**Microsoft.AZ-500.vDec-2023.by.Lazyo.168q**

Number: AZ-500
Passing Score: 800
Time Limit: 120
File Version: 21.0

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

**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

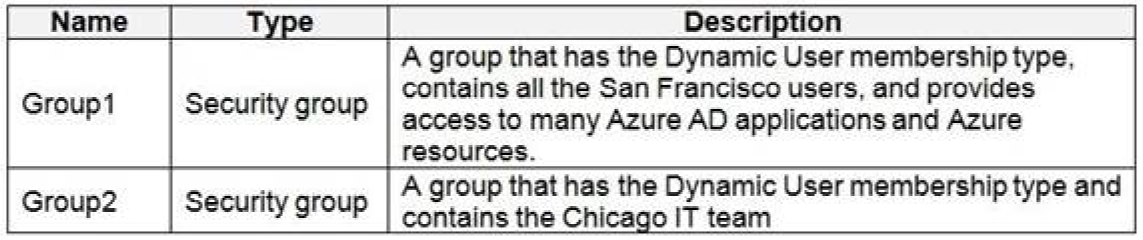
Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment

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

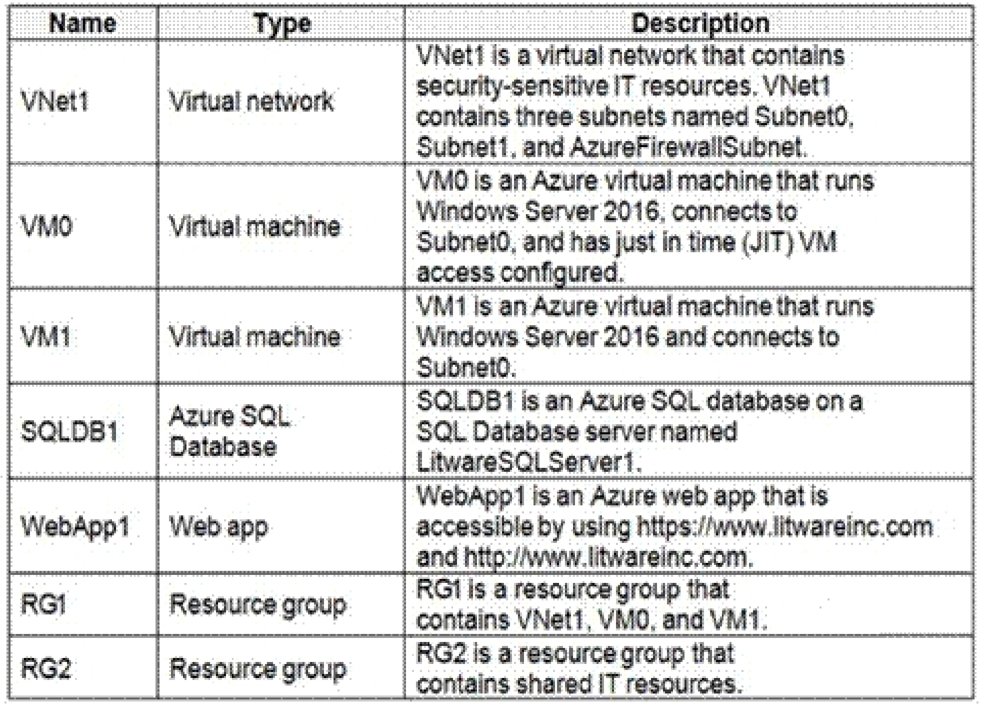
Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD
Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

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.



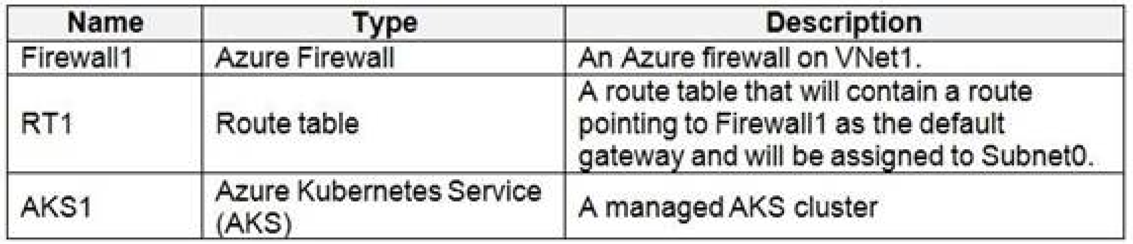
| Name | Type | Description |
|---|---|---|
| VNet1 | Virtual network | VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet. |
| VM0 | Virtual machine | VM0 is an Azure virtual machine that runs Windows 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.



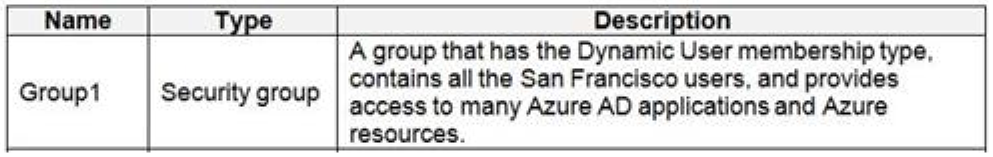
| Name | Type | Description |
|---|---|---|
| Firewall1 | Azure Firewall | An Azure firewall on VNet1. |
| RT1 | Route table | A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0. |
| AKS1 | Azure Kubernetes Service (AKS) | A managed AKS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

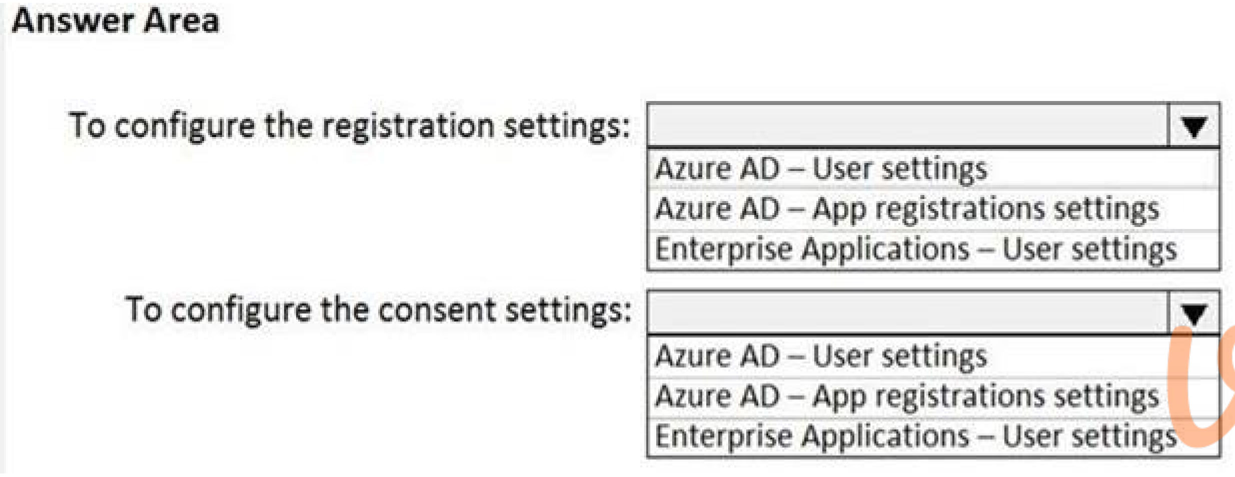
**QUESTION 2**

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:**

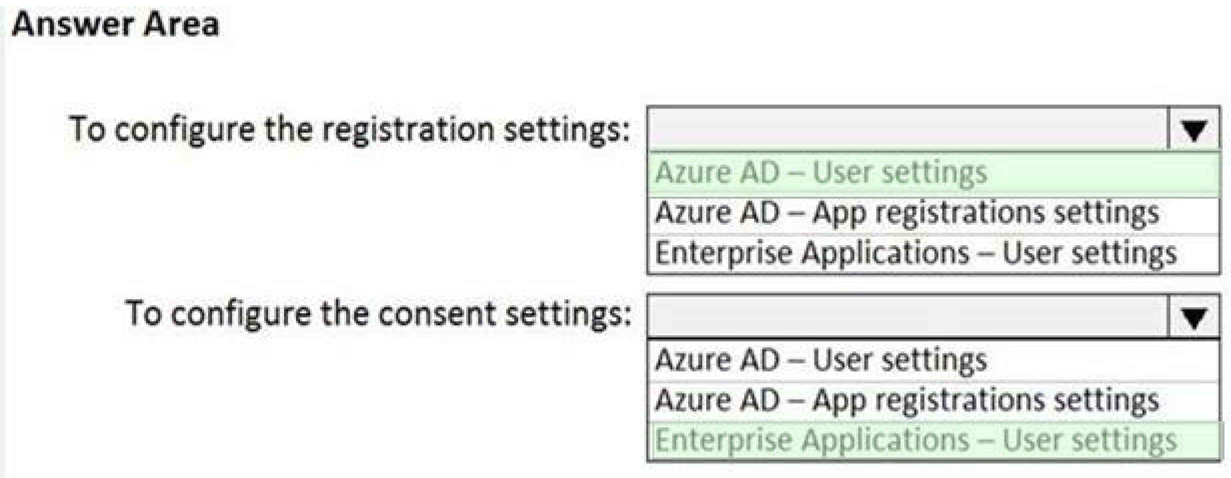


Answer Area

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.

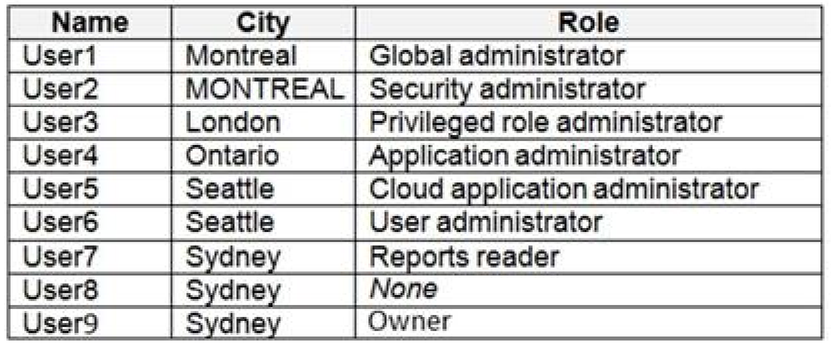
The company hosts its entire server infrastructure in Azure.

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

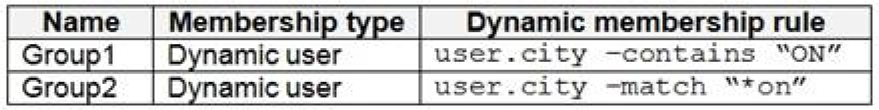
Azure AD

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.

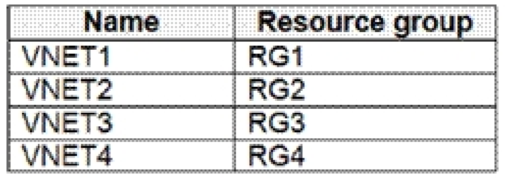


| Name | Membership type | Dynamic membership rule |
|---|---|---|
| Group1 | Dynamic user | `user.city -contains “ON”` |
| Group2 | Dynamic user | `user.city -match “*on”` |

Sub1

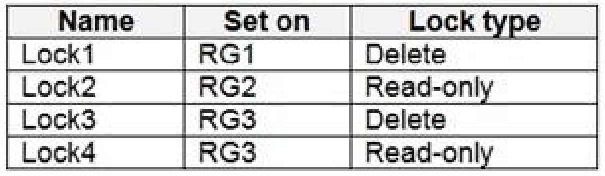
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.



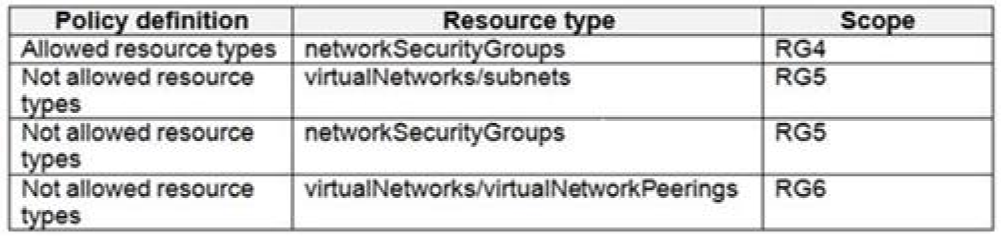
| Name | Resource group |
|---|---|
| VNET1 | RG1 |
| VNET2 | RG2 |
| VNET3 | RG3 |
| VNET4 | RG4 |

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 |

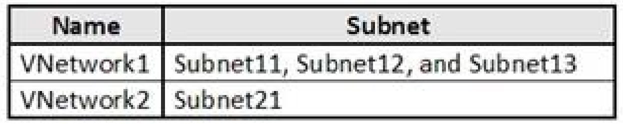
Sub1 contains the Azure policies shown in the following table.



| 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 |

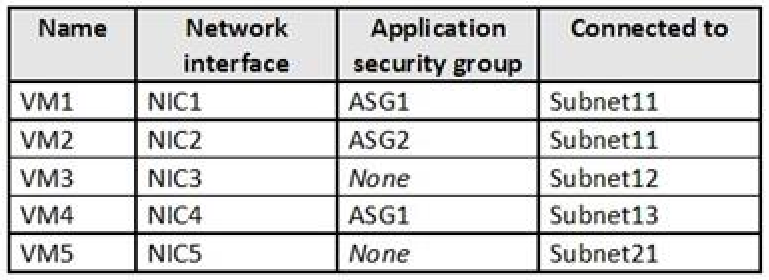
Sub2

Sub2 contains the virtual networks shown in the following table.



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

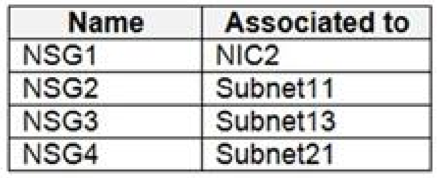
Sub2 contains the virtual machines shown in the following table.



| 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 |

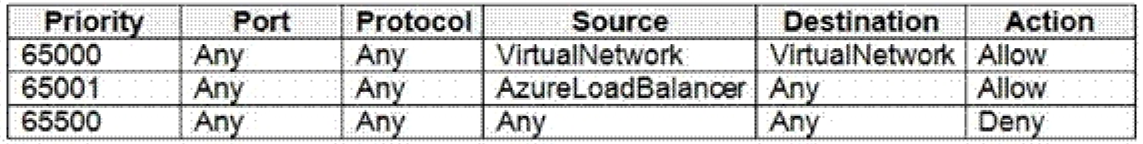
All virtual machines have public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

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



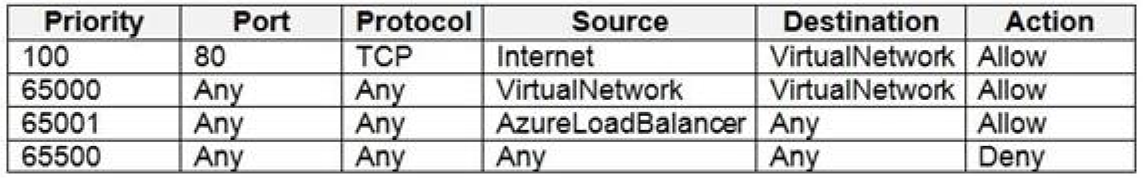
| Name | Associated to |
|---|---|
| NSG1 | NIC2 |
| NSG2 | Subnet11 |
| NSG3 | Subnet13 |
| NSG4 | Subnet21 |

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



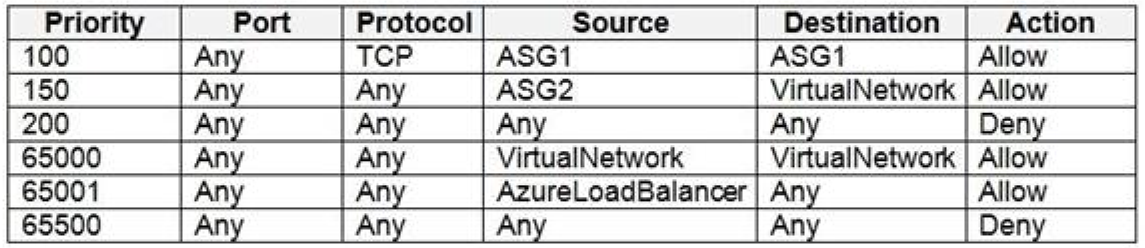
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

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



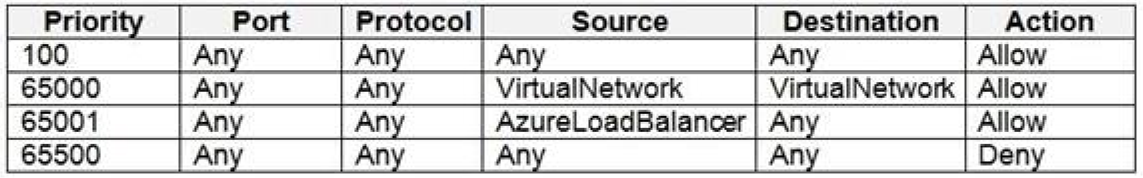
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 100 | 80 | TCP | Internet | VirtualNetwork | Allow |
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny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

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



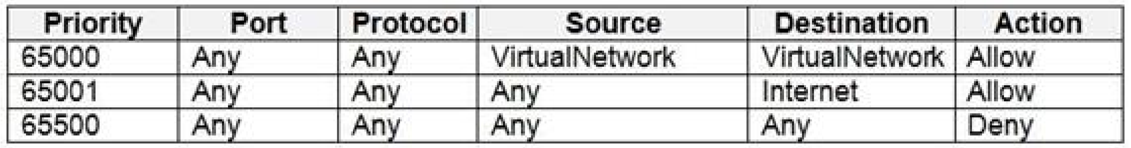
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 100 | Any | TCP | ASG1 | ASG1 | Allow |
| 150 | Any | Any | ASG2 | VirtualNetwork | Allow |
| 200 | Any | Any | Any | Any | Deny |
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any |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

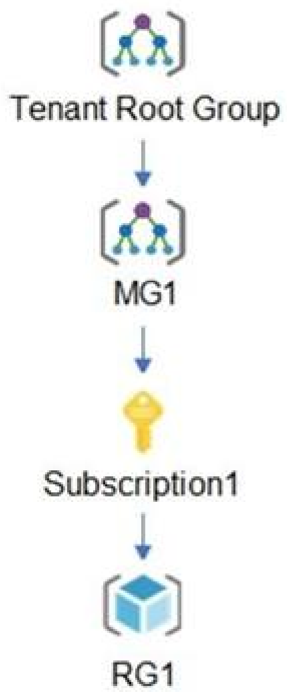
You need to ensure that User2 can implement PIM.
What should you do first?

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.

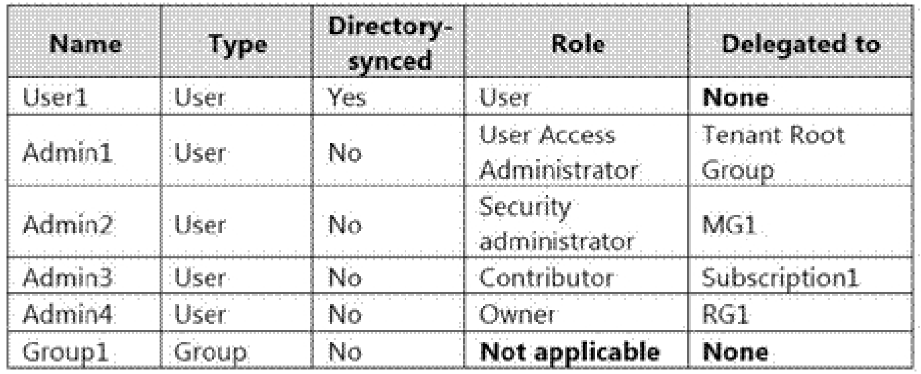
**Correct Answer: A**
**Section:**
**Explanation:**
To start using PIM in your directory, you must first enable PIM.
1. Sign in to the Azure portal as a Global Administrator of your directory.
You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft 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.

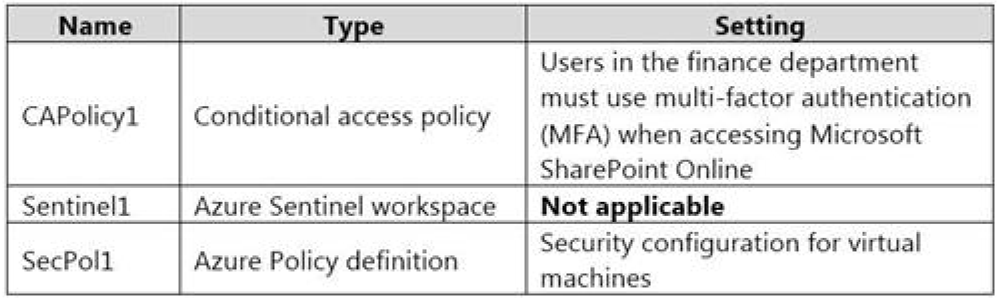


The Azure Active Directory (Azure AD) tenant contains the users shown in the following table.



| 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** |

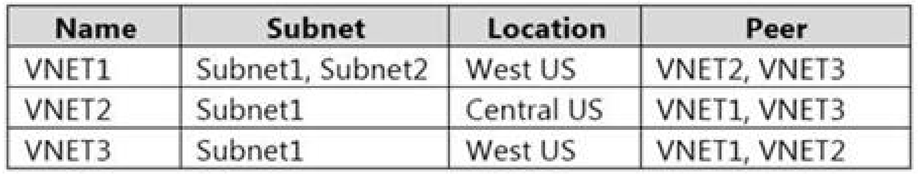
Azure AD contains the resources shown in the following table.



| 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 |

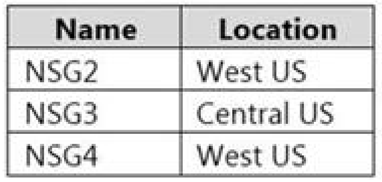
Subscription1 Resources

Subscription1 contains the virtual networks shown in the following table.



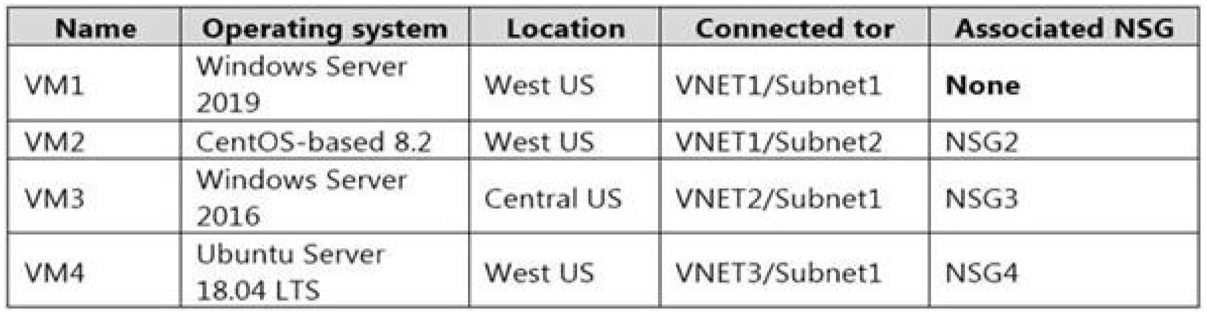
| Name | Subnet | Location | Peer |
|---|---|---|---|
| VNET1 | Subnet1, Subnet2 | West US | VNET2, VNET3 |
| VNET2 | Subnet1 | Central US | VNET1, VNET3 |
| VNET3 | Subnet1 | West US | VNET1, VNET2 |

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



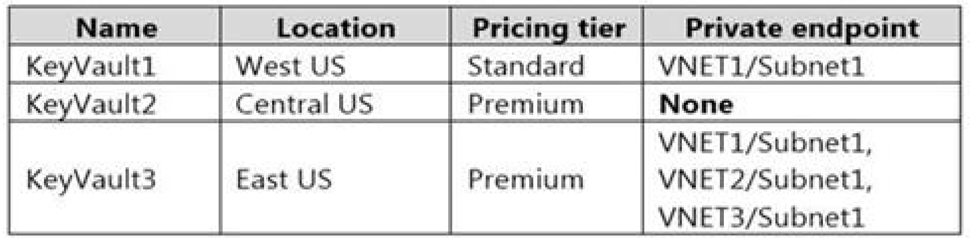
| Name | Location |
|---|---|
| NSG2 | West US |
| NSG3 | Central US |
| NSG4 | West US |

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 |

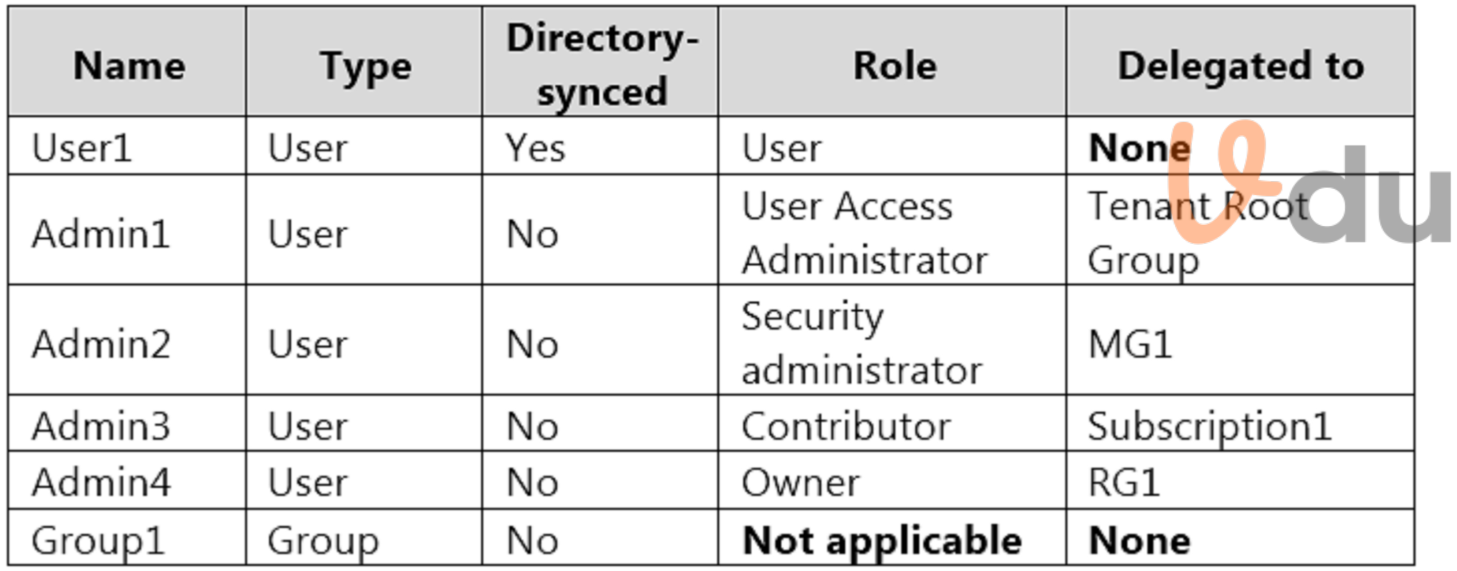
Subscription1 contains a storage account named storage1 in the West US Azure region.

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.

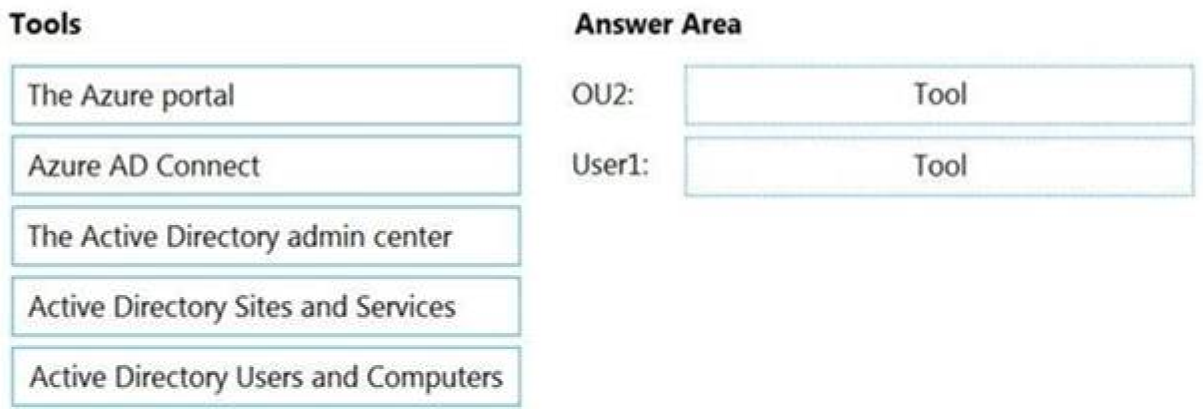
**QUESTION 1**

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**

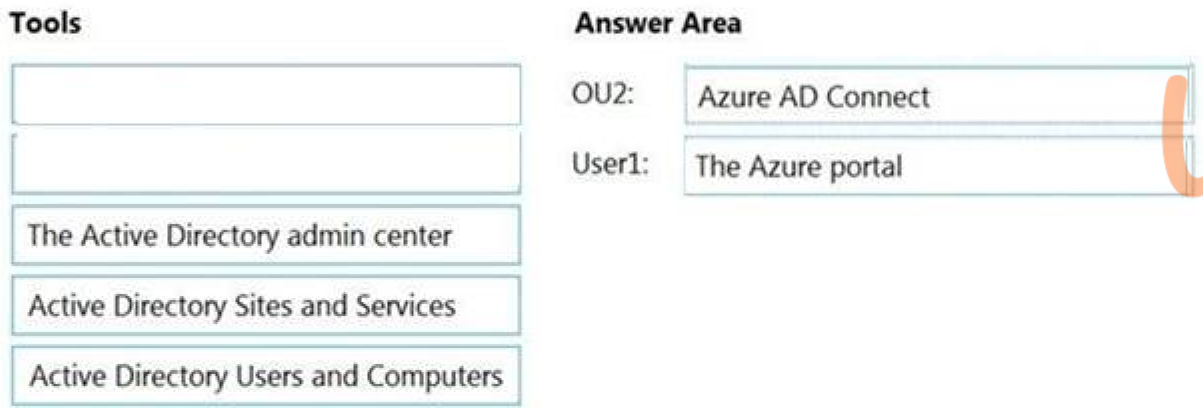
- The Azure portal
- Azure AD Connect
- The Active Directory admin center
- Active Directory Sites and Services
- Active Directory Users and Computers

**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**

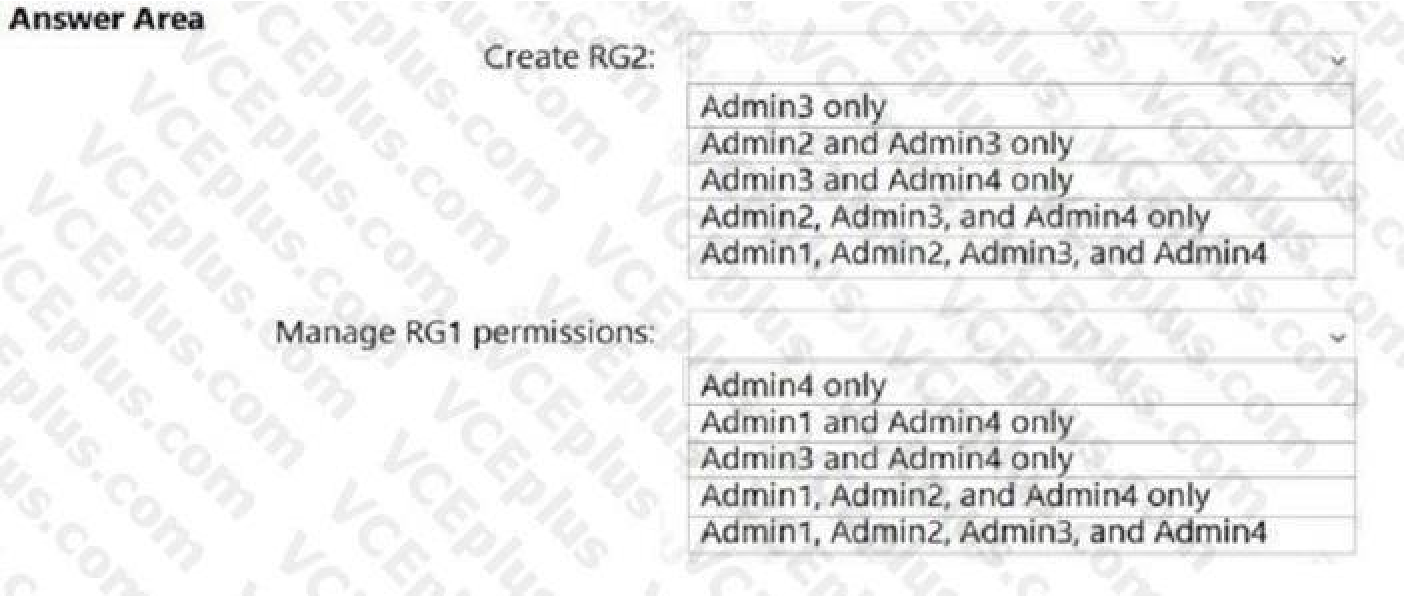
HOTSPOT

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**

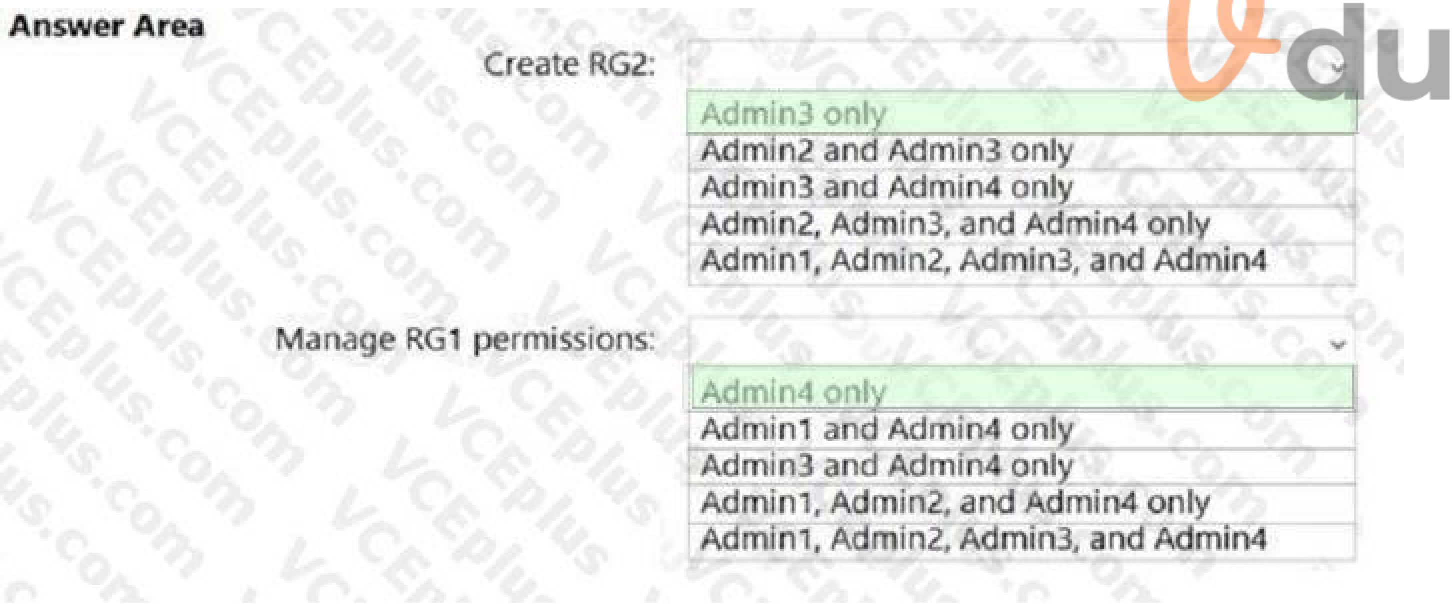
Create RG2:

- 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.

**04 - Manage identity and access**

**QUESTION 1**

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.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies. You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to Sa1.
Solution: You create a new stored access policy.
Does this meet the goal?

A. Yes
B. No

**Correct Answer: B**
**Section:**
**Explanation:**
Creating a new (additional) stored access policy with have no effect on the existing policy or the SAS's linked to it. To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately effects all of the shared access signatures associated with it. References: https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

**QUESTION 2**
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 a hybrid configuration of Azure Active Directory (AzureAD).
You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.
Solution: You deploy the On-premises data gateway to the on-premises network.
Does this meet the goal?

A. Yes
B. No

**Correct Answer: B**
**Section:**
**Explanation:**
Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway. Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions: Create Azure Virtual Network. Create a custom DNS server in the Azure Virtual Network.
Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver. Configure forwarding between the custom DNS server and your on-premises DNS server. References: https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

**QUESTION 3**
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 a hybrid configuration of Azure Active Directory (AzureAD).
You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.
Solution: You create a site-to-site VPN between the virtual network and the on-premises network.
Does this meet the goal?

A. Yes
B. No

**Correct Answer: A**
**Section:**
**Explanation:**
You can connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway. Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions: Create Azure Virtual Network. Create a custom DNS server in the Azure Virtual Network.
Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver. Configure forwarding between the custom DNS server and your on-premises DNS server. References: https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

**QUESTION 4**
Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant.
You need to recommend an integration solution that meets the following requirements:
Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant Minimizes the number of servers required for the solution. Which authentication method should you include in the recommendation?

A. federated identity with Active Directory Federation Services (AD FS)
B. password hash synchronization with seamless single sign-on (SSO)
C. pass-through authentication with seamless single sign-on (SSO)

**Correct Answer: B**
**Section:**
**Explanation:**
Password hash synchronization requires the least effort regarding deployment, maintenance, and infrastructure. This level of effort typically applies to organizations that only need their users to sign in to Office 365, SaaS apps, and other Azure AD-based resources. When turned on, password hash synchronization is part of the Azure AD Connect sync process and runs every two minutes. Incorrect Answers:
A: A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load. C: For pass-through authentication, you need one or more (we recommend three) lightweight agents installed on existing servers. These agents must have access to your on-premises Active Directory Domain Services, including your onpremises AD domain controllers. They need outbound access to the Internet and access to your domain controllers. For this reason, it's not supported to deploy the agents in a perimeter network. Pass-through Authentication requires unconstrained network access to domain controllers. All network traffic is encrypted and limited to authentication requests. References: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

**QUESTION 5**
Your network contains an on-premises Active Directory domain named corp.contoso.com.
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. You sync all on-premises identities to Azure AD.
You need to prevent users who have a givenName attribute that starts with TEST from being synced to Azure AD. The solution must minimize administrative effort. What should you use?

A. Synchronization Rules Editor
B. Web Service Configuration Tool
C. the Azure AD Connect wizard
D. Active Directory Users and Computers

**Correct Answer: A**
**Section:**
**Explanation:**
Use the Synchronization Rules Editor and write attribute-based filtering rule.
References: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

**QUESTION 6**

Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.
You need to configure each subscription to have the same role assignments.
What should you use?

A. Azure Security Center
B. Azure Policy
C. Azure AD Privileged Identity Management (PIM)
D. Azure Blueprints

**Correct Answer: D**
**Section:**
**Explanation:**
Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements.
Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:
Role Assignments
Policy Assignments
Azure Resource Manager templates
Resource Groups
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

**QUESTION 7**

You have an Azure subscription.
You create an Azure web app named Contoso1812 that uses an S1 App Service plan.
You plan to create a CNAME DNS record for www.contoso.com that points to Contoso1812.
You need to ensure that users can access Contoso1812 by using the https://www.contoso.com URL.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Turn on the system-assigned managed identity for Contoso1812.
B. Add a hostname to Contoso1812.
C. Scale out the App Service plan of Contoso1812.
D. Add a deployment slot to Contoso1812.
E. Scale up the App Service plan of Contoso1812.
F. Upload a PFX file to Contoso1812.

**Correct Answer: B, F**
**Section:**
**Explanation:**
B: You can configure Azure DNS to host a custom domain for your web apps. For example, you can create an Azure web app and have your users access it using either www.contoso.com or contoso.com as a fully qualified domain name (FQDN).
To do this, you have to create three records:
A root "A" record pointing to contoso.com
A root "TXT" record for verification
A "CNAME" record for the www name that points to the A record
F: To use HTTPS, you need to upload a PFX file to the Azure Web App. The PFX file will contain the SSL certificate required for HTTPS.
References:

https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain

**QUESTION 8**

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.

You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies. You discover that unauthorized users accessed both the file service and the blob service.

You need to revoke all access to Sa1.

Solution: You create a lock on Sa1.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

**Section:**

**Explanation:**

To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it. References:

https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

**QUESTION 9**

DRAG DROP

You are implementing conditional access policies.

You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.

You need to identify the risk level of the following risk events:

Users with leaked credentials

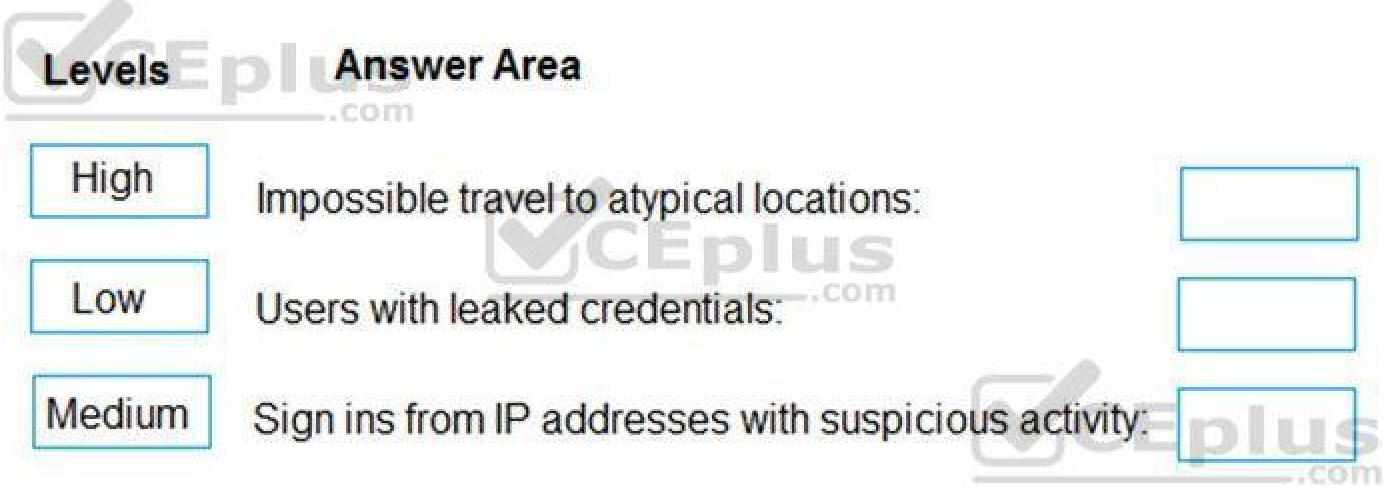
Impossible travel to atypical locations

Sign ins from IP addresses with suspicious activity

Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level 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:**



Levels

Answer Area

High

Low

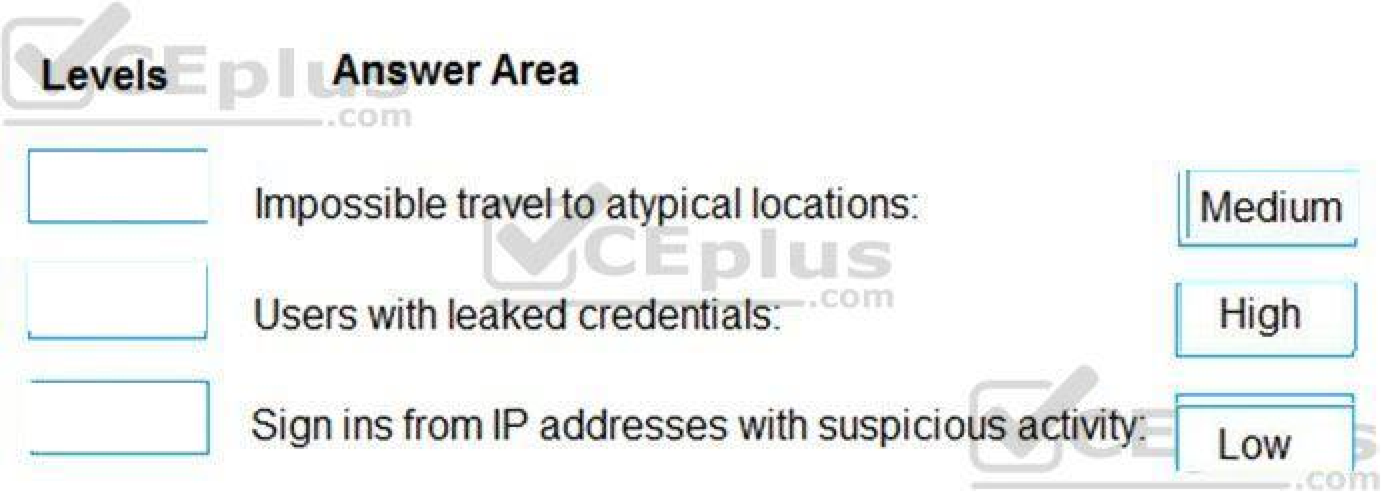
Medium

Impossible travel to atypical locations:

Users with leaked credentials:

Sign ins from IP addresses with suspicious activity:

**Correct Answer:**

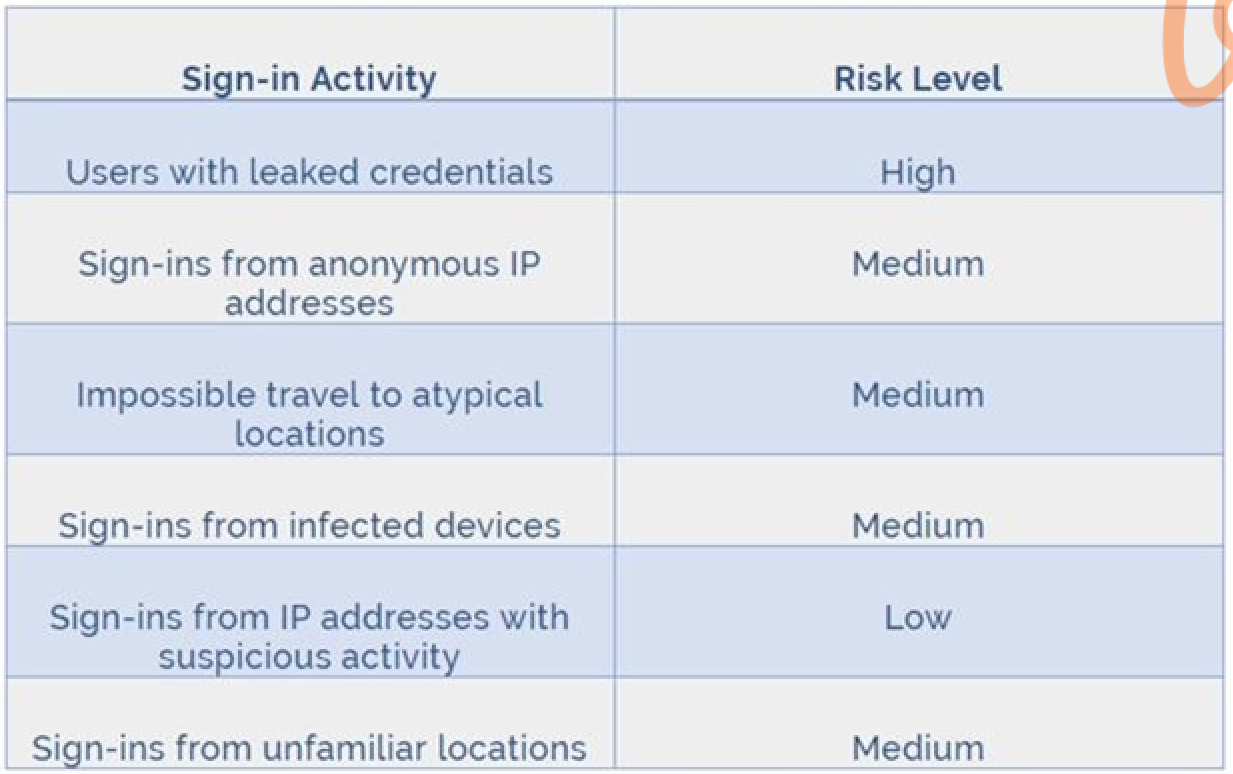


Levels

Answer Area

| | | |
|---|---|---|
| | Impossible travel to atypical locations: | Medium |
| | Users with leaked credentials: | High |
| | Sign ins from IP addresses with suspicious activity: | Low |

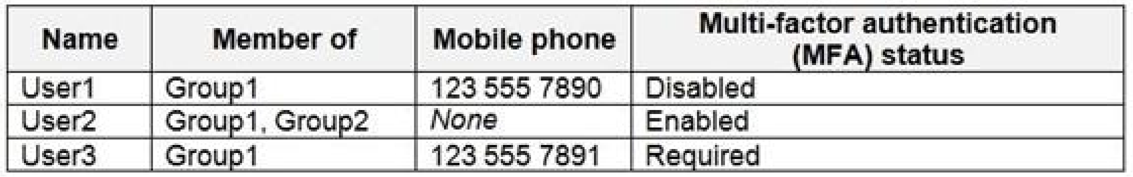
**Section:**
**Explanation:**
Azure AD Identity protection can detect six types of suspicious sign-in activities:
Users with leaked credentials
Sign-ins from anonymous IP addresses
Impossible travel to atypical locations
Sign-ins from infected devices
Sign-ins from IP addresses with suspicious activity
Sign-ins from unfamiliar locations
These six types of events are categorized in to 3 levels of risks – High, Medium & Low:



| Sign-in Activity | Risk Level |
|---|---|
| Users with leaked credentials | High |
| Sign-ins from anonymous IP addresses | Medium |
| Impossible travel to atypical locations | Medium |
| Sign-ins from infected devices | Medium |
| Sign-ins from IP addresses with suspicious activity | Low |
| Sign-ins from unfamiliar locations | Medium |

References:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/

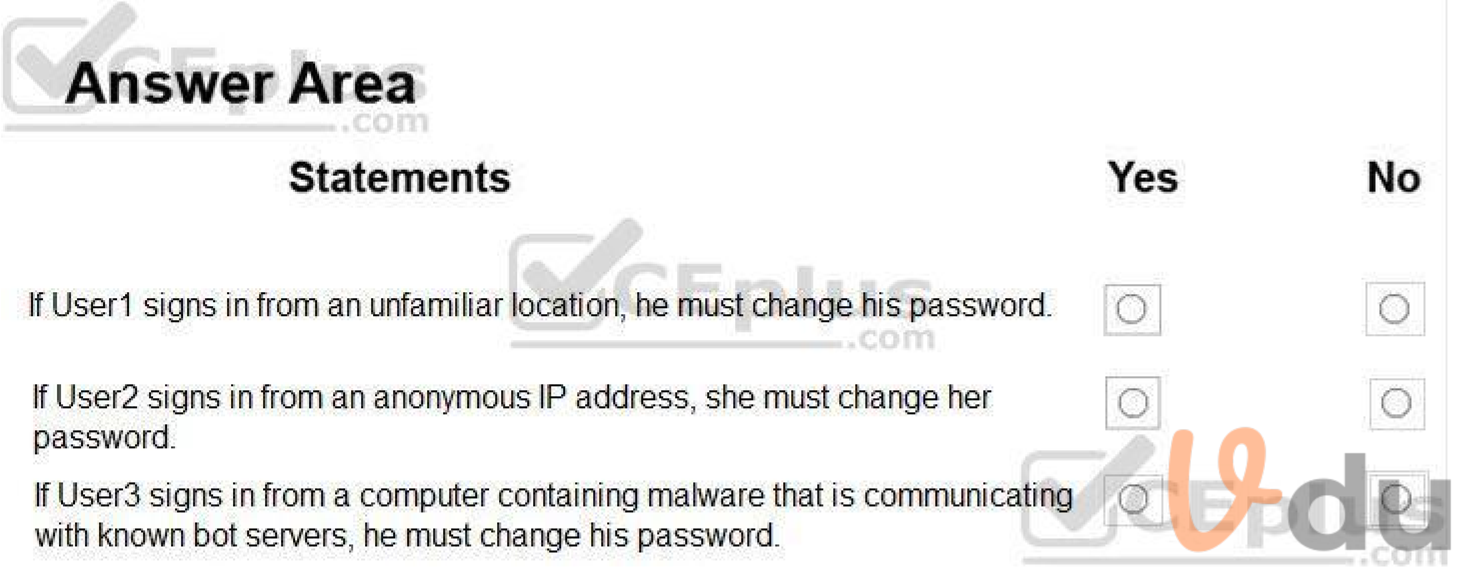
**QUESTION 10**
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.



| Name | Member of | Mobile phone | Multi-factor authentication (MFA) status |
|---|---|---|---|
| User1 | Group1 | 123 555 7890 | Disabled |
| User2 | Group1, Group2 | *None* | Enabled |
| User3 | Group1 | 123 555 7891 | Required |

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:
Assignment: Include Group1, Exclude Group2
Conditions: Sign-in risk of Medium and above
Access: Allow access, Require password change
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

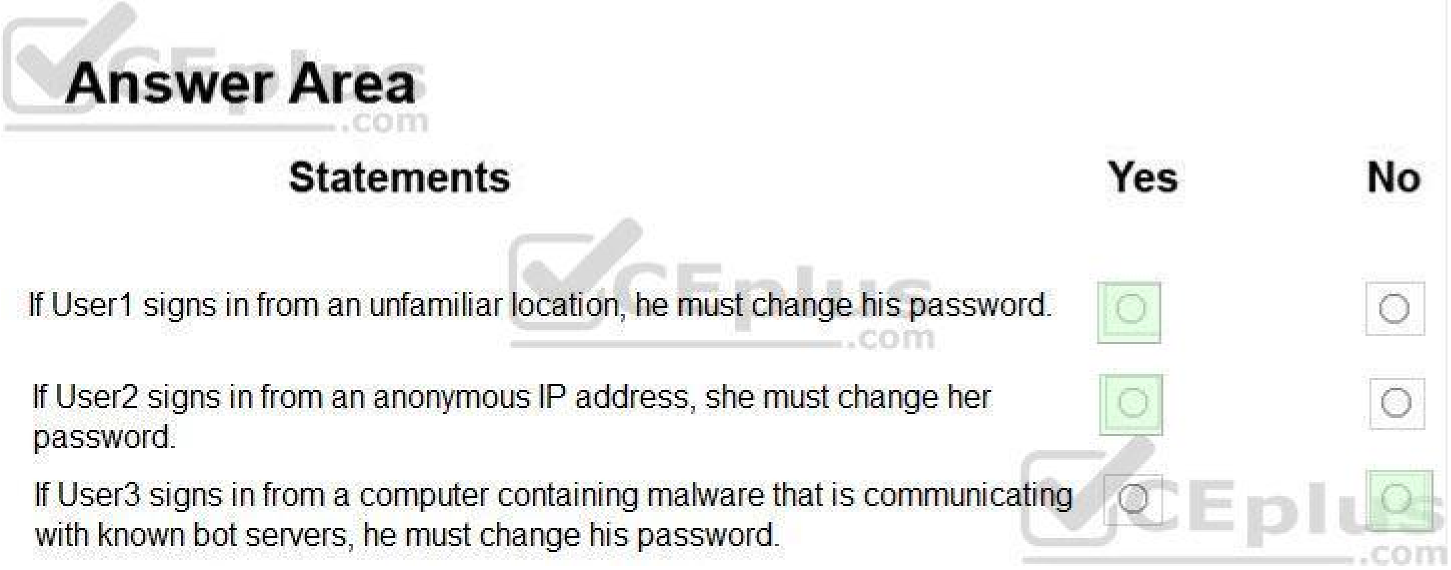
**Hot Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| If User1 signs in from an unfamiliar location, he must change his password. | ○ | ○ |
| If User2 signs in from an anonymous IP address, she must change her password. | ○ | ○ |
| If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password. | ○ | ○ |

**Answer Area:**

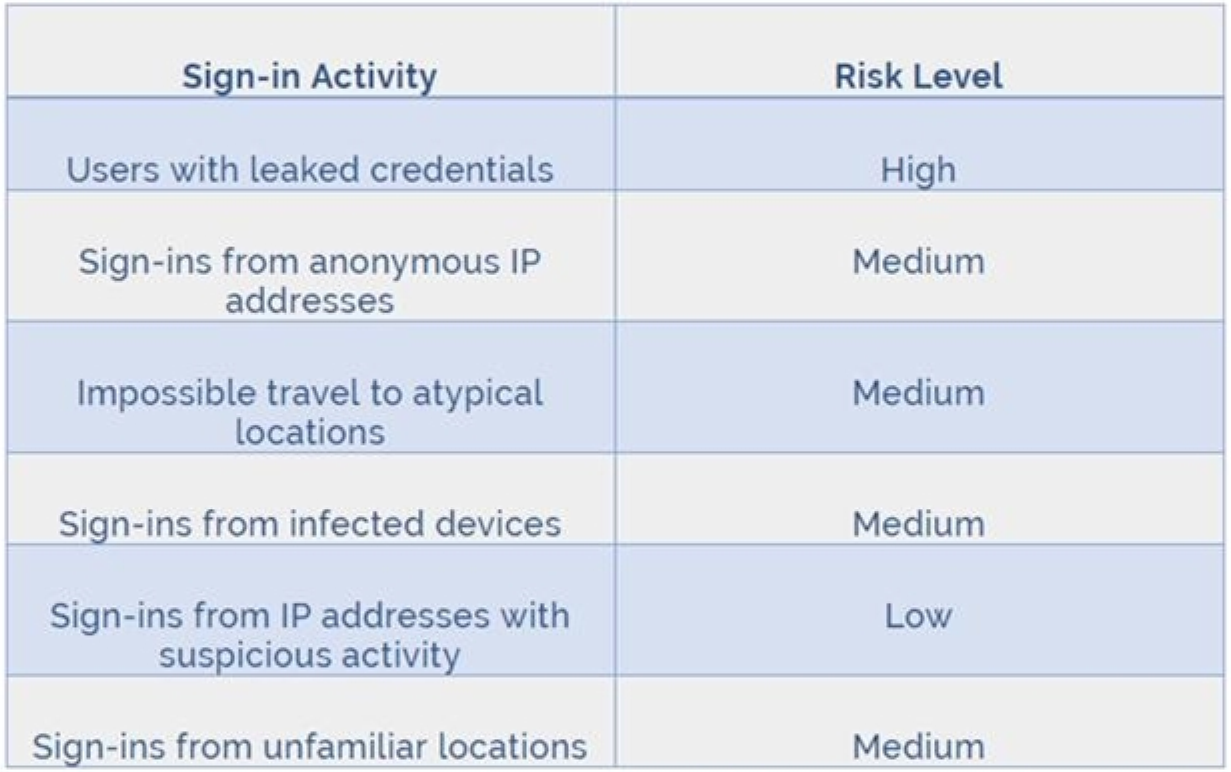


Answer Area

| Statements | Yes | No |
|---|---|---|
| If User1 signs in from an unfamiliar location, he must change his password. | [✓ ○] | ○ |
| If User2 signs in from an anonymous IP address, she must change her password. | [✓ ○] | ○ |
| If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password. | ○ | [✓ ○] |

**Section:**
**Explanation:**
Box 1: Yes
User1 is member of Group1. Sign in from unfamiliar location is risk level Medium.
Box 2: Yes
User2 is member of Group1. Sign in from anonymous IP address is risk level Medium.
Box 3: No

Sign-ins from IP addresses with suspicious activity is low.
Note:



| Sign-in Activity | Risk Level |
|---|---|
| Users with leaked credentials | High |
| Sign-ins from anonymous IP addresses | Medium |
| Impossible travel to atypical locations | Medium |
| Sign-ins from infected devices | Medium |
| Sign-ins from IP addresses with suspicious activity | Low |
| Sign-ins from unfamiliar locations | Medium |

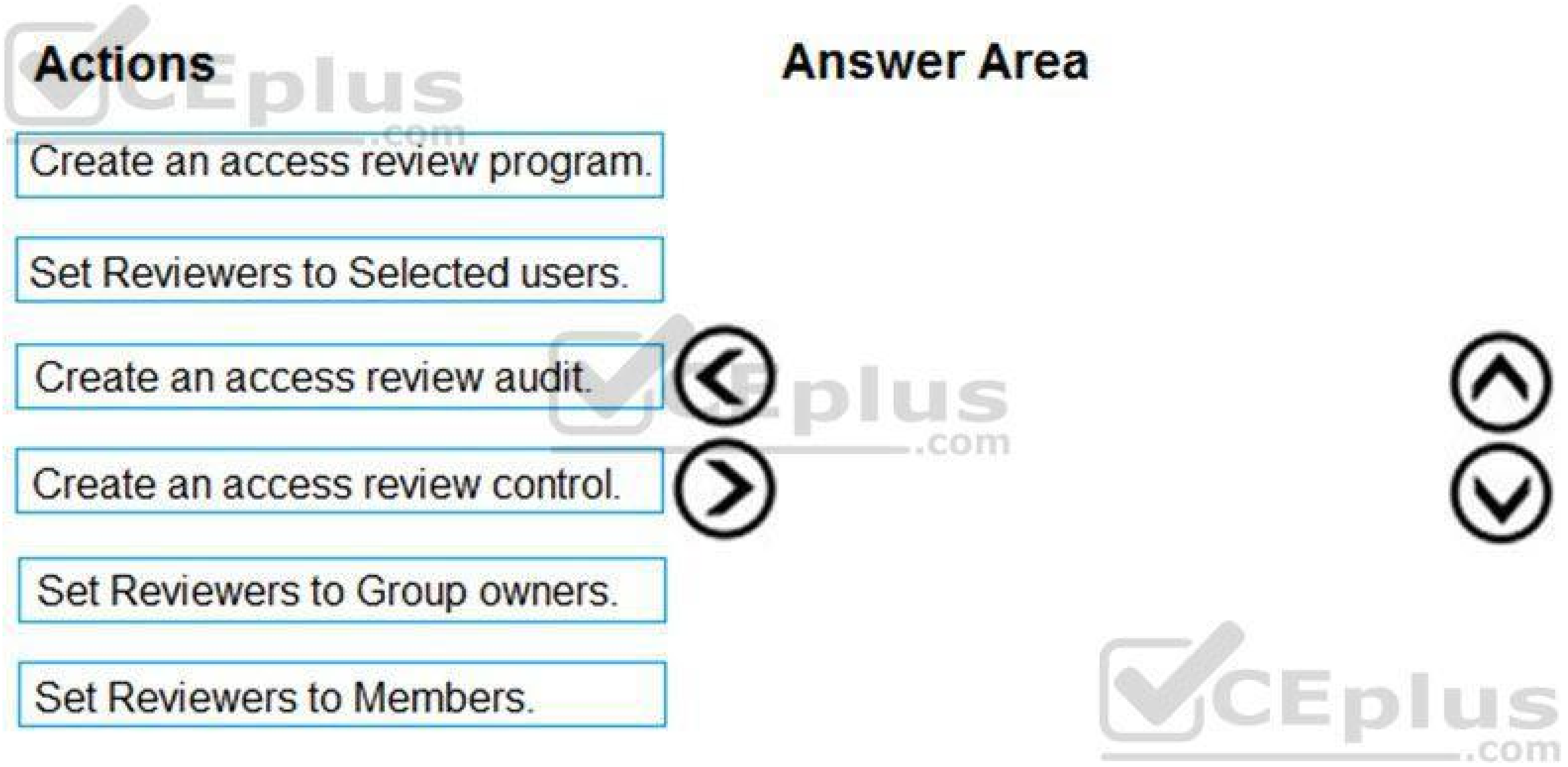
Azure AD Identity protection can detect six types of suspicious sign-in activities:
Users with leaked credentials
Sign-ins from anonymous IP addresses
Impossible travel to atypical locations
Sign-ins from infected devices
Sign-ins from IP addresses with suspicious activity
Sign-ins from unfamiliar locations
These six types of events are categorized in to 3 levels of risks – High, Medium & Low:
References:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/

**QUESTION 11**

DRAG DROP

You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.
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 an access review program.

Set Reviewers to Selected users.

Create an access review audit.

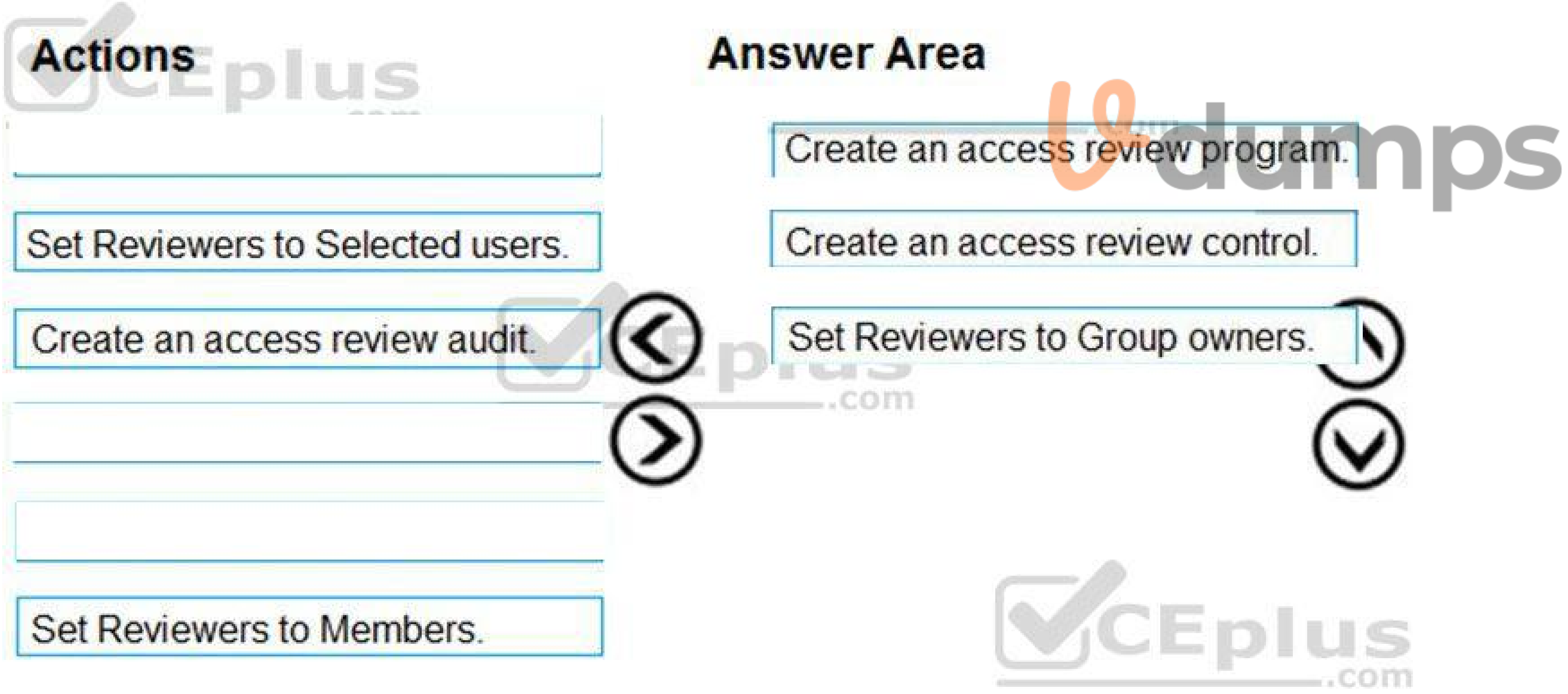
Create an access review control.

Set Reviewers to Group owners.

Set Reviewers to Members.

Answer Area

**Correct Answer:**



Actions

Set Reviewers to Selected users.

Create an access review audit.

Set Reviewers to Members.

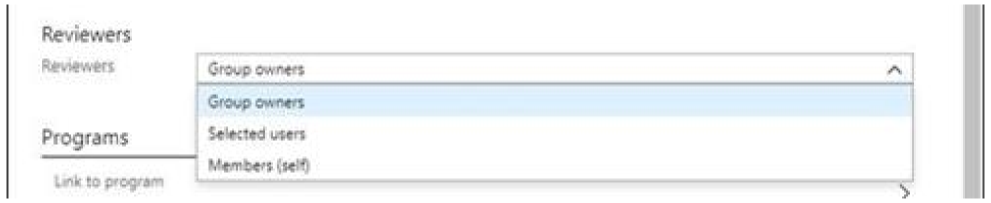
Answer Area

Create an access review program.

Create an access review control.

Set Reviewers to Group owners.

**Section:**
**Explanation:**
Step 1: Create an access review program
Step 2: Create an access review control
Step 3: Set Reviewers to Group owners
In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.



Reviewers

Reviewers: Group owners

- Group owners
- Selected users
- Members (self)

Programs

Link to program

References:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review
https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls

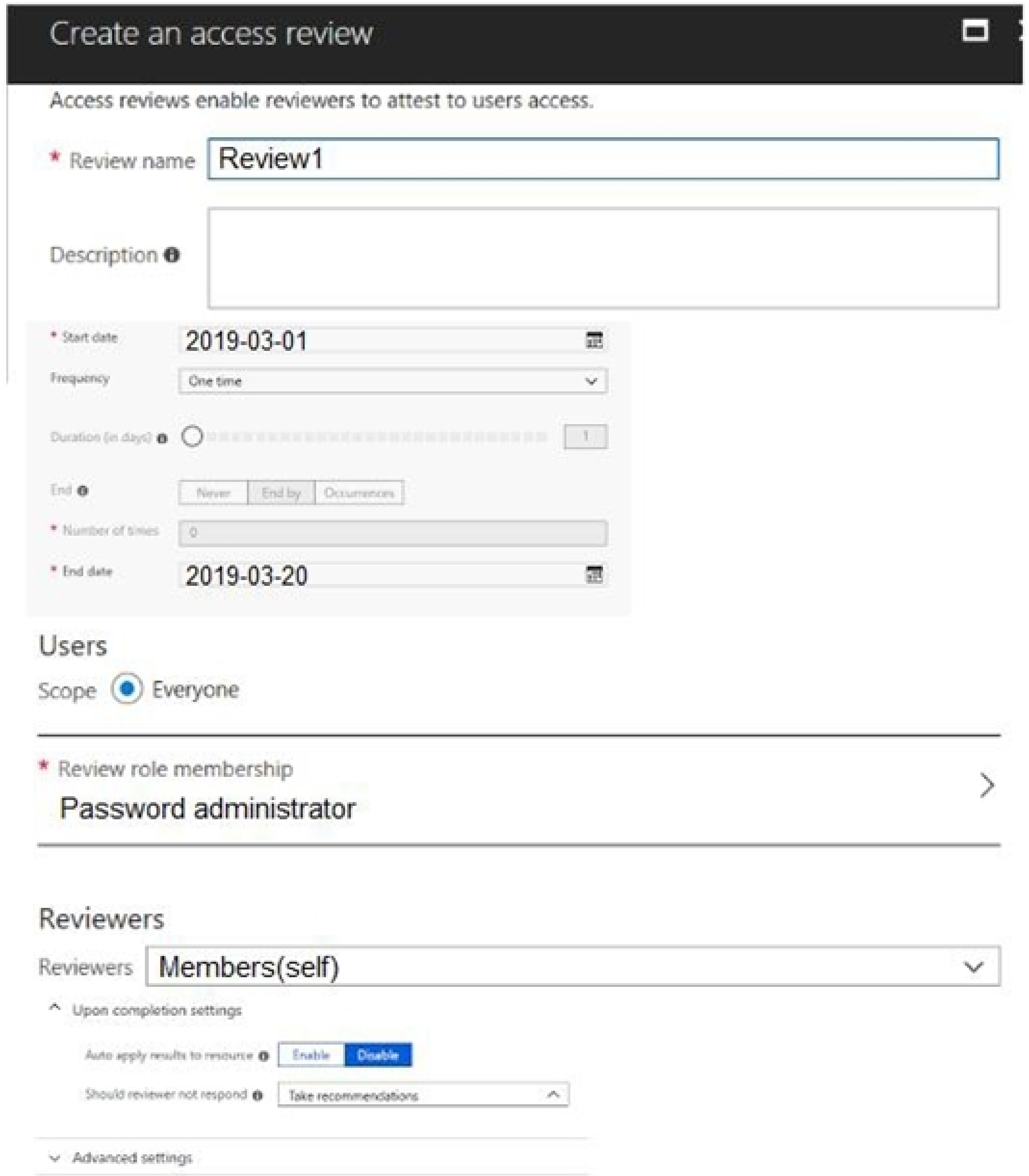
**QUESTION 12**

HOTSPOT

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

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

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



Create an access review

Access reviews enable reviewers to attest to users access.

* Review name: Review1

Description:

* Start date: 2019-03-01

Frequency: One time

Duration (in days): 1

End: Never | End by | Occurrences

* Number of times: 0

* End date: 2019-03-20

Users

Scope: ● Everyone

* Review role membership: Password administrator

Reviewers

Reviewers: Members(self)

Upon completion settings

Auto apply results to resource: Enable | Disable (selected)

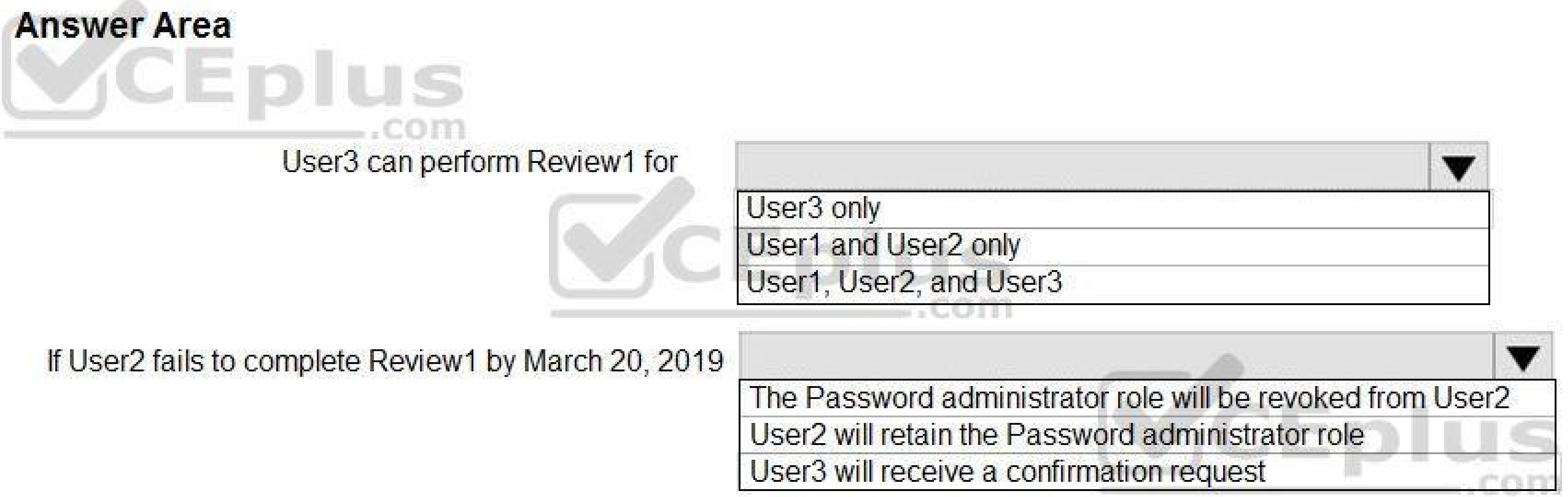
Should reviewer not respond: Take recommendations

Advanced settings

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:**

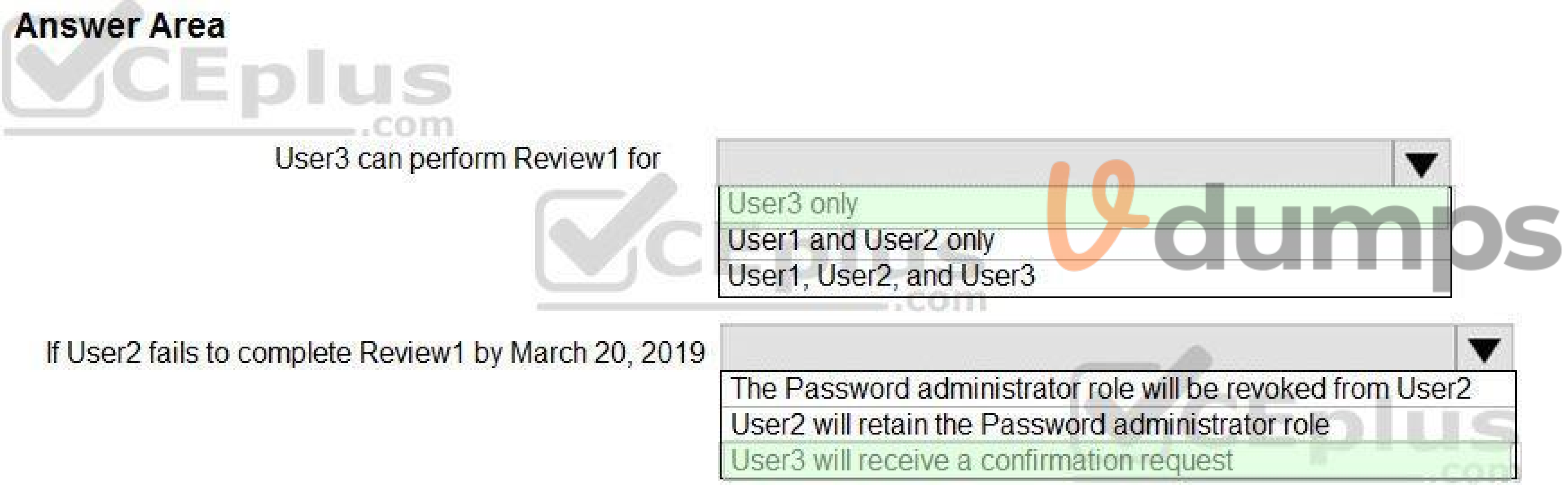


Answer Area

User3 can perform Review1 for
- User3 only
- User1 and User2 only
- User1, User2, and User3

If User2 fails to complete Review1 by March 20, 2019
- The Password administrator role will be revoked from User2
- User2 will retain the Password administrator role
- User3 will receive a confirmation request

**Answer Area:**



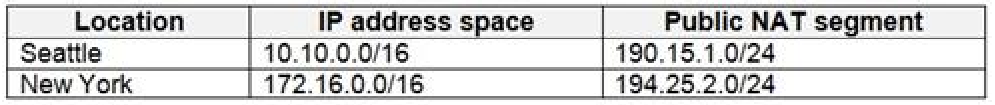
Answer Area

User3 can perform Review1 for
- [✓ User3 only]
- User1 and User2 only
- User1, User2, and User3

If User2 fails to complete Review1 by March 20, 2019
- The Password administrator role will be revoked from User2
- User2 will retain the Password administrator role
- [✓ User3 will receive a confirmation request]

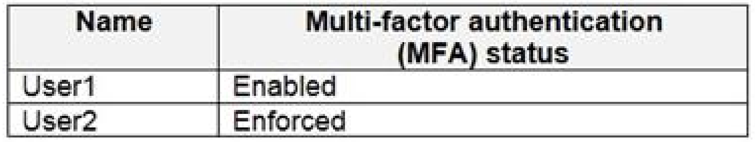
**Section:**
**Explanation:**
Box 1: User3 only
Use the Members (self) option to have the users review their own role assignments.
Box 2: User3 will receive a confirmation request
Use the Should reviewer not respond list to specify what happens for users that are not reviewed by the reviewer within the review period. This setting does not impact users who have been reviewed by the reviewers manually. If the final reviewer's decision is Deny, then the user's access will be removed.
No change - Leave user's access unchanged
Remove access - Remove user's access
Approve access - Approve user's access
Take recommendations - Take the system's recommendation on denying or approving the user's continued access
References:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review

**QUESTION 13**
HOTSPOT
Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.



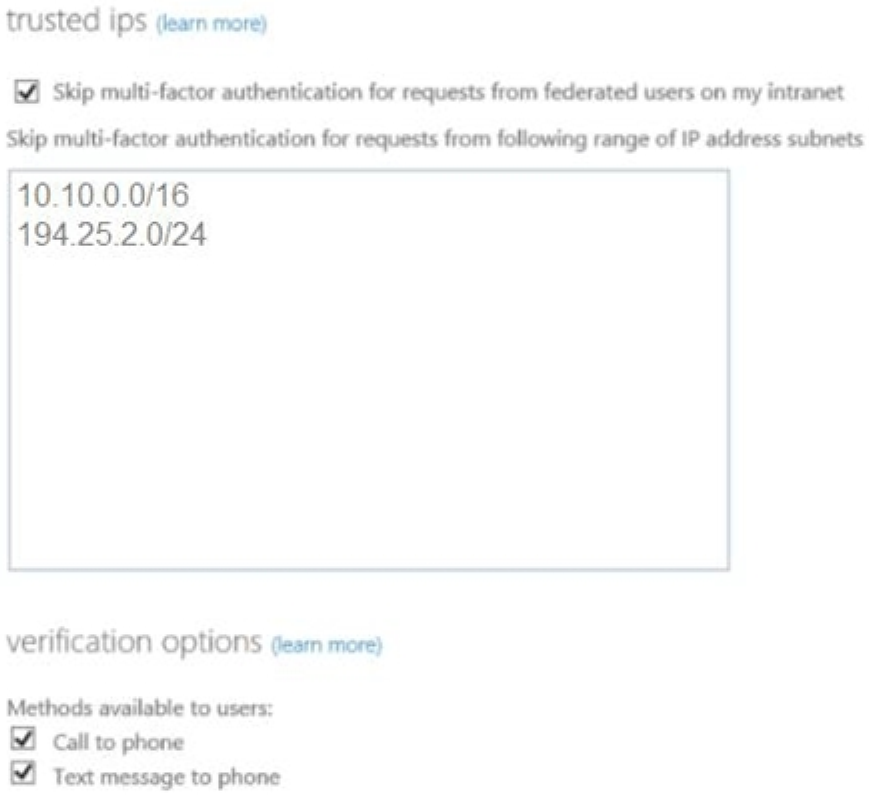
| Location | IP address space | Public NAT segment |
|---|---|---|
| Seattle | 10.10.0.0/16 | 190.15.1.0/24 |
| New York | 172.16.0.0/16 | 194.25.2.0/24 |

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



| Name | Multi-factor authentication (MFA) status |
|---|---|
| User1 | Enabled |
| User2 | Enforced |

The MFA service settings are configured as shown in the exhibit. (Click the Exhibit tab.)



trusted ips (learn more)

☑ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

```
10.10.0.0/16
194.25.2.0/24
```

verification options (learn more)

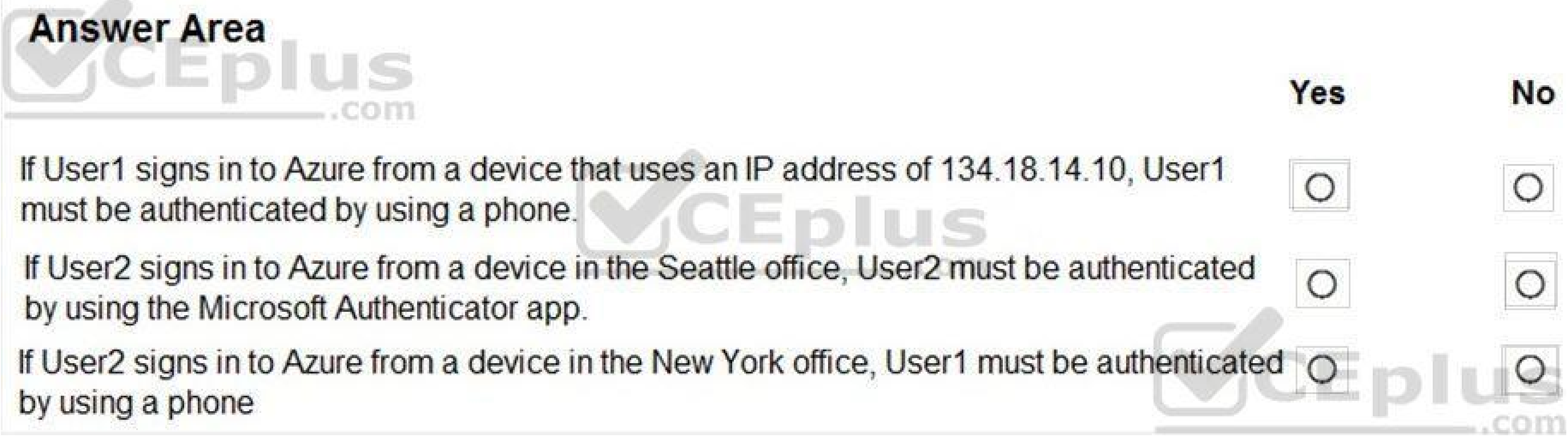
Methods available to users:

☑ Call to phone

☑ Text message to phone

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

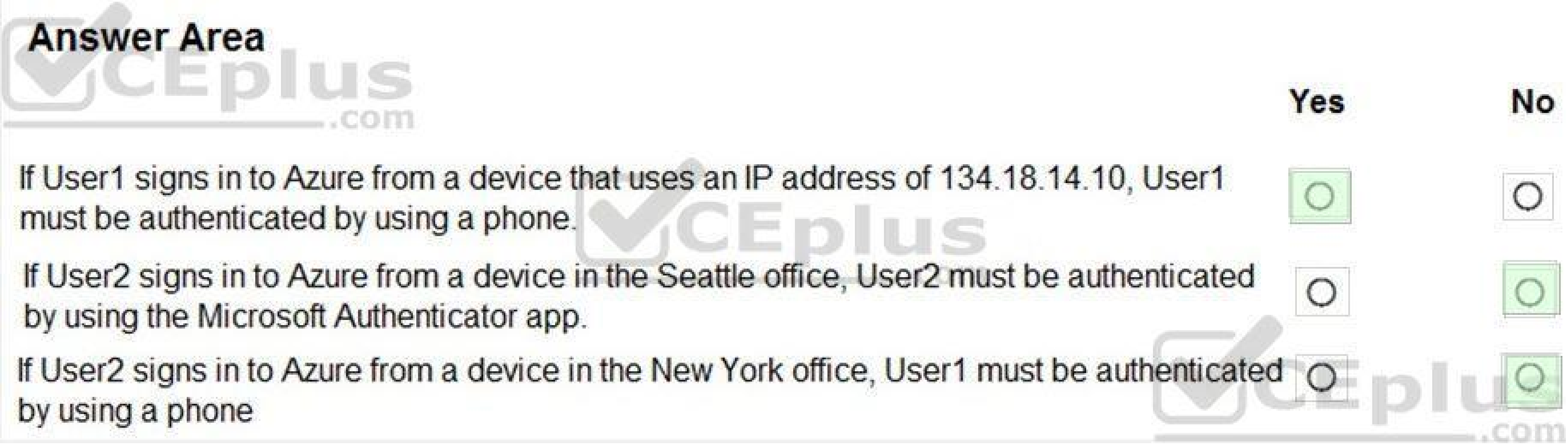
**Hot Area:**



Answer Area

| | Yes | No |
|---|---|---|
| If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone. | ○ | ○ |
| If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app. | ○ | ○ |
| If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone | ○ | ○ |

**Answer Area:**

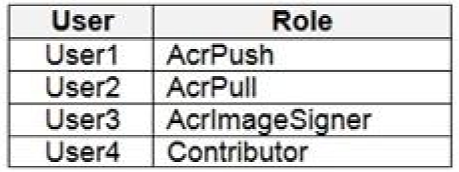


**Answer Area**

| | Yes | No |
|---|---|---|
| If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone. | [✓ ○] | ○ |
| If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app. | ○ | [✓ ○] |
| If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone | ○ | [✓ ○] |

**Section:**
**Explanation:**
Box 2: No
Use of Microsoft Authenticator is not required.
Note: Microsoft Authenticator is a multifactor app for mobile devices that generates time-based codes used during the Two-Step Verification process.
Box 3: No
The New York IP address subnet is included in the "skip multi-factor authentication for request.
References:
https://www.cayosoft.com/difference-enabling-enforcing-mfa/

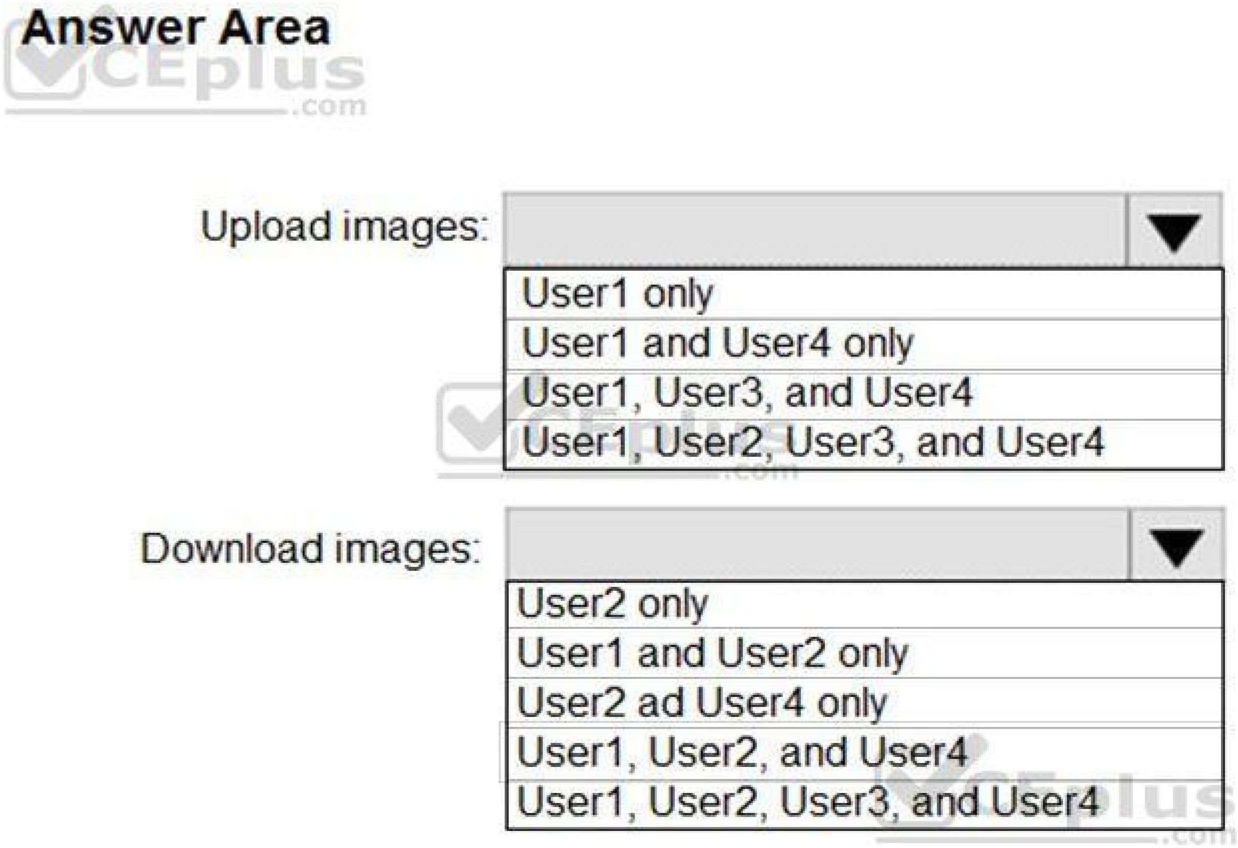
**QUESTION 14**
HOTSPOT
You have an Azure Container Registry named Registry1.
You add role assignment for Registry1 as shown in the following table.



| User | Role |
|---|---|
| User1 | AcrPush |
| User2 | AcrPull |
| User3 | AcrImageSigner |
| User4 | Contributor |

Which users can upload images to Registry1 and download images from Registry1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**



Answer Area

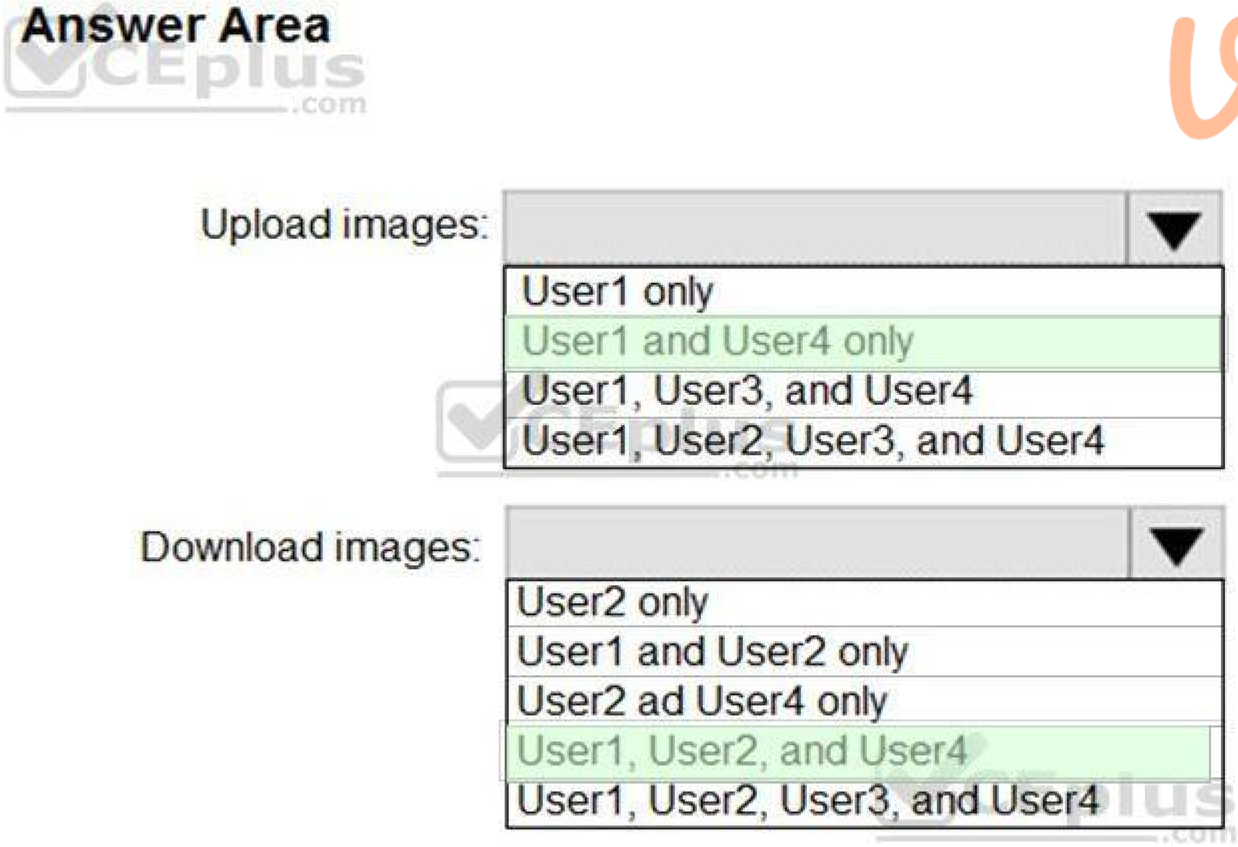
Upload images:

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

Download images:

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

**Answer Area:**



Answer Area

Upload images:

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

Download images:

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

**Section:**

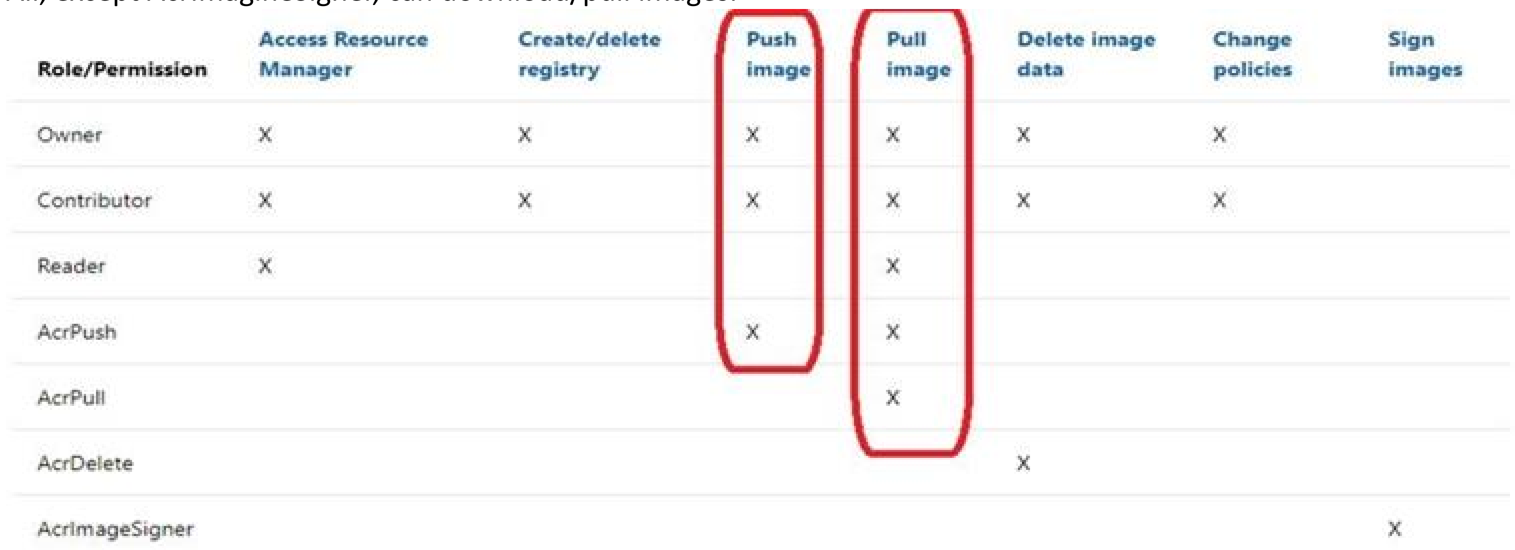
**Explanation:**

Box 1: User1 and User4 only

Owner, Contributor and AcrPush can push images.

Box 2: User1, User2, and User4

All, except AcrImagineSigner, can download/pull images.



| Role/Permission | Access Resource Manager | Create/delete registry | Push image | Pull image | Delete image data | Change policies | Sign images |
|---|---|---|---|---|---|---|---|
| Owner | X | X | X | X | X | X | |
| Contributor | X | X | X | X | X | X | |
| Reader | X | | | X | | | |
| AcrPush | | | X | X | | | |
| AcrPull | | | | X | | | |
| AcrDelete | | | | | X | | |
| AcrImageSigner | | | | | | | X |

References:
https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles

**QUESTION 15**

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 a hybrid configuration of Azure Active Directory (Azure AD).

You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.

You need to configure the environment to support the planned authentication.

Solution: You deploy Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

**Section:**

**Explanation:**

Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:

Create Azure Virtual Network.

Create a custom DNS server in the Azure Virtual Network.

Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver. Configure forwarding between the custom DNS server and your on-premises DNS server.

References:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

**QUESTION 16**

Your network contains an Active Directory forest named contoso.com. You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to configure synchronization by using the Express Settings installation option in Azure AD Connect.

You need to identify which roles and groups are required to perform the planned configurations. The solution must use the principle of least privilege.

Which two roles and groups should you identify? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

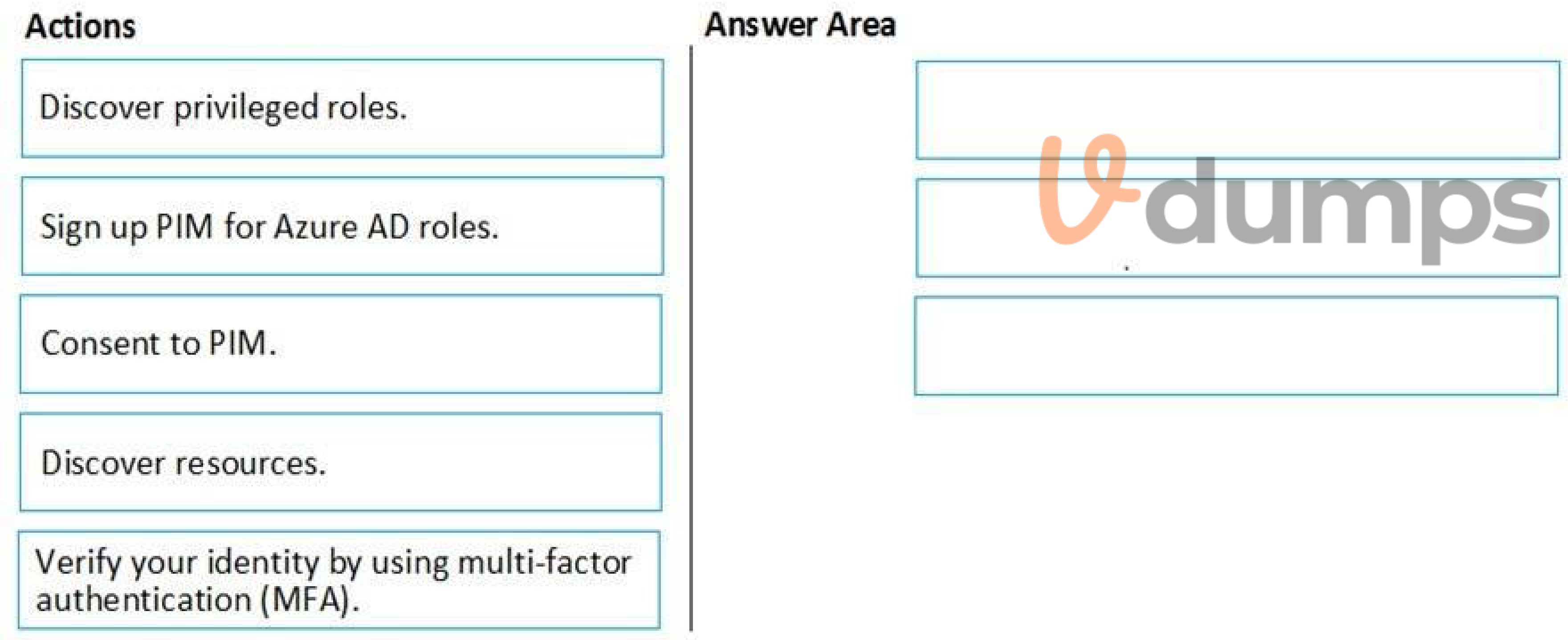
A. the Domain Admins group in Active Directory

B. the Security administrator role in Azure AD
C. the Global administrator role in Azure AD
D. the User administrator role in Azure AD
E. the Enterprise Admins group in Active Directory

**Correct Answer: C, E**
**Section:**
**Explanation:**
References:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

**QUESTION 17**
DRAG DROP
You create an Azure subscription with Azure AD Premium P2.
You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure roles.
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

Discover privileged roles.

Sign up PIM for Azure AD roles.

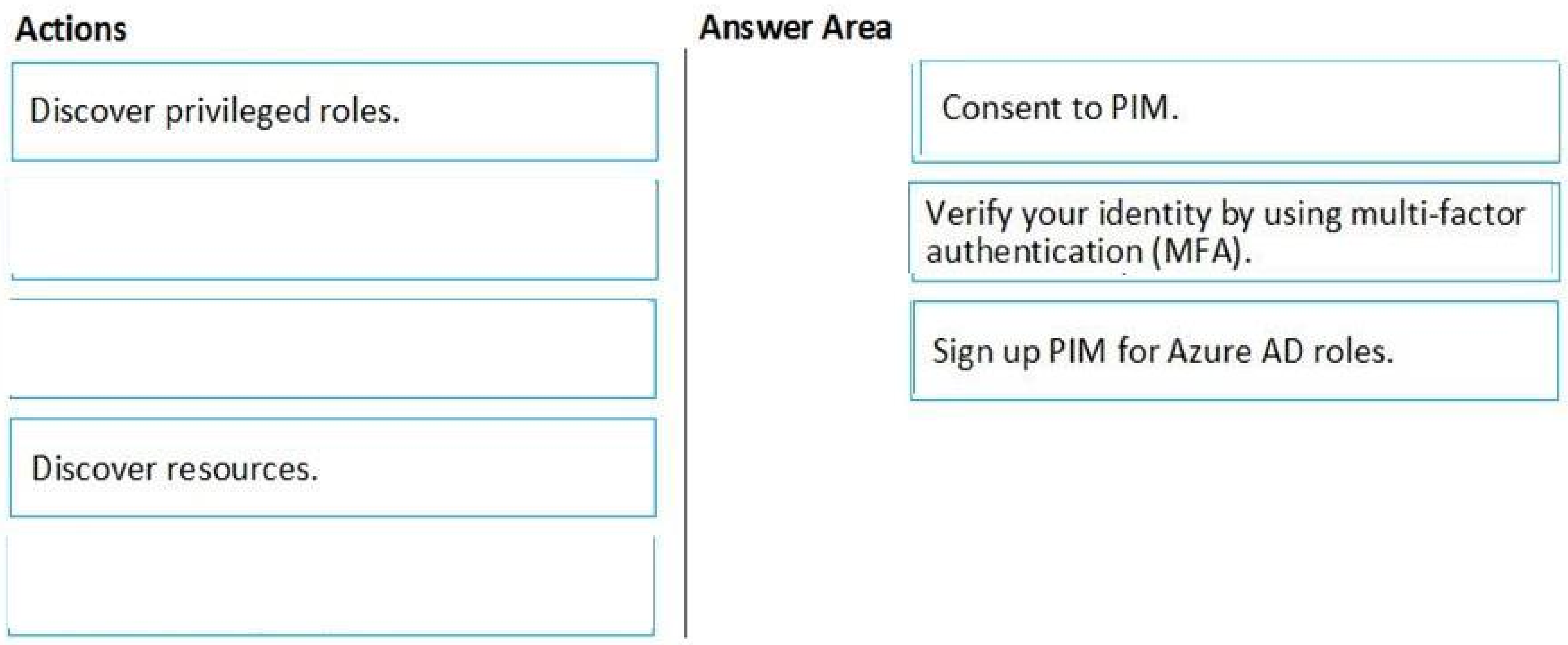
Consent to PIM.

Discover resources.

Verify your identity by using multi-factor authentication (MFA).

Answer Area

**Correct Answer:**



Actions

Discover privileged roles.

Discover resources.

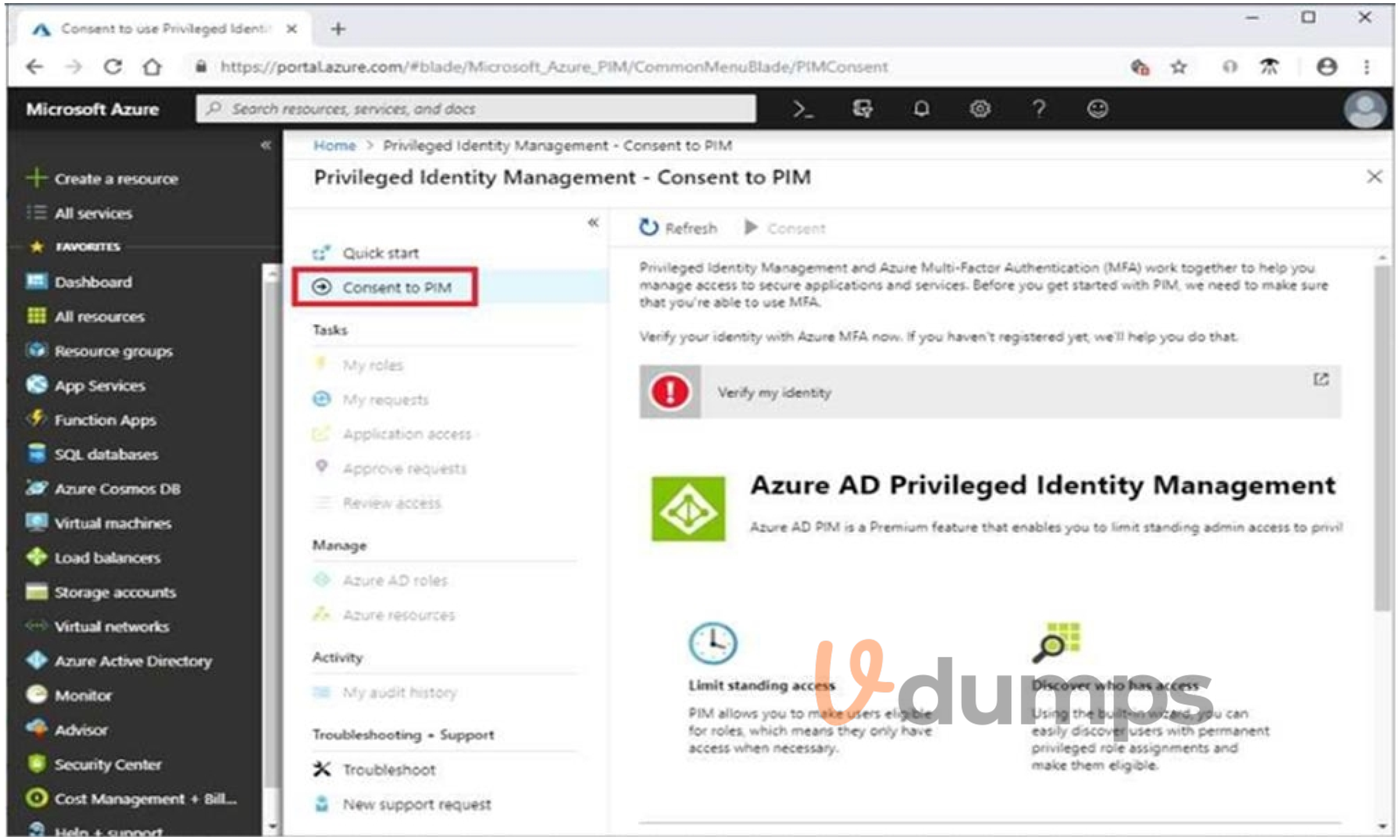
Answer Area

Consent to PIM.

Verify your identity by using multi-factor authentication (MFA).

Sign up PIM for Azure AD roles.

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



Privileged Identity Management - Consent to PIM

Privileged Identity Management and Azure Multi-Factor Authentication (MFA) work together to help you manage access to secure applications and services. Before you get started with PIM, we need to make sure that you're able to use MFA.

Verify your identity with Azure MFA now. If you haven't registered yet, we'll help you do that.

Azure AD Privileged Identity Management

Azure AD PIM is a Premium feature that enables you to limit standing admin access to privil

Limit standing access

PIM allows you to make users eligible for roles, which means they only have access when necessary.

Discover who has access

Using the built-in wizard, you can easily discover users with permanent privileged role assignments and make them eligible.

Step: 2 Verify your identity by using multi-factor authentication (MFA)
Click Verify my identity to verify your identity with Azure MF
You'll be asked to pick an account.
Step 3: Sign up PIM for Azure AD roles
Once you have enabled PIM for your directory, you'll need to sign up PIM to manage Azure AD roles.

**QUESTION 18**

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 a hybrid configuration of Azure Active Directory (Azure AD).
You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.
You need to configure the environment to support the planned authentication.
Solution: You deploy an Azure AD Application Proxy.
Does this meet the goal?

A. Yes

B. No

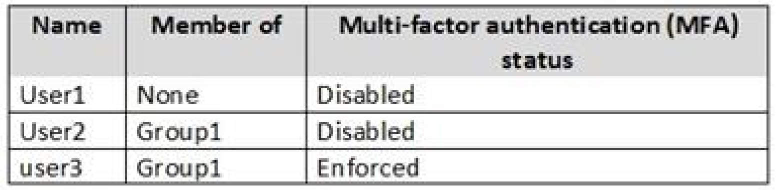
**Correct Answer: B**
**Section:**
**Explanation:**
Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:
Create Azure Virtual Network.
Create a custom DNS server in the Azure Virtual Network.
Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver. Configure forwarding between the custom DNS server and your on-premises DNS server.
Reference:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

**QUESTION 19**
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.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.
You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to Sa1.
Solution: You regenerate the Azure storage account access keys.
Does this meet the goal?

A. Yes
B. No

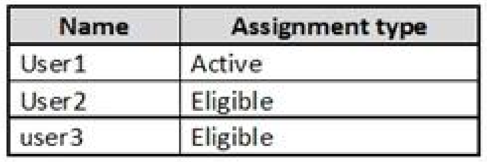
**Correct Answer: A**
**Section:**
**Explanation:**
Generating new storage account keys will invalidate all SAS's that were based on the previous keys.

**QUESTION 20**
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.



| Name | Member of | Multi-factor authentication (MFA) status |
|---|---|---|
| User1 | None | Disabled |
| User2 | Group1 | Disabled |
| user3 | Group1 | Enforced |

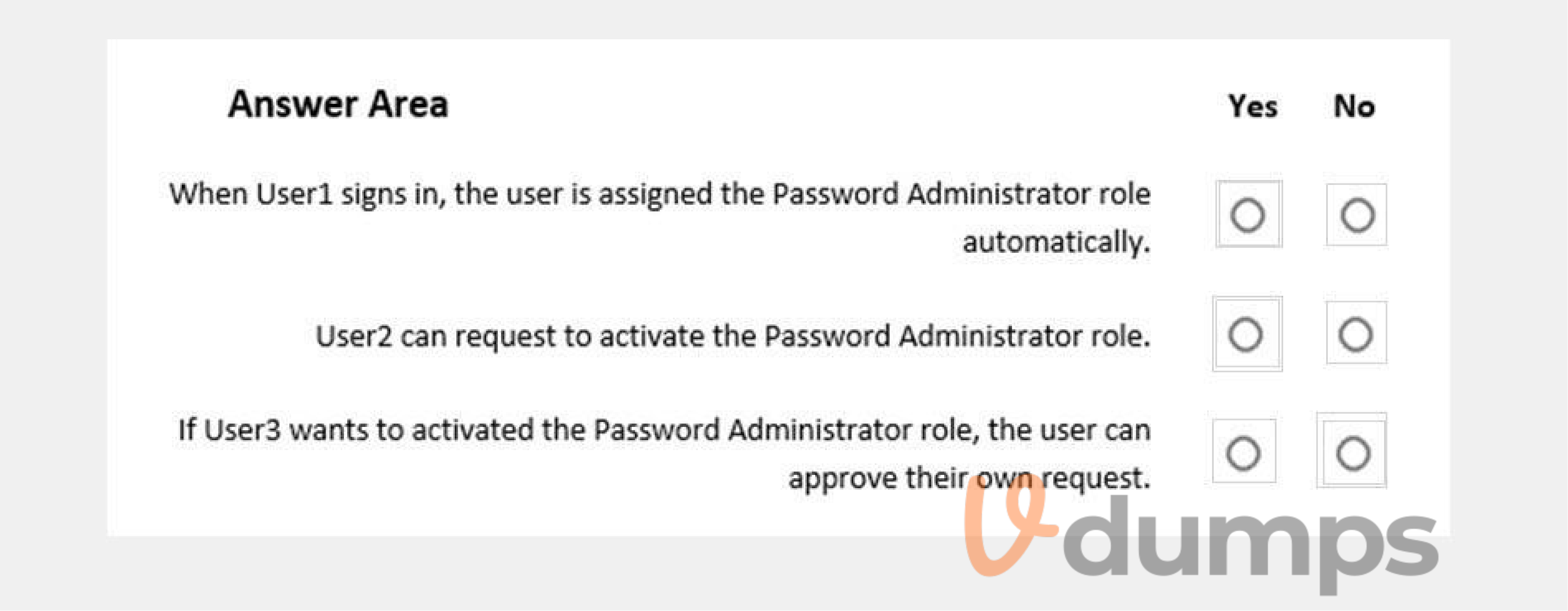
Azure AD Privileged Identity Management (PIM) is enabled for the tenant.
In PIM, the Password Administrator role has the following settings:
Maximum activation duration (hours): 2
Send email notifying admins of activation: Disable
Require incident/request ticket number during activation: Disable
Require Azure Multi-Factor Authentication for activation: Enable
Require approval to activate this role: Enable
Selected approver: Group1
You assign users the Password Administrator role as shown in the following table.



| Name | Assignment type |
|---|---|
| User1 | Active |
| User2 | Eligible |
| user3 | Eligible |

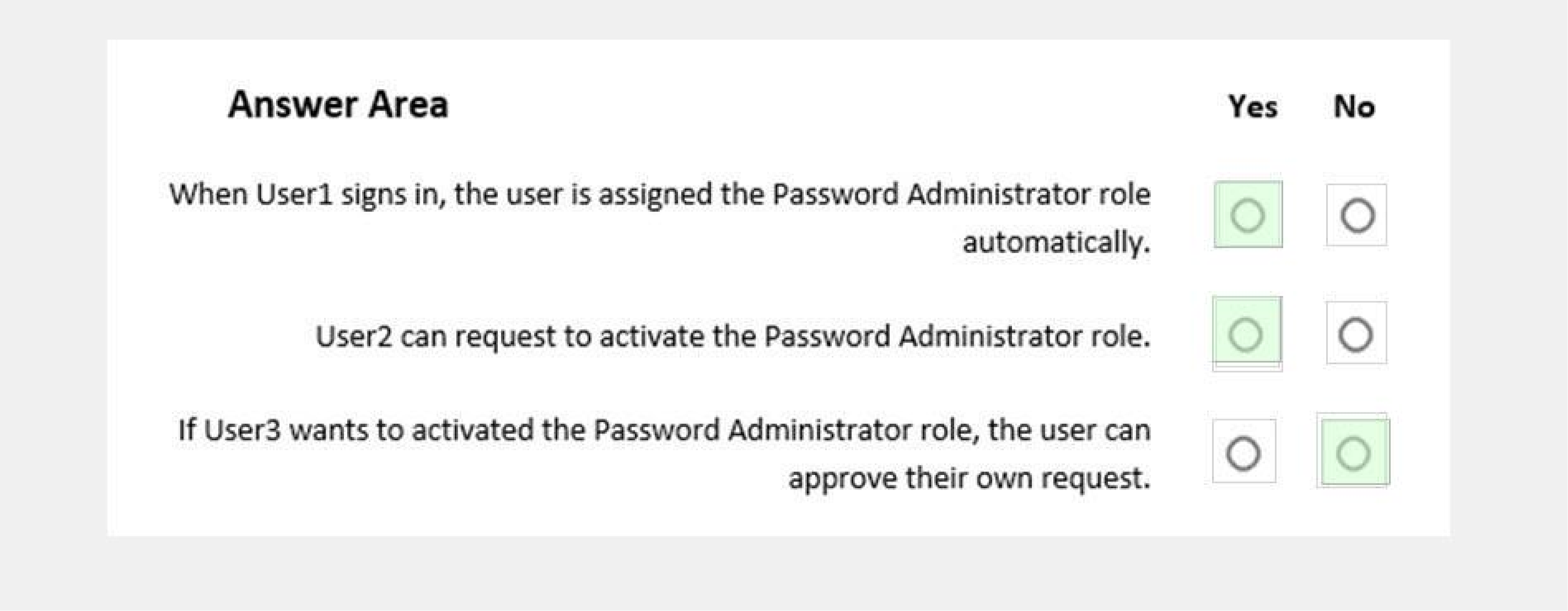
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

**Hot Area:**



| Answer Area | Yes | No |
|---|---|---|
| When User1 signs in, the user is assigned the Password Administrator role automatically. | ○ | ○ |
| User2 can request to activate the Password Administrator role. | ○ | ○ |
| If User3 wants to activated the Password Administrator role, the user can approve their own request. | ○ | ○ |

**Answer Area:**



| Answer Area | Yes | No |
|---|---|---|
| When User1 signs in, the user is assigned the Password Administrator role automatically. | [✓ ○] | ○ |
| User2 can request to activate the Password Administrator role. | [✓ ○] | ○ |
| If User3 wants to activated the Password Administrator role, the user can approve their own request. | ○ | [✓ ○] |

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

Box 1: Yes
Active assignments don't require the member to perform any action to use the role. Members assigned as active have the privileges assigned to the role at all times.
Box 2: Yes
While Multi-Factor Authentication is disabled for User2 and the setting Require Azure Multi-Factor Authentication for activation is enabled, User2 can request the role but will need to enable MFA to use the role.
Note: Eligible assignments require the member of the role to perform an action to use the role. Actions might include performing a multi-factor authentication (MFA) check, providing a business justification, or requesting approval from designated approvers.
Box 3: No
User3 is Group1, which is a Selected Approver Group, however, self-approval is not allowed and someone else from group is required to approve the request.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assign-roles

**QUESTION 21**
You have a hybrid configuration of Azure Active Directory (Azure AD) that has Single Sign-On (SSO) enabled. You have an Azure SQL Database instance that is configured to support Azure AD authentication.
Database developers must connect to the database instance from the domain joined device and authenticate by using their on-premises Active Directory account.
You need to ensure that developers can connect to the instance by using Microsoft SQL Server Management Studio. The solution must minimize authentication prompts.
Which authentication method should you recommend?

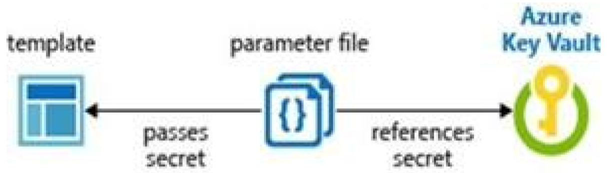
A. Active Directory - Password
B. Active Directory - Universal with MFA support
C. SQL Server Authentication
D. Active Directory - Integrated

**Correct Answer: D**
**Section:**
**Explanation:**
Active Directory - Integrated
Azure Active Directory Authentication is a mechanism of connecting to Microsoft Azure SQL Database by using identities in Azure Active Directory (Azure AD). Use this method for connecting to SQL Database if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.
Reference:
https://docs.microsoft.com/en-us/sql/ssms/f1-help/connect-to-server-database-engine?view=sql-server-2017 https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

**QUESTION 22**
You plan to use Azure Resource Manager templates to perform multiple deployments of identically configured Azure virtual machines. The password for the administrator account of each deployment is stored as a secret in different Azure key vaults.
You need to identify a method to dynamically construct a resource ID that will designate the key vault containing the appropriate secret during each deployment. The name of the key vault and the name of the secret will be provided as inline parameters.
What should you use to construct the resource ID?

A. a key vault access policy
B. a linked template
C. a parameters file
D. an automation account

**Correct Answer: C**
**Section:**
**Explanation:**
You reference the key vault in the parameter file, not the template. The following image shows how the parameter file references the secret and passes that value to the template.



Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-keyvault-parameter

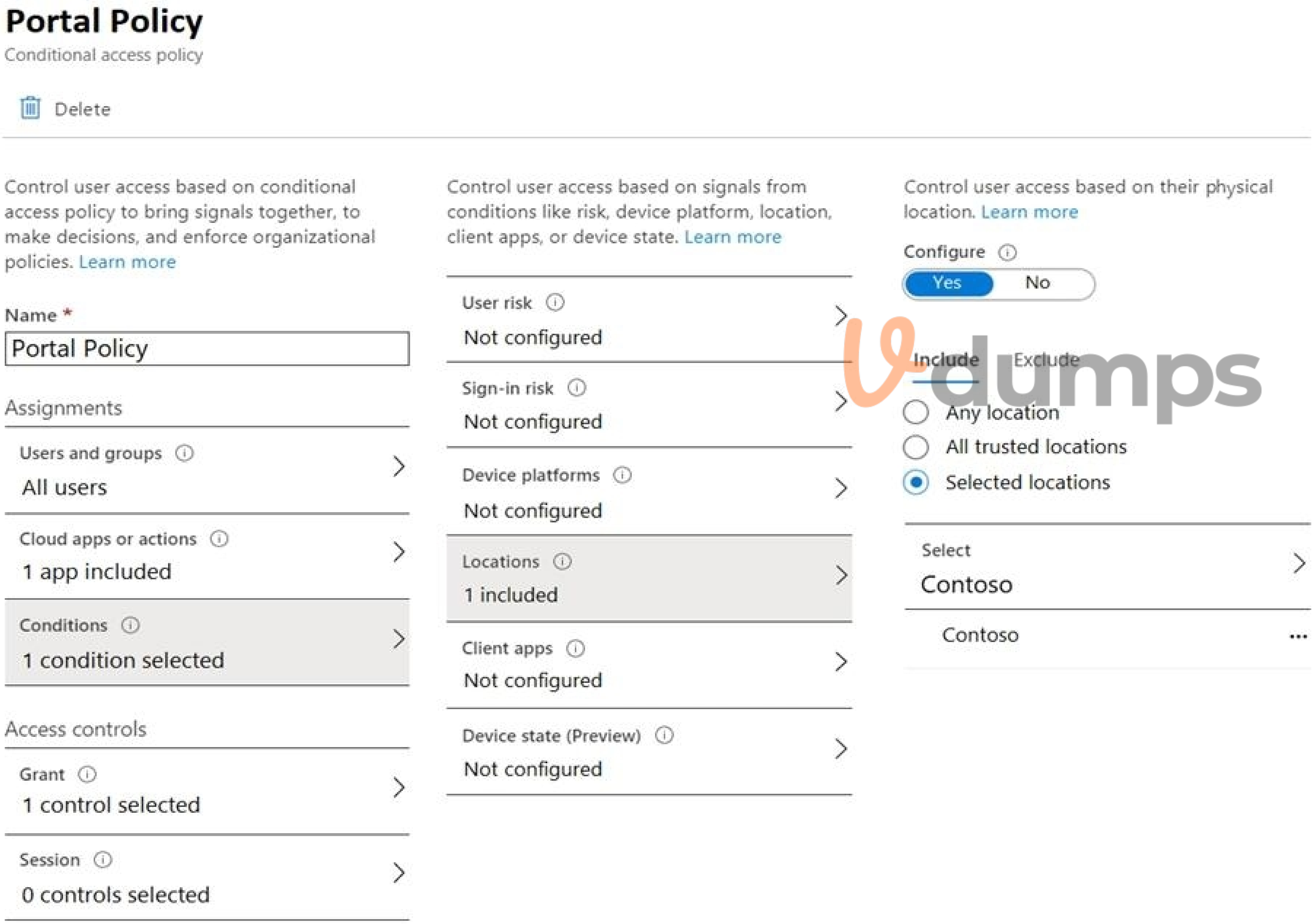
**QUESTION 23**

HOTSPOT

You create a new Azure subscription that is associated to a new Azure Active Directory (Azure AD) tenant.

You create one active conditional access policy named Portal Policy. Portal Policy is used to provide access to the Microsoft Azure Management cloud app.

The Conditions settings for Portal Policy are configured as shown in the Conditions exhibit. (Click the Conditions tab.)



**Portal Policy**

Conditional access policy

Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *
Portal Policy

Assignments

Users and groups: All users

Cloud apps or actions: 1 app included

Conditions: 1 condition selected

Access controls

Grant: 1 control selected

Session: 0 controls selected

Control user access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk: Not configured

Sign-in risk: Not configured

Device platforms: Not configured

Locations: 1 included

Client apps: Not configured

Device state (Preview): Not configured

Control user access based on their physical location. Learn more

Configure: [✓ Yes] No

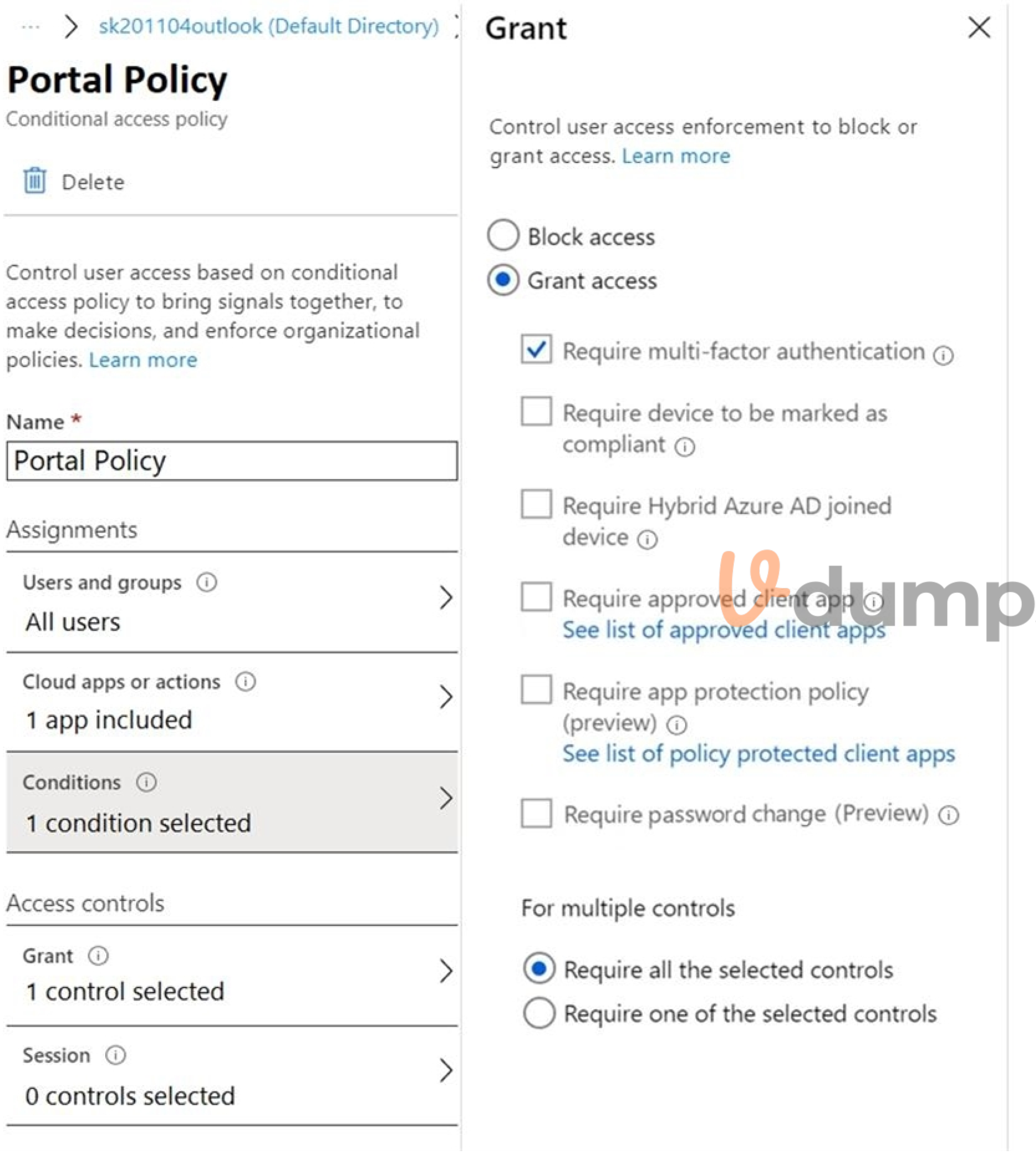
Include | Exclude

○ Any location
○ All trusted locations
● Selected locations

Select
Contoso

Contoso ...

The Grant settings for Portal Policy are configured as shown in the Grant exhibit. (Click the Grant tab.)



··· > sk201104outlook (Default Directory)

**Portal Policy**

Conditional access policy

Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Portal Policy

Assignments

Users and groups ⓘ
All users

Cloud apps or actions ⓘ
1 app included

Conditions ⓘ
1 condition selected

Access controls

Grant ⓘ
1 control selected

Session ⓘ
0 controls selected

**Grant**

Control user access enforcement to block or grant access. Learn more

○ Block access
● Grant access

☑ Require multi-factor authentication ⓘ

□ Require device to be marked as compliant ⓘ

□ Require Hybrid Azure AD joined device ⓘ

□ Require approved client app ⓘ
See list of approved client apps

□ Require app protection policy (preview) ⓘ
See list of policy protected client apps

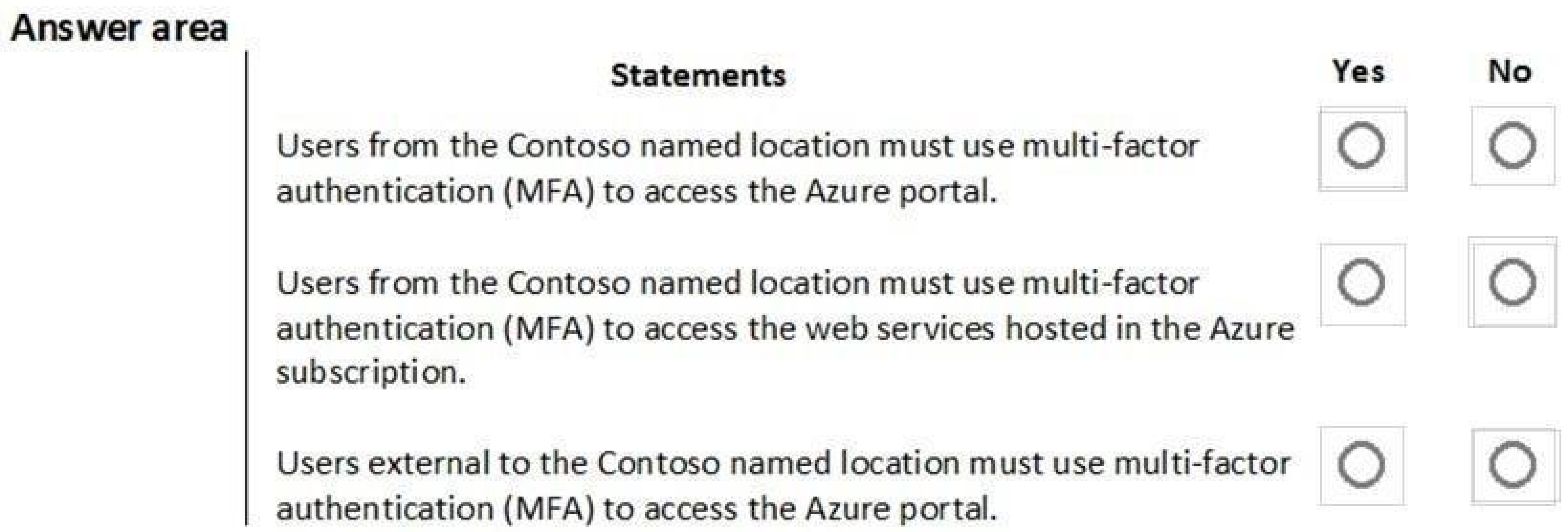
□ Require password change (Preview) ⓘ

For multiple controls

● Require all the selected controls
○ Require one of the selected controls

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

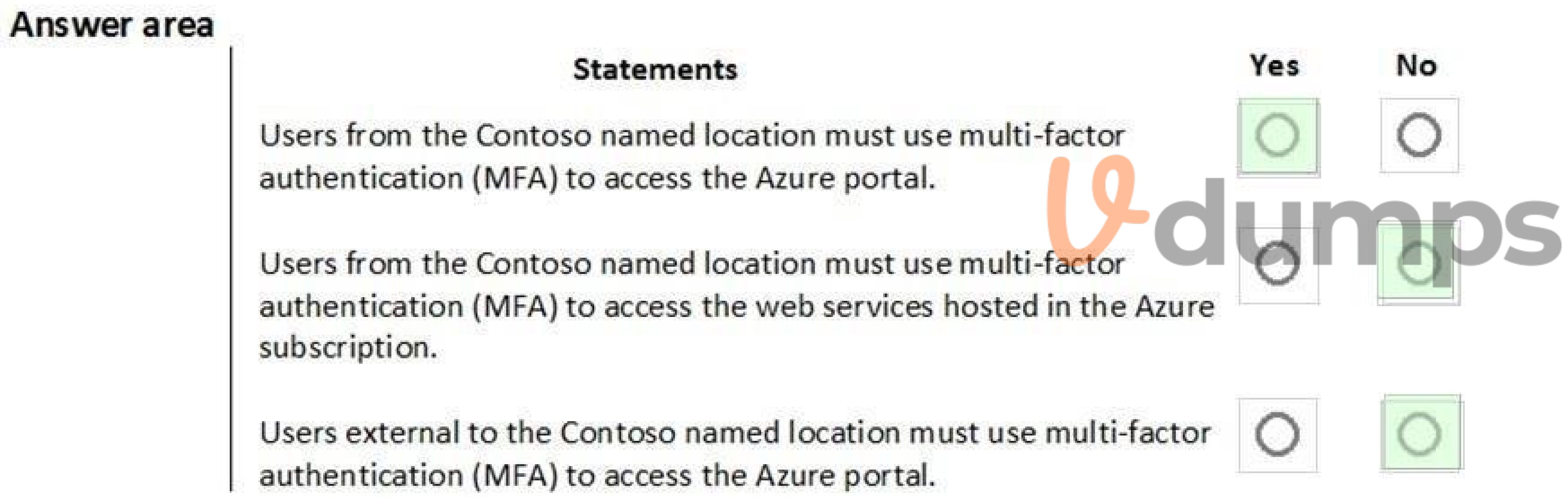
**Hot Area:**



Answer area

| Statements | Yes | No |
|---|---|---|
| Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal. | ○ | ○ |
| Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription. | ○ | ○ |
| Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal. | ○ | ○ |

**Answer Area:**



Answer area

| Statements | Yes | No |
|---|---|---|
| Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal. | [✓ ○] | ○ |
| Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription. | ○ | [✓ ○] |
| Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal. | ○ | [✓ ○] |

**Section:**
**Explanation:**
Box 1: Yes
The Contoso location is included in the policy and MFA is required.
Box 2: No
The policy applies to the Azure portal and Azure management endpoints. The policy does not apply to web services host in Azure.
Box 3: No
The policy applies only to users in the Contoso location. The policy does not apply to users external to the Contoso location.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

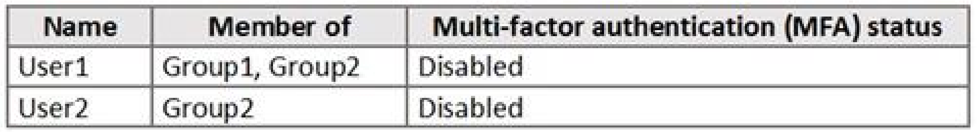
**QUESTION 24**
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
An administrator named Admin1 has access to the following identities:
An OpenID-enabled user account
A Hotmail account

An account in contoso.com
An account in an Azure AD tenant named fabrikam.com
You plan to use Azure Account Center to transfer the ownership of Sub1 to Admin1.
To which accounts can you transfer the ownership of Sub1?

A. contoso.com only
B. contoso.com, fabrikam.com, and Hotmail only
C. contoso.com and fabrikam.com only
D. contoso.com, fabrikam.com, Hotmail, and OpenID-enabled user account

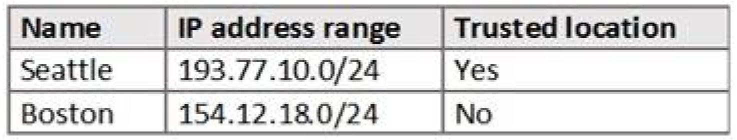
**Correct Answer: C**
**Section:**
**Explanation:**
When you transfer billing ownership of your subscription to an account in another Azure AD tenant, you can move the subscription to the new account's tenant. If you do so, all users, groups, or service principals who had role based access (RBAC) to manage subscriptions and its resources lose their access. Only the user in the new account who accepts your transfer request will have access to manage the resources.
Reference:
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transferring-subscription-to-an-account-in-another-azure-ad-tenant

**QUESTION 25**
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



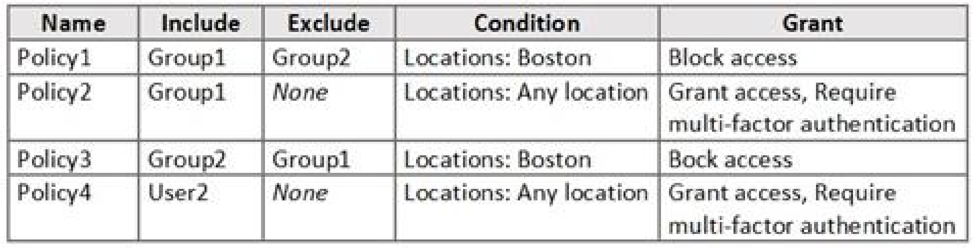
| Name | Member of | Multi-factor authentication (MFA) status |
|---|---|---|
| User1 | Group1, Group2 | Disabled |
| User2 | Group2 | Disabled |

The tenant contains the named locations shown in the following table.



| Name | IP address range | Trusted location |
|---|---|---|
| Seattle | 193.77.10.0/24 | Yes |
| Boston | 154.12.18.0/24 | No |

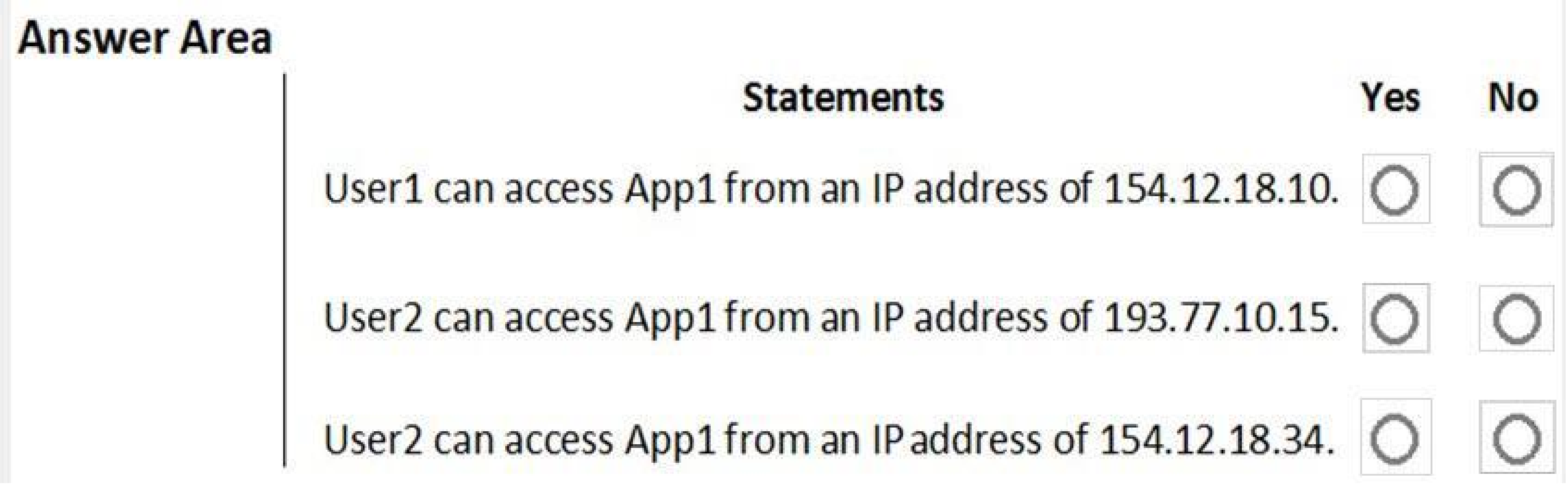
You create the conditional access policies for a cloud app named App1 as shown in the following table.



| Name | Include | Exclude | Condition | Grant |
|---|---|---|---|---|
| Policy1 | Group1 | Group2 | Locations: Boston | Block access |
| Policy2 | Group1 | *None* | Locations: Any location | Grant access, Require multi-factor authentication |
| Policy3 | Group2 | Group1 | Locations: Boston | Bock access |
| Policy4 | User2 | *None* | Locations: Any location | Grant access, Require multi-factor authentication |

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

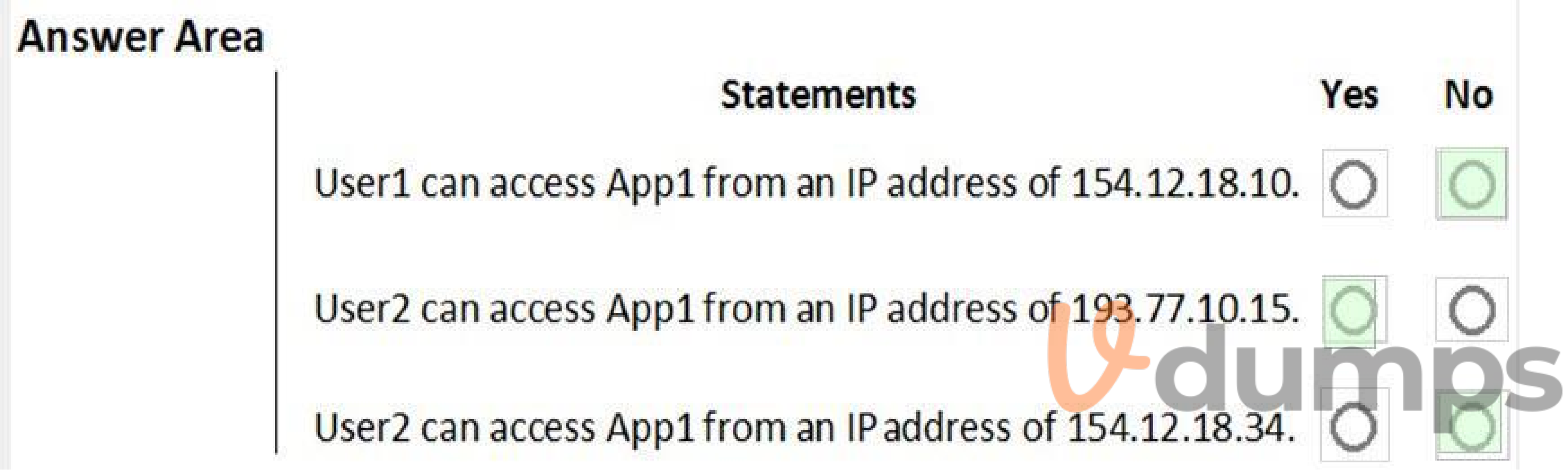
**Hot Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| User1 can access App1 from an IP address of 154.12.18.10. | ○ | ○ |
| User2 can access App1 from an IP address of 193.77.10.15. | ○ | ○ |
| User2 can access App1 from an IP address of 154.12.18.34. | ○ | ○ |

**Answer Area:**

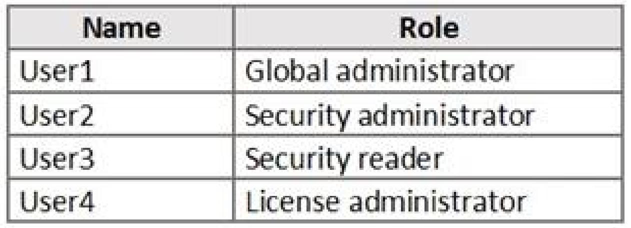


Answer Area

| Statements | Yes | No |
|---|---|---|
| User1 can access App1 from an IP address of 154.12.18.10. | ○ | [✓ ○] |
| User2 can access App1 from an IP address of 193.77.10.15. | [✓ ○] | ○ |
| User2 can access App1 from an IP address of 154.12.18.34. | ○ | [✓ ○] |

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

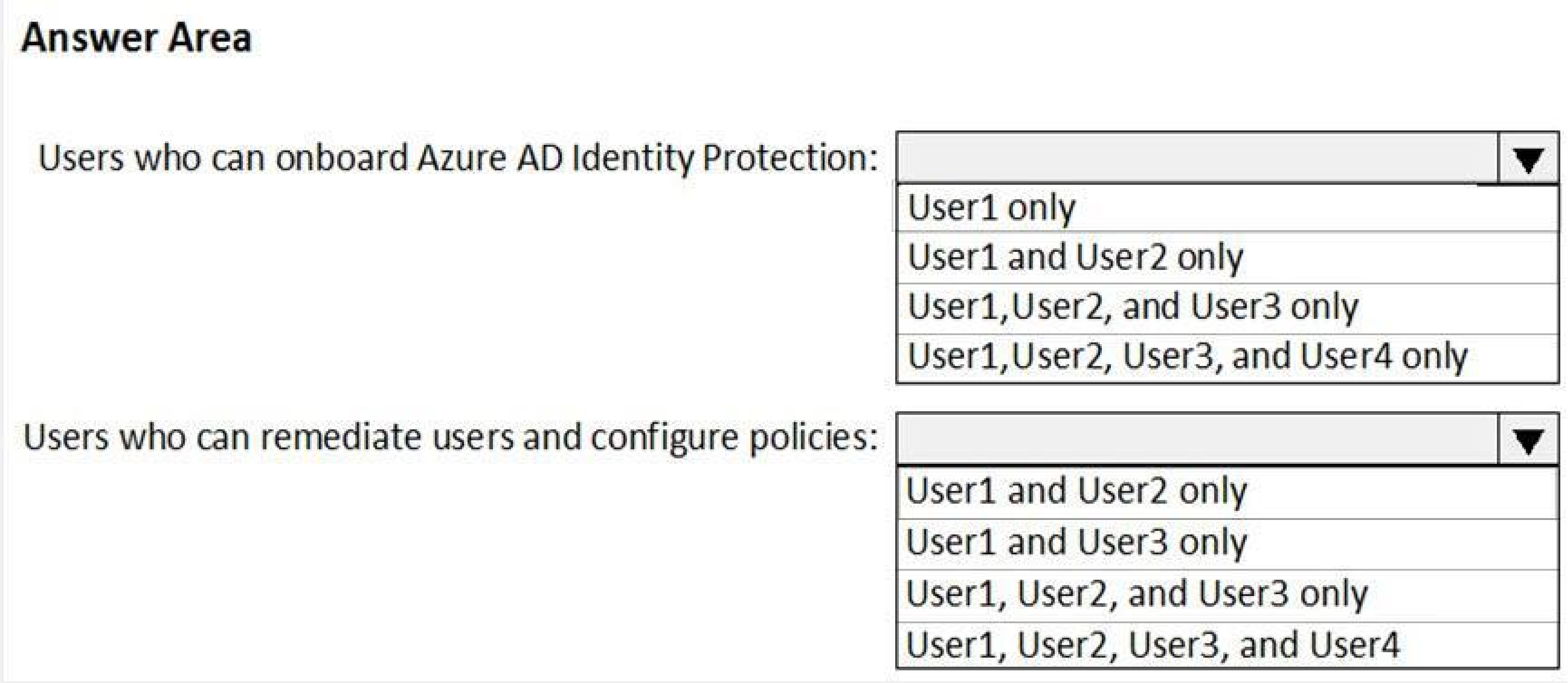
**QUESTION 26**
HOTSPOT
You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.



| Name | Role |
|---|---|
| User1 | Global administrator |
| User2 | Security administrator |
| User3 | Security reader |
| User4 | License administrator |

Each user is assigned an Azure AD Premium P2 license.
You plan to onboard and configure Azure AD Identity Protection.
Which users can onboard Azure AD Identity Protection, remediate users, and configure policies? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**



Answer Area

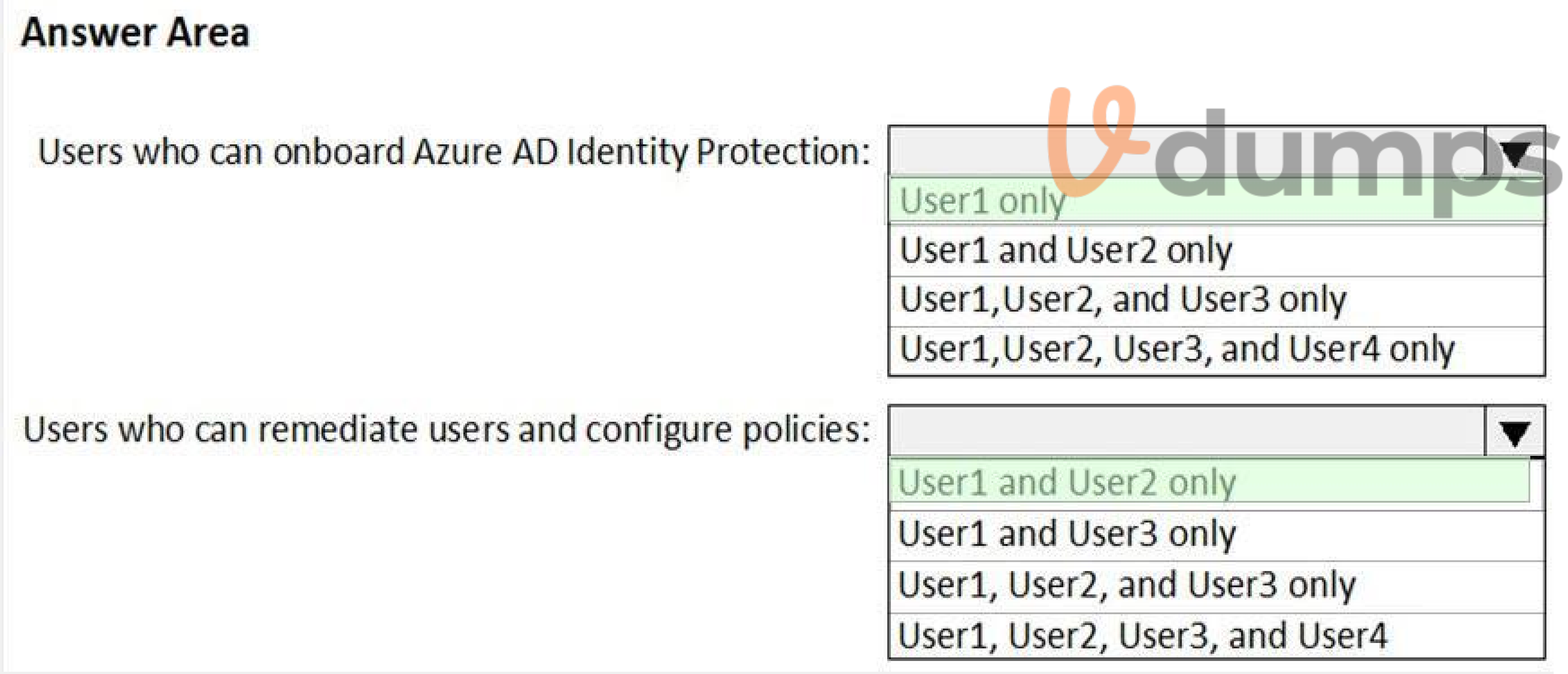
Users who can onboard Azure AD Identity Protection:

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

Users who can remediate users and configure policies:

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

**Answer Area:**



Answer Area

Users who can onboard Azure AD Identity Protection:

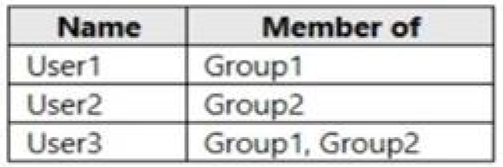
- [✓ User1 only]
- User1 and User2 only
- User1,User2, and User3 only
- User1,User2, User3, and User4 only

Users who can remediate users and configure policies:

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

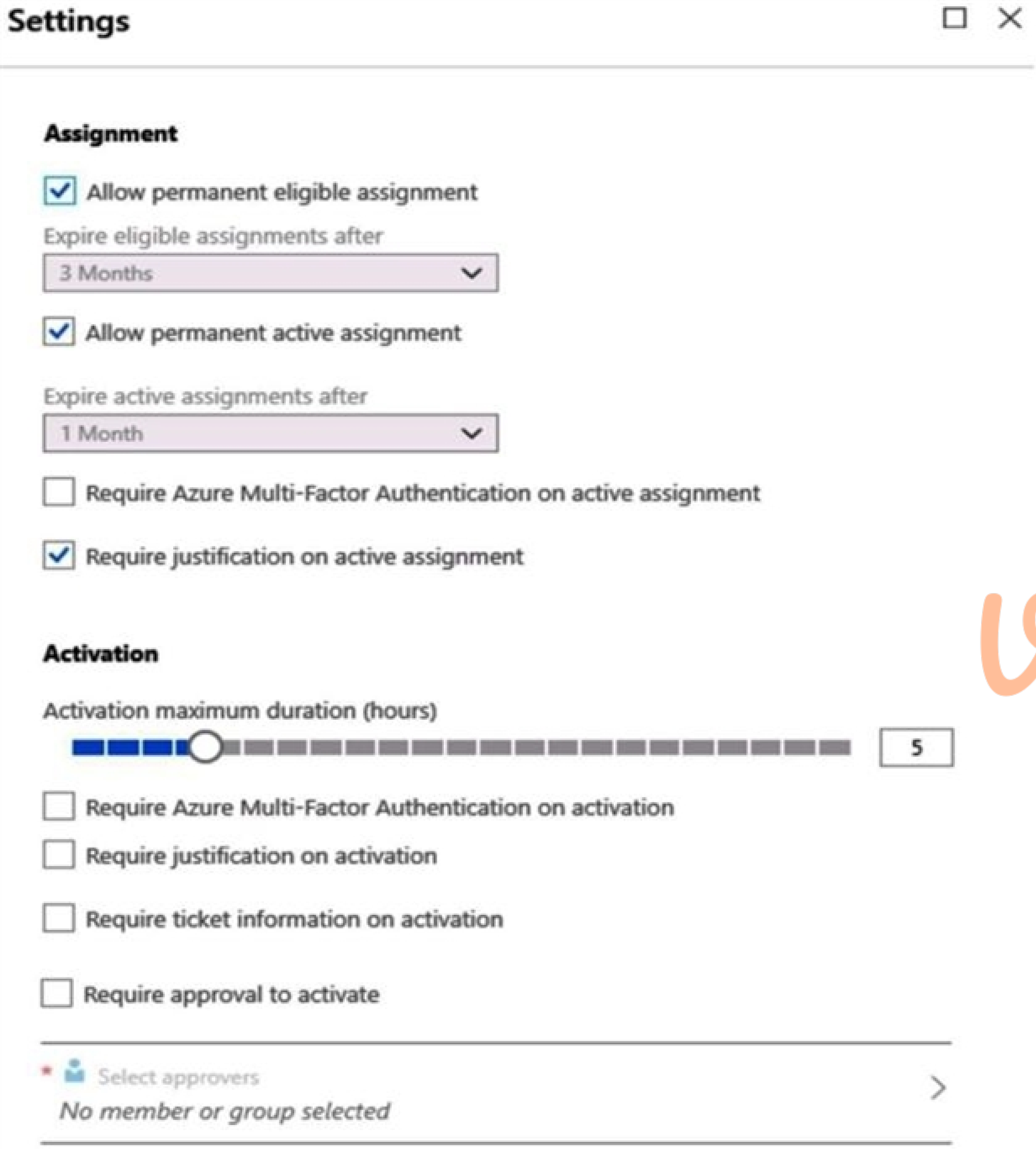
**Section:**
**Explanation:**

**QUESTION 27**
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



| Name | Member of |
|---|---|
| User1 | Group1 |
| User2 | Group2 |
| User3 | Group1, Group2 |

From Azure AD Privileged Identity Management (PIM), you configure the settings for the Security Administrator role as shown in the following exhibit.



Settings

Assignment

☑ Allow permanent eligible assignment

Expire eligible assignments after: 3 Months

☑ Allow permanent active assignment

Expire active assignments after: 1 Month

□ Require Azure Multi-Factor Authentication on active assignment

☑ Require justification on active assignment

Activation

Activation maximum duration (hours): 5

□ Require Azure Multi-Factor Authentication on activation

□ Require justification on activation

□ Require ticket information on activation

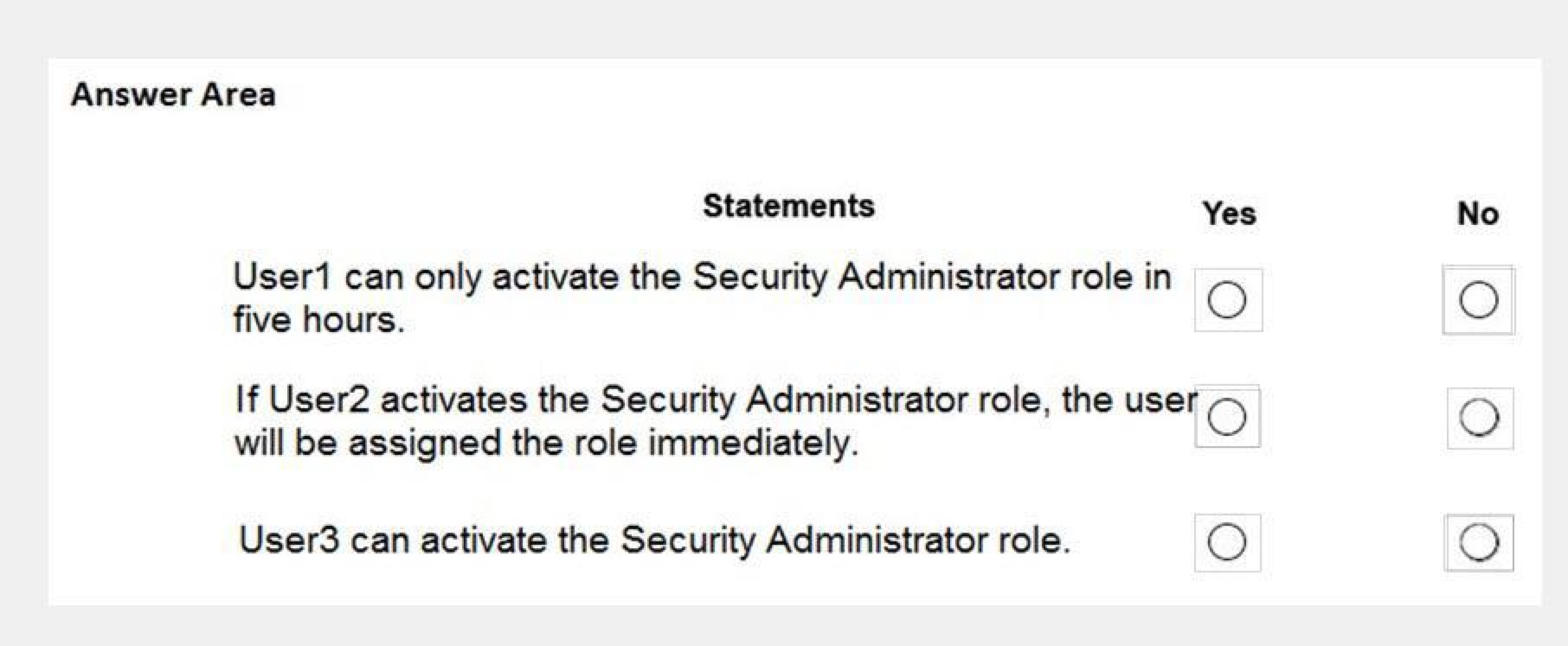
□ Require approval to activate

* Select approvers

*No member or group selected*

From PIM, you assign the Security Administrator role to the following groups:
Group1: Active assignment type, permanently assigned
Group2: Eligible assignment type, permanently eligible
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

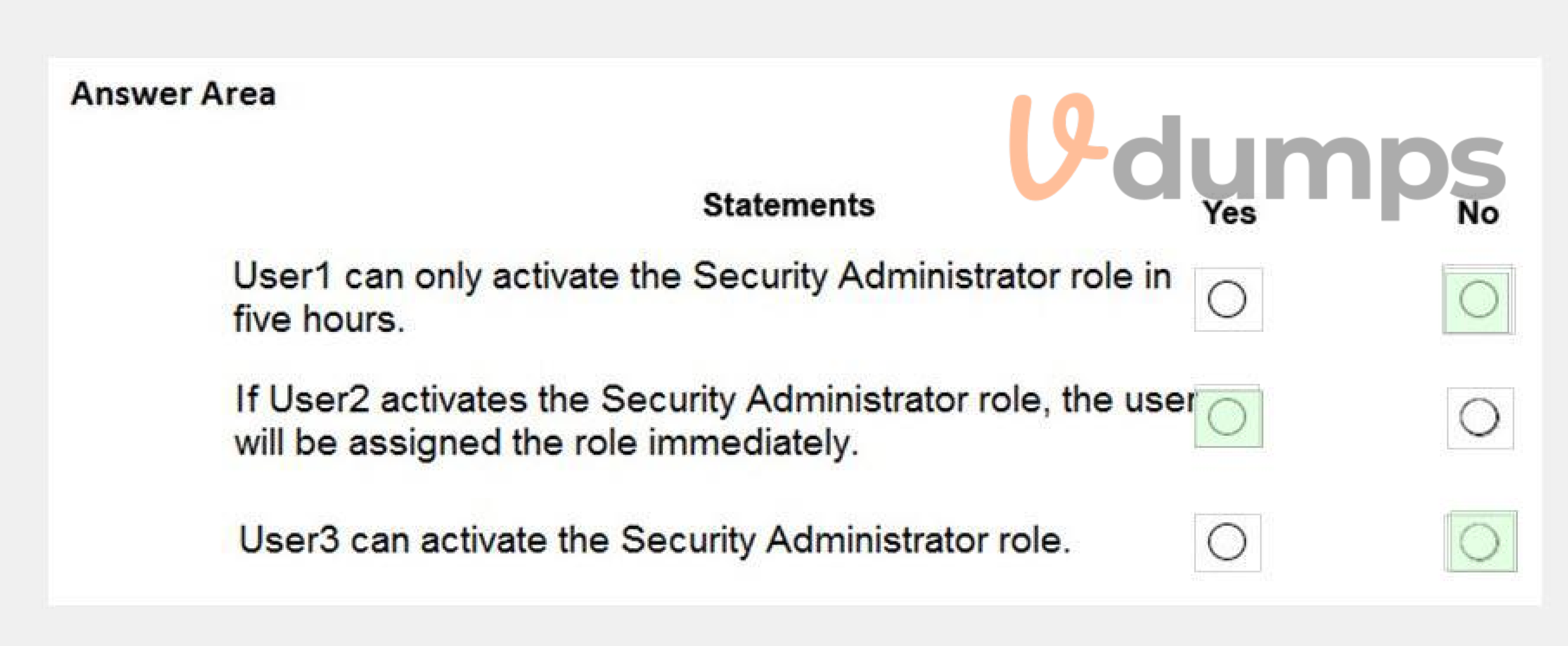
**Hot Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| User1 can only activate the Security Administrator role in five hours. | ○ | ○ |
| If User2 activates the Security Administrator role, the user will be assigned the role immediately. | ○ | ○ |
| User3 can activate the Security Administrator role. | ○ | ○ |

**Answer Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| User1 can only activate the Security Administrator role in five hours. | ○ | [✓ ○] |
| If User2 activates the Security Administrator role, the user will be assigned the role immediately. | [✓ ○] | ○ |
| User3 can activate the Security Administrator role. | ○ | [✓ ○] |

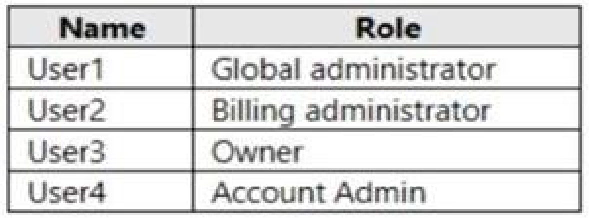
**Section:**
**Explanation:**
Box 1: No
User1 is a member of Group1. Group1: Active assignment type, permanently assigned
Box 2: Yes
Active Type: A role assignment that doesn't require a user to perform any action to use the role. Users assigned as active have the privileges assigned to the role
Box 3: No
User3 is member of Group1 and Group2.
Group1: Active assignment type, permanently assigned
Group2: Eligible assignment type, permanently eligible

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings

**QUESTION 28**

HOTSPOT

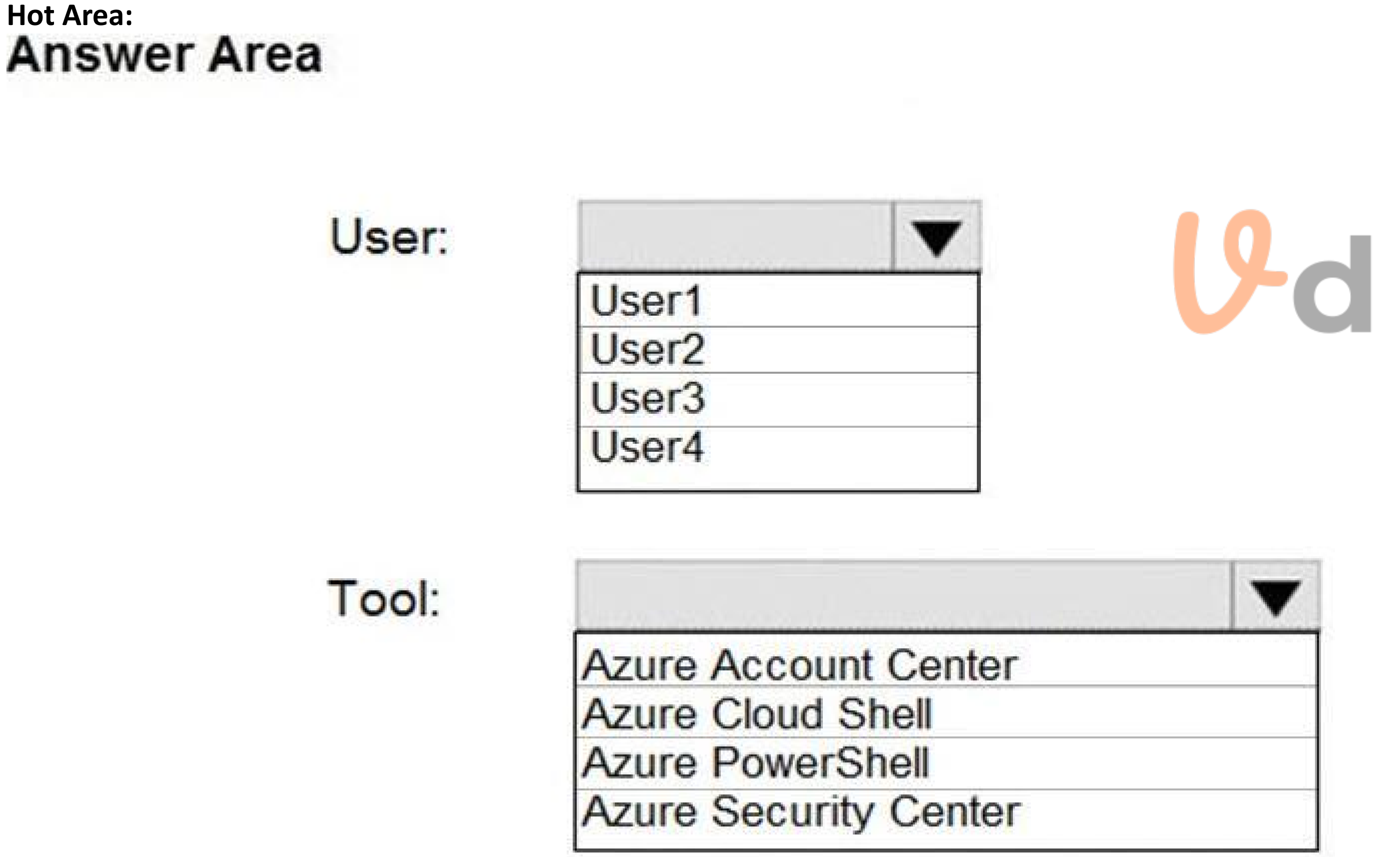
Your company has an Azure subscription named Subscription1 that contains the users shown in the following table.



| Name | Role |
|---|---|
| User1 | Global administrator |
| User2 | Billing administrator |
| User3 | Owner |
| User4 | Account Admin |

The company is sold to a new owner.
The company needs to transfer ownership of Subscription1.
Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**

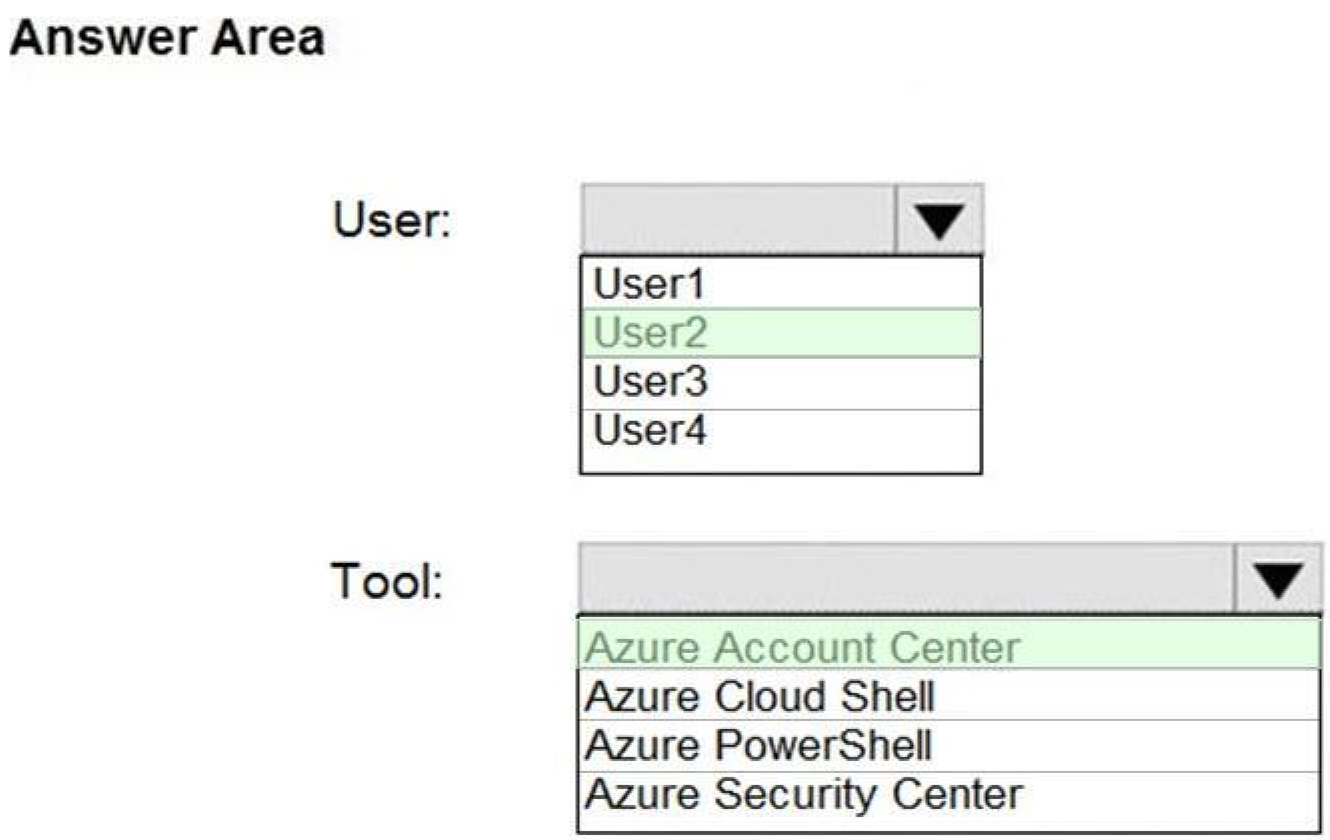


Answer Area

User:
- User1
- User2
- User3
- User4

Tool:
- Azure Account Center
- Azure Cloud Shell
- Azure PowerShell
- Azure Security Center

**Answer Area:**



Answer Area

User:

User1
User2
User3
User4

Tool:

Azure Account Center
Azure Cloud Shell
Azure PowerShell
Azure Security Center

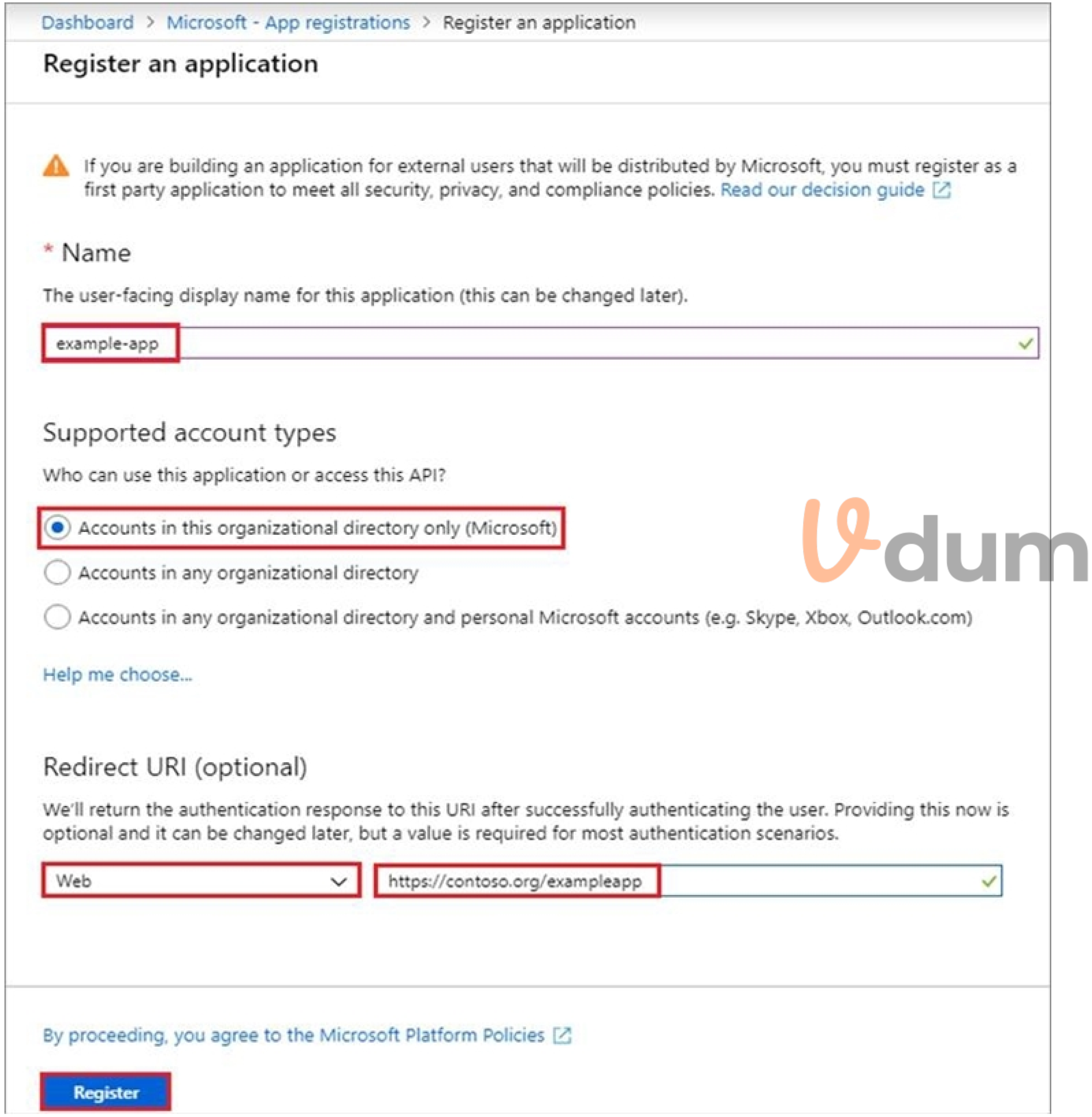
**Section:**
**Explanation:**
Box 1; User2
Billing Administrator
Select Transfer billing ownership for the subscription that you want to transfer.
Enter the email address of a user who's a billing administrator of the account that will be the new owner for the subscription.
Box 2: Azure Account Center
Azure Account Center can be used.
Reference:
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transfer-billing-ownership-of-an-azure-subscription

**QUESTION 29**
SIMULATION
The developers at your company plan to create a web app named App10598168 and to publish the app to https://www.contoso.com.
You need to perform the following tasks:
Ensure that App10598168 is registered to Azure Active Directory (Azure AD).
Generate a password for App10598168.
To complete this task, sign in to the Azure portal.

A.

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
Step 1: Register the Application
1. Sign in to your Azure Account through the Azure portal.

2. Select Azure Active Directory.
3. Select App registrations.
4. Select New registration.
5. Name the application App10598168 . Select a supported account type, which determines who can use the application. Under Redirect URI, select Web for the type of application you want to create. Enter the URI: https:// www.contoso.com , where the access token is sent to.



Dashboard > Microsoft - App registrations > Register an application

Register an application

If you are building an application for external users that will be distributed by Microsoft, you must register as a first party application to meet all security, privacy, and compliance policies. Read our decision guide

* Name

The user-facing display name for this application (this can be changed later).

example-app

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Microsoft)
○ Accounts in any organizational directory
○ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | https://contoso.org/exampleapp

By proceeding, you agree to the Microsoft Platform Policies

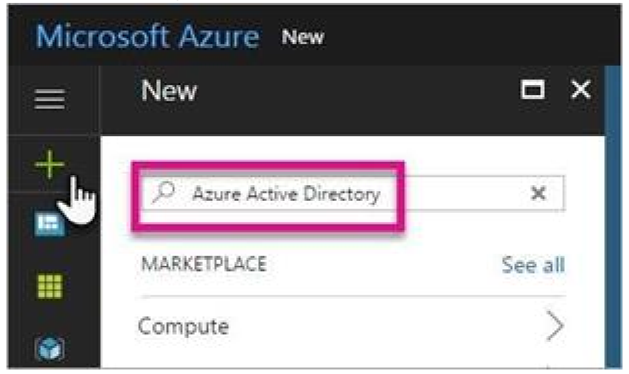
6. Click Register
Step 2: Create a new application secret
If you choose not to use a certificate, you can create a new application secret.
7 Select Certificates & secrets.

8. Select Client secrets -> New client secret.
9. Provide a description of the secret, and a duration. When done, select Add.
After saving the client secret, the value of the client secret is displayed. Copy this value because you aren't able to retrieve the key later. You provide the key value with the application ID to sign in as the application. Store the key value where your application can retrieve it.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

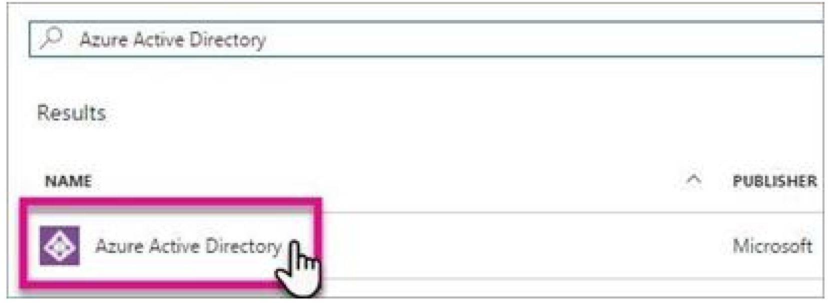
**QUESTION 30**
SIMULATION
You need to create a new Azure Active Directory (Azure AD) directory named 11641655.onmicrosoft.com and a user named User1 in the new directory. The solution must ensure that User1 is enabled for Azure Multi-Factor Authentication
(MFA).
To complete this task, sign in to the Azure portal.

A.

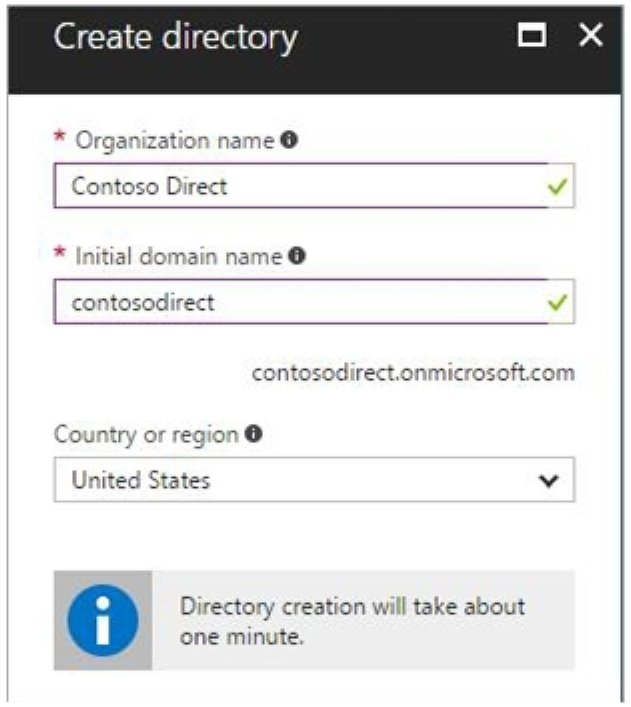
**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
Step 1: Create an Azure Active Directory tenant
1. Browse to the Azure portal and sign in with an account that has an Azure subscription.
2. Select the plus icon (+) and search for Azure Active Directory.



3. Select Azure Active Directory in the search results.



4. Select Create.
5. Provide an Organization name and an Initial domain name (10598168). Then select Create. Your directory is created.



Create directory

* Organization name: Contoso Direct

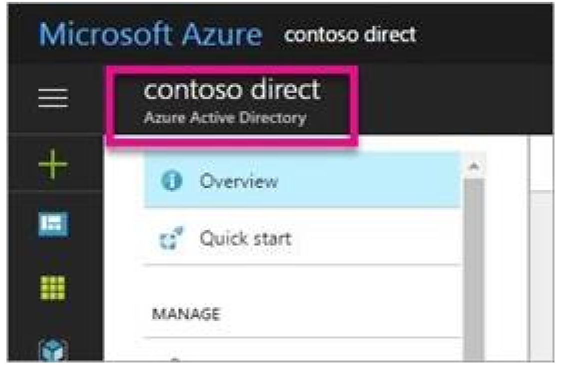
* Initial domain name: contosodirect

contosodirect.onmicrosoft.com

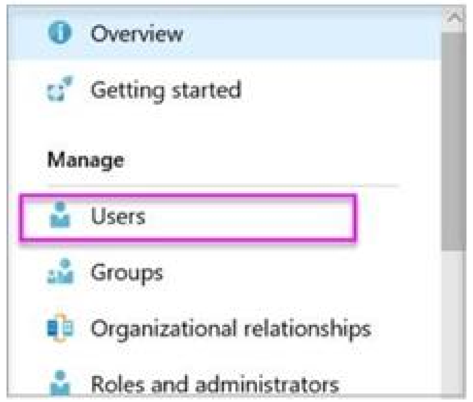
Country or region: United States

Directory creation will take about one minute.

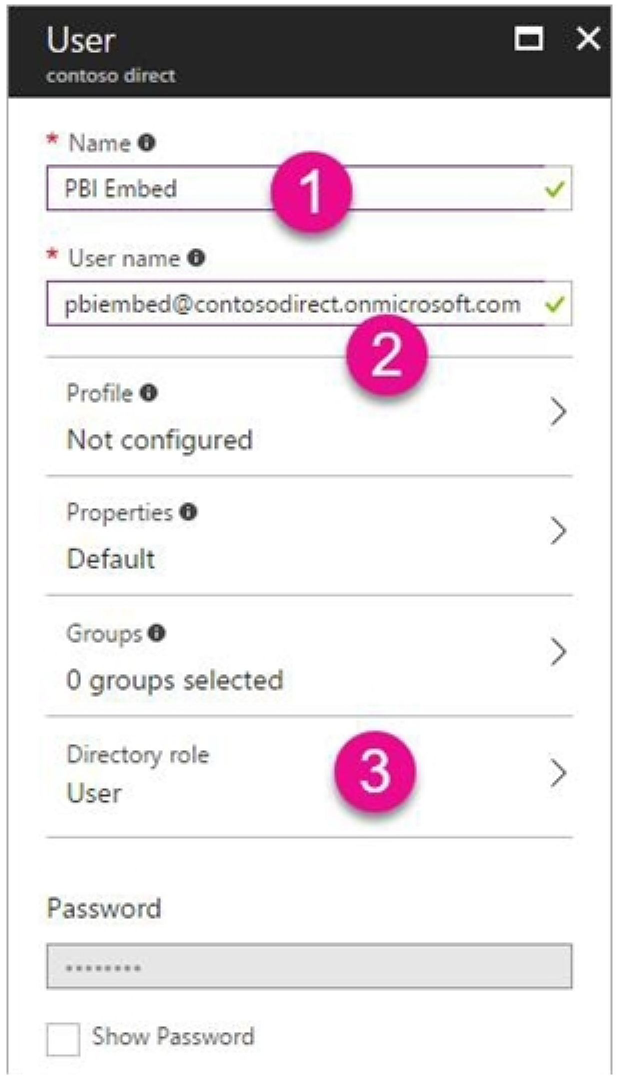
6. After directory creation is complete, select the information box to manage your new directory.
Next, you're going to add tenant users.
Step 2: Create an Azure Active Directory tenant user
7. In the Azure portal, make sure you are on the Azure Active Directory fly out.



8. Under Manage, select Users.



9. Select All users and then select + New user.
10. Provide a Name and User name (user1) for the regular user tenant You can also show the temporary password. When you're done, select Create.
Name: user1
User name: user1@11641655.onmicrosoft.com



User
contoso direct

* Name
PBI Embed

* User name
pbiembed@contosodirect.onmicrosoft.com

Profile
Not configured

Properties
Default

Groups
0 groups selected

Directory role
User

Password
••••••••

□ Show Password

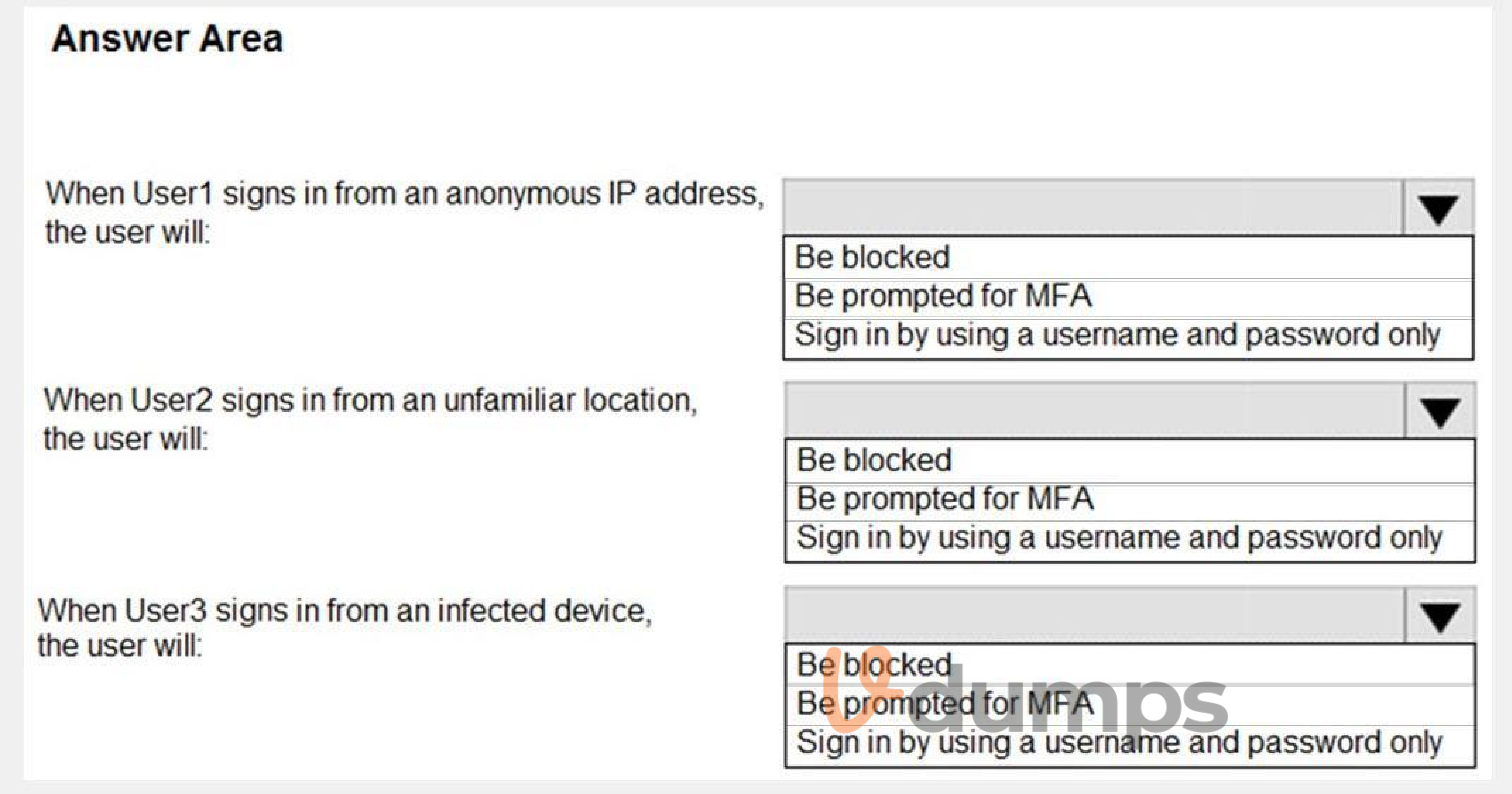
Reference:
https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant

**QUESTION 31**
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

| Name | Member of | Multi-factor authentication (MFA) status |
|---|---|---|
| User1 | Group1, Group2 | Enabled |
| User2 | Group1 | Disabled |
| User3 | Group1 | Disabled |

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:
Assignments: Include Group1, exclude Group2
Conditions: Sign-in risk level: Medium and above
Access Allow access, Require multi-factor authentication
You need to identify what occurs when the users sign in to Azure AD.
What should you identify for each user? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**



**Answer Area**

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

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

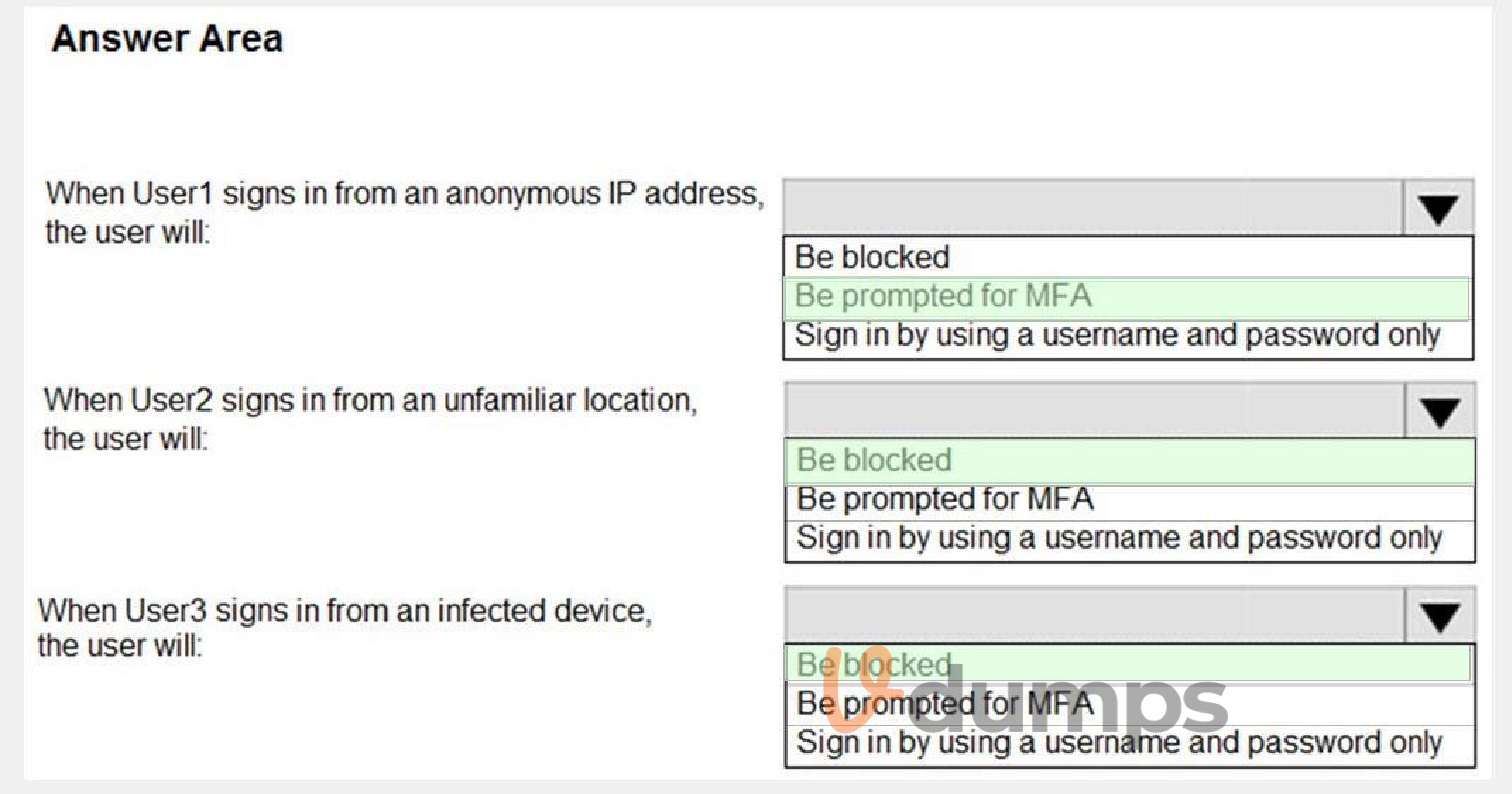
When User2 signs in from an unfamiliar location, the user will:

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

When User3 signs in from an infected device, the user will:

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

**Answer Area:**



Answer Area

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

- Be blocked
- [✓ Be prompted for MFA]
- Sign in by using a username and password only

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

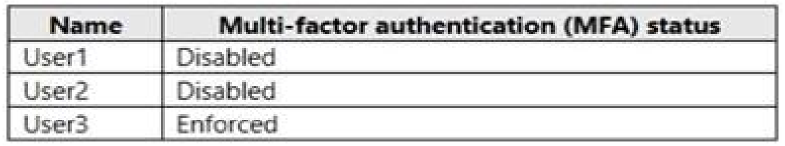
- [✓ Be blocked]
- Be prompted for MFA
- Sign in by using a username and password only

When User3 signs in from an infected device, the user will:

- [✓ Be blocked]
- Be prompted for MFA
- Sign in by using a username and password only

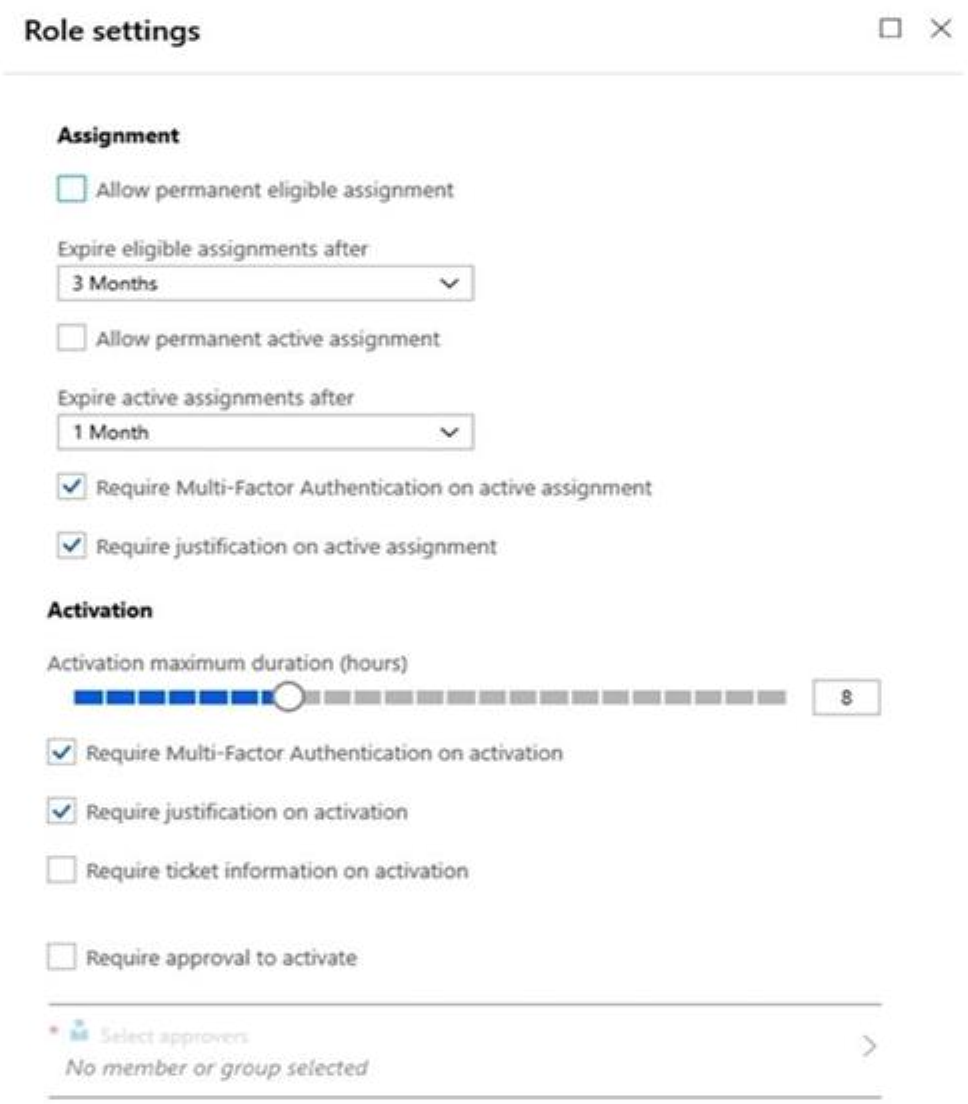
**Section:**
**Explanation:**
References:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

**QUESTION 32**
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



| Name | Multi-factor authentication (MFA) status |
|---|---|
| User1 | Disabled |
| User2 | Disabled |
| User3 | Enforced |

In Azure AD Privileged Identity Management (PIM), the Role settings for the Contributor role are configured as shown in the exhibit. (Click the Exhibit tab.)



Role settings

**Assignment**

□ Allow permanent eligible assignment

Expire eligible assignments after

3 Months

□ Allow permanent active assignment

Expire active assignments after

1 Month

☑ Require Multi-Factor Authentication on active assignment

☑ Require justification on active assignment

**Activation**

Activation maximum duration (hours)

8

☑ Require Multi-Factor Authentication on activation

☑ Require justification on activation

□ Require ticket information on activation

□ Require approval to activate

* Select approvers

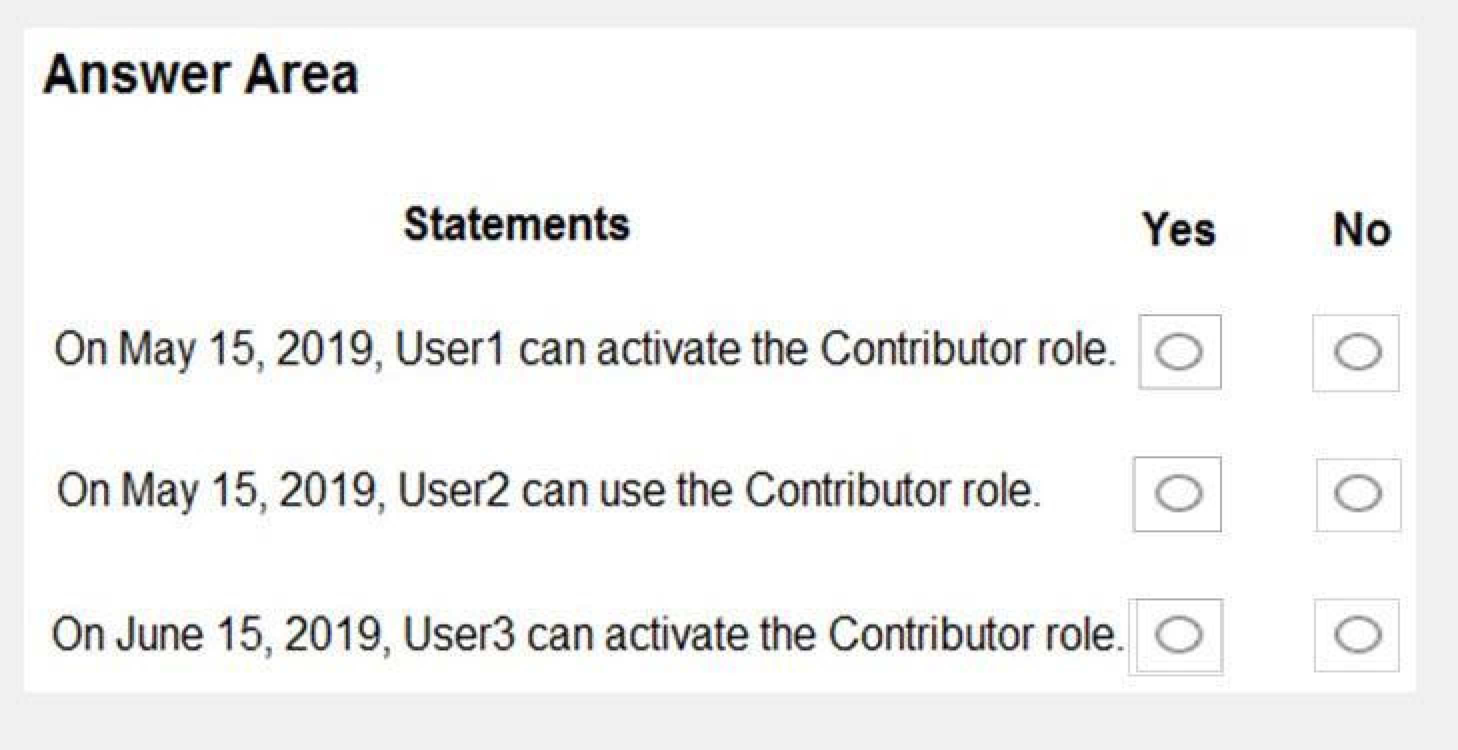
No member or group selected

You assign users the Contributor role on May 1, 2019 as shown in the following table.

| Name | Assignment type |
|---|---|
| User1 | Eligible |
| User2 | Active |
| User3 | Active |

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

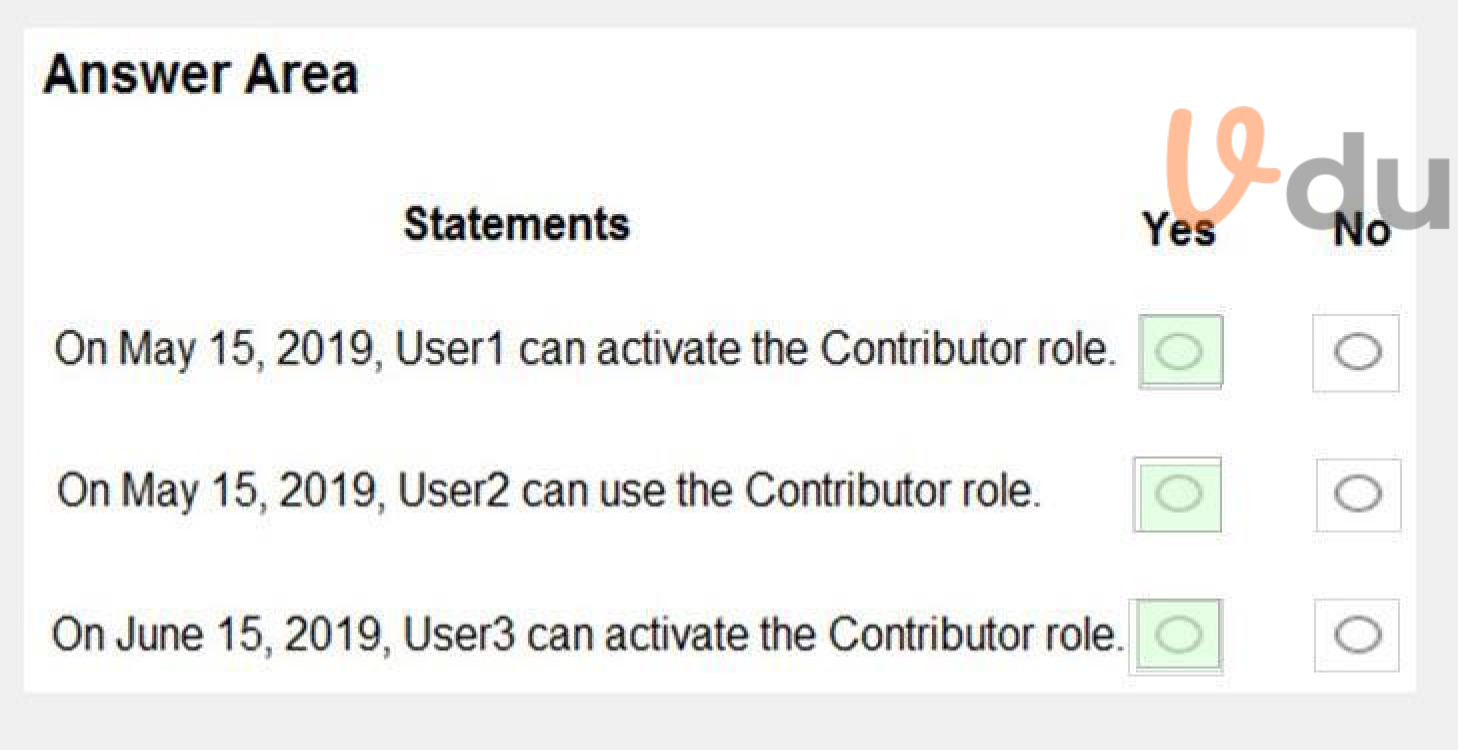
**Hot Area:**



## Answer Area

| Statements | Yes | No |
|---|---|---|
| On May 15, 2019, User1 can activate the Contributor role. | ○ | ○ |
| On May 15, 2019, User2 can use the Contributor role. | ○ | ○ |
| On June 15, 2019, User3 can activate the Contributor role. | ○ | ○ |

**Answer Area:**

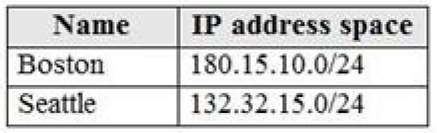


## Answer Area

| Statements | Yes | No |
|---|---|---|
| On May 15, 2019, User1 can activate the Contributor role. | [✓ ○] | ○ |
| On May 15, 2019, User2 can use the Contributor role. | [✓ ○] | ○ |
| On June 15, 2019, User3 can activate the Contributor role. | [✓ ○] | ○ |

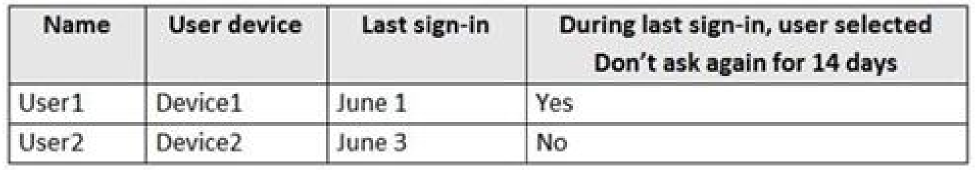
**Section:**
**Explanation:**
References:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assign-roles

**QUESTION 33**
HOTSPOT
You work at a company named Contoso, Ltd. that has the offices shown in the following table.



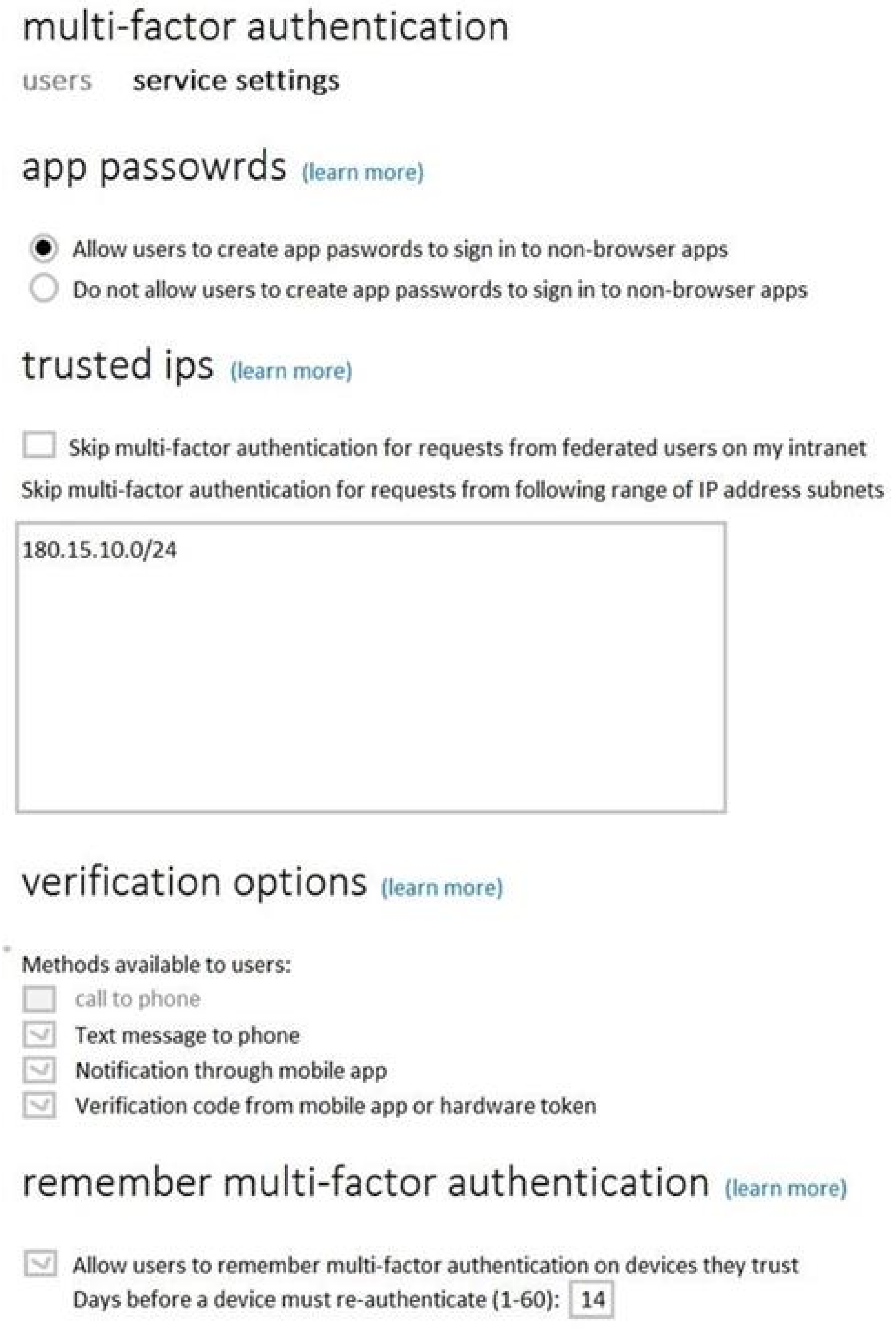
| Name | IP address space |
|---|---|
| Boston | 180.15.10.0/24 |
| Seattle | 132.32.15.0/24 |

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



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

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



multi-factor authentication

users service settings

app passowrds (learn more)

● Allow users to create app paswords to sign in to non-browser apps
○ Do not allow users to create app passwords to sign in to non-browser apps

trusted ips (learn more)

□ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

180.15.10.0/24

verification options (learn more)

Methods available to users:

□ call to phone
☑ Text message to phone
☑ Notification through mobile app
☑ Verification code from mobile app or hardware token

remember multi-factor authentication (learn more)

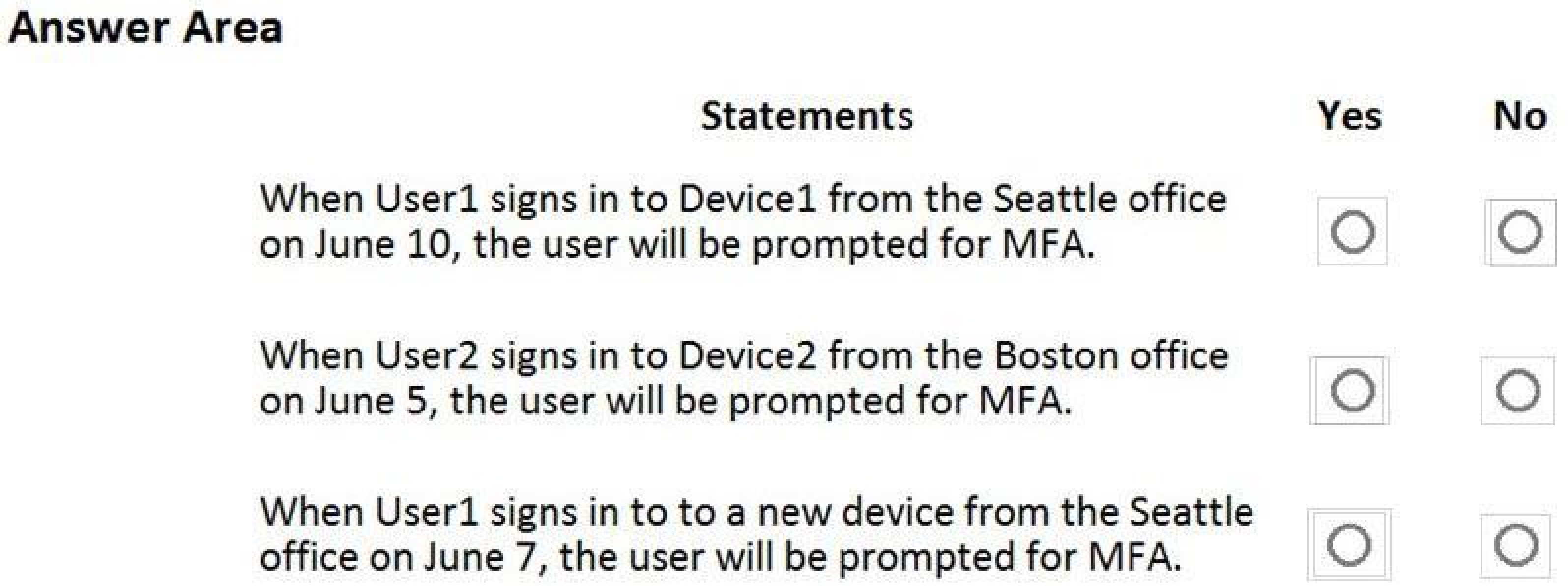
☑ Allow users to remember multi-factor authentication on devices they trust

Days before a device must re-authenticate (1-60): 14

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

NOTE: Each correct selection is worth one point.

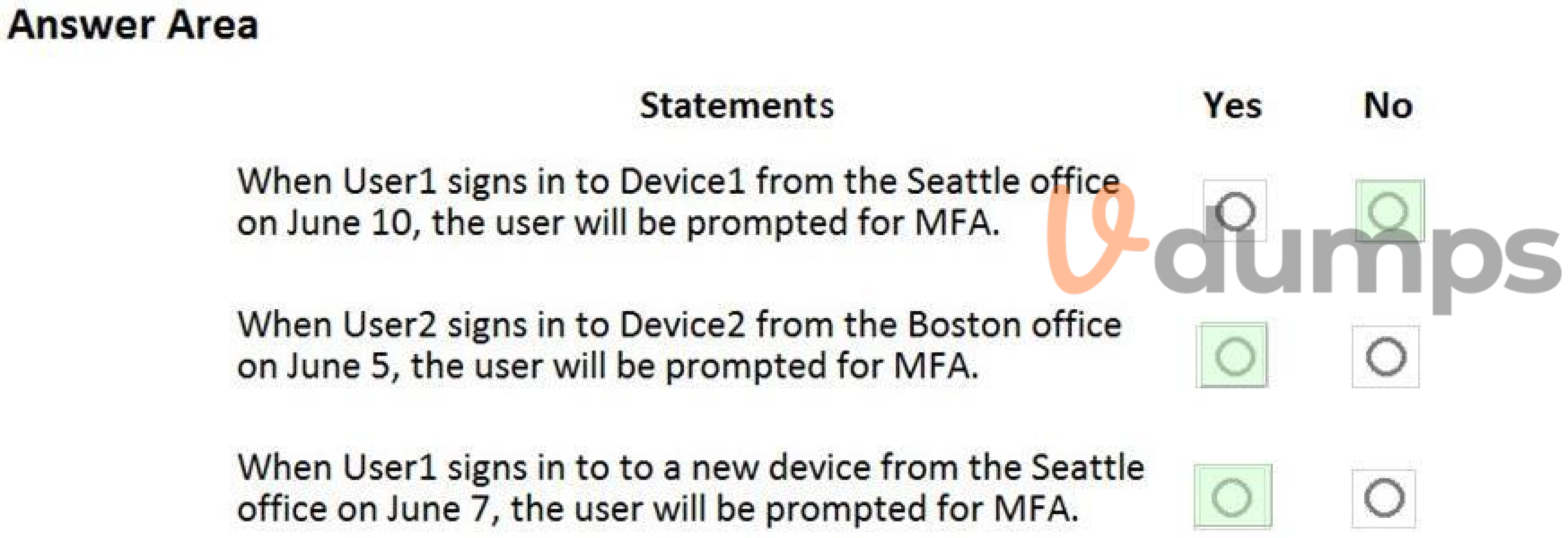
**Hot Area:**



## Answer Area

| Statements | Yes | No |
|---|---|---|
| When User1 signs in to Device1 from the Seattle office on June 10, the user will be prompted for MFA. | ○ | ○ |
| When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA. | ○ | ○ |
| When User1 signs in to to a new device from the Seattle office on June 7, the user will be prompted for MFA. | ○ | ○ |

**Answer Area:**



## Answer Area

| Statements | Yes | No |
|---|---|---|
| When User1 signs in to Device1 from the Seattle office on June 10, the user will be prompted for MFA. | ○ | [✓ ○] |
| When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA. | [✓ ○] | ○ |
| When User1 signs in to to a new device from the Seattle office on June 7, the user will be prompted for MFA. | [✓ ○] | ○ |

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

**QUESTION 34**
You have an Azure subscription.
You configure the subscription to use a different Azure Active Directory (Azure AD) tenant.
What are two possible effects of the change? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Role assignments at the subscription level are lost.
B. Virtual machine managed identities are lost.
C. Virtual machine disk snapshots are lost.
D. Existing Azure resources are deleted.

**Correct Answer: A, B**

**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory

**QUESTION 35**
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.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.
You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to Sa1.
Solution: You generate new SASs.
Does this meet the goal?

A. Yes
B. No

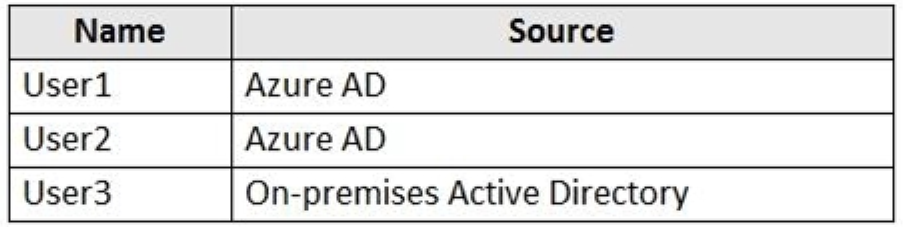
**Correct Answer: B**
**Section:**
**Explanation:**
Instead you should create a new stored access policy.
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy.
Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.
References:
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

**QUESTION 36**
You have an Azure subscription that contains virtual machines.
You enable just in time (JIT) VM access to all the virtual machines.
You need to connect to a virtual machine by using Remote Desktop.
What should you do first?

A. From Azure Directory (Azure AD) Privileged Identity Management (PIM), activate the Security administrator user role.
B. From Azure Active Directory (Azure AD) Privileged Identity Management (PIM), activate the Owner role for the virtual machine.
C. From the Azure portal, select the virtual machine, select Connect, and then select Request access.
D. From the Azure portal, select the virtual machine and add the Network Watcher Agent virtual machine extension.

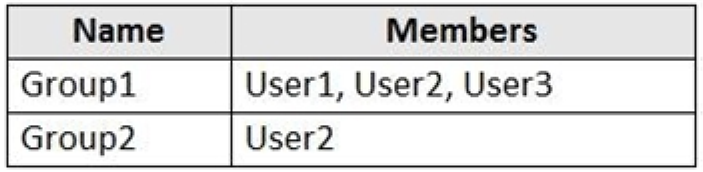
**Correct Answer: C**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/connect-logon

**QUESTION 37**
HOTSPOT
Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.



| Name | Source |
|---|---|
| User1 | Azure AD |
| User2 | Azure AD |
| User3 | On-premises Active Directory |

The tenant contains the groups shown in the following table.

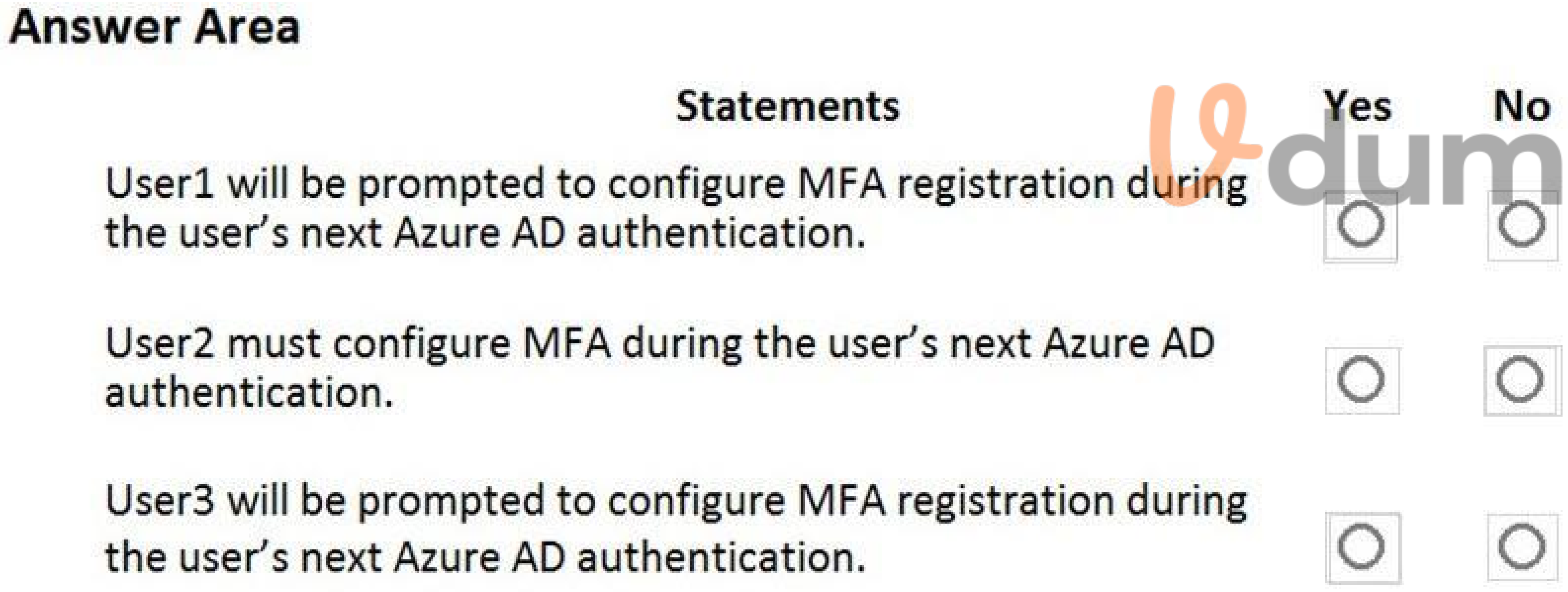


| Name | Members |
|---|---|
| Group1 | User1, User2, User3 |
| Group2 | User2 |

You configure a multi-factor authentication (MFA) registration policy that has the following settings:
Assignments:
- Include: Group1
- Exclude Group2

Controls: Require Azure MFA registration
Enforce Policy: On
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

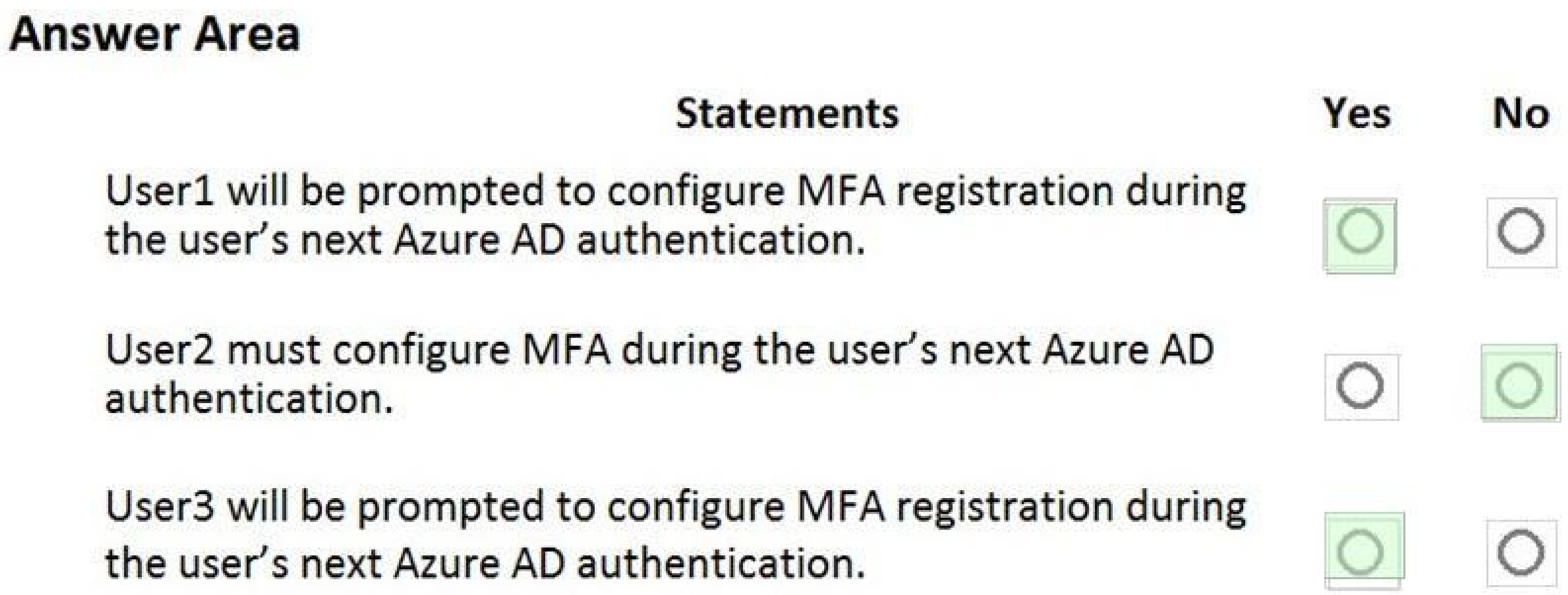
**Hot Area:**



**Answer Area**

| Statements | Yes | No |
|---|---|---|
| User1 will be prompted to configure MFA registration during the user's next Azure AD authentication. | ○ | ○ |
| User2 must configure MFA during the user's next Azure AD authentication. | ○ | ○ |
| User3 will be prompted to configure MFA registration during the user's next Azure AD authentication. | ○ | ○ |

**Answer Area:**



## Answer Area

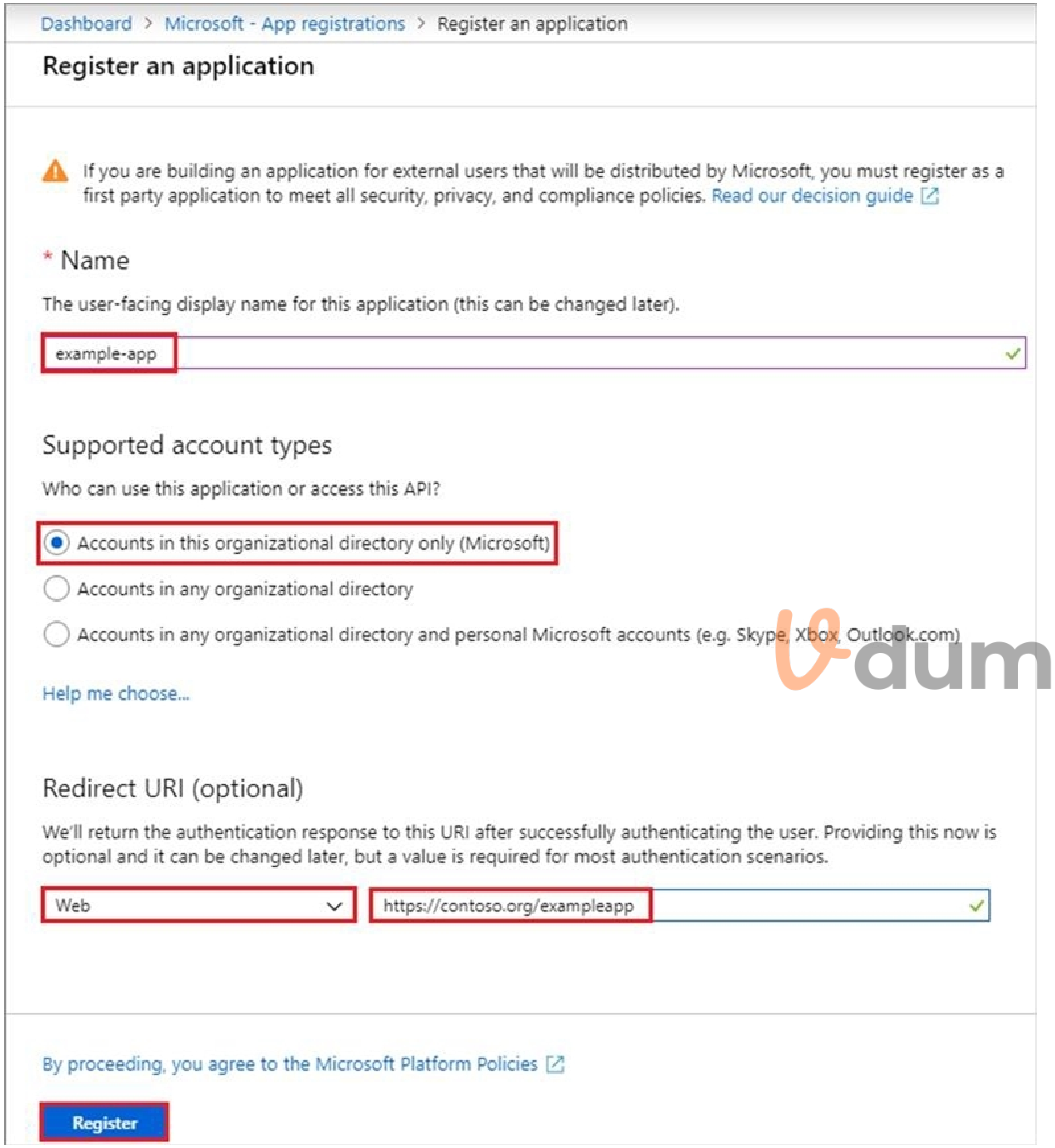
| Statements | Yes | No |
|---|---|---|
| User1 will be prompted to configure MFA registration during the user's next Azure AD authentication. | [✓ ○] | ○ |
| User2 must configure MFA during the user's next Azure AD authentication. | ○ | [✓ ○] |
| User3 will be prompted to configure MFA registration during the user's next Azure AD authentication. | [✓ ○] | ○ |

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

**QUESTION 38**
SIMULATION
The developers at your company plan to publish an app named App11641655 to Azure.
You need to ensure that the app is registered to Azure Active Directory (Azure AD). The registration must use the sign-on URLs of https://app.contoso.com.
To complete this task, sign in to the Azure portal and modify the Azure resources.

A.

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
Step 1: Register the Application
1. Sign in to your Azure Account through the Azure portal.
2. Select Azure Active Directory.
3. Select App registrations.
4. Select New registration.
5. Name the application App11641655. Select a supported account type, which determines who can use the application. Under Redirect URI, select Web for the type of application you want to create. Enter the URI: https://app.contoso.com , where the access token is sent to.



Dashboard > Microsoft - App registrations > Register an application

Register an application

If you are building an application for external users that will be distributed by Microsoft, you must register as a first party application to meet all security, privacy, and compliance policies. Read our decision guide

* Name

The user-facing display name for this application (this can be changed later).

example-app

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Microsoft)

○ Accounts in any organizational directory

○ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

https://contoso.org/exampleapp

By proceeding, you agree to the Microsoft Platform Policies

6. Click Register
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

**QUESTION 39**

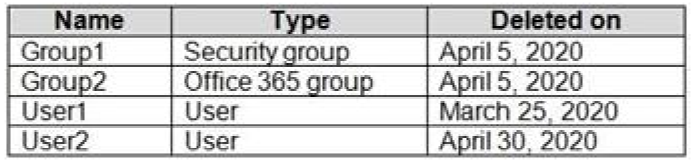
You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

The User administrator role is assigned to a user named Admin1.
An external partner has a Microsoft account that uses the user1@outlook.com sign in.
Admin1 attempts to invite the external partner to sign in to the Azure AD tenant and receives the following error message: "Unable to invite user user1@outlook.com Generic authorization exception."
You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant.
What should you do?

A. From the Roles and administrators blade, assign the Security administrator role to Admin1.
B. From the Organizational relationships blade, add an identity provider.
C. From the Custom domain names blade, add a custom domain.
D. From the Users blade, modify the External collaboration settings.

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

**QUESTION 40**
You have an Azure Active Directory (Azure AD) tenant.
You have the deleted objects shown in the following table.



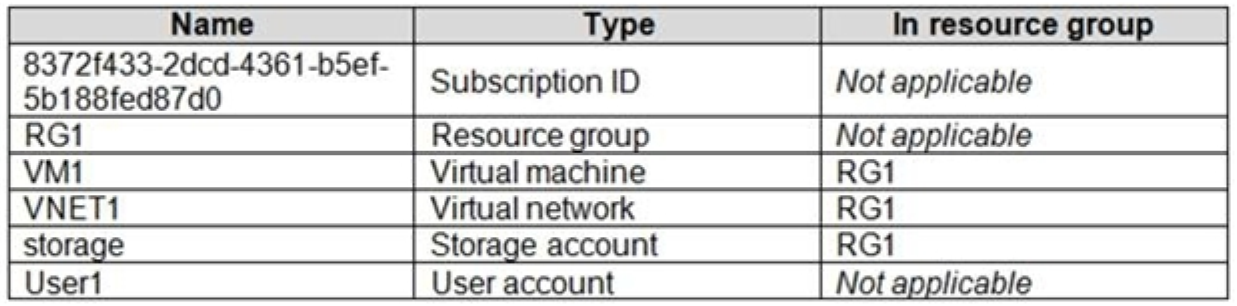
| Name | Type | Deleted on |
|---|---|---|
| Group1 | Security group | April 5, 2020 |
| Group2 | Office 365 group | April 5, 2020 |
| User1 | User | March 25, 2020 |
| User2 | User | April 30, 2020 |

On May 4, 2020, you attempt to restore the deleted objects by using the Azure Active Directory admin center.
Which two objects can you restore? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Group1
B. Group2
C. User2
D. User1

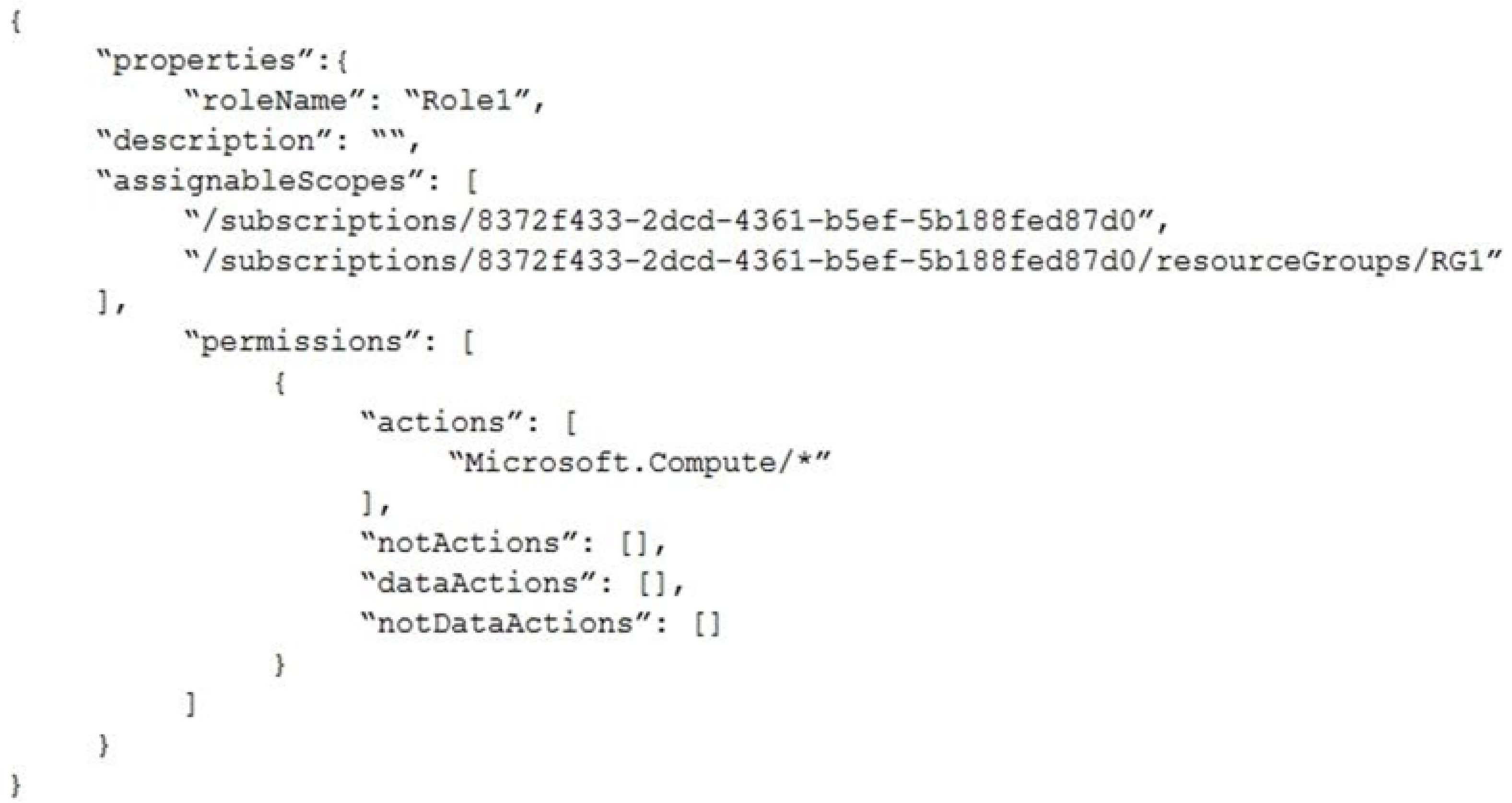
**Correct Answer: B, C**
**Section:**
**Explanation:**
Deleted users and deleted Office 365 groups are available for restore for 30 days.
You cannot restore a deleted security group.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-restore-deleted

**QUESTION 41**
HOTSPOT
You have an Azure subscription named Subscription1 that contains the resources shown in the following table.



| Name | Type | In resource group |
|---|---|---|
| 8372f433-2dcd-4361-b5ef-5b188fed87d0 | Subscription ID | *Not applicable* |
| RG1 | Resource group | *Not applicable* |
| VM1 | Virtual machine | RG1 |
| VNET1 | Virtual network | RG1 |
| storage | Storage account | RG1 |
| User1 | User account | *Not applicable* |

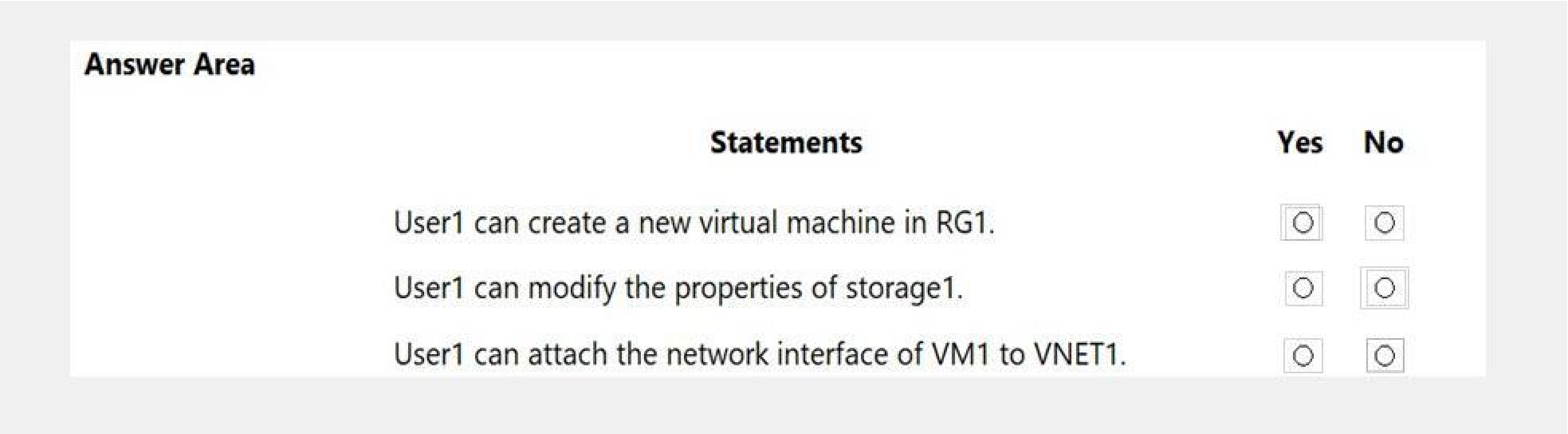
You create an Azure role by using the following JSON file.



```
{
     “properties”:{
          “roleName”: “Role1”,
     “description”: “”,
     “assignableScopes”: [
          “/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0”,
          “/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG1”
     ],
          “permissions”: [
               {
                    “actions”: [
                         “Microsoft.Compute/*”
                    ],
                    “notActions”: [],
                    “dataActions”: [],
                    “notDataActions”: []
               }
          ]
     }
}
```

You assign Role1 to User1 for 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.

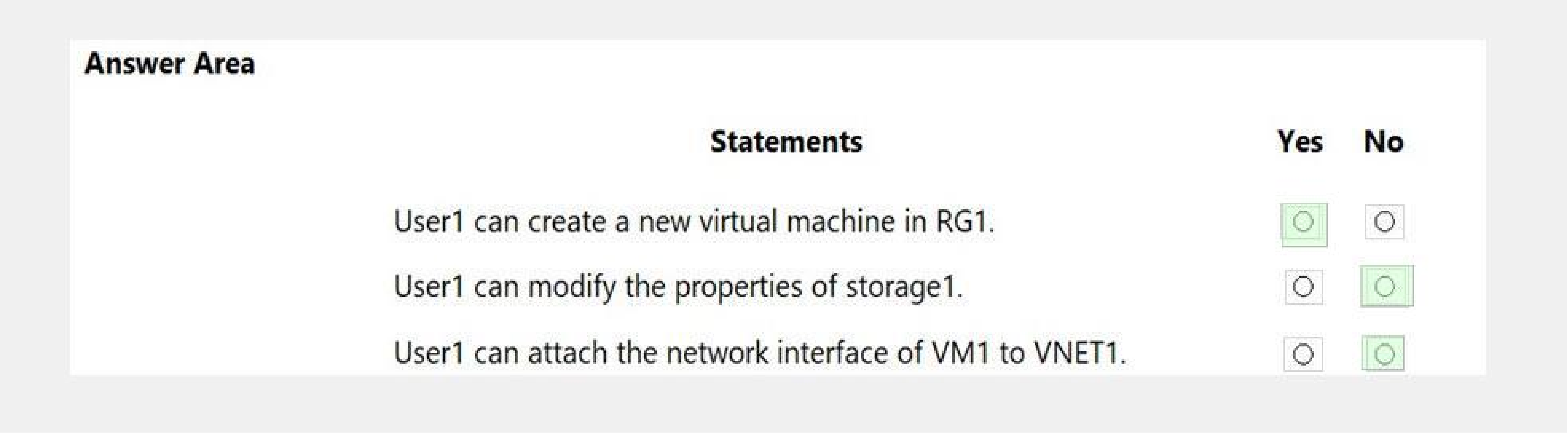
**Hot Area:**



**Answer Area**

| Statements | Yes | No |
|---|---|---|
| User1 can create a new virtual machine in RG1. | ○ | ○ |
| User1 can modify the properties of storage1. | ○ | ○ |
| User1 can attach the network interface of VM1 to VNET1. | ○ | ○ |

**Answer Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| User1 can create a new virtual machine in RG1. | [✓ ○] | ○ |
| User1 can modify the properties of storage1. | ○ | [✓ ○] |
| User1 can attach the network interface of VM1 to VNET1. | ○ | [✓ ○] |

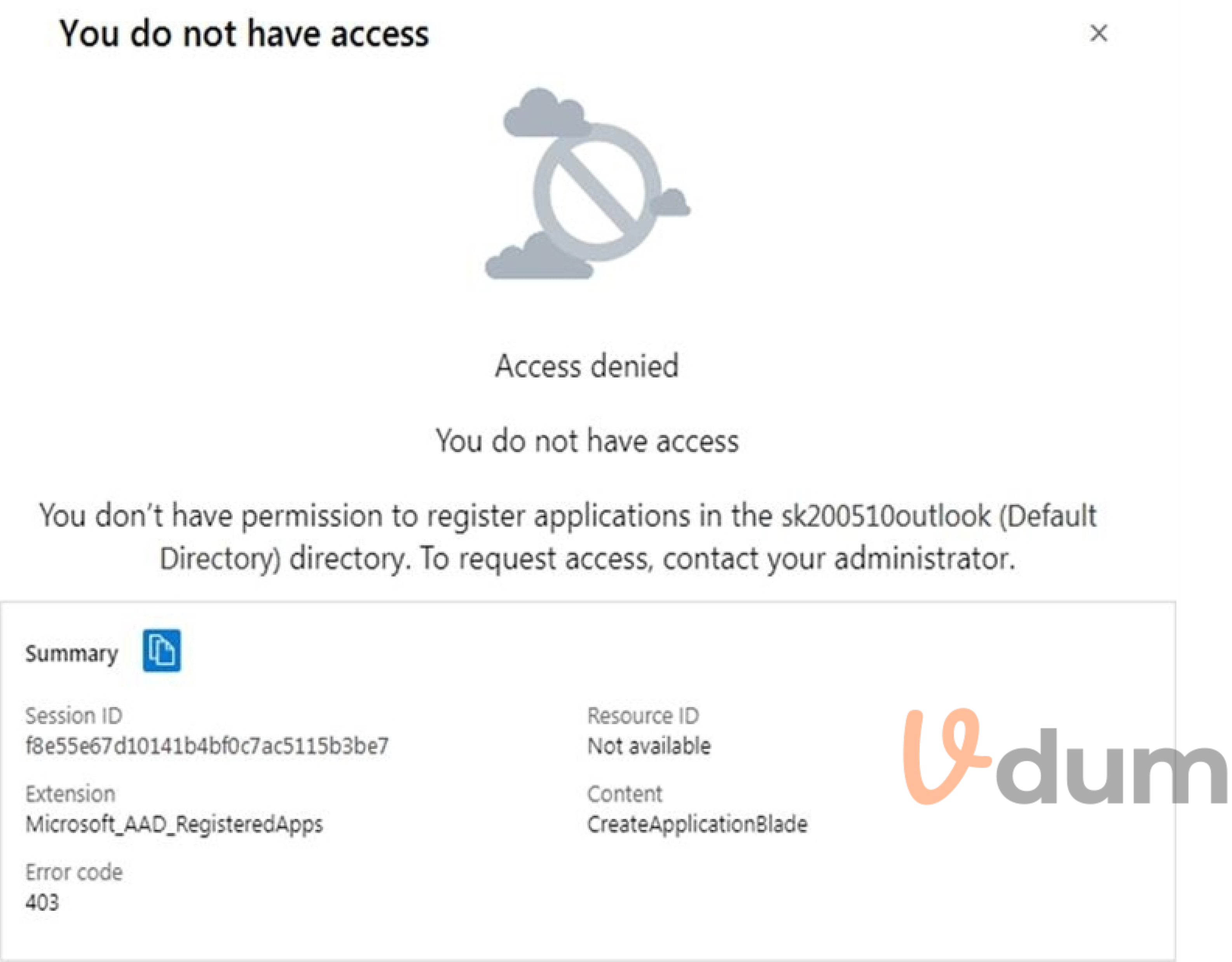
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#compute

**QUESTION 42**
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1.
You plan to publish several apps in the tenant.
You need to ensure that User1 can grant admin consent for the published apps.
Which two possible user roles can you assign to User1 to achieve this goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Security administrator
B. Cloud application administrator
C. Application administrator
D. User administrator
E. Application developer

**Correct Answer: B, C**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent

**QUESTION 43**
You have an Azure subscription that is associated with an Azure Active Directory (Azure AD) tenant.
When a developer attempts to register an app named App1 in the tenant, the developer receives the error message shown in the following exhibit.



You do not have access

Access denied

You do not have access

You don’t have permission to register applications in the sk200510outlook (Default Directory) directory. To request access, contact your administrator.

Summary

Session ID
f8e55e67d10141b4bf0c7ac5115b3be7

Resource ID
Not available

Extension
Microsoft_AAD_RegisteredApps

Content
CreateApplicationBlade

Error code
403

You need to ensure that the developer can register App1 in the tenant.
What should you do for the tenant?

A. Modify the Directory properties.

B. Set Enable Security defaults to Yes.

C. Configure the Consent and permissions settings for enterprise applications.

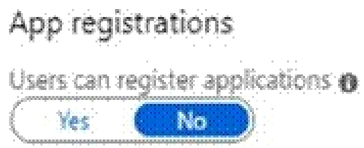
D. Modify the User settings.

**Correct Answer: D**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

**QUESTION 44**

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant and a user named User1.

The App registrations settings for the tenant are configured as shown in the following exhibit.



App registrations

Users can register applications

Yes [✓ No]

You plan to deploy an app named App1.

You need to ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.

Which role should you assign to User1?

A. App Configuration Data Owner for the subscription

B. Managed Application Contributor for the subscription

C. Cloud application administrator in Azure AD

D. Application developer in Azure AD

**Correct Answer: D**

**Section:**

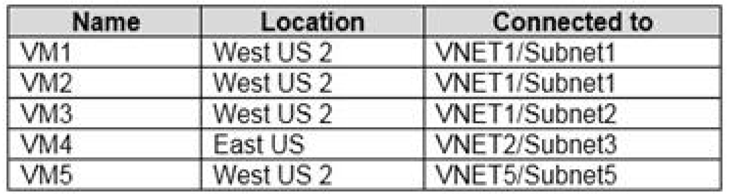
**Explanation:**

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task

**QUESTION 45**

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



| Name | Location | Connected to |
|---|---|---|
| VM1 | West US 2 | VNET1/Subnet1 |
| VM2 | West US 2 | VNET1/Subnet1 |
| VM3 | West US 2 | VNET1/Subnet2 |
| VM4 | East US | VNET2/Subnet3 |
| VM5 | West US 2 | VNET5/Subnet5 |

Each virtual machine has a single network interface.

You add the network interface of VM1 to an application security group named ASG1.

You need to identify the network interfaces of which virtual machines you can add to ASG1.

What should you identify?

A. VM2 only

B. VM2 and VM3 only

C. VM2, VM3, VM4, and VM5

D. VM2, VM3, and VM5 only

**Correct Answer: B**

**Section:**

**Explanation:**

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups

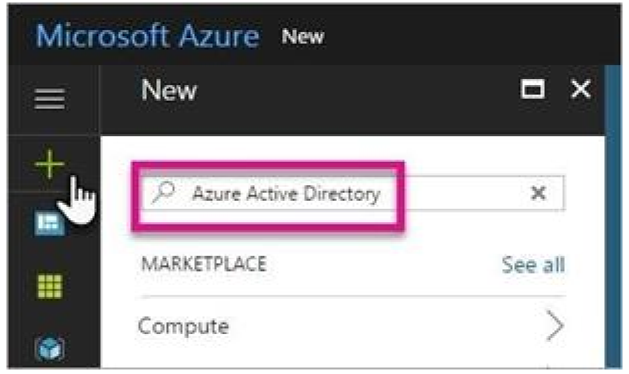
**QUESTION 46**

SIMULATION

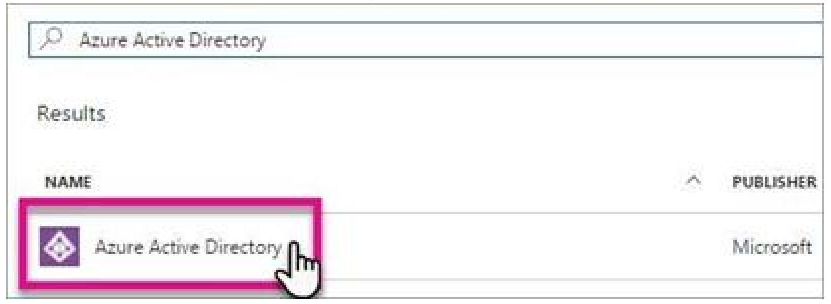
You need to create a new Azure Active Directory (Azure AD) directory named 10317806.onmicrosoft.com. The new directory must contain a user named user10317806 who is configured to sign in by using Azure Multi-Factor Authentication (MFA).

A.

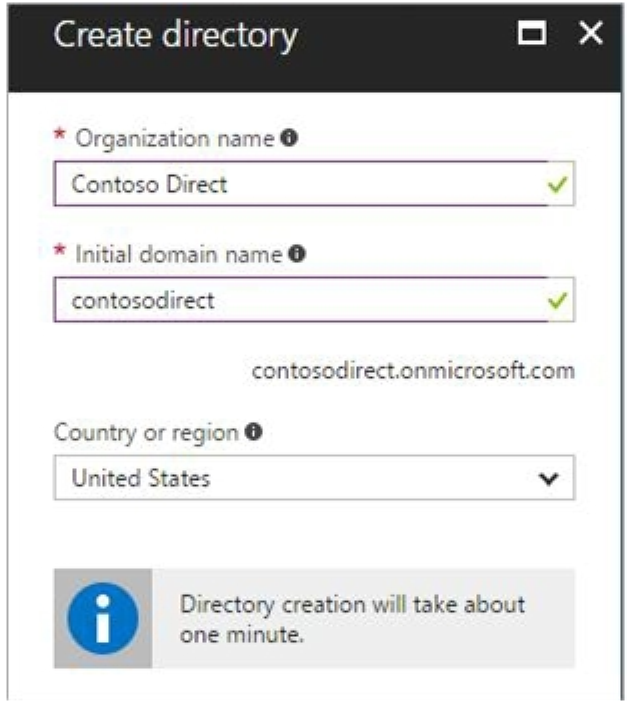
**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
To create a new Azure AD tenant:
1. Browse to the Azure portal and sign in with an account that has an Azure subscription.
2. Select the plus icon (+) and search for Azure Active Directory.



3. Select Azure Active Directory in the search results.



4. Select Create.
5. Provide an Organization name (10317806) and an Initial domain name (10317806). Then select Create. This will create the directory named 10317806.onmicrosoft.com.


Create directory

* Organization name: Contoso Direct

* Initial domain name: contosodirect

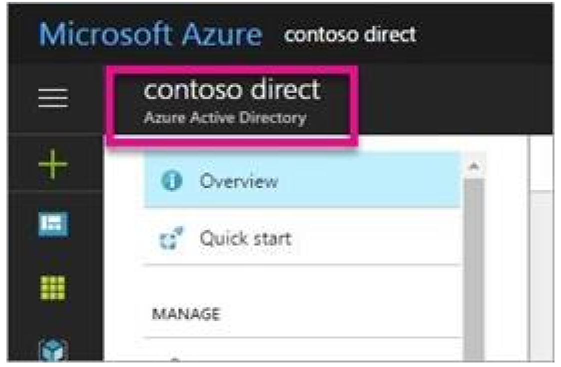
contosodirect.onmicrosoft.com

Country or region: United States

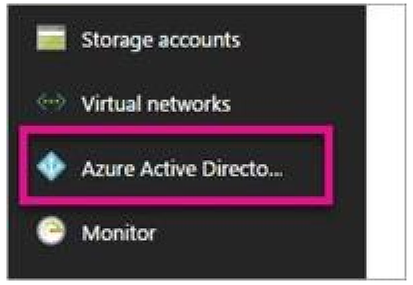
Directory creation will take about one minute.

6. After directory creation is complete, select the information box to manage your new directory.
To create the user:

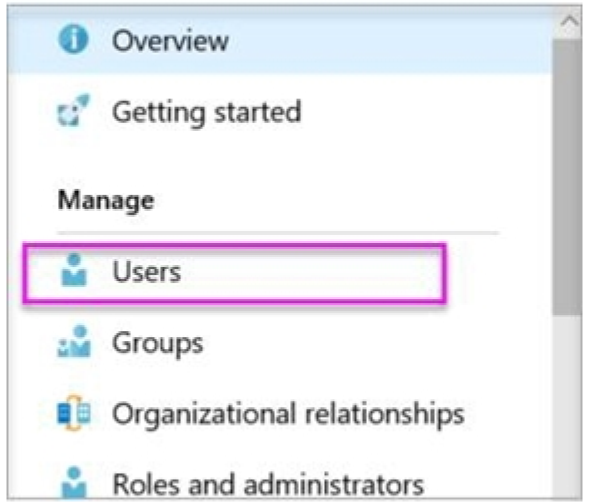
1. In the Azure portal, make sure you are on the Azure Active Directory fly out.



If not, select the Azure Active Directory icon from the left services navigation.



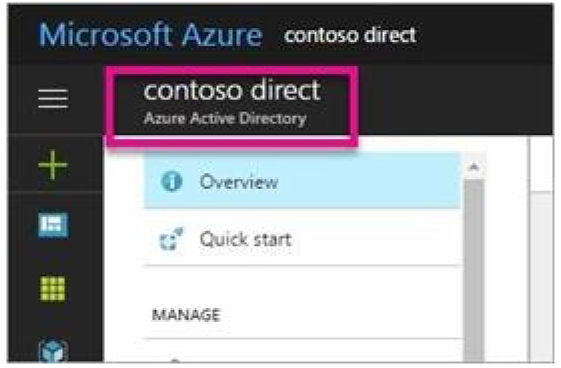
2. Under Manage, select Users.



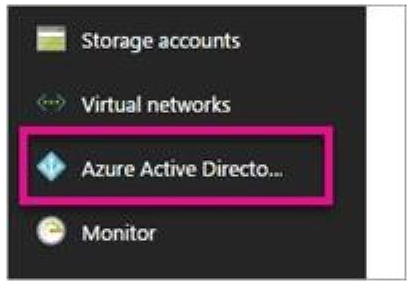
3. Select All users and then select + New user.
4. Provide a Name and User name (user10317806) for the user. When you're done, select Create.

To enable MFA:

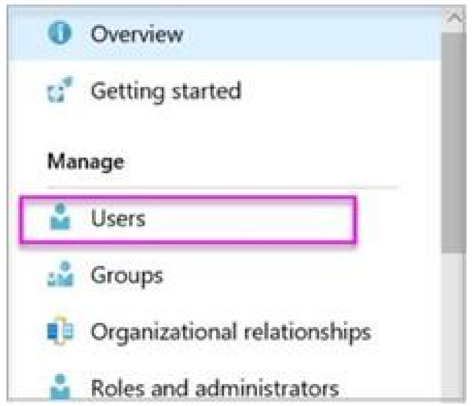
1. In the Azure portal, make sure you are on the Azure Active Directory fly out.



If not, select the Azure Active Directory icon from the left services navigation.



2. Under Manage, select Users.



3. Click on the Multi-Factor Authentication link.
4. Tick the checkbox next to the user's name and click the Enable link.
Reference:
https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant

**QUESTION 47**
You have an Azure subscription named Subcription1 that contains an Azure Active Directory (Azure AD) tenant named contoso.com and a resource group named RG1.
You create a custom role named Role1 for contoso.com.
Where you can use Role1 for permission delegation?

A. contoso.com only
B. contoso.com and RG1 only
C. contoso.com and Subscription1 only
D. contoso.com, RG1, and Subscription1

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

**QUESTION 48**
You have an Azure subscription.
You enable Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
Your company's security policy for administrator accounts has the following conditions:
The accounts must use multi-factor authentication (MFA).
The accounts must use 20-character complex passwords.
The passwords must be changed every 180 days.
The accounts must be managed by using PIM.
You receive multiple alerts about administrators who have not changed their password during the last 90 days.
You need to minimize the number of generated alerts.
Which PIM alert should you modify?

A. Roles are being assigned outside of Privileged Identity Management

B. Roles don't require multi-factor authentication for activation
C. Administrators aren't using their privileged roles
D. Potential stale accounts in a privileged role

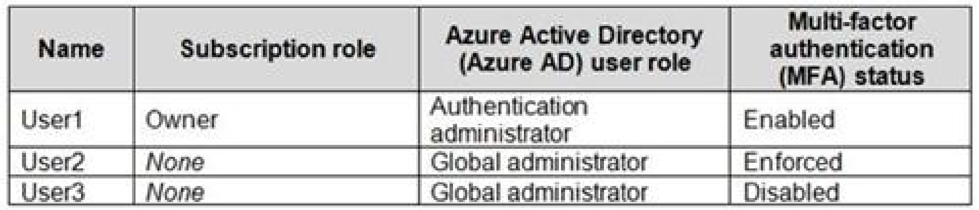
**Correct Answer: D**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new

**QUESTION 49**
Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD). Azure AD Connect is installed on a domain member server named Server1.
You need to ensure that a domain administrator for the adatum.com domain can modify the synchronization options. The solution must use the principle of least privilege. Which Azure AD role should you assign to the domain administrator?

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

**Correct Answer: B**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

**QUESTION 50**
You have an Azure subscription that contains the users shown in the following table.



| Name | Subscription role | Azure Active Directory (Azure AD) user role | Multi-factor authentication (MFA) status |
|---|---|---|---|
| User1 | Owner | Authentication administrator | Enabled |
| User2 | *None* | Global administrator | Enforced |
| User3 | *None* | Global administrator | Disabled |

Which users can enable Azure AD Privileged Identity Management (PIM)?

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

**Correct Answer: D**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

**QUESTION 51**
You have an Azure subscription.
You plan to create a custom role-based access control (RBAC) role that will provide permission to read the Azure Storage account.

Which property of the RBAC role definition should you configure?

A. NotActions []
B. DataActions []
C. AssignableScopes []
D. Actions []

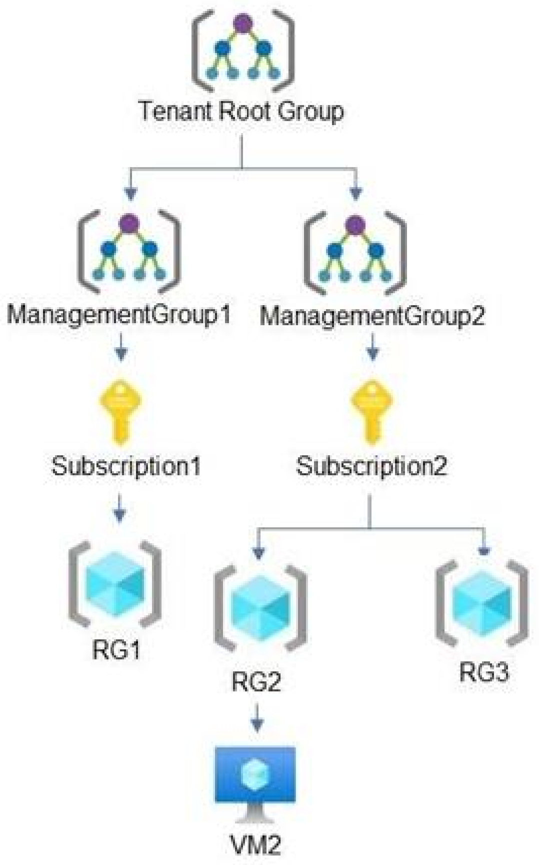
**Correct Answer: D**
**Section:**
**Explanation:**
To 'Read a storage account', ie. list the blobs in the storage account, you need an 'Action' permission. To read the data in a storage account, ie. open a blob, you need a 'DataAction' permission.
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-definitions

**QUESTION 52**
You have an Azure subscription linked to an Azure Active Directory Premium Plan 1 tenant.
You plan to implement Azure Active Directory (Azure AD) Identity Protection.
You need to ensure that you can configure a user risk policy and a sign-in risk policy.
What should you do first?

A. Purchase Azure Active Directory Premium Plan 2 licenses for all users.
B. Register all users for Azure Multi-Factor Authentication (MFA).
C. Enable security defaults for Azure AD.
D. Enable Azure Defender in Azure Security Center.

**Correct Answer: A**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa

**QUESTION 53**
HOTSPOT
You have the hierarchy of Azure resources shown in the following exhibit.

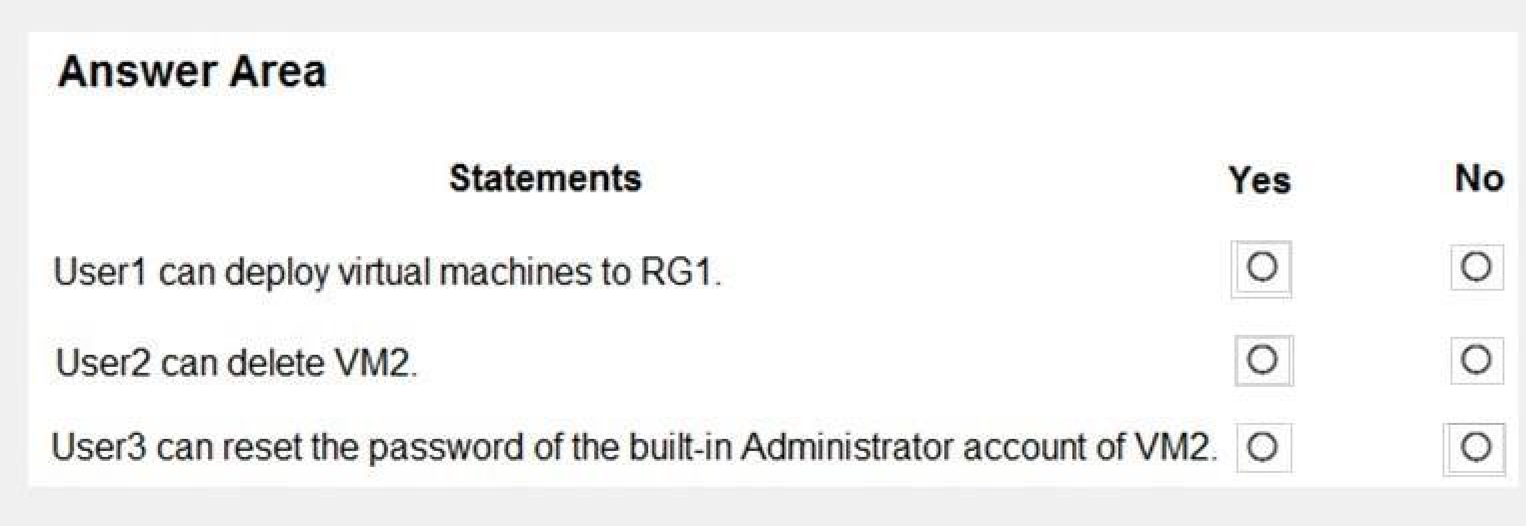


RG1, RG2, and RG3 are resource groups.
RG2 contains a virtual machine named VM1.
You assign role-based access control (RBAC) roles to the users shown in the following table.

| Name | Role | Added to resource |
|---|---|---|
| User1 | Contributor | Tenant Root Group |
| User2 | Virtual Machine Contributor | Subscription2 |
| User3 | Virtual Machine Administrator Login | RG2 |

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

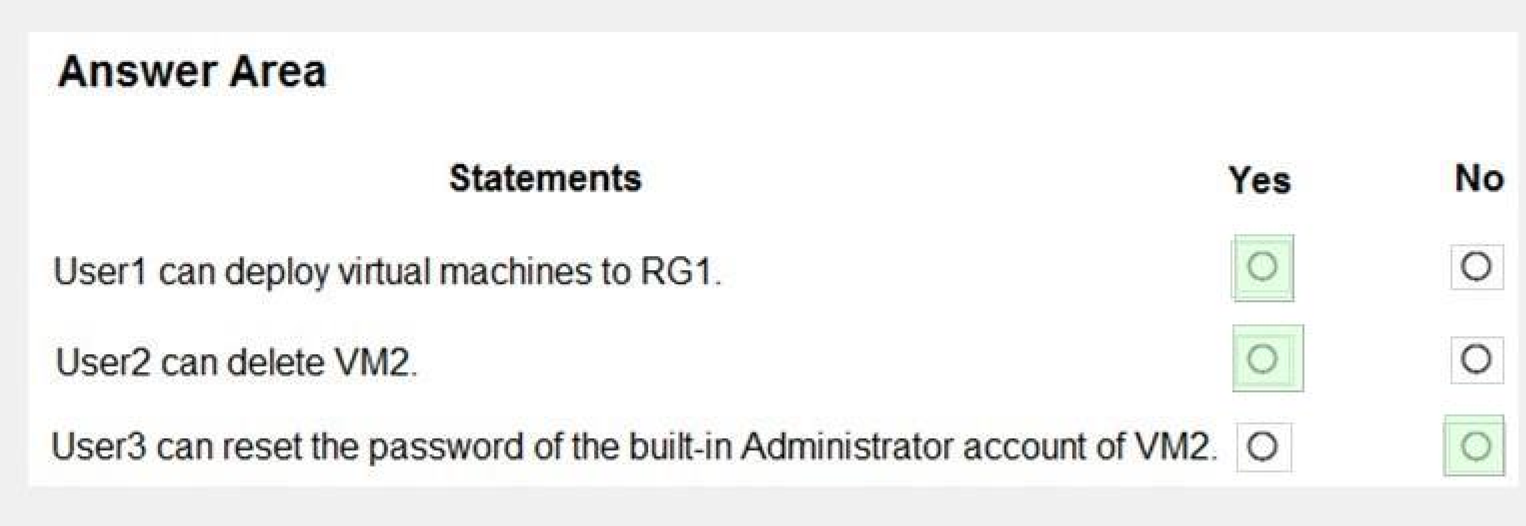
**Hot Area:**



## Answer Area

| Statements | Yes | No |
|---|---|---|
| User1 can deploy virtual machines to RG1. | ○ | ○ |
| User2 can delete VM2. | ○ | ○ |
| User3 can reset the password of the built-in Administrator account of VM2. | ○ | ○ |

**Answer Area:**



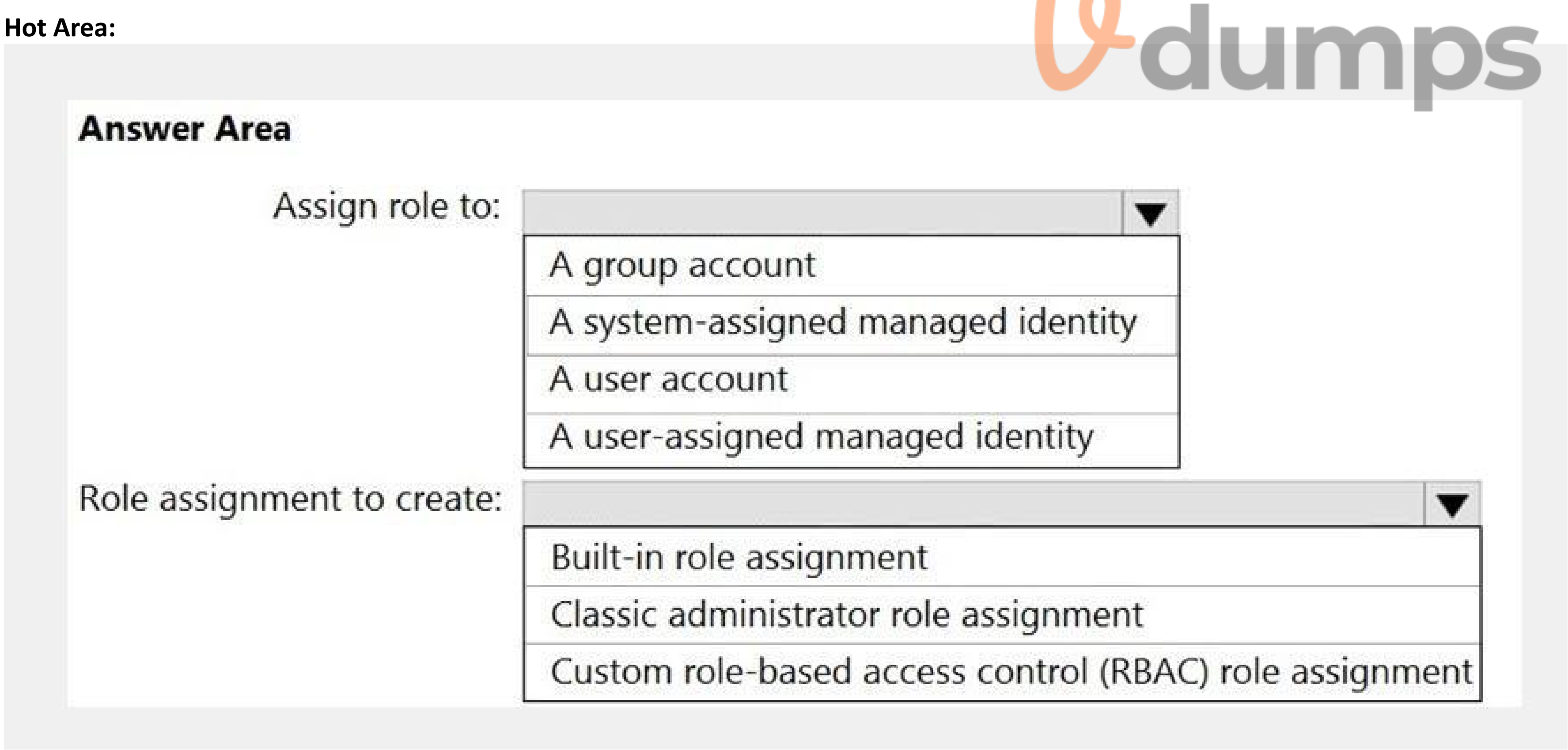
**Answer Area**

| Statements | Yes | No |
|---|---|---|
| User1 can deploy virtual machines to RG1. | [✓ ○] | ○ |
| User2 can delete VM2. | [✓ ○] | ○ |
| User3 can reset the password of the built-in Administrator account of VM2. | ○ | [✓ ○] |

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

**QUESTION 54**
HOTSPOT
You plan to implement an Azure function named Function1 that will create new storage accounts for containerized application instances.
You need to grant Function1 the minimum required privileges to create the storage accounts. The solution must minimize administrative effort.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**

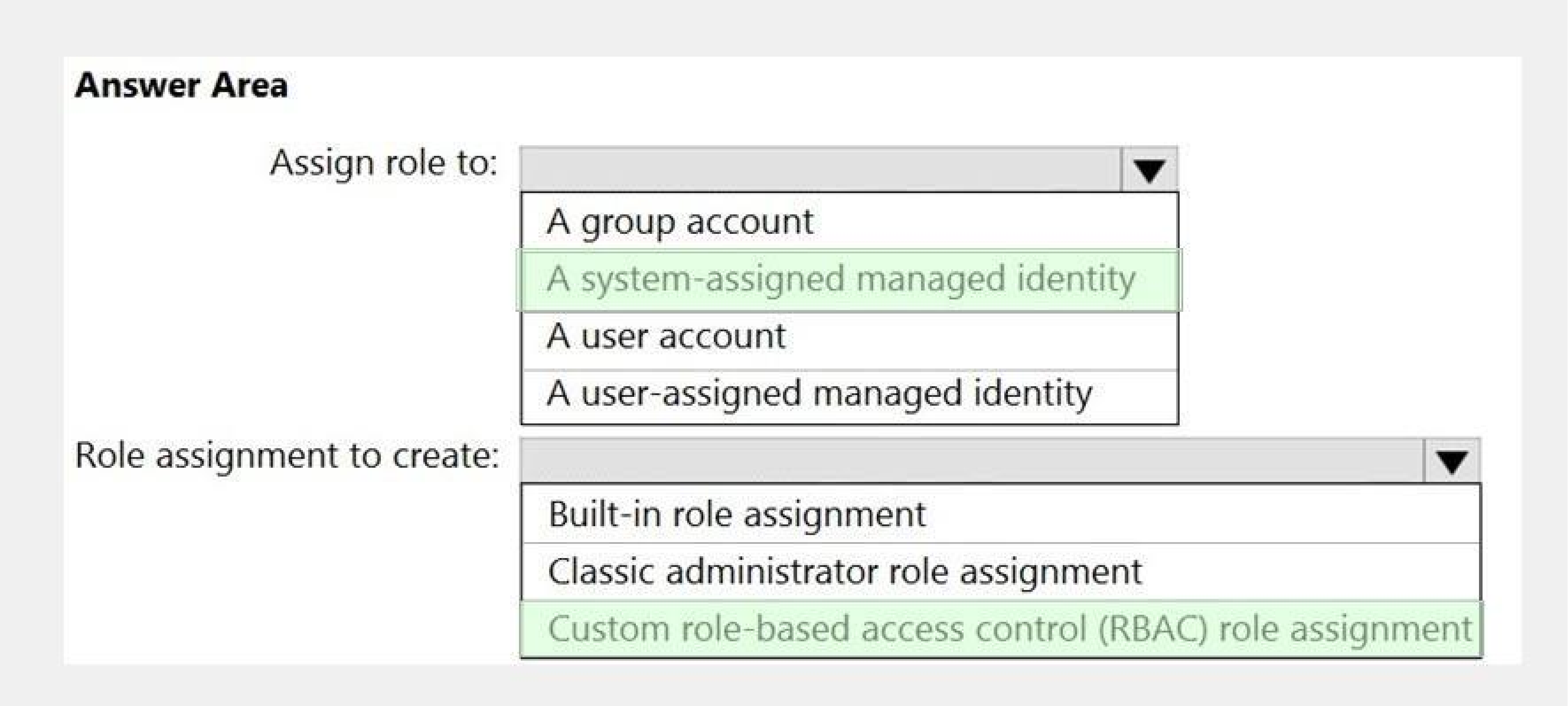


**Answer Area**

Assign role to: ▼
- A group account
- A system-assigned managed identity
- A user account
- A user-assigned managed identity

Role assignment to create: ▼
- Built-in role assignment
- Classic administrator role assignment
- Custom role-based access control (RBAC) role assignment

**Answer Area:**



**Answer Area**

Assign role to:

- A group account
- [✓ A system-assigned managed identity]
- A user account
- A user-assigned managed identity

Role assignment to create:

- Built-in role assignment
- Classic administrator role assignment
- [✓ Custom role-based access control (RBAC) role assignment]

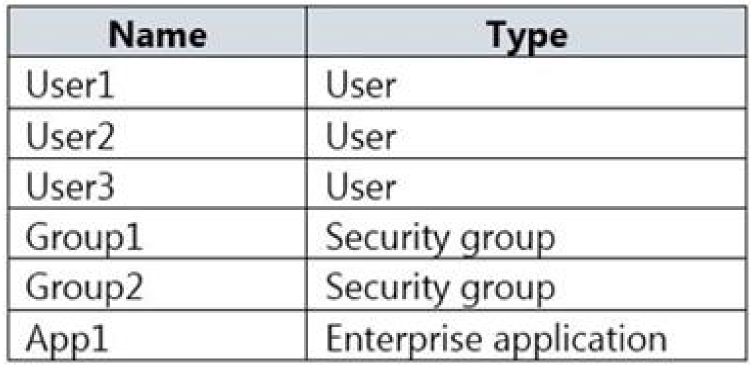
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/howto-assign-access-portal

**QUESTION 55**
You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant.
You need to grant Function1 the minimum required privileges.
Which additional resource will be created in Azure AD?

A. a service principal
B. an X.509 certificate
C. a managed identity
D. a user account

**Correct Answer: A**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

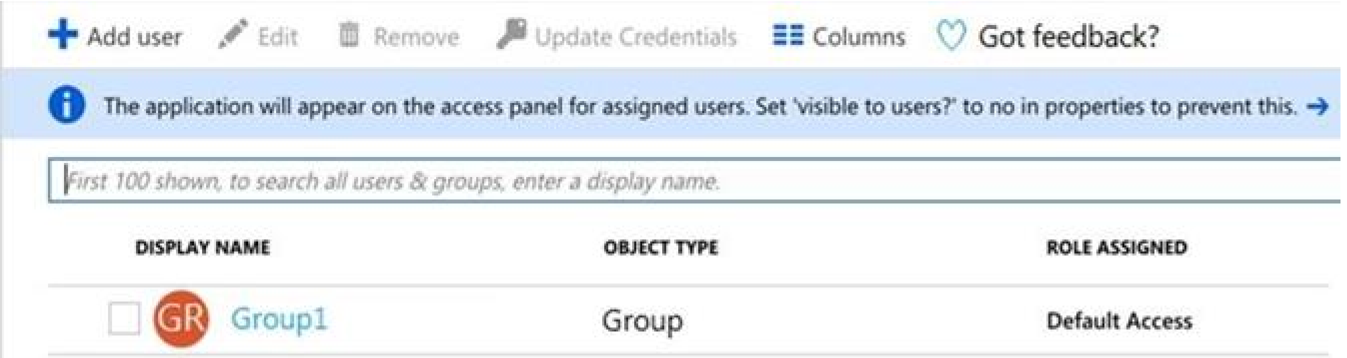
**QUESTION 56**
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant that contains the resources shown in the following table.



| Name | Type |
|---|---|
| User1 | User |
| User2 | User |
| User3 | User |
| Group1 | Security group |
| Group2 | Security group |
| App1 | Enterprise application |

User2 is the owner of Group2.

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

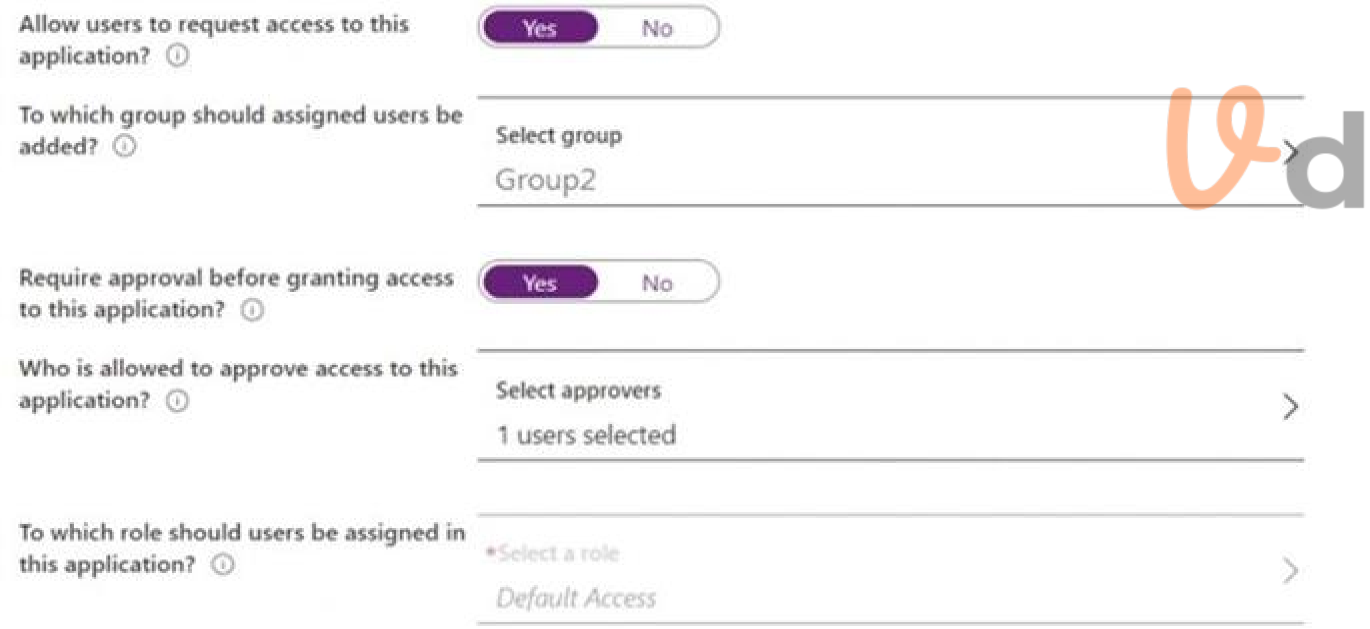


The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

| DISPLAY NAME | OBJECT TYPE | ROLE ASSIGNED |
|---|---|---|
| □ GR Group1 | Group | Default Access |

You enable self-service application access for App1 as shown in the following exhibit.



Allow users to request access to this application? ⓘ [✓ Yes] No

To which group should assigned users be added? ⓘ Select group: Group2

Require approval before granting access to this application? ⓘ [✓ Yes] No

Who is allowed to approve access to this application? ⓘ Select approvers: 1 users selected

To which role should users be assigned in this application? ⓘ *Select a role: Default Access

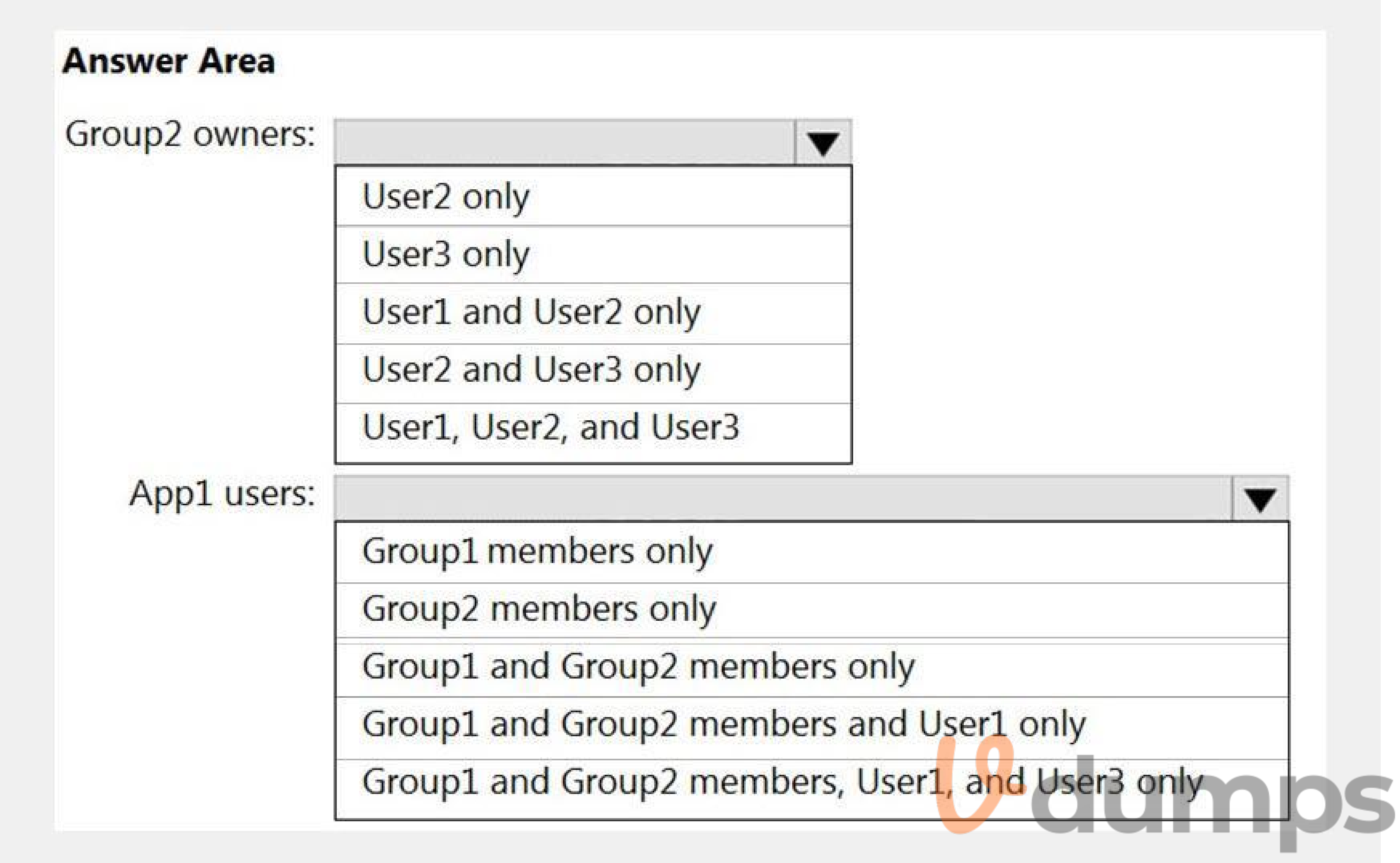
User3 is configured to approve access to Appl.

You need to identify the owners of Group2 and the users of Appl.

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**

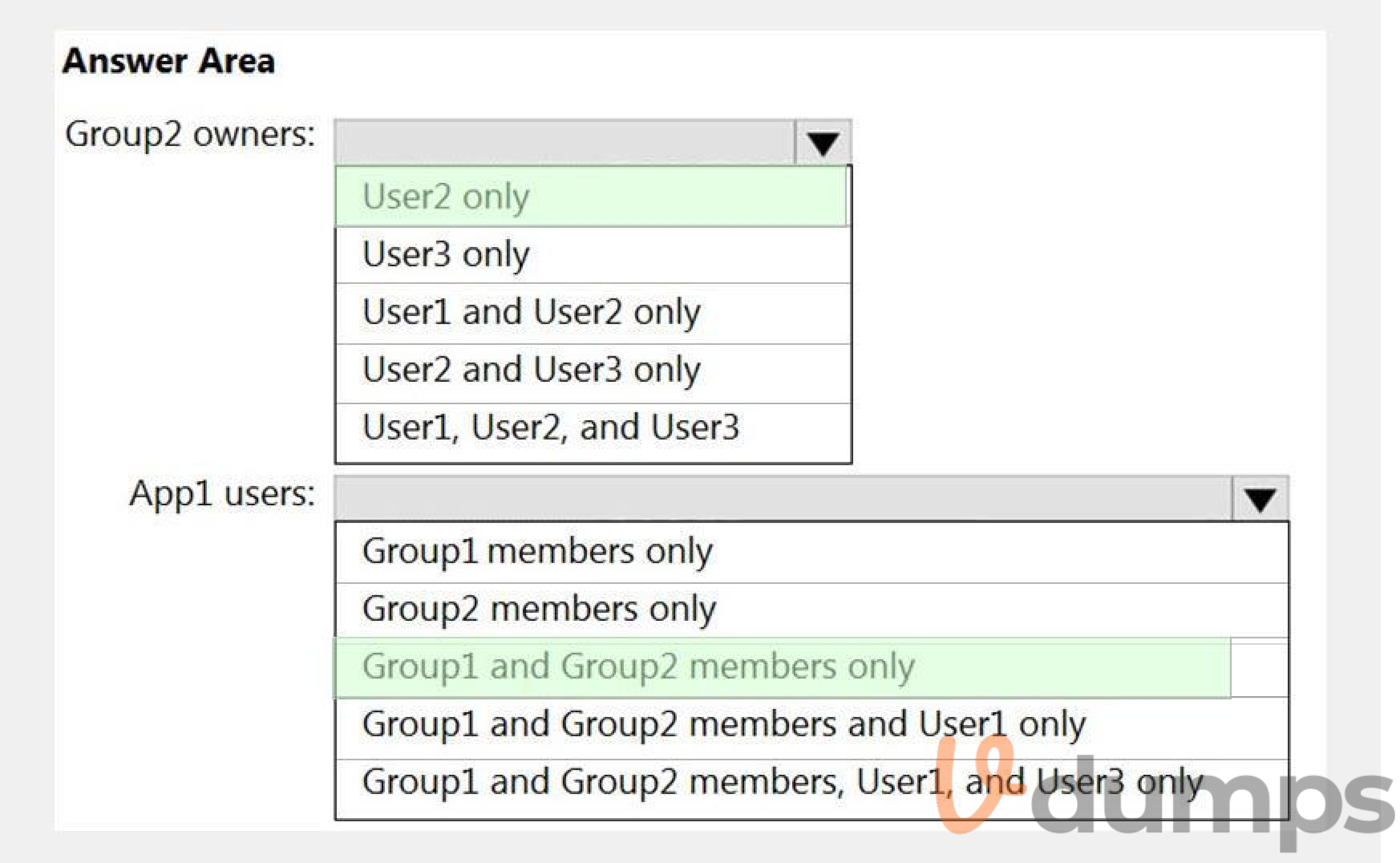
Group2 owners: ▼

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

App1 users: ▼

- Group1 members only
- Group2 members only
- Group1 and Group2 members only
- Group1 and Group2 members and User1 only
- Group1 and Group2 members, User1, and User3 only

**Answer Area:**



**Answer Area**

Group2 owners:

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

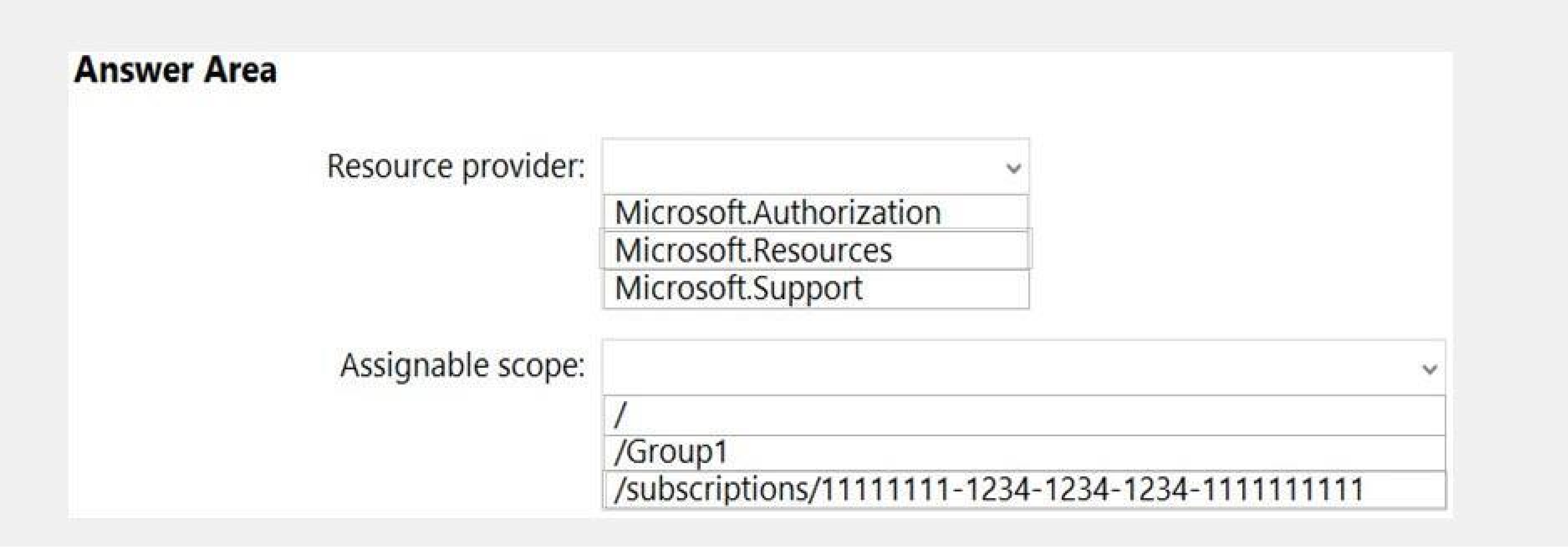
App1 users:

- Group1 members only
- Group2 members only
- [✓ Group1 and Group2 members only]
- Group1 and Group2 members and User1 only
- Group1 and Group2 members, User1, and User3 only

**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access

**QUESTION 57**
HOTSPOT
You have a management group named Group1 that contains an Azure subscription named sub1. Sub1 has a subscription ID of 11111111-1234-1234-1234-1111111111.
You need to create a custom Azure role-based access control (RBAC) role that will delegate permissions to manage the tags on all the objects in Group1.
What should you include in 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**

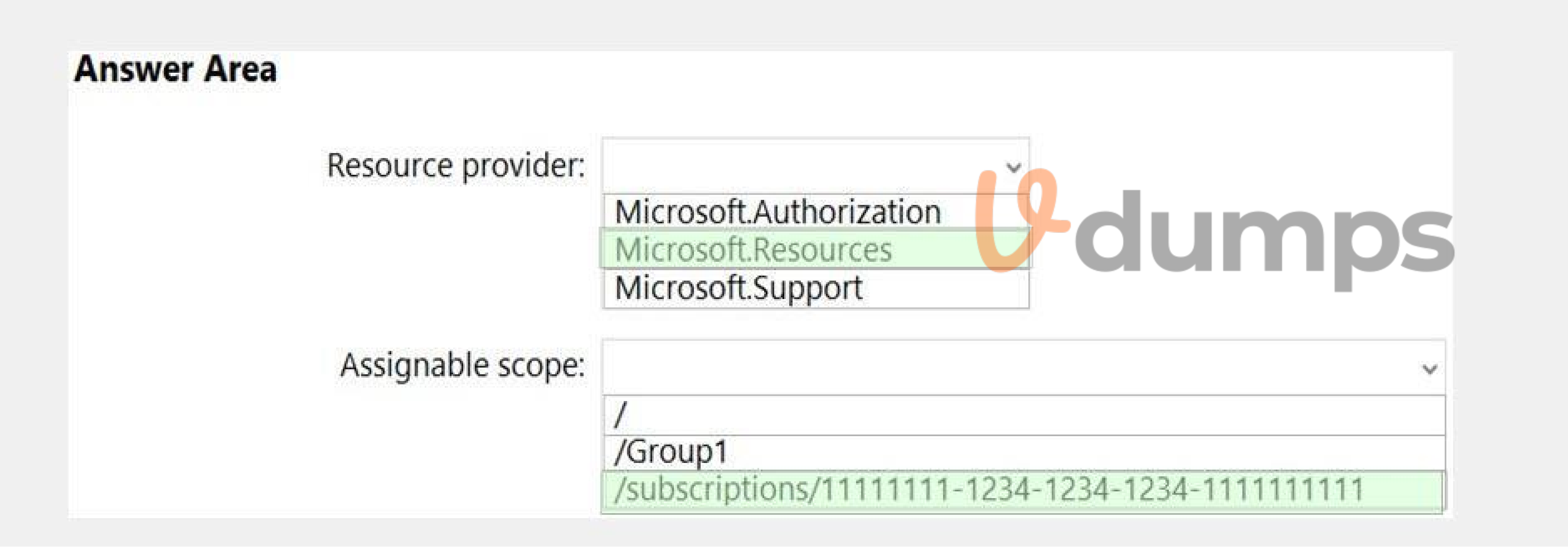
Resource provider:

- Microsoft.Authorization
- Microsoft.Resources
- Microsoft.Support

Assignable scope:

- /
- /Group1
- /subscriptions/11111111-1234-1234-1234-1111111111

**Answer Area:**



**Answer Area**

Resource provider:

- Microsoft.Authorization
- [✓ Microsoft.Resources]
- Microsoft.Support

Assignable scope:

- /
- /Group1
- [✓ /subscriptions/11111111-1234-1234-1234-1111111111]

**Section:**

**Explanation:**

Note: Assigning a custom RBAC role as the Management Group level is currently in preview only. So, for now the answer to the assignable scope is the subscription level.

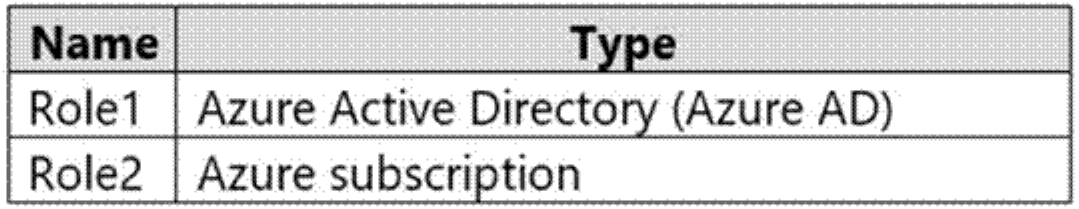
Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#step-5-assignable-scopes

**QUESTION 58**

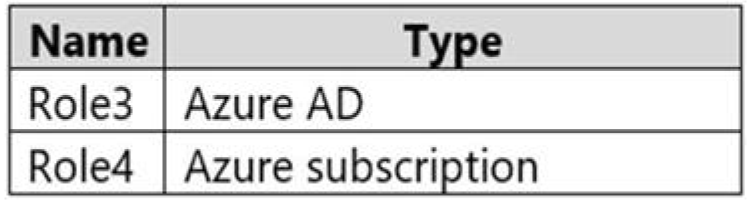
HOTSPOT

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



| Name | Type |
|---|---|
| Role1 | Azure Active Directory (Azure AD) |
| Role2 | Azure subscription |

In the Azure portal, you plan to create new custom roles by cloning existing roles. The new roles will be configured as shown in the following table.

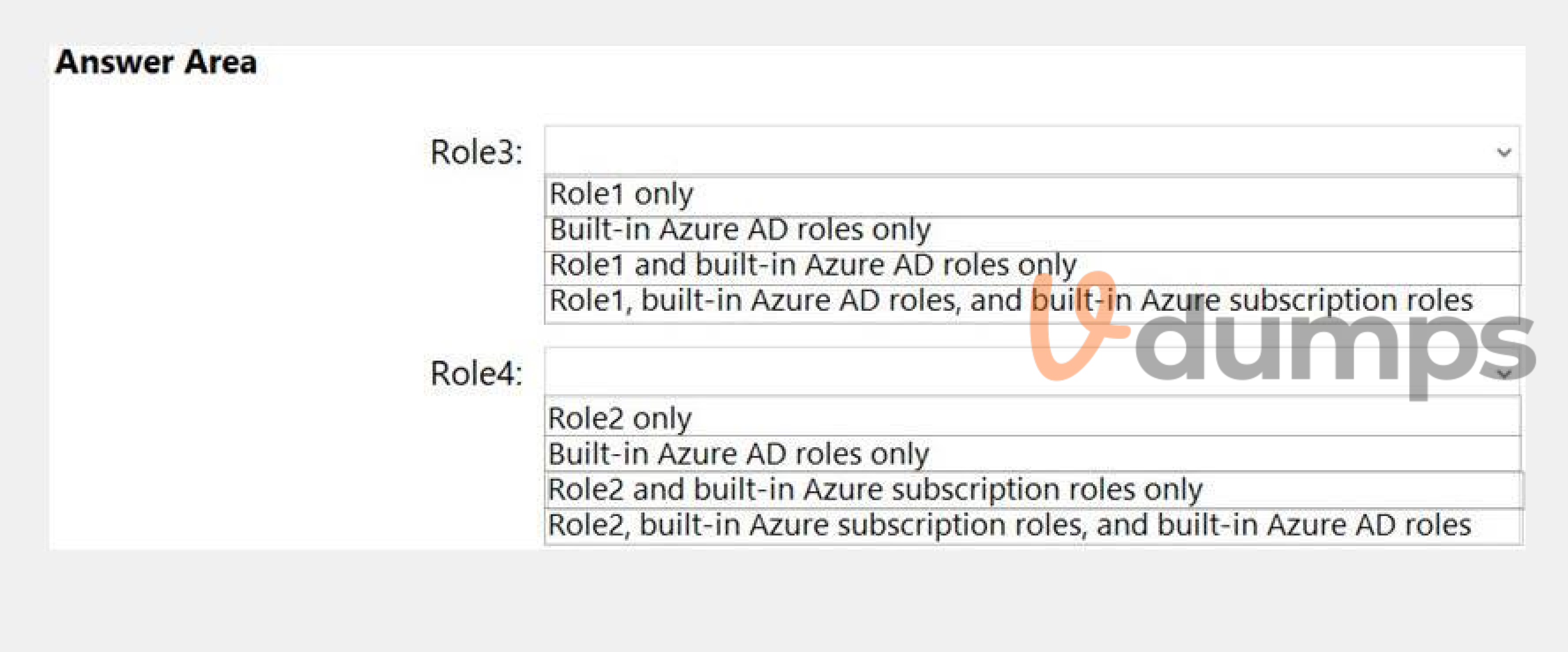


| Name | Type |
|---|---|
| Role3 | Azure AD |
| Role4 | Azure subscription |

Which roles can you clone to create each new role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Hot Area:**

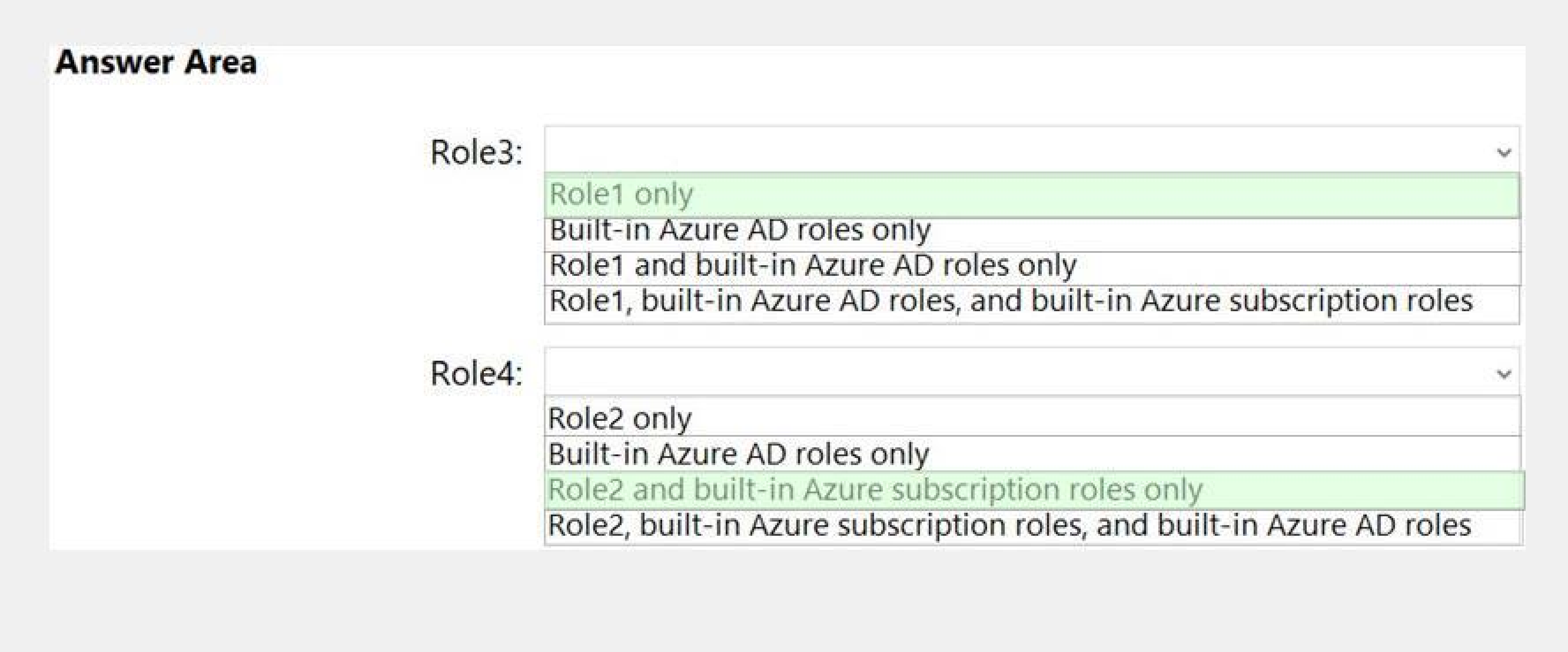


Answer Area

Role3:
- Role1 only
- Built-in Azure AD roles only
- Role1 and built-in Azure AD roles only
- Role1, built-in Azure AD roles, and built-in Azure subscription roles

Role4:
- Role2 only
- Built-in Azure AD roles only
- Role2 and built-in Azure subscription roles only
- Role2, built-in Azure subscription roles, and built-in Azure AD roles

**Answer Area:**



**Answer Area**

Role3:

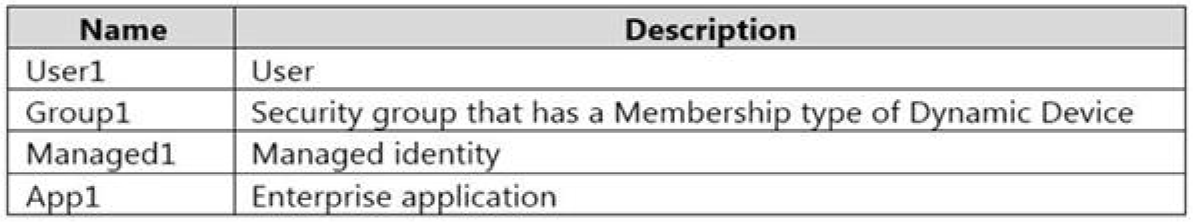
- [✓ Role1 only]
- Built-in Azure AD roles only
- Role1 and built-in Azure AD roles only
- Role1, built-in Azure AD roles, and built-in Azure subscription roles

Role4:

- Role2 only
- Built-in Azure AD roles only
- [✓ Role2 and built-in Azure subscription roles only]
- Role2, built-in Azure subscription roles, and built-in Azure AD roles

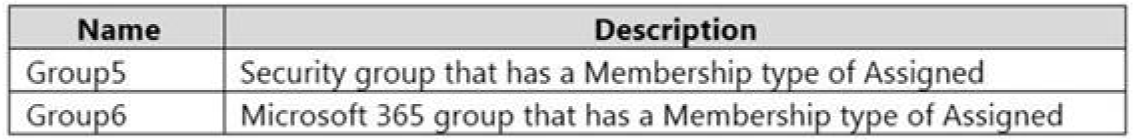
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-create
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal

**QUESTION 59**
HOTSPOT
You have an Azure subscription that contains the Azure Active Directory (Azure AD) resources shown in the following table.



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

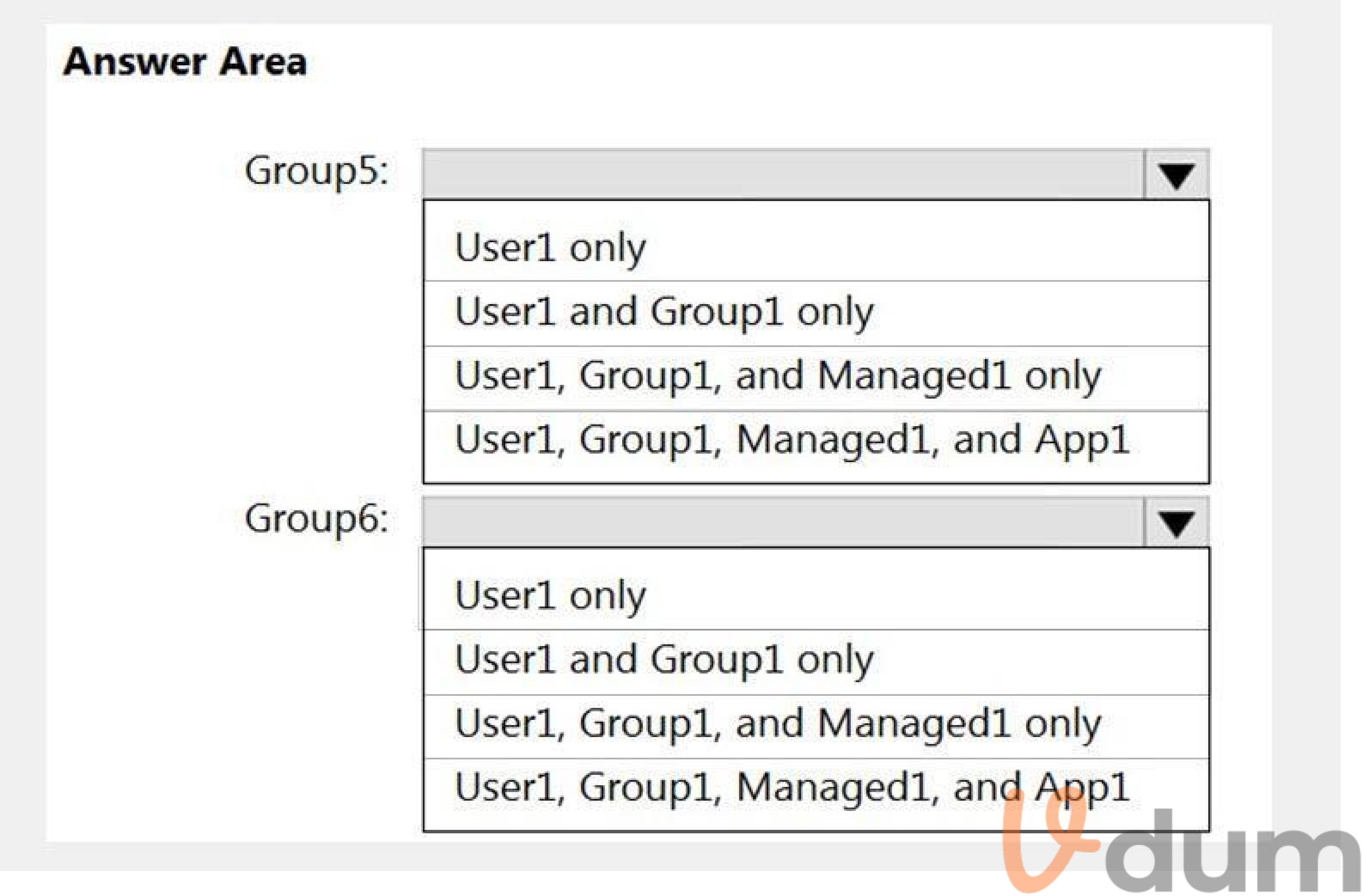
You create the groups shown in the following table.



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

Which resources can you add to Group5 and Group6? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**



Answer Area

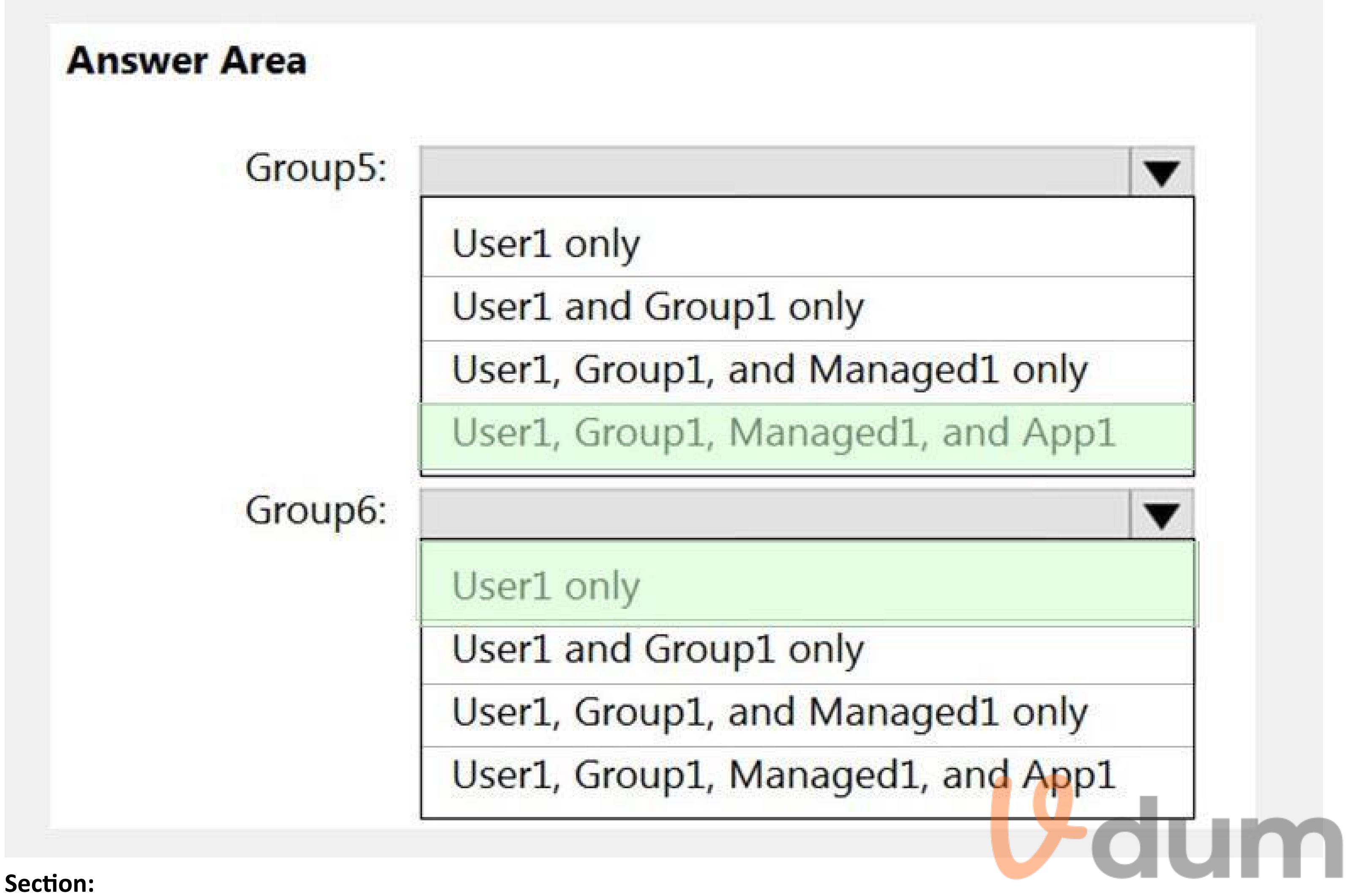
Group5:

- User1 only
- User1 and Group1 only
- User1, Group1, and Managed1 only
- User1, Group1, Managed1, and App1

Group6:

- User1 only
- User1 and Group1 only
- User1, Group1, and Managed1 only
- User1, Group1, Managed1, and App1

**Answer Area:**



**Answer Area**

Group5:

- User1 only
- User1 and Group1 only
- User1, Group1, and Managed1 only
- [✓ User1, Group1, Managed1, and App1]

Group6:

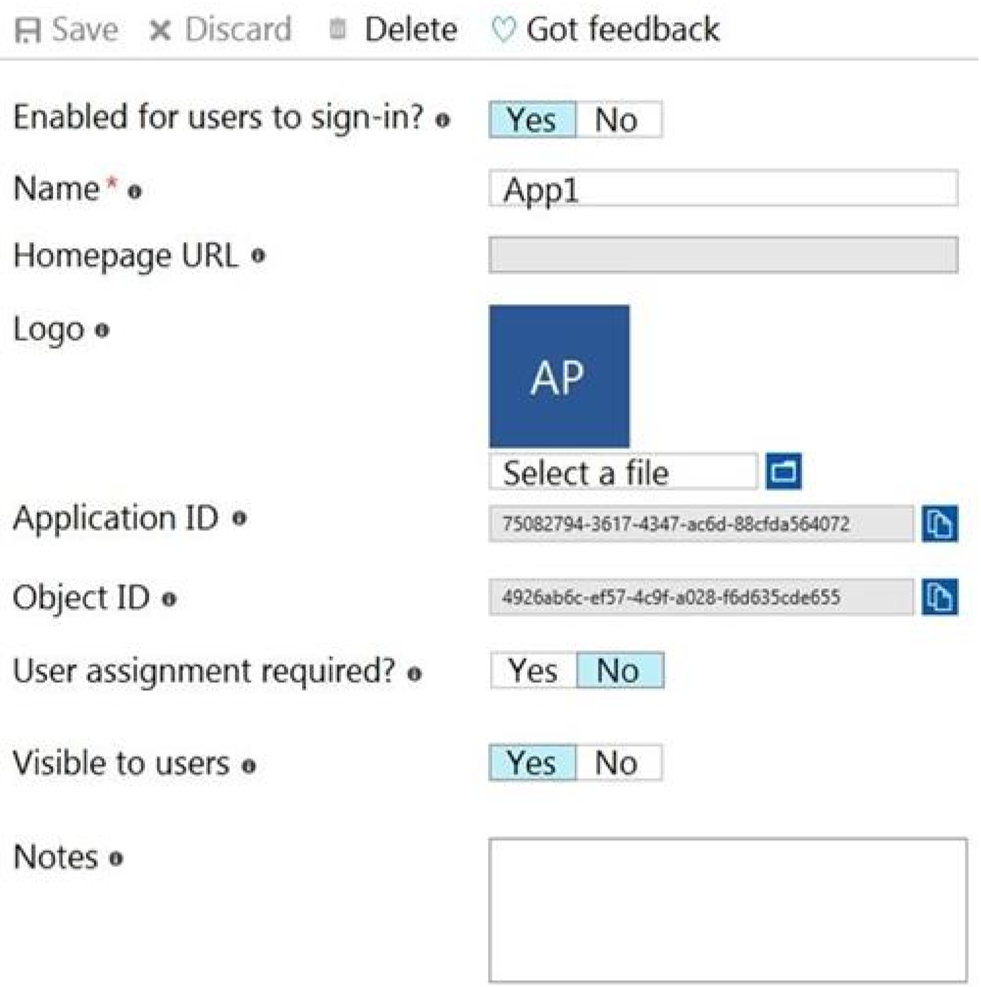
- [✓ User1 only]
- User1 and Group1 only
- User1, Group1, and Managed1 only
- User1, Group1, Managed1, and App1

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

**QUESTION 60**
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains three security groups named Group1, Group2, and Group3 and the users shown in the following table.

| Name | Role | Member of |
|---|---|---|
| User1 | Application administrator | Group1 |
| User2 | Application developer | Group2 |
| User3 | Cloud application administrator | Group3 |

Group3 is a member of Group2.
In contoso.com, you register an enterprise application named App1 that has the following settings:
Owners: User1
Users and groups: Group2
You configure the properties of App1 as shown in the following exhibit.



Enabled for users to sign-in? [✓ Yes] No

Name * App1

Homepage URL

Logo AP

Select a file

Application ID 75082794-3617-4347-ac6d-88cfda564072

Object ID 4926ab6c-ef57-4c9f-a028-f6d635cde655

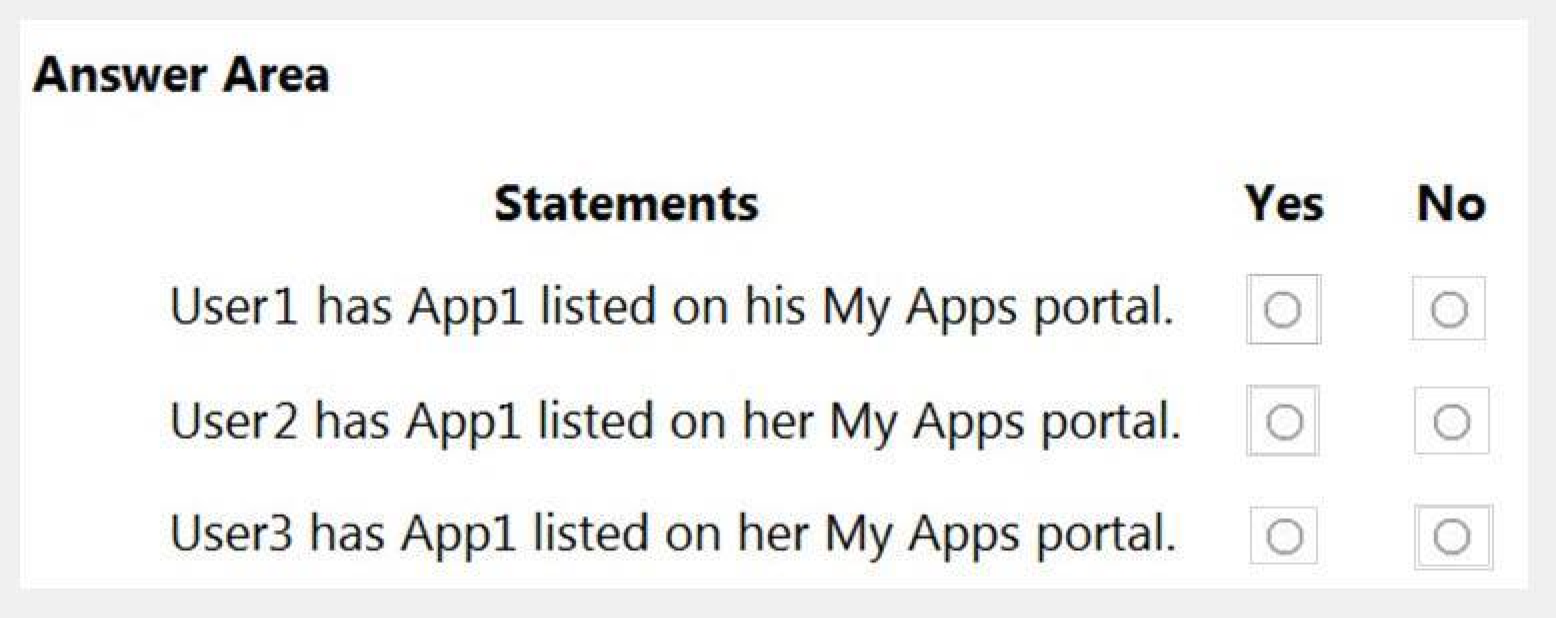
User assignment required? Yes [✓ No]

Visible to users [✓ Yes] No

Notes

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

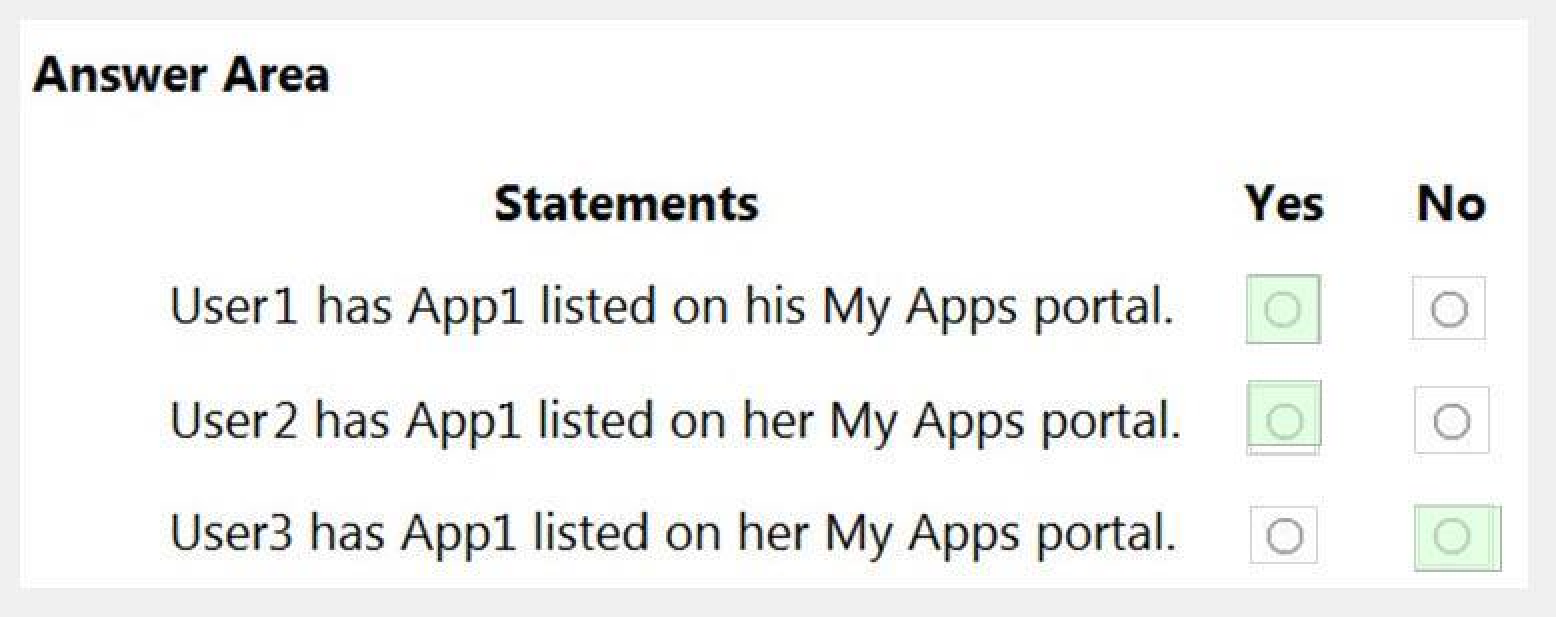
**Hot Area:**



**Answer Area**

| Statements | Yes | No |
|---|---|---|
| User1 has App1 listed on his My Apps portal. | ○ | ○ |
| User2 has App1 listed on her My Apps portal. | ○ | ○ |
| User3 has App1 listed on her My Apps portal. | ○ | ○ |

**Answer Area:**

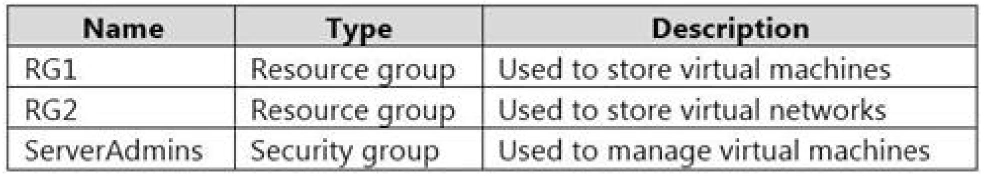


Answer Area

| Statements | Yes | No |
|---|---|---|
| User1 has App1 listed on his My Apps portal. | [✓ ○] | ○ |
| User2 has App1 listed on her My Apps portal. | [✓ ○] | ○ |
| User3 has App1 listed on her My Apps portal. | ○ | [✓ ○] |

**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal

**QUESTION 61**
You have an Azure subscription that contains the resources shown in the following table.



| Name | Type | Description |
|---|---|---|
| RG1 | Resource group | Used to store virtual machines |
| RG2 | Resource group | Used to store virtual networks |
| ServerAdmins | Security group | Used to manage virtual machines |

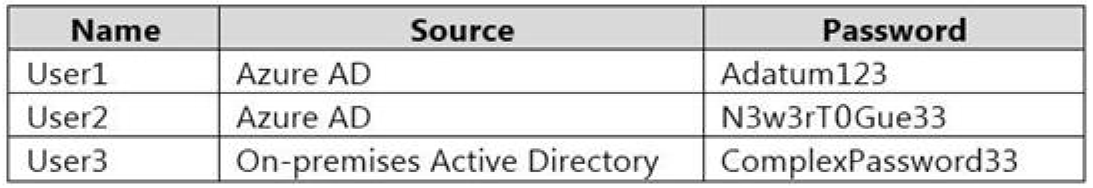
You need to ensure that ServerAdmins can perform the following tasks:
Create virtual machines in RG1 only.
Connect the virtual machines to the existing virtual networks in RG2 only.
The solution must use the principle of least privilege.
Which two role-based access control (RBAC) roles should you assign to ServerAdmins? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a custom RBAC role for RG2
B. the Network Contributor role for RG2
C. the Contributor role for the subscription
D. a custom RBAC role for the subscription
E. the Network Contributor role for RG1
F. the Virtual Machine Contributor role for RG1

**Correct Answer: A, F**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

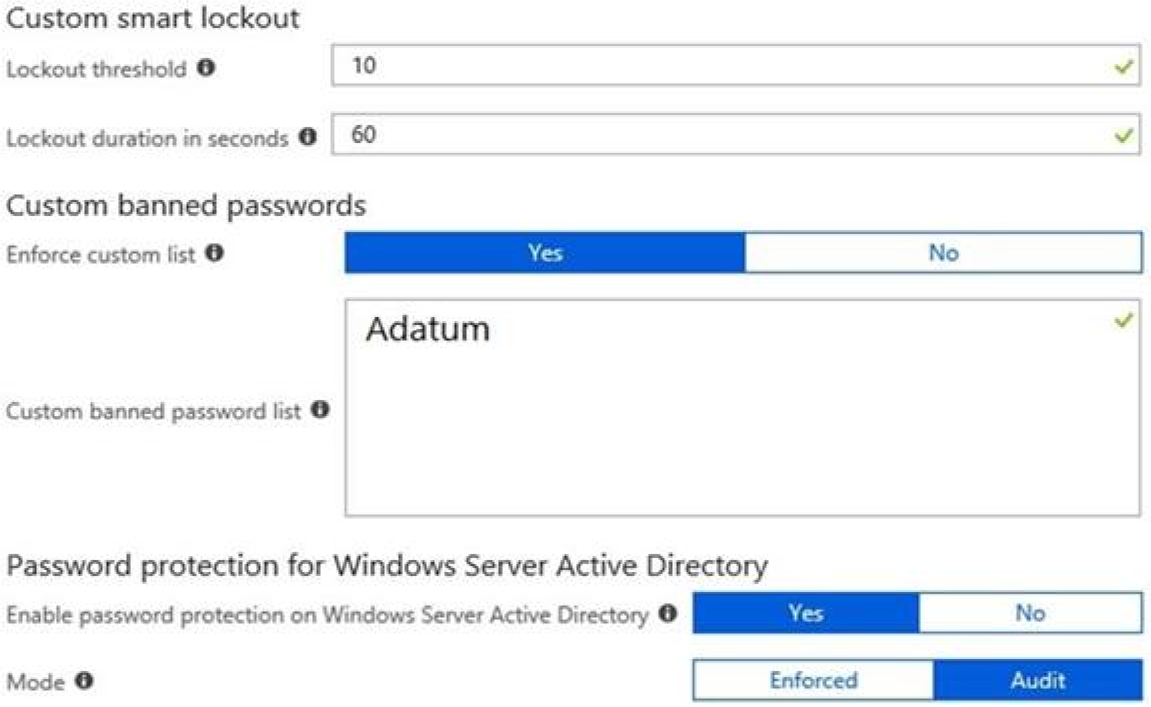
**QUESTION 62**
HOTSPOT

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD).
The Azure AD tenant contains the users shown in the following table.



| Name | Source | Password |
|---|---|---|
| User1 | Azure AD | Adatum123 |
| User2 | Azure AD | N3w3rT0Gue33 |
| User3 | On-premises Active Directory | ComplexPassword33 |

You configure the Authentication methods – Password Protection settings for adatum.com 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: Adatum

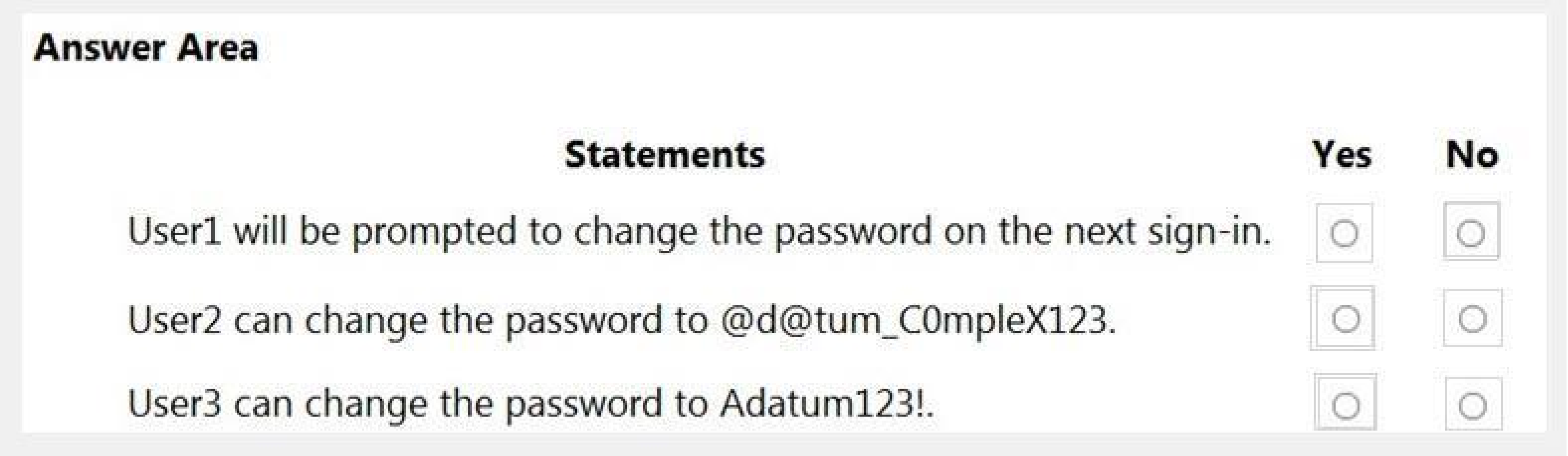
Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory: [✓ Yes] No

Mode: Enforced [✓ Audit]

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

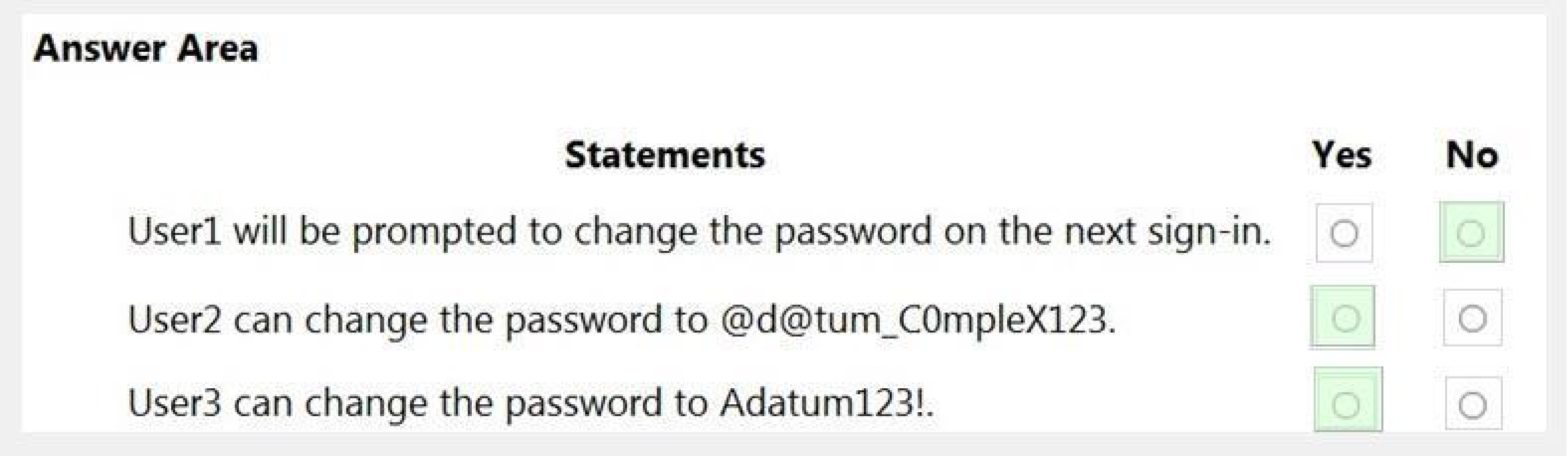
**Hot Area:**



**Answer Area**

| Statements | Yes | No |
|---|---|---|
| User1 will be prompted to change the password on the next sign-in. | ○ | ○ |
| User2 can change the password to @d@tum_C0mpleX123. | ○ | ○ |
| User3 can change the password to Adatum123!. | ○ | ○ |

**Answer Area:**



**Answer Area**

| Statements | Yes | No |
|---|---|---|
| User1 will be prompted to change the password on the next sign-in. | ○ | [✓ ○] |
| User2 can change the password to @d@tum_C0mpleX123. | [✓ ○] | ○ |
| User3 can change the password to Adatum123!. | [✓ ○] | ○ |

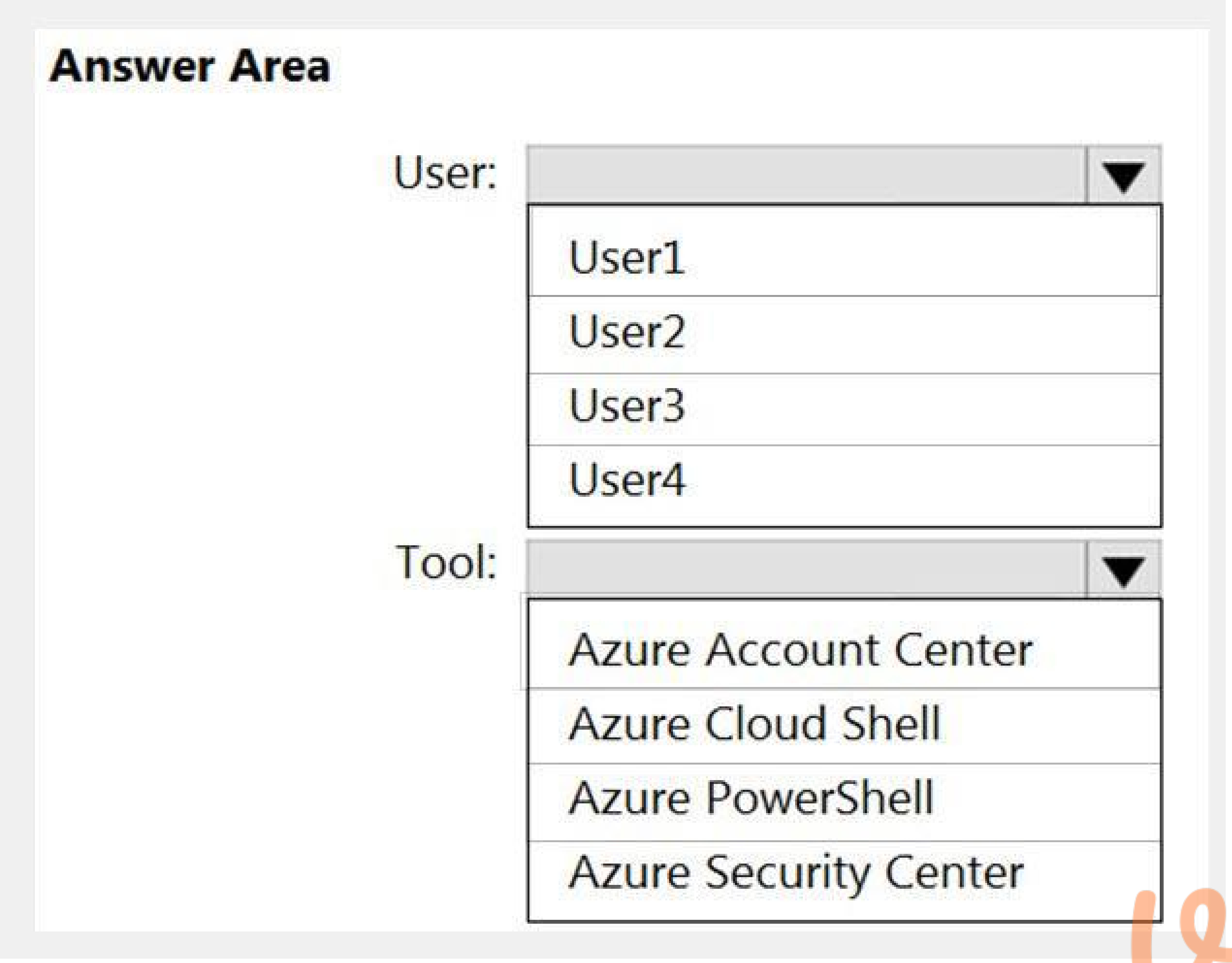
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad

**QUESTION 63**
HOTSPOT
Your company has an Azure subscription named Subscription1. Subscription1 is associated with the Azure Active Directory tenant that includes the users shown in the following table.

| Name | Role |
|---|---|
| User1 | Global administrator |
| User2 | Billing administrator |
| User3 | Owner |
| User4 | Account Admin |

The company is sold to a new owner.
The company needs to transfer ownership of Subscription1.
Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**



**Answer Area**

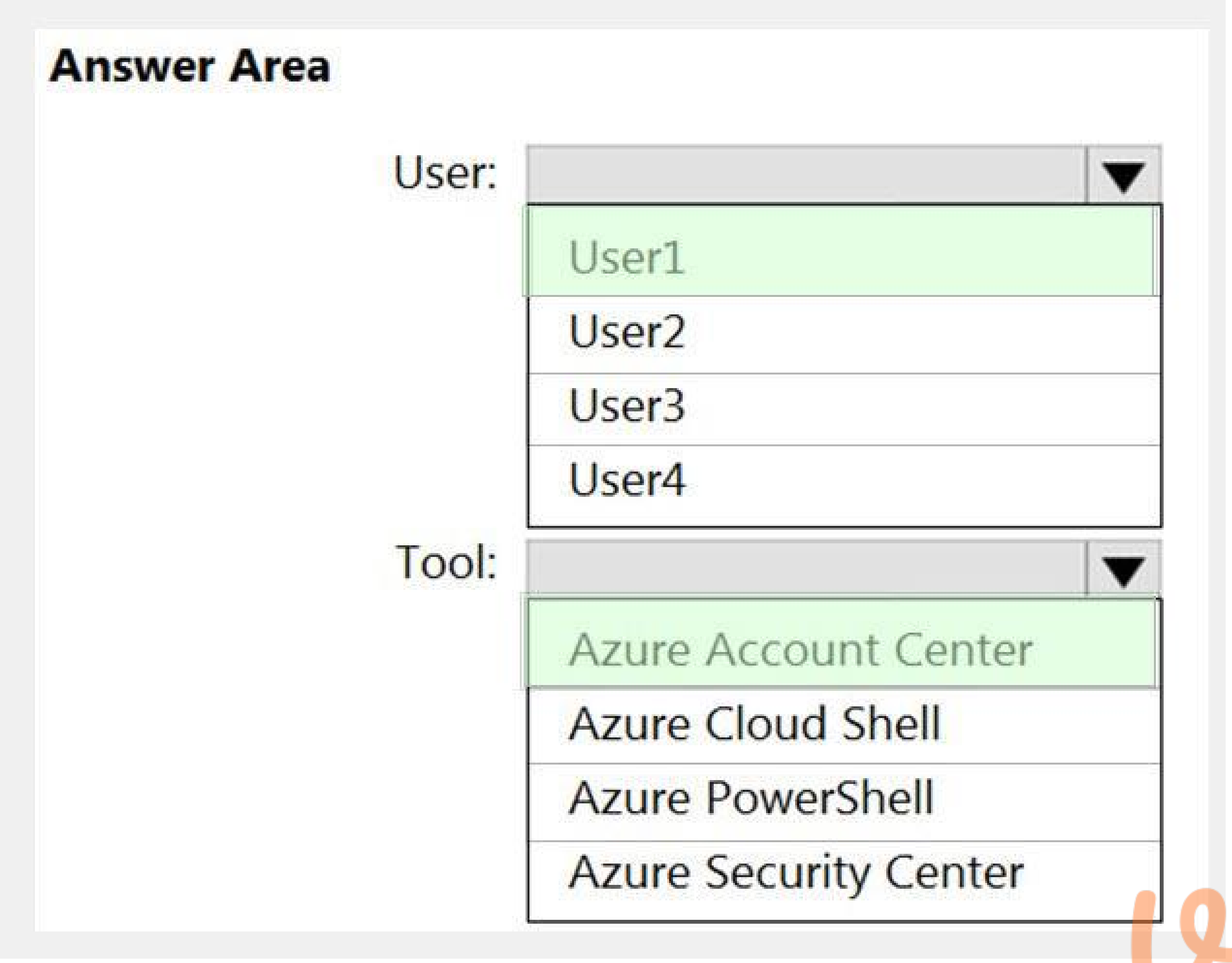
User:

- User1
- User2
- User3
- User4

Tool:

- Azure Account Center
- Azure Cloud Shell
- Azure PowerShell
- Azure Security Center

**Answer Area:**



**Answer Area**

User:

- [✓ User1]
- User2
- User3
- User4

Tool:

- [✓ Azure Account Center]
- Azure Cloud Shell
- Azure PowerShell
- Azure Security Center

**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer

**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.

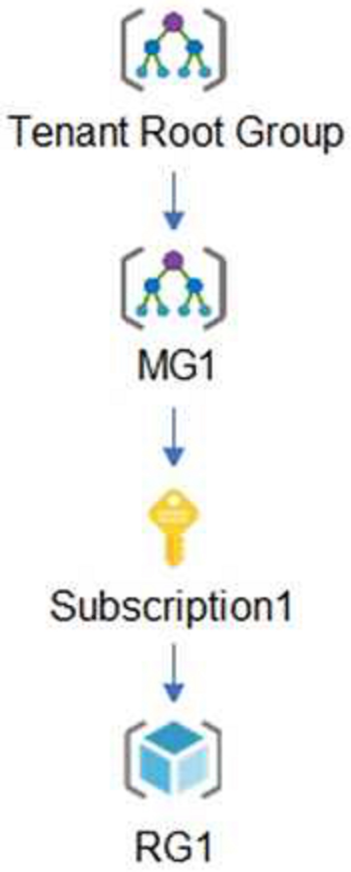
Existing Environment

Network Environment

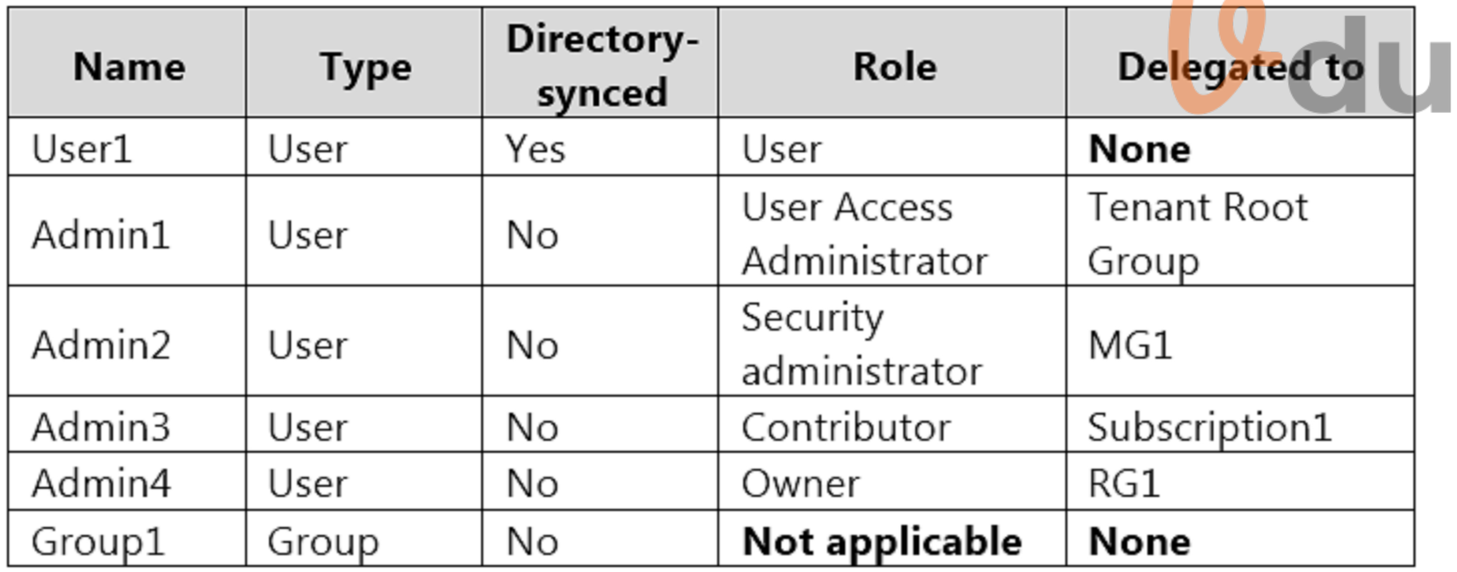
Fabrikam has a Microsoft 365 subscription and an Azure subscription named subscription1.

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.

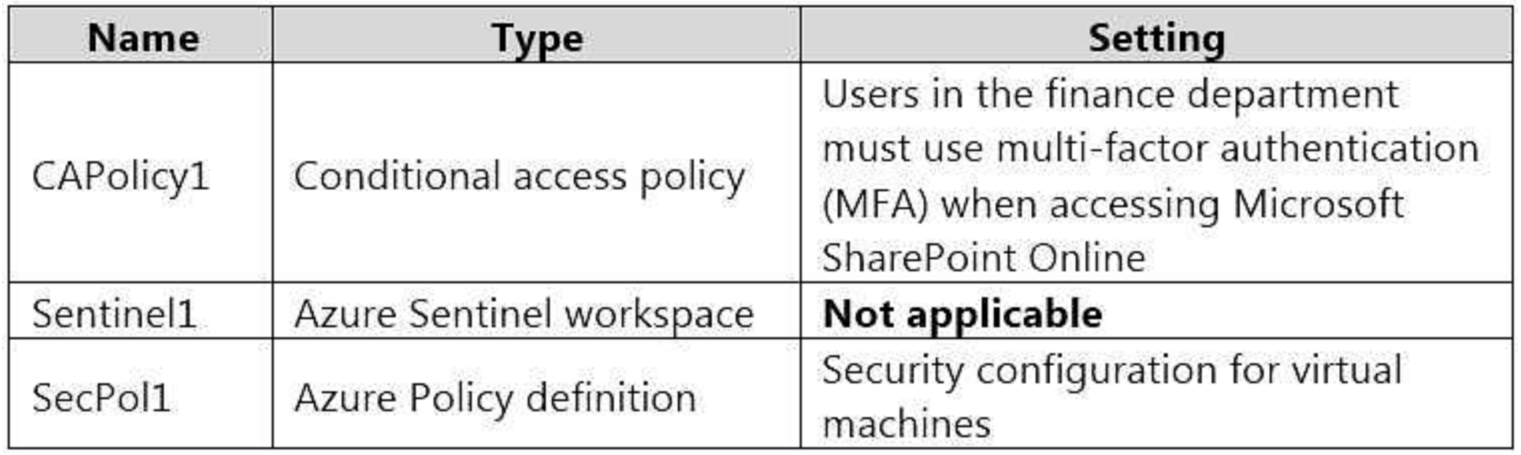


The Azure Active Directory (Azure AD) tenant contains the users shown in the following table.



| 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** |

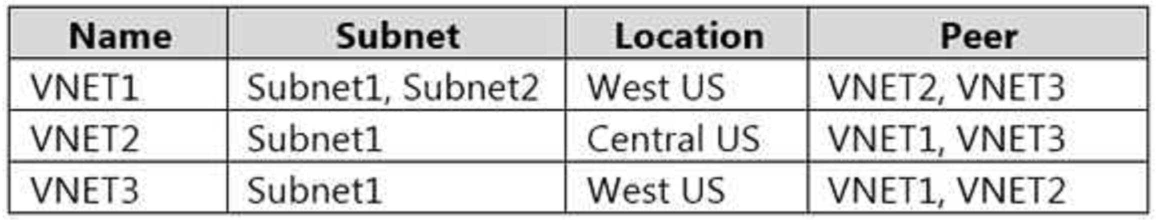
Azure AD contains the resources shown in the following table.



| 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 |

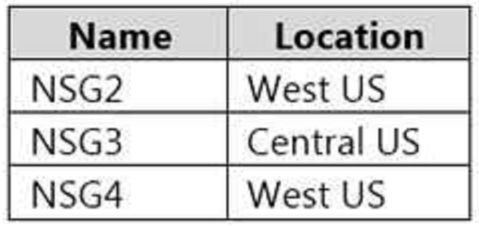
Subscription1 Resources

Subscription1 contains the virtual networks shown in the following table.



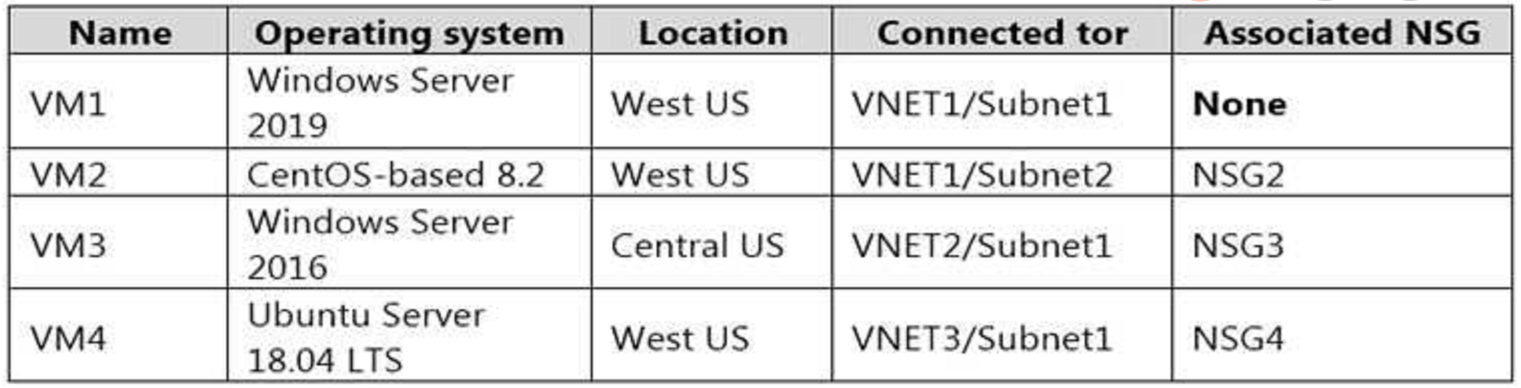
| Name | Subnet | Location | Peer |
|---|---|---|---|
| VNET1 | Subnet1, Subnet2 | West US | VNET2, VNET3 |
| VNET2 | Subnet1 | Central US | VNET1, VNET3 |
| VNET3 | Subnet1 | West US | VNET1, VNET2 |

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



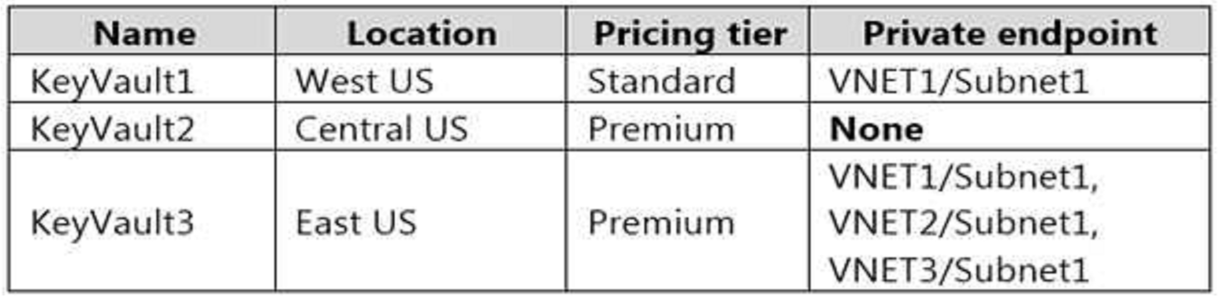
| Name | Location |
|---|---|
| NSG2 | West US |
| NSG3 | Central US |
| NSG4 | West US |

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 |

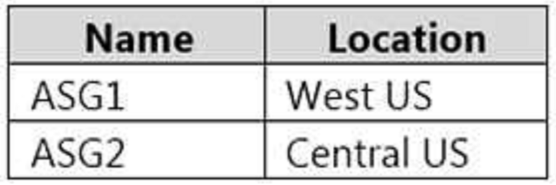
Subscription1 contains a storage account named storage1 in the West US Azure region.

Planned Changes and Requirements

Planned Changes

Fabrikam plans to implement the following changes:

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

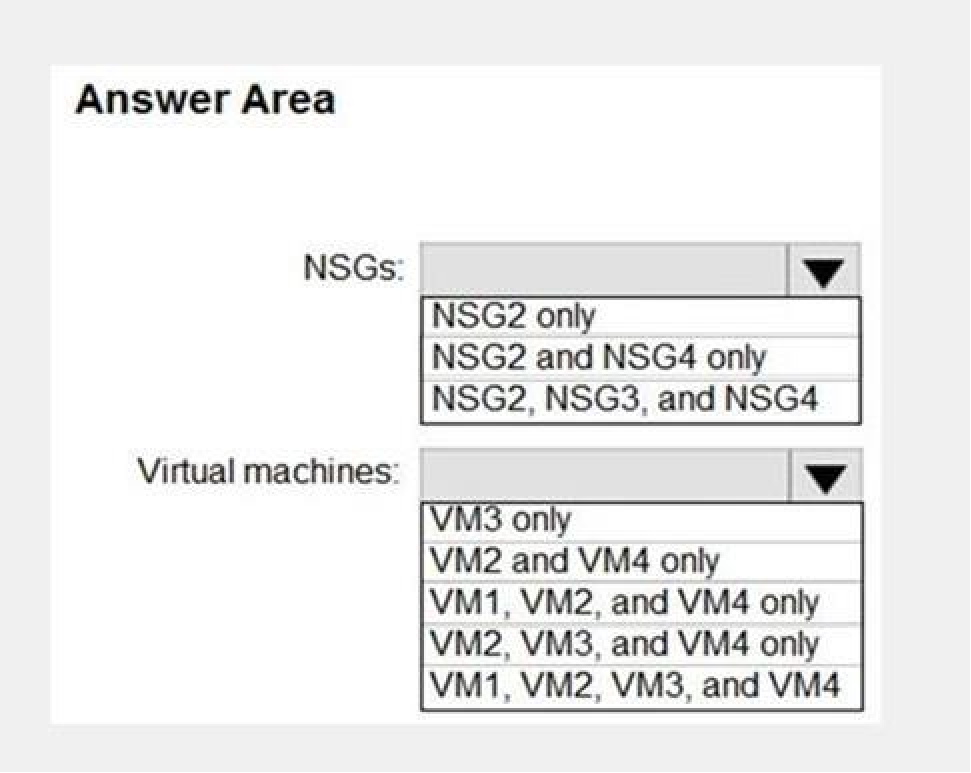


| Name | Location |
|---|---|
| ASG1 | West US |
| ASG2 | Central US |

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:**

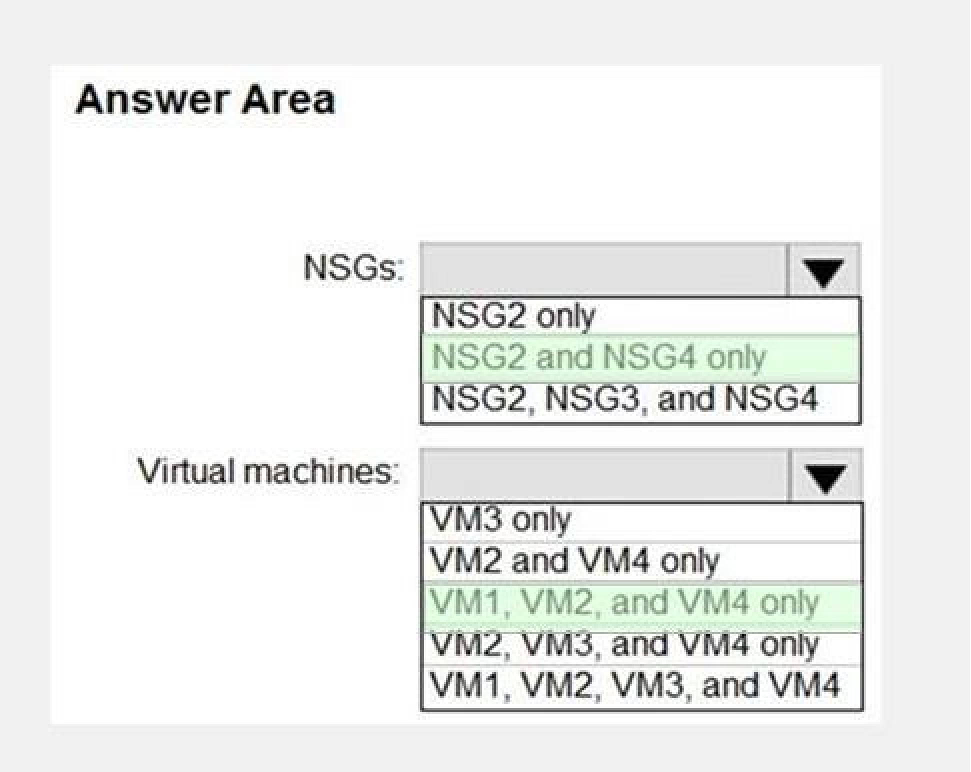


Answer Area

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

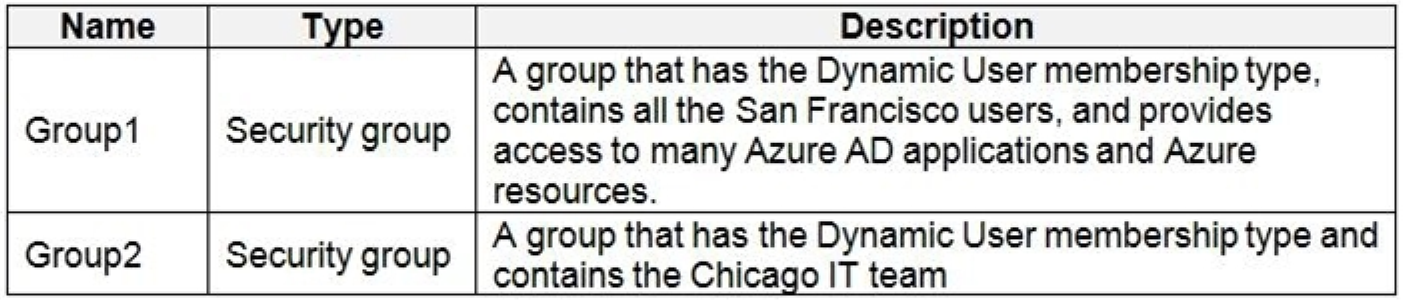
**Correct Answer: A**
**Section:**
**Explanation:**
The key vault needs to be in the same subscription and same region as the VM.
VM4 is in West US. KeyVault1 is the only key vault in the same region as the VM.
Reference: https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault

**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

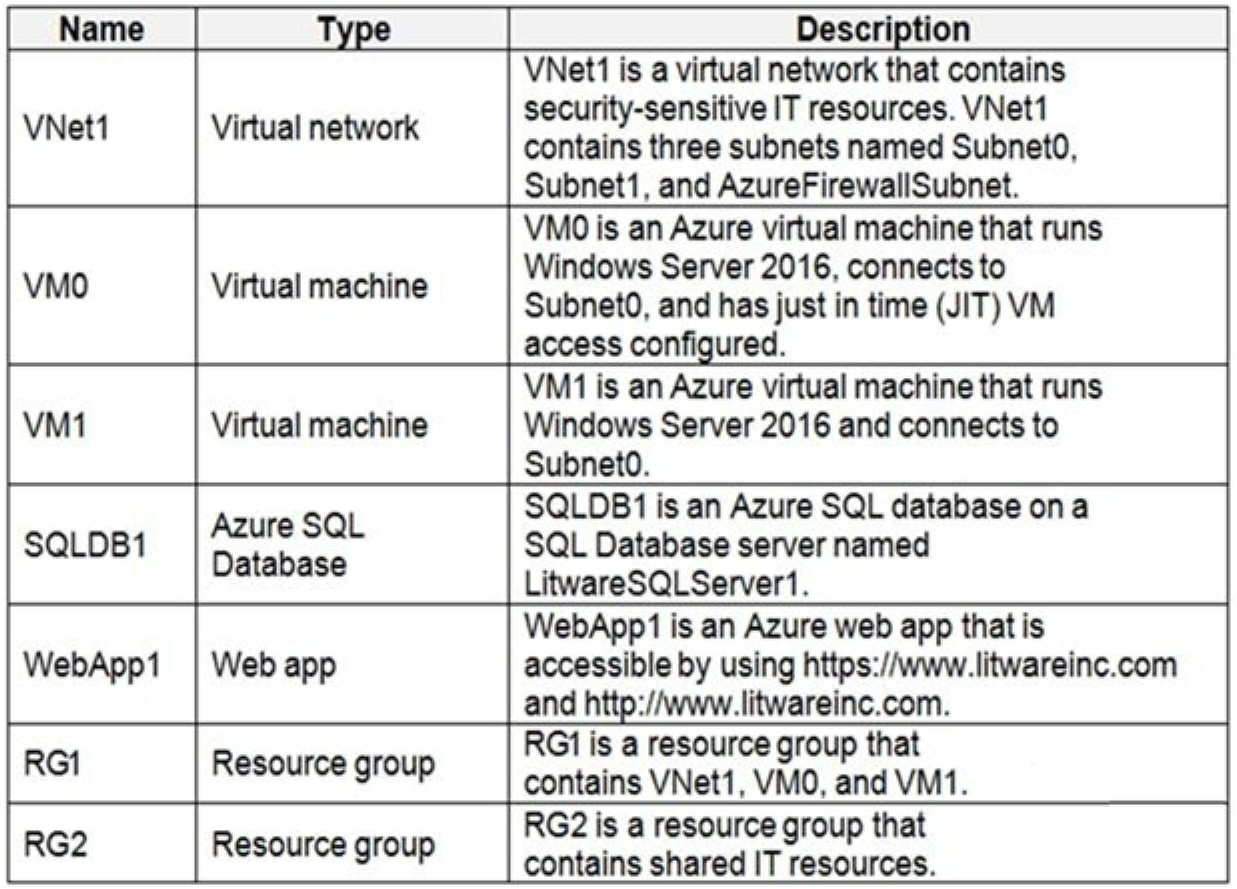
**Correct Answer: A**
**Section:**
**Explanation:**

**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. |

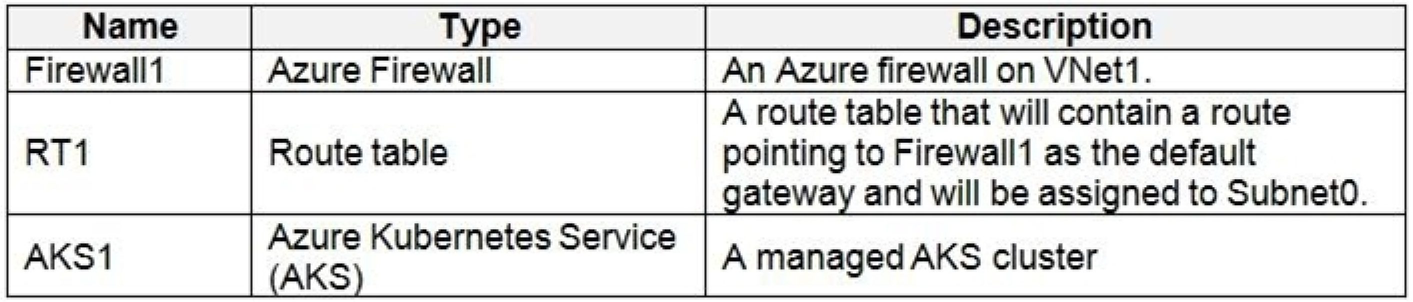
Identity and Access Requirements

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.

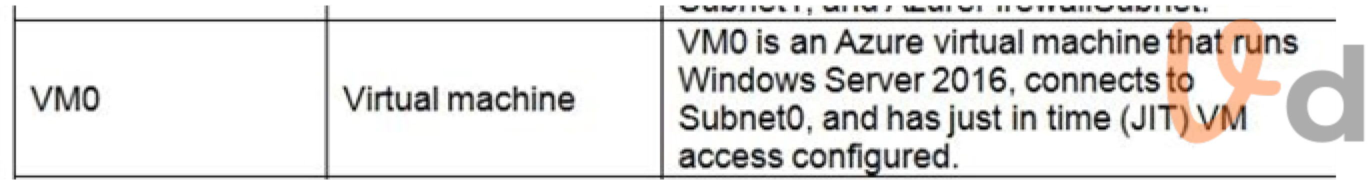
WebApp1 must enforce mutual authentication.

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?

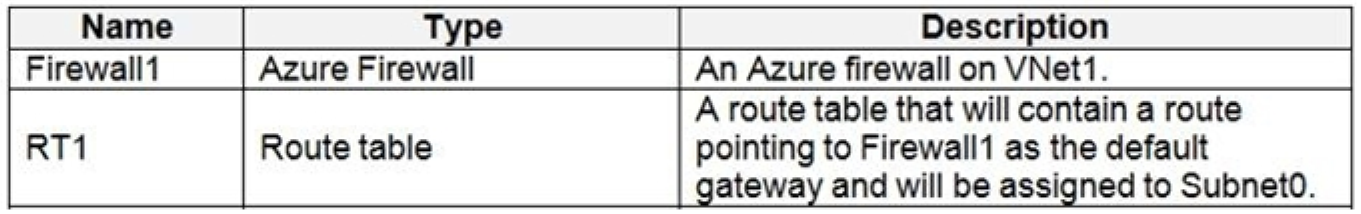
A. Move VM0 to Subnet1.
B. On Firewall, configure a network traffic filtering rule.
C. Assign RT1 to AzureFirewallSubnet.
D. On Firewall, configure a DNAT rule.

**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.

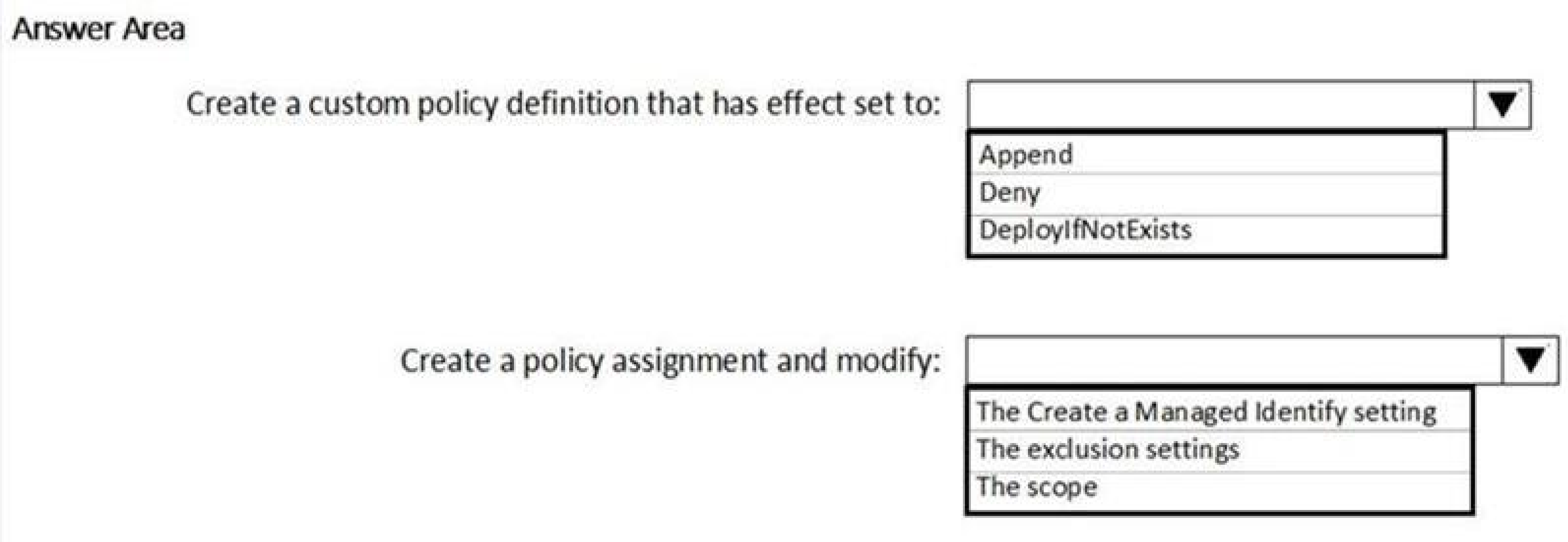


| Name | Type | Description |
|---|---|---|
| Firewall1 | Azure Firewall | An Azure firewall on VNet1. |
| RT1 | Route table | A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0. |

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

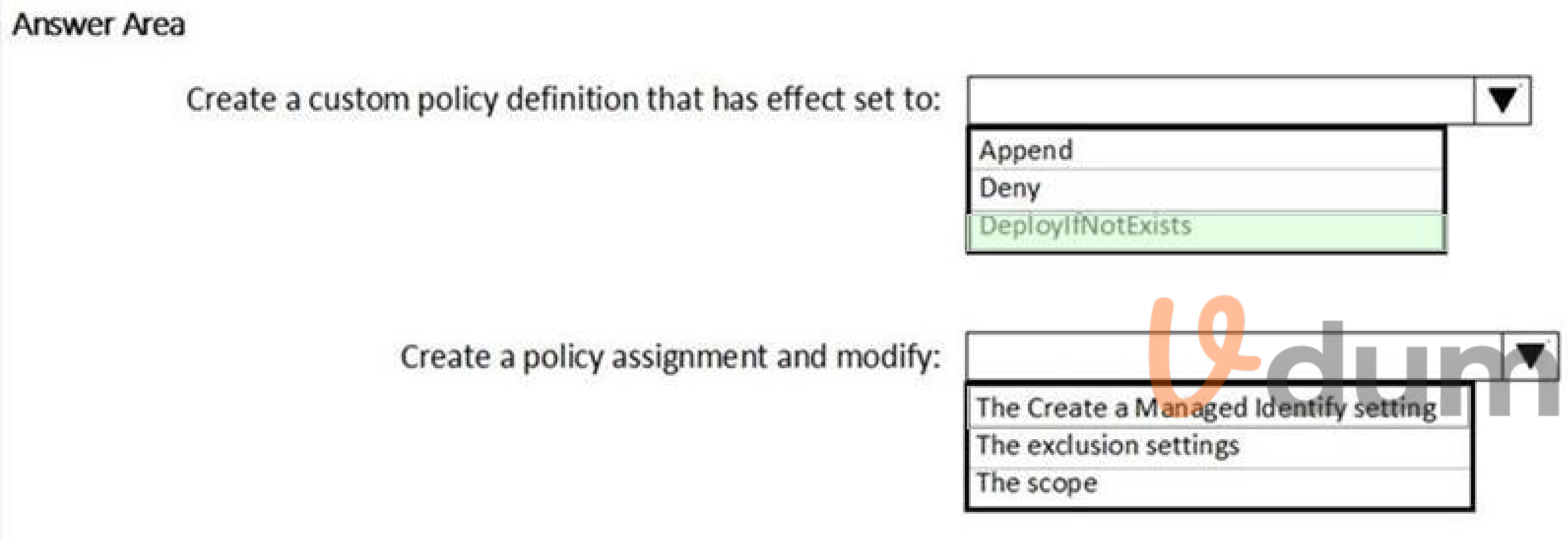
Create a custom policy definition that has effect set to:

- 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:

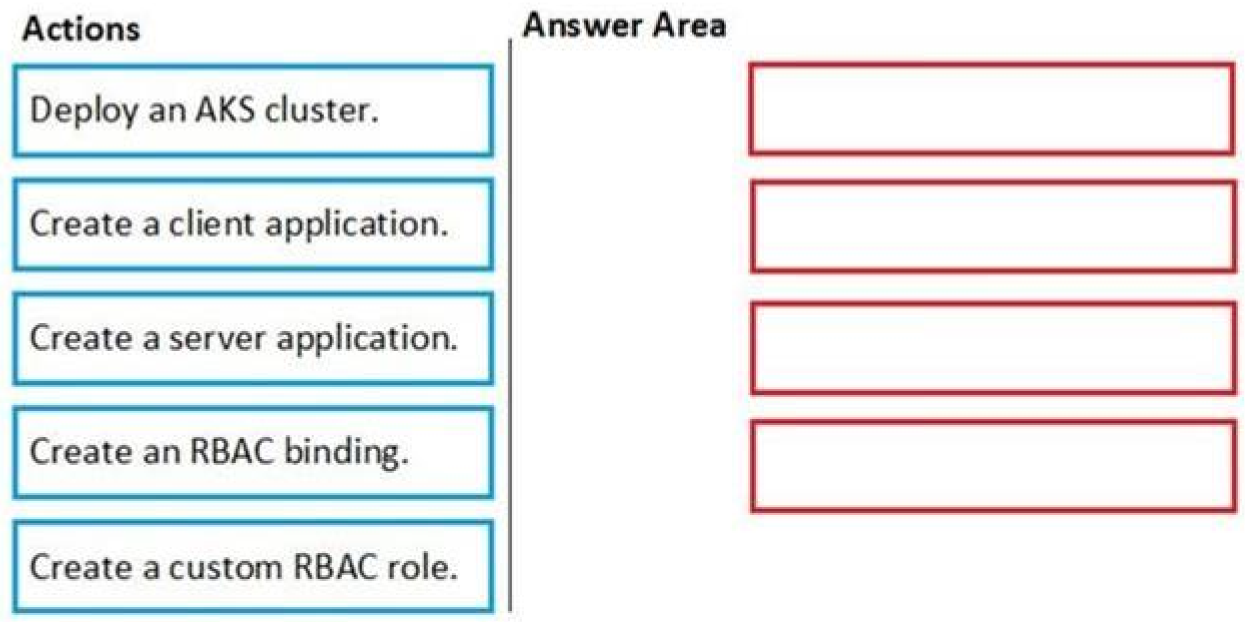
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

**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:**

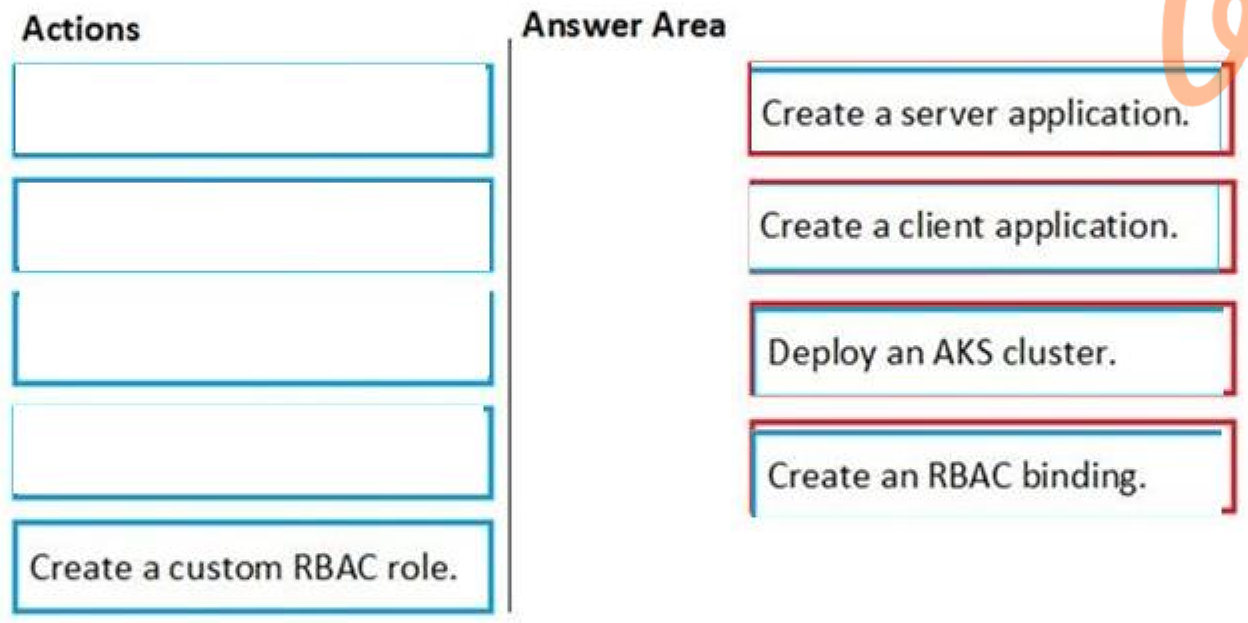


Actions

- 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.

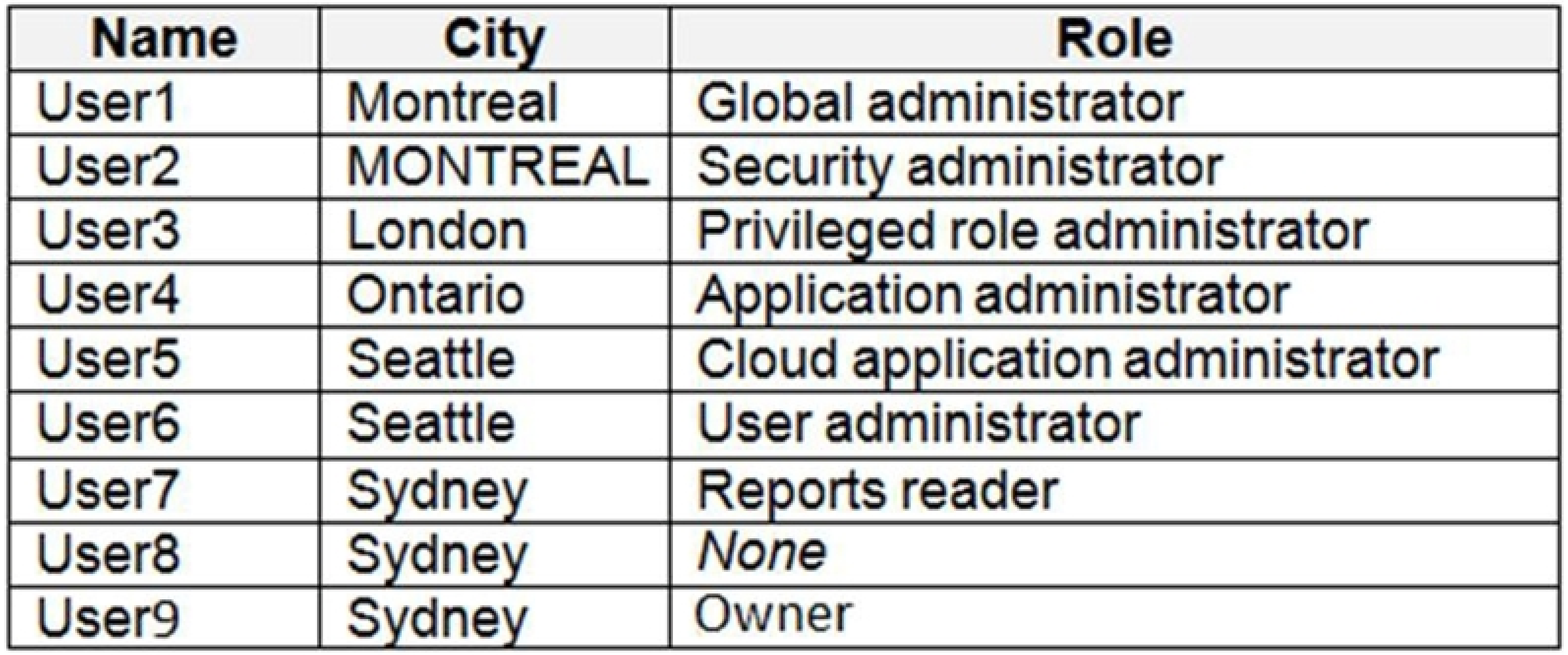
The company hosts its entire server infrastructure in Azure.

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

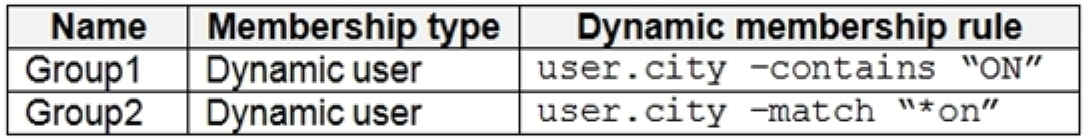
Azure AD

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.

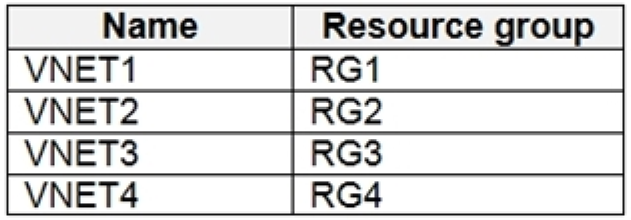


| Name | Membership type | Dynamic membership rule |
|---|---|---|
| Group1 | Dynamic user | `user.city -contains “ON”` |
| Group2 | Dynamic user | `user.city -match “*on”` |

Sub1

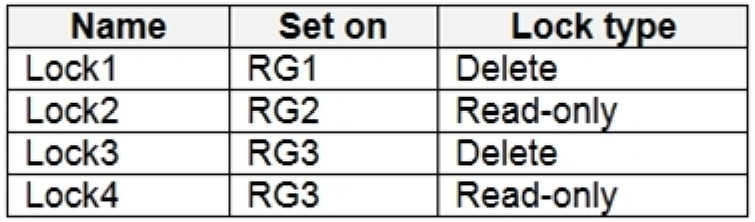
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.



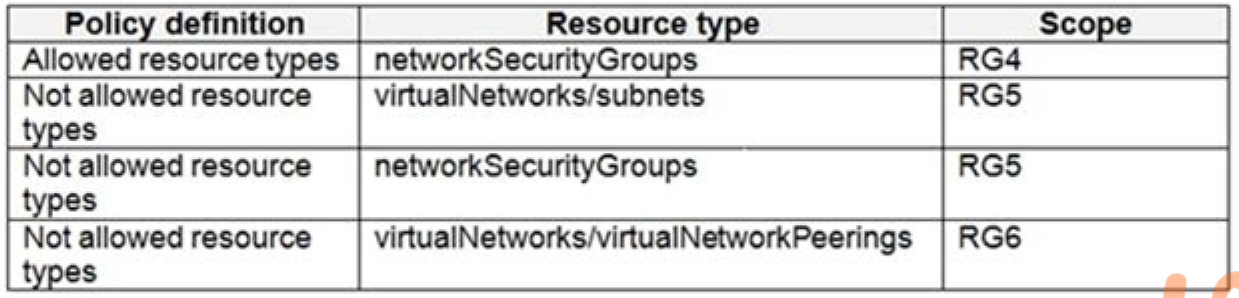
| Name | Resource group |
|---|---|
| VNET1 | RG1 |
| VNET2 | RG2 |
| VNET3 | RG3 |
| VNET4 | RG4 |

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 |

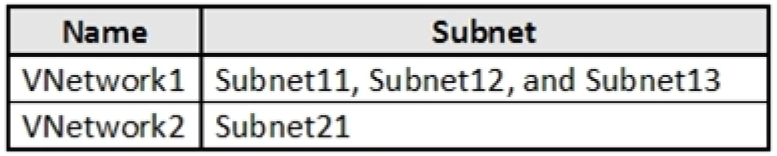
Sub1 contains the Azure policies shown in the following table.



| 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 |

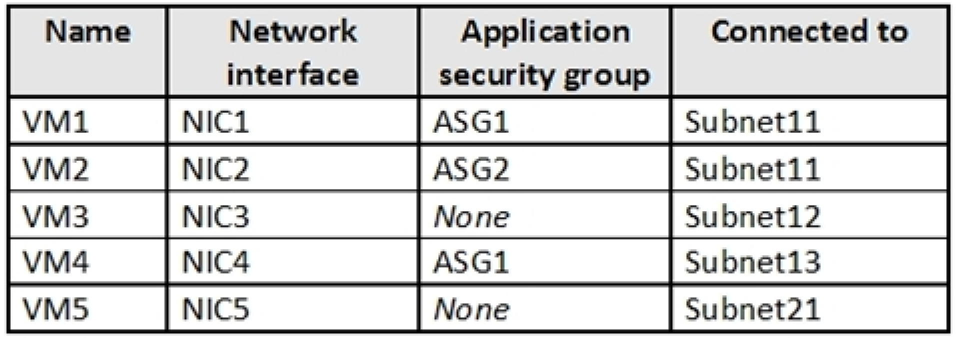
Sub2

Sub2 contains the virtual networks shown in the following table.



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

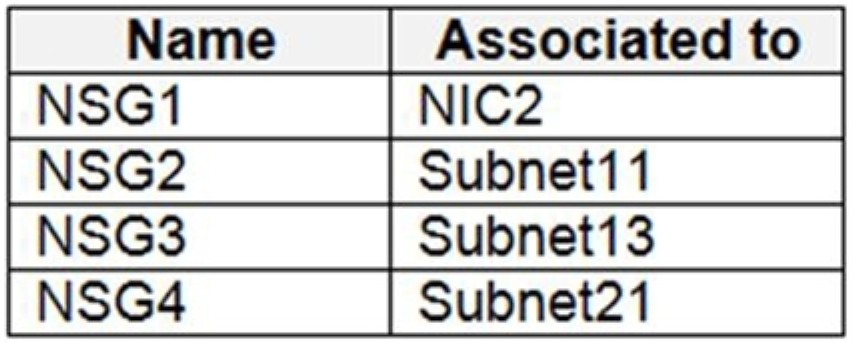
Sub2 contains the virtual machines shown in the following table.



| 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 |

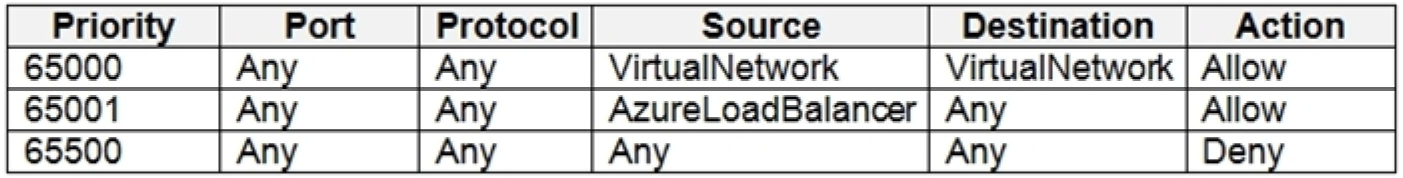
All virtual machines have public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

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



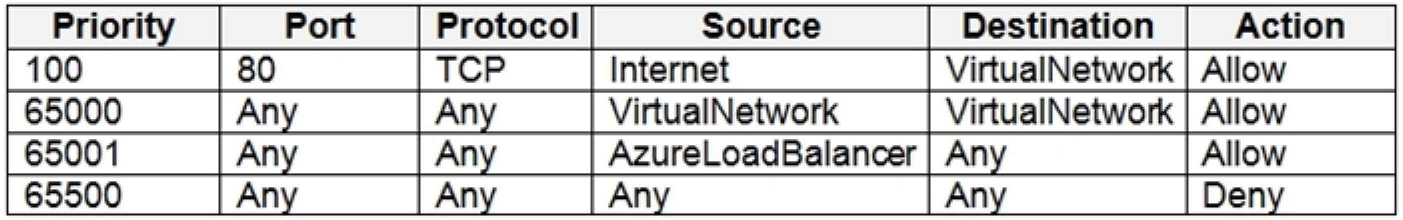
| Name | Associated to |
|---|---|
| NSG1 | NIC2 |
| NSG2 | Subnet11 |
| NSG3 | Subnet13 |
| NSG4 | Subnet21 |

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



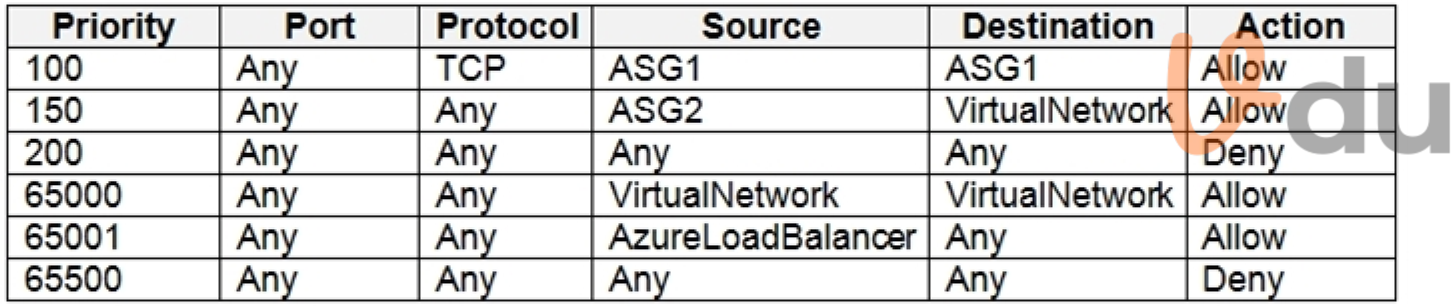
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny |

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



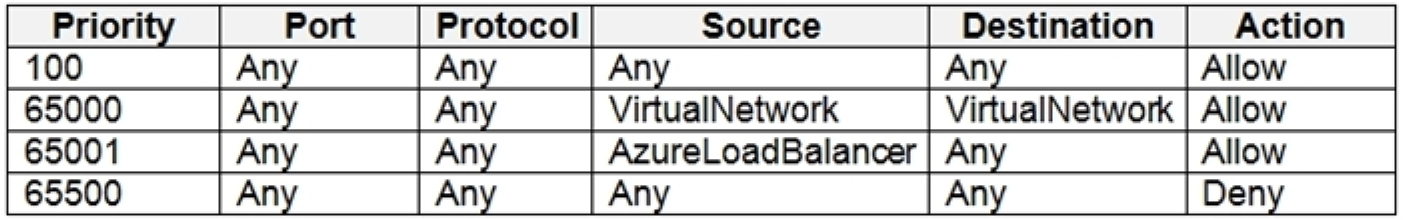
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 100 | 80 | TCP | Internet | VirtualNetwork | Allow |
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | Any | Any | Any | Any | Deny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

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



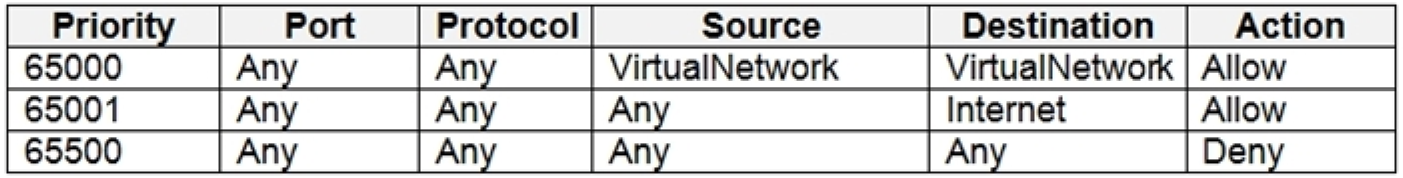
| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 100 | Any | TCP | ASG1 | ASG1 | Allow |
| 150 | Any | Any | ASG2 | VirtualNetwork | Allow |
| 200 | Any | Any | Any | Any | Deny |
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any |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

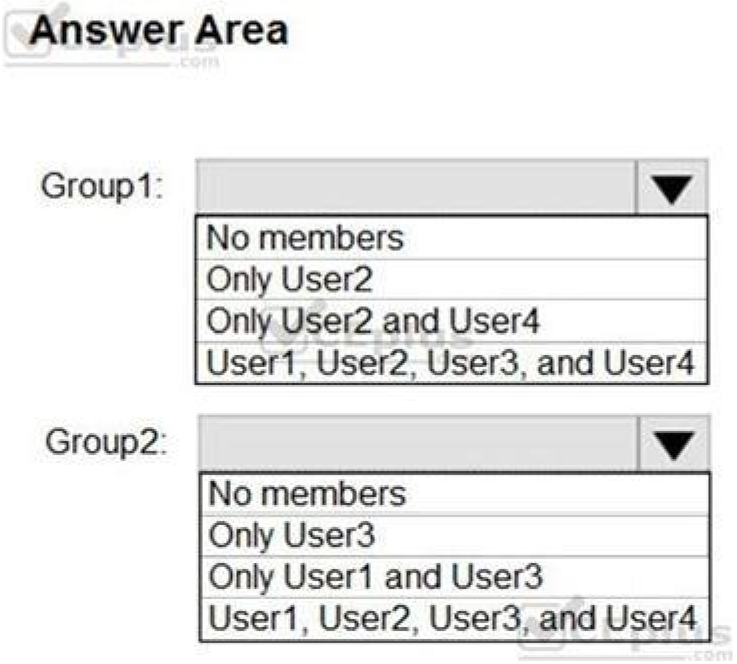
Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

**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

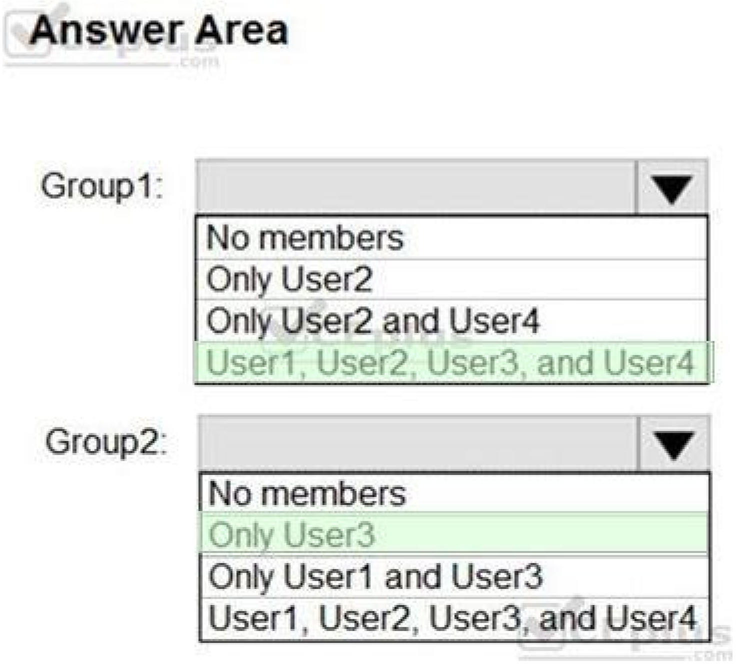
Group1:

- 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

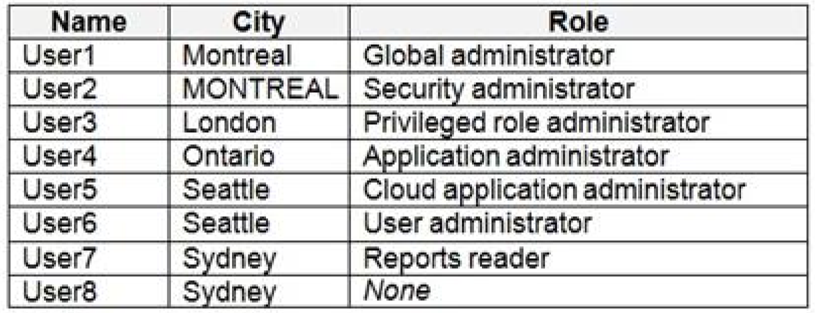
Contains "ON" is true for Montreal (User1), MONTREAL (User2), London (User 3), and Ontario (User4) as string and regex operations are not case sensitive.

Box 2: Only User3

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

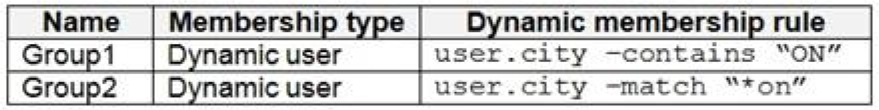
Scenario:

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**

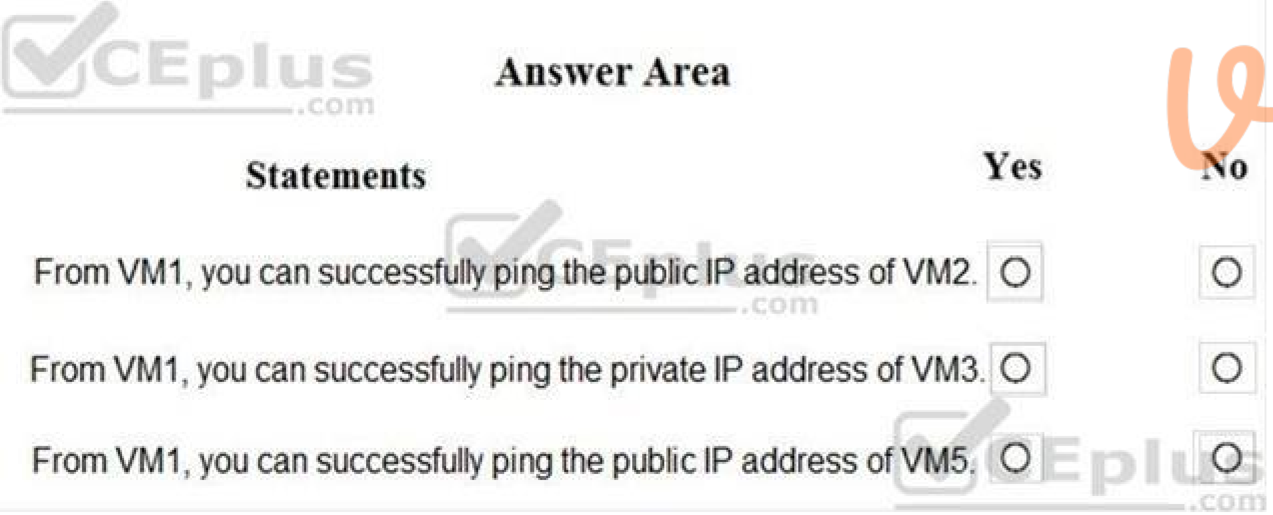
HOTSPOT

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.

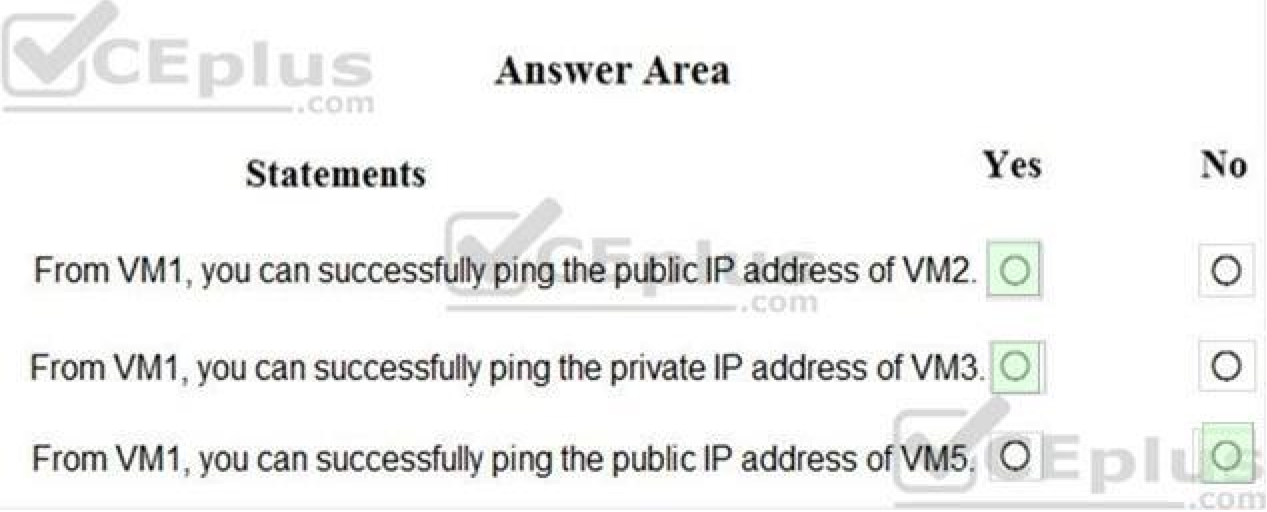
**Hot Area:**



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. | ○ | ○ |

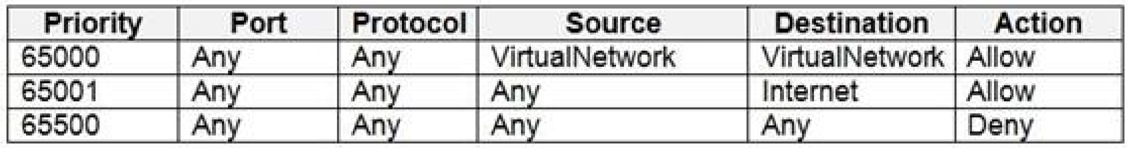
**Answer Area:**



Answer Area

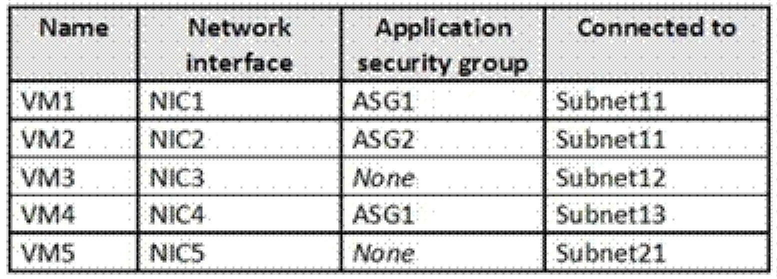
| Statements | Yes | No |
|---|---|---|
| From VM1, you can successfully ping the public IP address of VM2. | [✓ ○] | ○ |
| From VM1, you can successfully ping the private IP address of VM3. | [✓ ○] | ○ |
| From VM1, you can successfully ping the public IP address of VM5. | ○ | [✓ ○] |

**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.

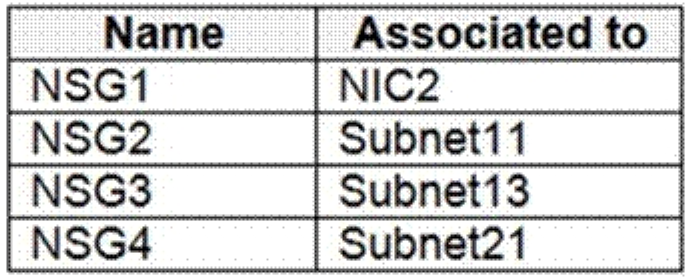


| Priority | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| 65000 | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | Any | Any | Any | Internet | Allow |
| 65500 | Any | Any | Any | Any | Deny |

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

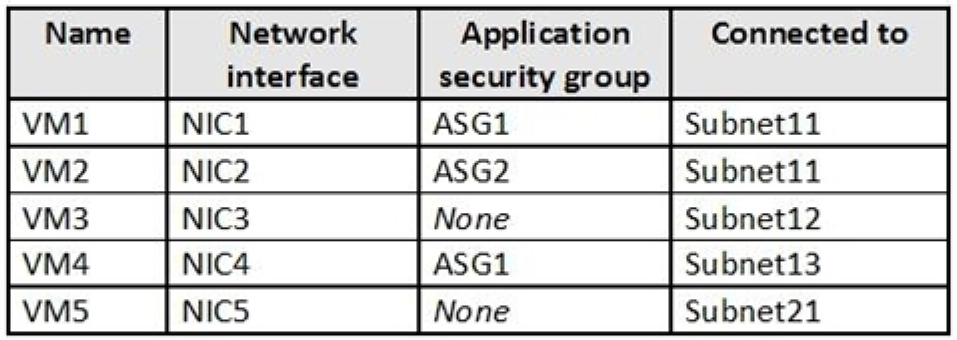


| Name | Network interface | Application security group | Connected to |
|---|---|---|---|
| VM1 | NIC1 | ASG1 | Subnet11 |
| VM2 | NIC2 | ASG2 | Subnet11 |
| VM3 | NIC3 | *None* | Subnet12 |
| VM4 | NIC4 | ASG1 | Subnet13 |
| VM5 | NIC5 | *None* | Subnet21 |

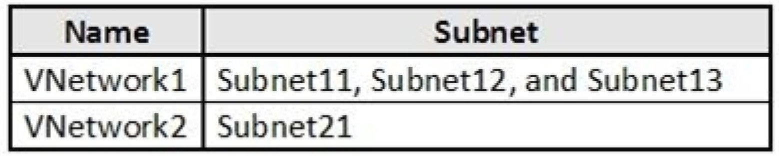


| Name | Associated to |
|---|---|
| NSG1 | NIC2 |
| NSG2 | Subnet11 |
| NSG3 | Subnet13 |
| NSG4 | Subnet21 |

Box 3: No (because VM5 is in a separate VNet).
Note: Sub2 contains the virtual machines shown in the following table.



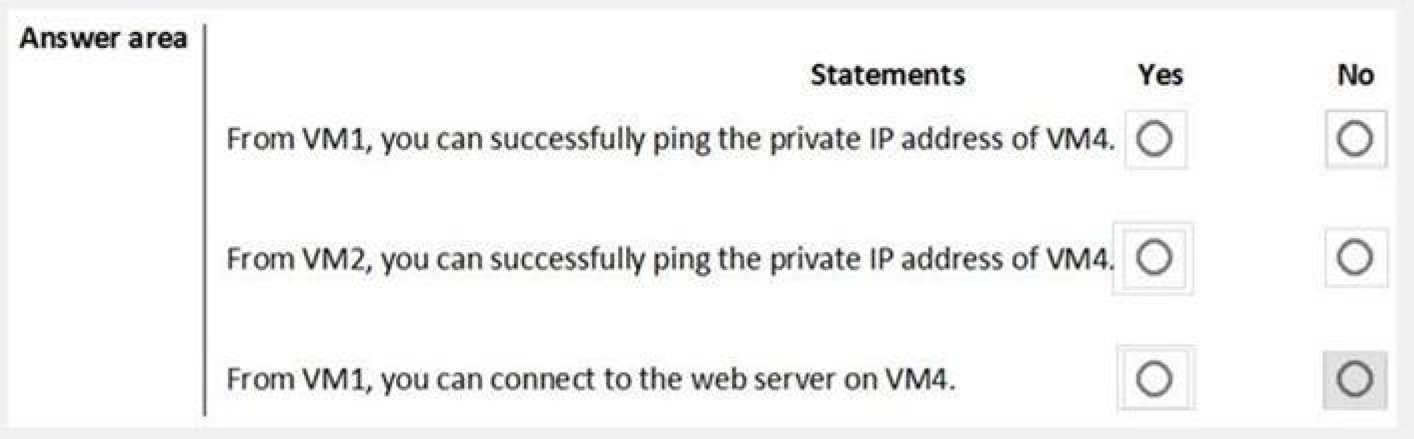
| Name | Network interface | Application security group | Connected to |
|---|---|---|---|
| VM1 | NIC1 | ASG1 | Subnet11 |
| VM2 | NIC2 | ASG2 | Subnet11 |
| VM3 | NIC3 | *None* | Subnet12 |
| VM4 | NIC4 | ASG1 | Subnet13 |
| VM5 | NIC5 | *None* | Subnet21 |



| 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.

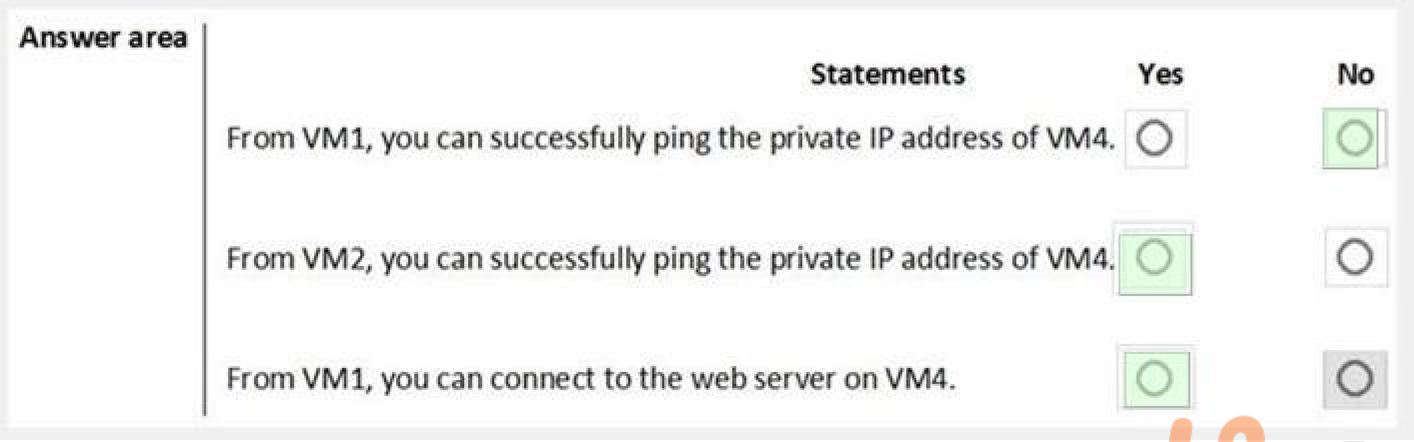
**Hot Area:**



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. | ● | ○ |

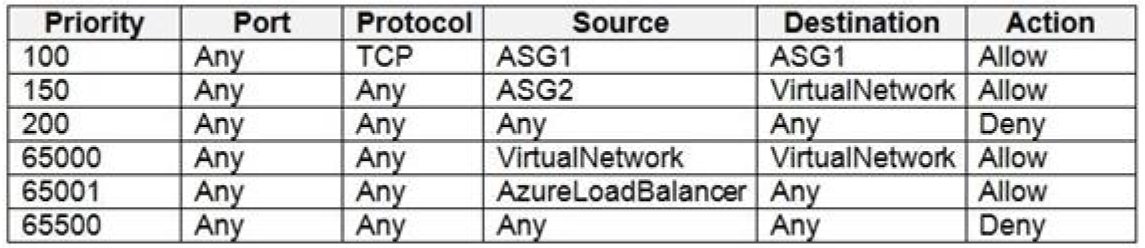
**Section:**

**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.

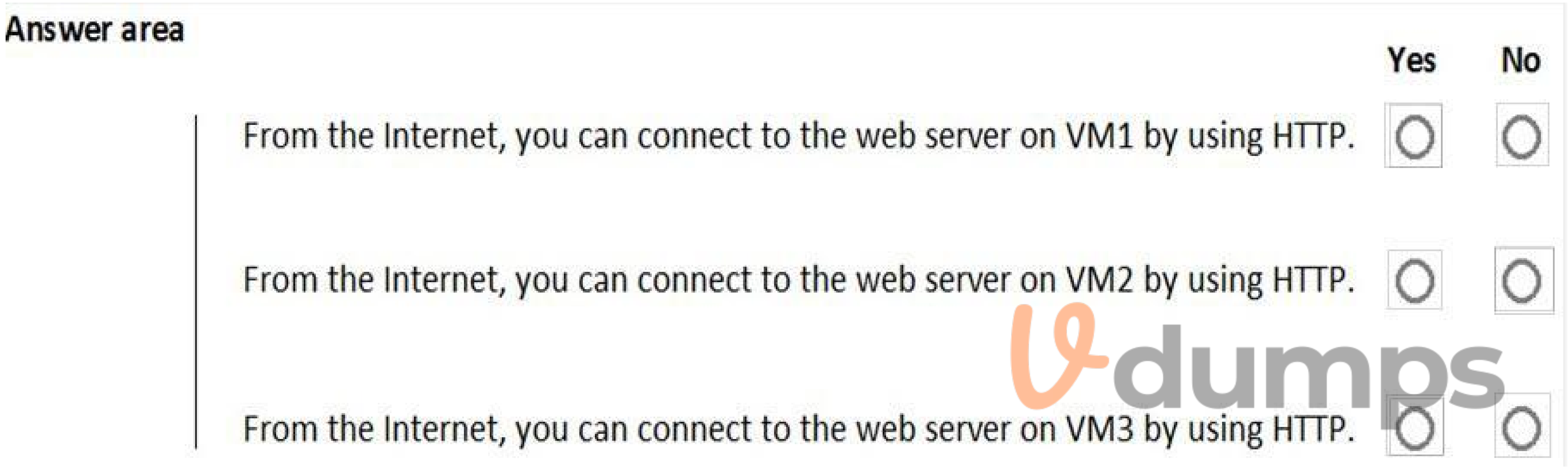
D. Configure DDoS protection for VNetwork1.

**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.

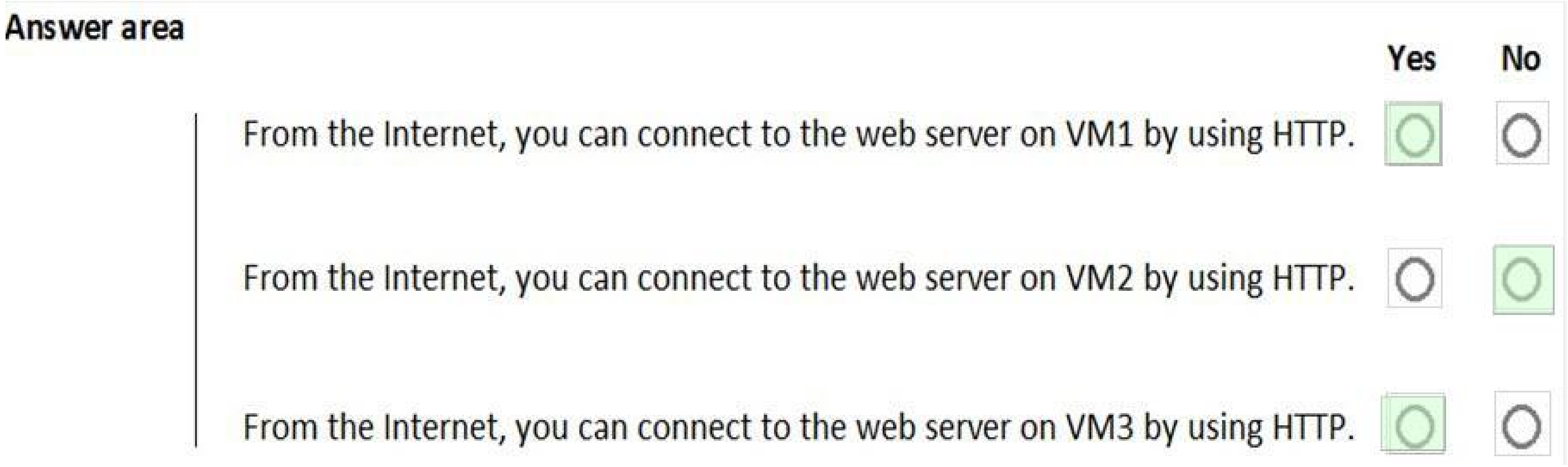
**Hot Area:**



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. | [✓ ○] | ○ |

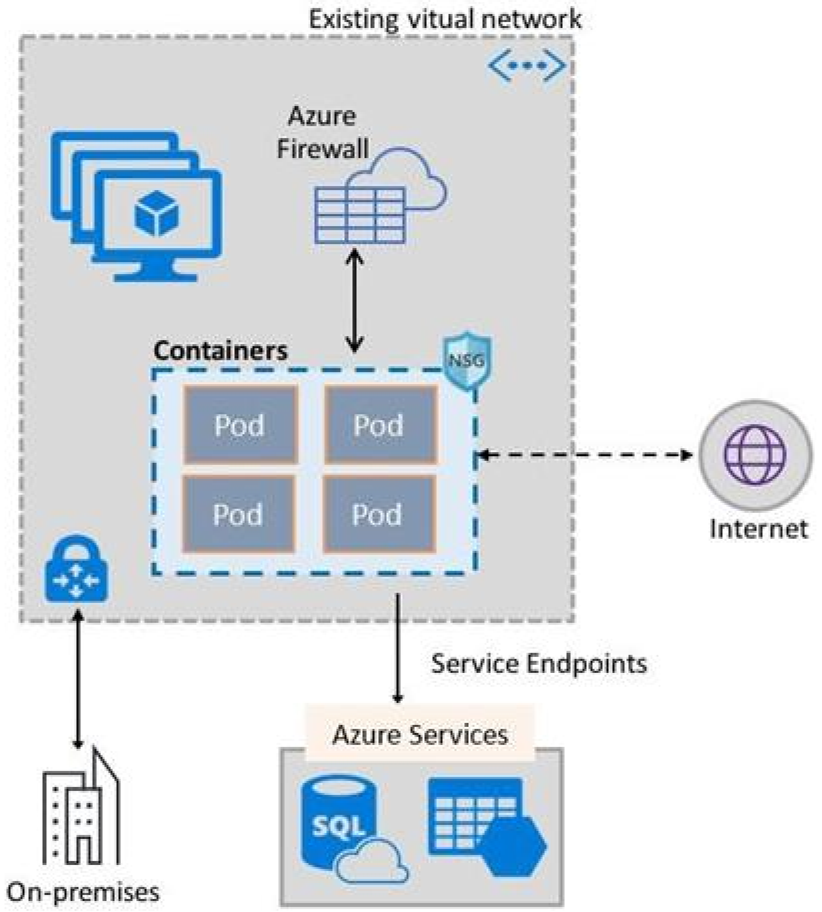
**Section:**
**Explanation:**
VM1: Yes. NSG2 applies to VM1 and this allows inbound traffic on port 80.
VM2: No. NSG2 and NSG1 apply to VM2. NSG2 allows the inbound traffic on port 80 but NSG1 does not allow it. VM3: Yes. There are no NSGs applying to VM3 so all ports will be open.

**04 - Implement platform protection**

**QUESTION 1**
You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1. You create a service endpoint for Subnet1.
Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 18.04.
You need to deploy Docker containers to VM1. The containers must be able to access Azure Storage resources and Azure SQL databases by using the service endpoint. What should you do on VM1 before you deploy the container?

A. Create an application security group and a network security group (NSG).
B. Edit the docker-compose.yml file.
C. Install the container network interface (CNI) plug-in.

**Correct Answer: C**
**Section:**
**Explanation:**
The Azure Virtual Network container network interface (CNI) plug-in installs in an Azure Virtual Machine. The plug-in supports both Linux and Windows platform. The plug-in assigns IP addresses from a virtual network to containers brought up in the virtual machine, attaching them to the virtual network, and connecting them directly to other containers and virtual network resources. The plug-in doesn't rely on overlay networks, or routes, for connectivity, and provides the same performance as virtual machines. The following picture shows how the plug-in provides Azure Virtual Network capabilities to Pods:



References:
https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview

**QUESTION 2**
You have Azure Resource Manager templates that you use to deploy Azure virtual machines.
You need to disable unused Windows features automatically as instances of the virtual machines are provisioned. What should you use?

A. device configuration policies in Microsoft Intune
B. an Azure Desired State Configuration (DSC) virtual machine extension
C. application security groups

D. device compliance policies in Microsoft Intune

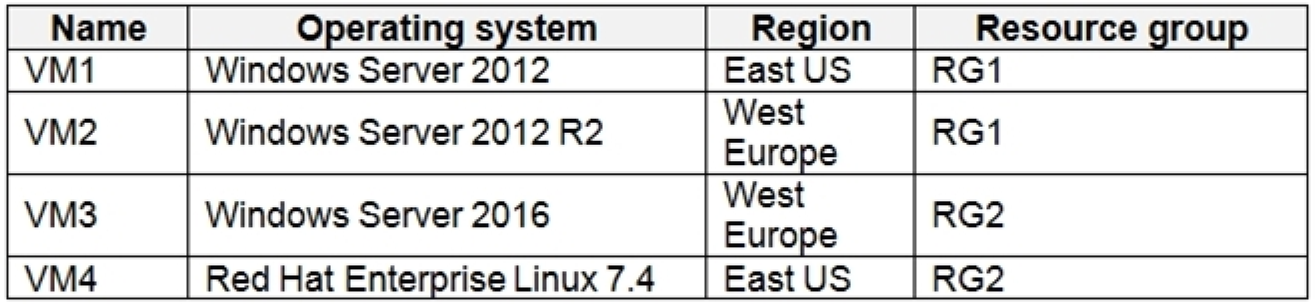
**Correct Answer: B**
**Section:**
**Explanation:**
The primary use case for the Azure Desired State Configuration (DSC) extension is to bootstrap a VM to the Azure Automation State Configuration (DSC) service. The service provides benefits that include ongoing management of the VM configuration and integration with other operational tools, such as Azure Monitoring. Using the extension to register VM's to the service provides a flexible solution that even works across Azure subscriptions.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview

**QUESTION 3**
You are configuring an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry. You need to use the auto-generated service principal to authenticate to the Azure Container Registry. What should you create?

A. an Azure Active Directory (Azure AD) group
B. an Azure Active Directory (Azure AD) role assignment
C. an Azure Active Directory (Azure AD) user
D. a secret in Azure Key Vault

**Correct Answer: B**
**Section:**
**Explanation:**
When you create an AKS cluster, Azure also creates a service principal to support cluster operability with other Azure resources. You can use this auto-generated service principal for authentication with an ACR registry. To do so, you need to create an Azure AD role assignment that grants the cluster's service principal access to the container registry. References: https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-auth-aks

**QUESTION 4**
You have the Azure virtual machines shown in the following table.



| Name | Operating system | Region | Resource group |
|---|---|---|---|
| VM1 | Windows Server 2012 | East US | RG1 |
| VM2 | Windows Server 2012 R2 | West Europe | RG1 |
| VM3 | Windows Server 2016 | West Europe | RG2 |
| VM4 | Red Hat Enterprise Linux 7.4 | East US | RG2 |

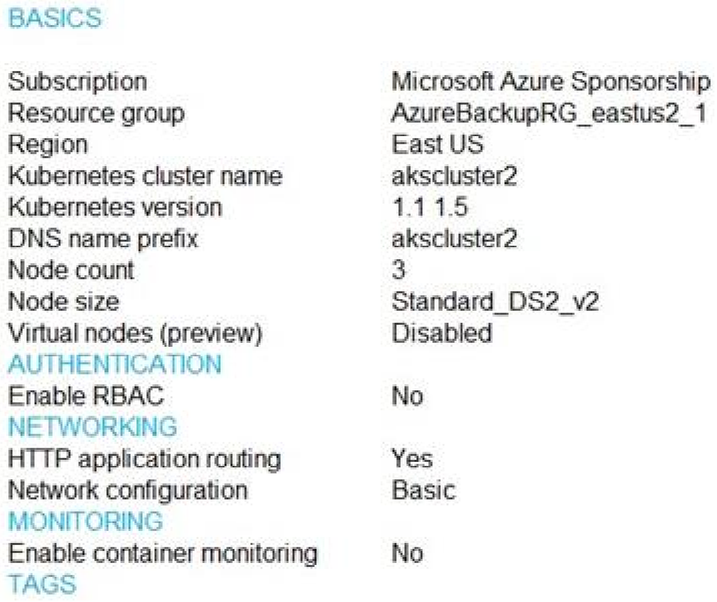
You create an Azure Log Analytics workspace named Analytics1 in RG1 in the East US region.
Which virtual machines can be enrolled in Analytics1?

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

**Correct Answer: A**
**Section:**
**Explanation:**
Note: Create a workspace
In the Azure portal, click All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics. Click Create, and then select choices for the following items:

Provide a name for the new Log Analytics workspace, such as DefaultLAWorkspace. OMS workspaces are now referred to as Log Analytics workspaces. Select a Subscription to link to by selecting from the drop-down list if the default selected is not appropriate. For Resource Group, select an existing resource group that contains one or more Azure virtual machines. Select the Location your VMs are deployed to. For additional information, see which regions Log Analytics is available in. Incorrect Answers:
B, C: A Log Analytics workspace provides a geographic location for data storage. VM2 and VM3 are at a different location. D: VM4 is a different resource group.
References: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-access

**QUESTION 5**
You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. (Click the Exhibit tab.)



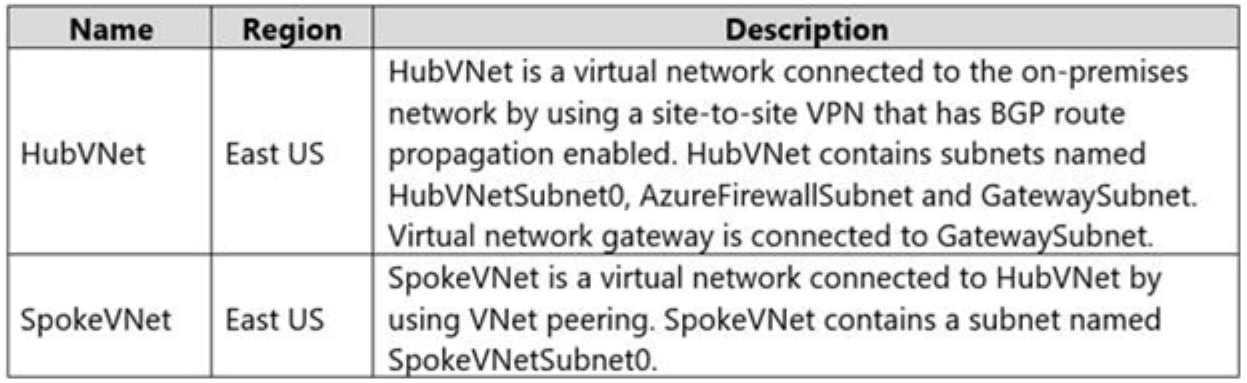
| | |
|---|---|
| BASICS | |
| Subscription | Microsoft Azure Sponsorship |
| Resource group | AzureBackupRG_eastus2_1 |
| Region | East US |
| Kubernetes cluster name | akscluster2 |
| Kubernetes version | 1.11.5 |
| DNS name prefix | akscluster2 |
| Node count | 3 |
| Node size | Standard_DS2_v2 |
| Virtual nodes (preview) | Disabled |
| AUTHENTICATION | |
| Enable RBAC | No |
| NETWORKING | |
| HTTP application routing | Yes |
| Network configuration | Basic |
| MONITORING | |
| Enable container monitoring | No |
| TAGS | |

You plan to deploy the cluster to production. You disable HTTP application routing.
You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address.
What should you do?

A. Create an AKS Ingress controller.
B. Install the container network interface (CNI) plug-in.
C. Create an Azure Standard Load Balancer.
D. Create an Azure Basic Load Balancer.

**Correct Answer: A**
**Section:**
**Explanation:**
An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services. References: https://docs.microsoft.com/en-us/azure/aks/ingress-tls

**QUESTION 6**
DRAG DROP
You have an Azure subscription that contains the virtual networks shown in the following table.



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

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

You plan to deploy an Azure firewall to HubVNet.

You create the following two routing tables:

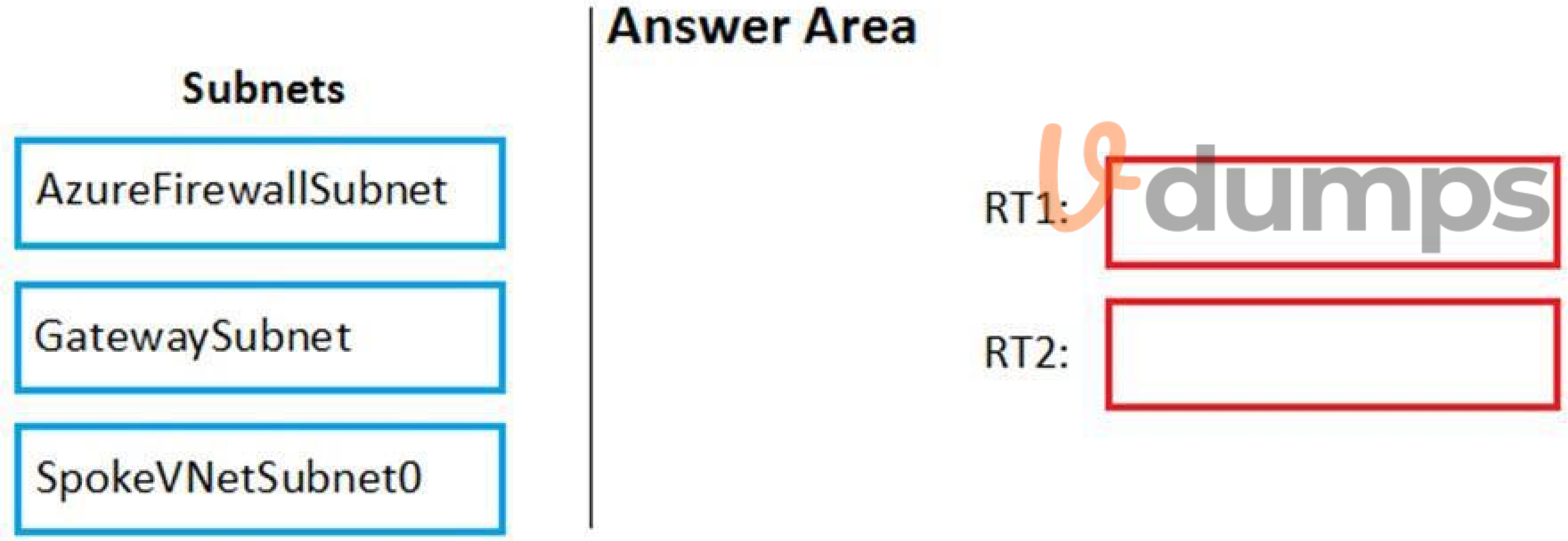
RT1: Includes a user-defined route that points to the private IP address of the Azure firewall as a next hop address RT2: Disables BGP route propagation and defines the private IP address of the Azure firewall as the default gateway

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

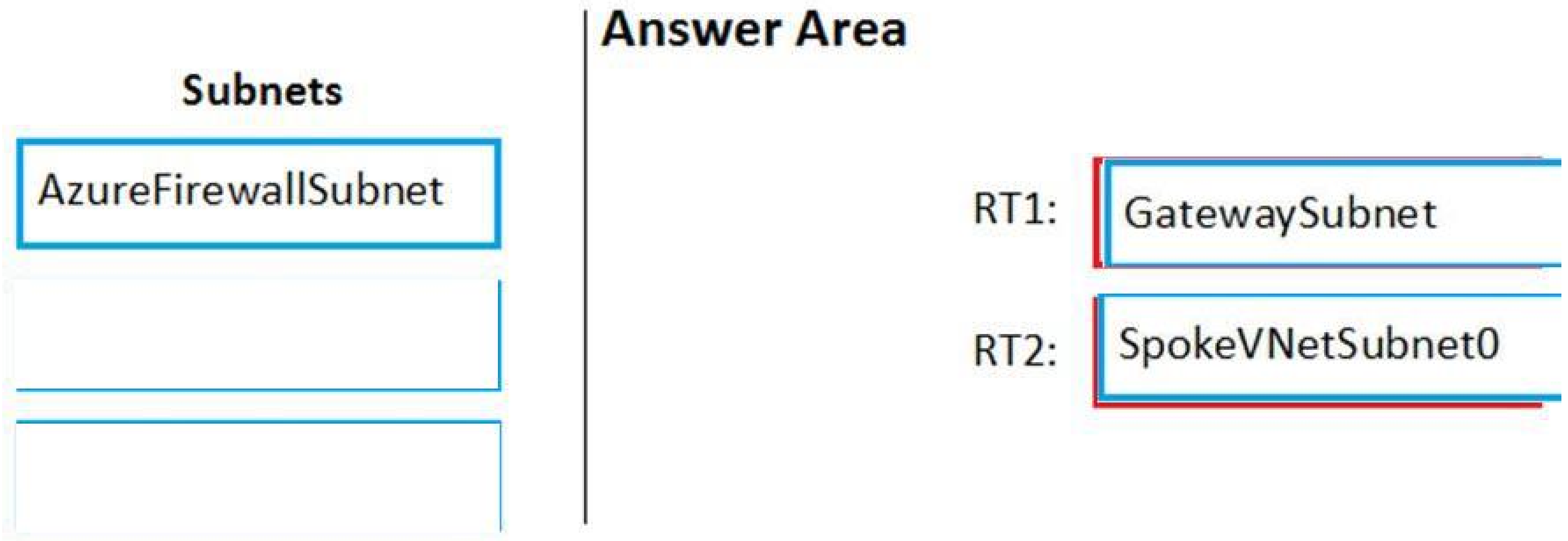
To which subnet should you associate each route table? To answer, drag the appropriate subnets to the correct route tables. Each subnet may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

**Select and Place:**



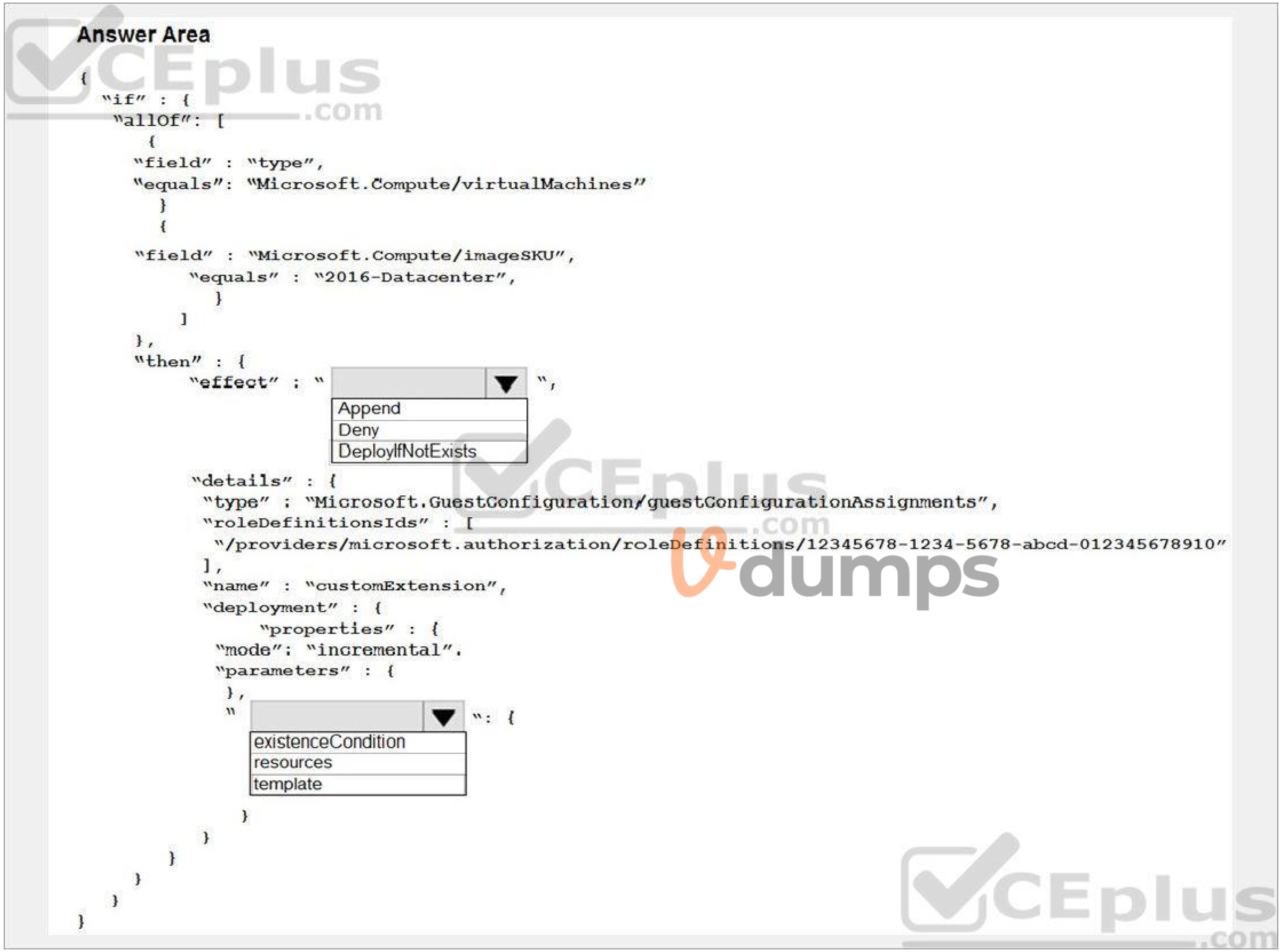
**Correct Answer:**



**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/firewall/tutorial-hybrid-portal#create-the-routes

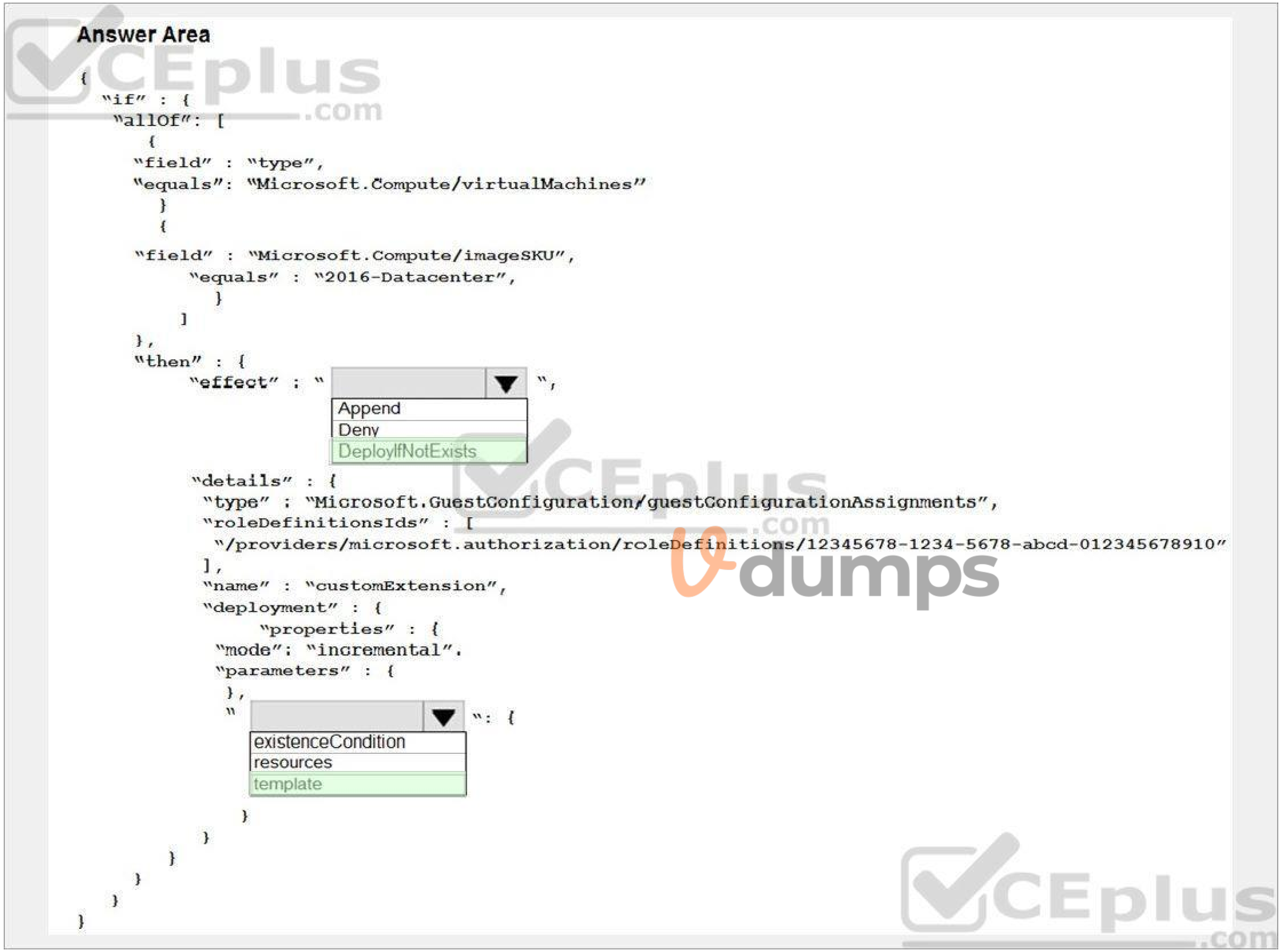
**QUESTION 7**
HOTSPOT
You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.
You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.
How should you complete the policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**



```
{
  "if" : {
   "allOf": [
      {
     "field" : "type",
     "equals": "Microsoft.Compute/virtualMachines"
       }
       {
     "field" : "Microsoft.Compute/imageSKU",
          "equals" : "2016-Datacenter",
            }
        ]
     },
     "then" : {
          "effect" : "                ",

          "details" : {
           "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
           "roleDefinitionsIds" : [
            "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
           ],
           "name" : "customExtension",
           "deployment" : {
                "properties" : {
            "mode": "incremental".
            "parameters" : {
             },
             "                ": {

                }
              }
           }
        }
     }
}
```

**Answer Area:**



```
{
  "if" : {
   "allOf": [
      {
     "field" : "type",
     "equals": "Microsoft.Compute/virtualMachines"
       }
       {
     "field" : "Microsoft.Compute/imageSKU",
          "equals" : "2016-Datacenter",
            }
         ]
     },
     "then" : {
          "effect" : "                    ",

          "details" : {
           "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
           "roleDefinitionsIds" : [
            "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
           ],
           "name" : "customExtension",
           "deployment" : {
                "properties" : {
            "mode": "incremental".
            "parameters" : {
             },
             "                   ": {

                 }
             }
          }
       }
     }
  }
```

**Section:**

**Explanation:**

Box 1: DeployIfNotExists

DeployIfNotExists executes a template deployment when the condition is met.

Box 2: Template

The details property of the DeployIfNotExists effects has all the subproperties that define the related resources to match and the template deployment to execute. Deployment [required]

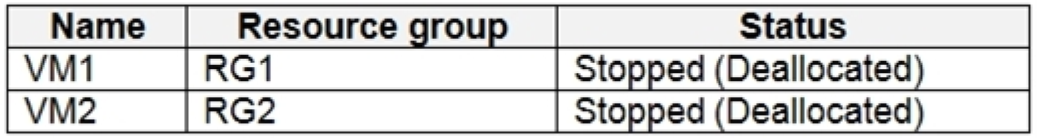
This property should include the full template deployment as it would be passed to the Microsoft.Resources/deployment

References:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

**QUESTION 8**

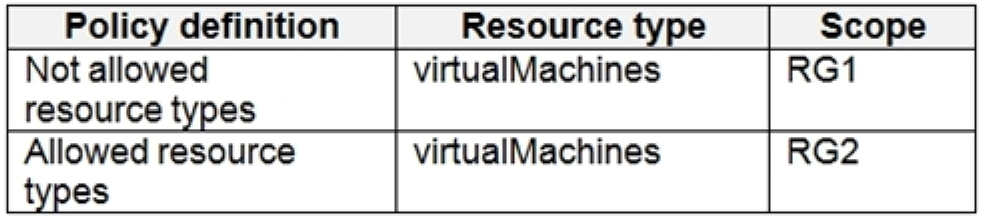
HOTSPOT

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



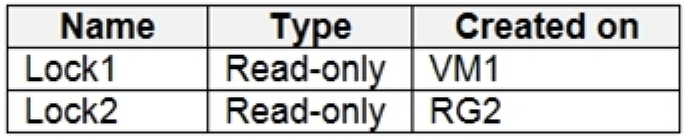
| Name | Resource group | Status |
|---|---|---|
| VM1 | RG1 | Stopped (Deallocated) |
| VM2 | RG2 | Stopped (Deallocated) |

You create the Azure policies shown in the following table.



| Policy definition | Resource type | Scope |
|---|---|---|
| Not allowed resource types | virtualMachines | RG1 |
| Allowed resource types | virtualMachines | RG2 |

You create the resource locks shown in the following table.

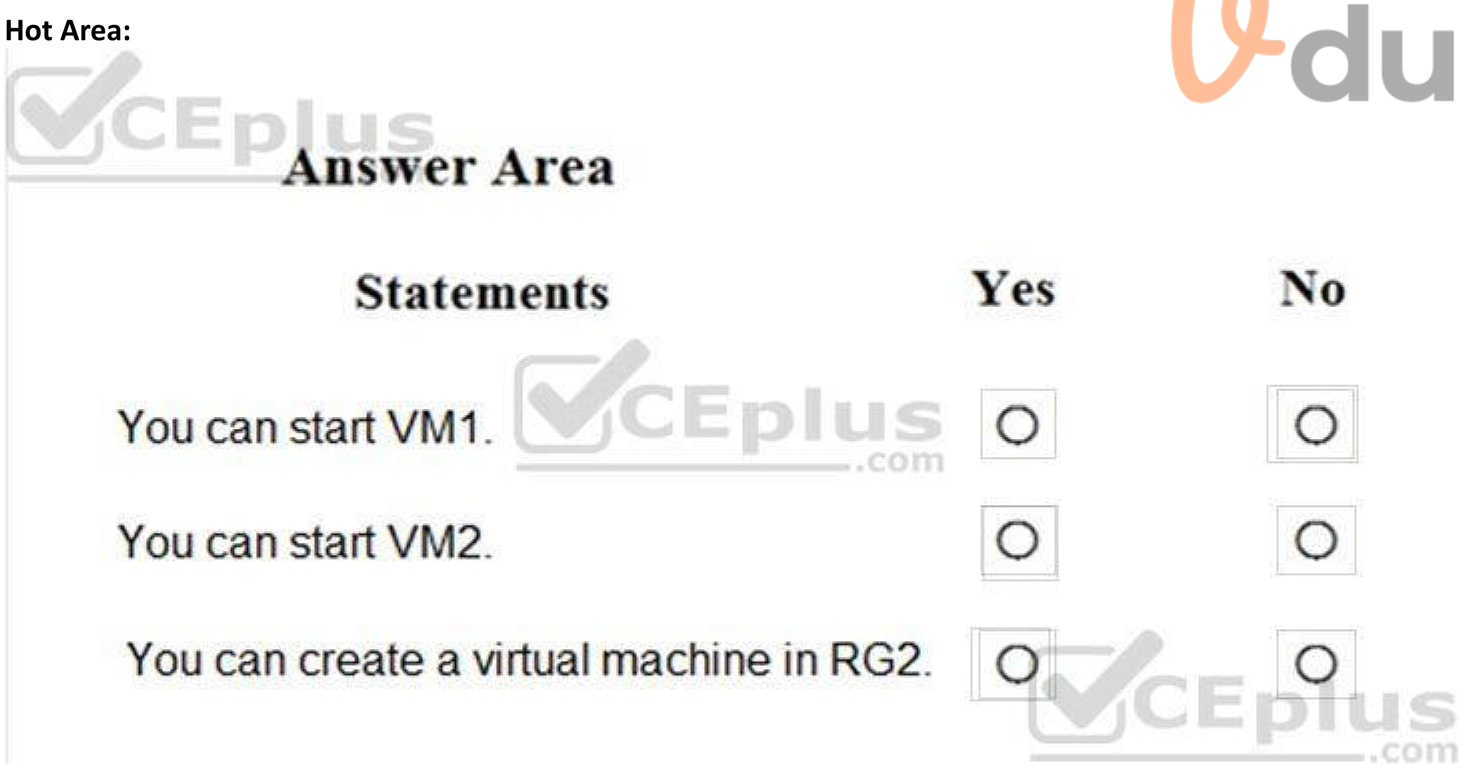


| Name | Type | Created on |
|---|---|---|
| Lock1 | Read-only | VM1 |
| Lock2 | Read-only | RG2 |

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

NOTE: Each correct selection is worth one point.

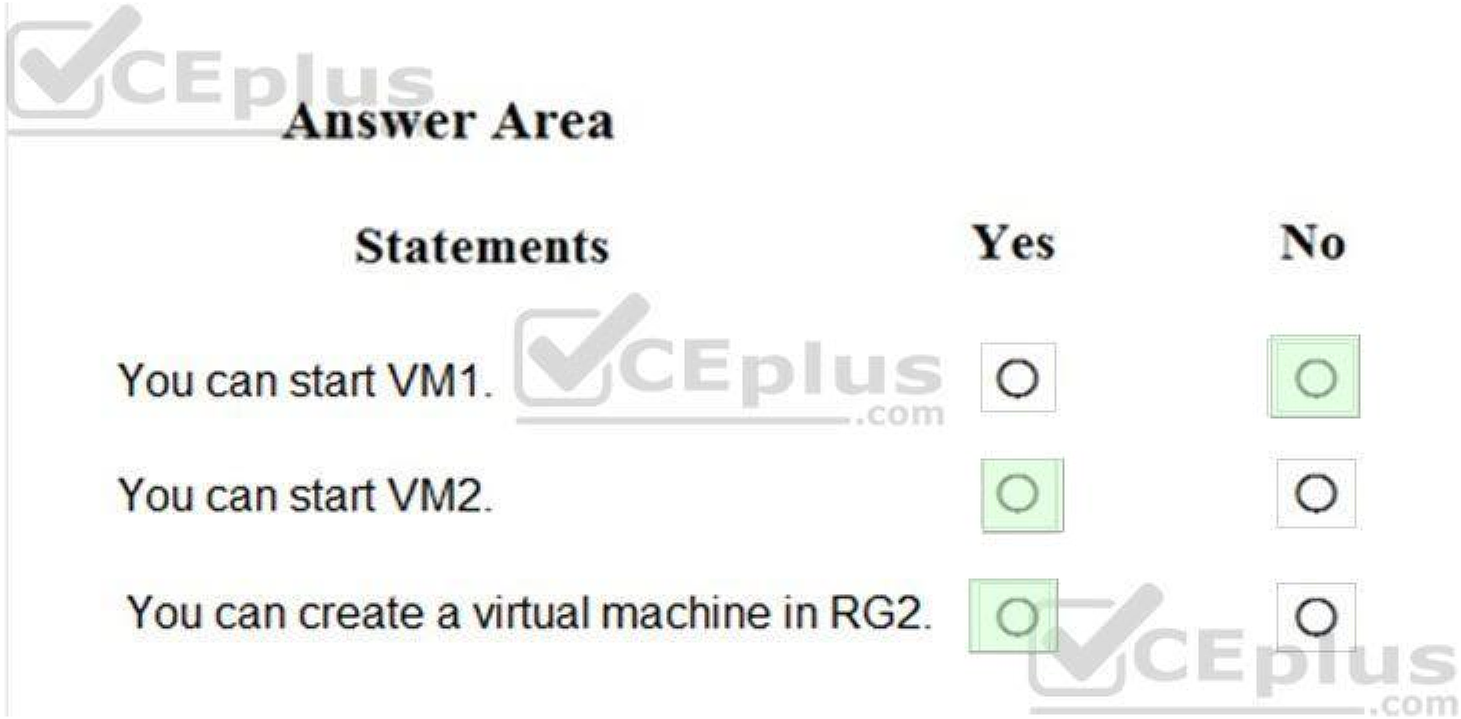
**Hot Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| You can start VM1. | ○ | ○ |
| You can start VM2. | ○ | ○ |
| You can create a virtual machine in RG2. | ○ | ○ |

**Answer Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| You can start VM1. | ○ | [✓ ○] |
| You can start VM2. | [✓ ○] | ○ |
| You can create a virtual machine in RG2. | [✓ ○] | ○ |

**Section:**

**Explanation:**

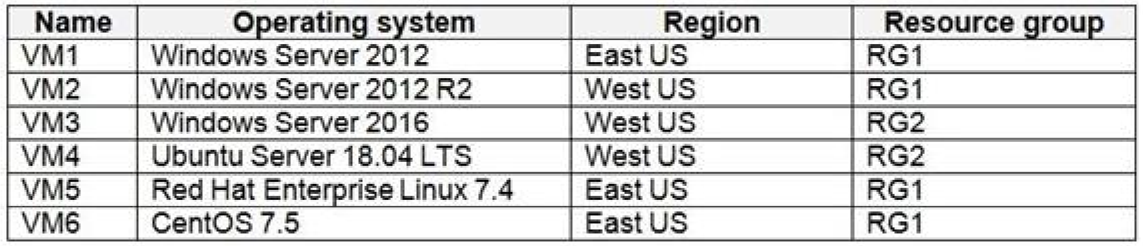
References:

https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

**QUESTION 9**

HOTSPOT

You have Azure virtual machines that have Update Management enabled. The virtual machines are configured as shown in the following table.



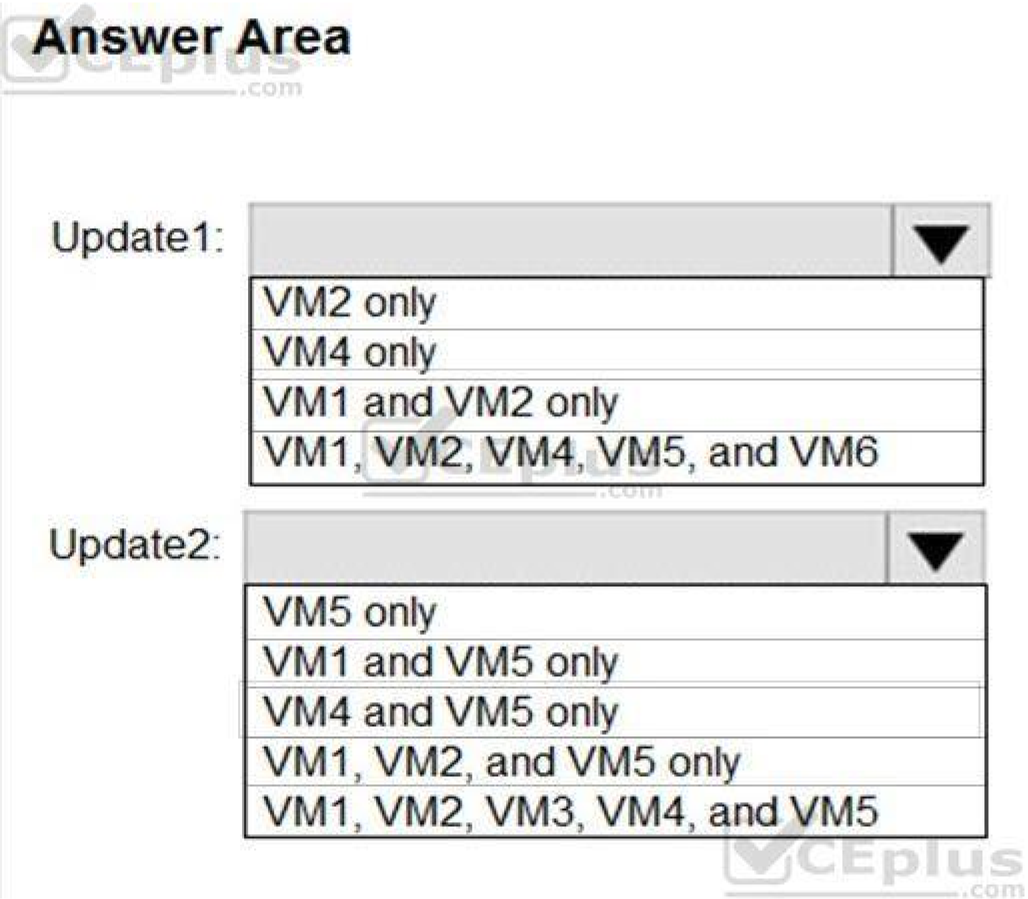
| Name | Operating system | Region | Resource group |
|---|---|---|---|
| VM1 | Windows Server 2012 | East US | RG1 |
| VM2 | Windows Server 2012 R2 | West US | RG1 |
| VM3 | Windows Server 2016 | West US | RG2 |
| VM4 | Ubuntu Server 18.04 LTS | West US | RG2 |
| VM5 | Red Hat Enterprise Linux 7.4 | East US | RG1 |
| VM6 | CentOS 7.5 | East US | RG1 |

You schedule two update deployments named Update1 and Update2. Update1 updates VM3. Update2 updates VM6.

Which additional virtual machines can be updated by using Update1 and Update2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Hot Area:**



Answer Area

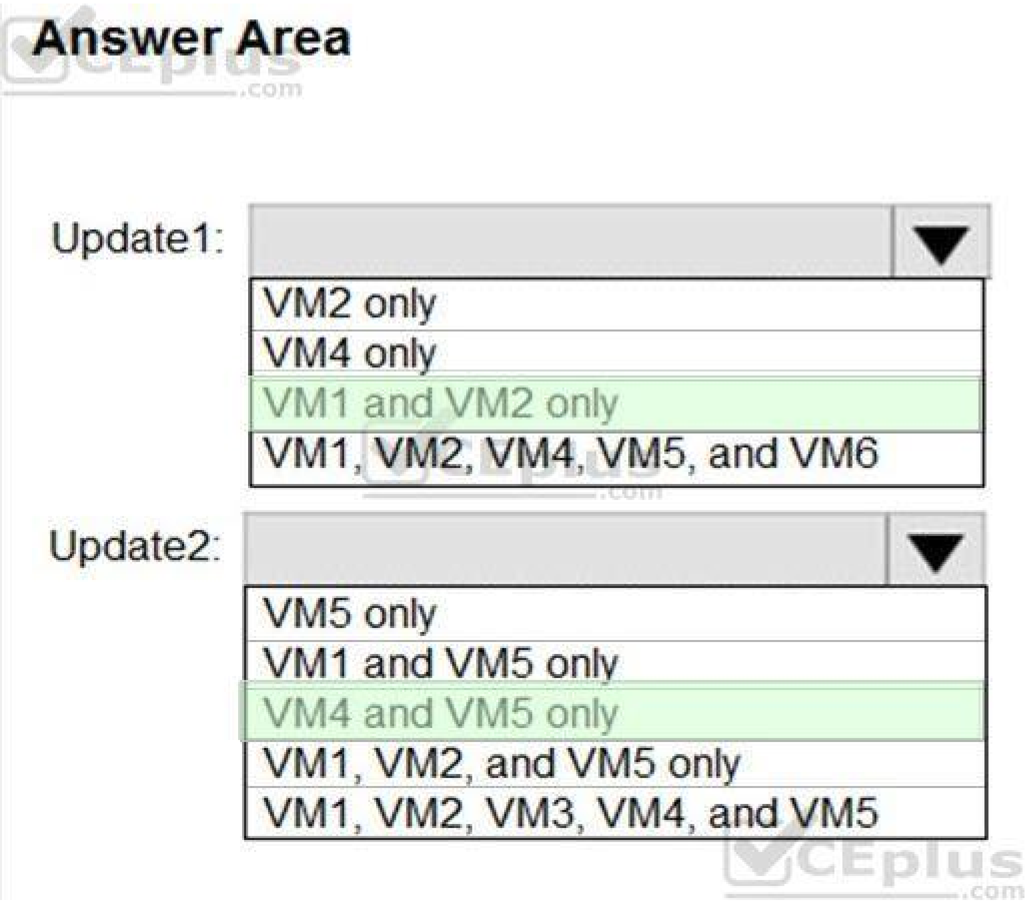
Update1: ▼

- VM2 only
- VM4 only
- VM1 and VM2 only
- VM1, VM2, VM4, VM5, and VM6

Update2: ▼

- VM5 only
- VM1 and VM5 only
- VM4 and VM5 only
- VM1, VM2, and VM5 only
- VM1, VM2, VM3, VM4, and VM5

**Answer Area:**



Answer Area

Update1: ▼

- VM2 only
- VM4 only
- [✓ VM1 and VM2 only]
- VM1, VM2, VM4, VM5, and VM6

Update2: ▼

- VM5 only
- VM1 and VM5 only
- [✓ VM4 and VM5 only]
- VM1, VM2, and VM5 only
- VM1, VM2, VM3, VM4, and VM5

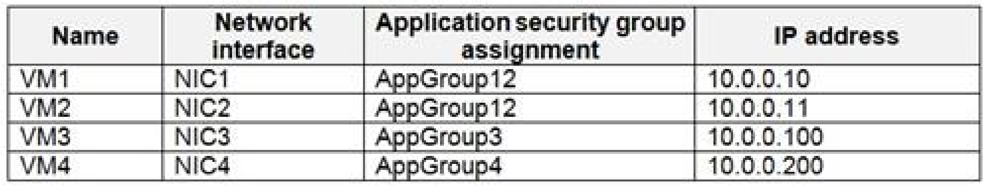
**Section:**

**Explanation:**

Update1: VM1 and VM2 only
VM3: Windows Server 2016 West US RG2
Update2: VM4 and VM5 only
VM6: CentOS 7.5 East US RG1
For Linux, the machine must have access to an update repository. The update repository can be private or public.
References:
https://docs.microsoft.com/en-us/azure/automation/automation-update-management

**QUESTION 10**

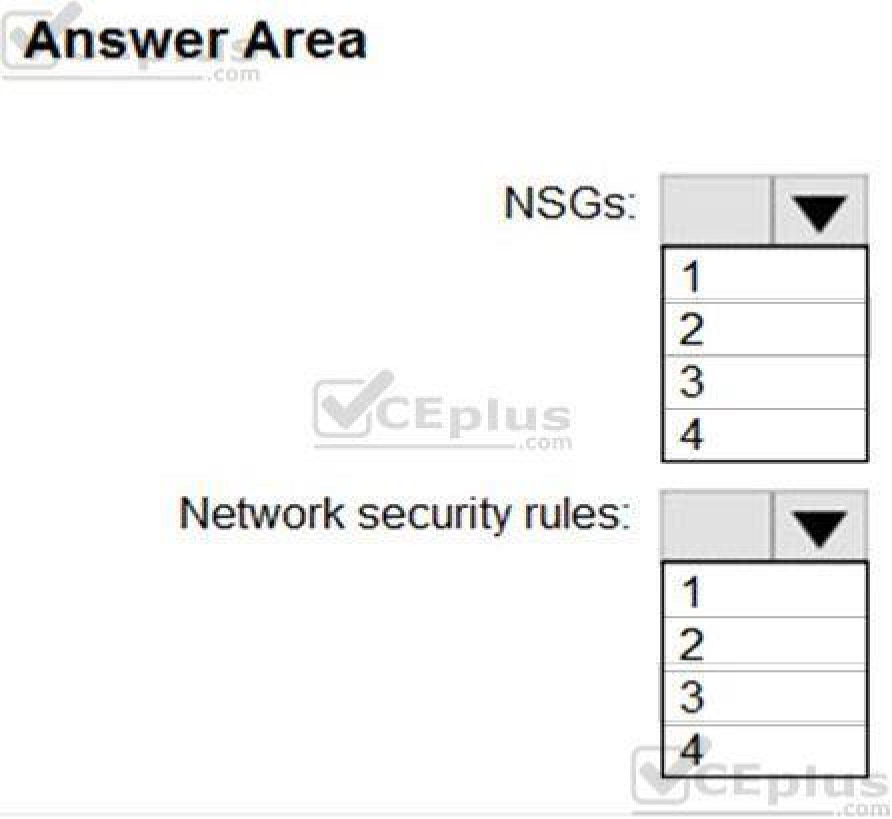
HOTSPOT
You have an Azure subscription named Sub1.
You create a virtual network that contains one subnet. On the subnet, you provision the virtual machines shown in the following table.



| Name | Network interface | Application security group assignment | IP address |
|---|---|---|---|
| VM1 | NIC1 | AppGroup12 | 10.0.0.10 |
| VM2 | NIC2 | AppGroup12 | 10.0.0.11 |
| VM3 | NIC3 | AppGroup3 | 10.0.0.100 |
| VM4 | NIC4 | AppGroup4 | 10.0.0.200 |

Currently, you have not provisioned any network security groups (NSGs).
You need to implement network security to meet the following requirements:
Allow traffic to VM4 from VM3 only.
Allow traffic from the Internet to VM1 and VM2 only.
Minimize the number of NSGs and network security rules.
How many NSGs and network security rules should you create? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**

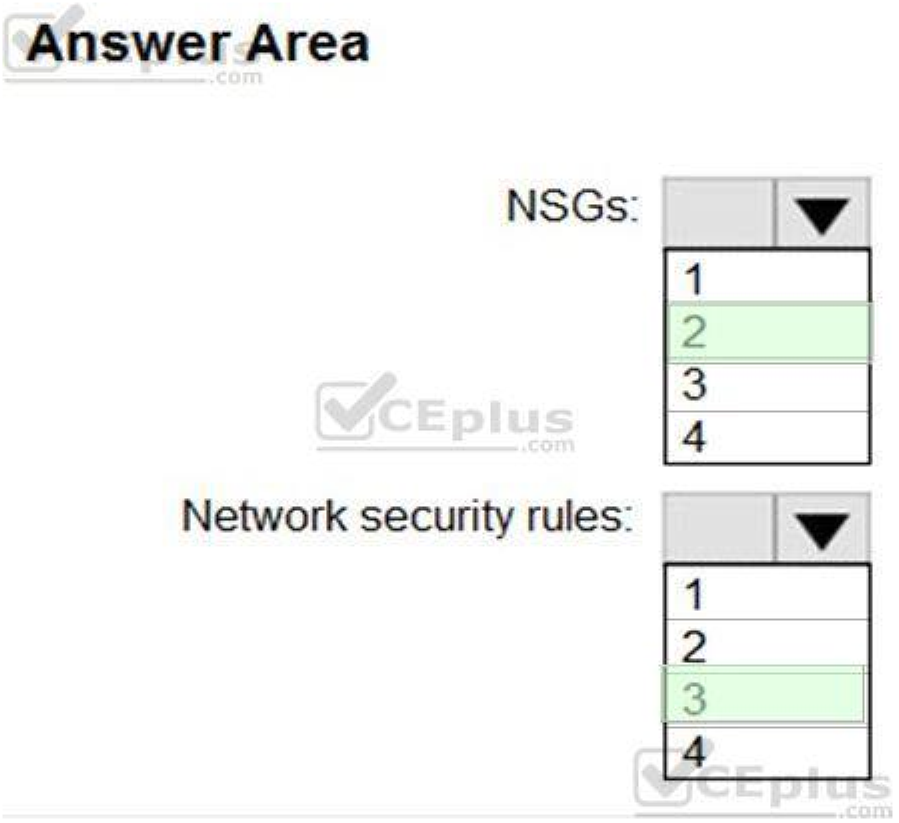


Answer Area

NSGs:
1
2
3
4

Network security rules:
1
2
3
4

**Answer Area:**



Answer Area

NSGs: 1 [✓ 2] 3 4

Network security rules: 1 2 [✓ 3] 4

**Section:**

**Explanation:**

NSGs: 2

Network security rules: 3

Not 2: You cannot specify multiple service tags or application groups) in a security rule.

References:

https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

**QUESTION 11**

HOTSPOT

You have an Azure key vault.

You need to delegate administrative access to the key vault to meet the following requirements:

Provide a user named User1 with the ability to set advanced access policies for the key vault.

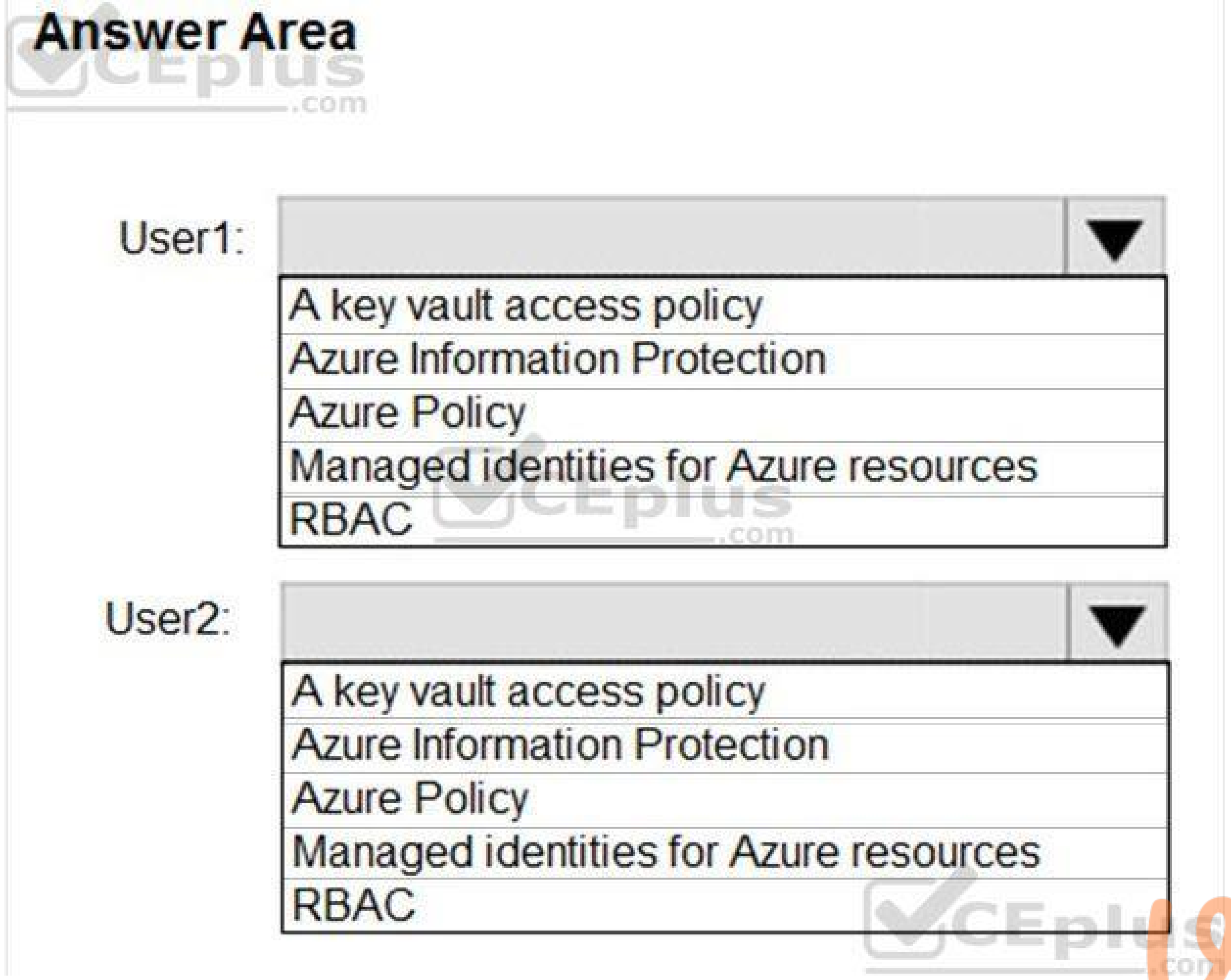
Provide a user named User2 with the ability to add and delete certificates in the key vault.

Use the principle of least privilege.

What should you use to assign access to each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Hot Area:**



Answer Area

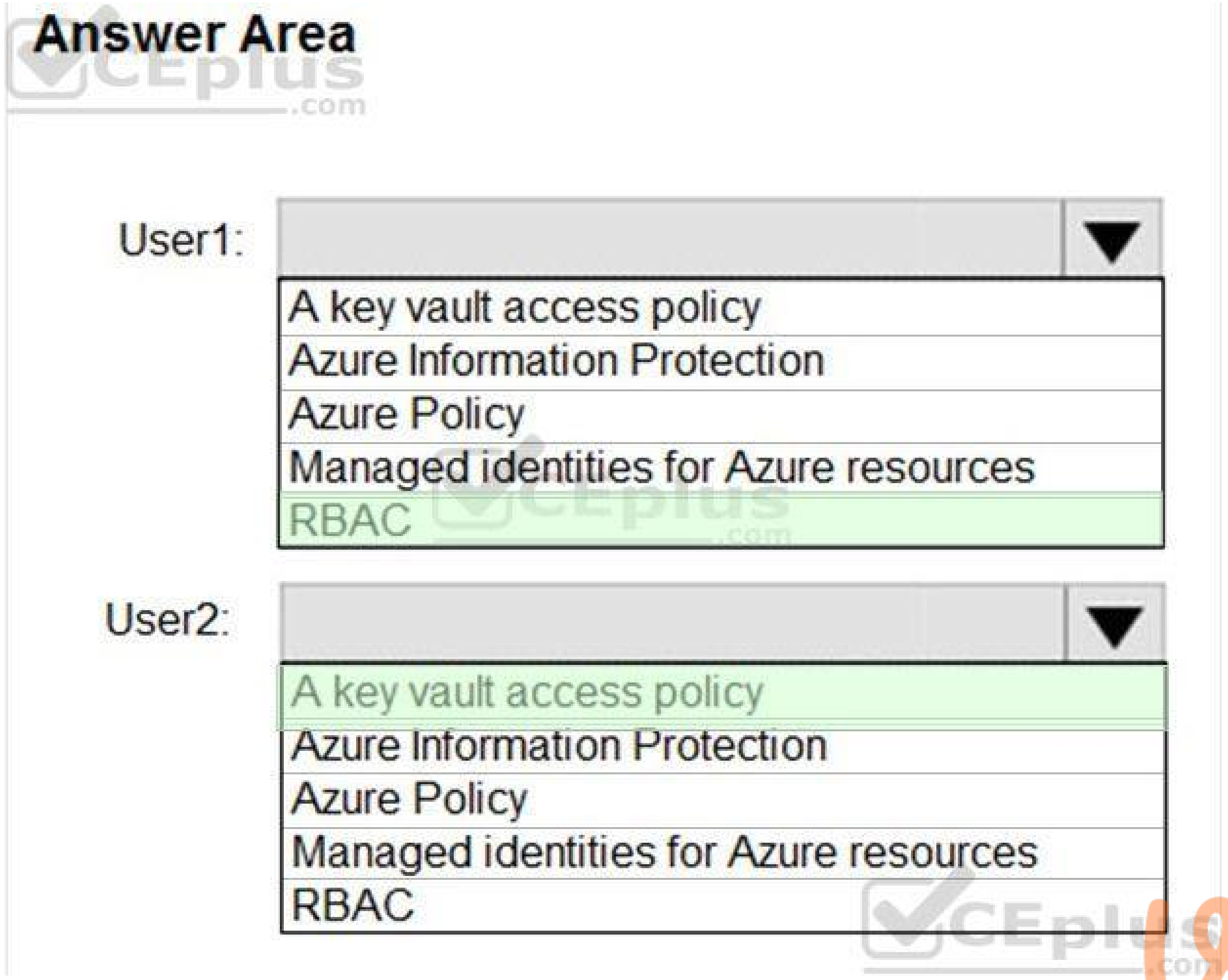
User1:

- A key vault access policy
- Azure Information Protection
- Azure Policy
- Managed identities for Azure resources
- RBAC

User2:

- A key vault access policy
- Azure Information Protection
- Azure Policy
- Managed identities for Azure resources
- RBAC

**Answer Area:**



Answer Area

User1:

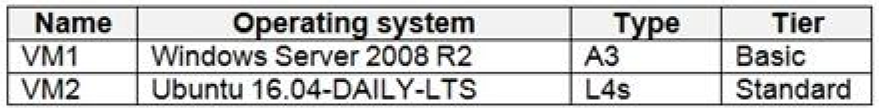
- A key vault access policy
- Azure Information Protection
- Azure Policy
- Managed identities for Azure resources
- [✓ RBAC]

User2:

- [✓ A key vault access policy]
- Azure Information Protection
- Azure Policy
- Managed identities for Azure resources
- RBAC

**Section:**
**Explanation:**
User1: RBAC
RBAC is used as the Key Vault access control mechanism for the management plane. It would allow a user with the proper identity to:
set Key Vault access policies
create, read, update, and delete key vaults
set Key Vault tags
Note: Role-based access control (RBAC) is a system that provides fine-grained access management of Azure resources. Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs.
User2: A key vault access policy
A key vault access policy is the access control mechanism to get access to the key vault data plane. Key Vault access policies grant permissions separately to keys, secrets, and certificates.
References:
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

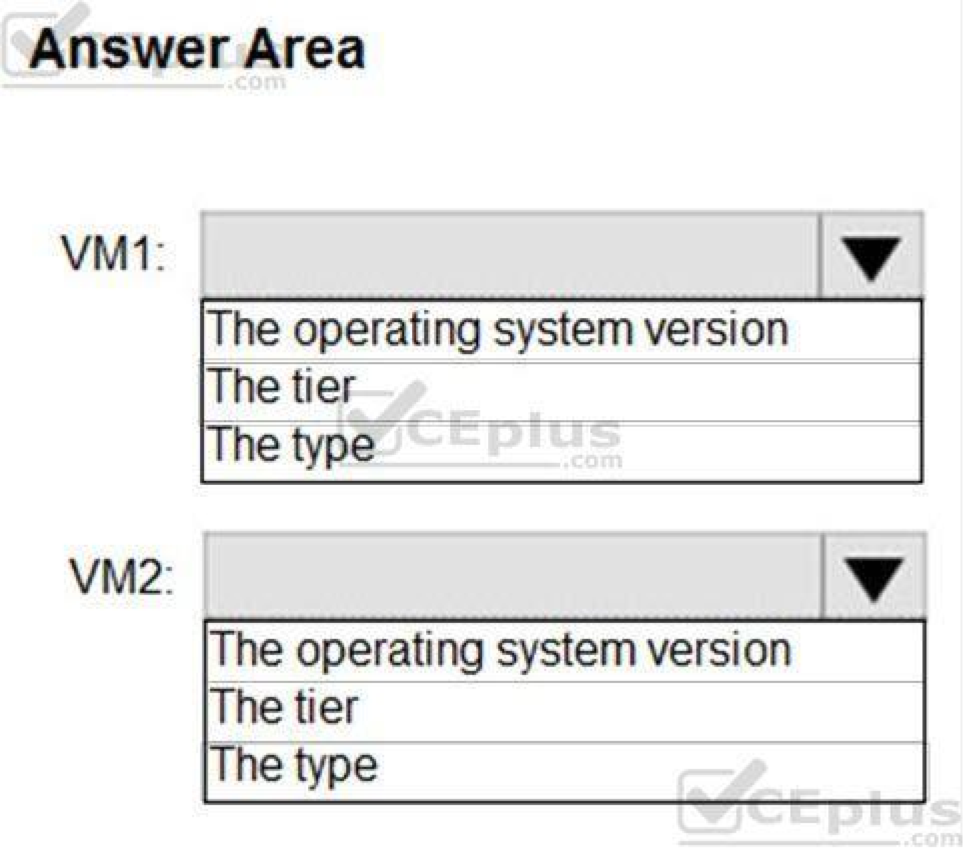
**QUESTION 12**
HOTSPOT
You have two Azure virtual machines in the East US2 region as shown in the following table.



| Name | Operating system | Type | Tier |
|---|---|---|---|
| VM1 | Windows Server 2008 R2 | A3 | Basic |
| VM2 | Ubuntu 16.04-DAILY-LTS | L4s | Standard |

You deploy and configure an Azure Key vault.
You need to ensure that you can enable Azure Disk Encryption on VM1 and VM2.
What should you modify on each virtual machine? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**

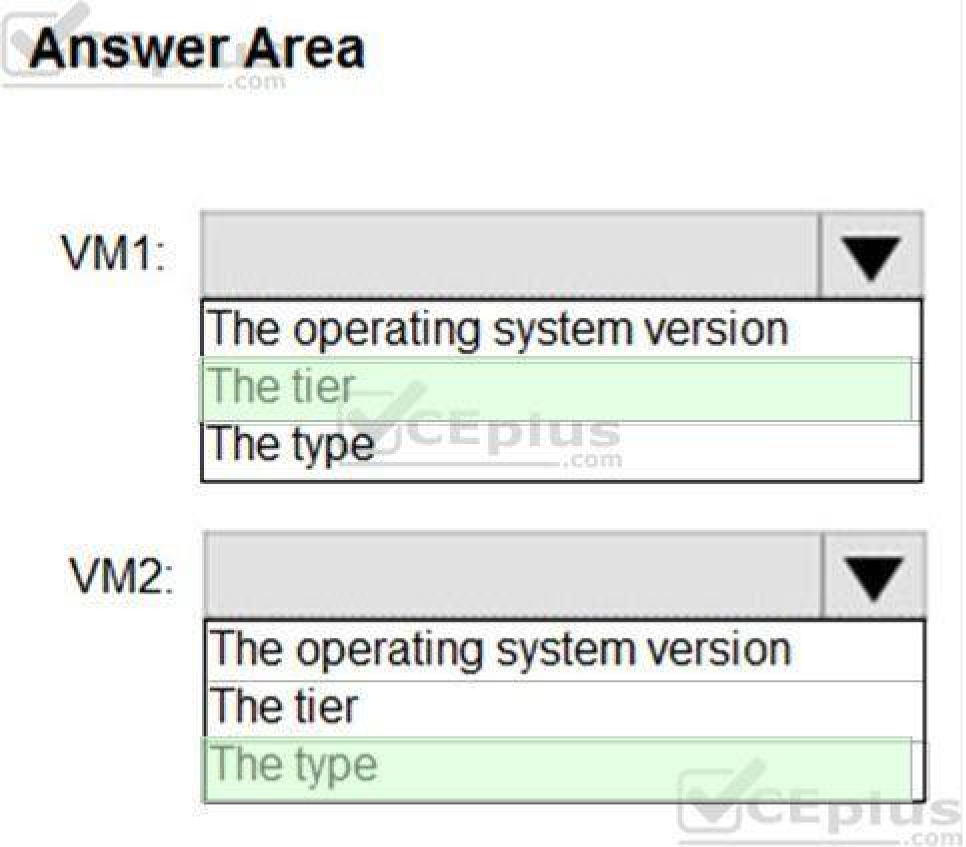


Answer Area

VM1:
- The operating system version
- The tier
- The type

VM2:
- The operating system version
- The tier
- The type

**Answer Area:**



Answer Area

VM1:
- The operating system version
- [✓ The tier]
- The type

VM2:
- The operating system version
- The tier
- [✓ The type]

**Section:**
**Explanation:**
VM1: The Tier
The Tier needs to be upgraded to standard.

Disk Encryption for Windows and Linux IaaS VMs is in General Availability in all Azure public regions and Azure Government regions for Standard VMs and VMs with Azure Premium Storage.
VM2: The type
Need to change the VMtype to any of A, D, DS, G, GS, F, and so on, series IaaS VMs.
Not the operating system version: Ubuntu 16.04 is supported.
References:
https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview
https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-faq#bkmk_LinuxOSSupport

**QUESTION 13**
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. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.
You need to deploy Microsoft Antimalware to the virtual machines.
Solution: You add an extension to each virtual machine.
Does this meet the goal?

A. Yes
B. No

**Correct Answer: A**
**Section:**
**Explanation:**
You can use Visual Studio to enable and configure the Microsoft Antimalware service. This entails selecting Microsoft Antimalware extension from the dropdown list under Installed Extensions and click Add to configure with default antimalware configuration.
References:
https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

**QUESTION 14**
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. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.
You need to deploy Microsoft Antimalware to the virtual machines.
Solution: You connect to each virtual machine and add a Windows feature.
Does this meet the goal?

A. Yes
B. No

**Correct Answer: B**
**Section:**
**Explanation:**
Microsoft Antimalware is deployed as an extension and not a feature.
References:
https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

**QUESTION 15**
From Azure Security, you create a custom alert rule.

You need to configure which users will receive an email message when the alert is triggered.
What should you do?

A. From Azure Monitor, create an action group.
B. From Security Center, modify the Security policy settings of the Azure subscription.
C. From Azure Active Directory (Azure AD). modify the members of the Security Reader role group.
D. From Security Center, modify the alert rule.

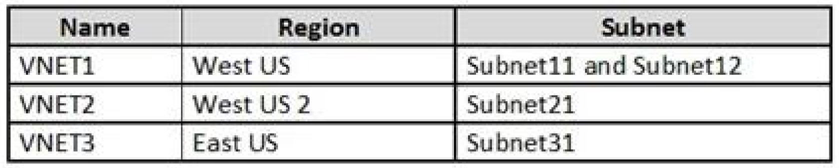
**Correct Answer: A**
**Section:**
**Explanation:**
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups

**QUESTION 16**
You are configuring and securing a network environment.
You deploy an Azure virtual machine named VM1 that is configured to analyze network traffic.
You need to ensure that all network traffic is routed through VM1.
What should you configure?

A. a system route
B. a network security group (NSG)
C. a user-defined route

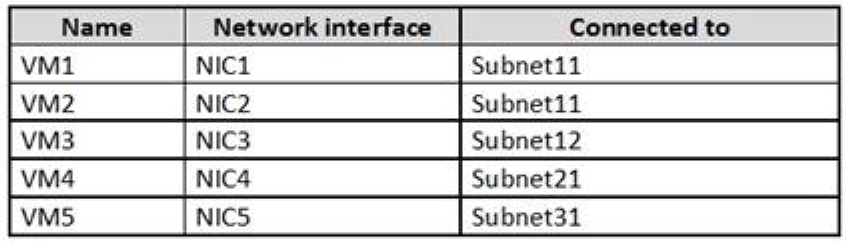
**Correct Answer: C**
**Section:**
**Explanation:**
Although the use of system routes facilitates traffic automatically for your deployment, there are cases in which you want to control the routing of packets through a virtual appliance. You can do so by creating user defined routes that specify the next hop for packets flowing to a specific subnet to go to your virtual appliance instead, and enabling IP forwarding for the VM running as the virtual appliance.
Note: User Defined Routes
For most environments you will only need the system routes already defined by Azure. However, you may need to create a route table and add one or more routes in specific cases, such as:
Force tunneling to the Internet via your on-premises network.
Use of virtual appliances in your Azure environment.
In the scenarios above, you will have to create a route table and add user defined routes to it.
Reference:
https://github.com/uglide/azure-content/blob/master/articles/virtual-network/virtual-networks-udr-overview.md

**QUESTION 17**
You have an Azure subscription that contains the virtual networks shown in the following table.



| Name | Region | Subnet |
|---|---|---|
| VNET1 | West US | Subnet11 and Subnet12 |
| VNET2 | West US 2 | Subnet21 |
| VNET3 | East US | Subnet31 |

The subscription contains the virtual machines shown in the following table.



| Name | Network interface | Connected to |
|---|---|---|
| VM1 | NIC1 | Subnet11 |
| VM2 | NIC2 | Subnet11 |
| VM3 | NIC3 | Subnet12 |
| VM4 | NIC4 | Subnet21 |
| VM5 | NIC5 | Subnet31 |

On NIC1, you configure an application security group named ASG1.
On which other network interfaces can you configure ASG1?

A. NIC2 only
B. NIC2, NIC3, NIC4, and NIC5
C. NIC2 and NIC3 only
D. NIC2, NIC3, and NIC4 only

**Correct Answer: C**
**Section:**
**Explanation:**
Only network interfaces in NVET1, which consists of Subnet11 and Subnet12, can be configured in ASG1, as all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.
Reference:
https://azure.microsoft.com/es-es/blog/applicationsecuritygroups/

**QUESTION 18**
You have 15 Azure virtual machines in a resource group named RG1.
All virtual machines run identical applications.
You need to prevent unauthorized applications and malware from running on the virtual machines.
What should you do?

A. Apply an Azure policy to RG1.
B. From Azure Security Center, configure adaptive application controls.
C. Configure Azure Active Directory (Azure AD) Identity Protection.
D. Apply a resource lock to RG1.

**Correct Answer: B**
**Section:**
**Explanation:**
Adaptive application control is an intelligent, automated end-to-end application whitelisting solution from Azure Security Center. It helps you control which applications can run on your Azure and non-Azure VMs (Windows and Linux), which, among other benefits, helps harden your VMs against malware. Security Center uses machine learning to analyze the applications running on your VMs and helps you apply the specific whitelisting rules using this intelligence.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application

**QUESTION 19**
You plan to deploy Azure container instances.
You have a containerized application that validates credit cards. The application is comprised of two containers: an application container and a validation container.
The application container is monitored by the validation container. The validation container performs security checks by making requests to the application container and waiting for responses after every transaction.
You need to ensure that the application container and the validation container are scheduled to be deployed together. The containers must communicate to each other only on ports that are not externally exposed.
What should you include in the deployment?

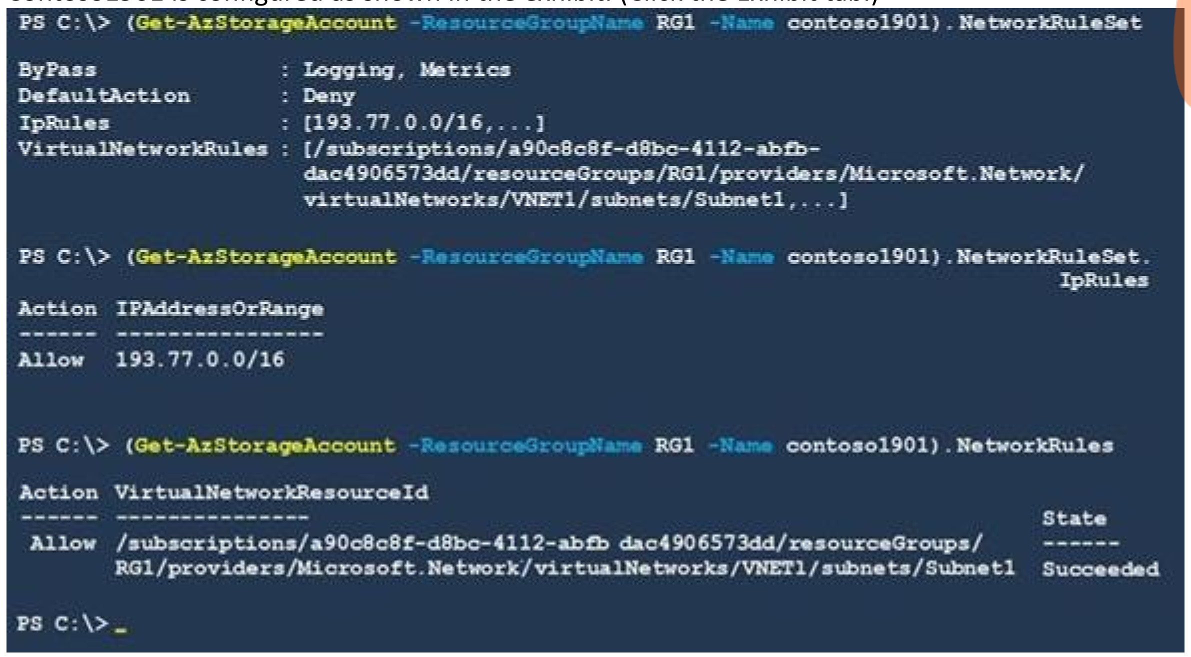
A. application security groups
B. network security groups (NSGs)
C. management groups
D. container groups

**Correct Answer: D**
**Section:**
**Explanation:**
Azure Container Instances supports the deployment of multiple containers onto a single host using a container group. A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process.
Reference:
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-container-groups

**QUESTION 20**
HOTSPOT
You create resources in an Azure subscription as shown in the following table.

| Name | Type | Region |
|---|---|---|
| RG1 | Resource group | West Europe |
| VNET1 | Azure virtual network | West Europe |
| Contoso1901 | Azure Storage account | West Europe |

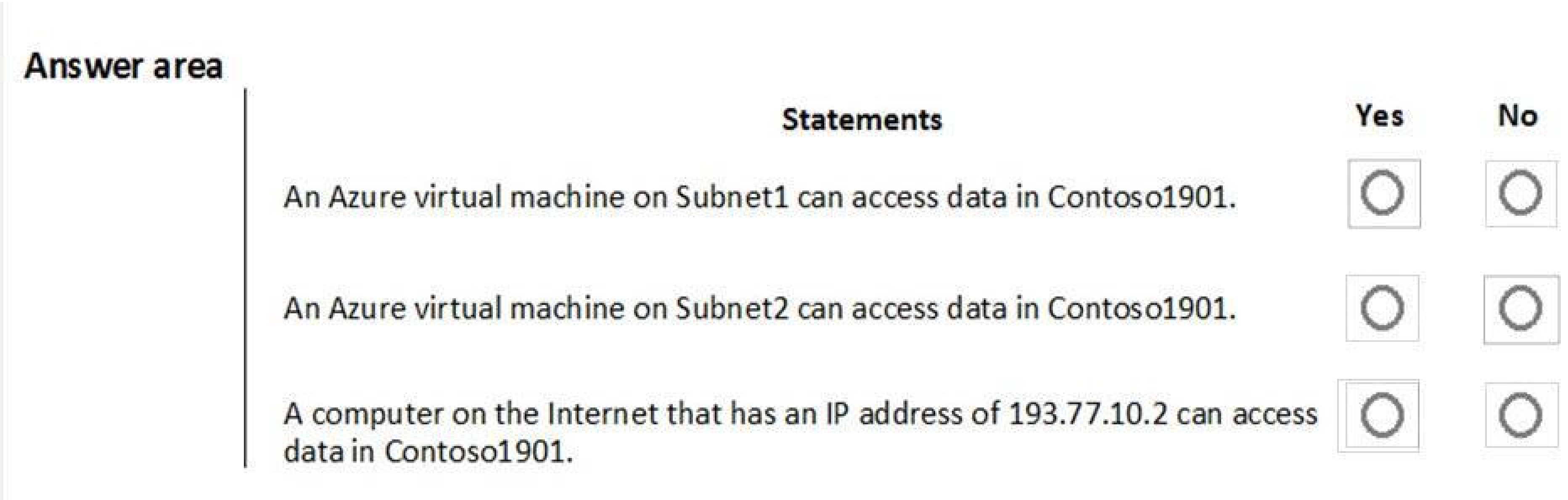
VNET1 contains two subnets named Subnet1 and Subnet2. Subnet1 has a network ID of 10.0.0.0/24. Subnet2 has a network ID of 10.1.1.0/24.
Contoso1901 is configured as shown in the exhibit. (Click the Exhibit tab.)



```
PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet

ByPass              : Logging, Metrics
DefaultAction       : Deny
IpRules             : [193.77.0.0/16,...]
VirtualNetworkRules : [/subscriptions/a90c8c8f-d8bc-4112-abfb-
                      dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/
                      virtualNetworks/VNET1/subnets/Subnet1,...]

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet.
                                                                                IpRules
Action  IPAddressOrRange
------  ----------------
Allow   193.77.0.0/16


PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRules

Action  VirtualNetworkResourceId
------  ---------------                                            State
 Allow  /subscriptions/a90c8c8f-d8bc-4112-abfb dac4906573dd/resourceGroups/    ------
        RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1  Succeeded

PS C:\>_
```

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

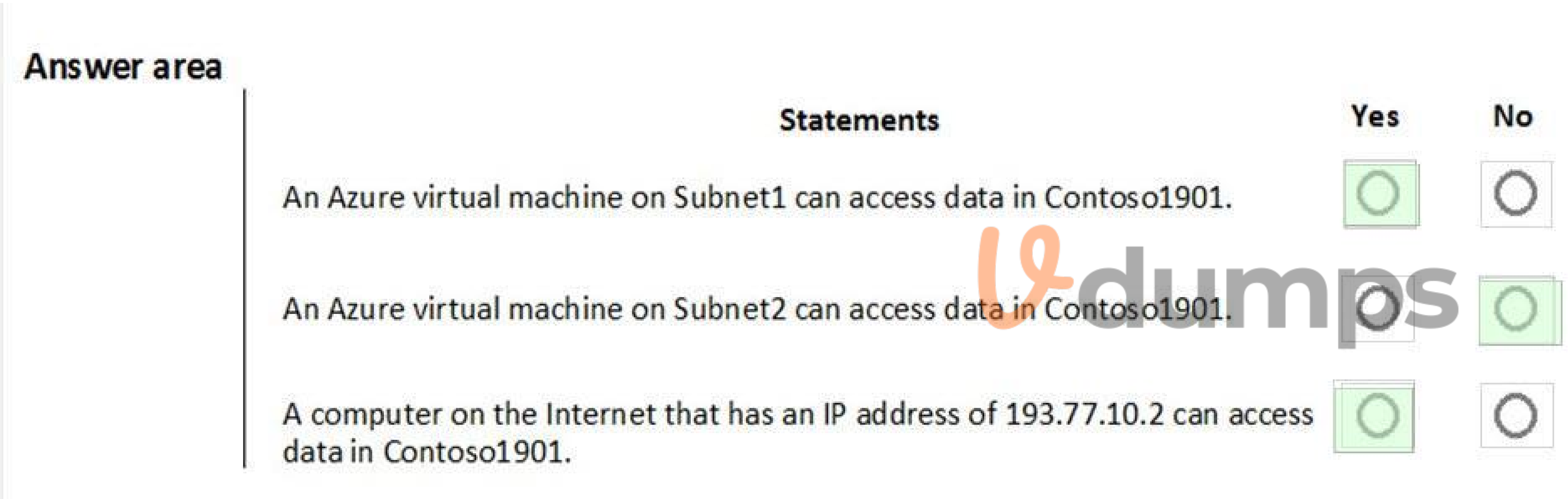
**Hot Area:**



Answer area

| Statements | Yes | No |
|---|---|---|
| An Azure virtual machine on Subnet1 can access data in Contoso1901. | ○ | ○ |
| An Azure virtual machine on Subnet2 can access data in Contoso1901. | ○ | ○ |
| A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901. | ○ | ○ |

**Answer Area:**



Answer area

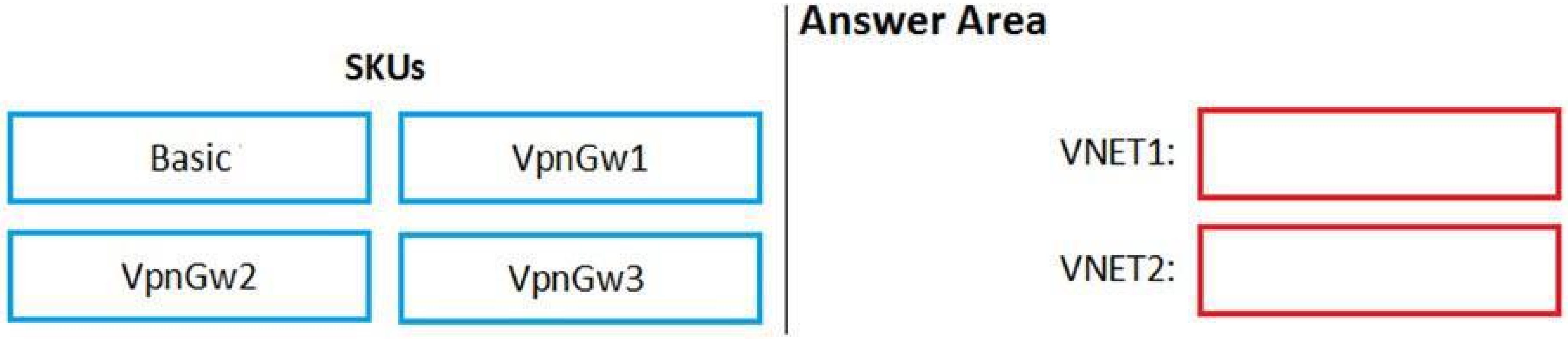
| Statements | Yes | No |
|---|---|---|
| An Azure virtual machine on Subnet1 can access data in Contoso1901. | [✓ ○] | ○ |
| An Azure virtual machine on Subnet2 can access data in Contoso1901. | ○ | [✓ ○] |
| A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901. | [✓ ○] | ○ |

**Section:**
**Explanation:**
Box 1: Yes
Access from Subnet1 is allowed.
Box 2: No
No access from Subnet2 is allowed.
Box 3: Yes
Access from IP address 193.77.10.2 is allowed.

**QUESTION 21**
DRAG DROP
You are configuring network connectivity for two Azure virtual networks named VNET1 and VNET2.
You need to implement VPN gateways for the virtual networks to meet the following requirements:
VNET1 must have six site-to-site connections that use BGP.
VNET2 must have 12 site-to-site connections that use BGP.
Costs must be minimized.
Which VPN gateway SKU should you use for each virtual network? To answer, drag the appropriate SKUs to the correct networks. Each SKU 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:**



SKUs

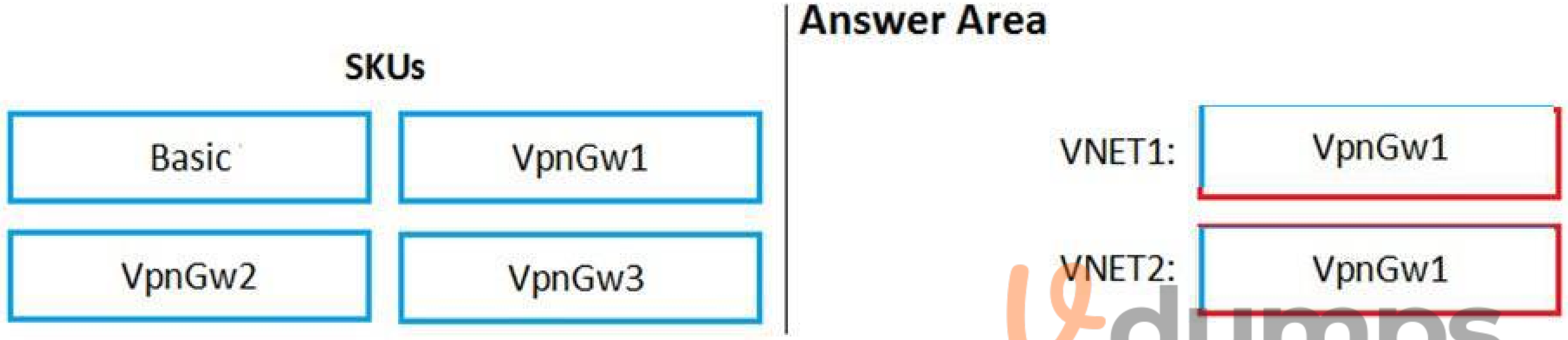
Basic | VpnGw1 | VpnGw2 | VpnGw3

Answer Area

VNET1:

VNET2:

**Correct Answer:**



SKUs

Basic | VpnGw1 | VpnGw2 | VpnGw3

Answer Area

VNET1: VpnGw1

VNET2: VpnGw1

**Section:**
**Explanation:**
References:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku

**QUESTION 22**
You are securing access to the resources in an Azure subscription.
A new company policy states that all the Azure virtual machines in the subscription must use managed disks.
You need to prevent users from creating virtual machines that use unmanaged disks.
What should you do?

A. Azure Monitor
B. Azure Policy
C. Azure Security Center
D. Azure Service Health

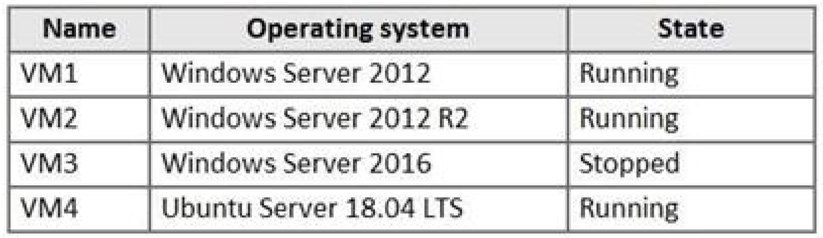
**Correct Answer: B**
**Section:**

**QUESTION 23**
You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.
You need to use automatically generated service principal for the AKS cluster to authenticate to the Azure Container Registry.
What should you create?

A. a secret in Azure Key Vault
B. a role assignment
C. an Azure Active Directory (Azure AD) user
D. an Azure Active Directory (Azure AD) group

**Correct Answer: B**
**Section:**
**Explanation:**
References:
https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal

**QUESTION 24**
You have the Azure virtual machines shown in the following table.



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

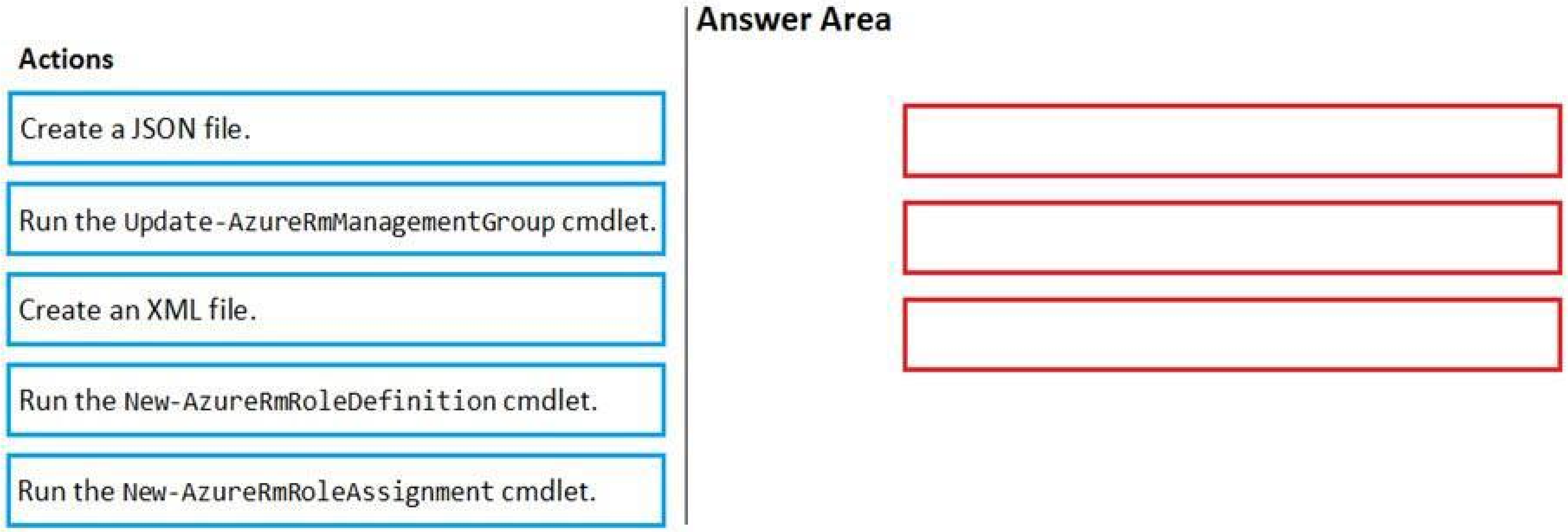
For which virtual machine can you enable Update Management?

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

**Correct Answer: C**
**Section:**
**Explanation:**
References:
https://docs.microsoft.com/en-us/azure/automation/automation-update-management?toc=%2Fazure%2Fautomation%2Ftoc.json

**QUESTION 25**
DRAG DROP
You have an Azure subscription named Sub1.
You have an Azure Active Directory (Azure AD) group named Group1 that contains all the members of your IT team.
You need to ensure that the members of Group1 can stop, start, and restart the Azure virtual machines in Sub1. The solution must use the principle of least privilege.
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:**

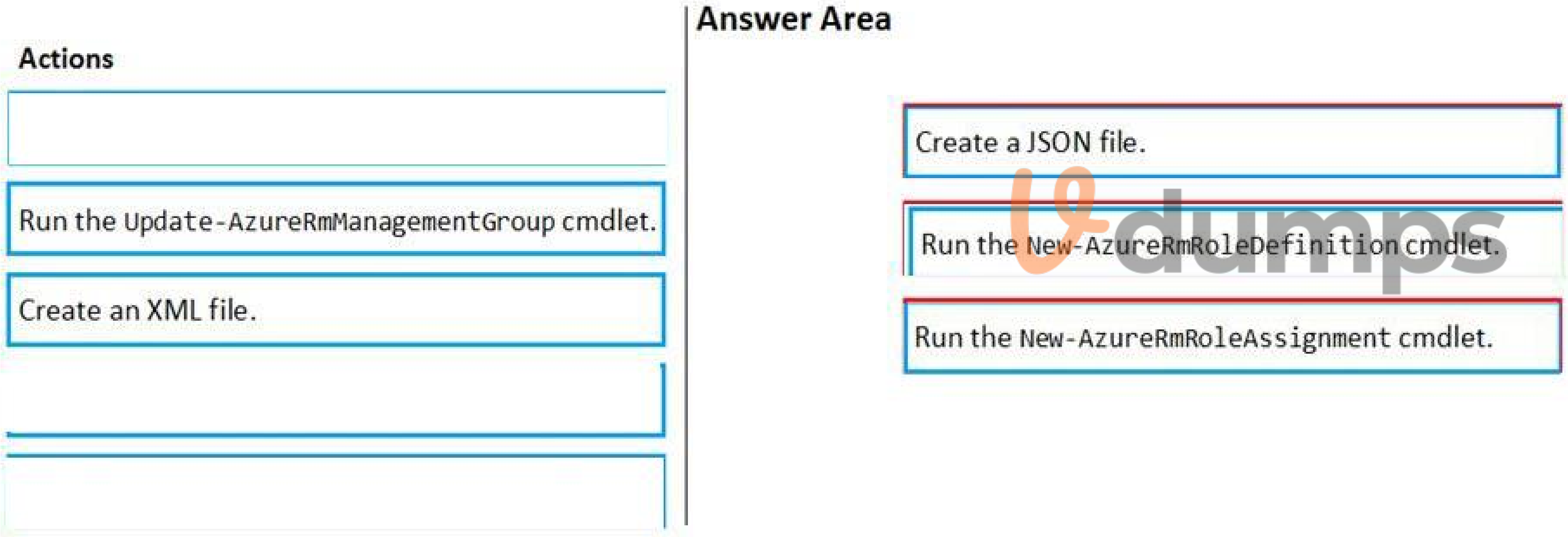


Actions

- Create a JSON file.
- Run the Update-AzureRmManagementGroup cmdlet.
- Create an XML file.
- Run the New-AzureRmRoleDefinition cmdlet.
- Run the New-AzureRmRoleAssignment cmdlet.

Answer Area

**Correct Answer:**



Actions

- Run the Update-AzureRmManagementGroup cmdlet.
- Create an XML file.

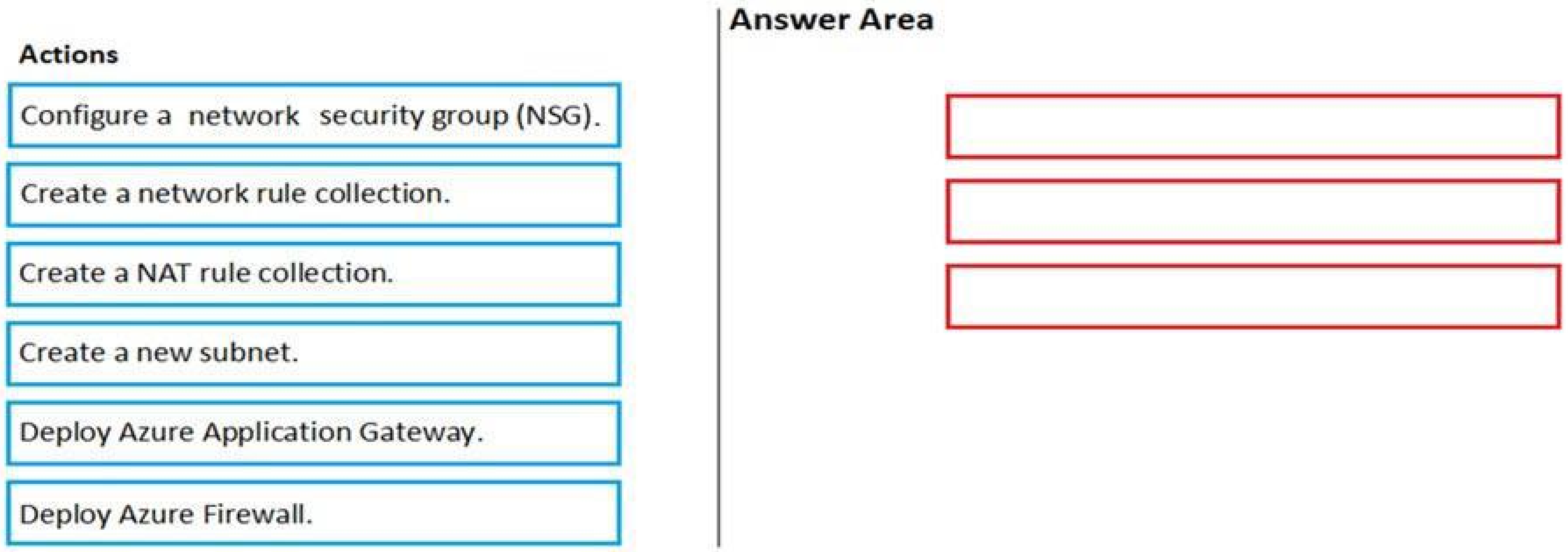
Answer Area

1. Create a JSON file.
2. Run the New-AzureRmRoleDefinition cmdlet.
3. Run the New-AzureRmRoleAssignment cmdlet.

**Section:**
**Explanation:**
References:
https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure

**QUESTION 26**
DRAG DROP
You have an Azure subscription that contains the following resources:
A virtual network named VNET1 that contains two subnets named Subnet1 and Subnet2.
A virtual machine named VM1 that has only a private IP address and connects to Subnet1.
You need to ensure that Remote Desktop connections can be established to VM1 from the internet.
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:**

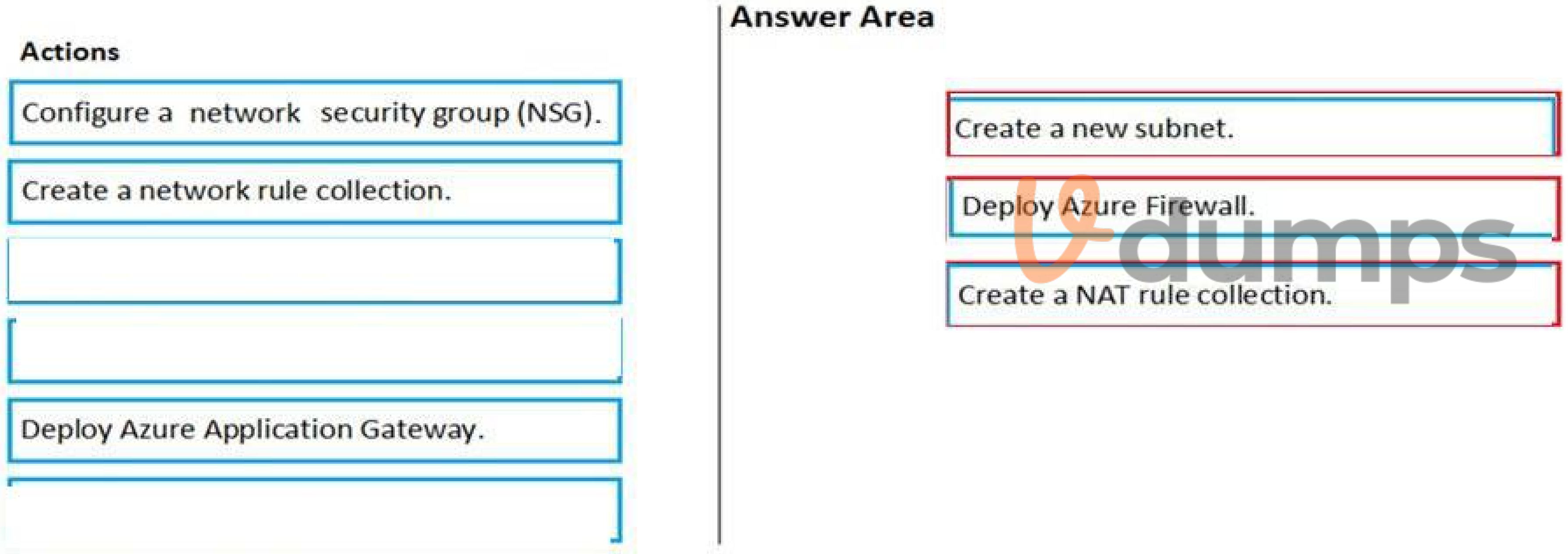


**Actions**

- Configure a network security group (NSG).
- Create a network rule collection.
- Create a NAT rule collection.
- Create a new subnet.
- Deploy Azure Application Gateway.
- Deploy Azure Firewall.

**Answer Area**

**Correct Answer:**



**Actions**

- Configure a network security group (NSG).
- Create a network rule collection.
- Deploy Azure Application Gateway.

**Answer Area**

- Create a new subnet.
- Deploy Azure Firewall.
- Create a NAT rule collection.

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

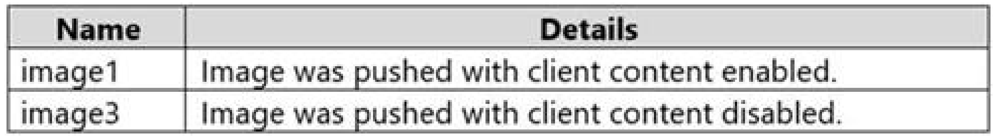
**QUESTION 27**
You have an Azure subscription that contains a user named User1 and an Azure Container Registry named ContReg1.
You enable content trust for ContReg1.
You need to ensure that User1 can create trusted images in ContReg1. The solution must use the principle of least privilege.
Which two roles should you assign to User1? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. AcrQuarantineReader
B. Contributor
C. AcrPush
D. AcrImageSigner

E. AcrQuarantineWriter

**Correct Answer: C, D**
**Section:**
**Explanation:**
References:
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles

**QUESTION 28**
You have an Azure Container Registry named ContReg1 that contains a container image named image1.
You enable content trust for ContReg1.
After content trust is enabled, you push two images to ContReg1 as shown in the following table.



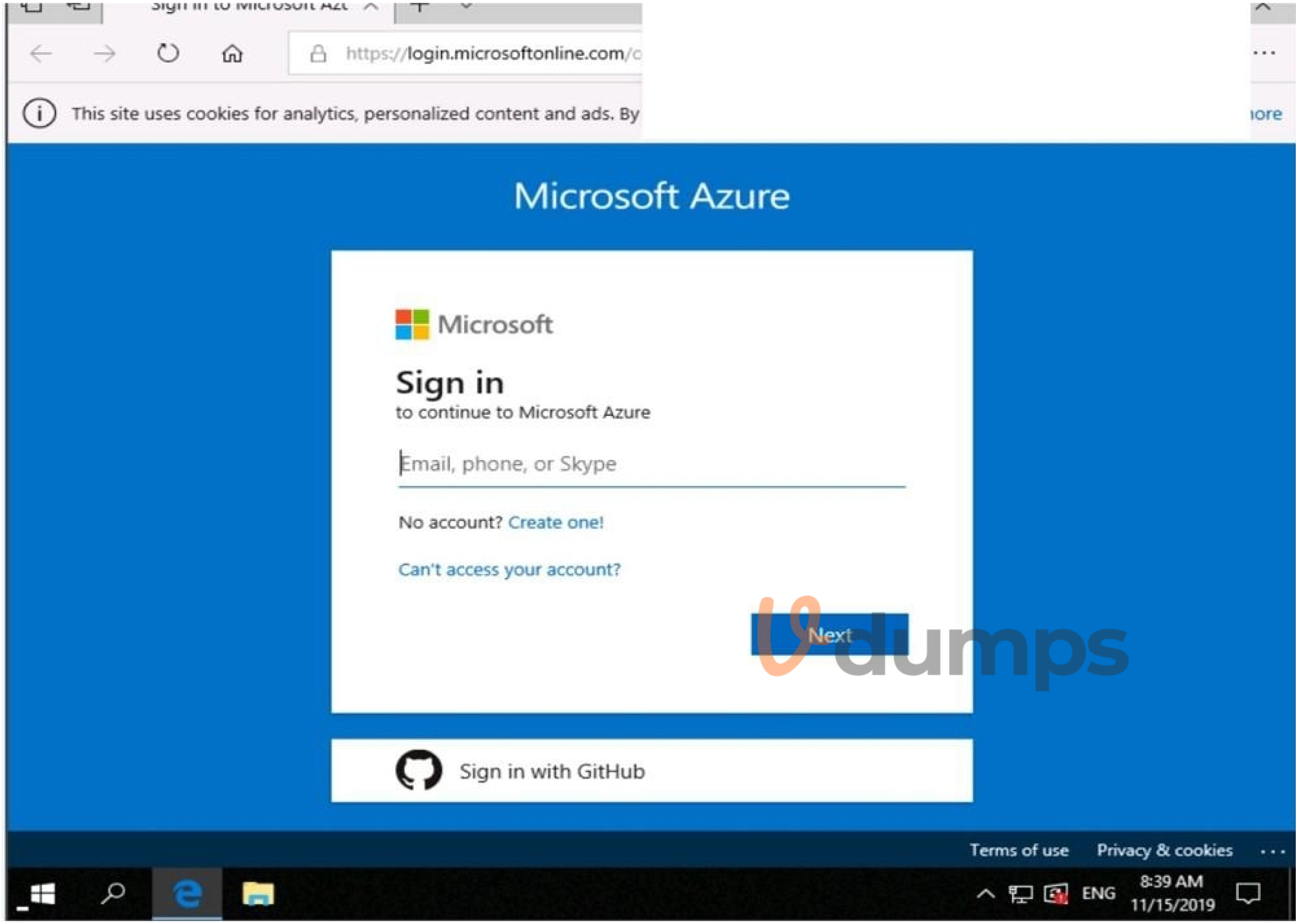
| Name | Details |
|---|---|
| image1 | Image was pushed with client content enabled. |
| image3 | Image was pushed with client content disabled. |

Which images are trusted images?

A. image1 and image2 only
B. image2 only
C. image1, image2, and image3

**Correct Answer: B**
**Section:**
**Explanation:**
Azure Container Registry implements Docker's content trust model, enabling pushing and pulling of signed images.
To push a trusted image tag to your container registry, enable content trust and push the image with docker push.
To work with trusted images, both image publishers and consumers need to enable content trust for their Docker clients. As a publisher, you can sign the images you push to a content trust-enabled registry.
Reference:
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust

**QUESTION 29**
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: User1-10598168@ExamUsers.com
Azure Password: Ag1Bh9!#Bd
The following information is for technical support purposes only:
Lab Instance: 10598168



https://login.microsoftonline.com/c

This site uses cookies for analytics, personalized content and ads. By

Microsoft Azure

Microsoft

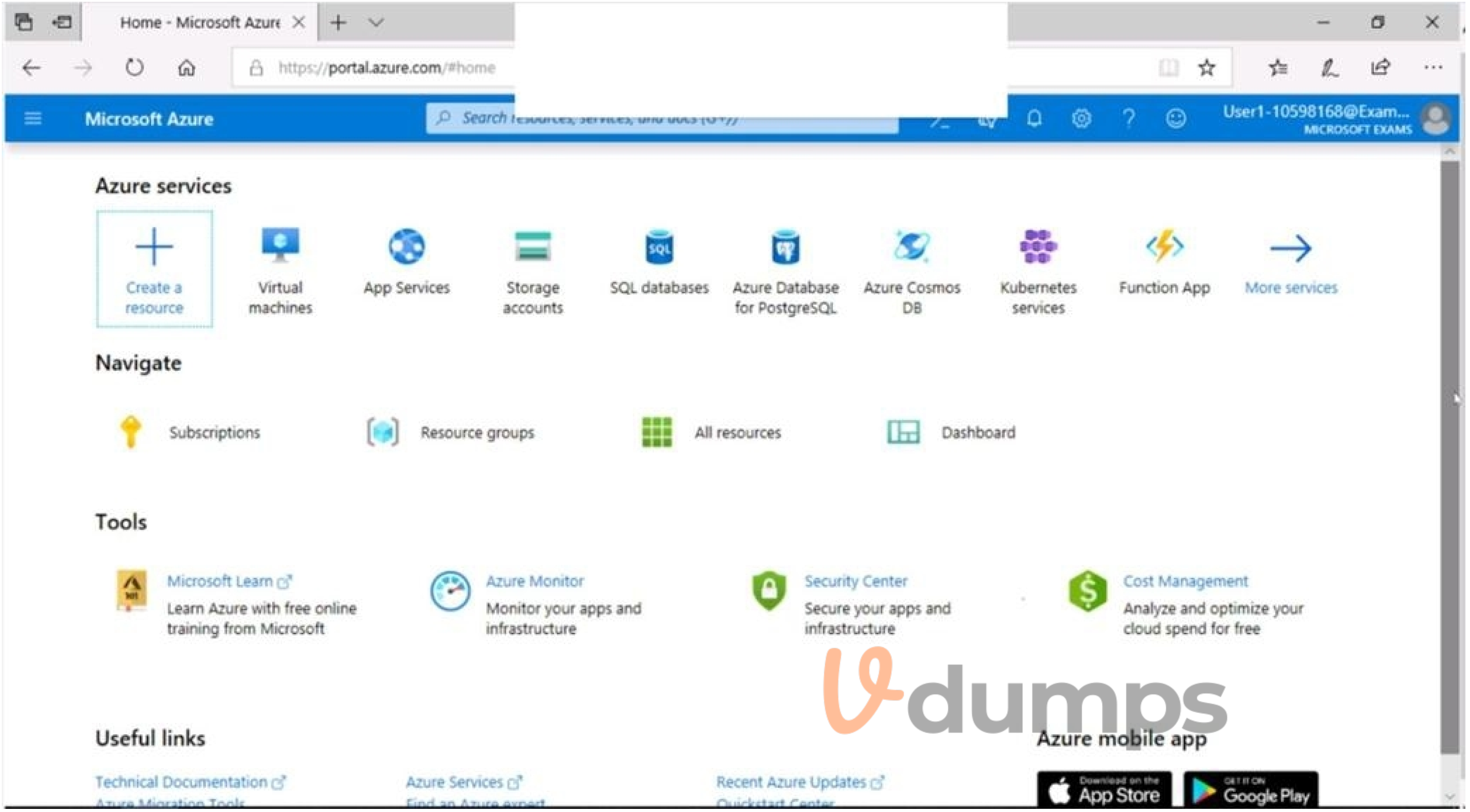
## Sign in

to continue to Microsoft Azure

Email, phone, or Skype

No account? Create one!

Can't access your account?



Home - Microsoft Azure

https://portal.azure.com/#home

Microsoft Azure

Search resources, services, and docs (G+/)

User1-10598168@Exam...
MICROSOFT EXAMS

Azure services

Create a resource | Virtual machines | App Services | Storage accounts | SQL databases | Azure Database for PostgreSQL | Azure Cosmos DB | Kubernetes services | Function App | More services

Navigate

Subscriptions | Resource groups | All resources | Dashboard

Tools

Microsoft Learn
Learn Azure with free online training from Microsoft

Azure Monitor
Monitor your apps and infrastructure

Security Center
Secure your apps and infrastructure

Cost Management
Analyze and optimize your cloud spend for free

Useful links

Technical Documentation
Azure Migration Tools

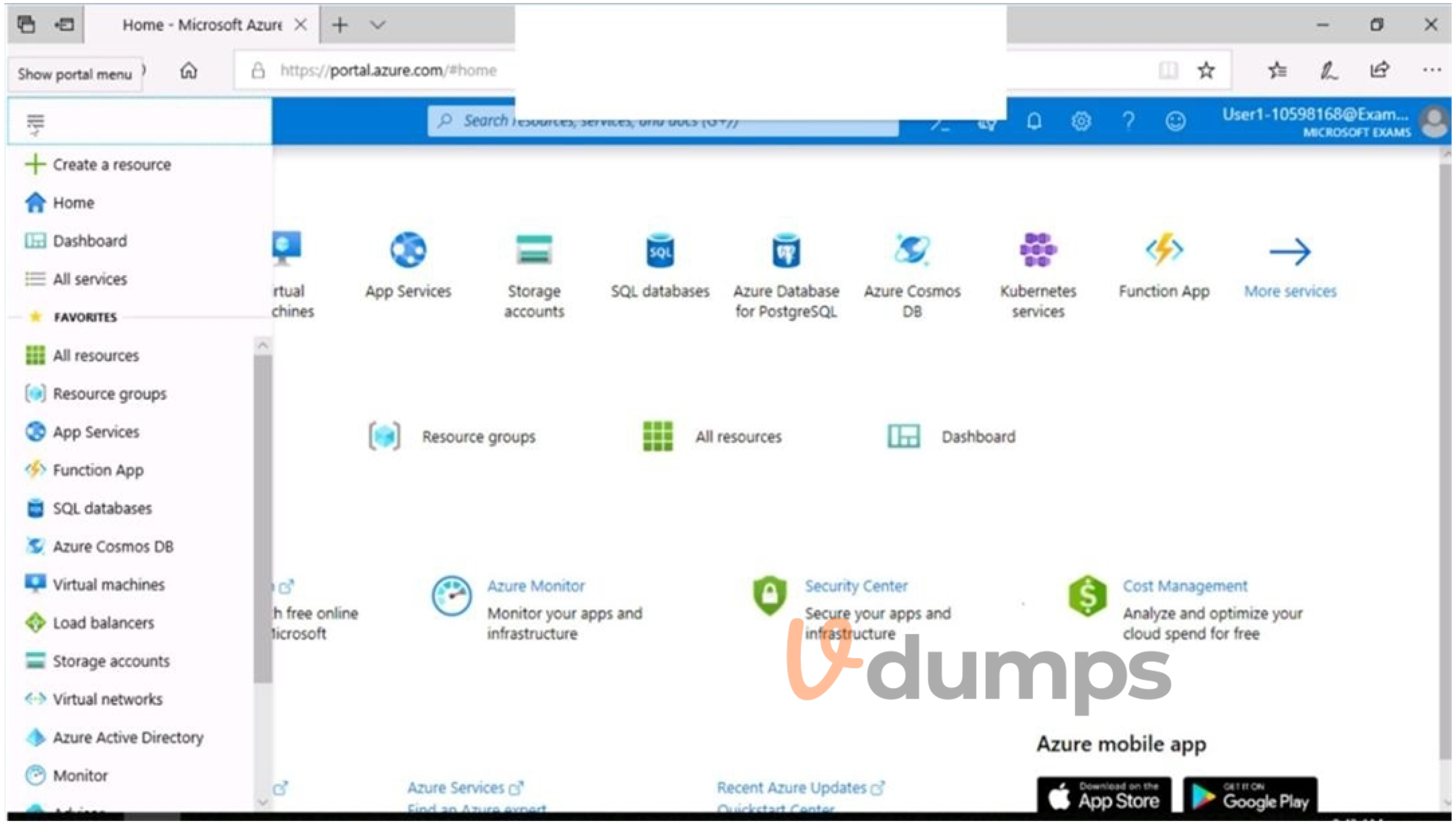
Azure Services
Find an Azure expert

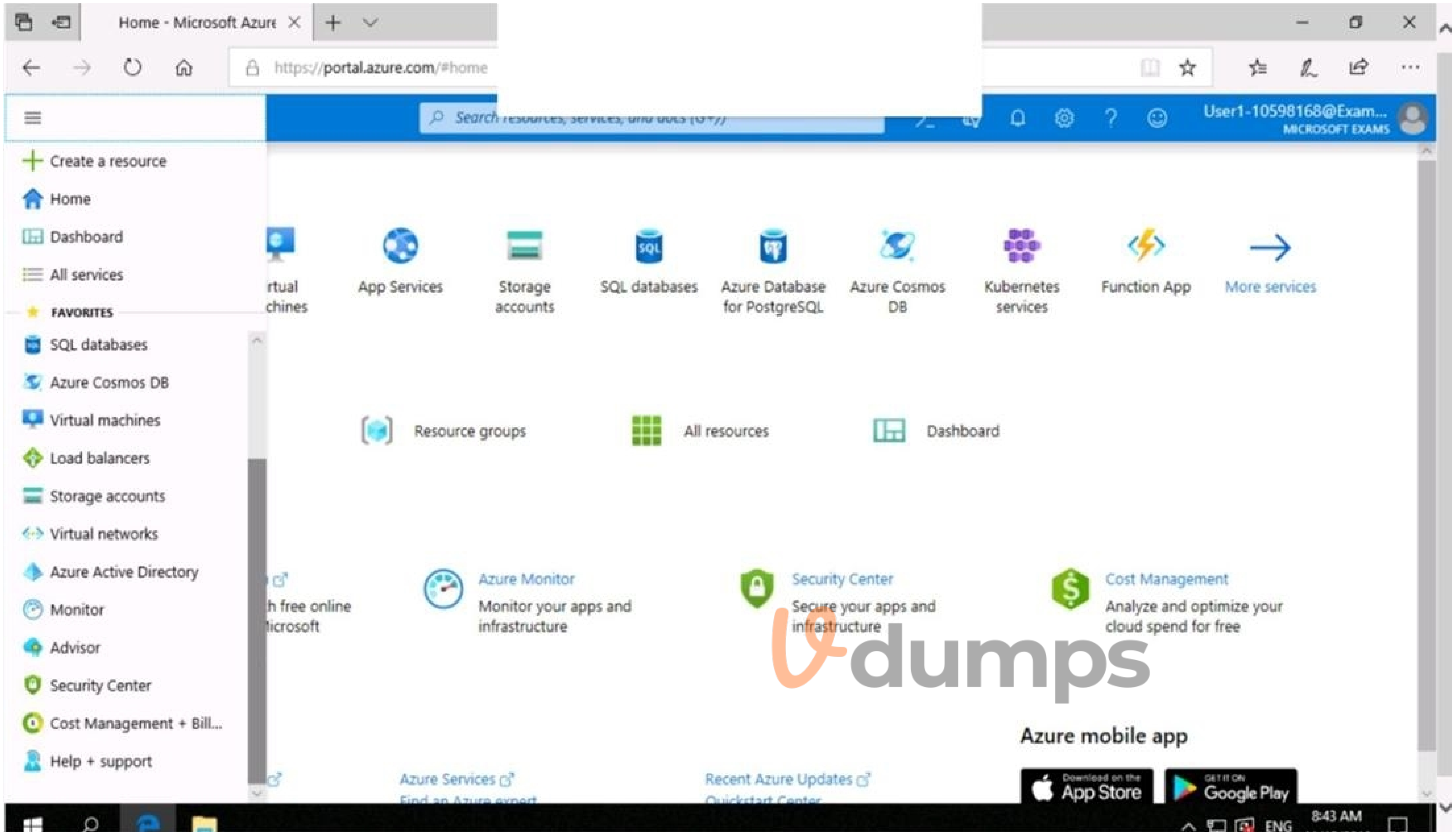
Recent Azure Updates
Quickstart Center

Azure mobile app

Download on the App Store

GET IT ON Google Play


Home - Microsoft Azure
Show portal menu
https://portal.azure.com/#home
Search resources, services, and docs (G+/)
User1-10598168@Exam...
MICROSOFT EXAMS
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
rtual chines
App Services
Storage accounts
SQL databases
Azure Database for PostgreSQL
Azure Cosmos DB
Kubernetes services
Function App
More services
Resource groups
All resources
Dashboard
h free online
licrosoft
Azure Monitor
Monitor your apps and infrastructure
Security Center
Secure your apps and infrastructure
Cost Management
Analyze and optimize your cloud spend for free
Azure mobile app
Azure Services
Find an Azure expert
Recent Azure Updates
Quickstart Center
App Store
Google Play



You need to configure Azure to allow RDP connections from the Internet to a virtual machine named VM1. The solution must minimize the attack surface of VM1.
To complete this task, sign in to the Azure portal.

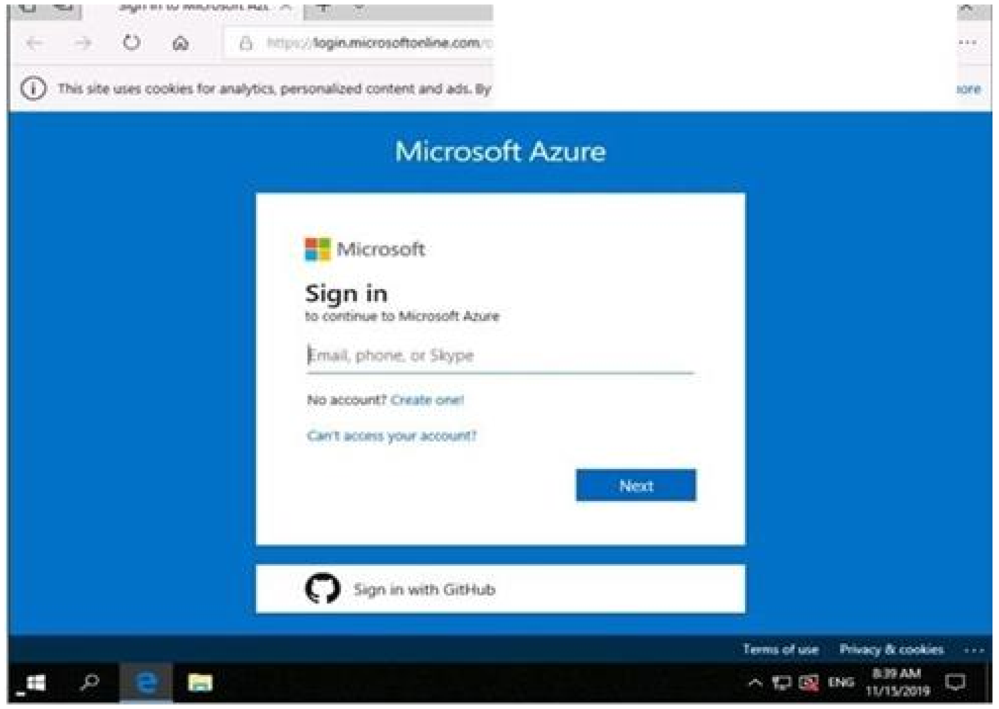
A.

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
To enable the RDP port in an NSG, follow these steps:
1. Sign in to the Azure portal.
2. In Virtual Machines, select VM1
3. In Settings, select Networking.
4. In Inbound port rules, check whether the port for RDP is set correctly. The following is an example of the configuration:
Priority: 300
Name: Port_3389
Port(Destination): 3389

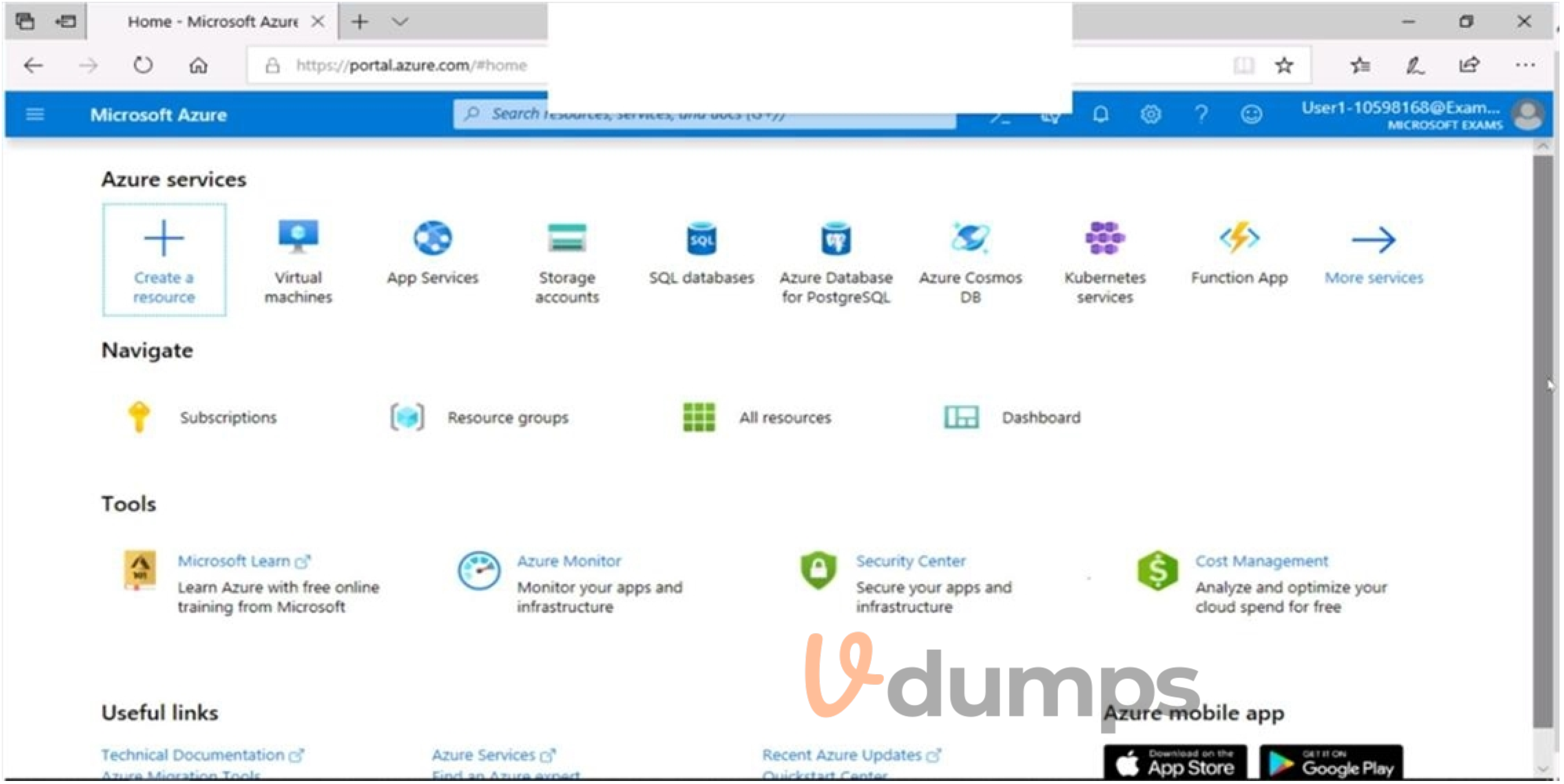
Protocol: TCP
Source: Any
Destinations: Any
Action: Allow
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-nsg-problem

**QUESTION 30**

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: User1-10598168@ExamUsers.com
Azure Password: Ag1Bh9!#Bd
The following information is for technical support purposes only:
Lab Instance: 10598168



This site uses cookies for analytics, personalized content and ads. By

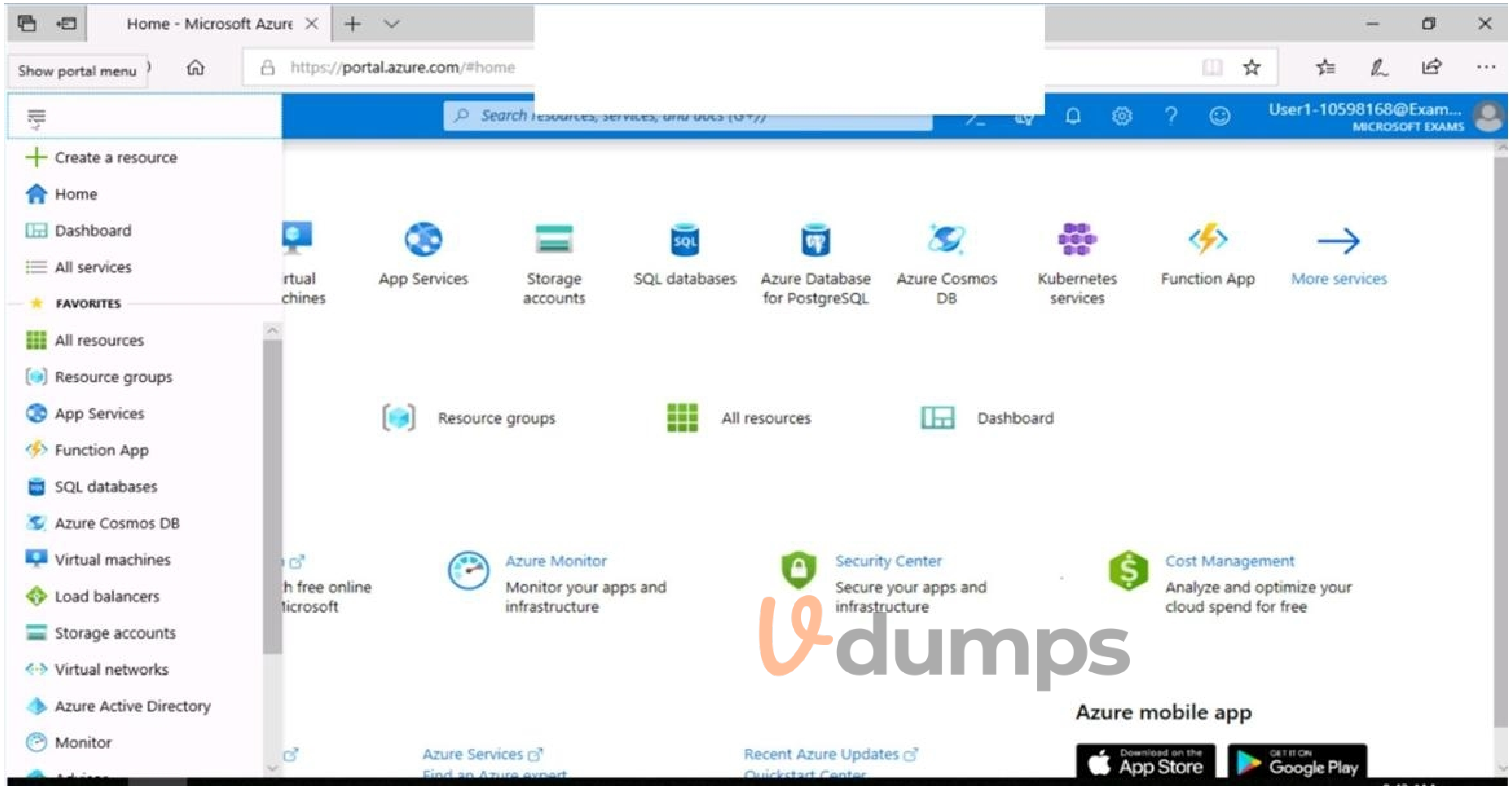


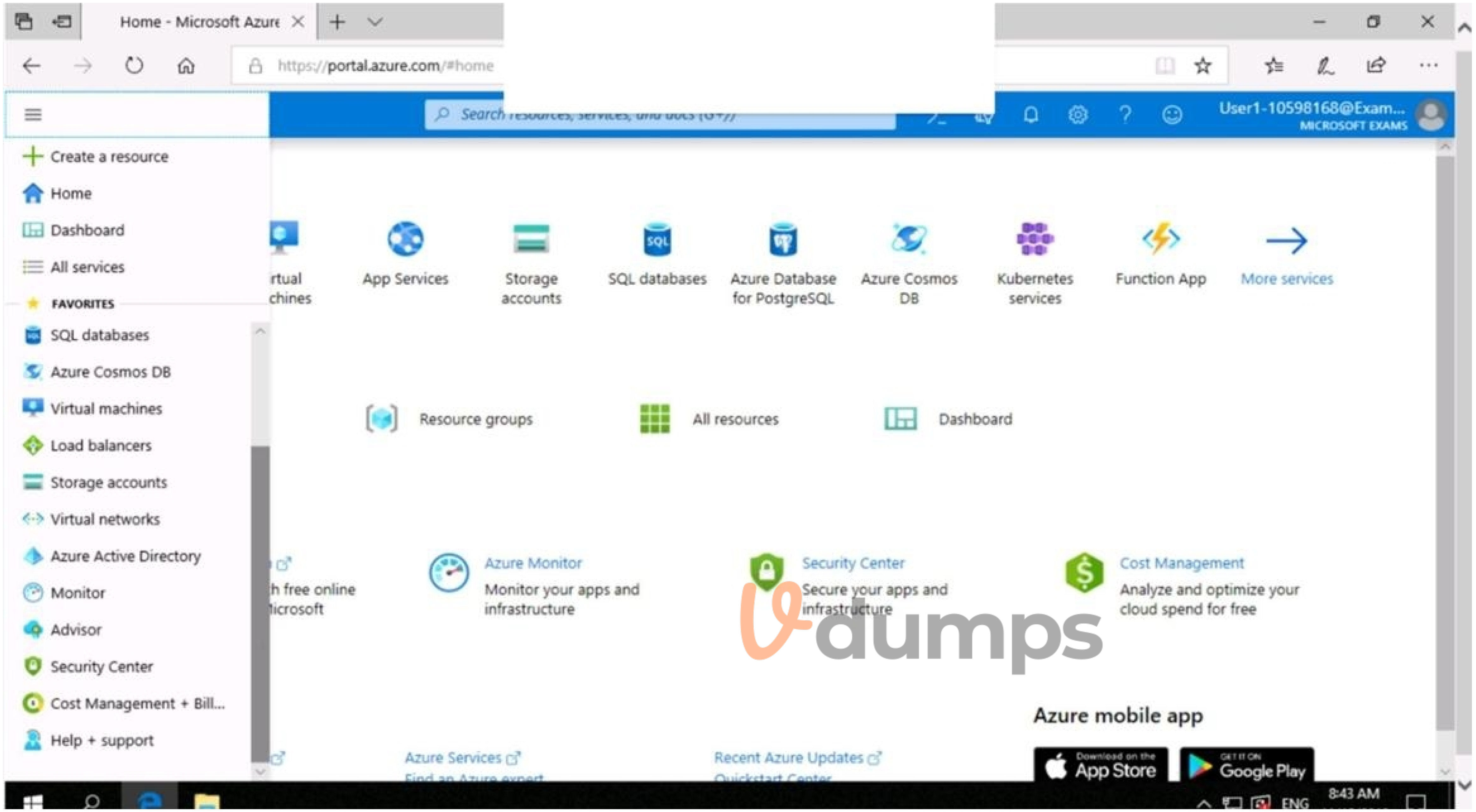
Learn Azure with free online training from Microsoft

Monitor your apps and infrastructure

Secure your apps and infrastructure

Analyze and optimize your cloud spend for free


Home - Microsoft Azure
Show portal menu
https://portal.azure.com/#home
Search resources, services, and docs (G+/)
User1-10598168@Exam...
MICROSOFT EXAMS
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
rtual chines
App Services
Storage accounts
SQL databases
Azure Database for PostgreSQL
Azure Cosmos DB
Kubernetes services
Function App
More services
Resource groups
All resources
Dashboard
h free online
licrosoft
Azure Monitor
Monitor your apps and infrastructure
Security Center
Secure your apps and infrastructure
Cost Management
Analyze and optimize your cloud spend for free
Azure mobile app
Azure Services
Find an Azure expert
Recent Azure Updates
Quickstart Center
Download on the App Store
GET IT ON Google Play



You need to add the network interface of a virtual machine named VM1 to an application security group named ASG1.
To complete this task, sign in to the Azure portal.

A.

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
1. In the Search resources, services, and docs box at the top of the portal, begin typing the name of a virtual machine, VM1 that has a network interface that you want to add to, or remove from, an application security group.
2. When the name of your VM appears in the search results, select it.
3. Under SETTINGS, select Networking. Select Configure the application security groups, select the application security groups that you want to add the network interface to, or unselect the application security groups that you want to remove the network interface from, and then select Save.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface

**QUESTION 31**

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.

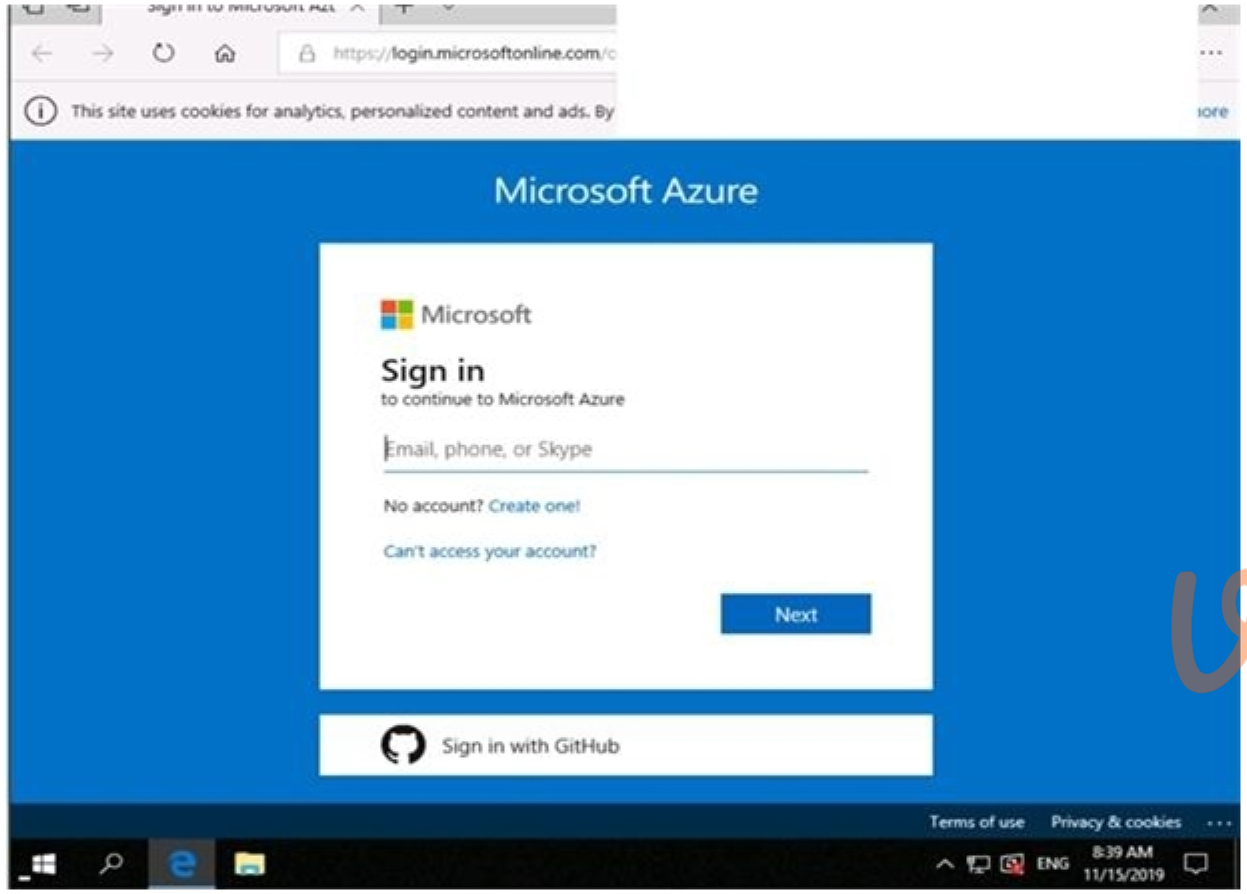
To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168



https://login.microsoftonline.com/c

This site uses cookies for analytics, personalized content and ads. By

Microsoft Azure

Microsoft

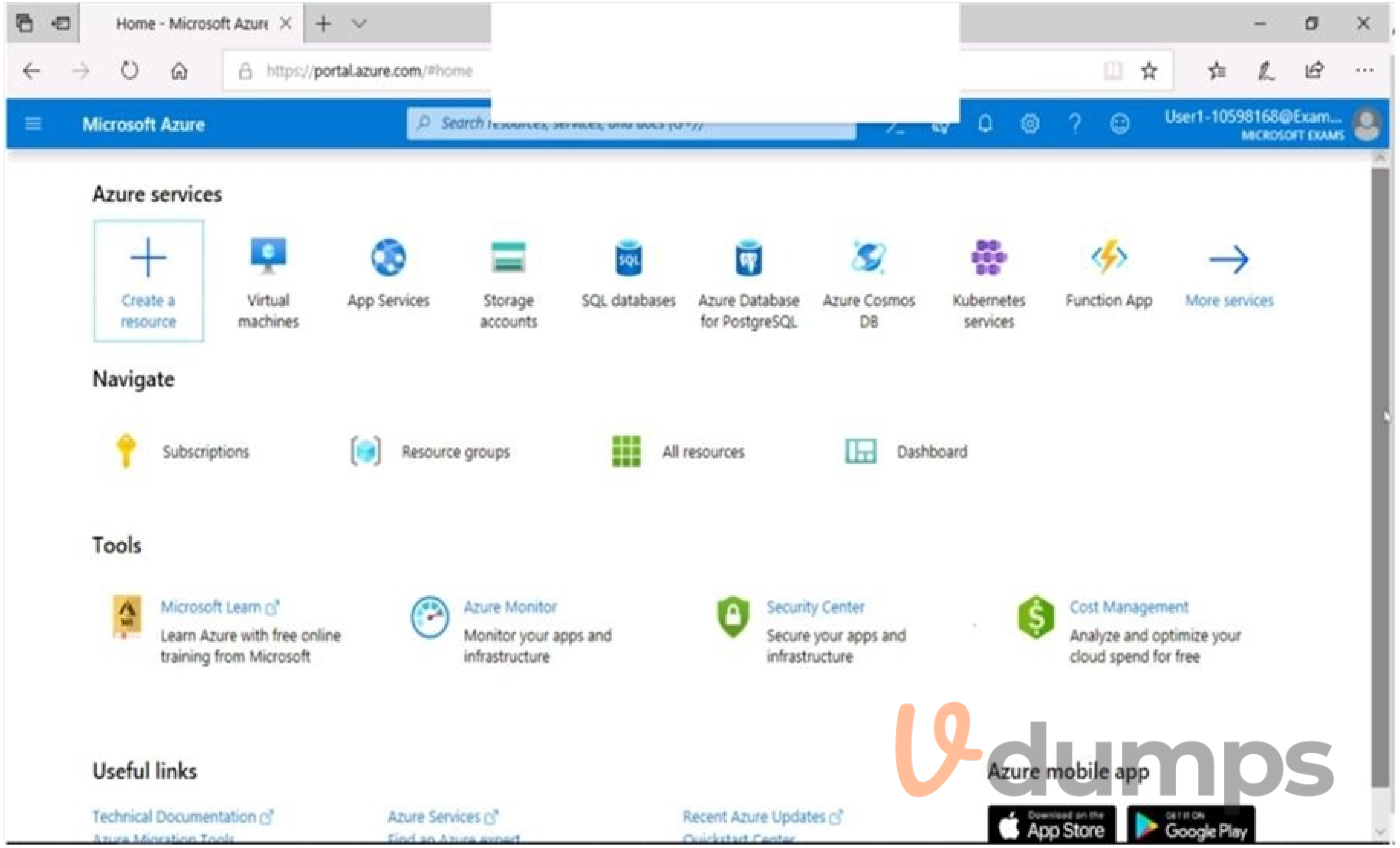
Sign in

to continue to Microsoft Azure

Email, phone, or Skype

No account? Create one!

Can't access your account?



Azure services

Navigate

Tools

Microsoft Learn
Learn Azure with free online training from Microsoft

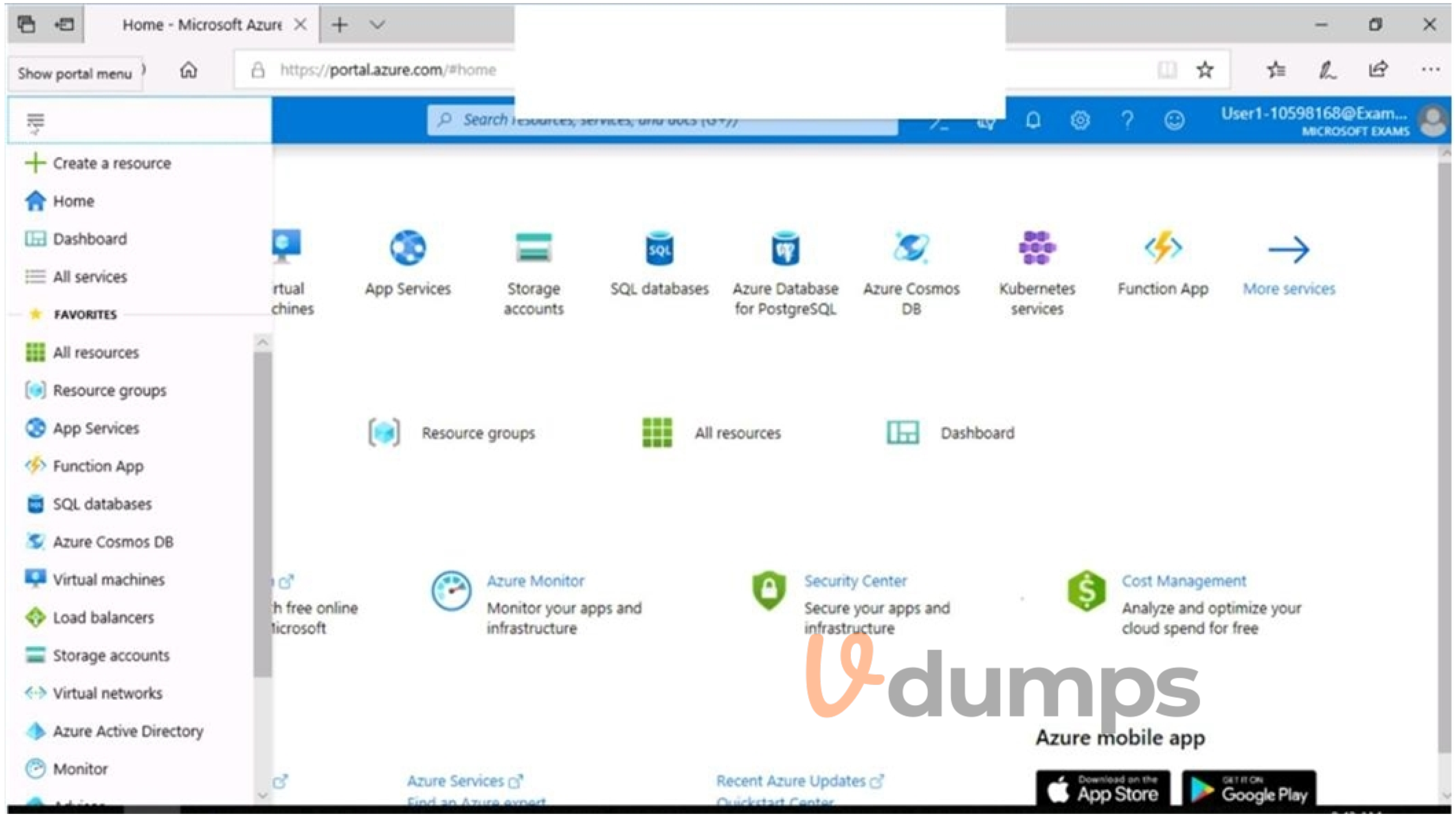
Azure Monitor
Monitor your apps and infrastructure

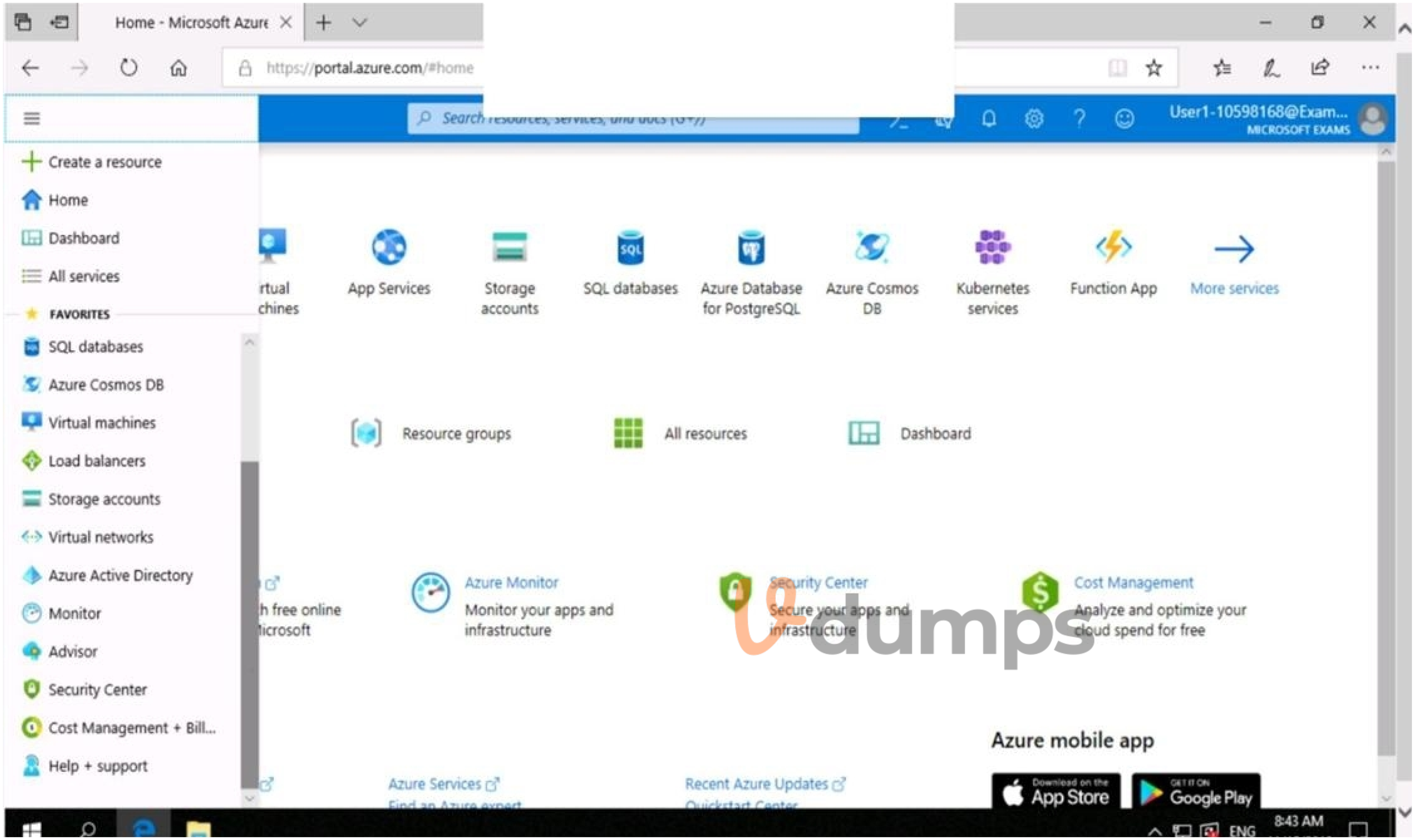
Security Center
Secure your apps and infrastructure

Cost Management
Analyze and optimize your cloud spend for free

Useful links

Azure mobile app

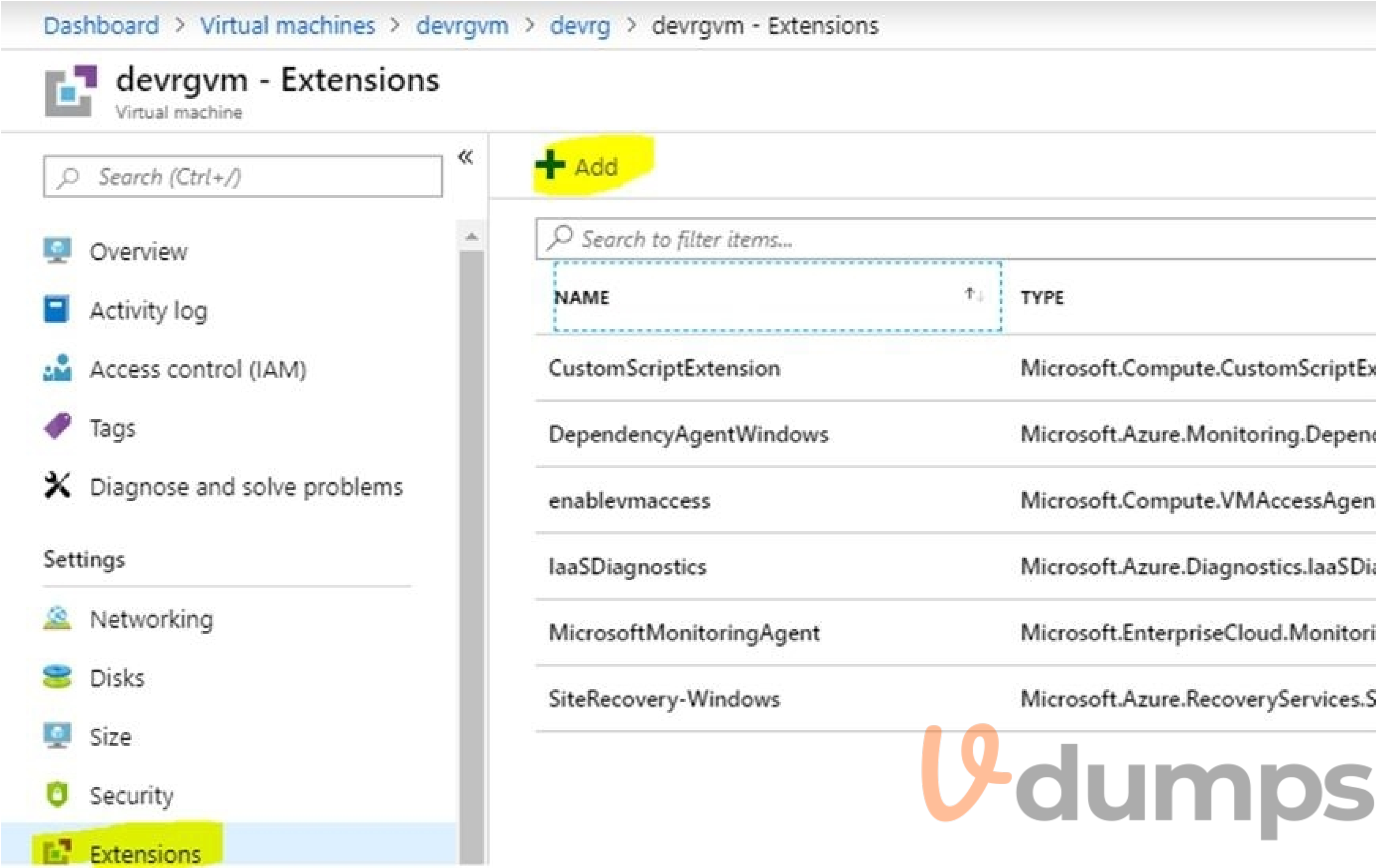

Home - Microsoft Azure
Show portal menu
https://portal.azure.com/#home
Search resources, services, and docs (G+/)
User1-10598168@Exam...
MICROSOFT EXAMS
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
rtual chines
App Services
Storage accounts
SQL databases
Azure Database for PostgreSQL
Azure Cosmos DB
Kubernetes services
Function App
More services
Resource groups
All resources
Dashboard
h free online
licrosoft
Azure Monitor
Monitor your apps and infrastructure
Security Center
Secure your apps and infrastructure
Cost Management
Analyze and optimize your cloud spend for free
Azure mobile app
Azure Services
Find an Azure expert
Recent Azure Updates
Quickstart Center
App Store
Google Play



You need to perform a full malware scan every Sunday at 02:00 on a virtual machine named VM1 by using Microsoft Antimalware for Virtual Machines.
To complete this task, sign in to the Azure portal.

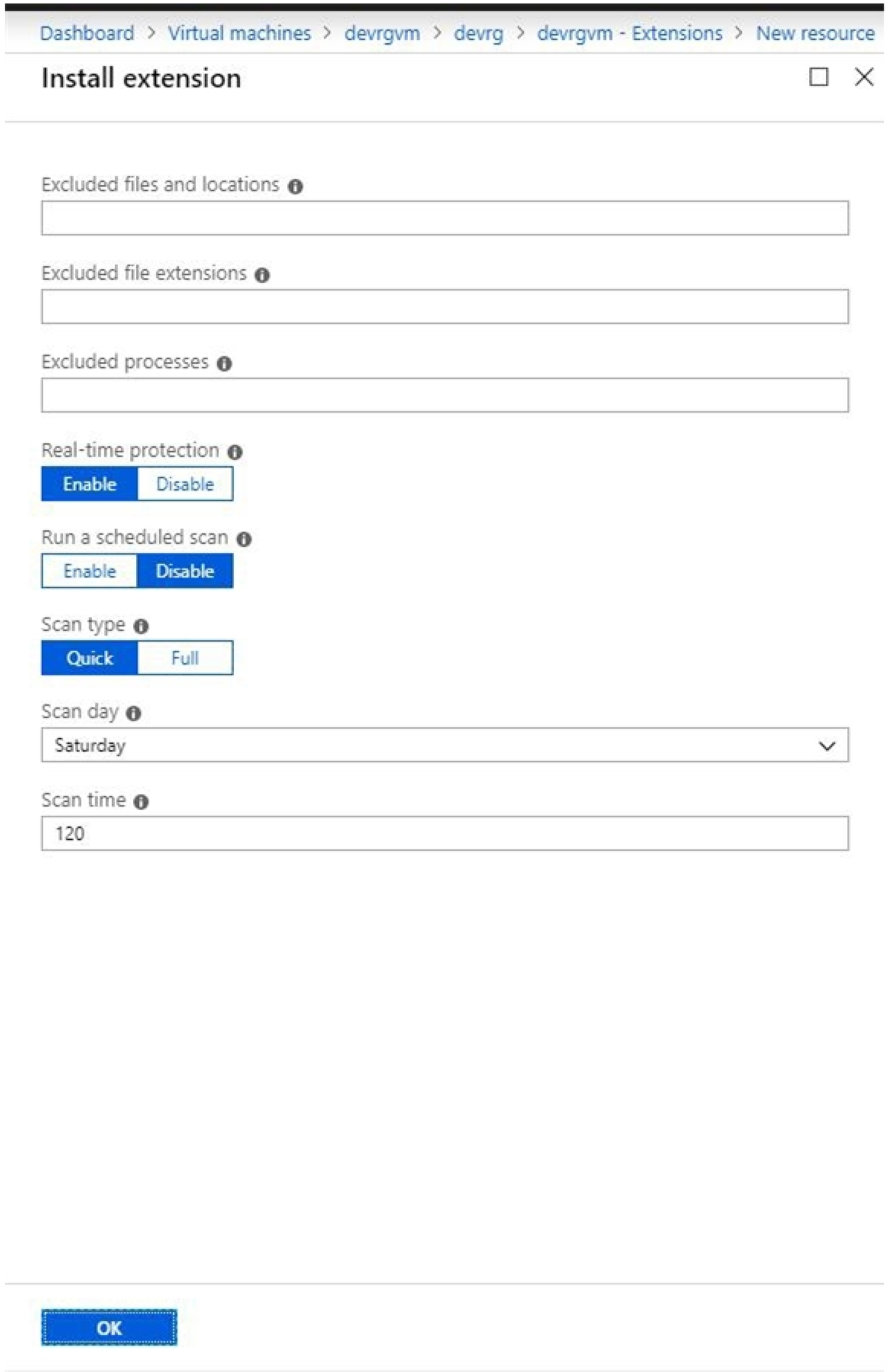
A.

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
Deploy the Microsoft Antimalware Extension using the Azure Portal for single VM deployment
1. In Azure Portal, go to the Azure VM1’s blade, navigate to the Extensions section and press Add.



| NAME | TYPE |
|---|---|
| CustomScriptExtension | Microsoft.Compute.CustomScriptEx |
| DependencyAgentWindows | Microsoft.Azure.Monitoring.Depen |
| enablevmaccess | Microsoft.Compute.VMAccessAgen |
| IaaSDiagnostics | Microsoft.Azure.Diagnostics.IaaSDi |
| MicrosoftMonitoringAgent | Microsoft.EnterpriseCloud.Monitori |
| SiteRecovery-Windows | Microsoft.Azure.RecoveryServices.S |

2. Select the Microsoft Antimalware extension and press Create.
3. Fill the “Install extension” form as desired and press OK.
Scheduled: Enable
Scan type: Full
Scan day: Sunday



Dashboard > Virtual machines > devrgvm > devrg > devrgvm - Extensions > New resource

Install extension

Excluded files and locations

Excluded file extensions

Excluded processes

Real-time protection: [✓ Enable] Disable

Run a scheduled scan: Enable [✓ Disable]

Scan type: [✓ Quick] Full

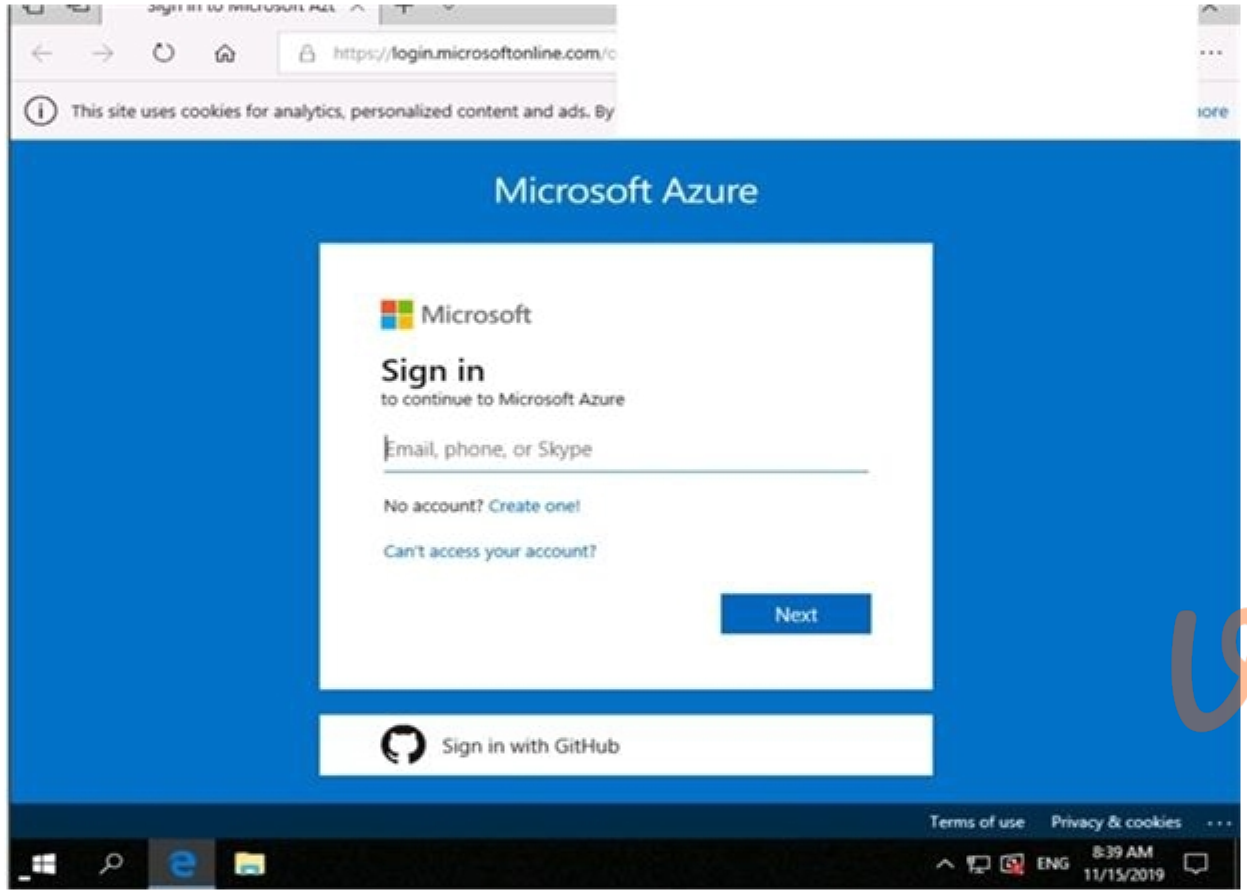
Scan day: Saturday

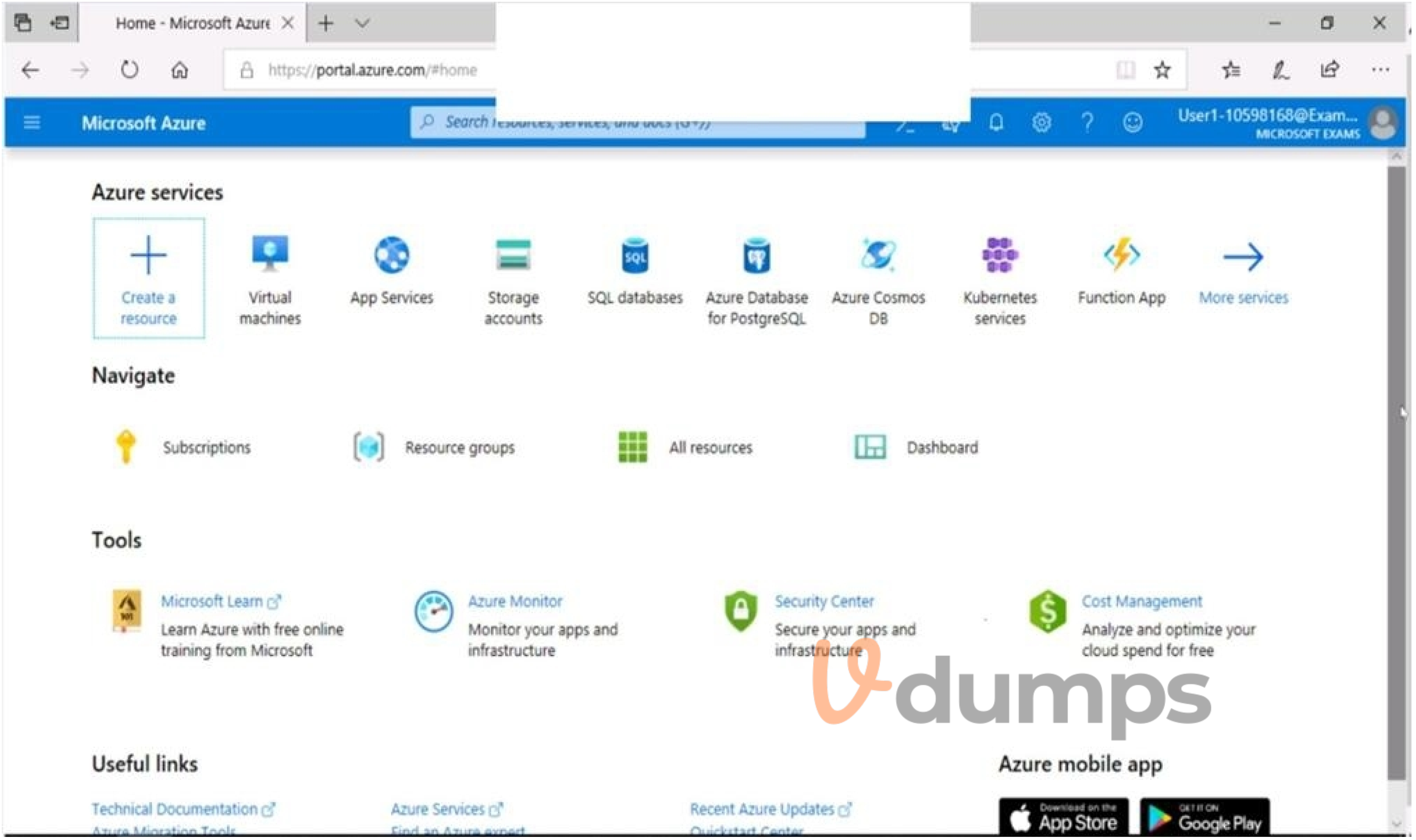
Scan time: 120

Reference:
https://www.e-apostolidis.gr/microsoft/azure/azure-vm-antimalware-extension-management/

**QUESTION 32**

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: User1-10598168@ExamUsers.com
Azure Password: Ag1Bh9!#Bd
The following information is for technical support purposes only:
Lab Instance: 10598168


https://login.microsoftonline.com/c
This site uses cookies for analytics, personalized content and ads. By
Microsoft Azure
Microsoft
Sign in
to continue to Microsoft Azure
Email, phone, or Skype
No account? Create one!
Can't access your account?
Next
Sign in with GitHub
Terms of use
Privacy & cookies
ENG
8:39 AM
11/15/2019

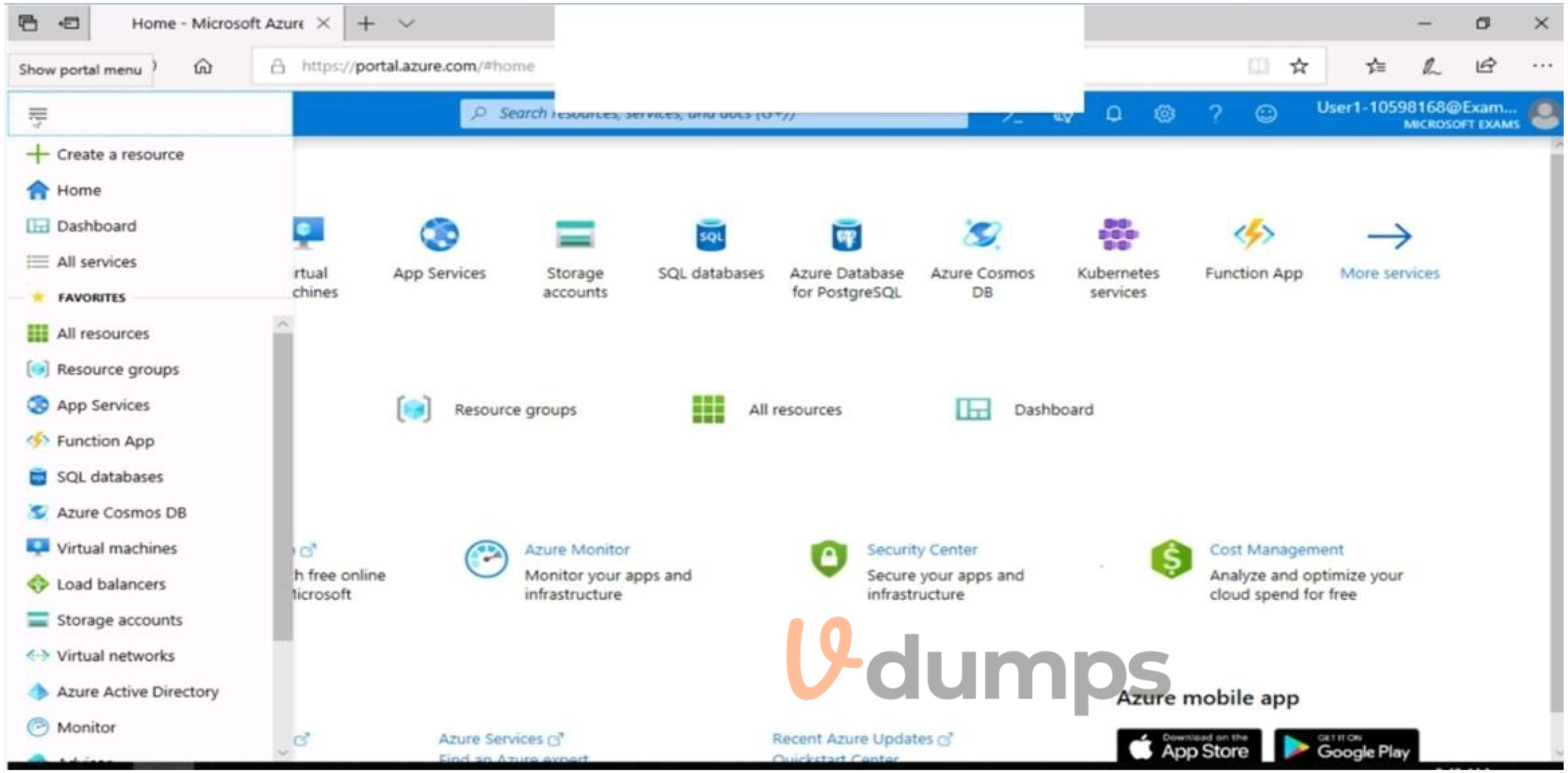


Learn Azure with free online training from Microsoft

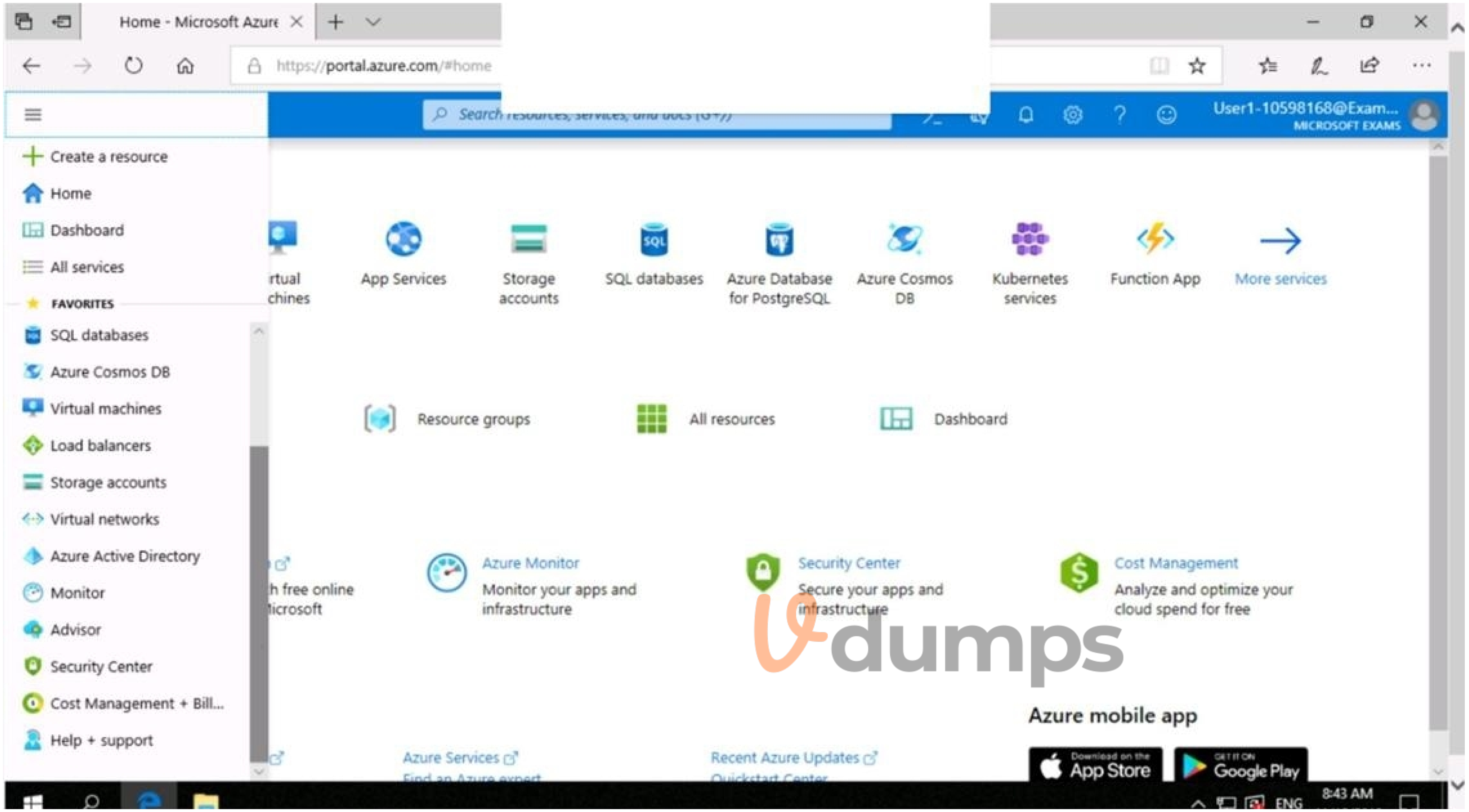
Monitor your apps and infrastructure

Secure your apps and infrastructure

Analyze and optimize your cloud spend for free



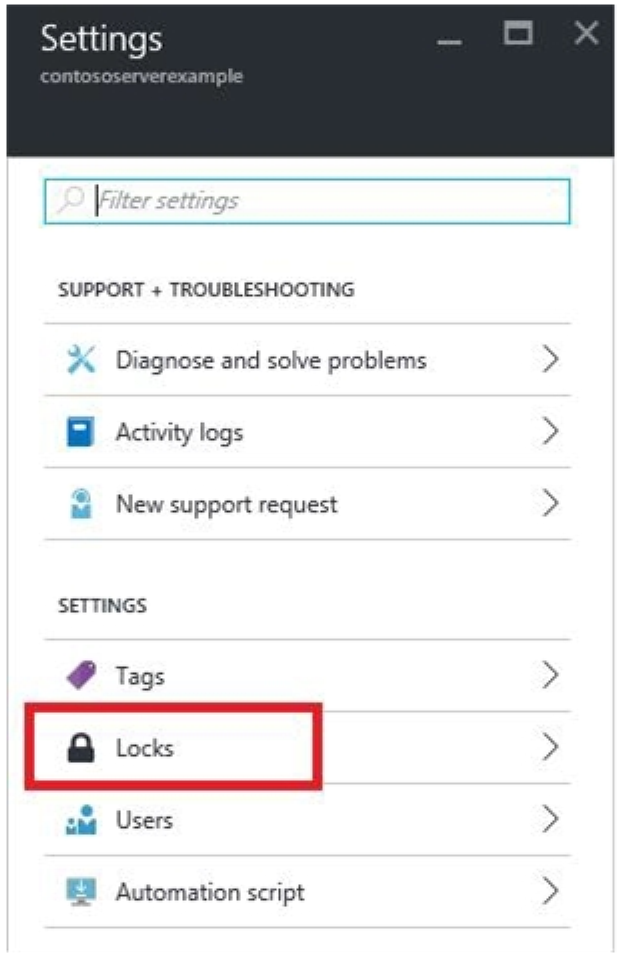
Home - Microsoft Azure
Show portal menu
https://portal.azure.com/#home
Search resources, services, and docs (G+/)
User1-10598168@Exam...
MICROSOFT EXAMS
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
rtual chines
App Services
Storage accounts
SQL databases
Azure Database for PostgreSQL
Azure Cosmos DB
Kubernetes services
Function App
More services
Resource groups
All resources
Dashboard
h free online
licrosoft
Azure Monitor
Monitor your apps and infrastructure
Security Center
Secure your apps and infrastructure
Cost Management
Analyze and optimize your cloud spend for free
Azure mobile app
Azure Services
Find an Azure expert
Recent Azure Updates
Quickstart Center
App Store
Google Play



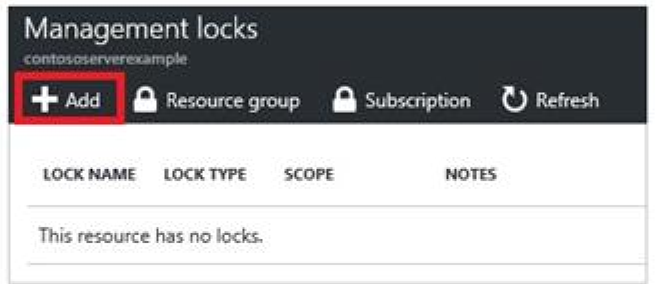
You need to prevent administrative users from accidentally deleting a virtual network named VNET1. The administrative users must be allowed to modify the settings of VNET1.
To complete this task, sign in to the Azure portal.

A.

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
Locking prevents other users in your organization from accidentally deleting or modifying critical resources, such as Azure subscription, resource group, or resource.
Note: In Azure, the term resource refers to an entity managed by Azure. For example, virtual machines, virtual networks, and storage accounts are all referred to as Azure resources.
1. In the Settings blade for virtual network VNET, select Locks.



2. To add a lock, select Add.



| LOCK NAME | LOCK TYPE | SCOPE | NOTES |
|---|---|---|---|
| This resource has no locks. | | | |

3. For Lock type select Delete lock, and click OK

Reference:

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

**QUESTION 33**

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.

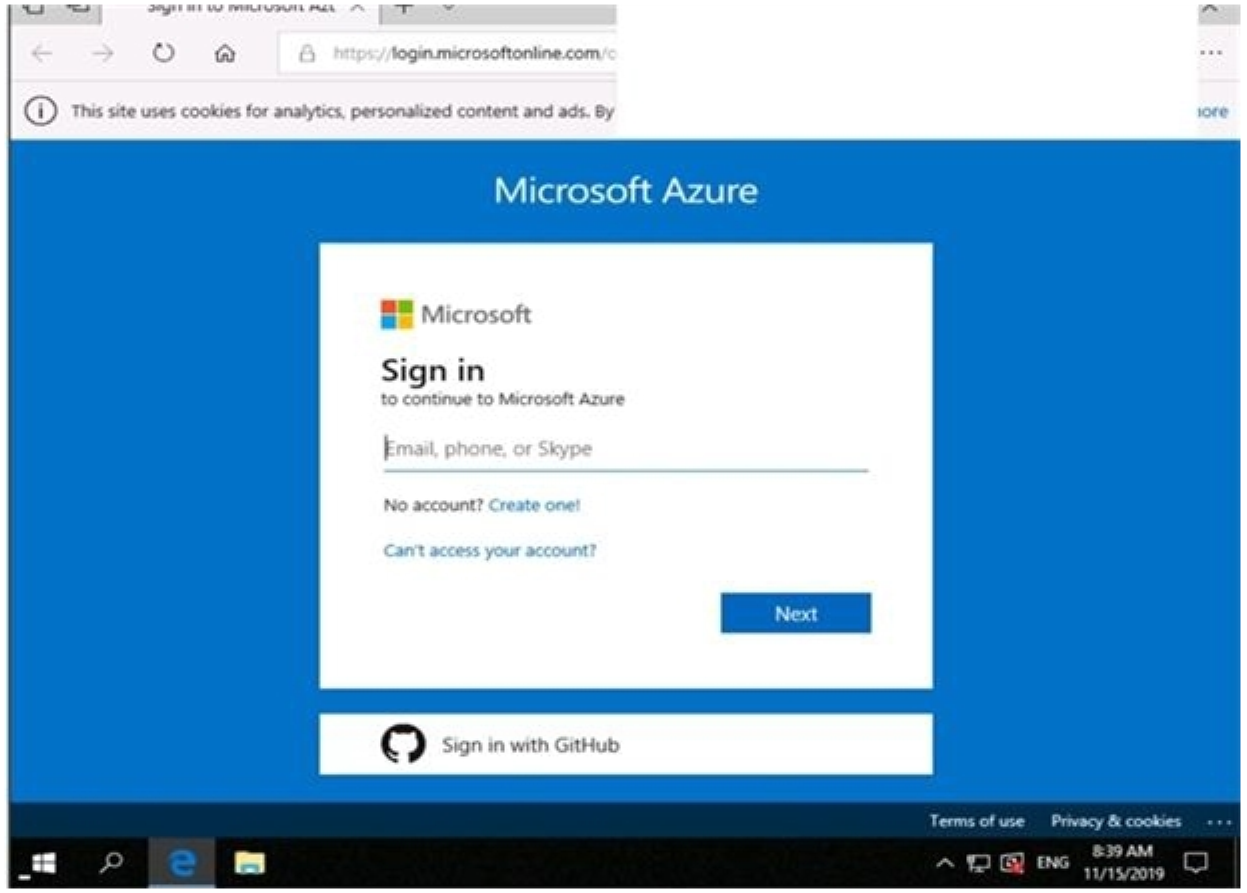
To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User1-10598168@ExamUsers.com

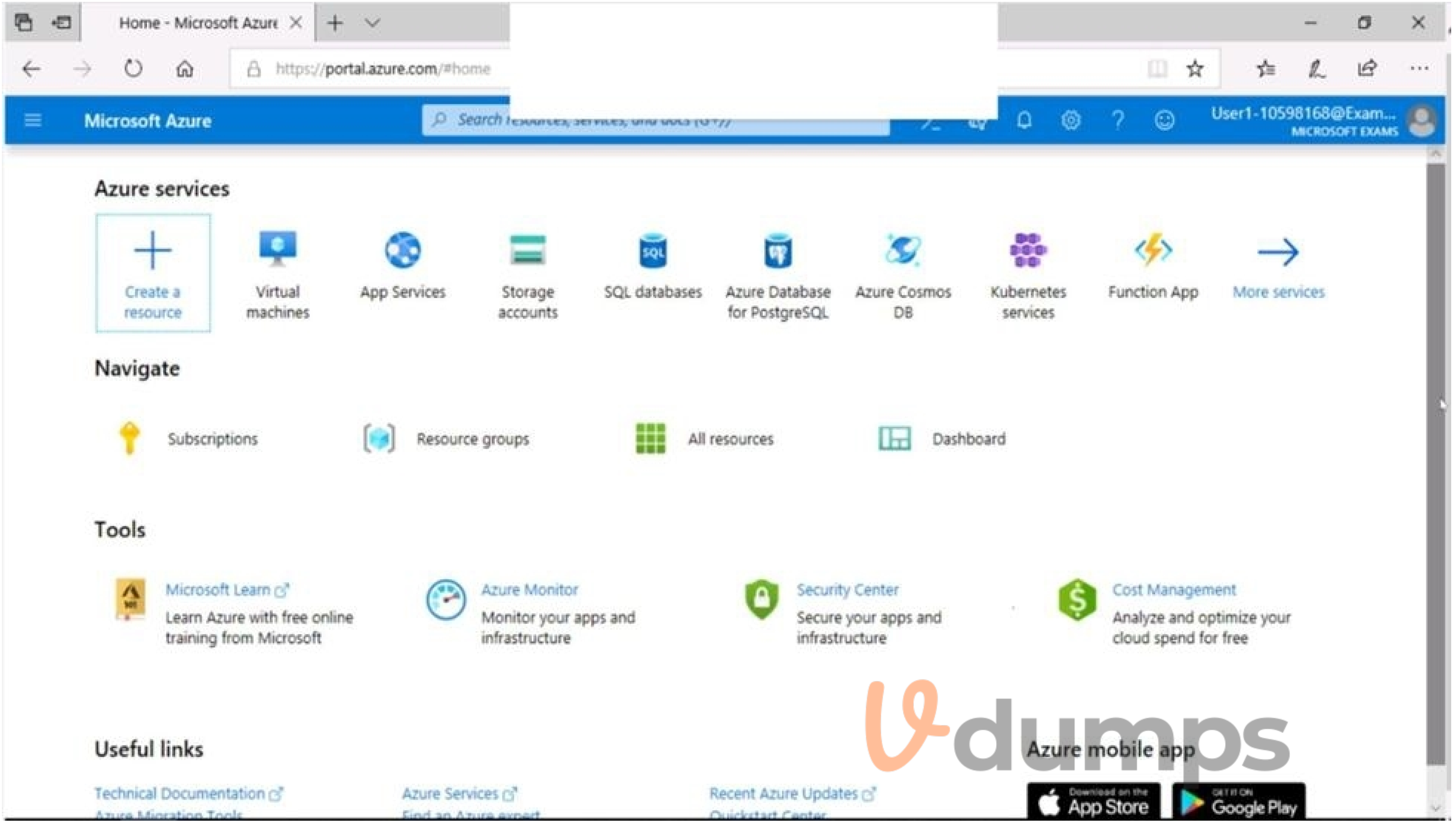
Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

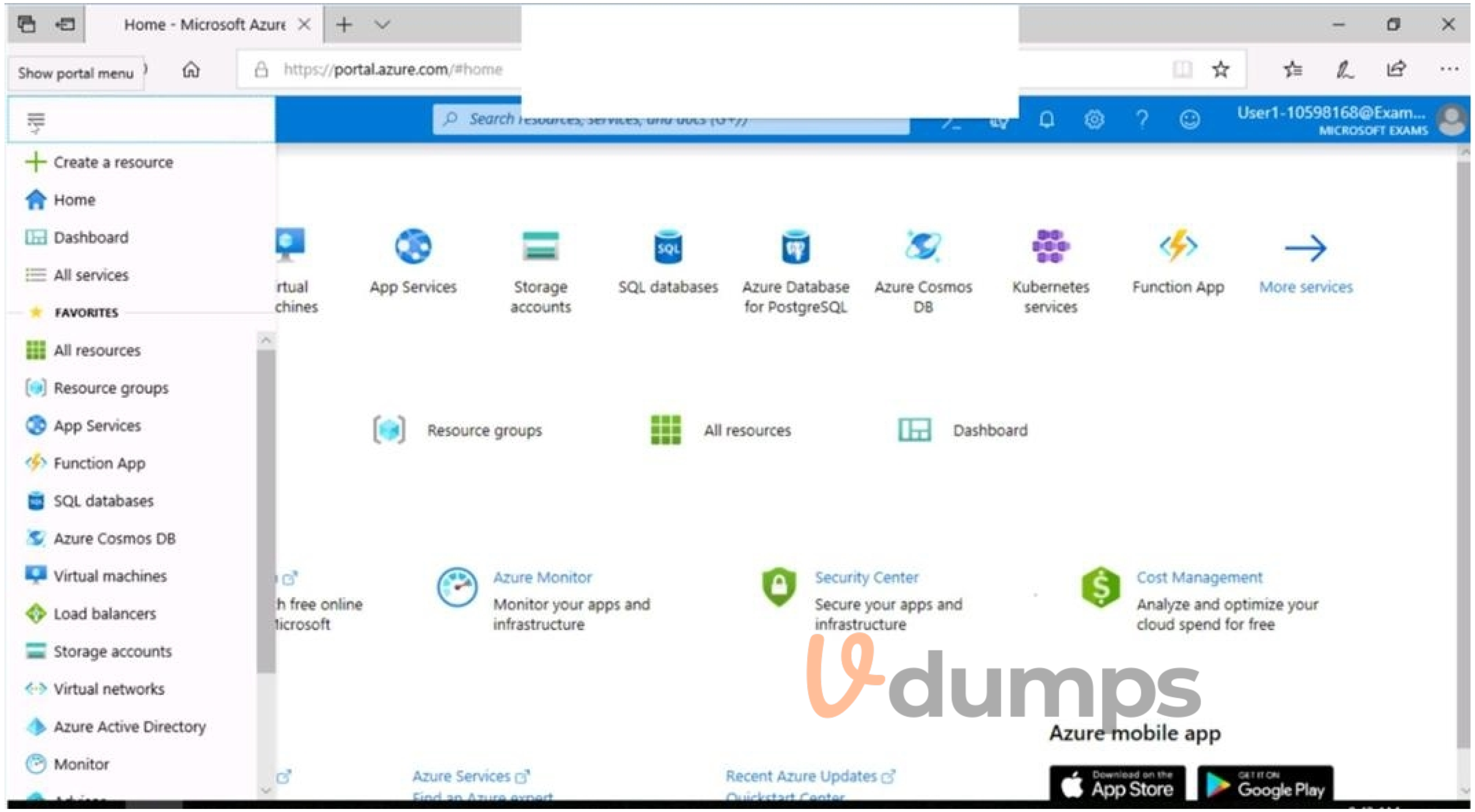
Lab Instance: 10598168

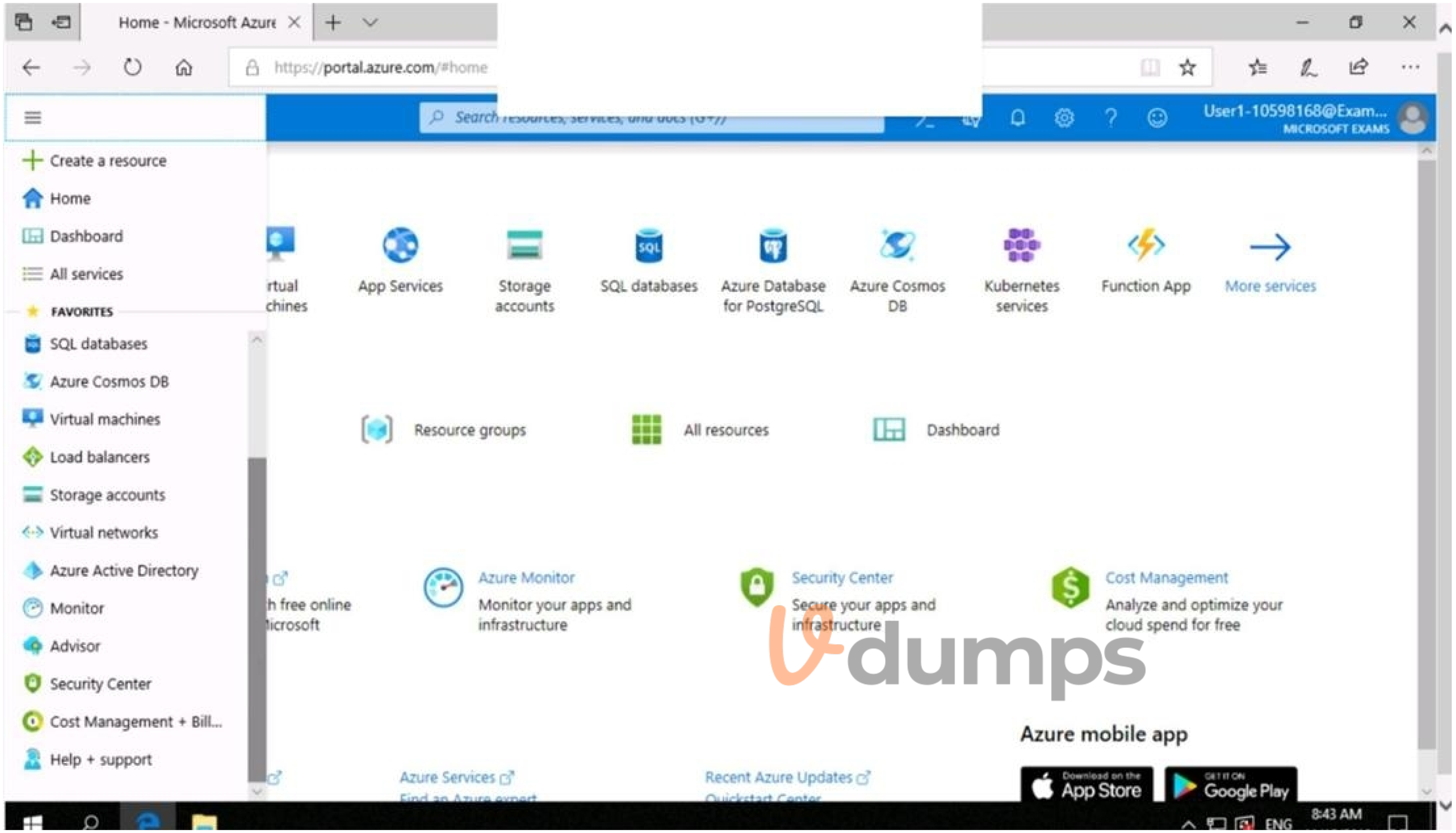


Sign in to Microsoft Azu
https://login.microsoftonline.com/c
This site uses cookies for analytics, personalized content and ads. By
Microsoft Azure
Microsoft
Sign in
to continue to Microsoft Azure
Email, phone, or Skype
No account? Create one!
Can't access your account?
Next
Sign in with GitHub
Terms of use
Privacy & cookies
ENG
8:39 AM
11/15/2019



Home - Microsoft Azure
https://portal.azure.com/#home
Microsoft Azure
Search resources, services, and docs (G+/)
User1-10598168@Exam...
MICROSOFT EXAMS
Azure services
Create a resource
Virtual machines
App Services
Storage accounts
SQL databases
Azure Database for PostgreSQL
Azure Cosmos DB
Kubernetes services
Function App
More services
Navigate
Subscriptions
Resource groups
All resources
Dashboard
Tools
Microsoft Learn
Learn Azure with free online training from Microsoft
Azure Monitor
Monitor your apps and infrastructure
Security Center
Secure your apps and infrastructure
Cost Management
Analyze and optimize your cloud spend for free
Useful links
Technical Documentation
Azure Migration Tools
Azure Services
Find an Azure expert
Recent Azure Updates
Quickstart Center
Azure mobile app
Download on the App Store
GET IT ON Google Play

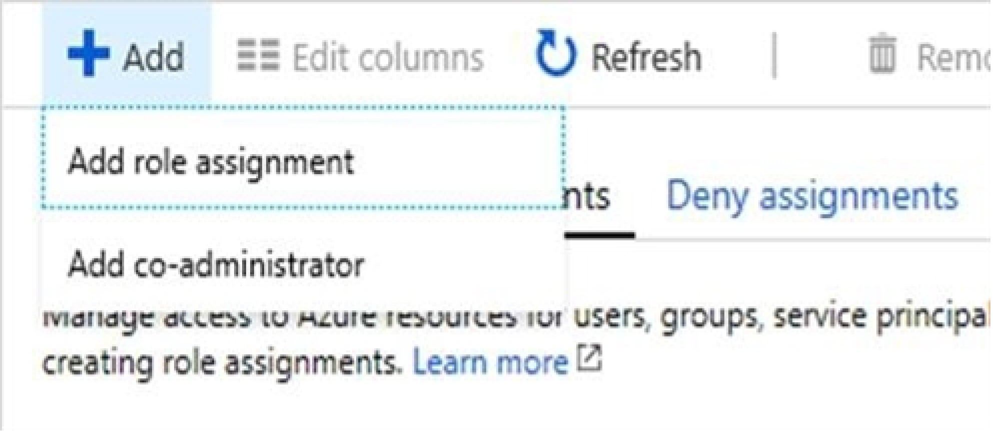

Home - Microsoft Azure
Show portal menu
https://portal.azure.com/#home
Search resources, services, and docs (G+/)
User1-10598168@Exam...
MICROSOFT EXAMS
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
rtual chines
App Services
Storage accounts
SQL databases
Azure Database for PostgreSQL
Azure Cosmos DB
Kubernetes services
Function App
More services
Resource groups
All resources
Dashboard
h free online
licrosoft
Azure Monitor
Monitor your apps and infrastructure
Security Center
Secure your apps and infrastructure
Cost Management
Analyze and optimize your cloud spend for free
Azure mobile app
Azure Services
Find an Azure expert
Recent Azure Updates
Quickstart Center
Download on the App Store
GET IT ON Google Play



You need to ensure that a user named user21059868 can manage the properties of the virtual machines in the RG1lod10598168 resource group. The solution must use the principle of least privilege.
To complete this task, sign in to the Azure portal.

A.

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
1. In Azure portal, locate and select the RG1lod10598168 resource group.
2. Click Access control (IAM).
3. Click the Role assignments tab to view all the role assignments at this scope.
4. Click Add > Add role assignment to open the Add role assignment pane.

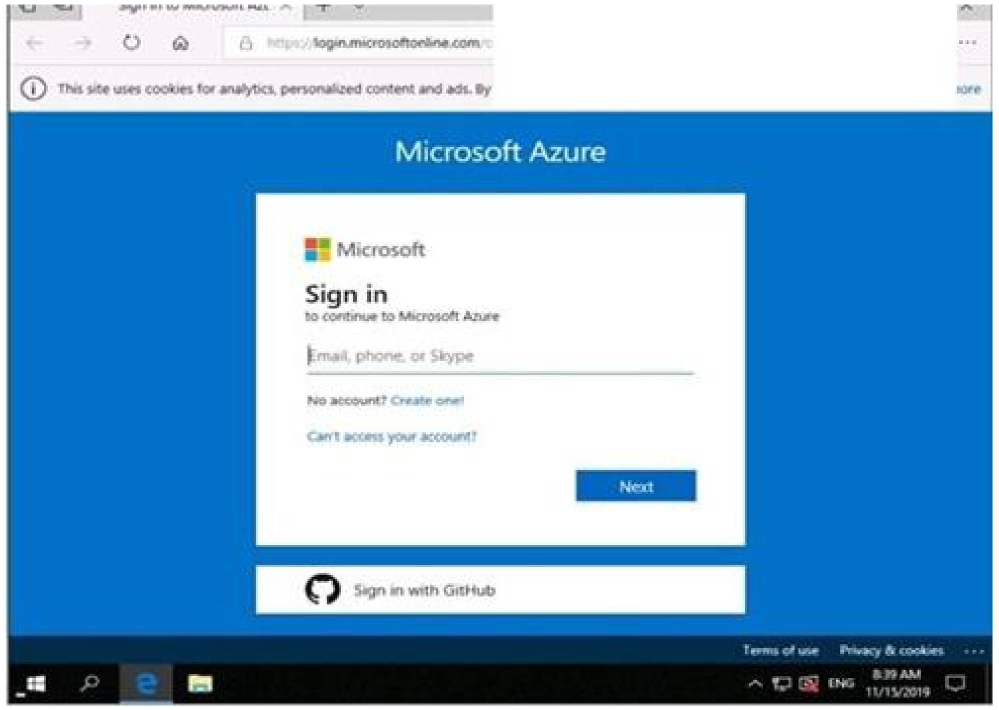


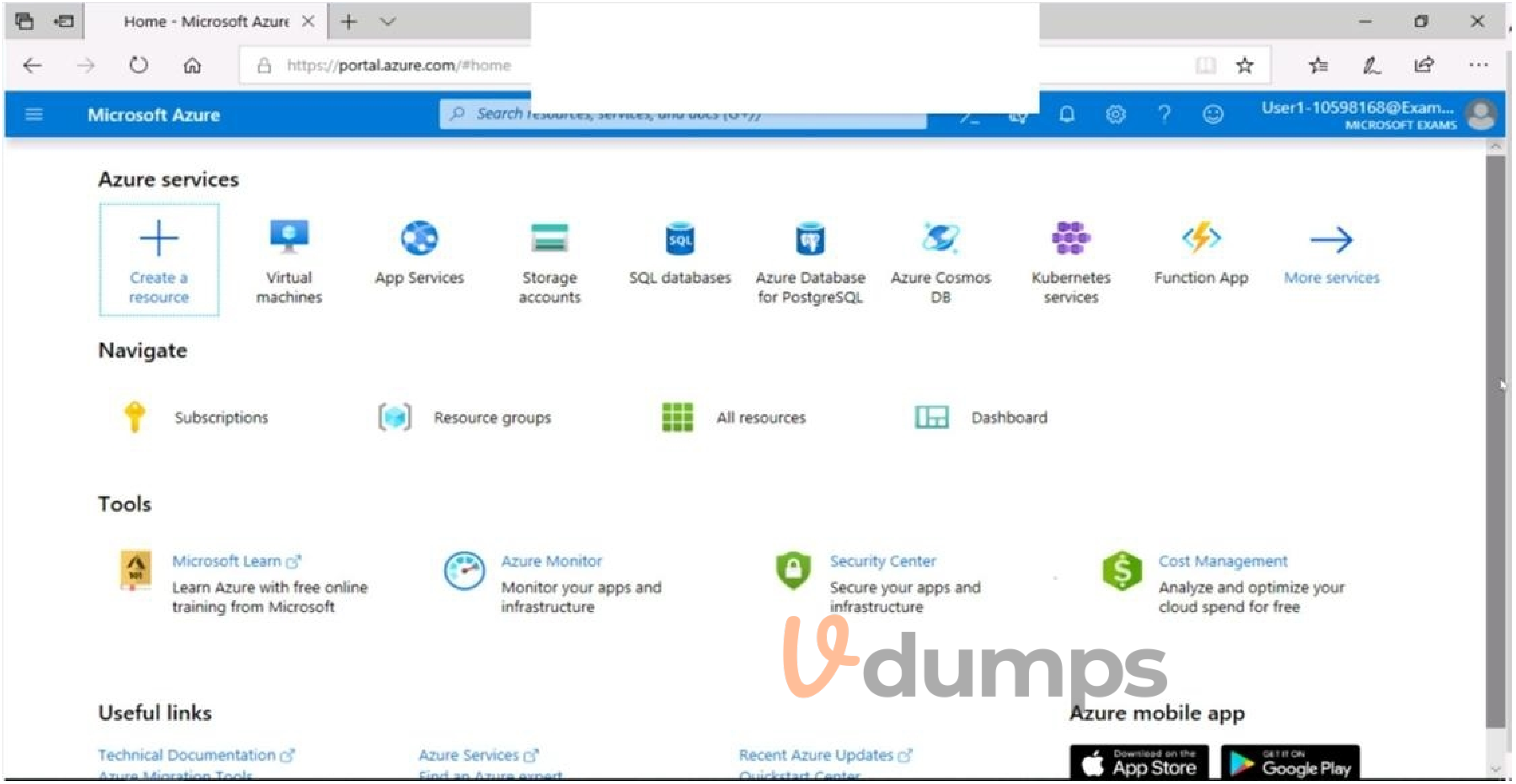
Manage access to Azure resources for users, groups, service principal
creating role assignments. Learn more

5. In the Role drop-down list, select the role Virtual Machine Contributor.
Virtual Machine Contributor lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.
6. In the Select list, select user user21059868
7. Click Save to assign the role.
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor

**QUESTION 34**

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: User1-10598168@ExamUsers.com
Azure Password: Ag1Bh9!#Bd
The following information is for technical support purposes only:
Lab Instance: 10598168


https://login.microsoftonline.com/
This site uses cookies for analytics, personalized content and ads. By
Microsoft Azure
Microsoft
Sign in
to continue to Microsoft Azure
Email, phone, or Skype
No account? Create one!
Can't access your account?
Next
Sign in with GitHub
Terms of use
Privacy & cookies
ENG
8:39 AM
11/15/2019

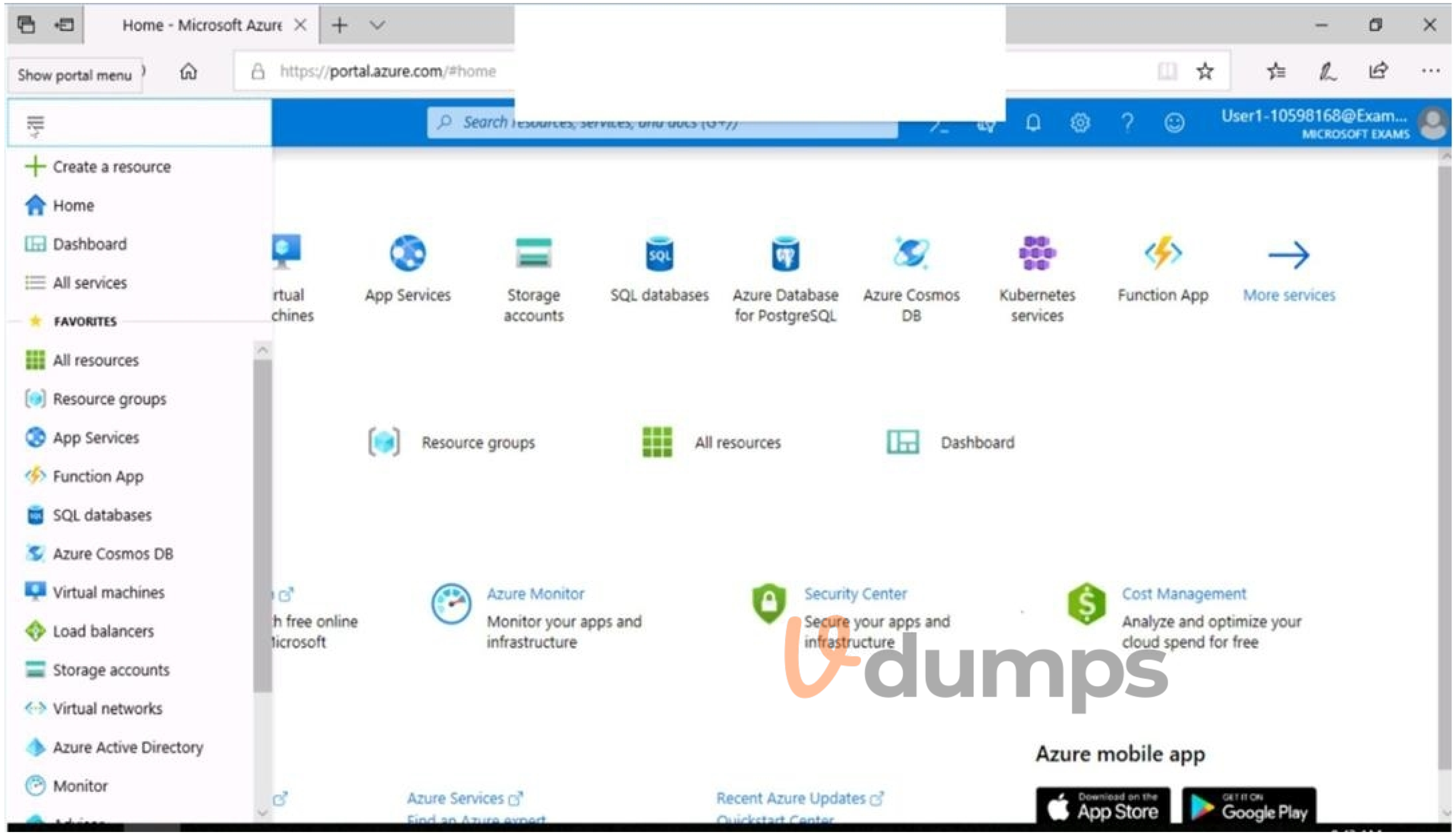


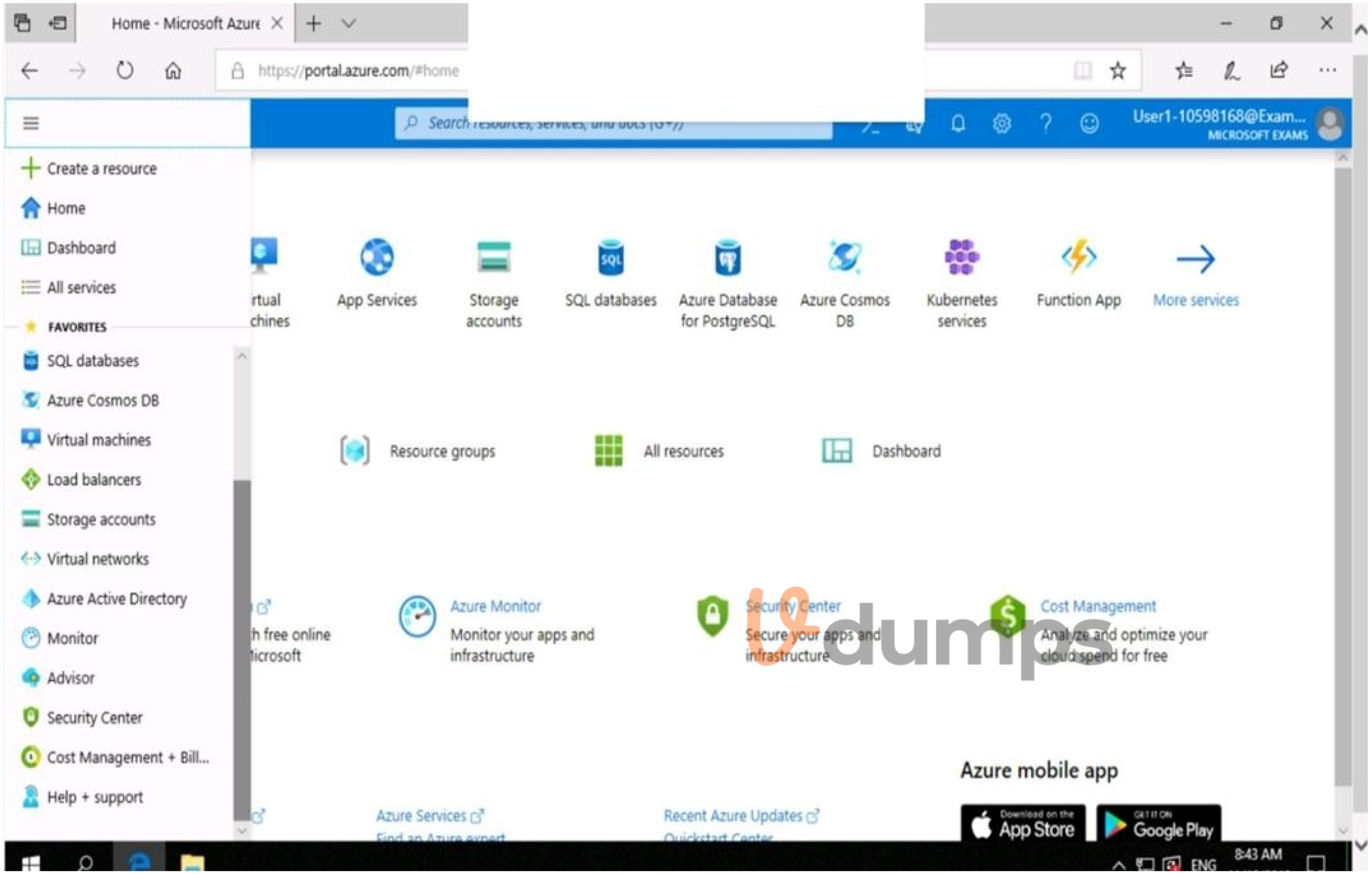
Learn Azure with free online training from Microsoft

Monitor your apps and infrastructure

Secure your apps and infrastructure

Analyze and optimize your cloud spend for free


Home - Microsoft Azure
Show portal menu
https://portal.azure.com/#home
Search resources, services, and docs (G+/)
User1-10598168@Exam...
MICROSOFT EXAMS
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
rtual chines
App Services
Storage accounts
SQL databases
Azure Database for PostgreSQL
Azure Cosmos DB
Kubernetes services
Function App
More services
Resource groups
All resources
Dashboard
h free online
licrosoft
Azure Monitor
Monitor your apps and infrastructure
Security Center
Secure your apps and infrastructure
Cost Management
Analyze and optimize your cloud spend for free
Azure mobile app
Azure Services
Find an Azure expert
Recent Azure Updates
Quickstart Center
Download on the App Store
GET IT ON Google Play



You need to ensure that only devices connected to a 131.107.0.0/16 subnet can access data in the rg1lod10598168 Azure Storage account.
To complete this task, sign in to the Azure portal.

A.

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
Step 1:
1. In Azure portal go to the storage account you want to secure. Here: rg1lod10598168
2. Click on the settings menu called Firewalls and virtual networks.
3. To deny access by default, choose to allow access from Selected networks. To allow traffic from all networks, choose to allow access from All networks.
4. Click Save to apply your changes.

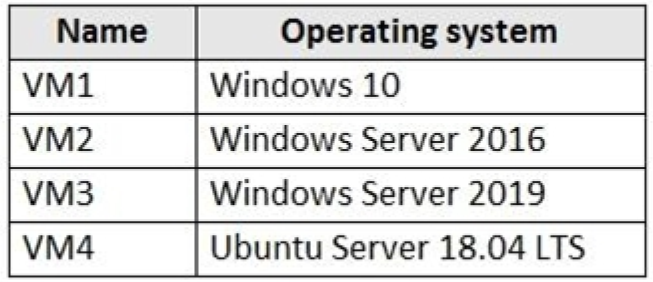
Step 2:
1. Go to the storage account you want to secure. Here: rg1lod10598168
2. Click on the settings menu called Firewalls and virtual networks.
3. Check that you've selected to allow access from Selected networks.
4. To grant access to a virtual network with a new network rule, under Virtual networks, click Add existing virtual network, select Virtual networks and Subnets options. Enter the 131.107.0.0/16 subnet and then click Add.
Note: When network rules are configured, only applications requesting data over the specified set of networks can access a storage account. You can limit access to your storage account to requests originating from specified IP addresses, IP ranges or from a list of subnets in an Azure Virtual Network (VNet).
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

**QUESTION 35**
You have Azure Resource Manager templates that you use to deploy Azure virtual machines.
You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.
What should you use?

A. device configuration policies in Microsoft Intune
B. Azure Automation State Configuration
C. security policies in Azure Security Center
D. device compliance policies in Microsoft Intune

**Correct Answer: B**
**Section:**
**Explanation:**
You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines.
Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSC-Service so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.
Reference:
https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started

**QUESTION 36**
You have an Azure subscription that contains the Azure virtual machines shown in the following table.



| Name | Operating system |
|---|---|
| VM1 | Windows 10 |
| VM2 | Windows Server 2016 |
| VM3 | Windows Server 2019 |
| VM4 | Ubuntu Server 18.04 LTS |

You create an MDM Security Baseline profile named Profile1.
You need to identify to which virtual machines Profile1 can be applied.
Which virtual machines should you identify?

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

**Correct Answer: A**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines

**QUESTION 37**
SIMULATION
You need to ensure that connections from the Internet to VNET1\subnet0 are allowed only over TCP port 7777. The solution must use only currently deployed resources.
To complete this task, sign in to the Azure portal.

A.

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
You need to configure the Network Security Group that is associated with subnet0.
1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET1. Alternatively, browse to Virtual Networks in the left navigation pane.
2. In the properties of VNET1, click on Subnets. This will display the subnets in VNET1 and the Network Security Group associated to each subnet. Note the name of the Network Security Group associated to Subnet0.
3. Type Network Security Groups into the search box and select the Network Security Group associated with Subnet0.
4. In the properties of the Network Security Group, click on Inbound Security Rules.
5. Click the Add button to add a new rule.
6. In the Source field, select Service Tag.
7. In the Source Service Tag field, select Internet.
8. Leave the Source port ranges and Destination field as the default values (* and All).
9. In the Destination port ranges field, enter 7777.
10. Change the Protocol to TCP.
11. Leave the Action option as Allow.
12. Change the Priority to 100.
13. Change the Name from the default Port_8080 to something more descriptive such as Allow_TCP_7777_from_Internet. The name cannot contain spaces. 14. Click the Add button to save the new rule.

**QUESTION 38**
SIMULATION
You need to prevent administrators from performing accidental changes to the Homepage app service plan.
To complete this task, sign in to the Azure portal.

A.

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
You need to configure a ‘lock’ for the app service plan. A read-only lock ensures that no one can make changes to the app service plan without first deleting the lock.
1. In the Azure portal, type App Service Plans in the search box, select App Service Plans from the search results then select Homepage. Alternatively, browse to App Service Plans in the left navigation pane.
2. In the properties of the app service plan, click on Locks.
3. Click the Add button to add a new lock.
4. Enter a name in the Lock name field. It doesn’t matter what name you provide for the exam.

5. For the Lock type, select Read-only.
6. Click OK to save the changes.

**QUESTION 39**
SIMULATION
You need to ensure that a user named Danny11597200 can sign in to any SQL database on a Microsoft SQL server named web11597200 by using SQL Server Management Studio (SSMS) and Azure Active Directory (Azure AD) credentials.
To complete this task, sign in to the Azure portal.

A.

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
You need to provision an Azure AD Admin for the SQL Server.
1. In the Azure portal, type SQL Server in the search box, select SQL Server from the search results then select the server named web11597200. Alternatively, browse to SQL Server in the left navigation pane.
2. In the SQL Server properties page, click on Active Directory Admin.
3. Click the Set Admin button.
4. In the Add Admin window, search for and select Danny11597200.
5. Click the Select button to add Danny11597200.
6. Click the Save button to save the changes.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?tabs=azure-powershell

**QUESTION 40**
SIMULATION
You need to configure a Microsoft SQL server named Web11597200 only to accept connections from the Subnet0 subnet on the VNET01 virtual network.
To complete this task, sign in to the Azure portal.

A.

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
You need to allow access to Azure services and configure a virtual network rule for the SQL Server.
1. In the Azure portal, type SQL Server in the search box, select SQL Server from the search results then select the server named web11597200. Alternatively, browse to SQL Server in the left navigation pane.
2. In the properties of the SQL Server, click Firewalls and virtual networks.
3. In the Virtual networks section, click on Add existing. This will open the Create/Update virtual network rule window.
4. Give the rule a name such as Allow_VNET01-Subnet0 (it doesn’t matter what name you enter for the exam).
5. In the Virtual network box, select VNET01.
6. In the Subnet name box, select Subnet0.
7. Click the OK button to save the rule.
8. Back in the Firewall / Virtual Networks window, set the Allow access to Azure services option to On.

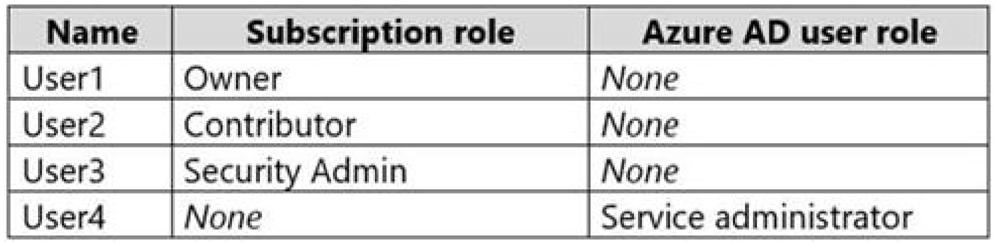
**QUESTION 41**
You have Azure Resource Manager templates that you use to deploy Azure virtual machines.

You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.
What should you use?

A. device configuration policies in Microsoft Intune
B. an Azure Desired State Configuration (DSC) virtual machine extension
C. security policies in Azure Security Center
D. Azure Logic Apps

**Correct Answer: B**
**Section:**
**Explanation:**
The primary use case for the Azure Desired State Configuration (DSC) extension is to bootstrap a VM to the Azure Automation State Configuration (DSC) service. The service provides benefits that include ongoing management of the VM configuration and integration with other operational tools, such as Azure Monitoring. Using the extension to register VM's to the service provides a flexible solution that even works across Azure subscriptions.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview

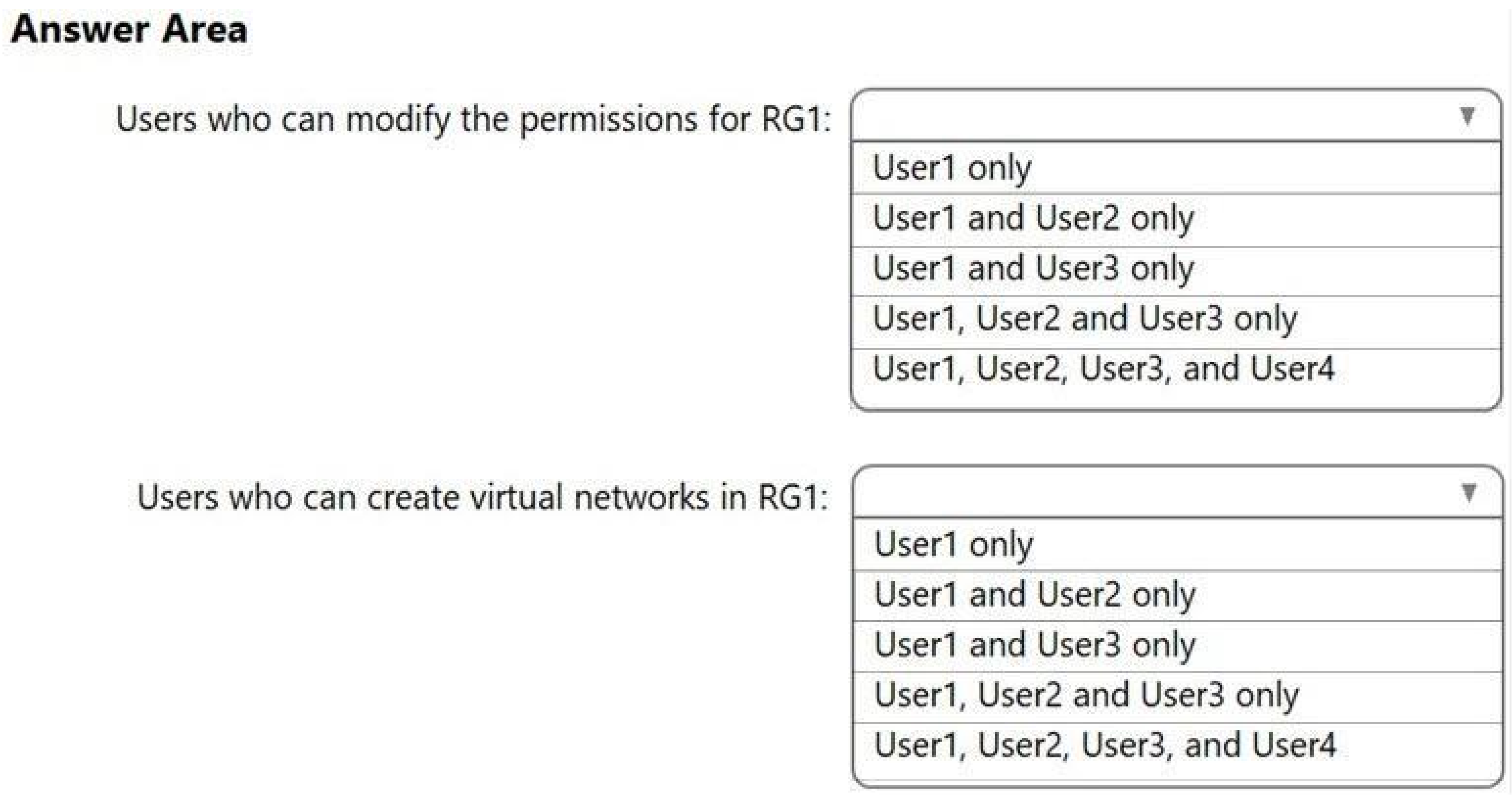
**QUESTION 42**
HOTSPOT
You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.



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

You create a resource group named RG1.
Which users can modify the permissions for RG1 and which users can create virtual networks in RG1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Hot Area:**



Answer Area

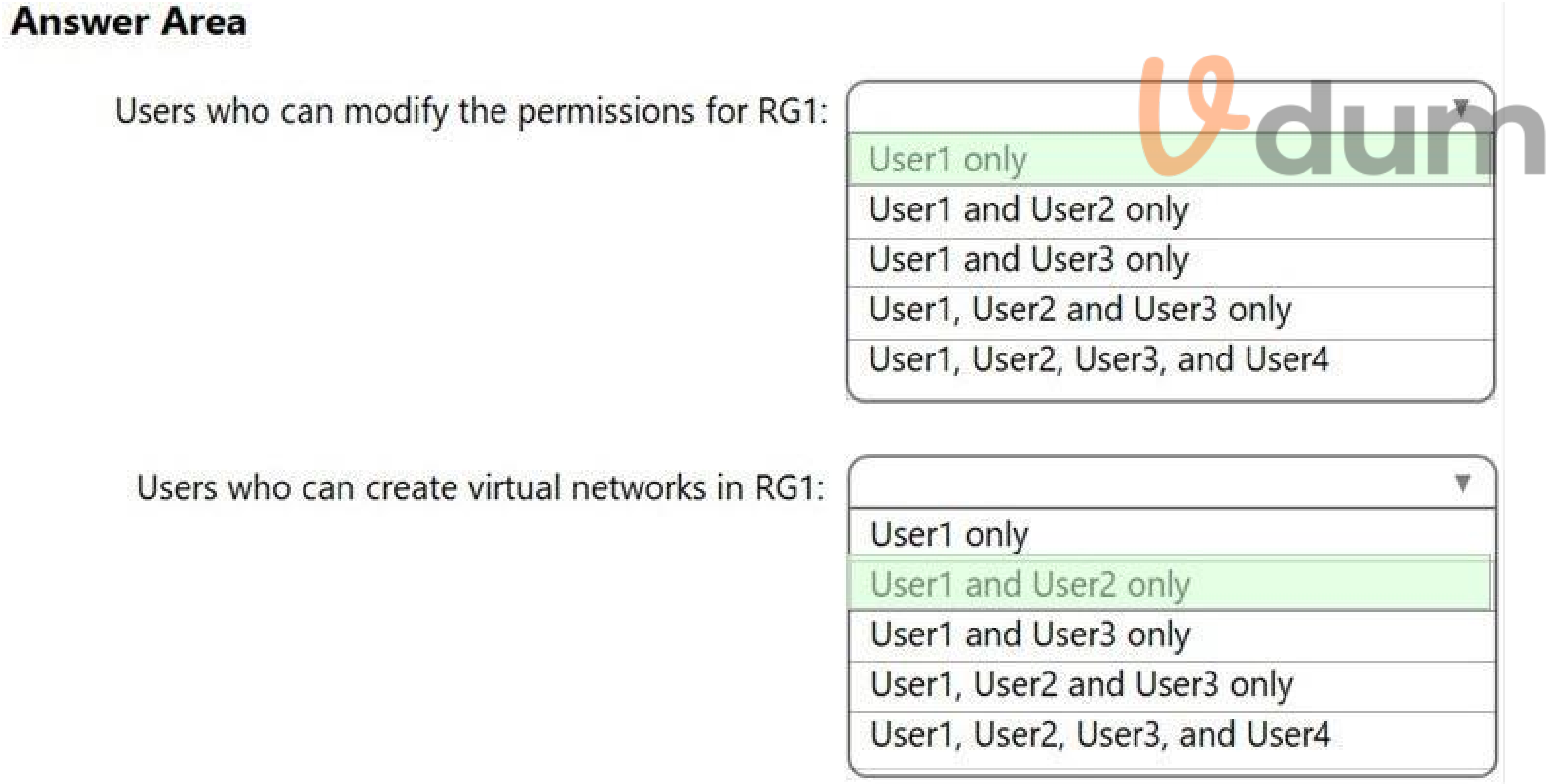
Users who can modify the permissions for RG1:

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

Users who can create virtual networks in RG1:

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

**Answer Area:**



Answer Area

Users who can modify the permissions for RG1:

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

Users who can create virtual networks in RG1:

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

**Section:**
**Explanation:**
Box 1: Only an owner can change permissions on resources.
Box 2: A Contributor can create/modify/delete anything in the subscription but cannot change permissions.

**QUESTION 43**
SIMULATION

You need to configure network connectivity between a virtual network named VNET1 and a virtual network named VNET2. The solution must ensure that virtual machines connected to VNET1 can communicate with virtual machines connected to VNET2.
To complete this task, sign in to the Azure portal and modify the Azure resources.

A.

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
You need to configure VNet Peering between the two networks. The questions states, “The solution must ensure that virtual machines connected to VNET1 can communicate with virtual machines connected to VNET2”. It doesn’t say the VMs on VNET2 should be able to communicate with VMs on VNET1. Therefore, we need to configure the peering to allow just the one-way communication.
1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET1. Alternatively, browse to Virtual Networks in the left navigation pane.
2. In the properties of VNET1, click on Peerings.
3. In the Peerings blade, click Add to add a new peering.
4. In the Name of the peering from VNET1 to remote virtual network box, enter a name such as VNET1-VNET2 (this is the name that the peering will be displayed as in VNET1)
5. In the Virtual Network box, select VNET2.
6. In the Name of the peering from remote virtual network to VNET1 box, enter a name such as VNET2-VNET1 (this is the name that the peering will be displayed as in VNET2). There is an option Allow virtual network access from VNET to remote virtual network. This should be left as Enabled.
7. For the option Allow virtual network access from remote network to VNET1, click the slider button to Disabled.
8. Click the OK button to save the changes.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering

**QUESTION 44**
SIMULATION
You need to deploy an Azure firewall to a virtual network named VNET3.
To complete this task, sign in to the Azure portal and modify the Azure resources.
This task might take several minutes to complete. You can perform other tasks while the task completes.

A.

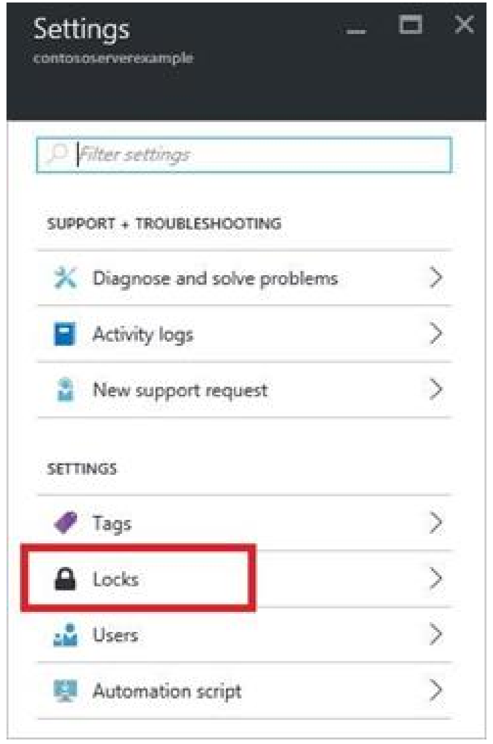
**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
To add an Azure firewall to a VNET, the VNET must first be configured with a subnet named AzureFirewallSubnet (if it doesn’t already exist).
Configure VNET3.
1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET3. Alternatively, browse to Virtual Networks in the left navigation pane.
2. In the Overview section, note the Location (region) and Resource Group of the virtual network. We’ll need these when we add the firewall.
3. Click on Subnets.
4. Click on + Subnet to add a new subnet.
5. Enter AzureFirewallSubnet in the Name box. The subnet must be named AzureFirewallSubnet.
6. Enter an appropriate IP range for the subnet in the Address range box.
7. Click the OK button to create the subnet.
Add the Azure Firewall.
1. In the settings of VNET3 click on Firewall.
2. Click the Click here to add a new firewall link.

3. The Resource group will default to the VNET3 resource group. Leave this default.
4. Enter a name for the firewall in the Name box.
5. In the Region box, select the same region as VNET3.
6. In the Public IP address box, select an available public IP address if one exists, or click Add new to add a new public IP address.
7. Click the Review + create button.
8. Review the settings and click the Create button to create the firewall.
Reference:
https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal

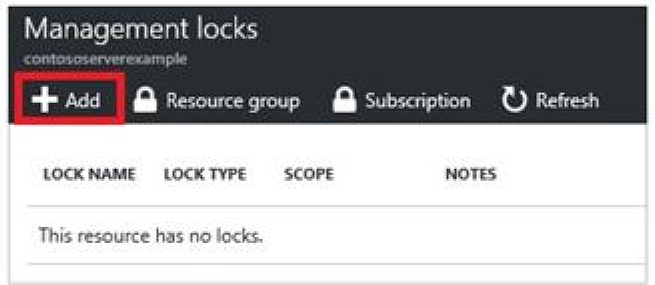
**QUESTION 45**
SIMULATION
You need to configure a virtual network named VNET2 to meet the following requirements:
Administrators must be prevented from deleting VNET2 accidentally.
Administrators must be able to add subnets to VNET2 regularly.
To complete this task, sign in to the Azure portal and modify the Azure resources.

A.

**Correct Answer: A**
**Section:**
**Explanation:**
Answer: A
Explanation:
Locking prevents other users in your organization from accidentally deleting or modifying critical resources, such as Azure subscription, resource group, or resource.
Note: In Azure, the term resource refers to an entity managed by Azure. For example, virtual machines, virtual networks, and storage accounts are all referred to as Azure resources.
1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET2. Alternatively, browse to Virtual Networks in the left navigation pane.
2. In the Settings blade for virtual network VNET2, select Locks.



3. To add a lock, select Add.



| LOCK NAME | LOCK TYPE | SCOPE | NOTES |
|---|---|---|---|
| This resource has no locks. | | | |

4. For Lock type select Delete lock, and click OK
Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

**QUESTION 46**
You have an Azure virtual machine named VM1.
From Azure Security Center, you get the following high-severity recommendation: “Install endpoint protection solutions on virtual machine”.
You need to resolve the issue causing the high-severity recommendation.
What should you do?

A. Add the Microsoft Antimalware extension to VM1.

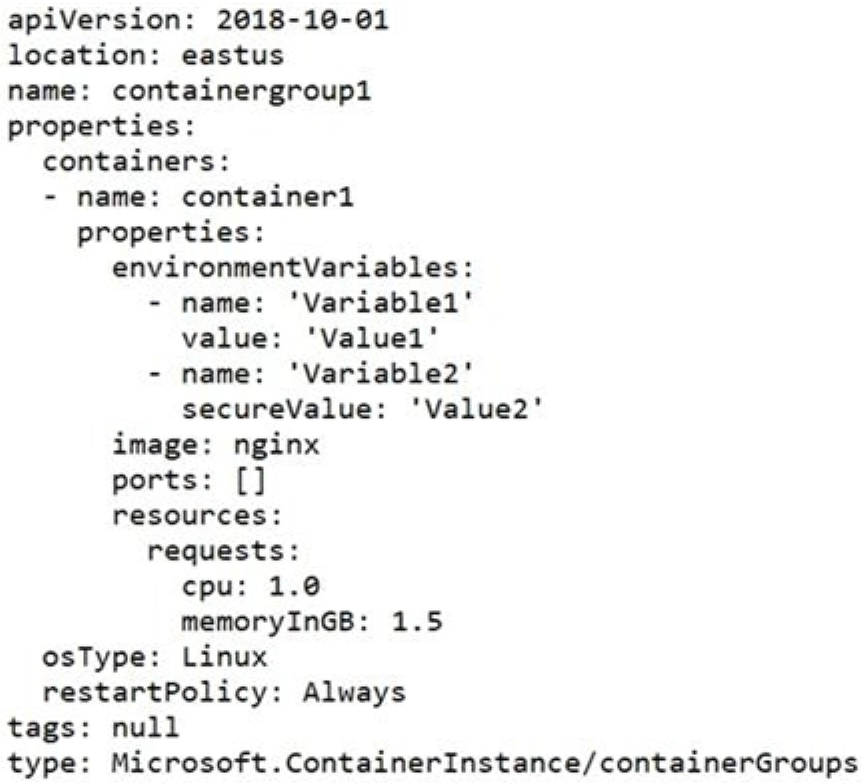
B. Install Microsoft System Center Security Management Pack for Endpoint Protection on VM1.

C. Add the Network Watcher Agent for Windows extension to VM1.

D. Onboard VM1 to Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

**Correct Answer: A**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-endpoint-protection

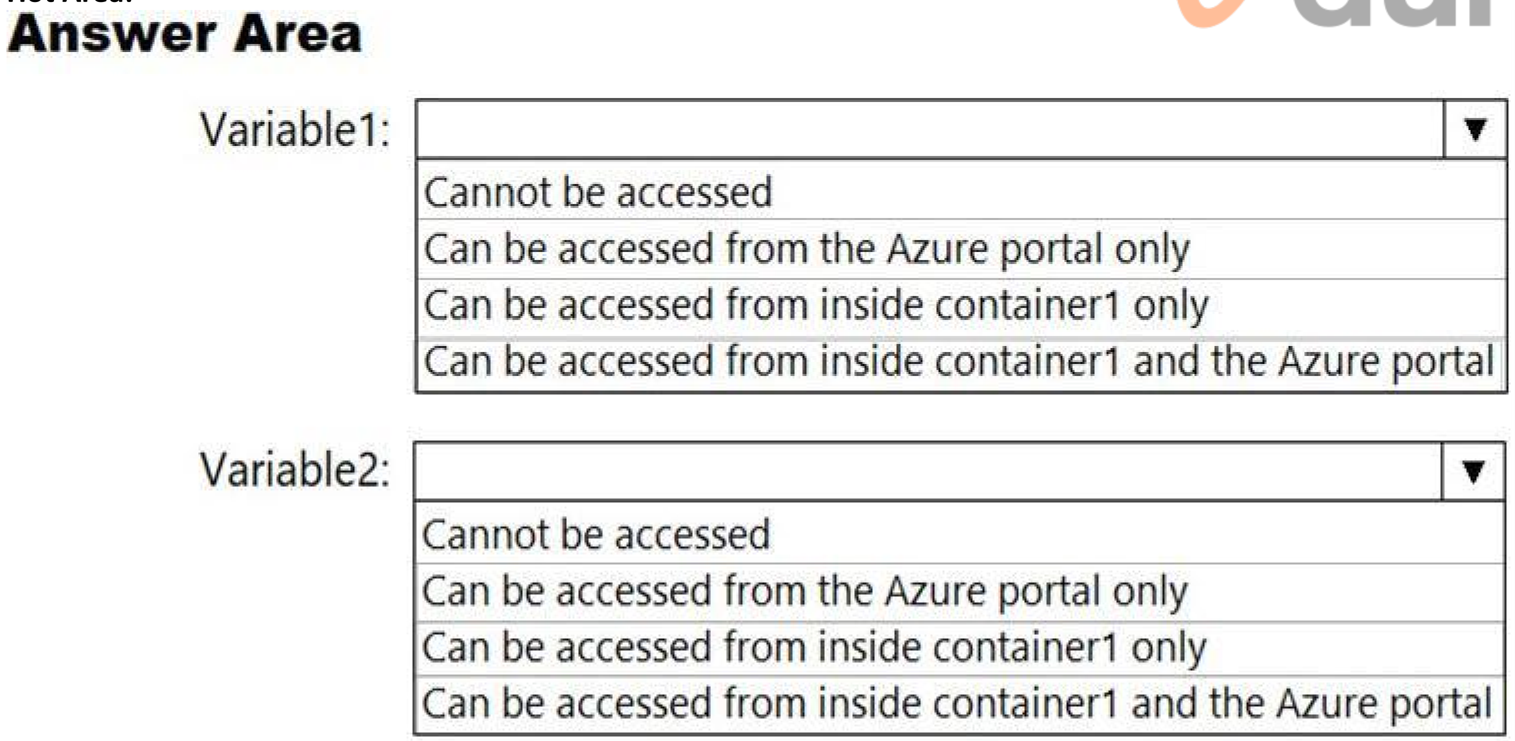
**QUESTION 47**
HOTSPOT
You have a file named File1.yaml that contains the following contents.



```
apiVersion: 2018-10-01
location: eastus
name: containergroup1
properties:
  containers:
  - name: container1
    properties:
      environmentVariables:
        - name: 'Variable1'
          value: 'Value1'
        - name: 'Variable2'
          secureValue: 'Value2'
      image: nginx
      ports: []
      resources:
        requests:
          cpu: 1.0
          memoryInGB: 1.5
  osType: Linux
  restartPolicy: Always
tags: null
type: Microsoft.ContainerInstance/containerGroups
```

You create an Azure container instance named container1 by using File1.yaml.
You need to identify where you can access the values of Variable1 and Variable2.
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**

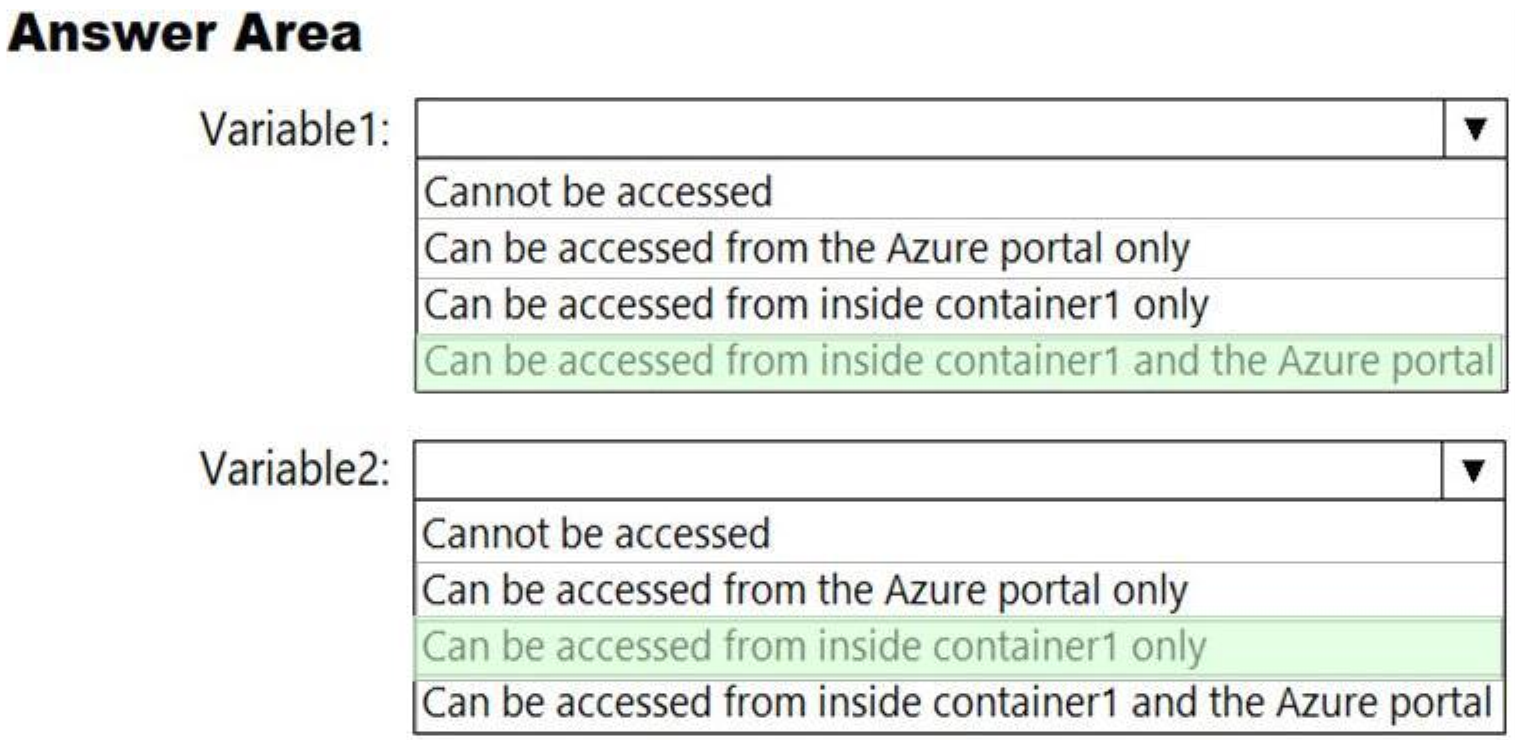
Variable1: ▼

- Cannot be accessed
- Can be accessed from the Azure portal only
- Can be accessed from inside container1 only
- Can be accessed from inside container1 and the Azure portal

Variable2: ▼

- Cannot be accessed
- Can be accessed from the Azure portal only
- Can be accessed from inside container1 only
- Can be accessed from inside container1 and the Azure portal

**Answer Area:**



**Answer Area**

Variable1: ▼

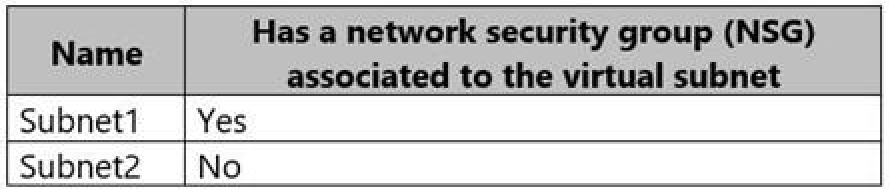
- Cannot be accessed
- Can be accessed from the Azure portal only
- Can be accessed from inside container1 only
- [✓ Can be accessed from inside container1 and the Azure portal]

Variable2: ▼

- Cannot be accessed
- Can be accessed from the Azure portal only
- [✓ Can be accessed from inside container1 only]
- Can be accessed from inside container1 and the Azure portal

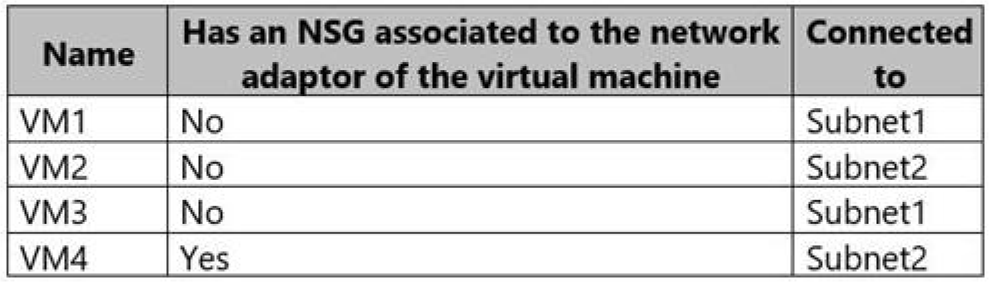
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-environment-variables

**QUESTION 48**
You have an Azure subscription that contains a virtual network. The virtual network contains the subnets shown in the following table.



| Name | Has a network security group (NSG) associated to the virtual subnet |
|---|---|
| Subnet1 | Yes |
| Subnet2 | No |

The subscription contains the virtual machines shown in the following table.



| Name | Has an NSG associated to the network adaptor of the virtual machine | Connected to |
|---|---|---|
| VM1 | No | Subnet1 |
| VM2 | No | Subnet2 |
| VM3 | No | Subnet1 |
| VM4 | Yes | Subnet2 |

You enable just in time (JIT) VM access for all the virtual machines.
You need to identify which virtual machines are protected by JIT.
Which virtual machines should you identify?

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

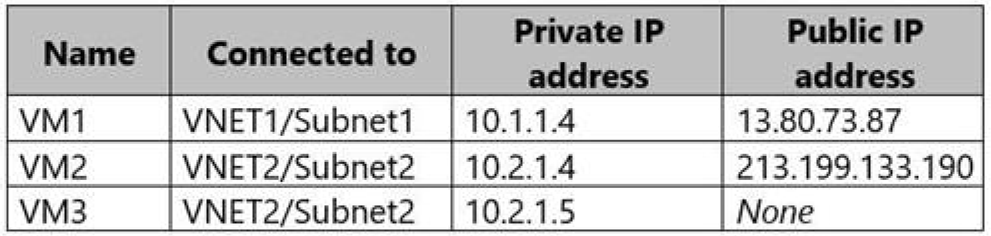
**Correct Answer: C**
**Section:**

**Explanation:**
An NSG needs to be enabled, either at the VM level or the subnet level.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

**QUESTION 49**

HOTSPOT

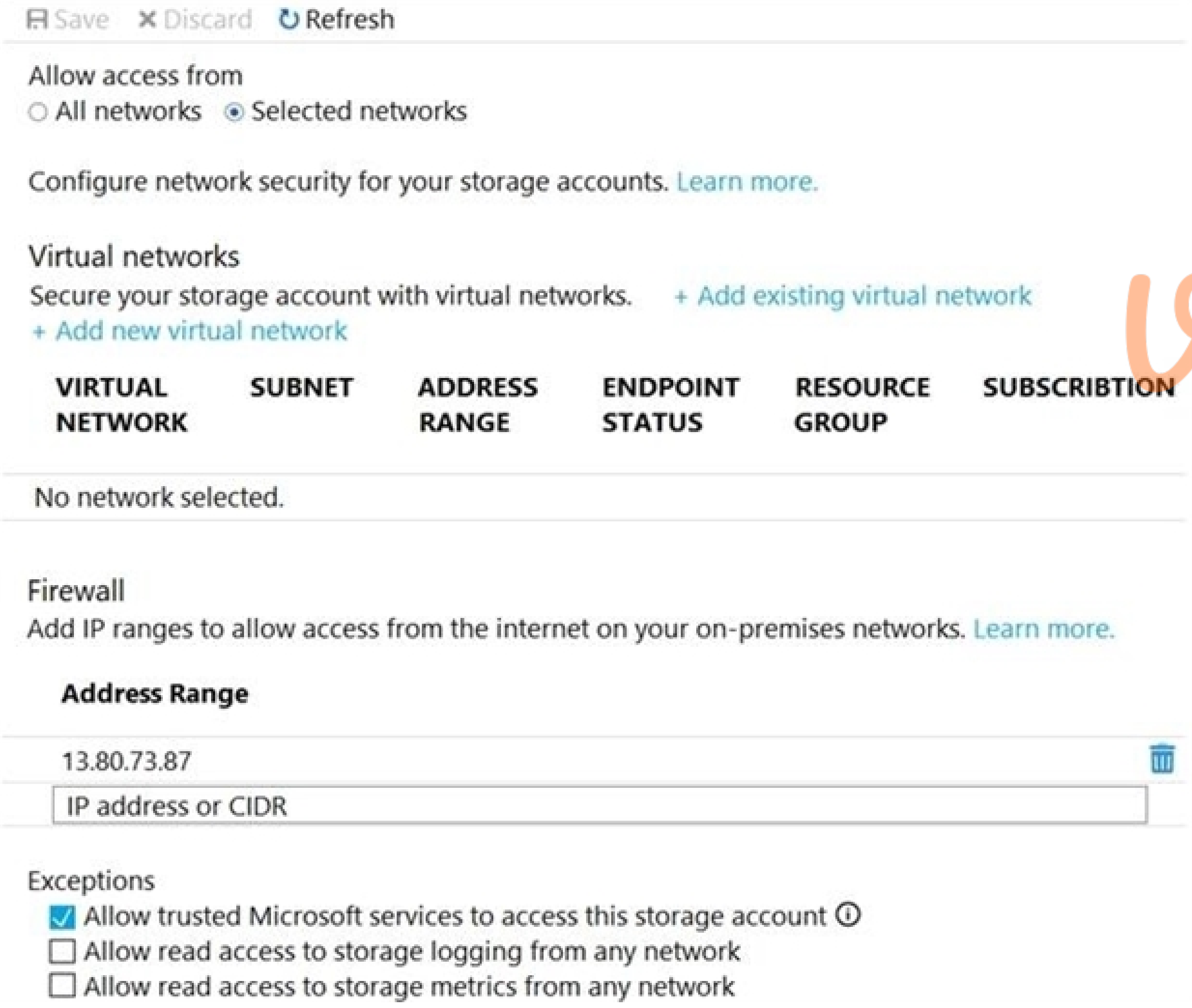
You have an Azure subscription that contains the virtual machines shown in the following table.



| Name | Connected to | Private IP address | Public IP address |
|---|---|---|---|
| VM1 | VNET1/Subnet1 | 10.1.1.4 | 13.80.73.87 |
| VM2 | VNET2/Subnet2 | 10.2.1.4 | 213.199.133.190 |
| VM3 | VNET2/Subnet2 | 10.2.1.5 | *None* |

Subnet1 and Subnet2 have a Microsoft.Storage service endpoint configured.

You have an Azure Storage account named storageacc1 that is configured as shown in the following exhibit.



Allow access from
○ All networks ● Selected networks

Configure network security for your storage accounts. Learn more.

Virtual networks
Secure your storage account with virtual networks. + Add existing virtual network
+ Add new virtual network

| VIRTUAL NETWORK | SUBNET | ADDRESS RANGE | ENDPOINT STATUS | RESOURCE GROUP | SUBSCRIPTION |
|---|---|---|---|---|---|
| No network selected. | | | | | |

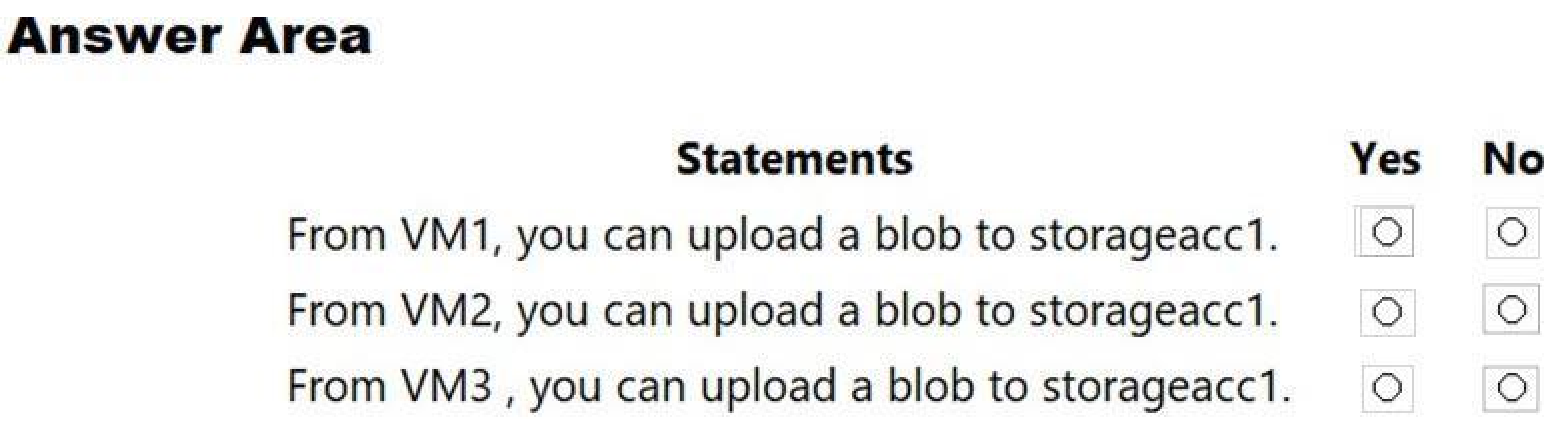
Firewall
Add IP ranges to allow access from the internet on your on-premises networks. Learn more.

| Address Range |
|---|
| 13.80.73.87 |
| IP address or CIDR |

Exceptions
☑ Allow trusted Microsoft services to access this storage account ⓘ
☐ Allow read access to storage logging from any network
☐ Allow read access to storage metrics from any network

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

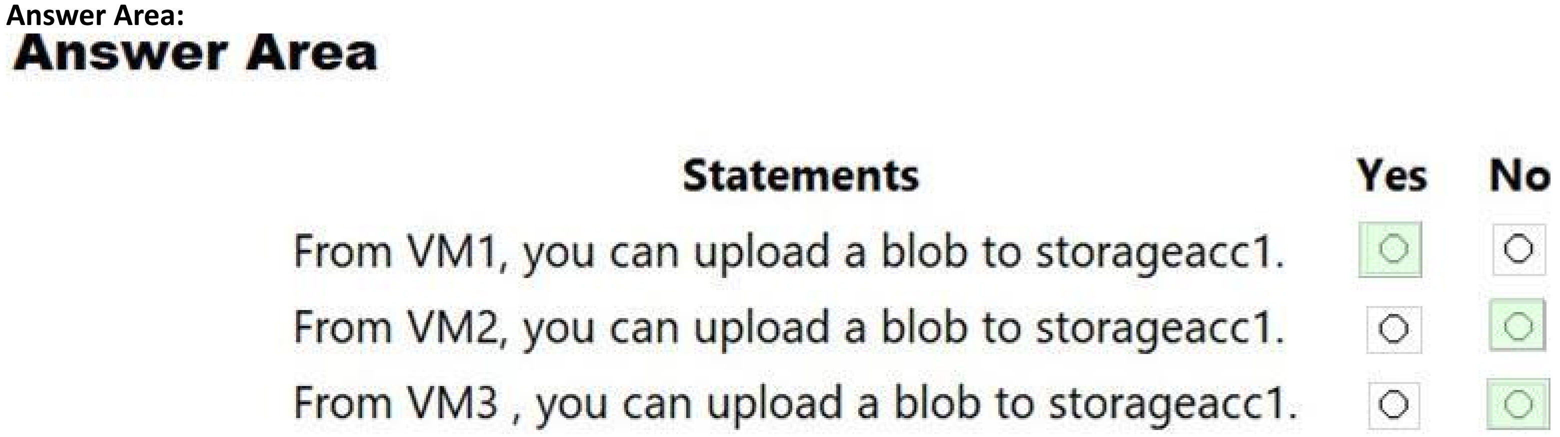
**Hot Area:**



**Answer Area**

| Statements | Yes | No |
|---|---|---|
| From VM1, you can upload a blob to storageacc1. | ○ | ○ |
| From VM2, you can upload a blob to storageacc1. | ○ | ○ |
| From VM3 , you can upload a blob to storageacc1. | ○ | ○ |

**Answer Area:**



**Answer Area**

| Statements | Yes | No |
|---|---|---|
| From VM1, you can upload a blob to storageacc1. | [✓ ○] | ○ |
| From VM2, you can upload a blob to storageacc1. | ○ | [✓ ○] |
| From VM3 , you can upload a blob to storageacc1. | ○ | [✓ ○] |

**Section:**
**Explanation:**
Box 1: Yes
The public IP of VM1 is allowed through the firewall.
Box 2: No
The allowed virtual network list is empty so VM2 cannot access storageacc1 directly. The public IP address of VM2 is not in the allowed IP list so VM2 cannot access storageacc1 over the Internet.
Box 3: No
The allowed virtual network list is empty so VM3 cannot access storageacc1 directly. VM3 does not have a public IP address so it cannot access storageacc1 over the Internet.
Reference:
https://docs.microsoft.com/en-gb/azure/storage/common/storage-network-security

**QUESTION 50**

You have Azure Resource Manager templates that you use to deploy Azure virtual machines.
You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.
What should you use?

A. device compliance policies in Microsoft Intune
B. Azure Automation State Configuration
C. application security groups
D. Azure Advisor

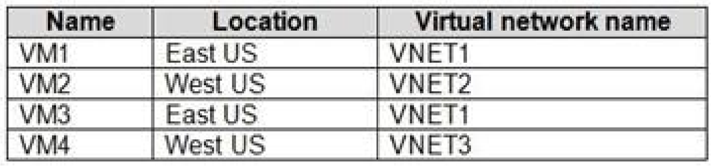
**Correct Answer: B**
**Section:**
**Explanation:**
You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager),on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines. Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSC Service so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.

**QUESTION 51**
You have an Azure Container Registry named Registry1.
From Azure Security Center, you enable Azure Container Registry vulnerability scanning of the images in Registry1.
You perform the following actions:
Push a Windows image named Image1 to Registry1.
Push a Linux image named Image2 to Registry1.
Push a Windows image named Image3 to Registry1.
Modify Image1 and push the new image as Image4 to Registry1.
Modify Image2 and push the new image as Image5 to Registry1.
Which two images will be scanned for vulnerabilities? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Image4
B. Image2
C. Image1
D. Image3
E. Image5

**Correct Answer: B, E**
**Section:**
**Explanation:**
Only Linux images are scanned. Windows images are not scanned.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/azure-container-registry-integration

**QUESTION 52**
You have an Azure subscription that contains the virtual machines shown in the following table.



| Name | Location | Virtual network name |
|---|---|---|
| VM1 | East US | VNET1 |
| VM2 | West US | VNET2 |
| VM3 | East US | VNET1 |
| VM4 | West US | VNET3 |

All the virtual networks are peered.
You deploy Azure Bastion to VNET2.
Which virtual machines can be protected by the bastion host?

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

**Correct Answer: A**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/bastion/vnet-peering

**QUESTION 53**
You have an Azure Active Directory (Azure AD) tenant named Contoso.com and an Azure Kubernetes Service (AKS) cluster AKS1.

You discover that AKS1 cannot be accessed by using accounts from Contoso.com.
You need to ensure AKS1 can be accessed by using accounts from Contoso.com. The solution must minimize administrative effort.
What should you do first?

A. From Azure recreate AKS1.

B. From AKS1, upgrade the version of Kubernetes.

C. From Azure AD, implement Azure AD Premium.

D. From Azure AD, configure the User settings.

**Correct Answer: A**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli

**QUESTION 54**
You have an Azure subscription that contains an Azure Container Registry named Registry1. Azure Defender is enabled in the subscription. You upload several container images to Register1.
You discover that vulnerability security scans were not performed.
You need to ensure that the container images are scanned for vulnerabilities when they are uploaded to Registry1.
What should you do?

A. From the Azure portal modify the Pricing tier settings.

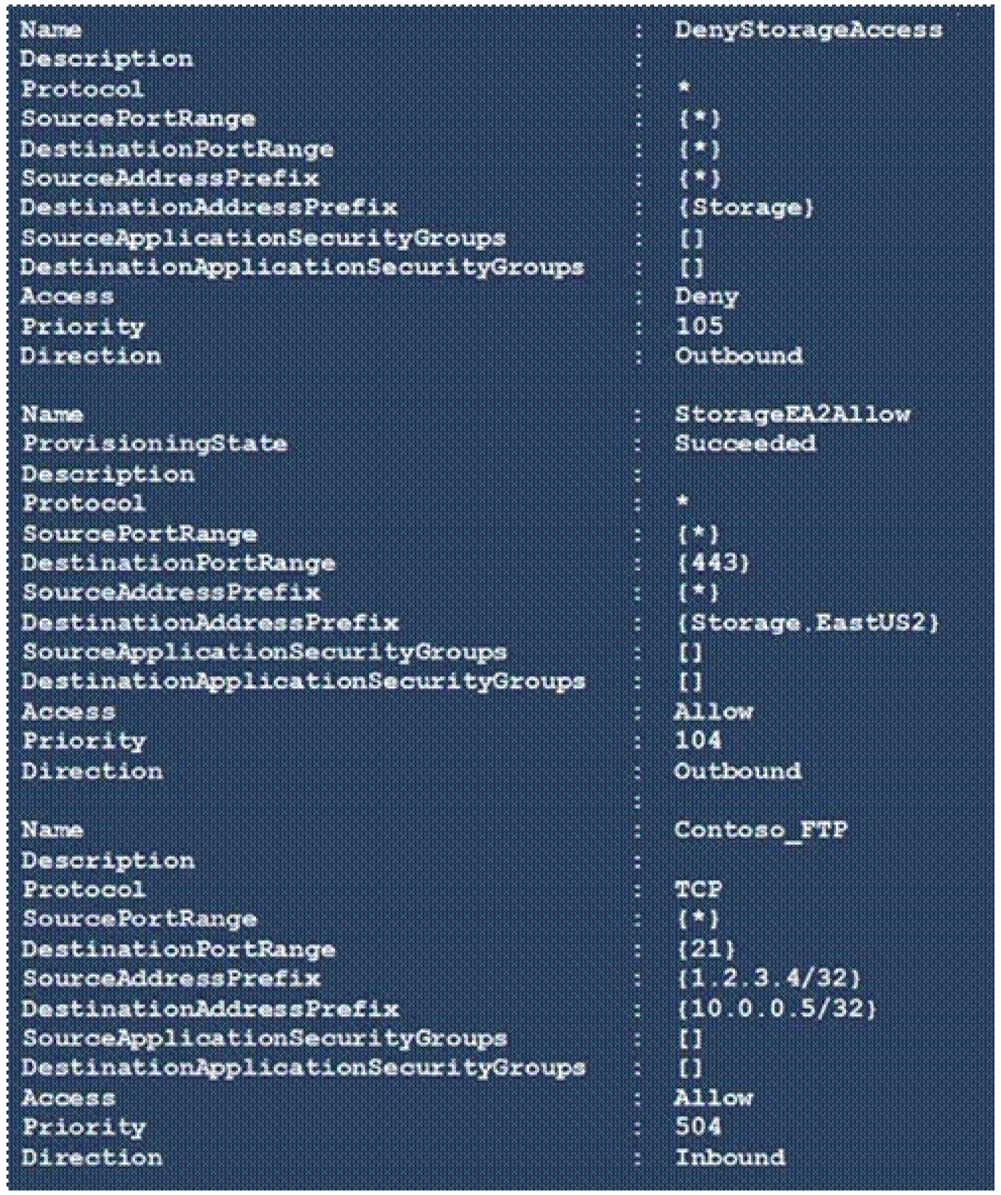
B. From Azure CLI, lock the container images.

C. Upload the container images by using AzCopy.

D. Push the container images to Registry1 by using Docker

**Correct Answer: A**
**Section:**
**Explanation:**
Reference:
https://charbelnemnom.com/scan-container-images-in-azure-container-registry-with-azure-security-center/

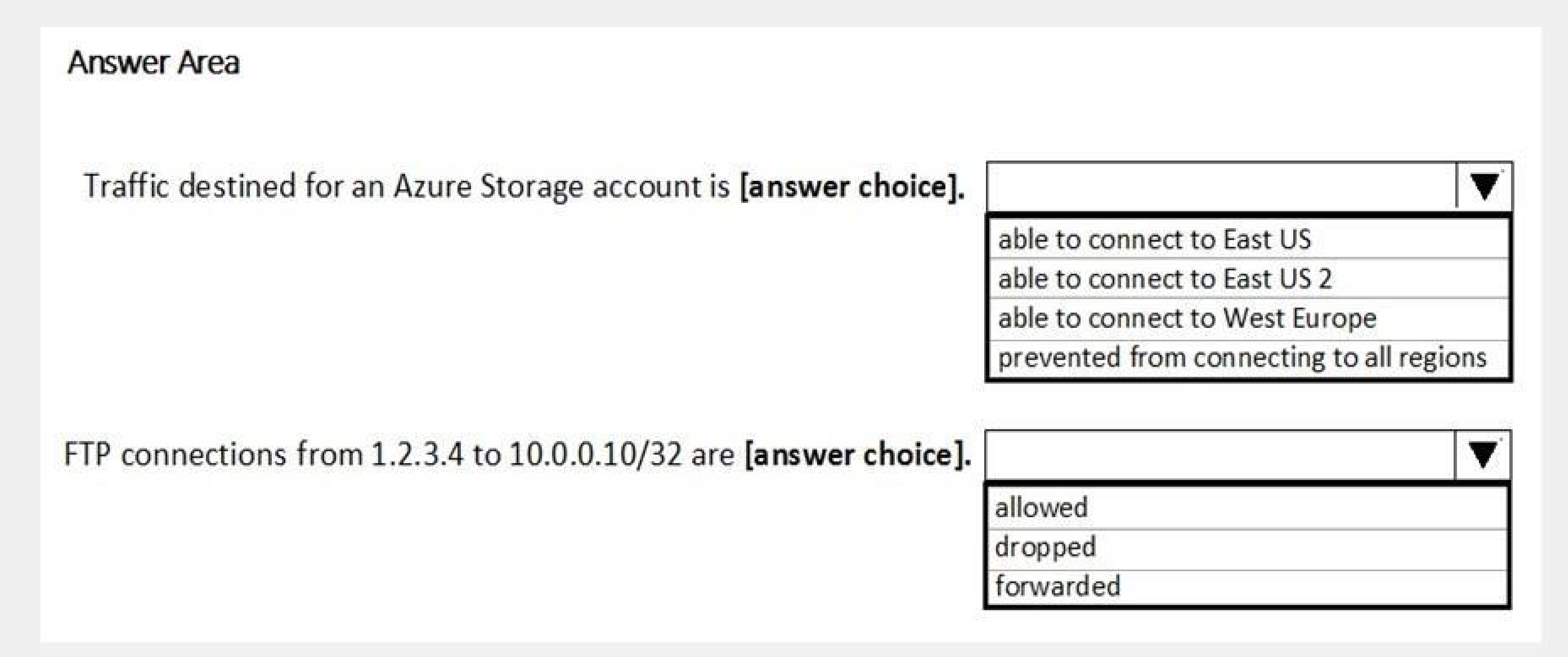
**QUESTION 55**
HOTSPOT
You have a network security group (NSG) bound to an Azure subnet.
You run Get-AzNetworkSecurityRuleConfig and receive the output shown in the following exhibit.



```
Name                                   : DenyStorageAccess
Description                            :
Protocol                               : *
SourcePortRange                        : {*}
DestinationPortRange                   : {*}
SourceAddressPrefix                    : {*}
DestinationAddressPrefix               : {Storage}
SourceApplicationSecurityGroups        : []
DestinationApplicationSecurityGroups   : []
Access                                 : Deny
Priority                               : 105
Direction                              : Outbound

Name                                   : StorageEA2Allow
ProvisioningState                      : Succeeded
Description                            :
Protocol                               : *
SourcePortRange                        : {*}
DestinationPortRange                   : {443}
SourceAddressPrefix                    : {*}
DestinationAddressPrefix               : {Storage.EastUS2}
SourceApplicationSecurityGroups        : []
DestinationApplicationSecurityGroups   : []
Access                                 : Allow
Priority                               : 104
Direction                              : Outbound
                                       :
Name                                   : Contoso_FTP
Description                            :
Protocol                               : TCP
SourcePortRange                        : {*}
DestinationPortRange                   : {21}
SourceAddressPrefix                    : {1.2.3.4/32}
DestinationAddressPrefix               : {10.0.0.5/32}
SourceApplicationSecurityGroups        : []
DestinationApplicationSecurityGroups   : []
Access                                 : Allow
Priority                               : 504
Direction                              : Inbound
```

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 Area

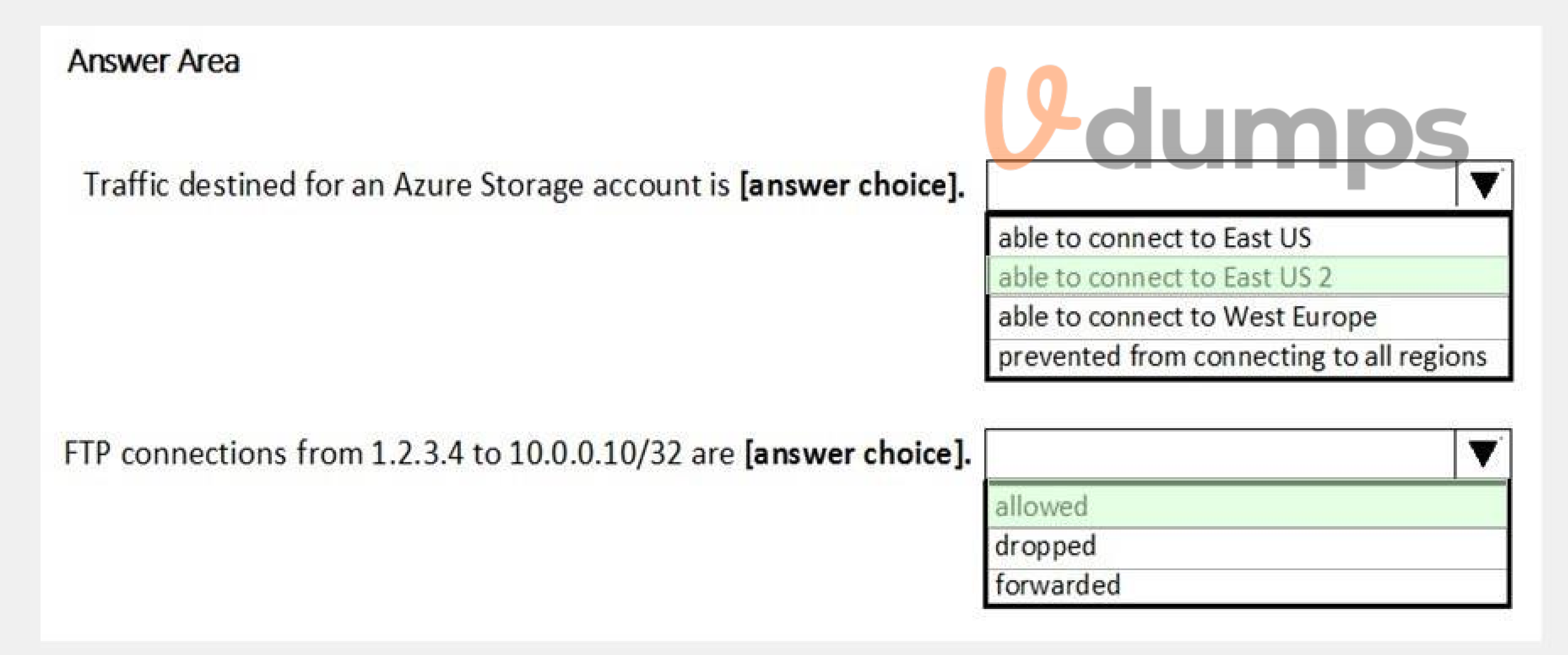
Traffic destined for an Azure Storage account is **[answer choice]**.

- able to connect to East US
- able to connect to East US 2
- able to connect to West Europe
- prevented from connecting to all regions

FTP connections from 1.2.3.4 to 10.0.0.10/32 are **[answer choice]**.

- allowed
- dropped
- forwarded

**Answer Area:**



Answer Area

Traffic destined for an Azure Storage account is **[answer choice]**.

- able to connect to East US
- [✓ able to connect to East US 2]
- able to connect to West Europe
- prevented from connecting to all regions

FTP connections from 1.2.3.4 to 10.0.0.10/32 are **[answer choice]**.

- [✓ allowed]
- dropped
- forwarded

**Section:**
**Explanation:**
Box 1: able to connect to East US 2
The StorageEA2Allow has DestinationAddressPrefix {Storage/EastUS2}
Box 2: allowed
TCP Port 21 controls the FTP session. Contoso_FTP has SourceAddressPrefix {1.2.3.4/32} and DestinationAddressPrefix {10.0.0.5/32}
Note:
The Get-AzureRmNetworkSecurityRuleConfig cmdlet gets a network security rule configuration for an Azure network security group. Security rules in network security groups enable you to filter the type of network traffic that can flow in and out of virtual network subnets and network interfaces.

Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group

**QUESTION 56**

You have a web app hosted on an on-premises server that is accessed by using a URL of https://www.contoso.com.
You plan to migrate the web app to Azure. You will continue to use https://www.contoso.com.
You need to enable HTTPS for the Azure web app.
What should you do first?

A. Export the public key from the on-premises server and save the key as a P7b file.

B. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using TripleDES.

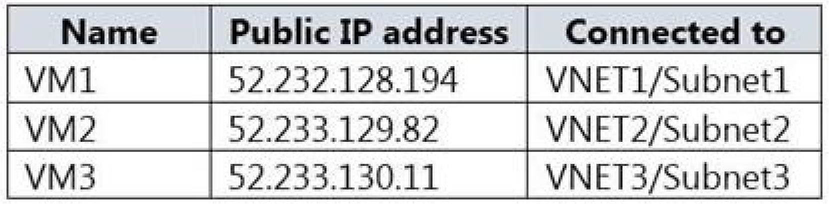
C. Export the public key from the on-premises server and save the key as a CER file.

D. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using AES256.

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

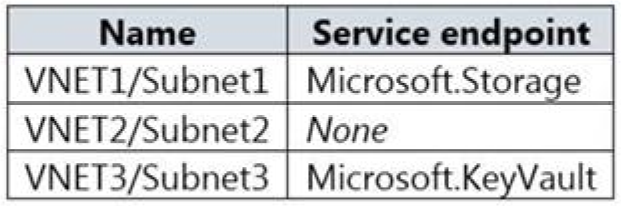
**QUESTION 57**

HOTSPOT
You have an Azure subscription that contains a storage account named storage1 and several virtual machines. The storage account and virtual machines are in the same Azure region. The network configurations of the virtual machines are shown in the following table.



| Name | Public IP address | Connected to |
|---|---|---|
| VM1 | 52.232.128.194 | VNET1/Subnet1 |
| VM2 | 52.233.129.82 | VNET2/Subnet2 |
| VM3 | 52.233.130.11 | VNET3/Subnet3 |

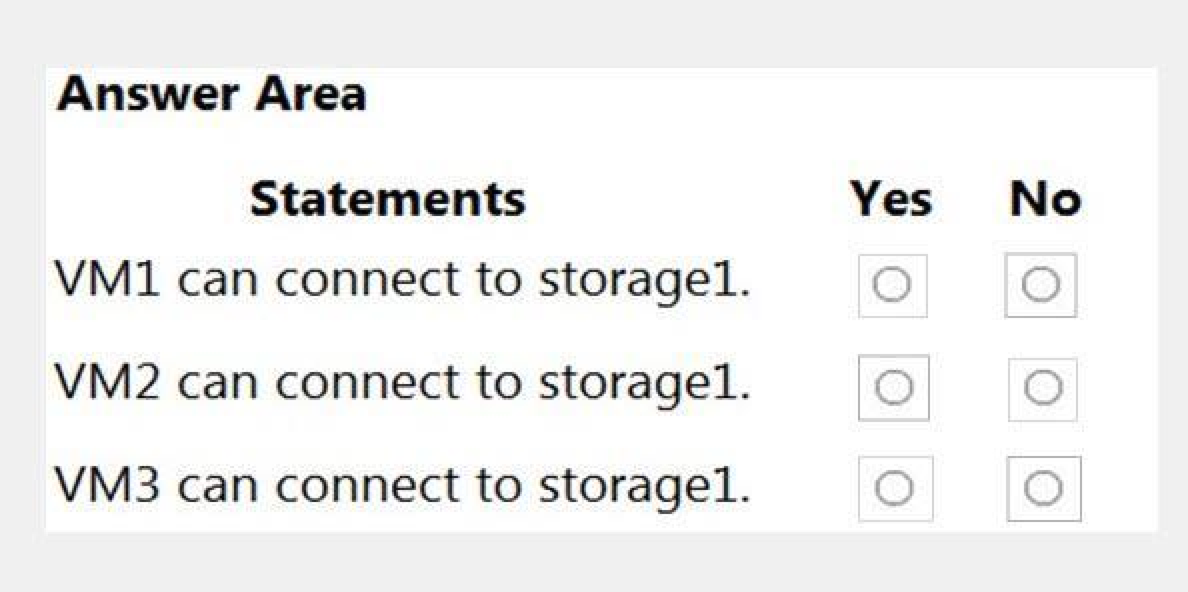
The virtual network subnets have service endpoints defined as shown in the following table.



| Name | Service endpoint |
|---|---|
| VNET1/Subnet1 | Microsoft.Storage |
| VNET2/Subnet2 | *None* |
| VNET3/Subnet3 | Microsoft.KeyVault |

You configure the following Firewall and virtual networks settings for storage1:
Allow access from: Selected networks
Virtual networks: VNET3\Subnet3
Firewall – Address range: 52.233.129.0/24
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

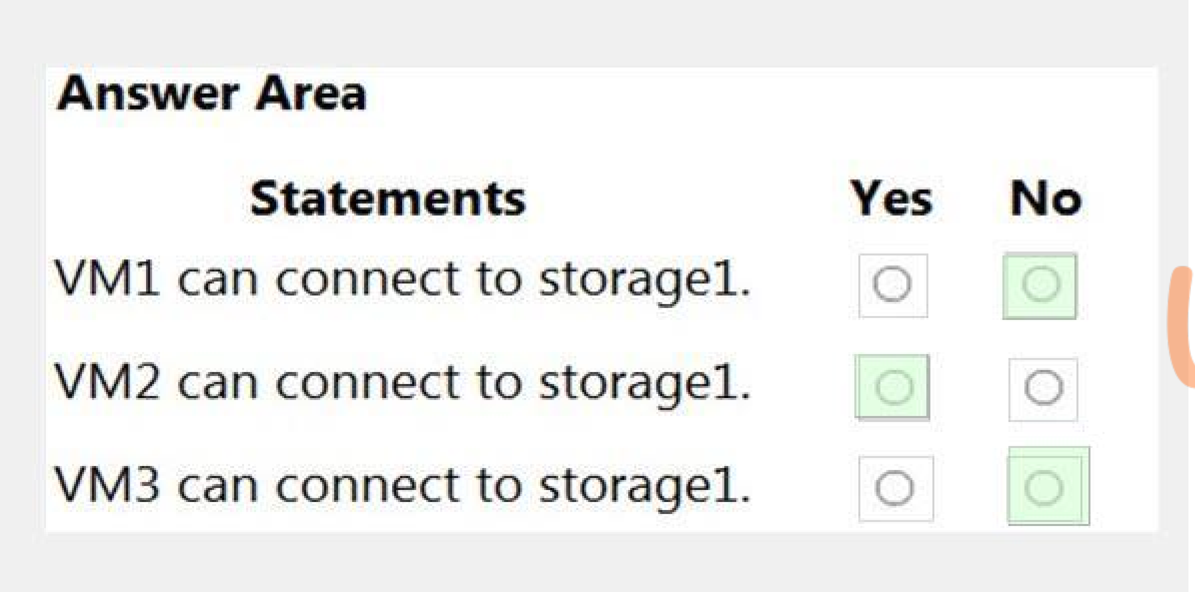
**Hot Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| VM1 can connect to storage1. | ○ | ○ |
| VM2 can connect to storage1. | ○ | ○ |
| VM3 can connect to storage1. | ○ | ○ |

**Answer Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| VM1 can connect to storage1. | ○ | [✓ ○] |
| VM2 can connect to storage1. | [✓ ○] | ○ |
| VM3 can connect to storage1. | ○ | [✓ ○] |

**Section:**

**Explanation:**

Box 1: No

VNet1 has a service endpoint configure for Azure Storage. However, the Azure storage does not allow access from VNet1 or the public IP address of VM1.

Box 2: Yes

VNet2 does not have a service endpoint configured. However, the Azure storage allows access from the public IP address of VM2.

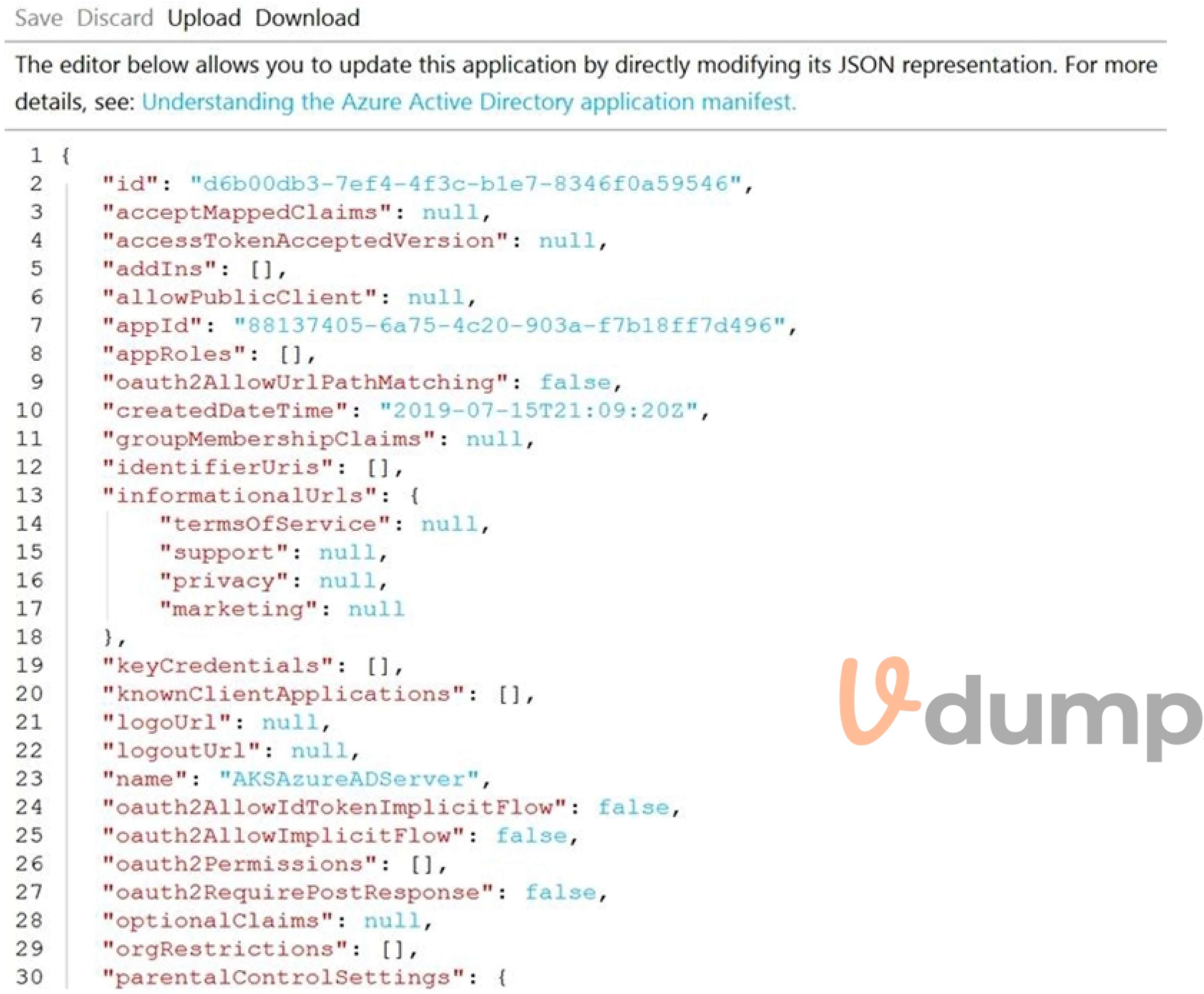
Box 3: No

Azure storage allows access from VNet3. However, VNet3 does not have a service endpoint for Azure storage. The Azure storage also does not allow access from the public IP of VM3.

**QUESTION 58**

You plan to create an Azure Kubernetes Service (AKS) cluster in an Azure subscription.

The manifest of the registered server application is shown in the following exhibit.



The editor below allows you to update this application by directly modifying its JSON representation. For more details, see: Understanding the Azure Active Directory application manifest.

```
{
    "id": "d6b00db3-7ef4-4f3c-b1e7-8346f0a59546",
    "acceptMappedClaims": null,
    "accessTokenAcceptedVersion": null,
    "addIns": [],
    "allowPublicClient": null,
    "appId": "88137405-6a75-4c20-903a-f7b18ff7d496",
    "appRoles": [],
    "oauth2AllowUrlPathMatching": false,
    "createdDateTime": "2019-07-15T21:09:20Z",
    "groupMembershipClaims": null,
    "identifierUris": [],
    "informationalUrls": {
        "termsOfService": null,
        "support": null,
        "privacy": null,
        "marketing": null
    },
    "keyCredentials": [],
    "knownClientApplications": [],
    "logoUrl": null,
    "logoutUrl": null,
    "name": "AKSAzureADServer",
    "oauth2AllowIdTokenImplicitFlow": false,
    "oauth2AllowImplicitFlow": false,
    "oauth2Permissions": [],
    "oauth2RequirePostResponse": false,
    "optionalClaims": null,
    "orgRestrictions": [],
    "parentalControlSettings": {
```

You need to ensure that the AKS cluster and Azure Active Directory (Azure AD) are integrated.
Which property should you modify in the manifest?

A. accessTokenAcceptedVersion

B. keyCredentials

C. groupMembershipClaims

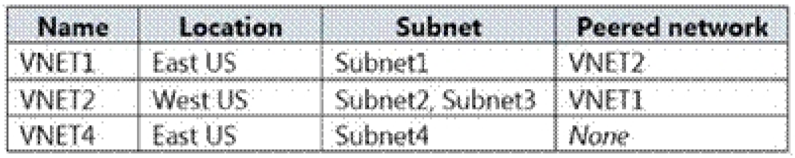
D. acceptMappedClaims

**Correct Answer: C**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli
https://www.codeproject.com/Articles/3211864/Operation-and-Maintenance-of-AKS-Applications

**QUESTION 59**

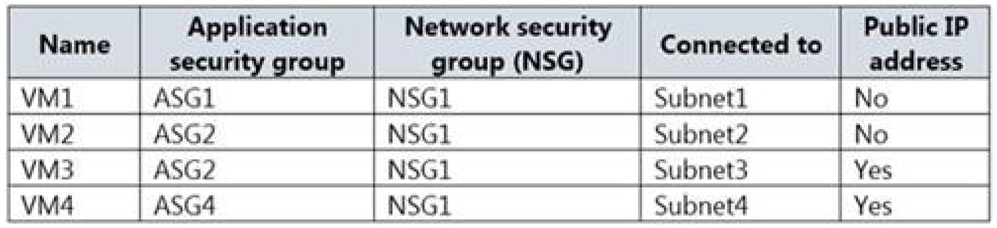
HOTSPOT

You have the Azure virtual networks shown in the following table.



| Name | Location | Subnet | Peered network |
|---|---|---|---|
| VNET1 | East US | Subnet1 | VNET2 |
| VNET2 | West US | Subnet2, Subnet3 | VNET1 |
| VNET4 | East US | Subnet4 | *None* |

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

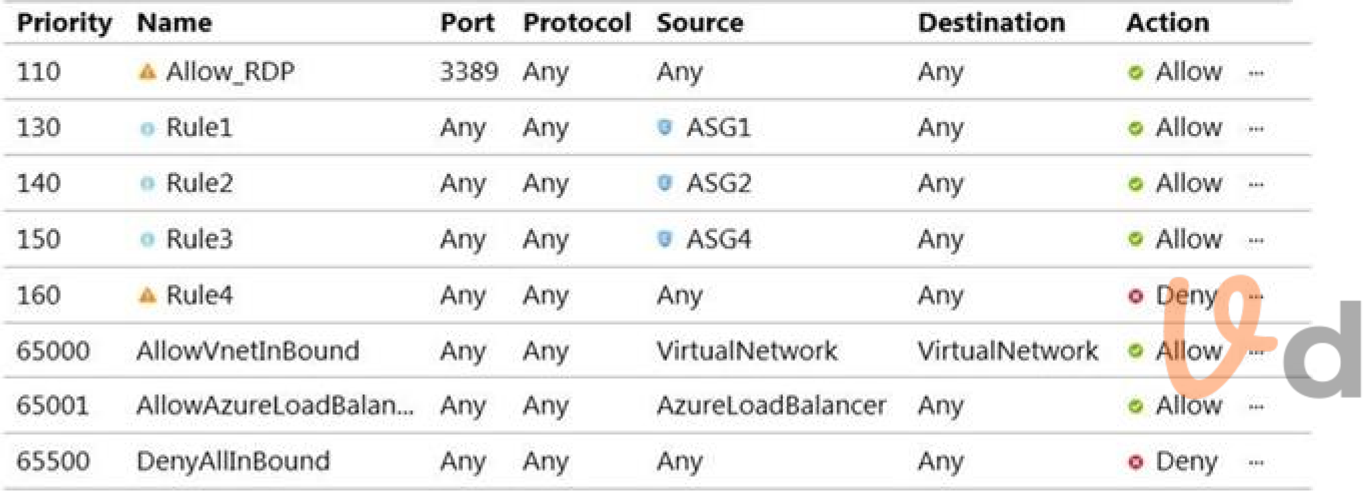


| Name | Application security group | Network security group (NSG) | Connected to | Public IP address |
|---|---|---|---|---|
| VM1 | ASG1 | NSG1 | Subnet1 | No |
| VM2 | ASG2 | NSG1 | Subnet2 | No |
| VM3 | ASG2 | NSG1 | Subnet3 | Yes |
| VM4 | ASG4 | NSG1 | Subnet4 | Yes |

The firewalls on all the virtual machines allow ping traffic.

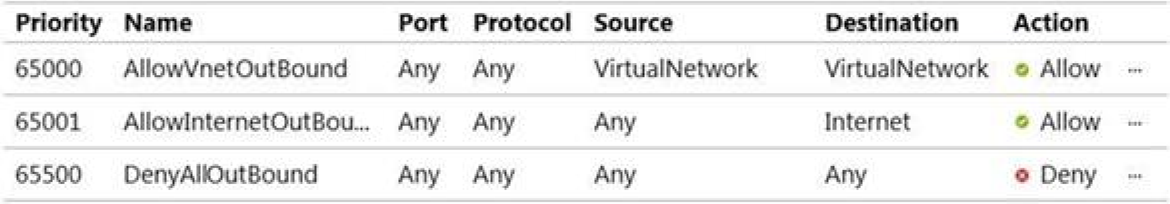
NSG1 is configured as shown in the following exhibit.

Inbound security rules



| Priority | Name | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|---|
| 110 | Allow_RDP | 3389 | Any | Any | Any | Allow ··· |
| 130 | Rule1 | Any | Any | ASG1 | Any | Allow ··· |
| 140 | Rule2 | Any | Any | ASG2 | Any | Allow ··· |
| 150 | Rule3 | Any | Any | ASG4 | Any | Allow ··· |
| 160 | Rule4 | Any | Any | Any | Any | Deny ··· |
| 65000 | AllowVnetInBound | Any | Any | VirtualNetwork | VirtualNetwork | Allow ··· |
| 65001 | AllowAzureLoadBalan... | Any | Any | AzureLoadBalancer | Any | Allow ··· |
| 65500 | DenyAllInBound | Any | Any | Any | Any | Deny ··· |

Outbound security rules

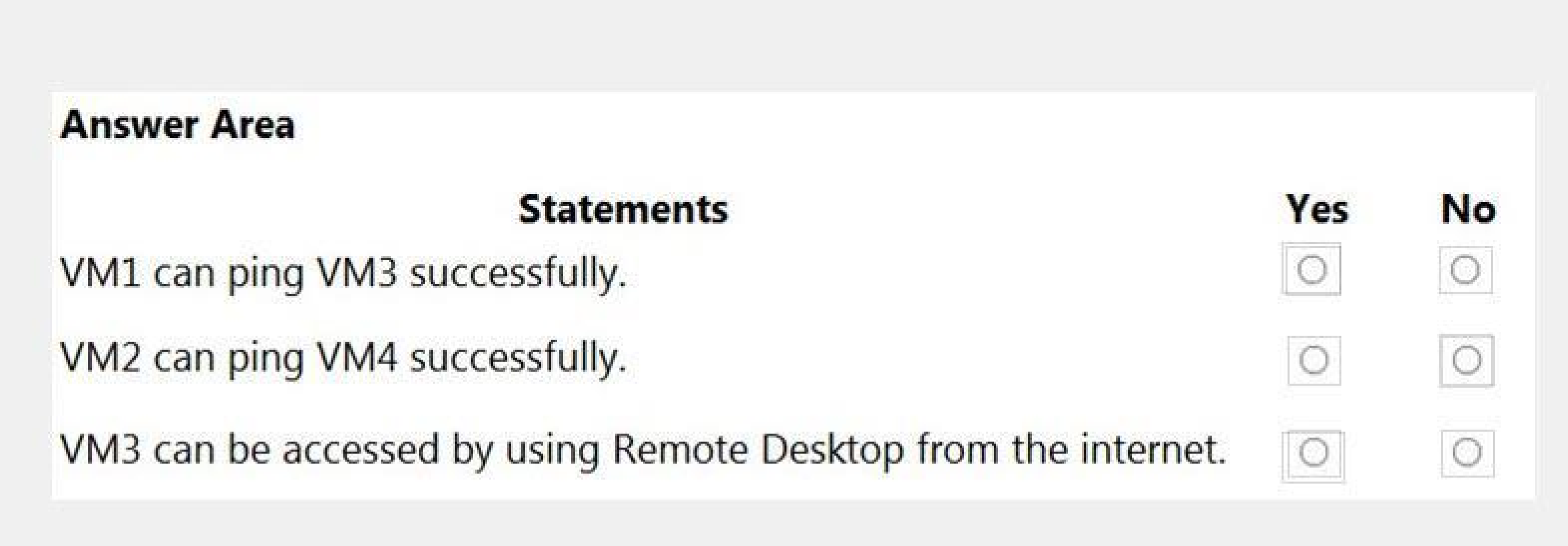


| Priority | Name | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|---|
| 65000 | AllowVnetOutBound | Any | Any | VirtualNetwork | VirtualNetwork | Allow ··· |
| 65001 | AllowInternetOutBou... | Any | Any | Any | Internet | Allow ··· |
| 65500 | DenyAllOutBound | Any | Any | Any | Any | Deny ··· |

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

NOTE: Each correct selection is worth one point.

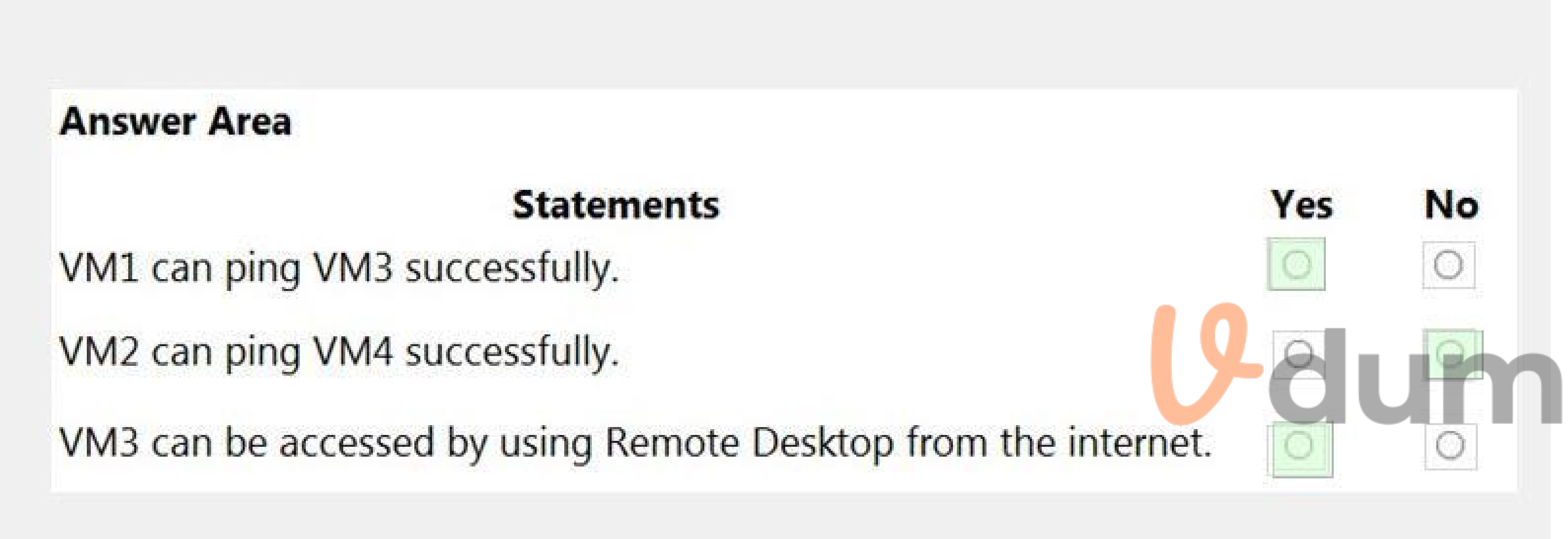
**Hot Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| VM1 can ping VM3 successfully. | ○ | ○ |
| VM2 can ping VM4 successfully. | ○ | ○ |
| VM3 can be accessed by using Remote Desktop from the internet. | ○ | ○ |

**Answer Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| VM1 can ping VM3 successfully. | ● | ○ |
| VM2 can ping VM4 successfully. | ○ | ● |
| VM3 can be accessed by using Remote Desktop from the internet. | ● | ○ |

**Section:**

**Explanation:**

Box 1: Yes

VM1 and VM3 are on peered VNets. The firewall rules with a source of ASG1 and ASG2 allow 'any' traffic on 'any' protocol so pings are allowed between VM1 and VM3.

Box 2: No

VM2 and VM4 are on separate VNets and the VNets are not peered. Therefore, the pings would have to go over the Internet. VM4 does have a public IP and the firewall allows pings. However, for VM2 to be able to ping VM4, VM2 would also need a public IP address. In Azure, pings don't go out through the default gateway as they would in a physical network. For an Azure VM to ping external IPs, the VM must have a public IP address assigned to it.

Box 3: Yes

VM3 has a public IP address and the firewall allows traffic on port 3389.

**QUESTION 60**

You have an Azure subscription that contains two virtual machines named VM1 and VM2 that run Windows Server 2019.

You are implementing Update Management in Azure Automation.

You plan to create a new update deployment named Update1.

You need to ensure that Update1 meets the following requirements:

Automatically applies updates to VM1 and VM2.

Automatically adds any new Windows Server 2019 virtual machines to Update1.

What should you include in Update1?

A. a security group that has a Membership type of Assigned
B. a security group that has a Membership type of Dynamic Device
C. a dynamic group query
D. a Kusto query language query

**Correct Answer: C**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/automation/update-management/configure-groups

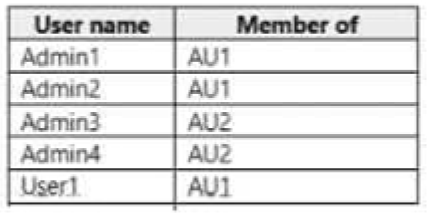
**QUESTION 61**
You have multiple development teams that will create apps in Azure.
You plan to create a standard development environment that will be deployed for each team.
You need to recommend a solution that will enforce resource locks across the development environments and ensure that the locks are applied in a consistent manner.
What should you include in the recommendation?

A. an Azure policy
B. an Azure Resource Manager template
C. a management group
D. an Azure blueprint

**Correct Answer: D**
**Section:**
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

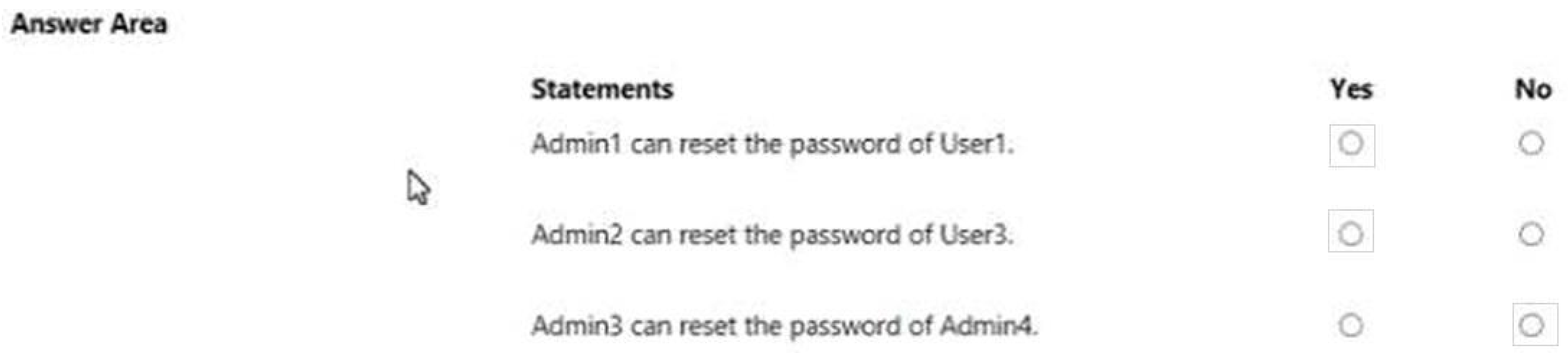
**Exam I**

**QUESTION 1**
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant that contains two administrative units named AU1 and AU2. Users are assigned to the administrative units as shown in the following table.



| User name | Member of |
|---|---|
| Admin1 | AU1 |
| Admin2 | AU1 |
| Admin3 | AU2 |
| Admin4 | AU2 |
| User1 | AU1 |

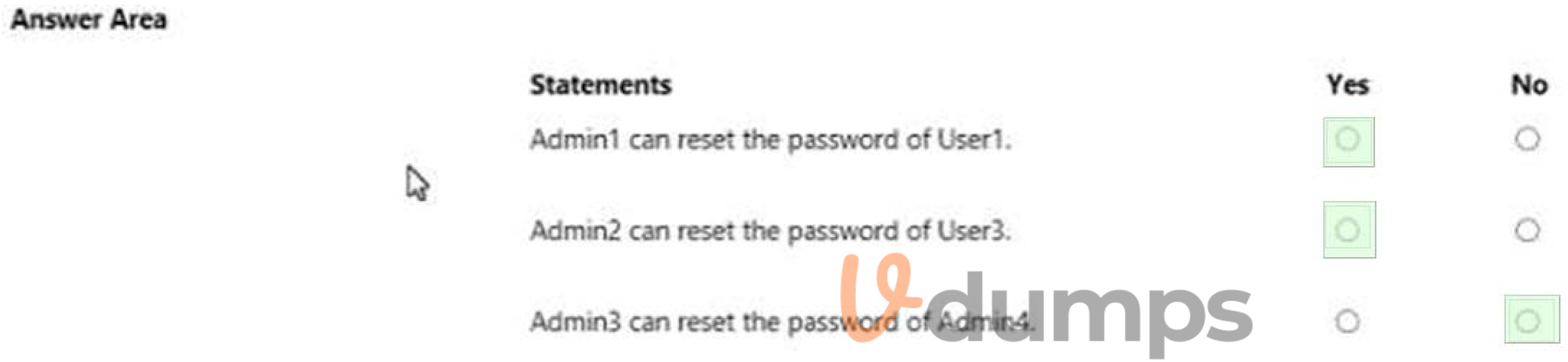
**Hot Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| Admin1 can reset the password of User1. | ○ | ○ |
| Admin2 can reset the password of User3. | ○ | ○ |
| Admin3 can reset the password of Admin4. | ○ | ○ |

**Answer Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| Admin1 can reset the password of User1. | [✓ ○] | ○ |
| Admin2 can reset the password of User3. | [✓ ○] | ○ |
| Admin3 can reset the password of Admin4. | ○ | [✓ ○] |

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

**QUESTION 2**
You have an Azure subscription that uses Microsoft Sentinel.
You need to create a Microsoft Sentinel notebook that will use the Guided Investigation - Anomaly Lookup template. What should you create first?

A. an analytics rule
B. a Log Analytics workspace
C. an Azure Machine Learning workspace
D. a hunting query

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

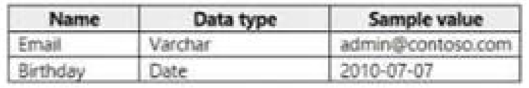
**QUESTION 3**
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.
You need to ensure that User1 can create and manage administrative units. The solution must use the principle of least privilege.
Which role should you assign to User1?

A. Privileged role administrator

B. Helpdesk administrator
C. Global administrator
D. Security administrator

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

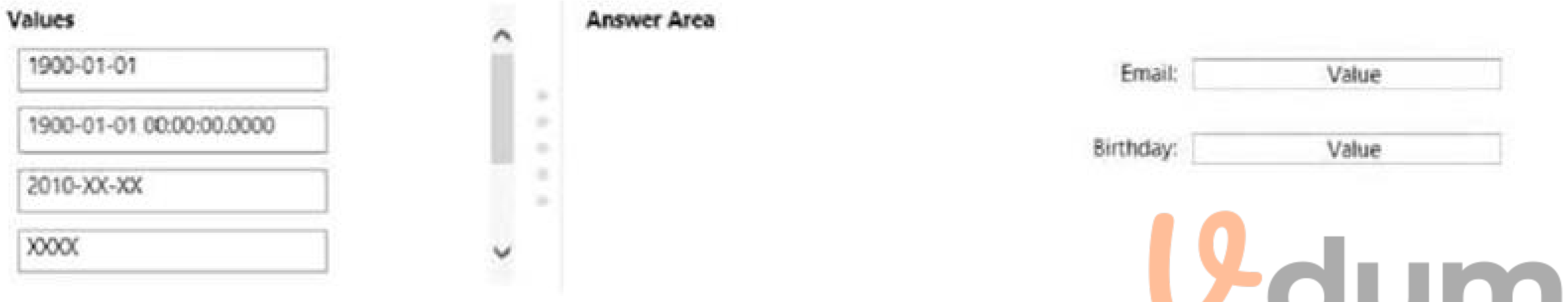
**QUESTION 4**
DRAG DROP
You have an Azure subscription that contains an Azure SQL database named SQLDB1. SQLDB1 contains the columns shown in the following table.



| Name | Data type | Sample value |
|---|---|---|
| Email | Varchar | admin@contoso.com |
| Birthday | Date | 2010-07-07 |

For the Email and Birthday columns, you implement dynamic data masking by using the default masking function. Which value will the users see in each column? To answer, drag the appropriate values to the correct columns. 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:**



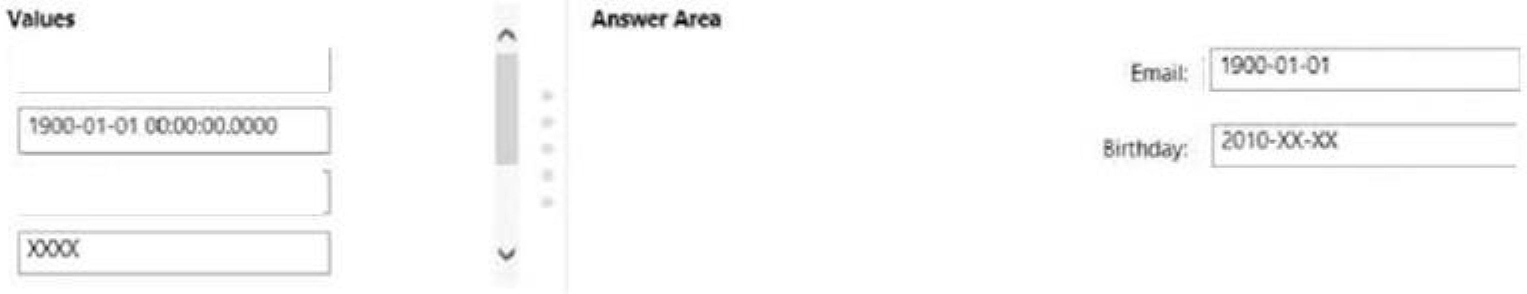
Values

1900-01-01
1900-01-01 00:00:00.0000
2010-XX-XX
XXXX

Answer Area

Email: Value
Birthday: Value

**Correct Answer:**



Values

1900-01-01 00:00:00.0000
XXXX

Answer Area

Email: 1900-01-01
Birthday: 2010-XX-XX

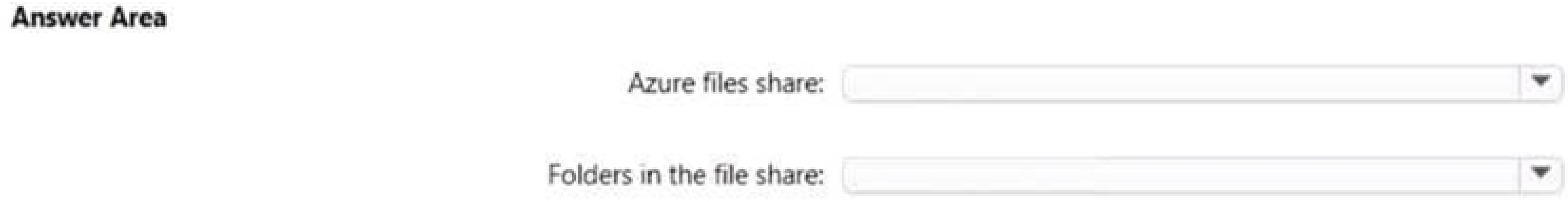
**Section:**
**Explanation:**

**QUESTION 5**
You have an Azure subscription that contains the resources shown in the following Table.
You plan to enable Microsoft Defender for Cloud for the subscription. Which resources can be protected by using Microsoft Defender for Cloud?

A. VM1, VNET1, and storage1 only
B. VM1, storage1, and Vault1 only
C. VM1.VNET1, storage1, and Vault1
D. VM1 and storage1 only
E. VM1 and VNET only

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

**QUESTION 6**
You have an Azure Active directory tenant that syncs with an Active Directory Domain Services (AD DS) domain. You plan to create an Azure file share that will contain folders and files.
Which identity store can you use to assign permissions to the Azure file share and folders within the share? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

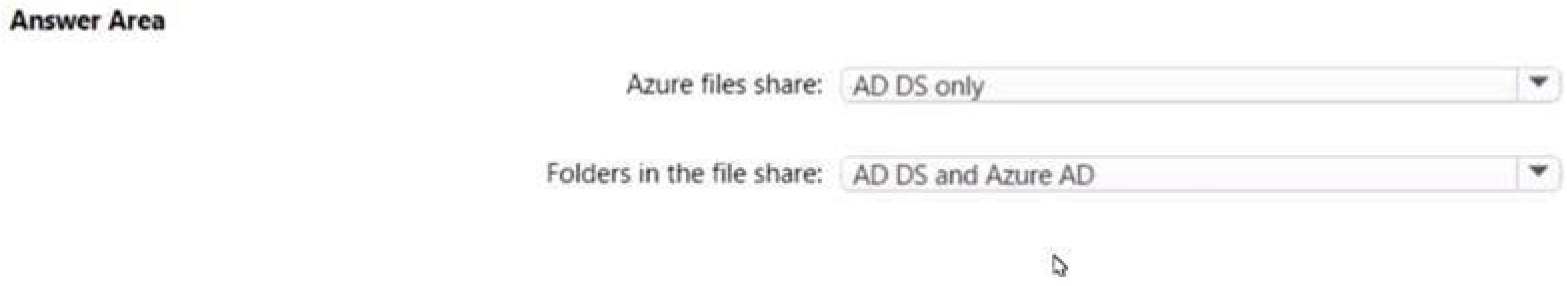


**Answer Area**

Azure files share:

Folders in the file share:

A.



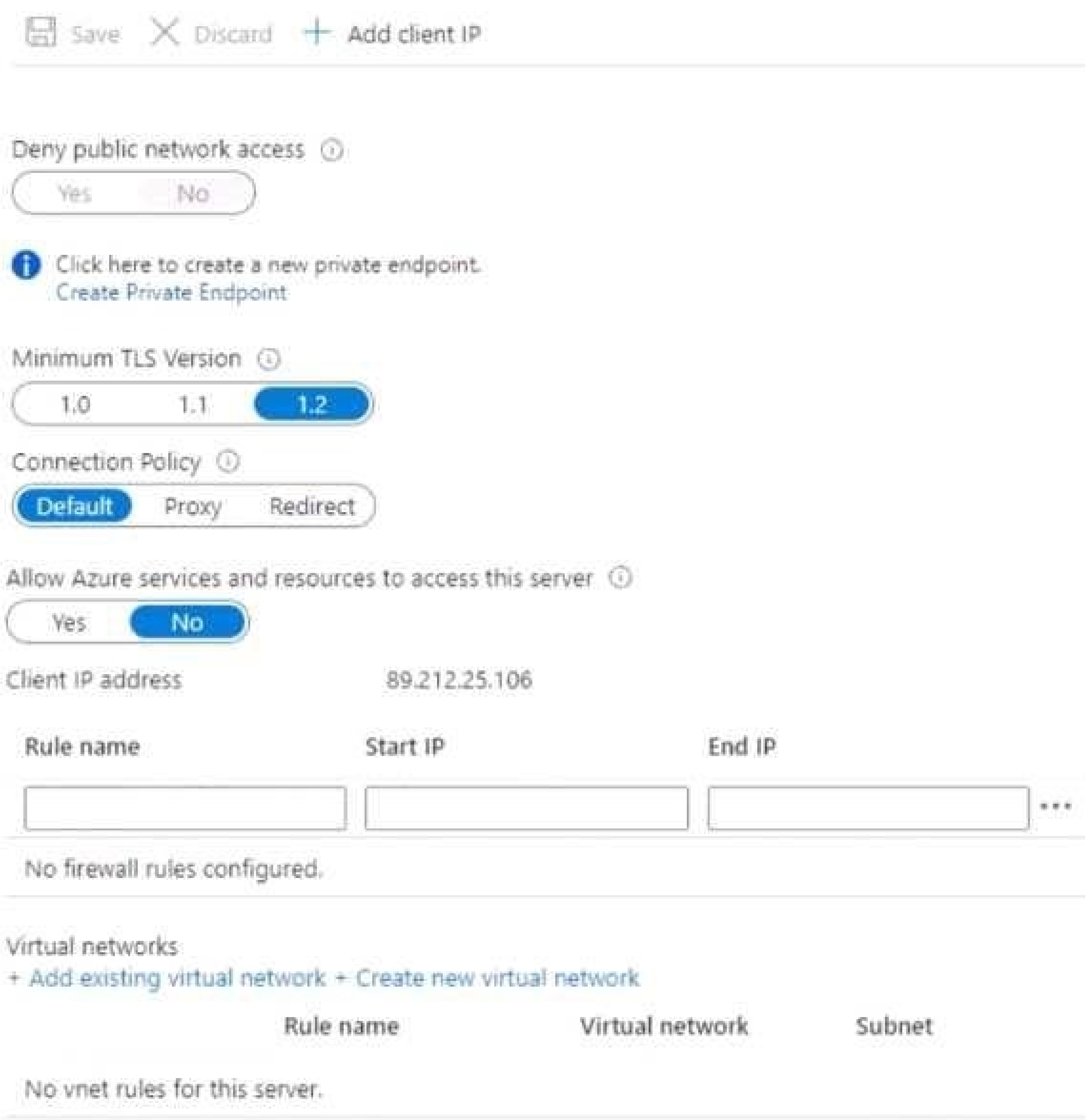
**Answer Area**

Azure files share: AD DS only

Folders in the file share: AD DS and Azure AD

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

**QUESTION 7**
You have an Azure subscription that contains an Azure SQL Database logic server named SQL1 and an Azure virtual machine named VM1. VM1 uses a private IP address only. The Firewall and virtual networks settings for SQL1 are shown in the following exhibit.



Save  Discard  + Add client IP

Deny public network access ⓘ

Yes  No

ⓘ Click here to create a new private endpoint.
Create Private Endpoint

Minimum TLS Version ⓘ

1.0  1.1  [✓ 1.2]

Connection Policy ⓘ

[✓ Default]  Proxy  Redirect

Allow Azure services and resources to access this server ⓘ

Yes  [✓ No]

Client IP address  89.212.25.106

| Rule name | Start IP | End IP |
|---|---|---|
| | | |

No firewall rules configured.

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

| Rule name | Virtual network | Subnet |
|---|---|---|

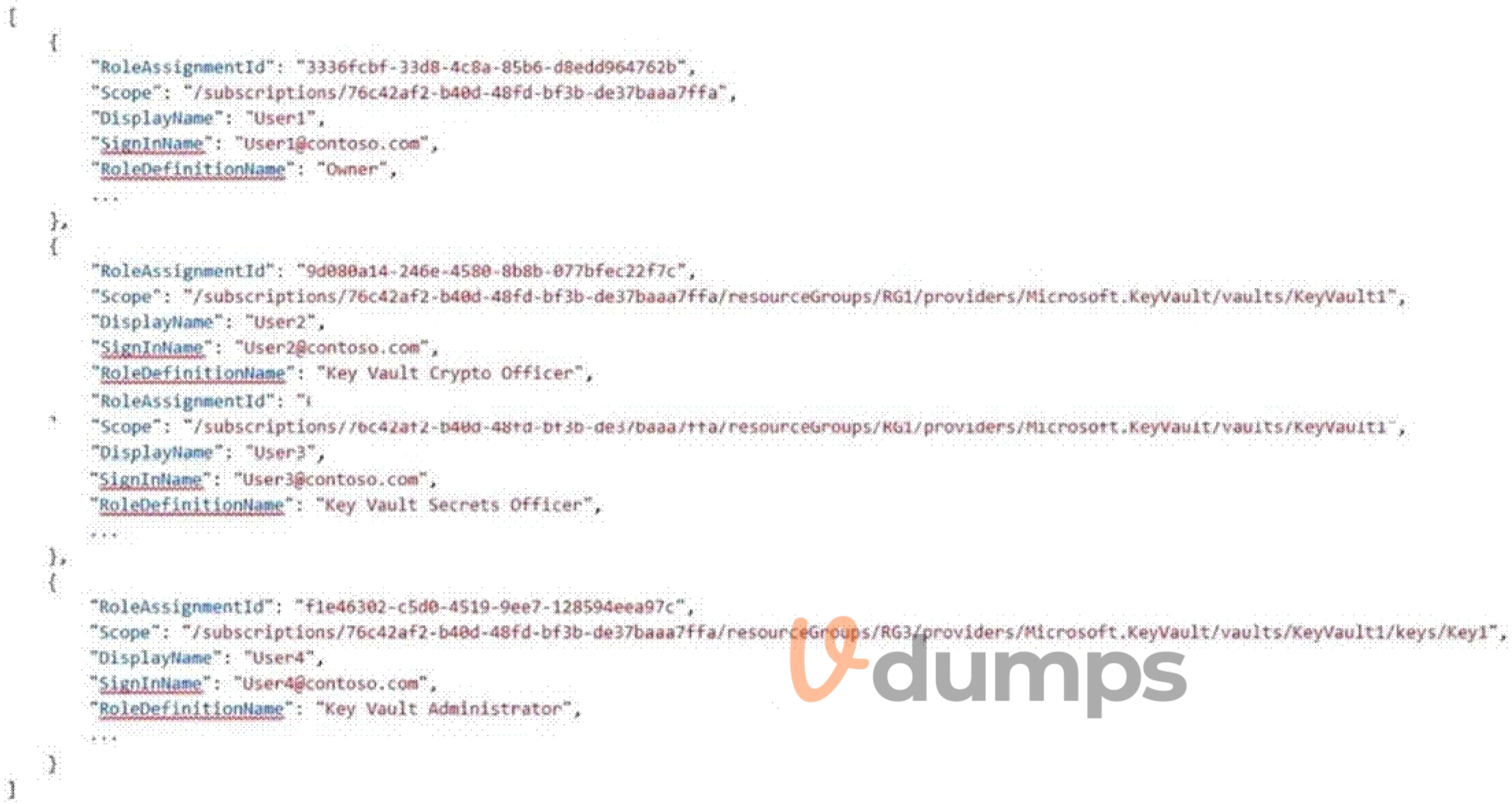
No vnet rules for this server.

You need to ensure that VM1 can connect to SQL1. The solution must use the principle of least privilege. What should you do?

A. Add an existing virtual network.
B. Set Connection Policy to Proxy.
C. Create a new firewall rule.
D. Set Allow Azure services and resources to access this server to Yes.

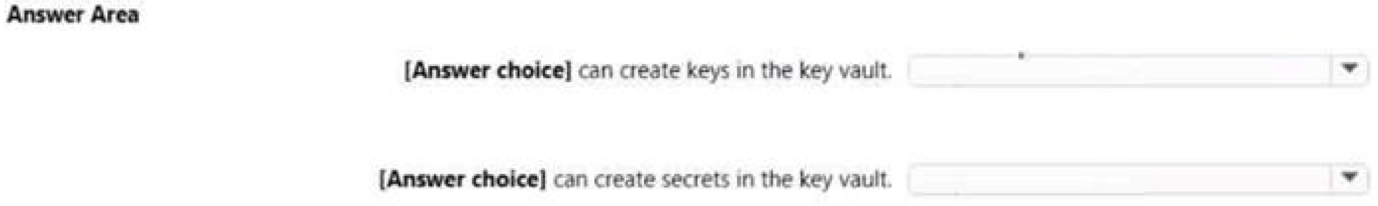
**Correct Answer: C**
**Section:**

**QUESTION 8**
You have an Azure subscription that contains an Azure key vault. The role assignments for the key vault are shown in the following exhibit.



```
[
    {
        "RoleAssignmentId": "3336fcbf-33d8-4c8a-85b6-d8edd964762b",
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa",
        "DisplayName": "User1",
        "SignInName": "User1@contoso.com",
        "RoleDefinitionName": "Owner",
        ...
    },
    {
        "RoleAssignmentId": "9d080a14-246e-4580-8b8b-077bfec22f7c",
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
        "DisplayName": "User2",
        "SignInName": "User2@contoso.com",
        "RoleDefinitionName": "Key Vault Crypto Officer",
        "RoleAssignmentId": "
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
        "DisplayName": "User3",
        "SignInName": "User3@contoso.com",
        "RoleDefinitionName": "Key Vault Secrets Officer",
        ...
    },
    {
        "RoleAssignmentId": "f1e46302-c5d0-4519-9ee7-128594eea97c",
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG3/providers/Microsoft.KeyVault/vaults/KeyVault1/keys/Key1",
        "DisplayName": "User4",
        "SignInName": "User4@contoso.com",
        "RoleDefinitionName": "Key Vault Administrator",
        ...
    }
]
```

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

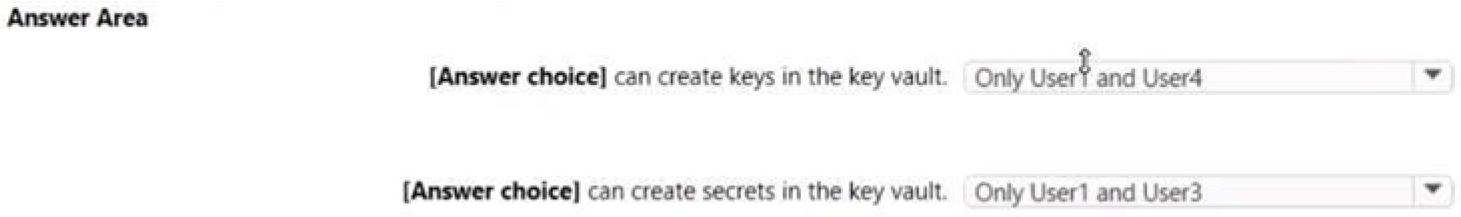


**Answer Area**

**[Answer choice]** can create keys in the key vault.

**[Answer choice]** can create secrets in the key vault.

A.



**Answer Area**

**[Answer choice]** can create keys in the key vault. Only User1 and User4

**[Answer choice]** can create secrets in the key vault. Only User1 and User3

**Correct Answer: A**

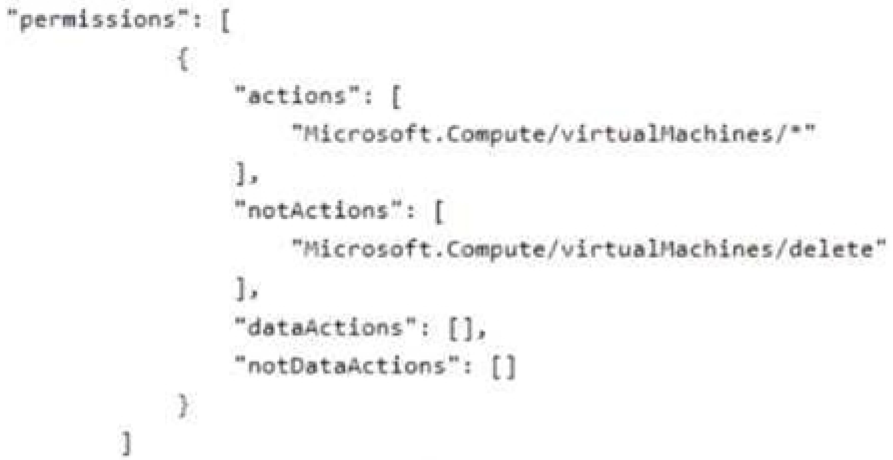
**Section:**

**QUESTION 9**

HOTSPOT

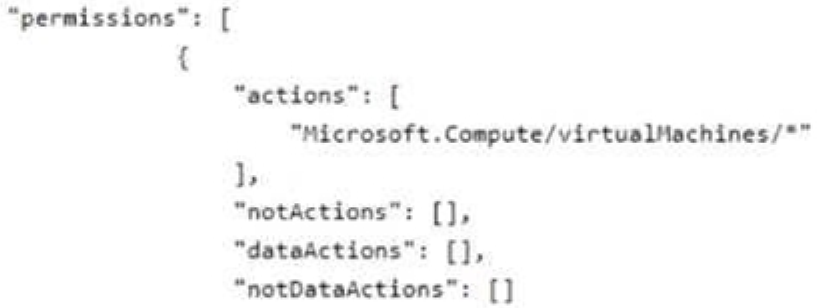
You have an Azure subscription that contains a resource group named RG1. RG1 contains a virtual machine named VM1 that uses Azure Active Directory (Azure AD) authentication. You have two custom Azure roles named Role1 and Role2 that are scoped to RG1.

The permissions for Role1 are shown in the following JSON code.



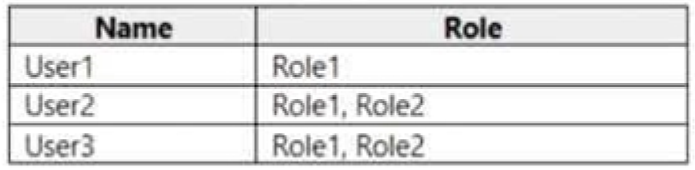
```
"permissions": [
            {
                "actions": [
                    "Microsoft.Compute/virtualMachines/*"
                ],
                "notActions": [
                    "Microsoft.Compute/virtualMachines/delete"
                ],
                "dataActions": [],
                "notDataActions": []
            }
        ]
```

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



```
"permissions": [
            {
                "actions": [
                    "Microsoft.Compute/virtualMachines/*"
                ],
                "notActions": [],
                "dataActions": [],
                "notDataActions": []
```

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

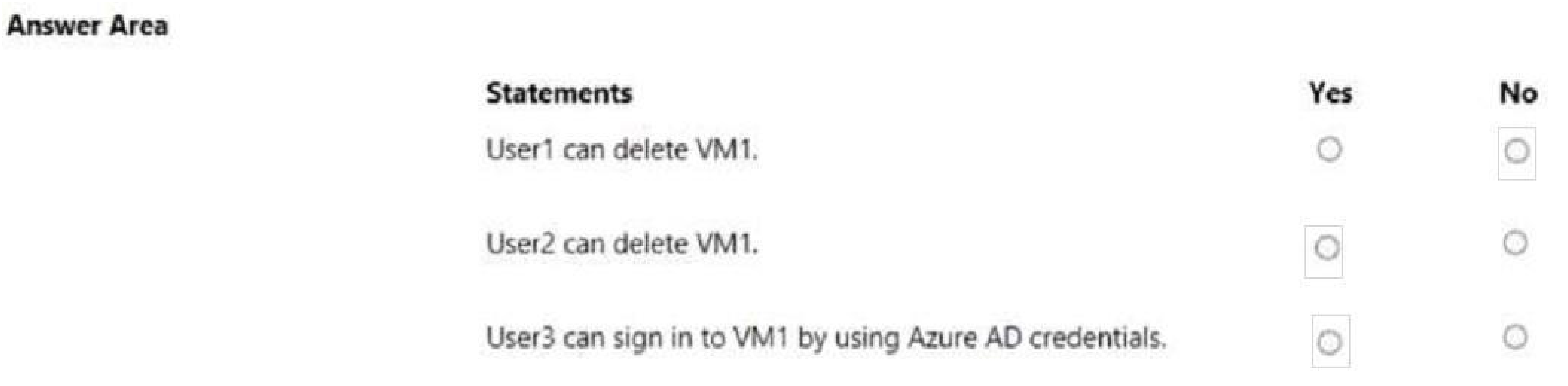


| Name | Role |
|---|---|
| User1 | Role1 |
| User2 | Role1, Role2 |
| User3 | Role1, Role2 |

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

NOTE: Each correct selection is worth one point.

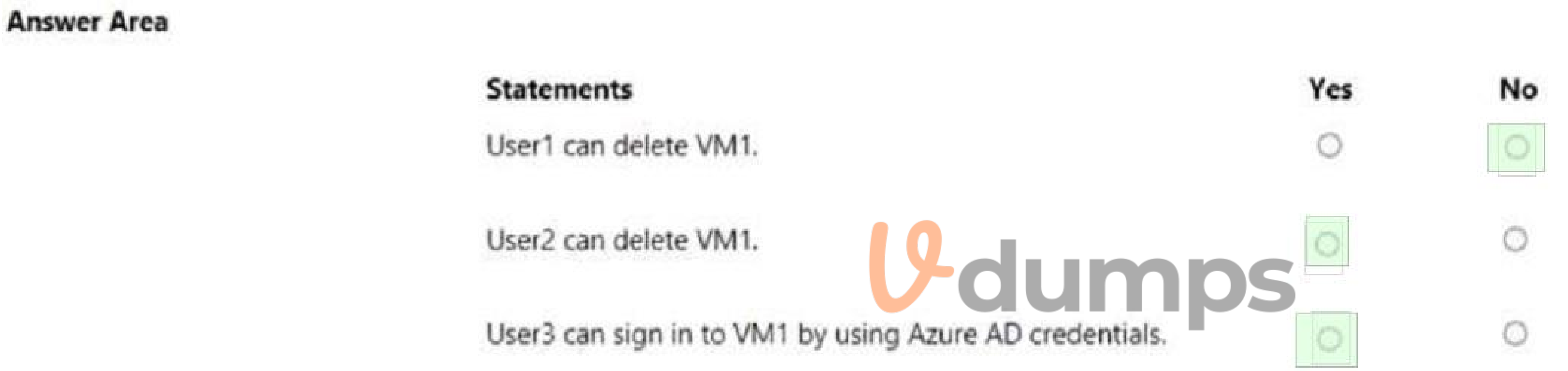
**Hot Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| User1 can delete VM1. | ○ | ○ |
| User2 can delete VM1. | ○ | ○ |
| User3 can sign in to VM1 by using Azure AD credentials. | ○ | ○ |

**Answer Area:**

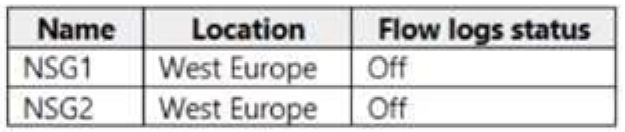


Answer Area

| Statements | Yes | No |
|---|---|---|
| User1 can delete VM1. | ○ | [✓ ○] |
| User2 can delete VM1. | [✓ ○] | ○ |
| User3 can sign in to VM1 by using Azure AD credentials. | [✓ ○] | ○ |

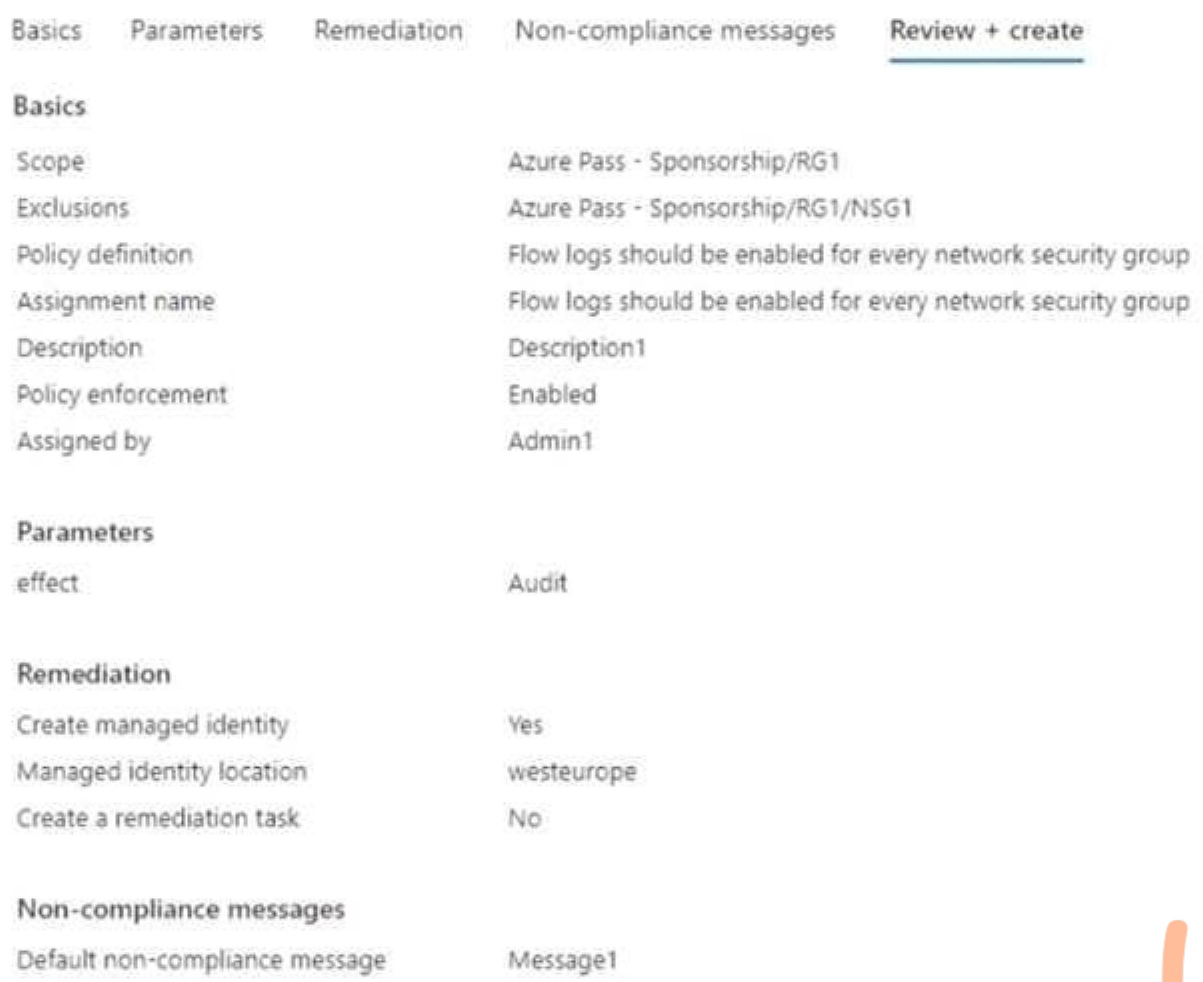
**Section:**
**Explanation:**

**QUESTION 10**
You have an Azure subscription that contains a resource group named RG1 and the network security groups (NSGs) shown in the following table.



| Name | Location | Flow logs status |
|---|---|---|
| NSG1 | West Europe | Off |
| NSG2 | West Europe | Off |

You create the Azure policy shown in the following exhibit.



**Basics**

| | |
|---|---|
| Scope | Azure Pass - Sponsorship/RG1 |
| Exclusions | Azure Pass - Sponsorship/RG1/NSG1 |
| Policy definition | Flow logs should be enabled for every network security group |
| Assignment name | Flow logs should be enabled for every network security group |
| Description | Description1 |
| Policy enforcement | Enabled |
| Assigned by | Admin1 |

**Parameters**

| | |
|---|---|
| effect | Audit |

**Remediation**

| | |
|---|---|
| Create managed identity | Yes |
| Managed identity location | westeurope |
| Create a remediation task | No |

**Non-compliance messages**

| | |
|---|---|
| Default non-compliance message | Message1 |

You assign the policy to RG1.
What will occur if you assign the policy to NSG1 and NSG2?

A. Flow logs will be enabled for NSG1 and NSG2.

B. Flow logs will be enabled for NSG2 only

C. Flow logs will be disabled for NSG1 and NSG2.

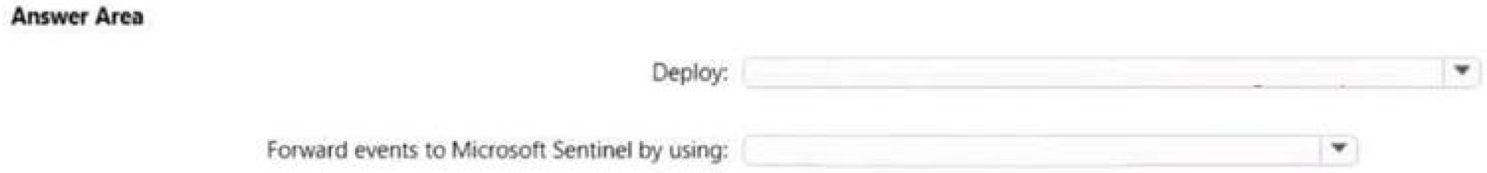
D. Flow logs will be enabled for NSG1 only.

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

**QUESTION 11**

You have a Microsoft Sentinel deployment.

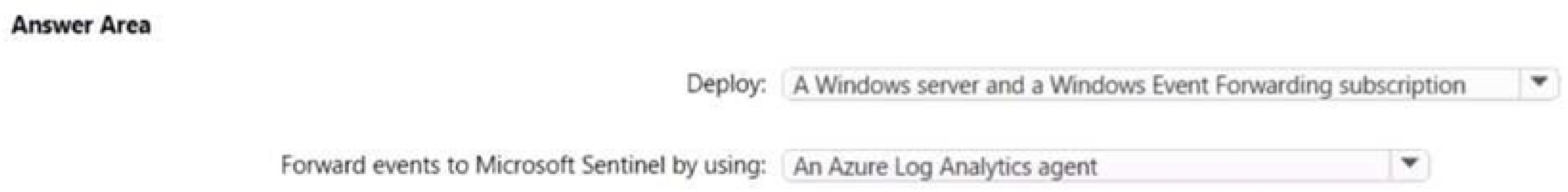
You need to connect a third-party security solution to the deployment. The third-party solution will send Common Event Format (CER-formatted messages. What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.


**Answer Area**

Deploy:

Forward events to Microsoft Sentinel by using:

A.



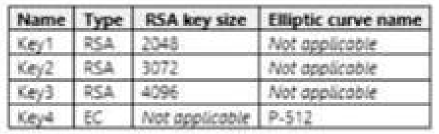
**Answer Area**

Deploy: A Windows server and a Windows Event Forwarding subscription

Forward events to Microsoft Sentinel by using: An Azure Log Analytics agent

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

**QUESTION 12**
You have an Azure subscription that contains an Azure SQL database named SQL1 and an Azure key vault named KeyVault1. KeyVault1 stores the keys shown in the following table.



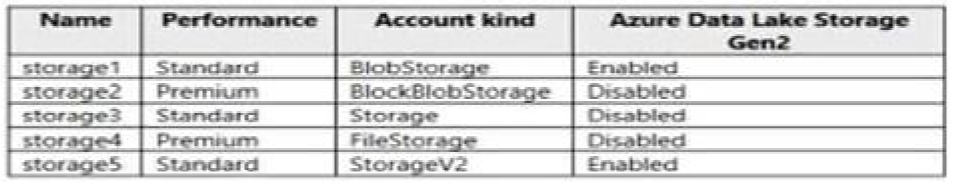
| Name | Type | RSA key size | Elliptic curve name |
|---|---|---|---|
| Key1 | RSA | 2048 | *Not applicable* |
| Key2 | RSA | 3072 | *Not applicable* |
| Key3 | RSA | 4096 | *Not applicable* |
| Key4 | EC | *Not applicable* | P-512 |

You reed to configure Transparent Data Encryption (TDE). TDE will use a customer-managed key for SQL1?

A. Key1. Key2 Key3. and Key4
B. Key1 only
C. Key2 only
D. Key1 and key2 only
E. Key2 and Key3 only

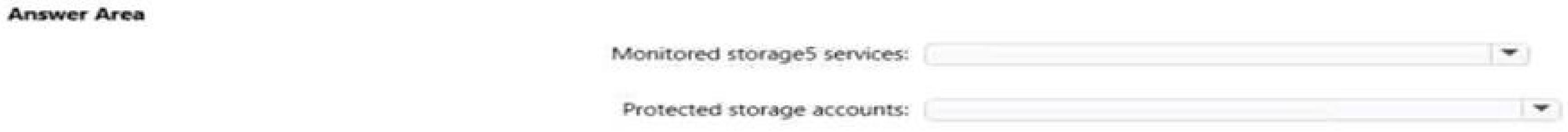
**Correct Answer: E**
**Section:**

**QUESTION 13**
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 Microsoft Defender for Storage.
Which storage services of storages are monitored by Microsoft Defender for Storage, and which storage accounts are protected by Microsoft Defender for Storage? To answer, select the appropriate options in the answer area.

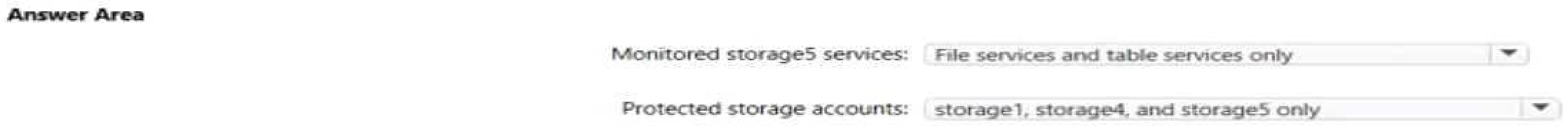


**Answer Area**

Monitored storage5 services:

Protected storage accounts:

A.



**Answer Area**

Monitored storage5 services: File services and table services only

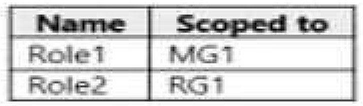
Protected storage accounts: storage1, storage4, and storage5 only

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

**QUESTION 14**

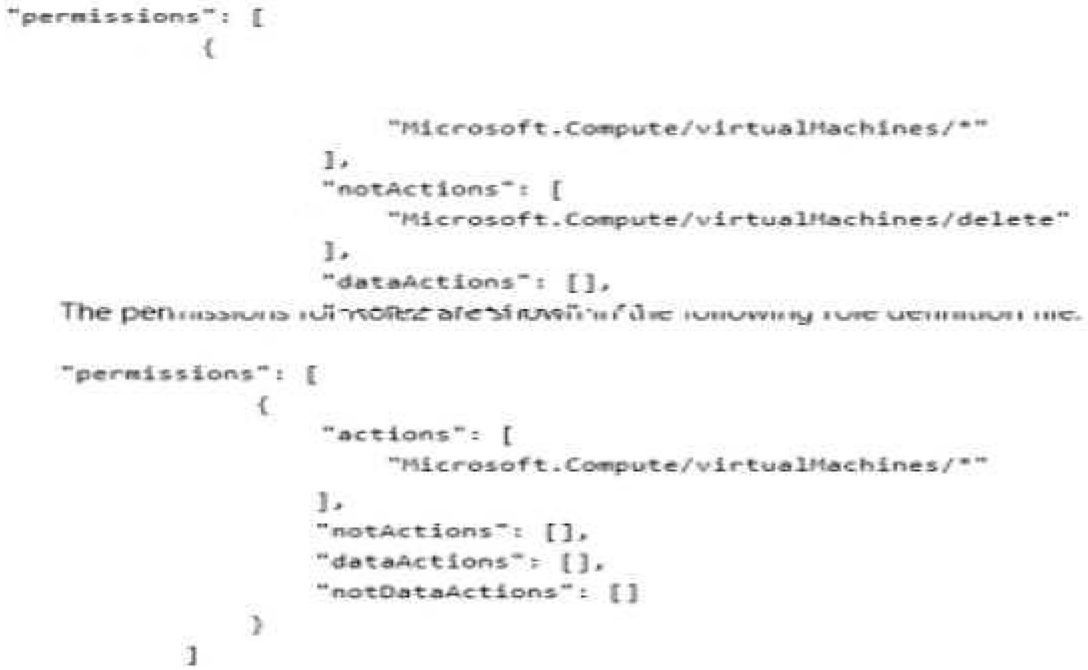
HOTSPOT

You have a management group named MG1 that contains an Azure subscription and a resource group named RG1. RG1 contains a virtual machine named VM1. You have the custom Azure roles shown in the following table.



| Name | Scoped to |
|---|---|
| Role1 | MG1 |
| Role2 | RG1 |

The permissions for Role1 are shown in the following role definition file.

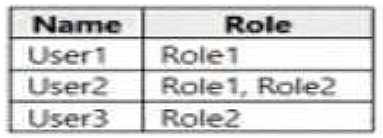


```
"permissions": [
        {


                  "Microsoft.Compute/virtualMachines/*"
              ],
              "notActions": [
                  "Microsoft.Compute/virtualMachines/delete"
              ],
              "dataActions": [],
```

The permissions for Role2 are shown in the following role definition file.

```
"permissions": [
         {
              "actions": [
                  "Microsoft.Compute/virtualMachines/*"
              ],
              "notActions": [],
              "dataActions": [],
              "notDataActions": []
         }
    ]
```

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

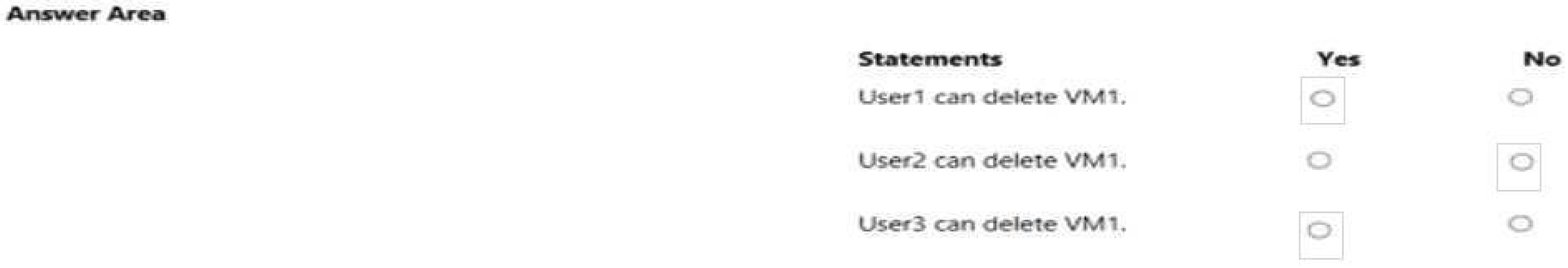


| Name | Role |
|---|---|
| User1 | Role1 |
| User2 | Role1, Role2 |
| User3 | Role2 |

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

NOTE: Each correct selection is worth one point.

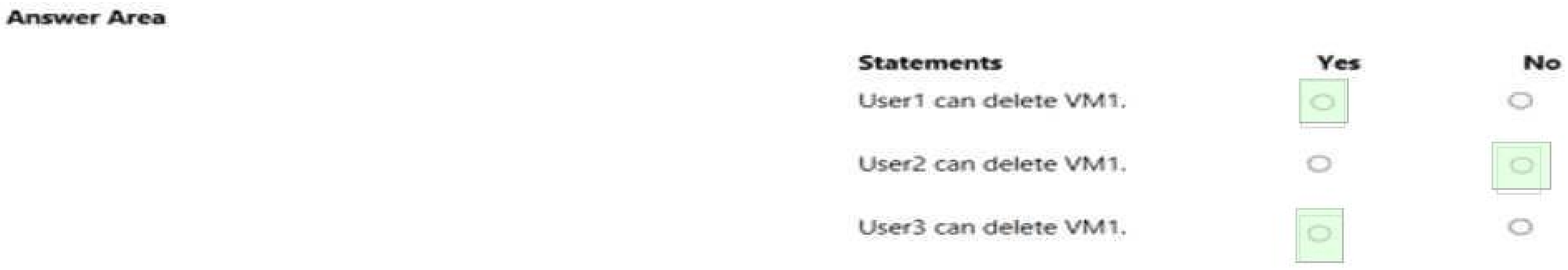
**Hot Area:**



**Answer Area**

| Statements | Yes | No |
|---|---|---|
| User1 can delete VM1. | ○ | ○ |
| User2 can delete VM1. | ○ | ○ |
| User3 can delete VM1. | ○ | ○ |

**Answer Area:**

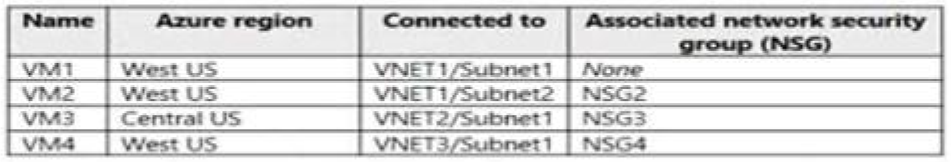


Answer Area

| Statements | Yes | No |
|---|---|---|
| User1 can delete VM1. | [✓ ○] | ○ |
| User2 can delete VM1. | ○ | [✓ ○] |
| User3 can delete VM1. | [✓ ○] | ○ |

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

**QUESTION 15**
You have an Azure subscription that contains the virtual machines shown in the following table.

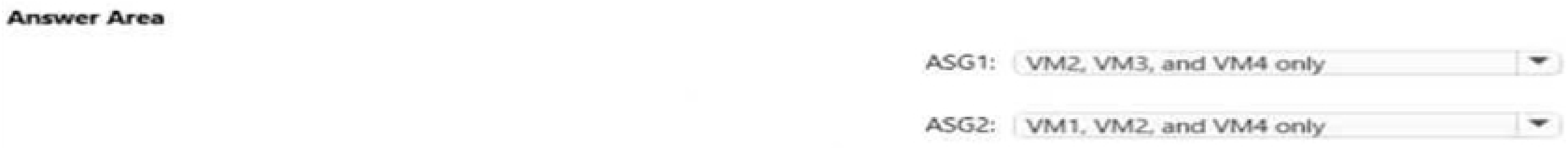


| Name | Azure region | Connected to | Associated network security group (NSG) |
|---|---|---|---|
| VM1 | West US | VNET1/Subnet1 | *None* |
| VM2 | West US | VNET1/Subnet2 | NSG2 |
| VM3 | Central US | VNET2/Subnet1 | NSG3 |
| VM4 | West US | VNET3/Subnet1 | NSG4 |

VNET1, VNET2, and VNET3 are peered with each other. You perform the following actions:
* Create two application security groups named ASG1 and ASG2 in the West US region.
* Add the network interface of VM1 to ASG1.

Answer Area

A.



Answer Area

ASG1: VM2, VM3, and VM4 only

ASG2: VM1, VM2, and VM4 only

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

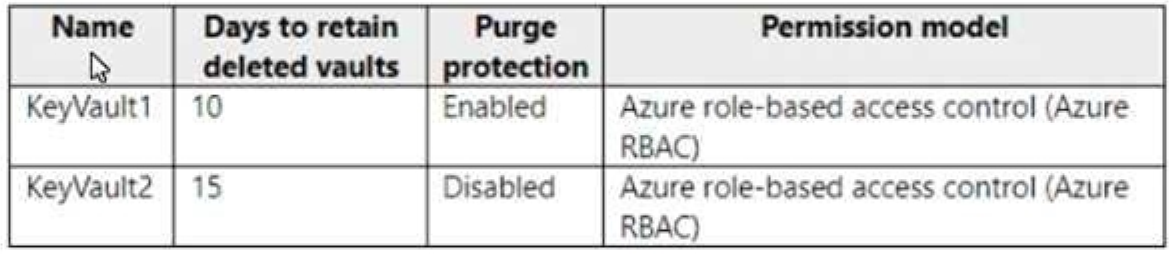
**QUESTION 16**
You have 15 Azure virtual machines in a resource group named RG1.
All virtual machines run identical applications.
You need to prevent unauthorized applications and malware from running on the virtual machines.
What should you do?

A. Configure Azure Active Directory (Azure AD) Identity Protection.
B. From Microsoft Defender for Cloud, configure adaptive application controls.
C. Apply an Azure policy to RGI.

D. Apply a resource lock to RGI.

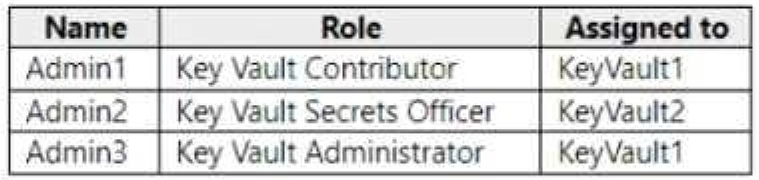
**Correct Answer: B**
**Section:**
**Explanation:**
Microsoft Defender for Cloud helps you prevent, detect, and respond to threats. Defender for Cloud gives you increased visibility into, and control over, the security of your Azure resources. It provides integrated security monitoring and policy management across your Azure subscriptions. It helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions. Defender for Cloud helps you optimize and monitor the security of your virtual machines by:
Providing security recommendations for the virtual machines. Example recommendations include:
apply system updates, configure ACLs endpoints, enable antimalware, enable network security groups, and apply disk encryption. Monitoring the state of your virtual machines.
https://learn.microsoft.com/en-us/azure/security/fundamentals/virtual-machines-overview

**QUESTION 17**
HOTSPOT
You have an Azure subscription that contains the key vaults shown in the following table.



| Name | Days to retain deleted vaults | Purge protection | Permission model |
|---|---|---|---|
| KeyVault1 | 10 | Enabled | Azure role-based access control (Azure RBAC) |
| KeyVault2 | 15 | Disabled | Azure role-based access control (Azure RBAC) |

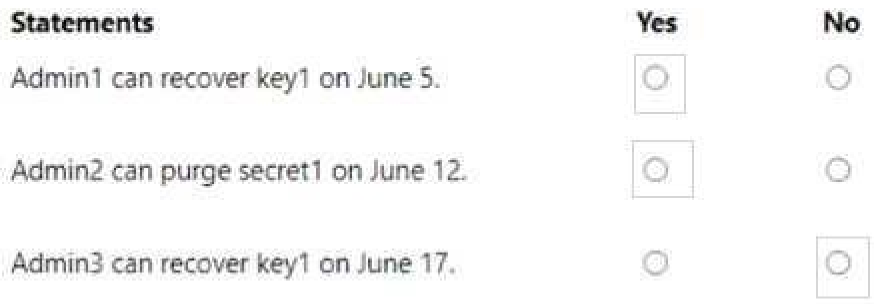
The subscription contains the users shown in the following table.



| Name | Role | Assigned to |
|---|---|---|
| Admin1 | Key Vault Contributor | KeyVault1 |
| Admin2 | Key Vault Secrets Officer | KeyVault2 |
| Admin3 | Key Vault Administrator | KeyVault1 |

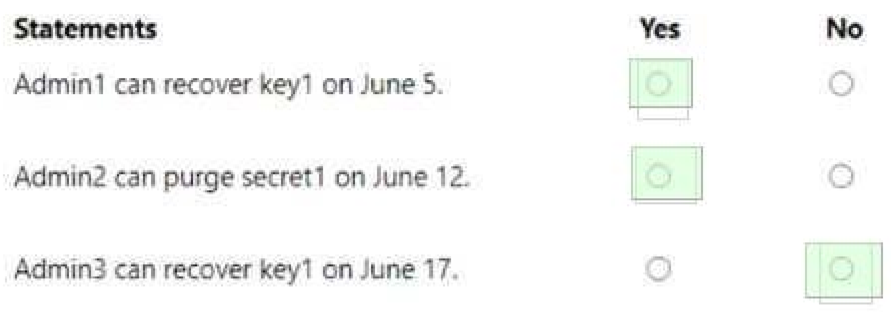
On June 1, you perform the following actions:
• Delete a key named key1 from KeyVault1.
• Delete a secret named secret 1 from KeyVault2.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

**Hot Area:**



| Statements | Yes | No |
|---|---|---|
| Admin1 can recover key1 on June 5. | ○ | ○ |
| Admin2 can purge secret1 on June 12. | ○ | ○ |
| Admin3 can recover key1 on June 17. | ○ | ○ |

**Answer Area:**



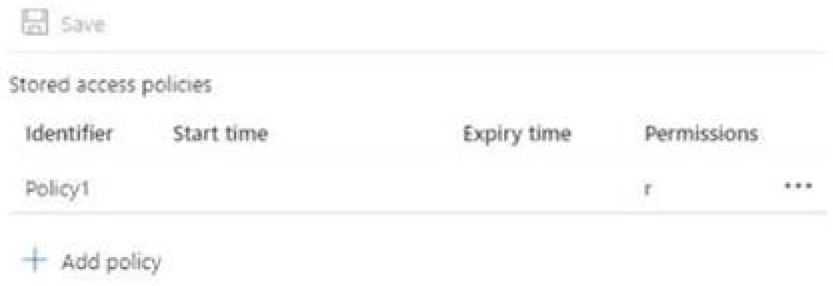
| Statements | Yes | No |
|---|---|---|
| Admin1 can recover key1 on June 5. | [✓ ○] | ○ |
| Admin2 can purge secret1 on June 12. | [✓ ○] | ○ |
| Admin3 can recover key1 on June 17. | ○ | [✓ ○] |

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

**QUESTION 18**

HOTSPOT

You have an Azure subscription that contains a blob container named cont1. Cont1 has the access policies shown in the following exhibit.

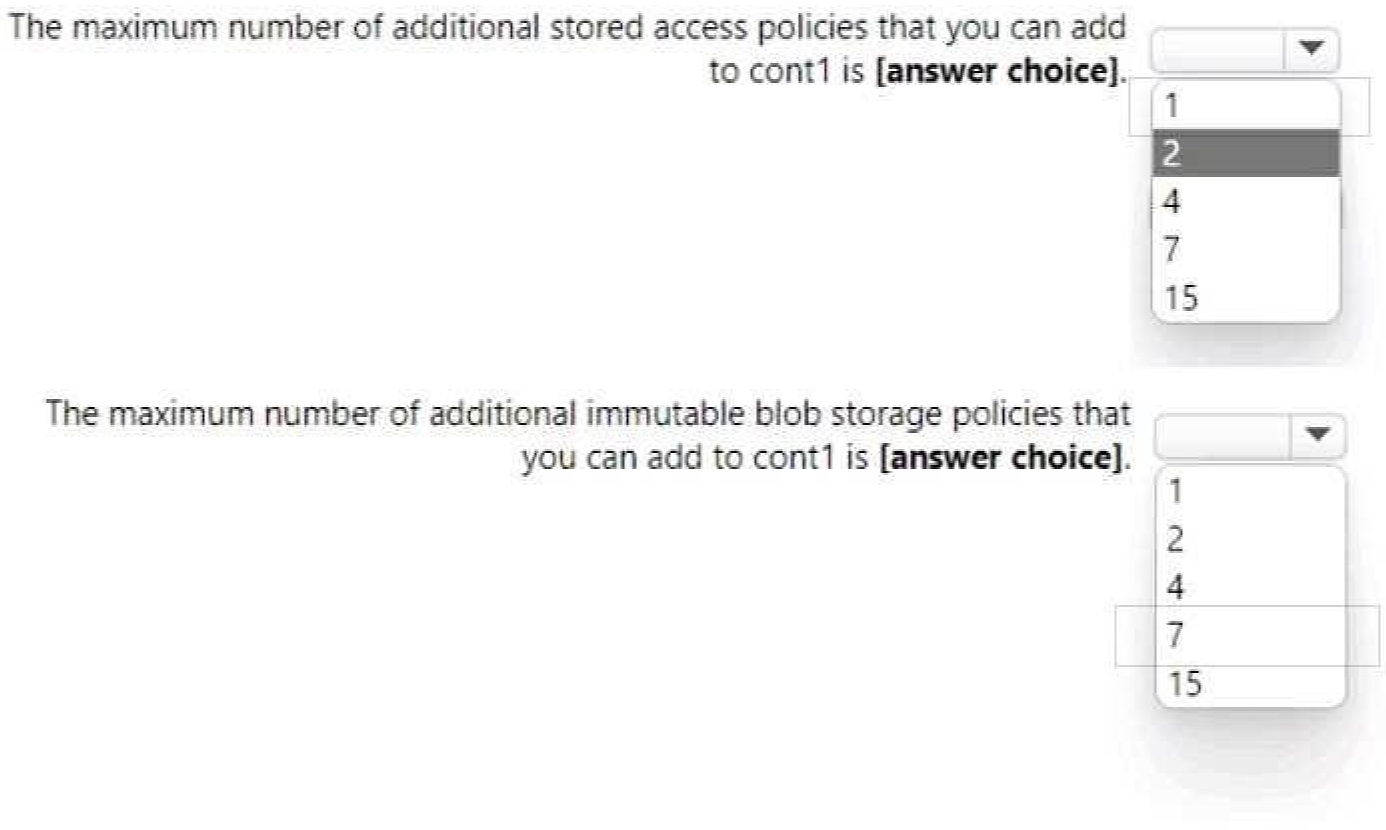


Stored access policies

| Identifier | Start time | Expiry time | Permissions | |
|---|---|---|---|---|
| Policy1 | | | r | ••• |

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

**Hot Area:**



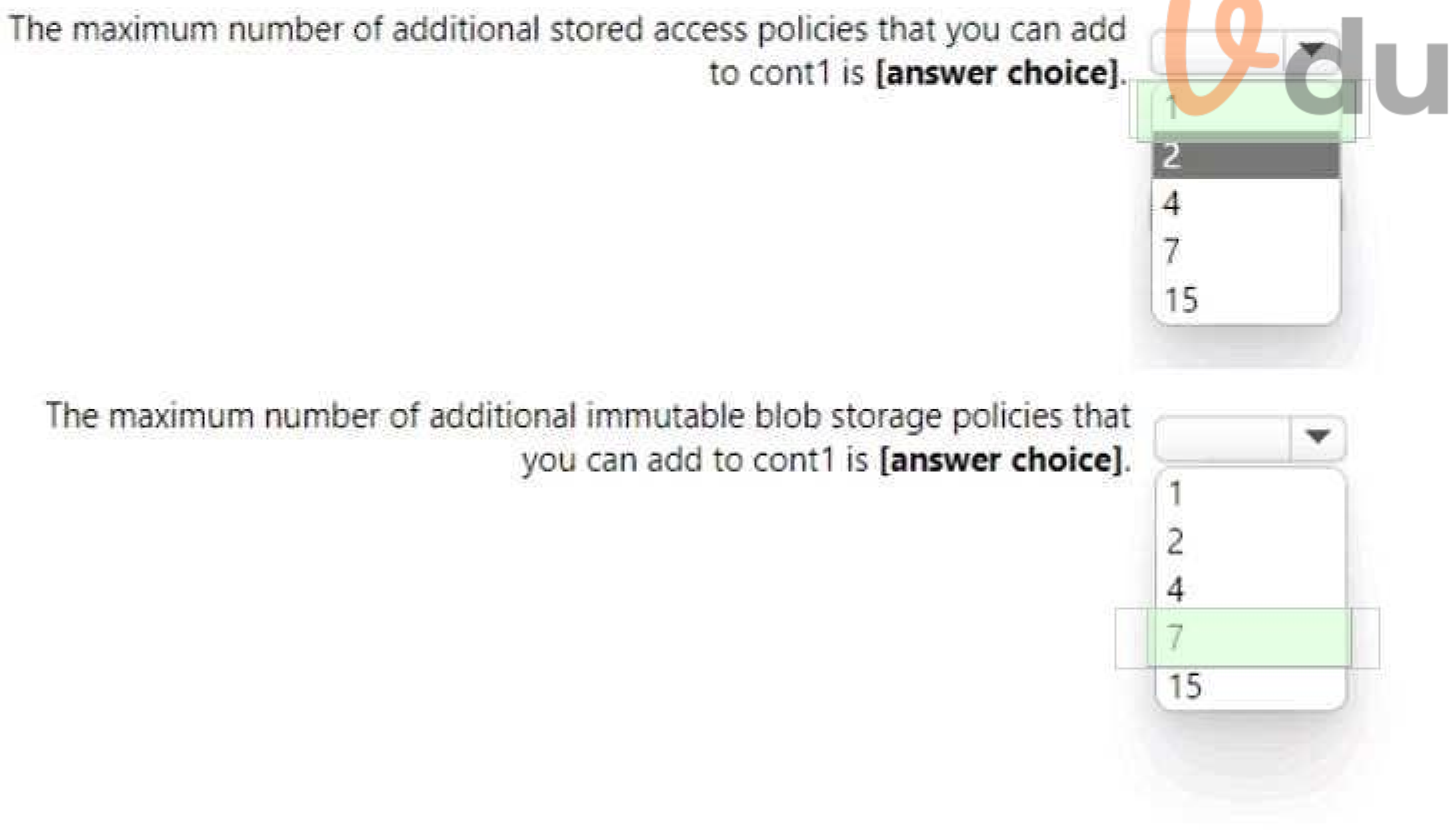
The maximum number of additional stored access policies that you can add to cont1 is **[answer choice]**.

1
2
4
7
15

The maximum number of additional immutable blob storage policies that you can add to cont1 is **[answer choice]**.

1
2
4
7
15

**Answer Area:**



The maximum number of additional stored access policies that you can add to cont1 is **[answer choice]**.

[✓ 1]
2
4
7
15

The maximum number of additional immutable blob storage policies that you can add to cont1 is **[answer choice]**.

1
2
4
[✓ 7]
15

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

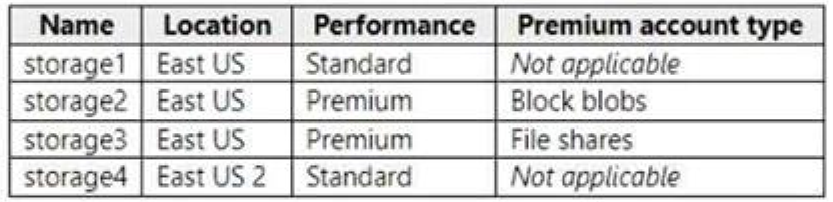
**QUESTION 19**
You have an Azure environment.

You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001:2013 standards. What should you use?

A. Azure Active Directory (Azure AD) Identity Protection
B. Microsoft Defender for Cloud
C. Microsoft Defender for Identity
D. Microsoft Sentinel

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

**QUESTION 20**
You have an Azure subscription that contains an Azure SQL database named DB1 in the East US Azure region. You create the storage accounts shown in the following table.



| Name | Location | Performance | Premium account type |
|---|---|---|---|
| storage1 | East US | Standard | *Not applicable* |
| storage2 | East US | Premium | Block blobs |
| storage3 | East US | Premium | File shares |
| storage4 | East US 2 | Standard | *Not applicable* |

You plan to enable auditing for DB1.
Which storage accounts can you use as the auditing destination for DB1?

A. storage1 only
B. storage1 and storage4 only
C. Storage2 and storage3 only
D. storage1, storage2 and storage3 only

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

**QUESTION 21**
You have an Azure subscription that contains an Azure Files share named share1 and a user named User1. Identity-based authentication is configured for share1. User1 attempts to access share1 from a Windows 10 device by using SMB.
Which type of token will Azure Files use to authorize the request?

A. OAuth 20
B. JSON Web Token (JWT)
C. Kerberos
D. SAML

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

**QUESTION 22**
You have an Azure Active Directory (Azure AD) tenant. The tenant contains users that are assigned Azure AD Premium Plan 2 licenses. You have an partner company that has a domain named The fabrikam.com domain contains a user named user'. User' has an email address of userl@tabrikam.com. You to provide User1 with to the resources in the tenant The solution must meet the following requirements:
user1 must be able to sign in by using the userl@fabrikam.com credentials You must be able to grant User1 access to the resources in the tenant Administrative effort must be minimized.
What should you do?

A. Create a user account for user1.
B. Create an invite for User1.
C. To the tenant add fabrikamcom as a custom domain
D. Set Enable guest self-service sign up via user flows to Yes for the tenant.

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

**QUESTION 23**
You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.
You need to use the automatically generated service principal for the AKS cluster to authenticate to the Azure Container Registry.
What should you create?

A. an Azure AD user
B. a secret in Azure Key Vault
C. an Azure AD group
D. a role assignment

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

**QUESTION 24**
You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.
Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 20.04.
You create a service endpoint for Microsoft. Storage in Subnet1.
You need to ensure that when you deploy Docker containers to VM1, the containers can access Azure Storage resources by using the service endpoint.
What should you do on VM1 before you deploy the container?

A. Create an application security group and a network security group (NSG).
B. Install the container network interface (CNI) plug-in.
C. Edit the docker-compose.ym1 file.

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

**QUESTION 25**
You have an Azure subscription that uses Microsoft Defender for Cloud.
You have an Amazon Web Services (AWS) account.
You need to add the AWS account to Defender for Cloud.
What should you do first?

A. From the Azure portal, add the AWS enterprise application.
B. From the AWS account, enable a security hub.
C. From Defender for Cloud, configure the Security solutions settings.
D. From Defender for Cloud, configure the Environment settings.

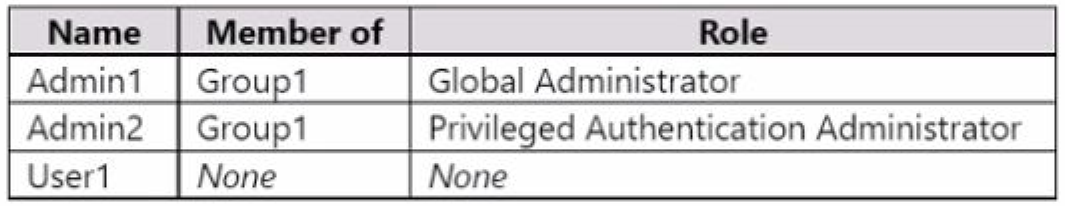
**Correct Answer: D**

**Section:**

**QUESTION 26**

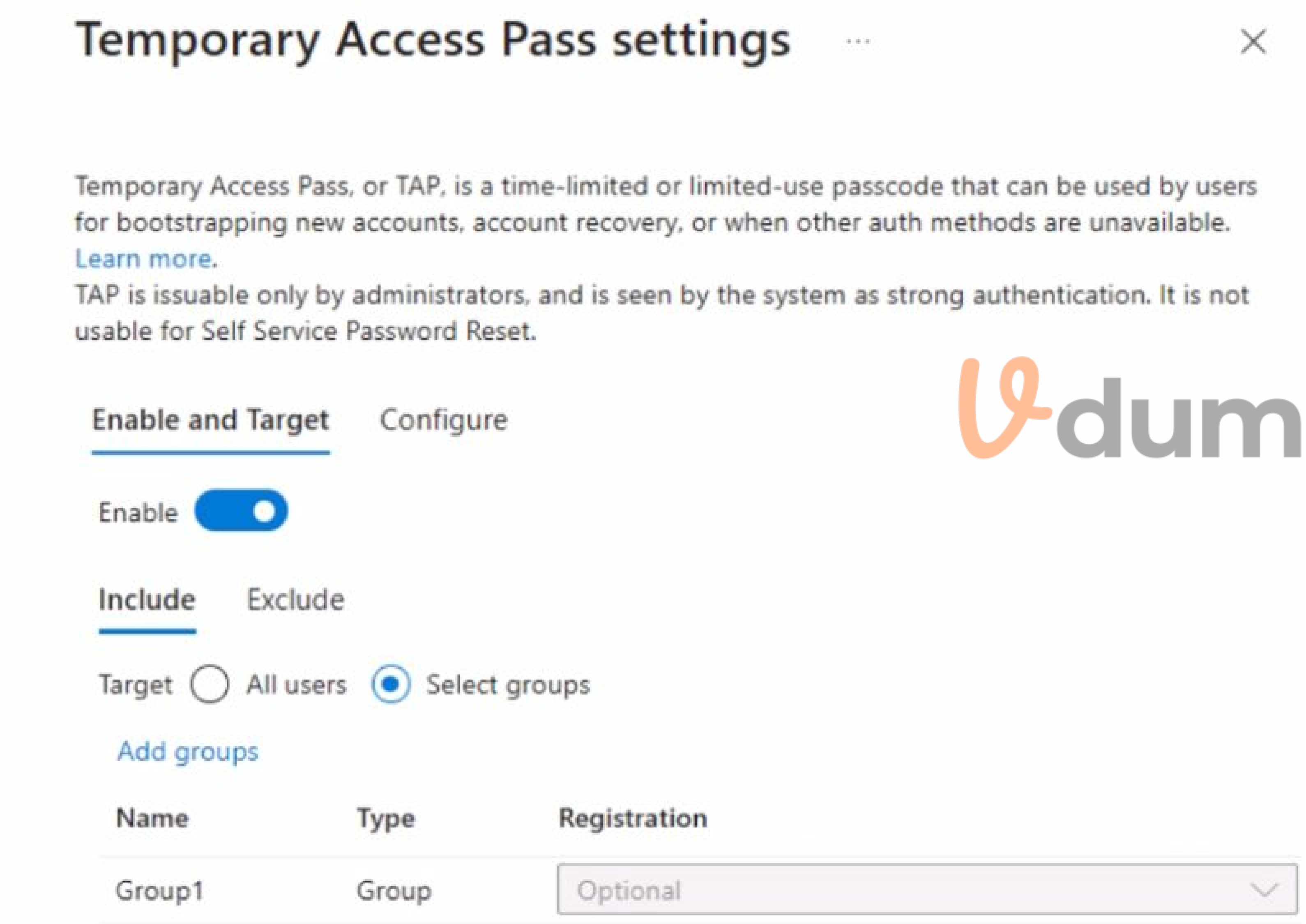
HOTSPOT

You have a Microsoft Entra tenant that contains the users shown in the following table.



| Name | Member of | Role |
|---|---|---|
| Admin1 | Group1 | Global Administrator |
| Admin2 | Group1 | Privileged Authentication Administrator |
| User1 | *None* | *None* |

You configure the Temporary Access Pass settings as shown in the following exhibit.



## Temporary Access Pass settings

Temporary Access Pass, or TAP, is a time-limited or limited-use passcode that can be used by users for bootstrapping new accounts, account recovery, or when other auth methods are unavailable. Learn more.

TAP is issuable only by administrators, and is seen by the system as strong authentication. It is not usable for Self Service Password Reset.

Enable and Target | Configure

Enable: On

Include | Exclude

Target ○ All users ● Select groups

Add groups

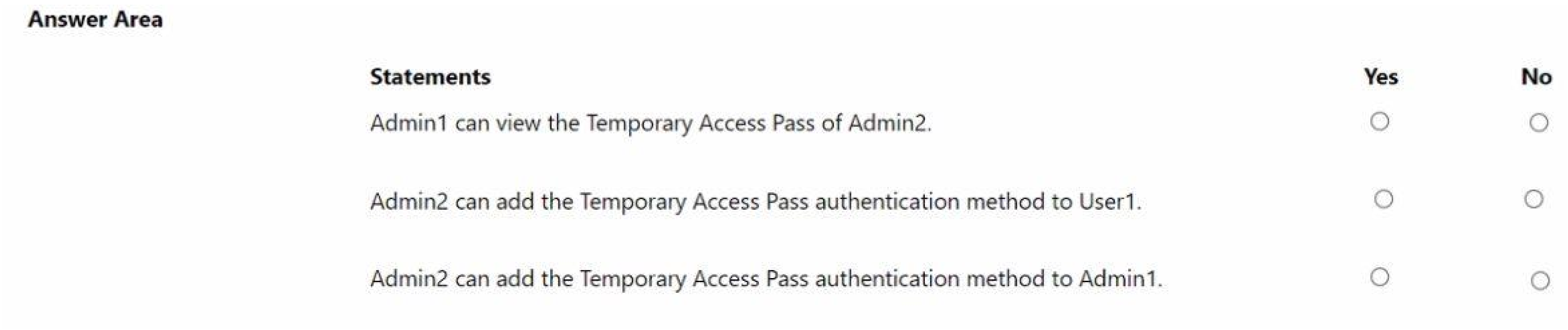
| Name | Type | Registration |
|---|---|---|
| Group1 | Group | Optional |

You add the Temporary Access Pass authentication method to Admin2.

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

NOTE: Each correct selection is worth one point.

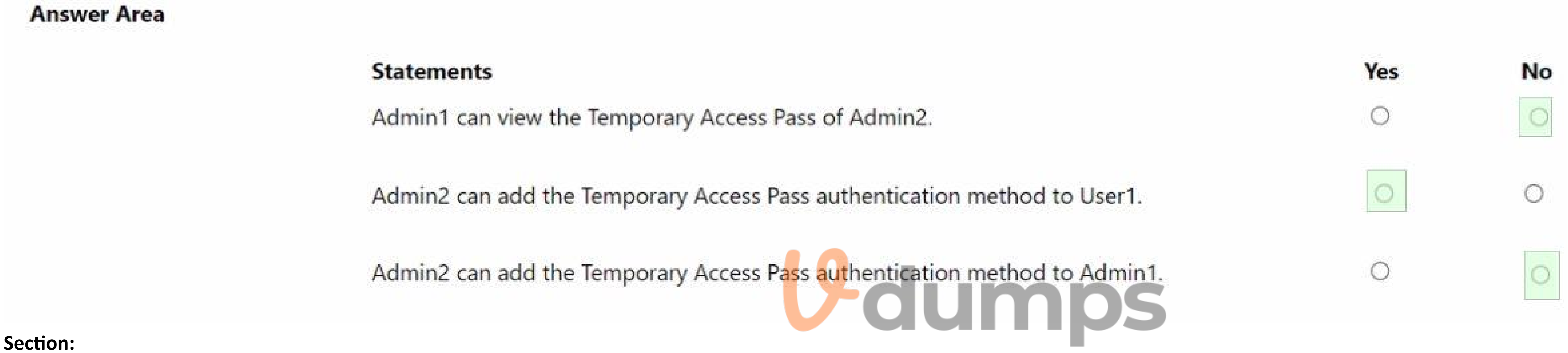
**Hot Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| Admin1 can view the Temporary Access Pass of Admin2. | ○ | ○ |
| Admin2 can add the Temporary Access Pass authentication method to User1. | ○ | ○ |
| Admin2 can add the Temporary Access Pass authentication method to Admin1. | ○ | ○ |

**Answer Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| Admin1 can view the Temporary Access Pass of Admin2. | ○ | [✓ ○] |
| Admin2 can add the Temporary Access Pass authentication method to User1. | [✓ ○] | ○ |
| Admin2 can add the Temporary Access Pass authentication method to Admin1. | ○ | [✓ ○] |

**Section:**

**Explanation:**