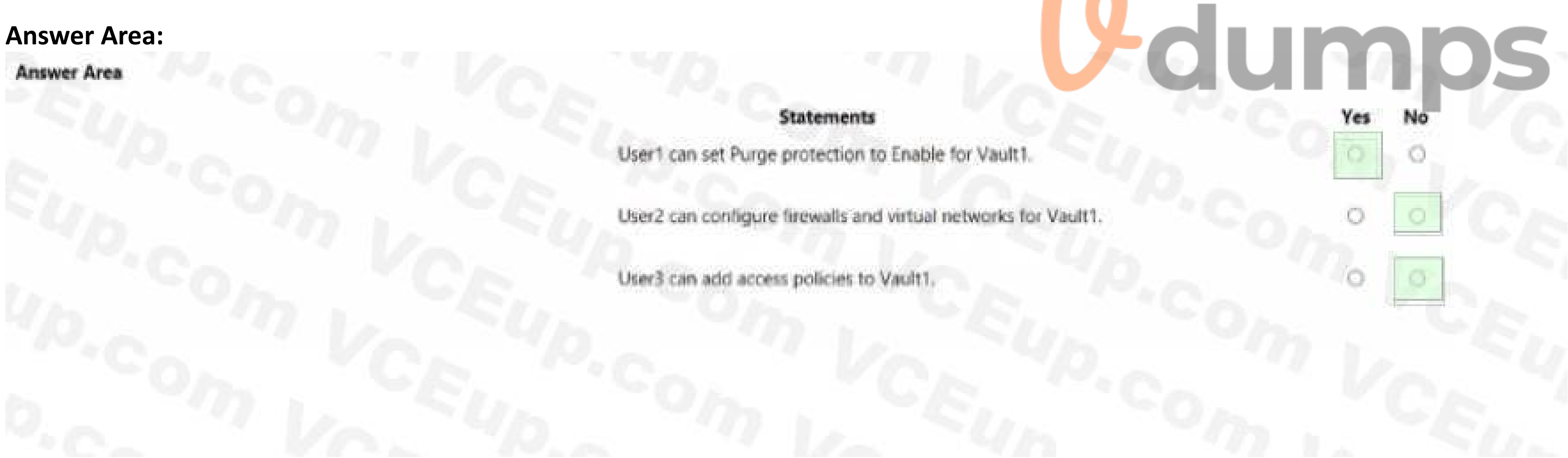
**Hot Area:**



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. | ○ | ○ |

**Answer Area:**



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. | ○ | [✓ ○] |

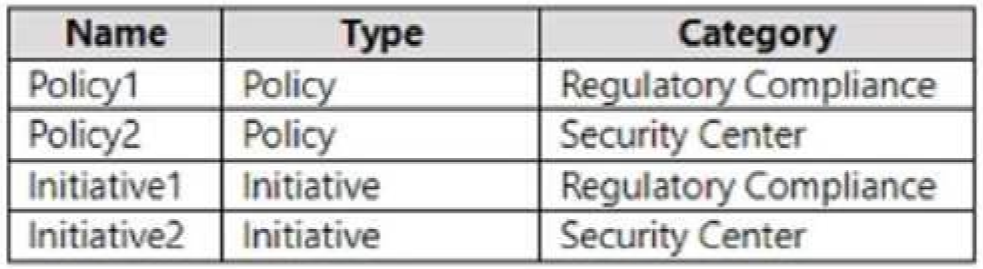
**Section:**
**Explanation:**

**QUESTION 27**
You have an Azure subscription that contains a Microsoft Defender External Attack Surface
Management (Defender EASM) resource named EASM1. EASM1 has discovery enabled and contains several inventory assets. You need to identify which inventory assets are vulnerable to the most critical web app security risks. Which Defender EASM dashboard should you use?

A. Attack Surface Summary
B. GDPRCompliance
C. Security Posture
D. OWASPToplO

**Correct Answer: D**
**Section:**

**QUESTION 28**
You have an Azure subscription that uses Microsoft Defender for Cloud. The subscription contains the Azure Policy definitions shown in the following table.



| Name | Type | Category |
|---|---|---|
| Policy1 | Policy | Regulatory Compliance |
| Policy2 | Policy | Security Center |
| Initiative1 | Initiative | Regulatory Compliance |
| Initiative2 | Initiative | Security Center |

Which definitions can be assigned as a security policy in Defender for Cloud?

A. Policy1 and Policy2 only
B. Initiative1 and Initiative2 only
C. Policy1 and Initiative1 only
D. Policy2 and Initiative2 only
E. Policy1, Policy2, Initiative1, and Initiative2

**Correct Answer: D**
**Section:**

**QUESTION 29**
You have an Azure subscription that uses Microsoft Defender for Cloud.
You need to use Defender for Cloud to review regulatory compliance with the Azure CIS 1.4,0 standard. The solution must minimize administrative effort. What should you do first?

A. Assign an Azure policy.
B. Manually add the Azure CIS 1.4.0 standard.
C. Disable one of the Out of the box standards.
D. Add a custom initiative.

**Correct Answer: A**
**Section:**

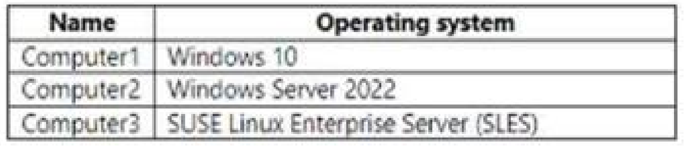
**QUESTION 30**
Your on-premises network contains a Hyper-V virtual machine named VM1. You need to use Azure Arc to onboard VM1 to Microsoft Defender for Cloud. What should you install first?

A. the Azure Monitor agent
B. the Azure Connected Machine agent
C. the Log Analytics agent
D. the guest configuration agent

**Correct Answer: B**
**Section:**

**QUESTION 31**

You have an Azure subscription. That contains the virtual machines shown in the following table.



| Name | Operating system |
|---|---|
| Computer1 | Windows 10 |
| Computer2 | Windows Server 2022 |
| Computer3 | SUSE Linux Enterprise Server (SLES) |

You need to enable file integrity monitoring in Microsoft Defender for Cloud. Which computers will support file integrity monitoring?

A. Computed only

B. Computer 1 and Computer2 only

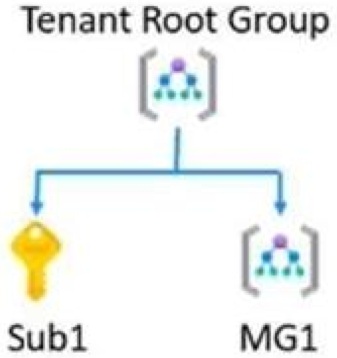
C. Computed and Computed only

D. Computer1, Computed, and Computed

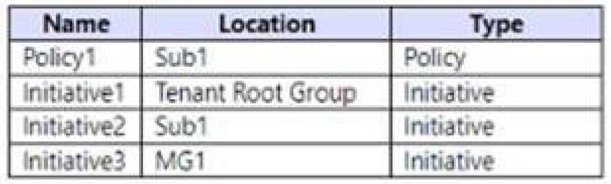
**Correct Answer: B**
**Section:**

**QUESTION 32**

You have an Azure subscription named Sub1 that uses Microsoft Defender for Cloud. You have the management group hierarchy shown in the following exhibit.



You create the definitions shown in the following table.



| Name | Location | Type |
|---|---|---|
| Policy1 | Sub1 | Policy |
| Initiative1 | Tenant Root Group | Initiative |
| Initiative2 | Sub1 | Initiative |
| Initiative3 | MG1 | Initiative |

You need to use Defender for Cloud to add a security policy. Which definitions can you use as a security policy?

A. Policy1 only

B. Policy1 and Initiative1 only

C. Initiative1 and Initiative2 only

D. Initiative1, Initiative2, and Initiatives only

E. Policy1, Initiative1, Initiative2, and Initiative3

**Correct Answer: B**
**Section:**

**QUESTION 33**

You have an Azure subscription that uses Azure AD Privileged Identity Management (PIM).
A user named User1 is eligible for the Billing administrator role.
You need to ensure that the role can only be used for a maximum of two hours.
What should you do?

A. Create a new access review.
B. Edit the role assignment settings.
C. Update the end date of the user assignment
D. Edit the role activation settings.

**Correct Answer: B**
**Section:**

**QUESTION 34**
You have an Azure subscription that contains the resources shown in the following table.
You need to configure storage1 to regenerate keys automatically every 90 days. Which cmdlet should you run?

A. set -A=StorageAccount
B. Add-A:StorogcAccountmanagementPolicyAction
C. Set-A;StorageAccountimanagementPolicy
D. Add-AsKeyVaultmanageStorageAccount

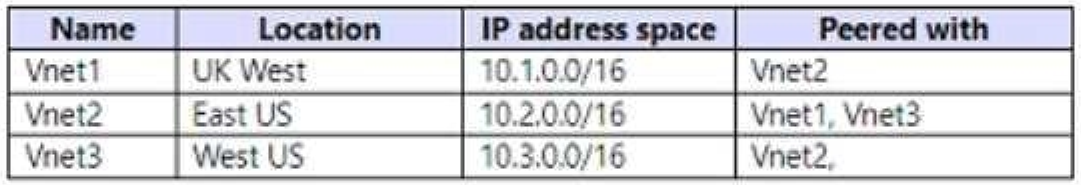
**Correct Answer: D**
**Section:**

**QUESTION 35**
You have an Azure subscription that contains a web app named Appl. App1 provides users with product images and videos. Users access App1 by using a URL of HTTPS://appl.contoso.com. You deploy two server pools named Pool! and Pool2. Pool1 hosts product images. Pool2 hosts product videos. You need to optimize The performance of Appl. The solution must meet the following requirements:
• Minimize the performance impact of TLS connections on Pool1 and Pool2.
• Route user requests to the server pools based on the requested URL path.
What should you include in the solution?

A. Azure Traffic Manager
B. Azure Bastion
C. Azure Application Gateway
D. Azure Front Door

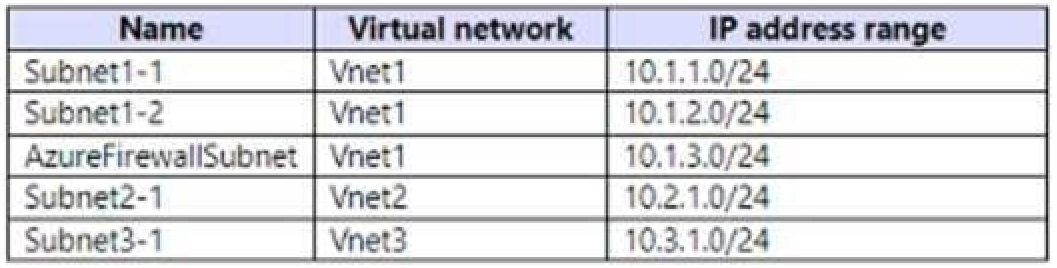
**Correct Answer: C**
**Section:**

**QUESTION 36**
HOTSPOT
You have an Azure subscription that contains the following Azure firewall:
• Name: Fw1
• Azure region: UK West
• Private IP address: 10.1.3.4
• Public IP address: 23.236.62.147
The subscription contains. The virtual networks shown in the following table.



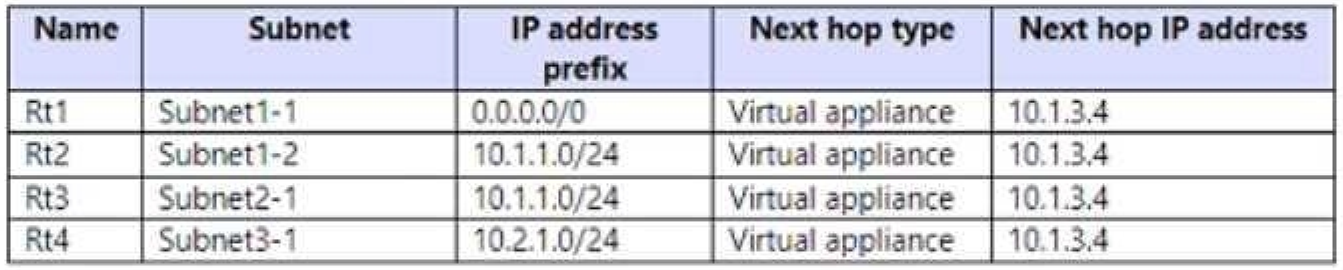
| Name | Location | IP address space | Peered with |
|---|---|---|---|
| Vnet1 | UK West | 10.1.0.0/16 | Vnet2 |
| Vnet2 | East US | 10.2.0.0/16 | Vnet1, Vnet3 |
| Vnet3 | West US | 10.3.0.0/16 | Vnet2, |

The subscription contains the subnets shown in the following table.



| Name | Virtual network | IP address range |
|---|---|---|
| Subnet1-1 | Vnet1 | 10.1.1.0/24 |
| Subnet1-2 | Vnet1 | 10.1.2.0/24 |
| AzureFirewallSubnet | Vnet1 | 10.1.3.0/24 |
| Subnet2-1 | Vnet2 | 10.2.1.0/24 |
| Subnet3-1 | Vnet3 | 10.3.1.0/24 |

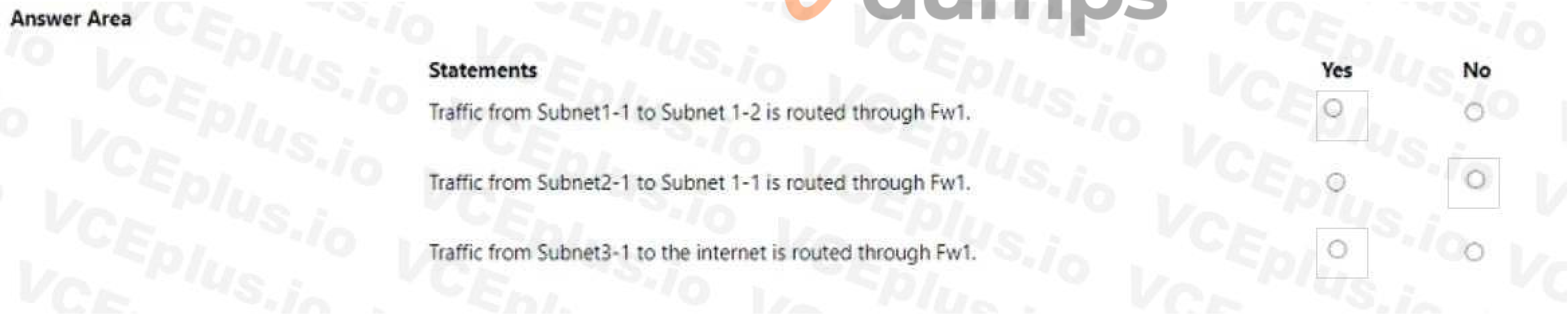
The subscription contains the routes shown in the following table.



| Name | Subnet | IP address prefix | Next hop type | Next hop IP address |
|---|---|---|---|---|
| Rt1 | Subnet1-1 | 0.0.0.0/0 | Virtual appliance | 10.1.3.4 |
| Rt2 | Subnet1-2 | 10.1.1.0/24 | Virtual appliance | 10.1.3.4 |
| Rt3 | Subnet2-1 | 10.1.1.0/24 | Virtual appliance | 10.1.3.4 |
| Rt4 | Subnet3-1 | 10.2.1.0/24 | Virtual appliance | 10.1.3.4 |

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

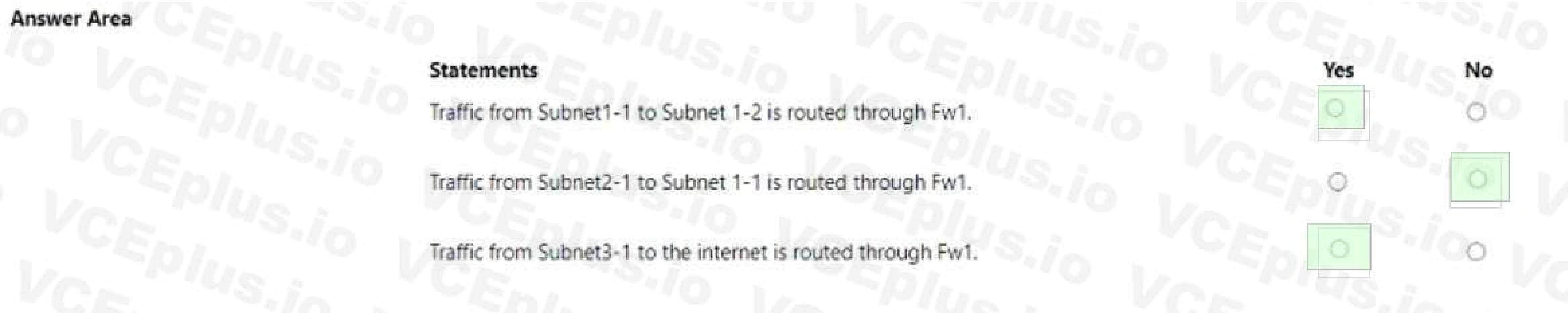
**Hot Area:**



**Answer Area**

| Statements | Yes | No |
|---|---|---|
| Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1. | ○ | ○ |
| Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1. | ○ | ○ |
| Traffic from Subnet3-1 to the internet is routed through Fw1. | ○ | ○ |

**Answer Area:**



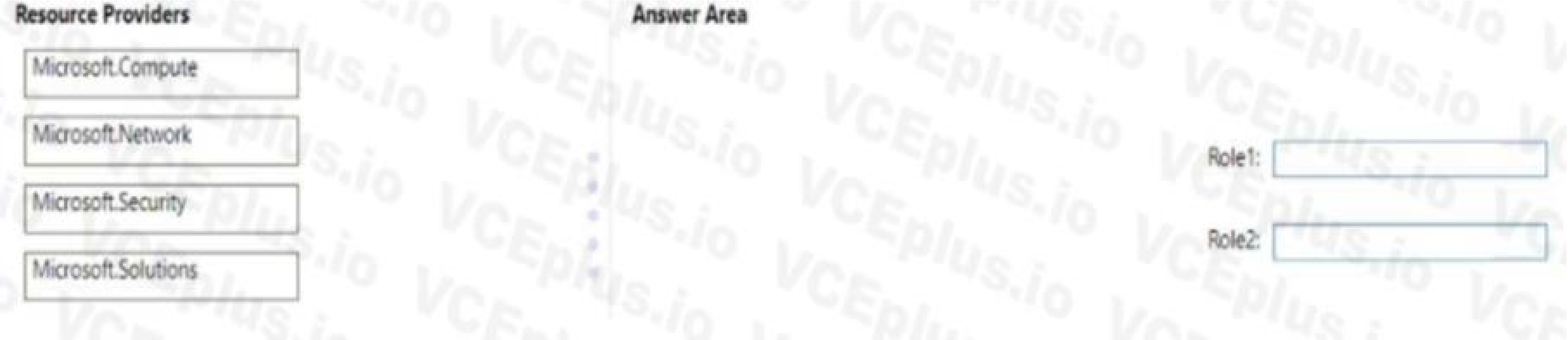
Answer Area

| Statements | Yes | No |
|---|---|---|
| Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1. | [✓ ○] | ○ |
| Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1. | ○ | [✓ ○] |
| Traffic from Subnet3-1 to the internet is routed through Fw1. | [✓ ○] | ○ |

**Section:**
**Explanation:**

**QUESTION 37**
DRAG DROP
You have an Azure subscription.
You plan to create two custom roles named Role1 and Role2.
The custom roles will be used to perform the following tasks:
• Members of Role1 will manage application security groups.
• Members of Role2 will manage Azure Bastion.
You need to add permissions to the custom roles.
Which resource provider should you use for each role? To answer, drag the appropriate resource providers to the correct roles. Each resource provider 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

**Select and Place:**



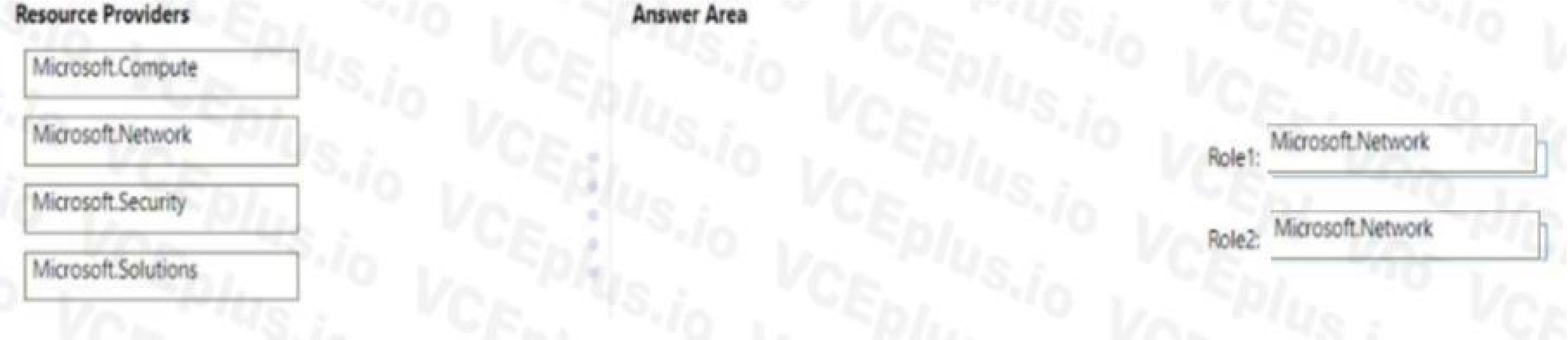
Resource Providers

Microsoft.Compute
Microsoft.Network
Microsoft.Security
Microsoft.Solutions

Answer Area

Role1:
Role2:

**Correct Answer:**



Resource Providers

Microsoft.Compute
Microsoft.Network
Microsoft.Security
Microsoft.Solutions

Answer Area

Role1: Microsoft.Network
Role2: Microsoft.Network

**Section:**

**Explanation:**

**QUESTION 38**

You have an Azure subscription that contains a resource group named RG1 and a security group named ServerAdmins. RG1 contains 10 virtual machines, a virtual network named VNET1, and a network security group JNSG) named NSG1. ServerAdmins can access the virtual machines by using RDP.

You need to ensure that NSG1 only allows RDP connections to the virtual machines for a maximum of 60 minutes when a member of ServerAdmins requests access. What should you configure?

A. an Azure policy assigned to RGl

B. a just in time (JIT) VM access policy in Microsoft Defender for Cloud

C. an Azure AD Privileged Identity Management (PiM) role assignment

D. an Azure Bastion host on VNET1

**Correct Answer: B**

**Section:**

**Explanation:**

**QUESTION 39**

DRAG DROP

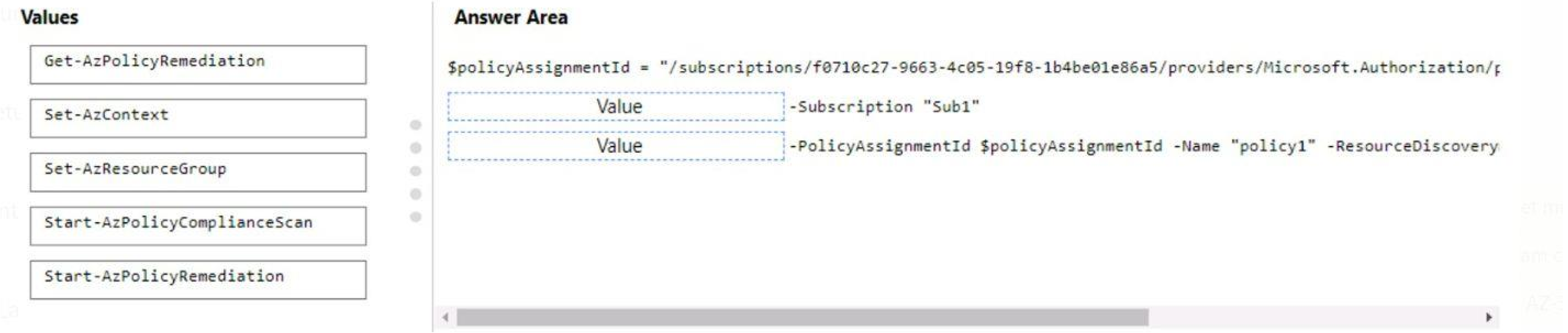
You have two Azure subscriptions named Sub1 and Sub2. Sub1 contains a resource group named RG1 and an Azure policy named Policy1.

You need to remediate the non-compliant resources in Sub1 based on Policy1.

How should you complete the PowerShell script? To answer, drag the appropriate values to the correct targets. Each value 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.

**Select and Place:**



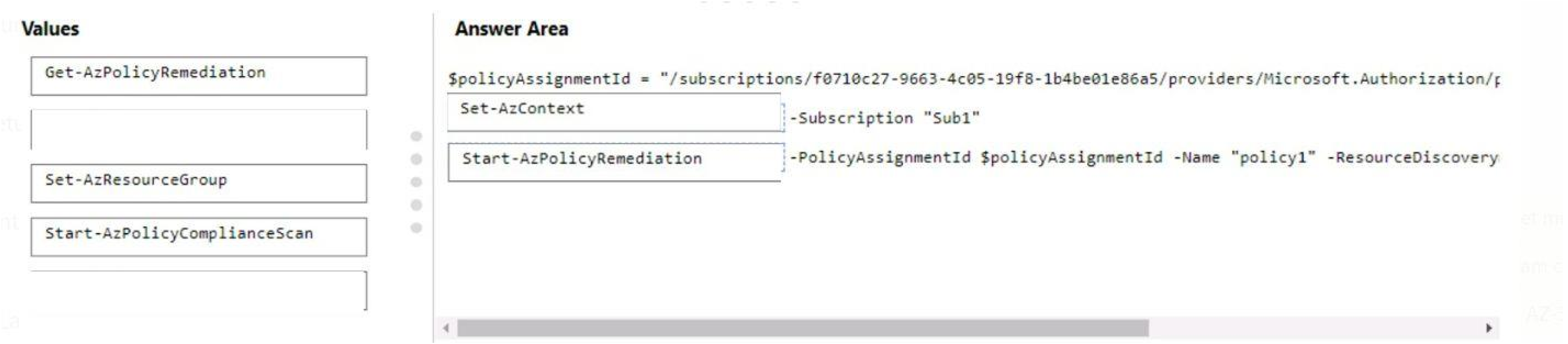
Values

- Get-AzPolicyRemediation
- Set-AzContext
- Set-AzResourceGroup
- Start-AzPolicyComplianceScan
- Start-AzPolicyRemediation

Answer Area

```
$policyAssignmentId = "/subscriptions/f0710c27-9663-4c05-19f8-1b4be01e86a5/providers/Microsoft.Authorization/p
Value -Subscription "Sub1"
Value -PolicyAssignmentId $policyAssignmentId -Name "policy1" -ResourceDiscovery
```

**Correct Answer:**



Values

Get-AzPolicyRemediation

Set-AzResourceGroup

Start-AzPolicyComplianceScan

Answer Area

```
$policyAssignmentId = "/subscriptions/f0710c27-9663-4c05-19f8-1b4be01e86a5/providers/Microsoft.Authorization/p
Set-AzContext -Subscription "Sub1"
Start-AzPolicyRemediation -PolicyAssignmentId $policyAssignmentId -Name "policy1" -ResourceDiscovery
```

**Section:**
**Explanation:**
For the first blank, use Set-AzContext to set the current subscription context.
For the second blank, use Start-AzPolicyRemediation to create and start a policy remediation for a policy assignment.
The final script should look like this:
$policyAssignmentId = "/subscriptions/f0710c27-9663-4c05-19781bdbedle86as/providers/Microsoft.
Authorization/f Value Set-AzContext -Subscription “Sub1”
Value Start-AzPolicyRemediation -PolicyAssignmentId $policyAssignmentId -Name "policy1" ResourceDiscovery

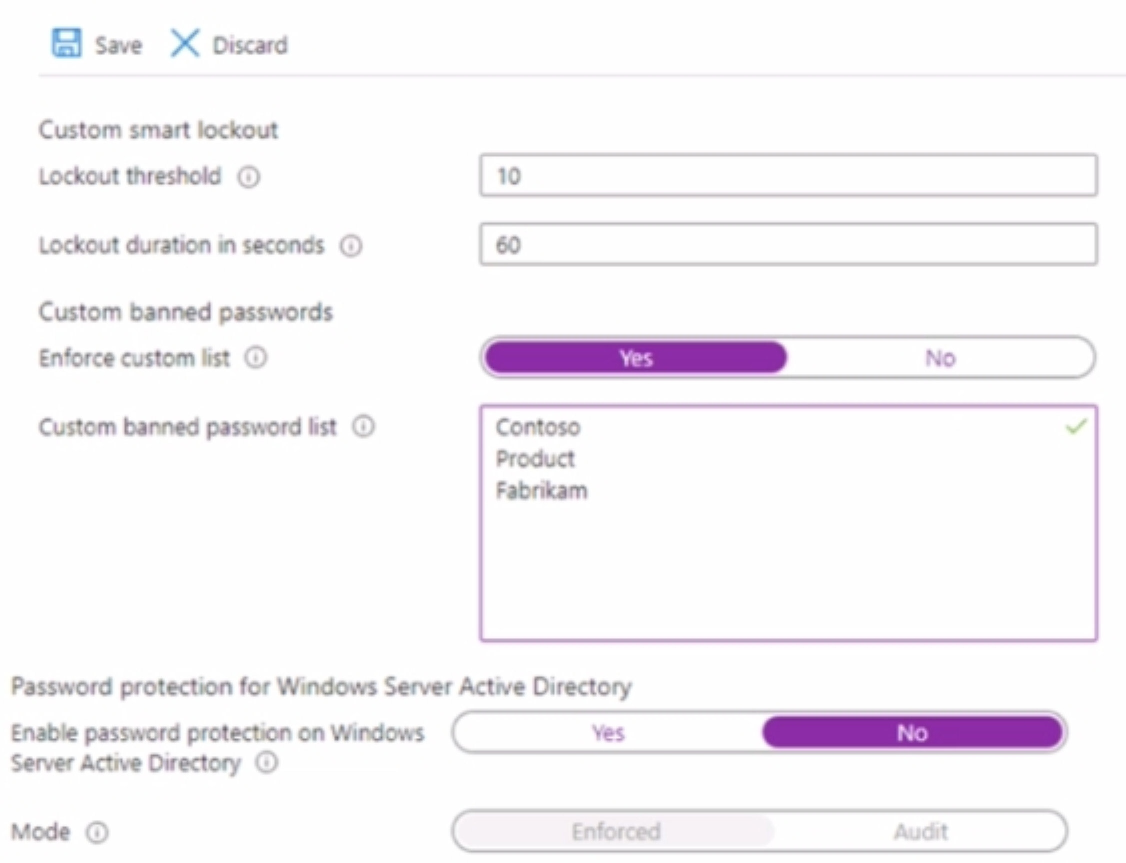
**QUESTION 40**
You have an Azure subscription that uses Microsoft Defender for Cloud. You have accounts for the following cloud services:
- Alibaba Cloud
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

What can you add to Defender for Cloud?

A. AWS only
B. Alibaba Cloud and AWS only
C. Alibaba Good and GCP only
D. AWS and GCP only
E. Alibaba Cloud, AWS. and GCP

**Correct Answer: D**
**Section:**

**QUESTION 41**
You have a Microsoft Entra tenant that contains three users named User1, User2, and User3.
You configure Microsoft Entra Password Protection as shown in the following exhibit.



Custom smart lockout

Lockout threshold: 10

Lockout duration in seconds: 60

Custom banned passwords

Enforce custom list: [✓ Yes] No

Custom banned password list:
Contoso
Product
Fabrikam

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory: Yes [✓ No]

Mode: Enforced Audit

The users perform the following tasks:
* User1 attempts to reset her password to COntOsO
* User2 attempts to reset her password to F@brikamHQ
* User3 attempts to reset her password to PrOduct123.
Which password reset attempts fail?

A. User1 only
B. User2only
C. User3 only
D. User1 and User3 only
E. User1, User2, and User3

**Correct Answer: E**
**Section:**

**QUESTION 42**
You have an Azure subscription that contains an Azure key vault named Vault1 and a virtual machine named VM1. VM1 has the Key Vault VM extension installed.
For Vault1, you rotate the keys, secrets, and certificates.
What will be updated automatically on VM1?

A. the keys only
B. the secrets only
C. the certificates only
D. the keys and secrets only
E. the secrets and certificates only
F. the keys, secrets, and certificates

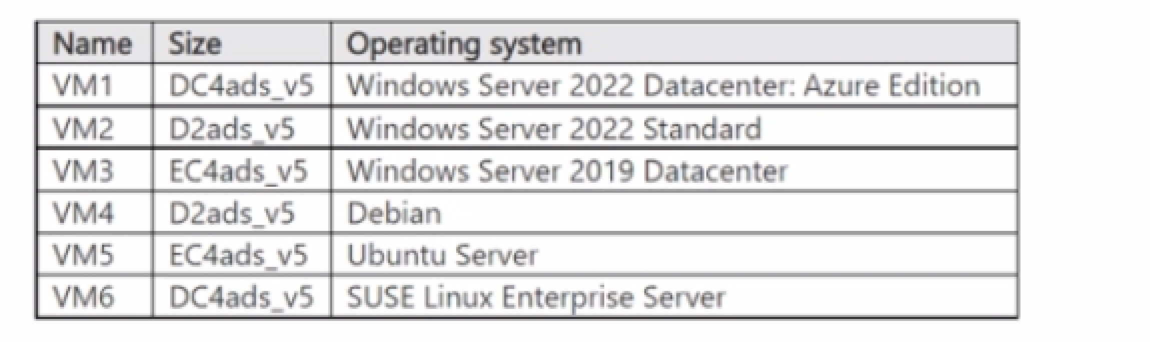
**Correct Answer: C**
**Section:**

**QUESTION 43**

HOTSPOT

You have an Azure subscription.

You plan to deploy the virtual machines shown in the following table.

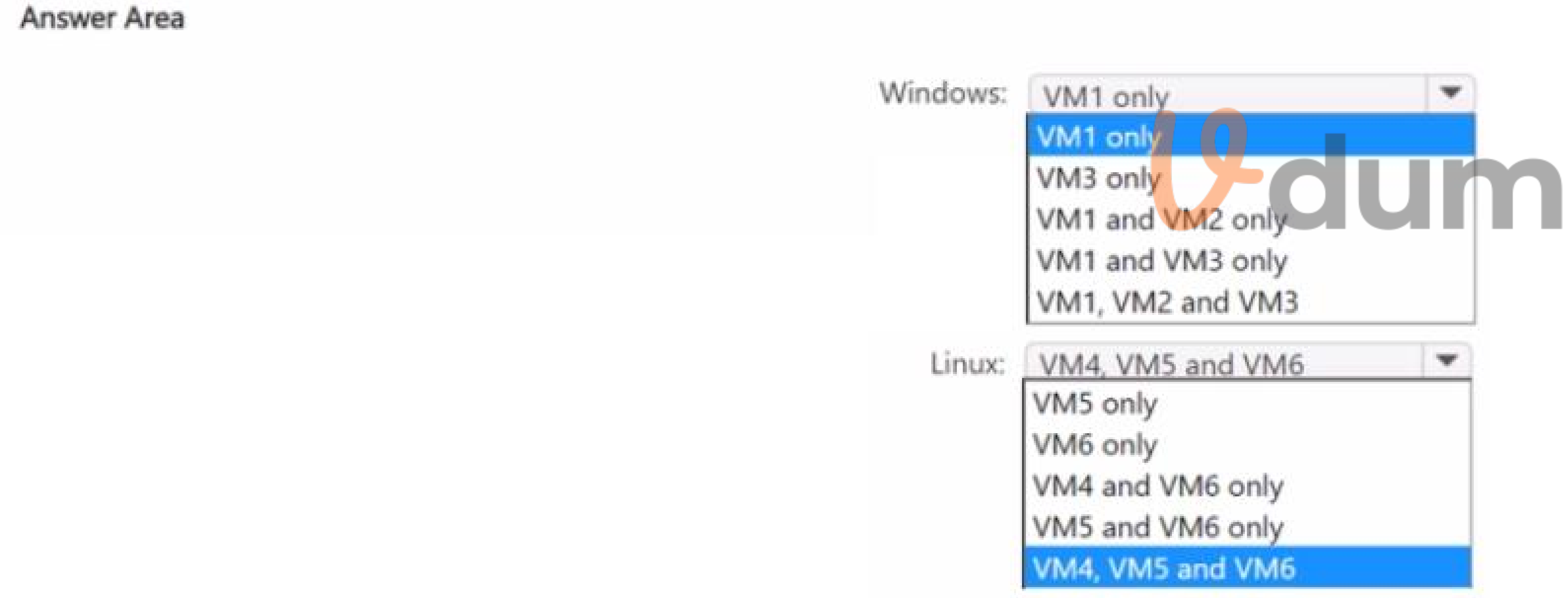


| Name | Size | Operating system |
|---|---|---|
| VM1 | DC4ads_v5 | Windows Server 2022 Datacenter: Azure Edition |
| VM2 | D2ads_v5 | Windows Server 2022 Standard |
| VM3 | EC4ads_v5 | Windows Server 2019 Datacenter |
| VM4 | D2ads_v5 | Debian |
| VM5 | EC4ads_v5 | Ubuntu Server |
| VM6 | DC4ads_v5 | SUSE Linux Enterprise Server |

You need to identify the virtual machines and operating systems that can be deployed as confidential virtual machines?

Which Windows virtual machines and which Linux virtual machines should you identify?

**Hot Area:**



Answer Area

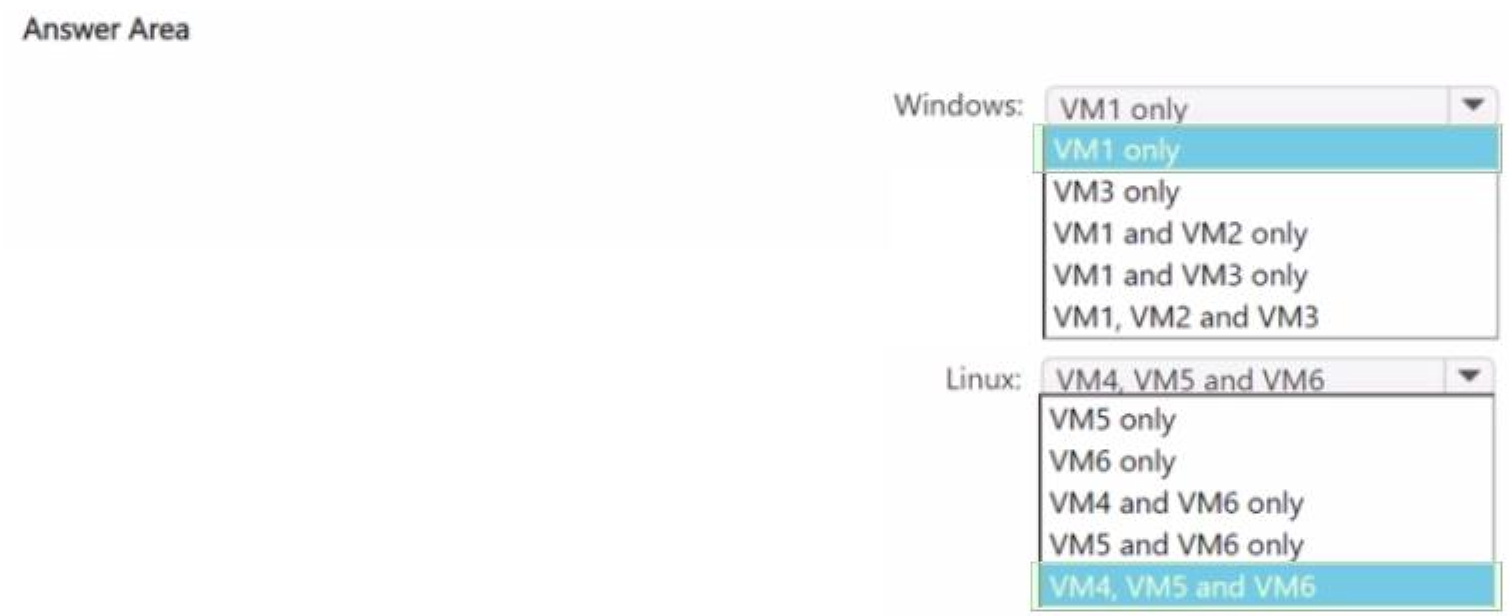
Windows: VM1 only

- VM1 only
- VM3 only
- VM1 and VM2 only
- VM1 and VM3 only
- VM1, VM2 and VM3

Linux: VM4, VM5 and VM6

- VM5 only
- VM6 only
- VM4 and VM6 only
- VM5 and VM6 only
- VM4, VM5 and VM6

**Answer Area:**



Answer Area

Windows: VM1 only

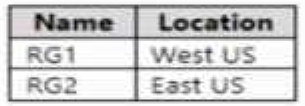
- VM1 only
- VM3 only
- VM1 and VM2 only
- VM1 and VM3 only
- VM1, VM2 and VM3

Linux: VM4, VM5 and VM6

- VM5 only
- VM6 only
- VM4 and VM6 only
- VM5 and VM6 only
- VM4, VM5 and VM6

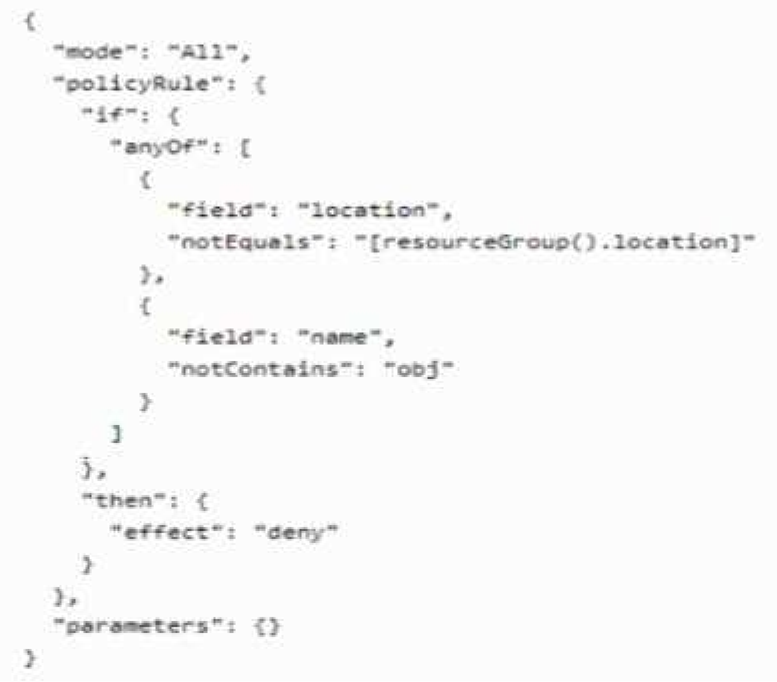
**Section:**
**Explanation:**

**QUESTION 44**
HOTSPOT
You have an Azure subscription named Sub1 that contains the resource groups shown in the following table.



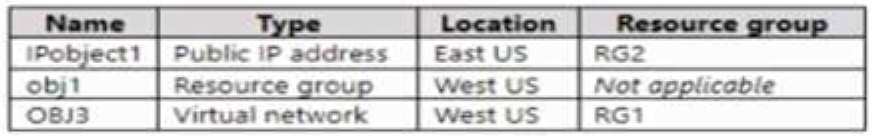
| Name | Location |
|---|---|
| RG1 | West US |
| RG2 | East US |

You create the Azure Policy definition shown in the following exhibit.



```
{
  "mode": "All",
  "policyRule": {
    "if": {
      "anyOf": [
        {
          "field": "location",
          "notEquals": "[resourceGroup().location]"
        },
        {
          "field": "name",
          "notContains": "obj"
        }
      ]
    },
    "then": {
      "effect": "deny"
    }
  },
  "parameters": {}
}
```

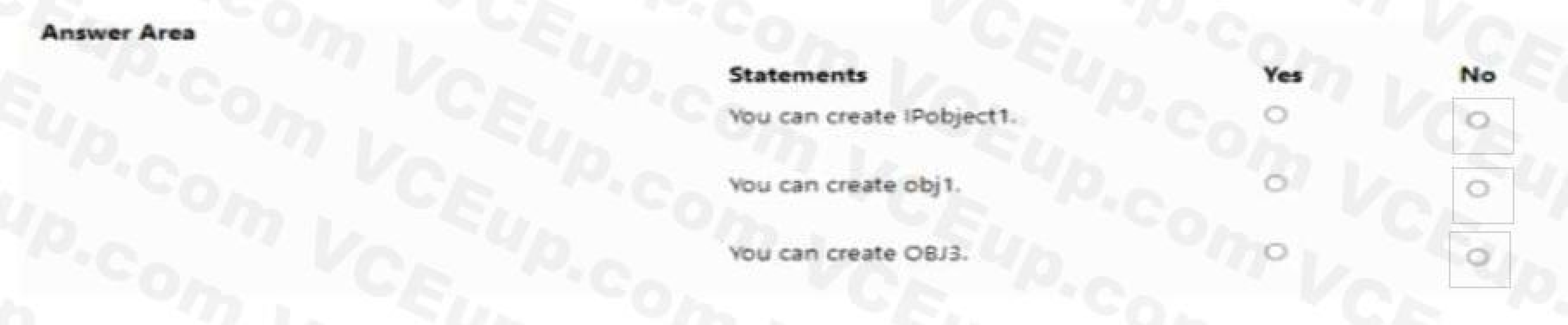
You assign the policy to Sub1.
You plan to create the resources shown in the following table.



| Name | Type | Location | Resource group |
|---|---|---|---|
| IPobject1 | Public IP address | East US | RG2 |
| obj1 | Resource group | West US | *Not applicable* |
| OBJ3 | Virtual network | West US | 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.

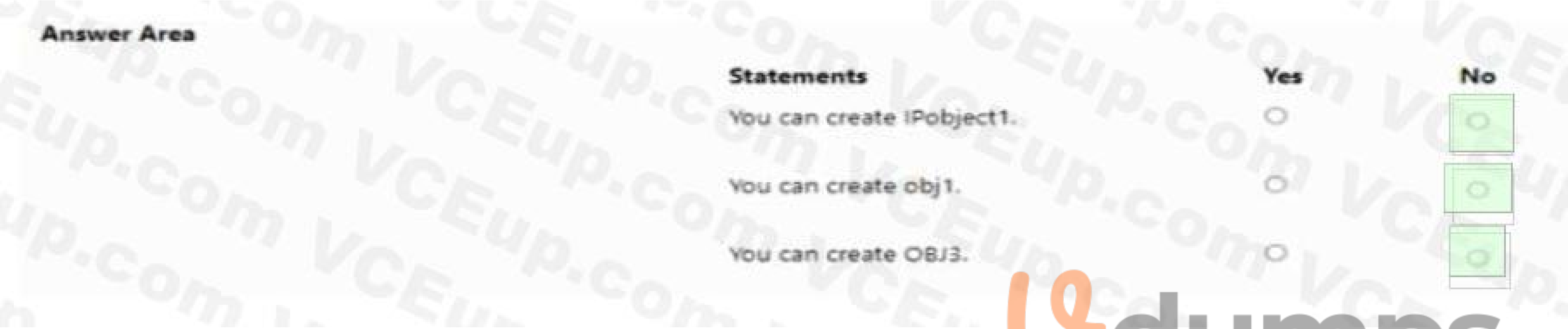
**Hot Area:**



**Answer Area**

| Statements | Yes | No |
|---|---|---|
| You can create IPobject1. | ○ | ○ |
| You can create obj1. | ○ | ○ |
| You can create OBJ3. | ○ | ○ |

**Answer Area:**

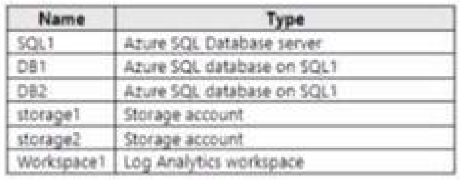


**Answer Area**

| Statements | Yes | No |
|---|---|---|
| You can create IPobject1. | ○ | [✓ ○] |
| You can create obj1. | ○ | [✓ ○] |
| You can create OBJ3. | ○ | [✓ ○] |

**Section:**
**Explanation:**

**QUESTION 45**
HOTSPOT
You have an Azure subscription that contains the resources shown in the following table.



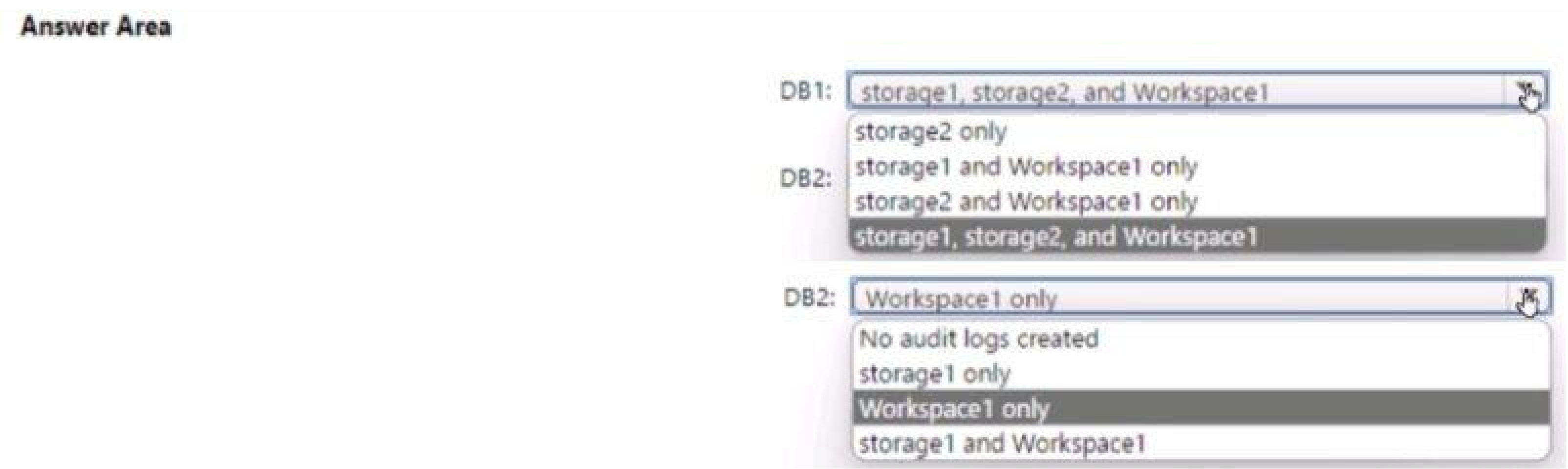
| Name | Type |
|---|---|
| SQL1 | Azure SQL Database server |
| DB1 | Azure SQL database on SQL1 |
| DB2 | Azure SQL database on SQL1 |
| storage1 | Storage account |
| storage2 | Storage account |
| Workspace1 | Log Analytics workspace |

SQL1 has the following configurations:
- Auditing: Enabled
- Audit log destination: storage1, Workspace1

DB1 has the following configurations:
- Auditing: Enabled
- Audit log destination: storage2

DB2 has auditing disabled.
Where are the audit logs for DB1 and DB2 stored? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.

**Hot Area:**



Answer Area

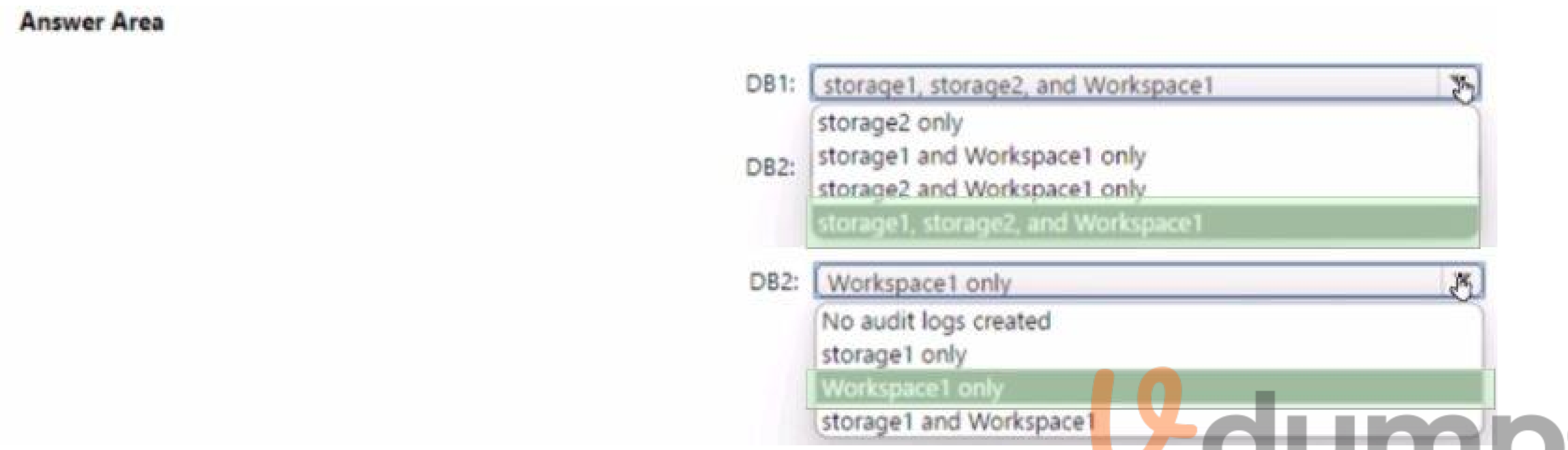
DB1: storage1, storage2, and Workspace1

- storage2 only
- storage1 and Workspace1 only
- storage2 and Workspace1 only
- [✓ storage1, storage2, and Workspace1]

DB2: Workspace1 only

- No audit logs created
- storage1 only
- [✓ Workspace1 only]
- storage1 and Workspace1

**Answer Area:**



Answer Area

DB1: storage1, storage2, and Workspace1

- storage2 only
- storage1 and Workspace1 only
- storage2 and Workspace1 only
- [✓ storage1, storage2, and Workspace1]

DB2: Workspace1 only

- No audit logs created
- storage1 only
- [✓ Workspace1 only]
- storage1 and Workspace1

**Section:**

**Explanation:**

**QUESTION 46**

HOTSPOT

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

Subnet1 and Subnet2 have a network security group {NSG). The NSG has an outbound rule that has the following configurations:

- Port; Any
- Source: Any
- Priority: 100
- Action: Deny
- Protocol: Any
- Destination: Storage

The subscription contains a storage account named storage1.

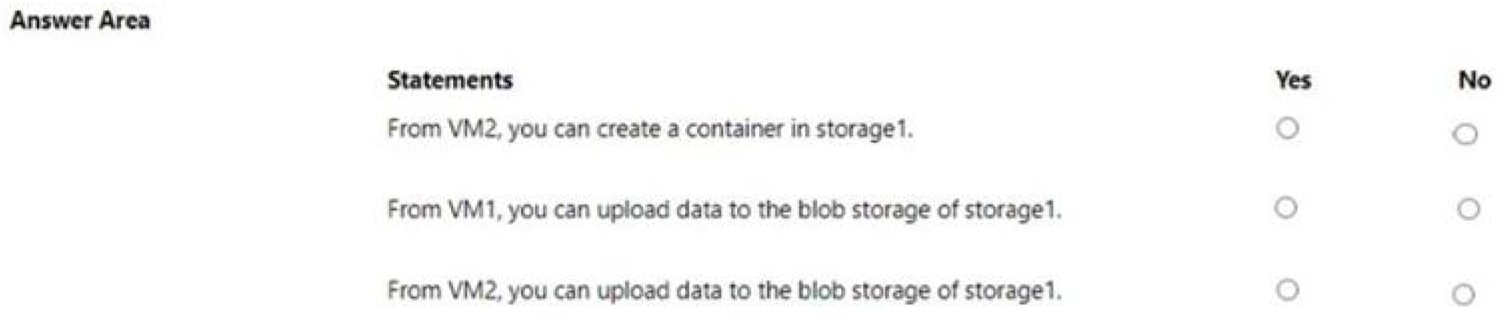
You create a private endpoint named Private1 that has the following settings:

- Resource type: Microsoft.Storage/storageAccounts
- Resource: storage1
- Target sub-resource: blob
- Virtual network: VNet1
- Subnet: Subnet1

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

NOTE: Each correct selection is worth one point.

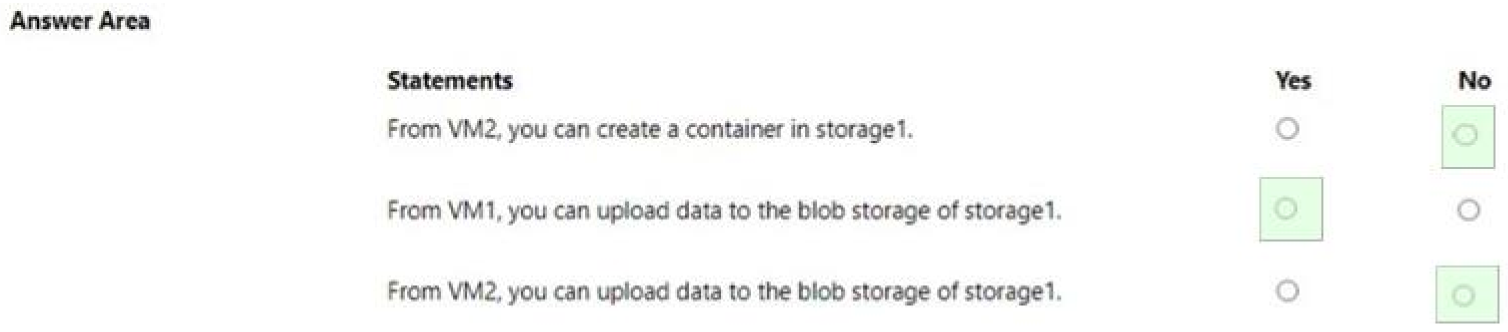
**Hot Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| From VM2, you can create a container in storage1. | ○ | ○ |
| From VM1, you can upload data to the blob storage of storage1. | ○ | ○ |
| From VM2, you can upload data to the blob storage of storage1. | ○ | ○ |

**Answer Area:**

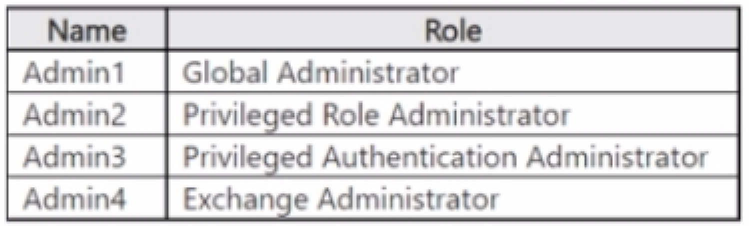


Answer Area

| Statements | Yes | No |
|---|---|---|
| From VM2, you can create a container in storage1. | ○ | [✓ ○] |
| From VM1, you can upload data to the blob storage of storage1. | [✓ ○] | ○ |
| From VM2, you can upload data to the blob storage of storage1. | ○ | [✓ ○] |

**Section:**
**Explanation:**

**QUESTION 47**
You have a Microsoft Entra tenant that uses Microsoft Entra Permissions Management and contains the accounts shown in the following table:



| Name | Role |
|---|---|
| Admin1 | Global Administrator |
| Admin2 | Privileged Role Administrator |
| Admin3 | Privileged Authentication Administrator |
| Admin4 | Exchange Administrator |

Which accounts will be listed as assigned to highly privileged roles on the Azure AD insights tab in the Entra Permissions Management portal?

A. Admin1 only
B. Admin2 and Admin3 only
C. Admin2 and Admin4 only
D. Admin1. Admin2, and Admin3 only
E. Admin2. Admin3, and Admin4 only
F. Admin1. Admin2, Admin3. and Admin4

**Correct Answer: D**
**Section:**

**QUESTION 48**
You have an Azure subscription named Subscription1 that is linked to a Microsoft Entra tenant named contoso.com and a resource group named RG1.
You create a custom role named Role1 in contoso.com.
Where can you use Role1 for permission delegation?

A. contoso.com only

B. contoso.com and RG1 only

C. contoso.com and Subscription 1 only

D. contoso.com. RG1. and Subscription!

**Correct Answer: D**
**Section:**

**QUESTION 49**

You have an Azure subscription that contains a SQL Server on Azure Virtual Machines instance named SQt1 and a Microsoft Sentinel workspace named Sentinel1.
You need to monitor security incidents on SQL1 by using Sentinel1.
What should you do first?

A. On SQL1, enable SQL1 Server audit.

B. On SQL1. install the Connected Machine agent for Azure Arc-enabled servers.

C. From the Azure portal, create a Log Analytics workspace.

D. From Sentinel1, enable VM insights.

**Correct Answer: A**
**Section:**