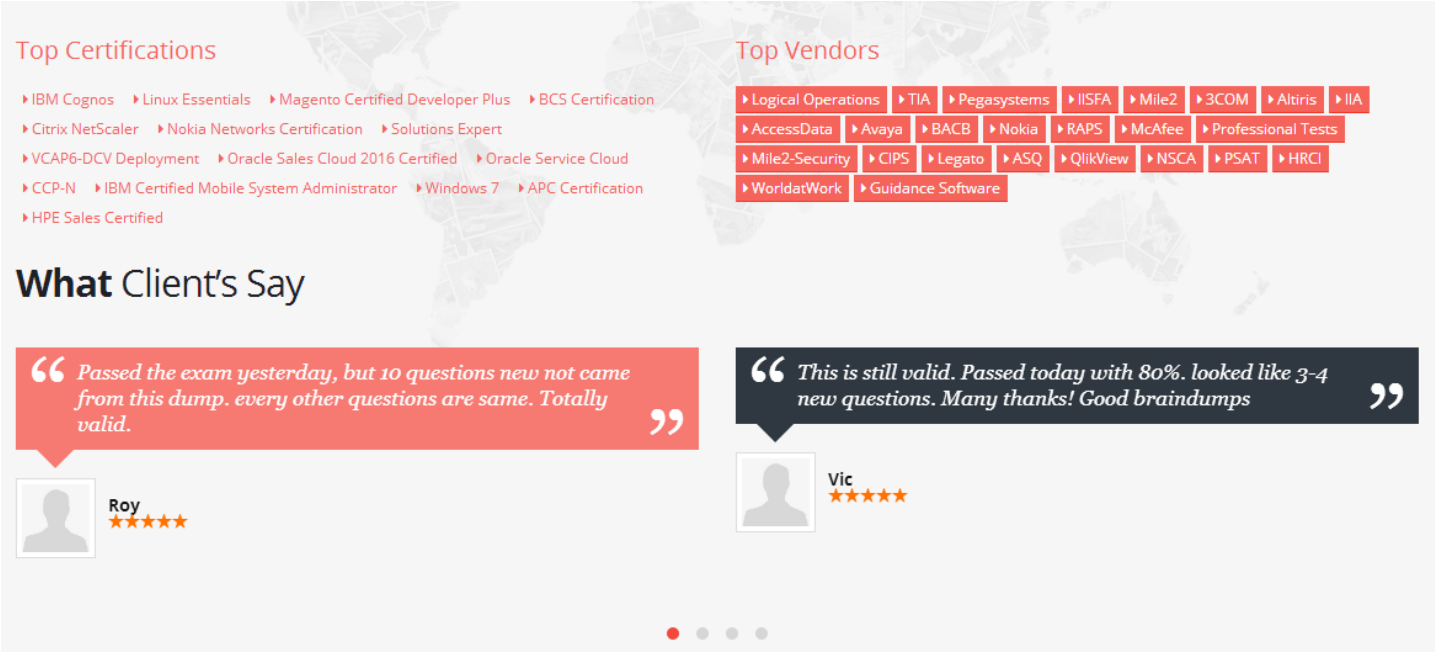
Lead2passExam



http://www.lead2passexam.com/

Available Exam Cram and Valid Dumps - Lead2Pass Exam

Exam : **AZ-500J**

Title : Microsoft Azure Security Technologies (AZ-500日本語版)

Vendor : Microsoft

Version : DEMO

QUESTION NO: 1
データとアプリケーションの要件を満たすようにWebApp1を構成する必要があります。
実行すべき2つのアクションはどれですか？それぞれの正解はソリューションの一部を示しています。
注：それぞれの正しい選択には1ポイントの価値があります。
A.パブリック証明書をアップロードします。
B.HTTPS Onlyプロトコル設定をオンにします。
C.最小TLSバージョンプロトコル設定を1.2に設定します。
D.App Serviceプランの価格帯を変更します。
E.受信クライアント証明書プロトコル設定をオンにします。
Answer: B E
Explanation:
Refer https://docs.microsoft.com/en-us/azure/app-service/app-service-web-configure-tls-mutual-auth
Topic 1, Litware, inc
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 question on 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 sections 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 on 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 Subent0.
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://litwareinc.com and http://www.litwareinc.com.
Resource Group1	Resource group	Resource Group1 is a resource group that contains VNet1, VM0, and VM1.
Resource Group2	Resource group	Resource Group2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Free tier.

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 Resource Group2 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 Resource Group1.
* The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
* Azure AD users must be 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 Resource Group1. Role1 must be available only for Resource Group1.
Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center.

QUESTION NO: 2
Group1のIDおよびアクセス要件を満たす必要があります。
あなたは何をするべきか？
A.メンバーシップルールをGroup1に追加します。
B.Group1を削除します。 Office 365のメンバーシップタイプを持つGroup1という名前の新しいグループを作成します。グループにユーザーとデバイスを追加します。
C.Group1のメンバーシップルールを変更します。
D.Group1のメンバーシップタイプを割り当て済みに変更します。動的なメンバーシップを持つ2つのグループを作成します。新しいグループをGroup1に追加します。
Answer: D
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership 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 NO: 3
セキュリティ運用要件を満たしていることを確認する必要があります。
最初に何をすべきですか？
A.セキュリティセンターで自動プロビジョニングをオンにします。

B.Security CenterとMicrosoft Cloud App Securityを統合します。
C.Security Centerの価格設定を標準にアップグレードします。
D.セキュリティセンターのワークスペース構成を変更します。
Answer: C
Explanation:
The Standard tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The Standard tier also adds advanced threat detection capabilities, which uses built-in behavioral analytics and machine learning to identify attacks and zero-day exploits, access and application controls to reduce exposure to network attacks and malware, and more.
Scenario: Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center.
References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing

QUESTION NO: 4
ユーザーがVM0にアクセスできることを確認する必要があります。ソリューションはプラットフォーム保護要件を満たしている必要があります。
あなたは何をするべきか？
A.VM0をSubnet1に移動します。
B.ファイアウォールで、ネットワークトラフィックフィルタリングルールを構成します。
C.RT1をAzureFirewallSubnetに割り当てます。
D.ファイアウォールで、DNATルールを構成します。
Answer: D
Explanation:
https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat

QUESTION NO: 5
プラットフォーム保護要件を満たすには、Role1 を作成する必要があります。
Role1 のロール定義をどのように完了する必要がありますか?
回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。

```
{
    "Name":  "Role1",
    "Id":  "11111111-1111-1111-1111-111111111111",
    "IsCustom" : true,
    "Description": "VM storage operator"
    "Actions" : [
                [ "Microsoft.Compute/" | "Microsoft.Resources/" | "Microsoft.Storage/" ]
                [ disks/* | storageAccounts/* | virtualMachines/disks/* ]
                ],
     "NotActions":  [
                    ],
     "AssignableScopes" :  [
                [ "/" | "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1" | "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4" ]
                    ]
}
```

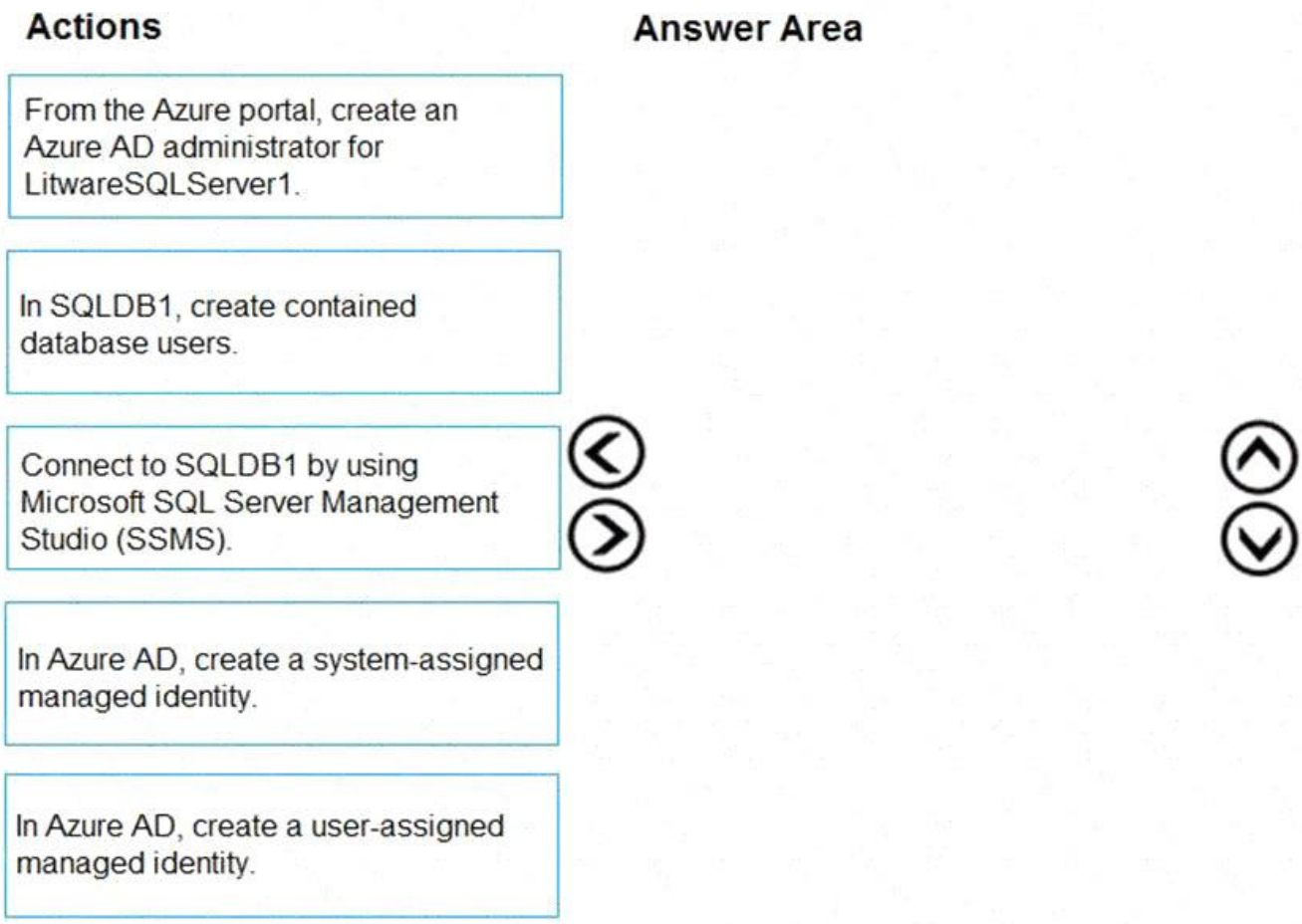
Answer:

```
{
    "Name":  "Role1",
    "Id":  "11111111-1111-1111-1111-111111111111",
    "IsCustom" : true,
    "Description": "VM storage operator"
    "Actions" : [
                [ "Microsoft.Compute/" | "Microsoft.Resources/" | "Microsoft.Storage/" ]
                [ disks/* | storageAccounts/* | virtualMachines/disks/* ]
                ],
     "NotActions":  [
                    ],
     "AssignableScopes" :  [
                [ "/" | "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1" | "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4" ]
                    ]
}
```

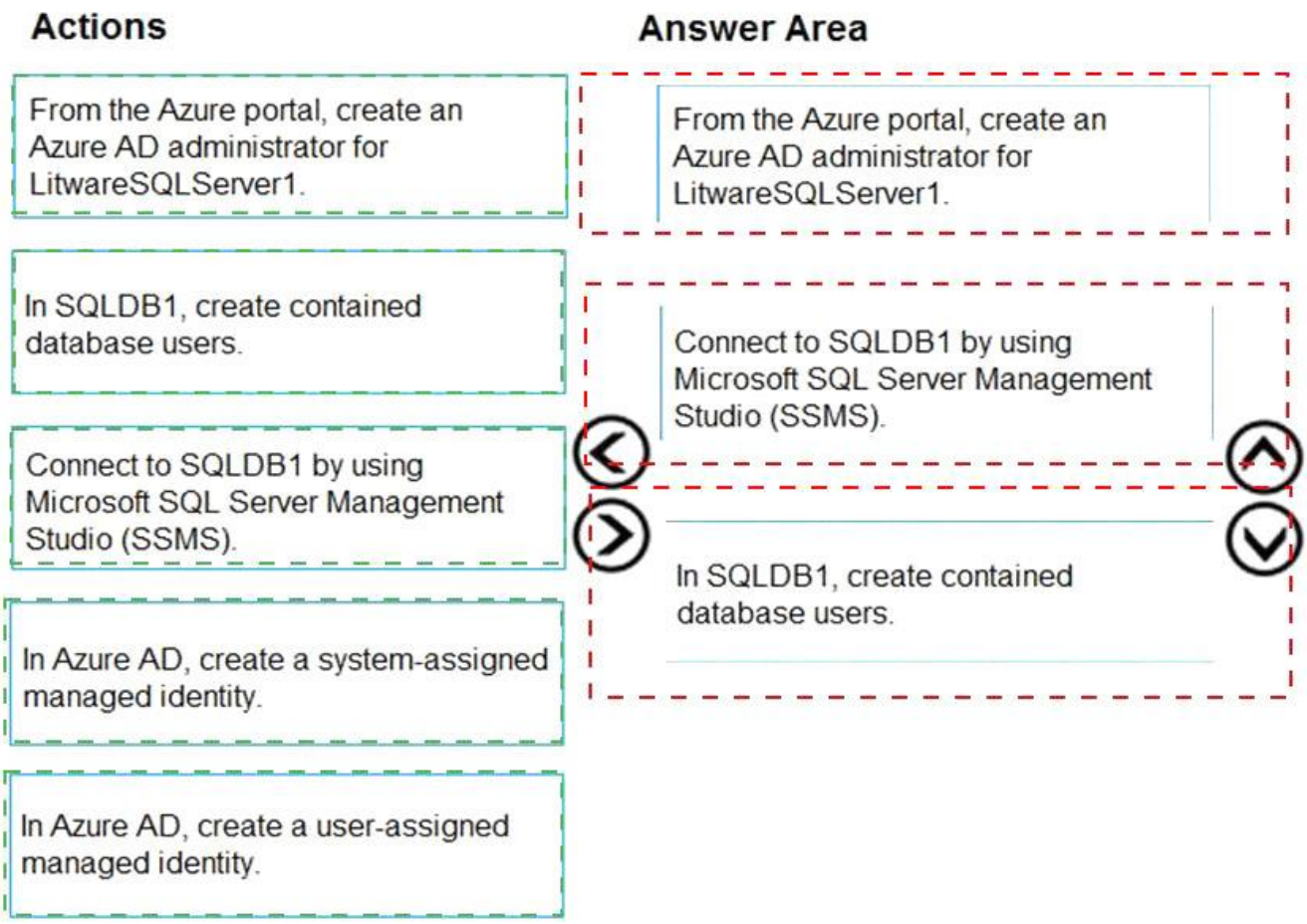
Explanation:
1) Microsoft.Compute/
2) disks

3) /subscrption/{subscriptionId}/resourceGroups/{Resource Group Id}
A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

QUESTION NO: 6
データとアプリケーションの要件を満たすようにSQLDB1を構成する必要があります。
どの3つのアクションを順番に実行することをお勧めしますか？回答するには、適切なアクションをアクションのリストから回答エリアに移動し、正しい順序に並べます。

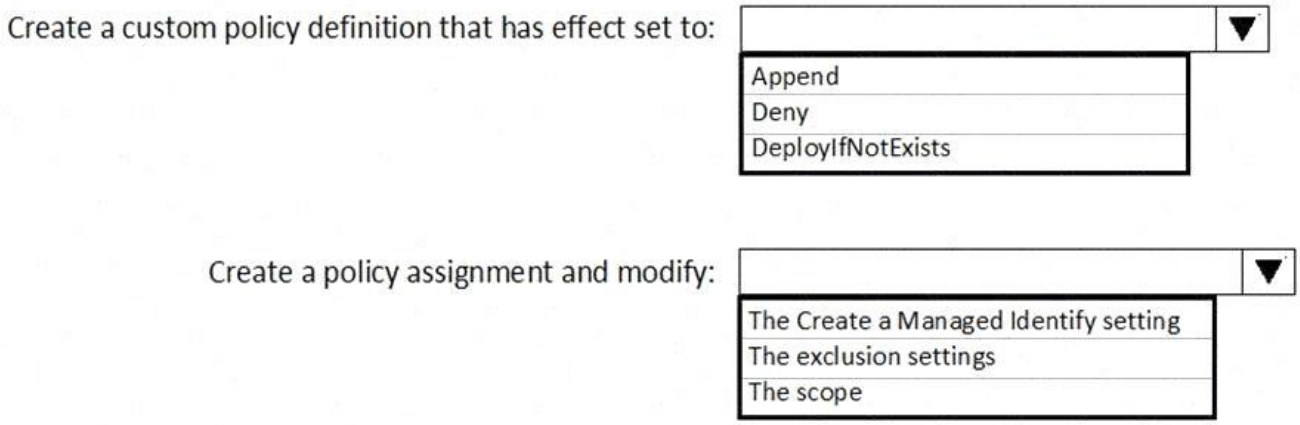


Answer:

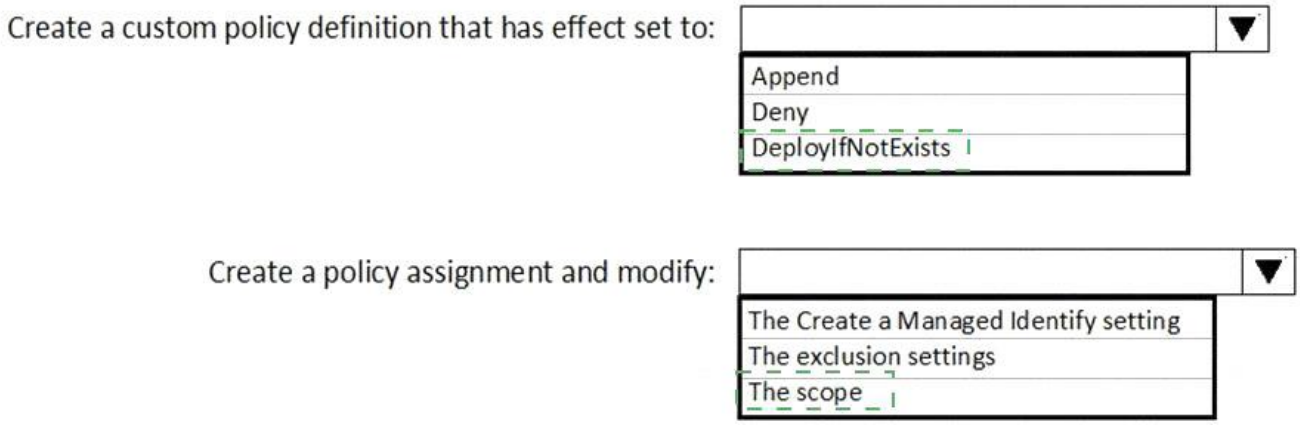


Explanation:
From the Azure portal, create an Azure AD administrator for LitwareSQLServer1 Connect to SQLDB1 by using SSMS In SQLDB1, create contained database users
https://www.youtube.com/watch?v=pEPyPsGEevw

QUESTION NO: 7
プラットフォーム保護の要件を満たすには、Microsoft Antimalwareを展開する必要があります。
あなたは何をするべきか？回答するには、回答エリアで適切なオプションを選択します。
注：それぞれの正しい選択には1ポイントの価値があります。

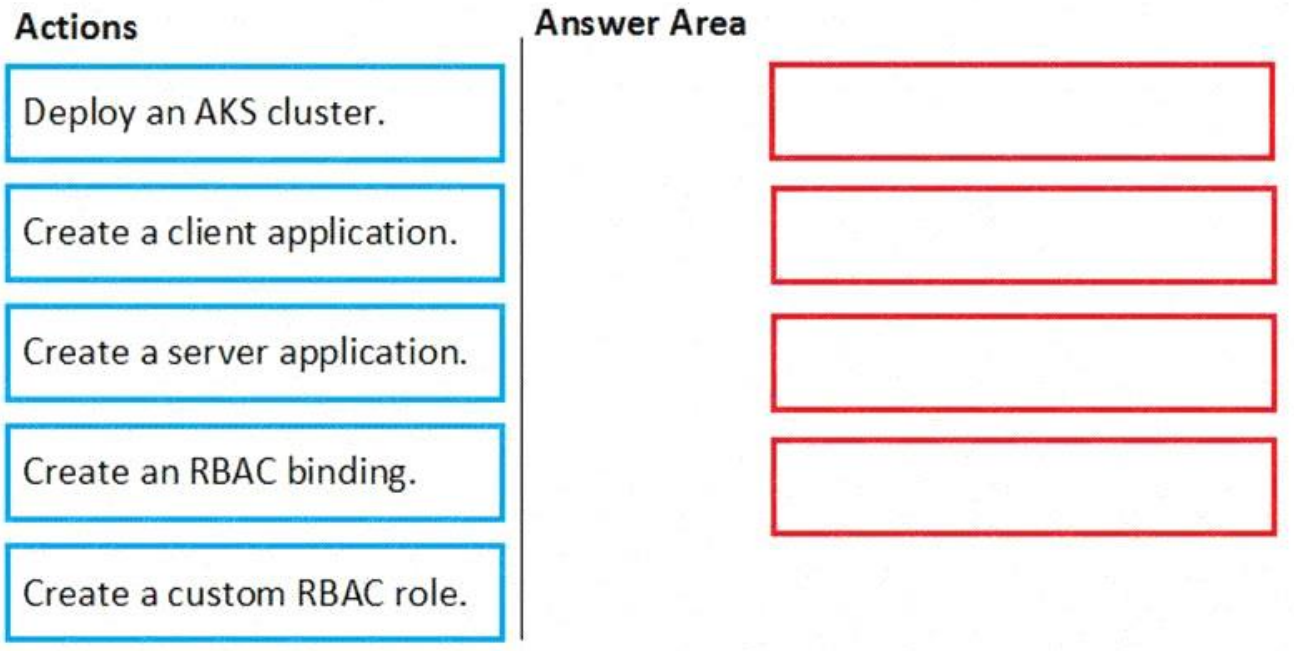


Answer:

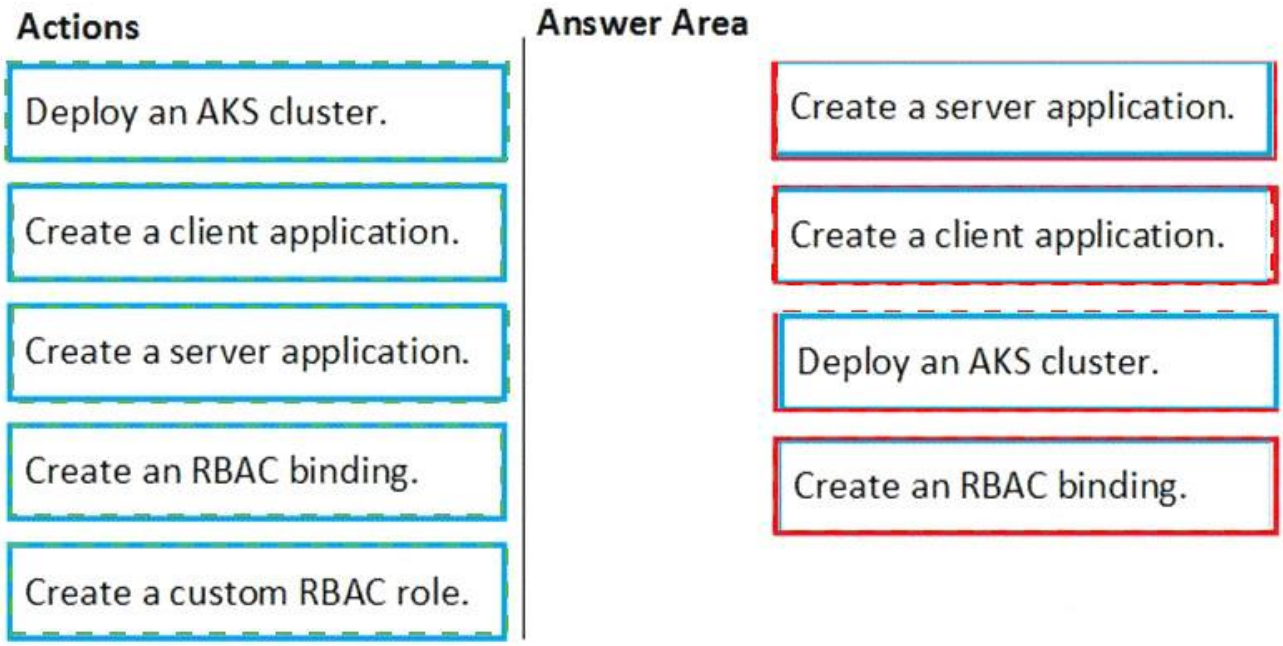


Explanation:
1. DeployifNotExists
2. Scope

QUESTION NO: 8
プラットフォーム保護の要件を満たすには、AKS1 をデプロイする必要があります。
どの 4 つのアクションを順番に実行する必要がありますか?
回答するには、適切なアクションをアクション
リストから回答領域に移動し、正しい順序に並べます。
注意：正解の選択肢は複数あります。正解の選択肢の中からどれを選択しても、得点は加算されます。



Answer:

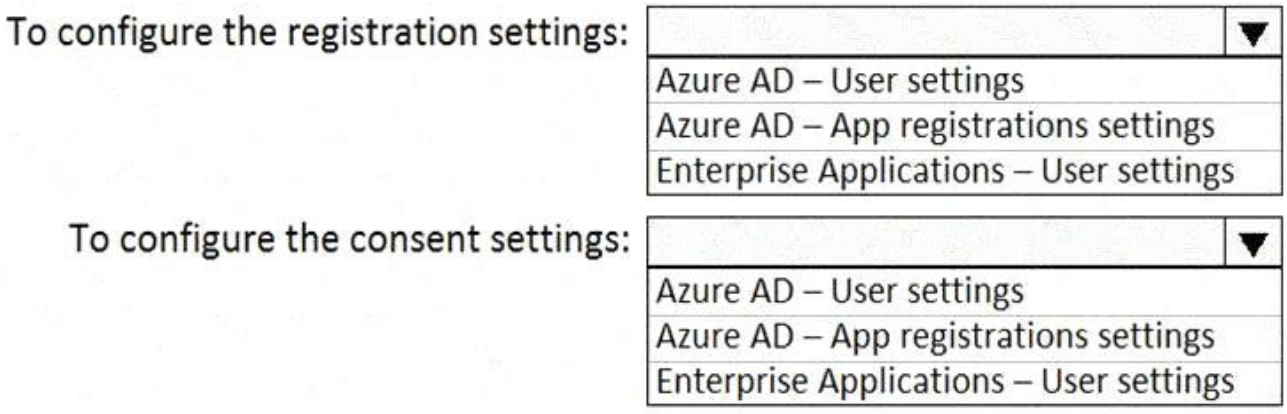


Explanation:

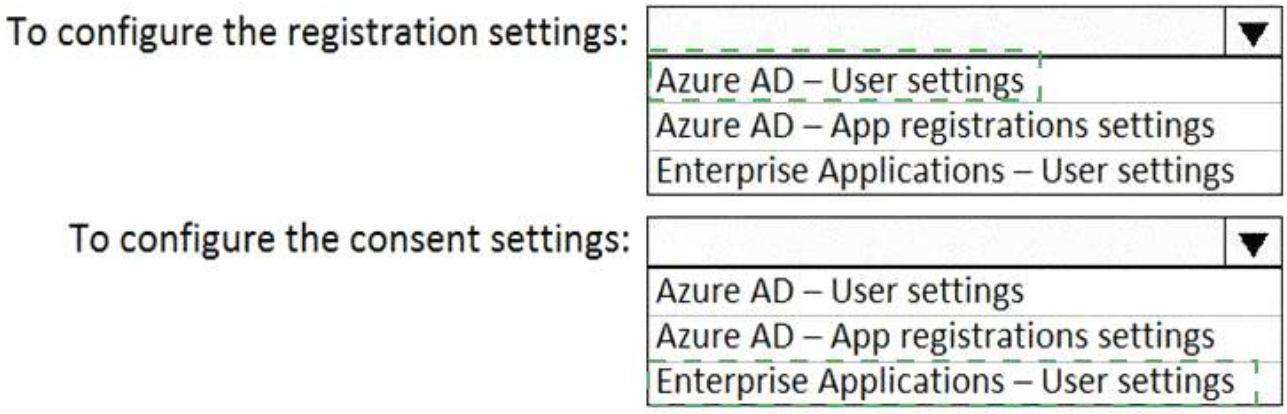
Scenario: Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.
Litewire plans to deploy AKS1, which is a managed AKS (Azure Kubernetes Services) cluster.
Step 1: Create a server application
To provide Azure AD authentication for an AKS cluster, two Azure AD applications 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

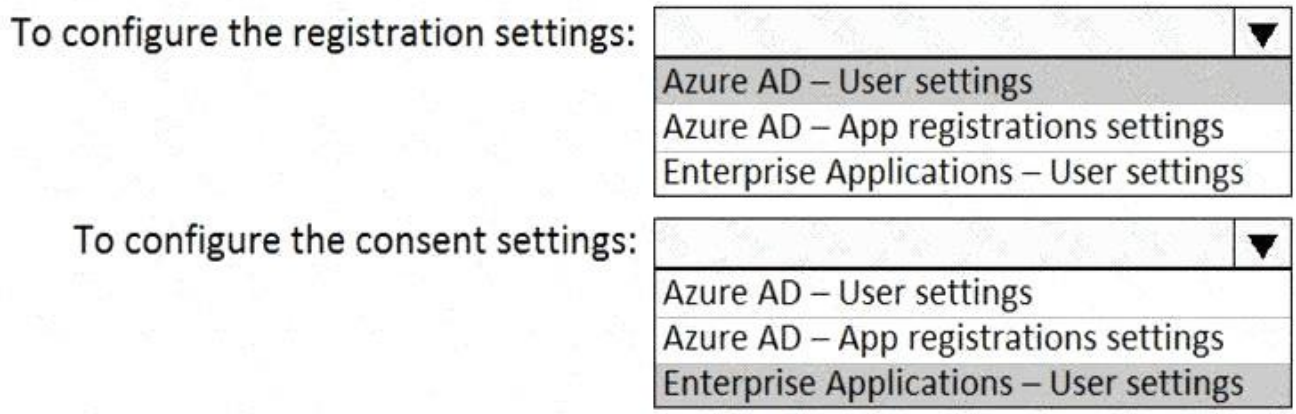
QUESTION NO: 9
Azure AD アプリケーションの登録と同意の構成が ID
とアクセスの要件を満たしていることを確認する必要があります。
Azure ポータルでは何を使用すればよいですか?
回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



Answer:



Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent
Topic 2, Contoso
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 question on 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 sections 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 on 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.
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
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*

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.

User2 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	networksSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2

Name	Subnet
VNetwork1	Subnet1.1, Subnet1.2 and Subent1.3
VNetwork2	Subnet2.1

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet1.1
VM2	NIC2	ASG2	Subnet1.1
VM3	NIC3	*None*	Subnet1.2
VM4	NIC4	ASG1	Subnet1.3
VM5	NIC5	*None*	Subnet2.1

All virtual machines have the 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	Subnet1.1
NSG3	Subnet1.3
NSG4	Subnet2.1

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

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 NO: 10
現在の状態でUser2がSub1のどの仮想ネットワークを変更および削除できるか？回答するには、回答領域で適切なオプションを選択します。
注：それぞれの正しい選択は1ポイントの価値があります。

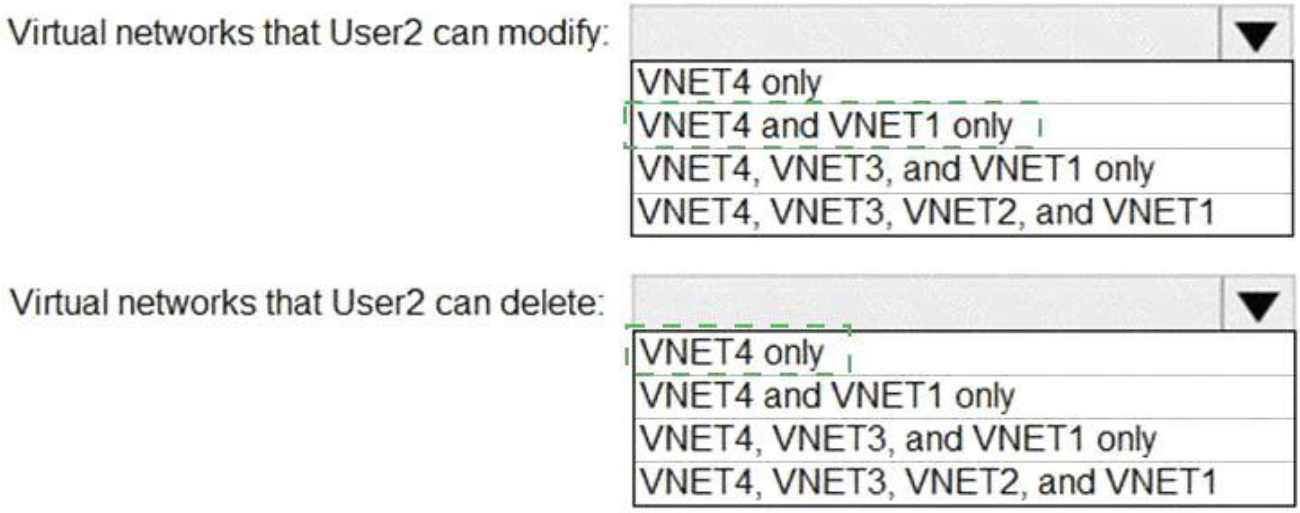
Virtual networks that User2 can modify:

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

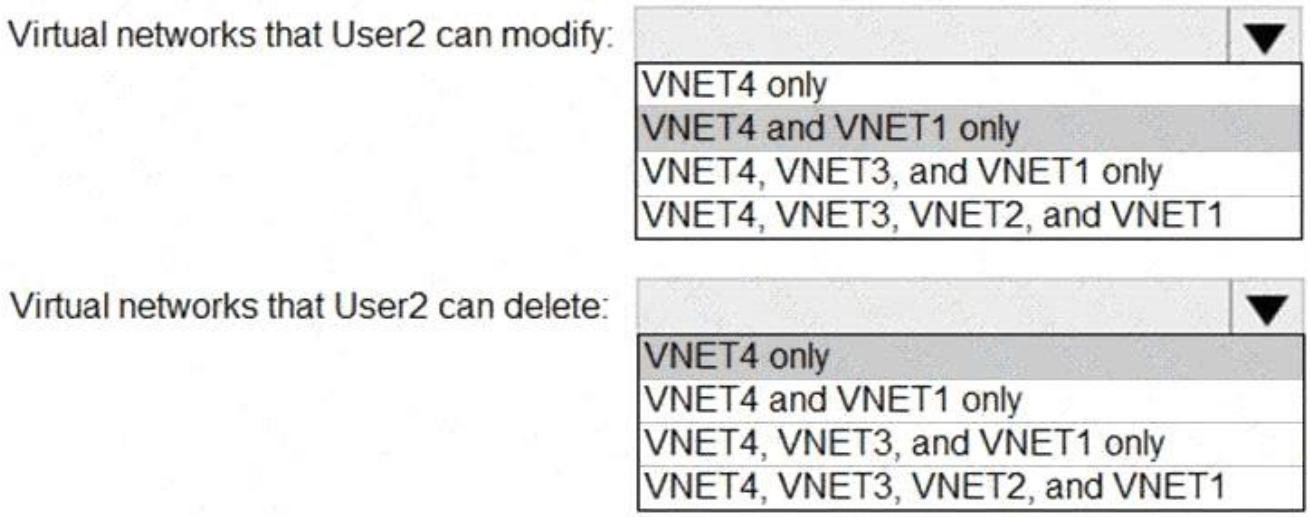
Virtual networks that User2 can delete:

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

Answer:



Explanation:



Box 1: VNET4 and VNET1 only
RG1 has only Delete lock, while there are no locks on RG4.
RG2 and RG3 both have Read-only locks.
Box 2: VNET4 only
There are no locks on RG4, while the other resource groups have either Delete or Read-only locks.
Note: As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.
* CanNotDelete means authorized users can still read and modify a resource, but they can ' t delete the resource.
* ReadOnly means authorized users can read a resource, but they can ' t delete or update the resource.
Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.
Scenario:

User2 is a Security administrator.
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.
User2 creates the virtual networks shown in the following table.

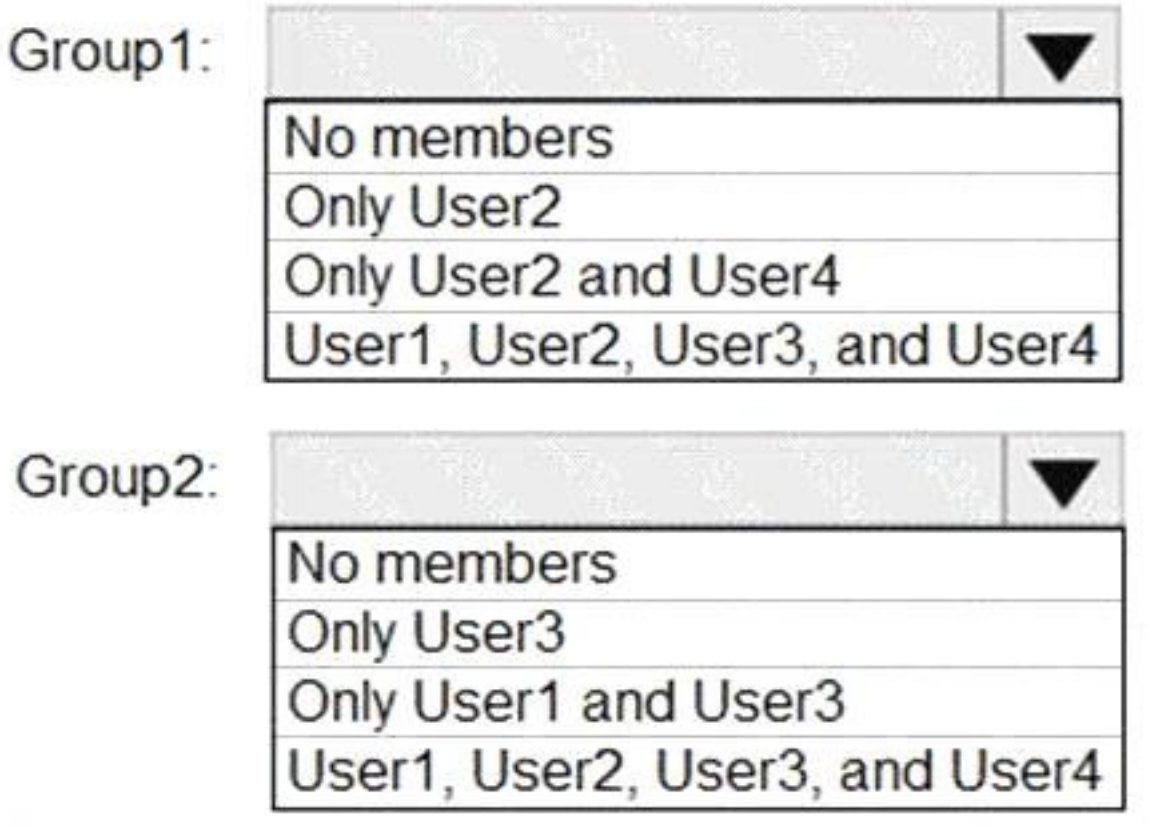
Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

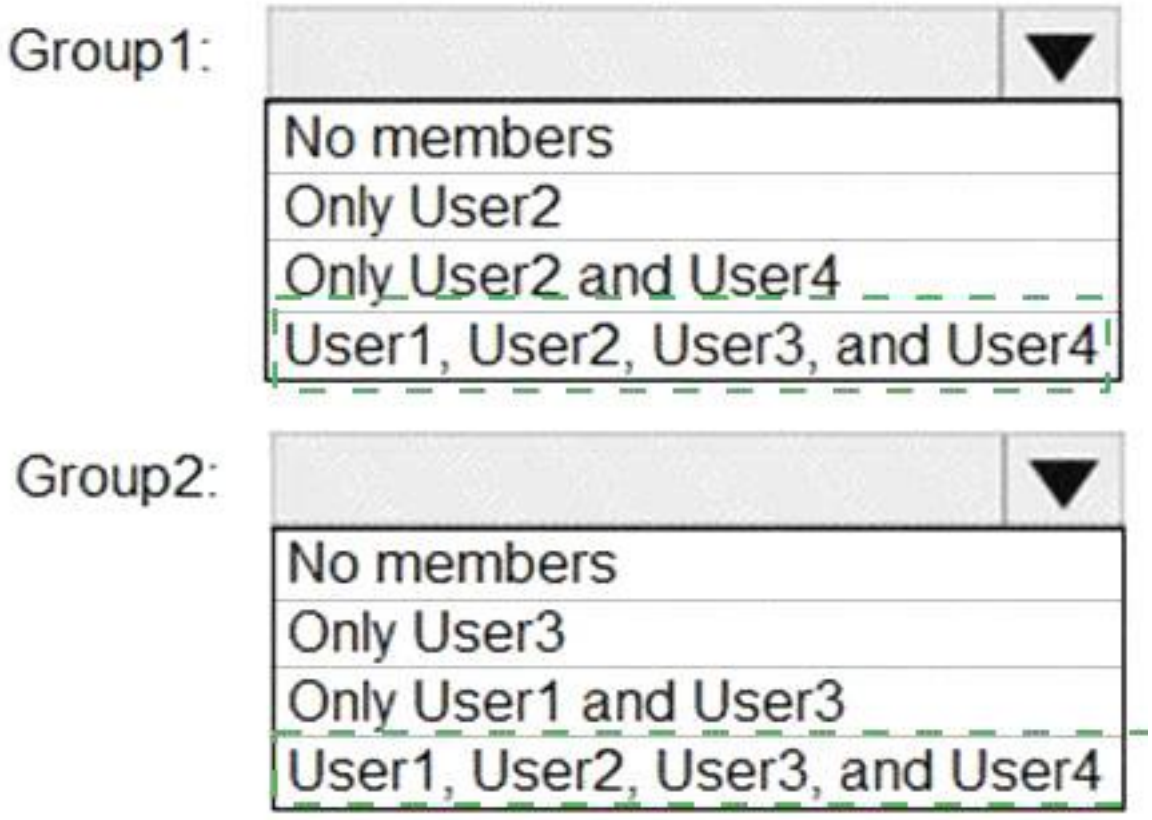
Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

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

QUESTION NO: 11
グループ1とグループ2のメンバーシップは何ですか?
回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



Answer:



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: User1, User2, User3, User4
References:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership

QUESTION NO: 12
VNetwork1の技術要件を満たす必要があります。
最初に何をすべきですか？
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.
Answer: A
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 NO: 13
Sub2のVM1、VM2、およびVM3のセキュリティを評価しています。
以下の各ステートメントについて、ステートメントが真である場合は「はい」を選択します。それ以外の場合は、「いいえ」を選択します。
注：それぞれの正しい選択には1ポイントの価値があります。

Answer Area

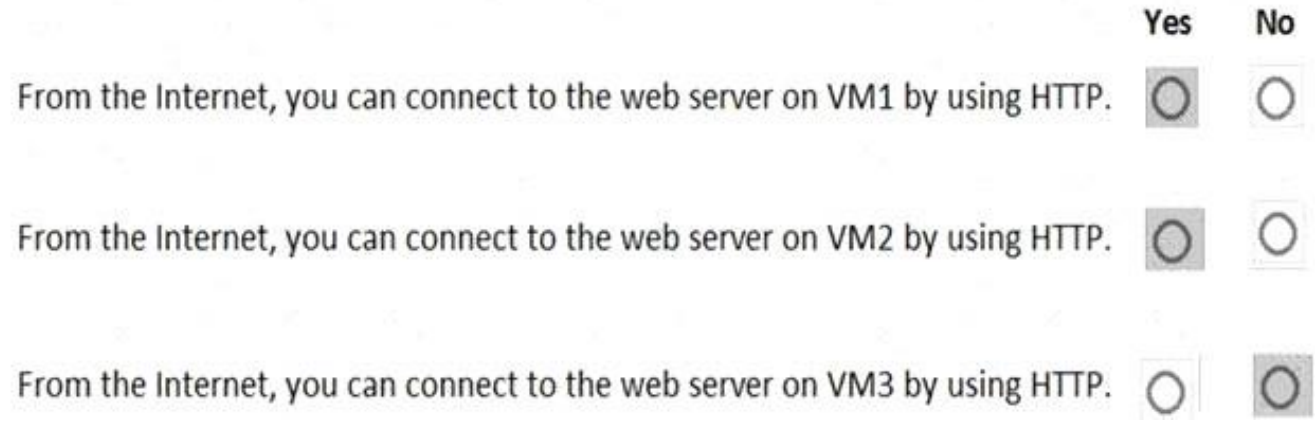
Statements	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	○	○
From the Internet, you can connect to the web server on VM2 by using HTTP.	○	○
From the Internet, you can connect to the web server on VM3 by using HTTP.	○	○

Answer:

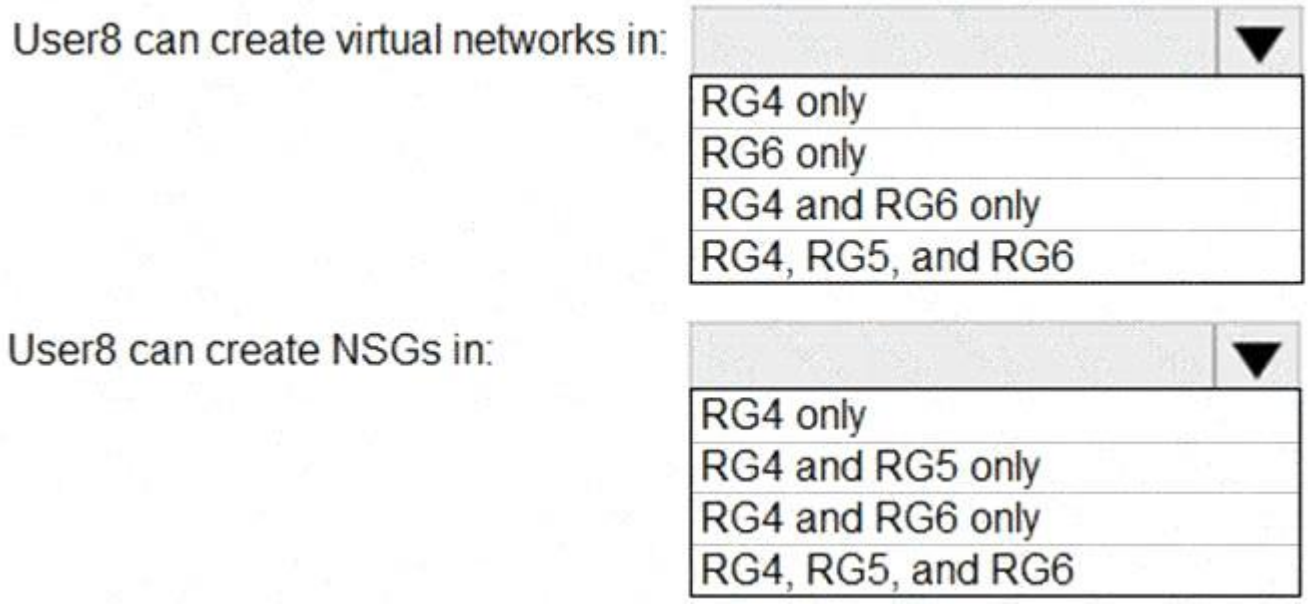
Answer Area

Statements	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.	○	○

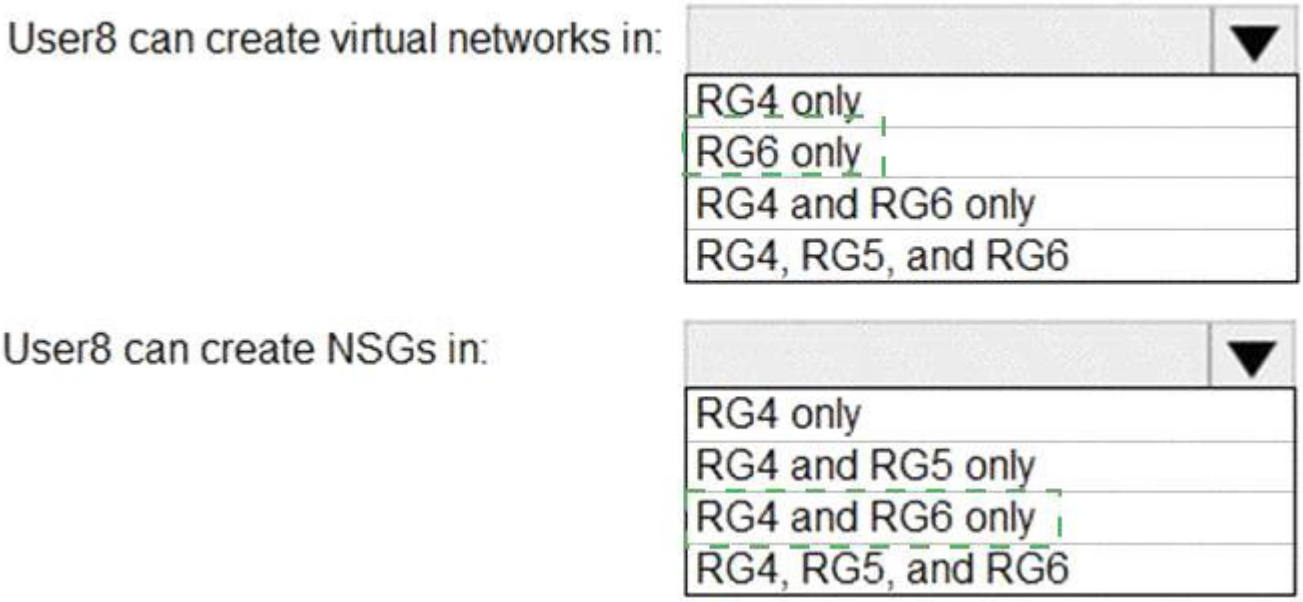
Explanation:



QUESTION NO: 14
User8にRG4、RG5、およびRG6の所有者ロールを割り当てます。
User8はどのリソースグループで仮想ネットワークとNSGを作成できますか？回答するには、回答エリアで適切なオプションを選択します。
注：それぞれの正しい選択には1ポイントの価値があります。



Answer:



Explanation:
Box1: RG6 only as there is not option for RG5 & RG6 which it should be.
Box2: RG4 & RG6

QUESTION NO: 15
Sub2の仮想マシン間のネットワーク通信に対するアプリケーションセキュリティグループの効果を評価しています。
以下の各ステートメントについて、ステートメントが真である場合は「はい」を選択します。それ以外の場合は、「いいえ」を選択します。
注：それぞれの正しい選択には1ポイントの価値があります。

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:

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.	○	○

Explanation:

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.	○	○

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 NO: 16
Sub2の仮想マシン間のネットワーク通信のセキュリティを評価しています。
以下の各ステートメントについて、ステートメントが真である場合は「はい」を選択します。それ以外の場合は、「いいえ」を選択します。
注：それぞれの正しい選択には1ポイントの価値があります。

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:

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.	○	○

Explanation:
Yes,
Yes
No

QUESTION NO: 17
User2がPIMを実装できることを確認する必要があります。
最初に何をすべきですか？
A.User2にグローバル管理者ロールを割り当てます。
B.contoso.comの認証方法を構成します。
C.contoso.comのIDセキュアスコアを構成します。
D.User2の多要素認証（MFA）を有効にします。
Answer: D
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
Topic 3, Fabrikam inc
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, VNET2/Subnet1, 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

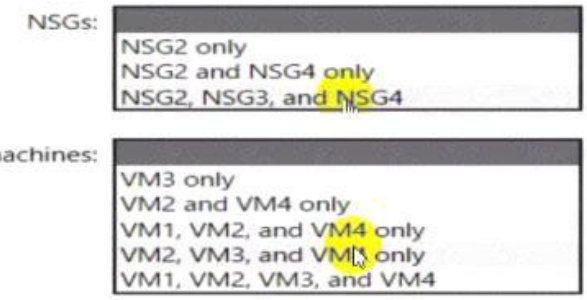
VM1, VM2, and VM3 must be encrypted by using Azure Disk Encryption.
Just in time (JIT) VM access for VM1, VM2, and VM3 must be enabled.
App1 must use a secure connection string stored in KeyVault1.
KeyVault1 traffic must NOT travel over the internet.

QUESTION NO: 18
JITVMアクセスを実装することを計画しています。どの仮想マシンがサポートされますか？
A.VM1およびVM3のみ
B.VM1。 VM2。 VM3、およびVM4
C.VM2、VM3、およびVM4のみ
D.VM1のみ
Answer: A

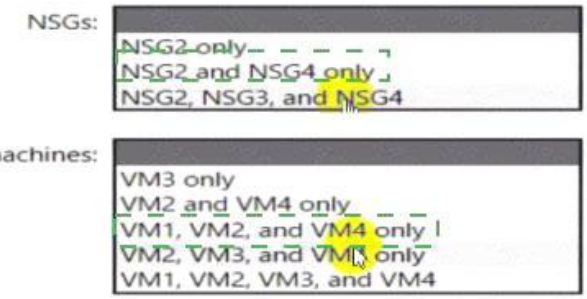
QUESTION NO: 19
技術的な要件を満たすには、storage1を暗号化する必要があります。どのキーボールトを使用できますか？
A.KeyVault1のみ
B.KeyVault2およびKeyVault3のみ
C.KeyVault1およびKeyVault3のみ
D.KeyVault1KeyVault2およびKeyVault3
Answer: B
Explanation:
The storage account and the key vault must be in the same region and in the same Azure Active Directory (Azure AD) tenant, but they can be in different subscriptions.
Storage1 is in the West US region. KeyVault1 is the only key vault in the same region.

Reference:
https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview

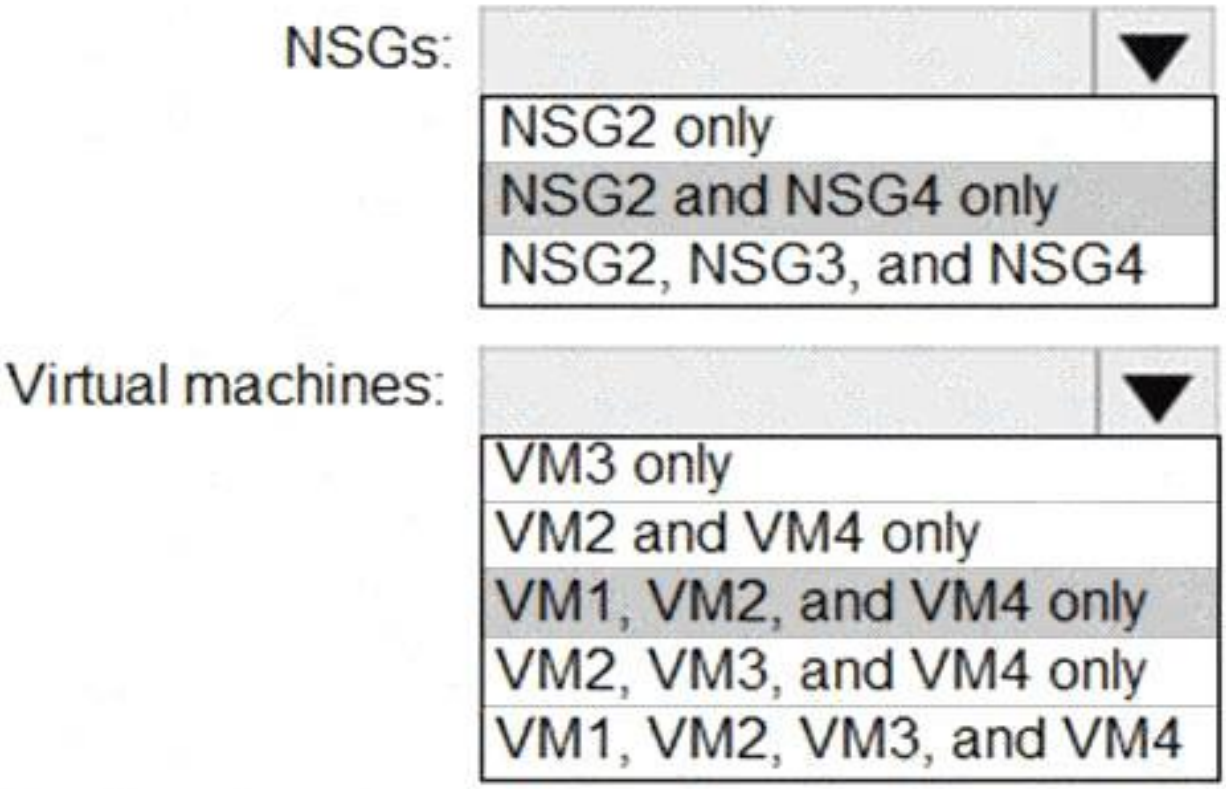
QUESTION NO: 20
ASG1およびASG2の計画された変更を実装します。
どのNSGでASG1を使用できますか。また、どの仮想マシンのネットワークインターフェイスをASG2に割り当てることができますか？
Answer Area



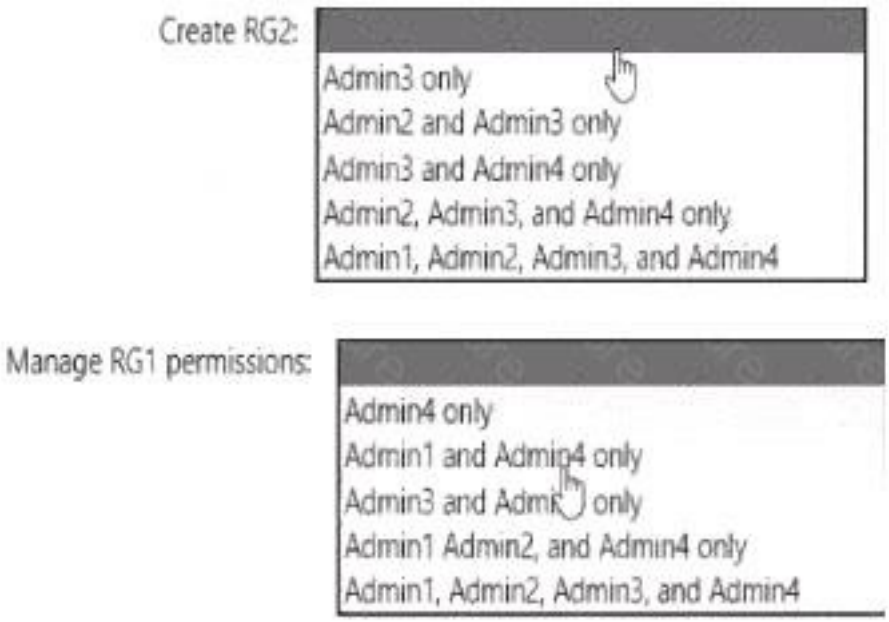
Answer:
Answer Area



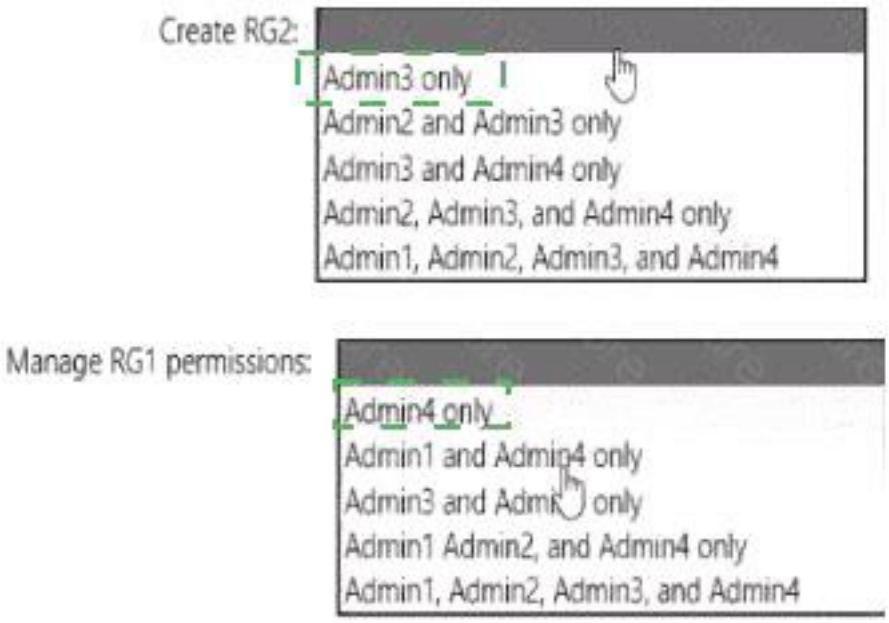
Explanation:
Graphical user interface, text, application, chat or text message Description automatically generated



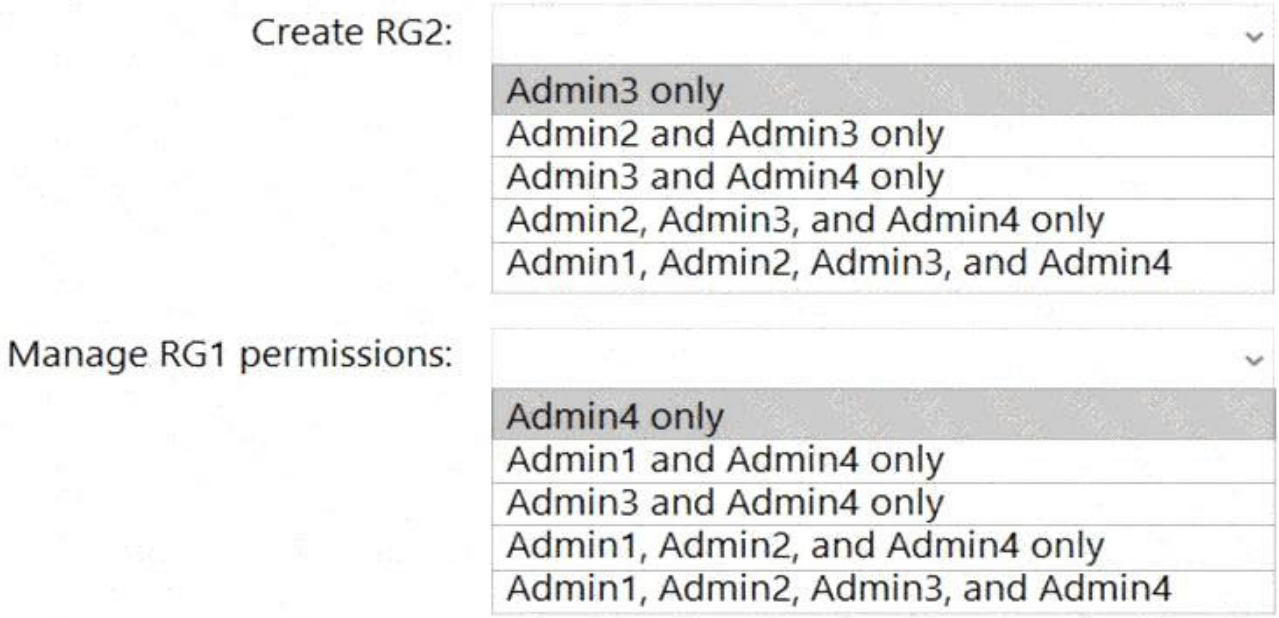
QUESTION NO: 21
RG2の作成とRG1の権限の管理を委任する必要があります。どのユーザーが各タスクを実行できますか？回答するには、回答領域で適切なオプションを選択します。注：正しい選択はそれぞれ1ポイントの価値があります



Answer:

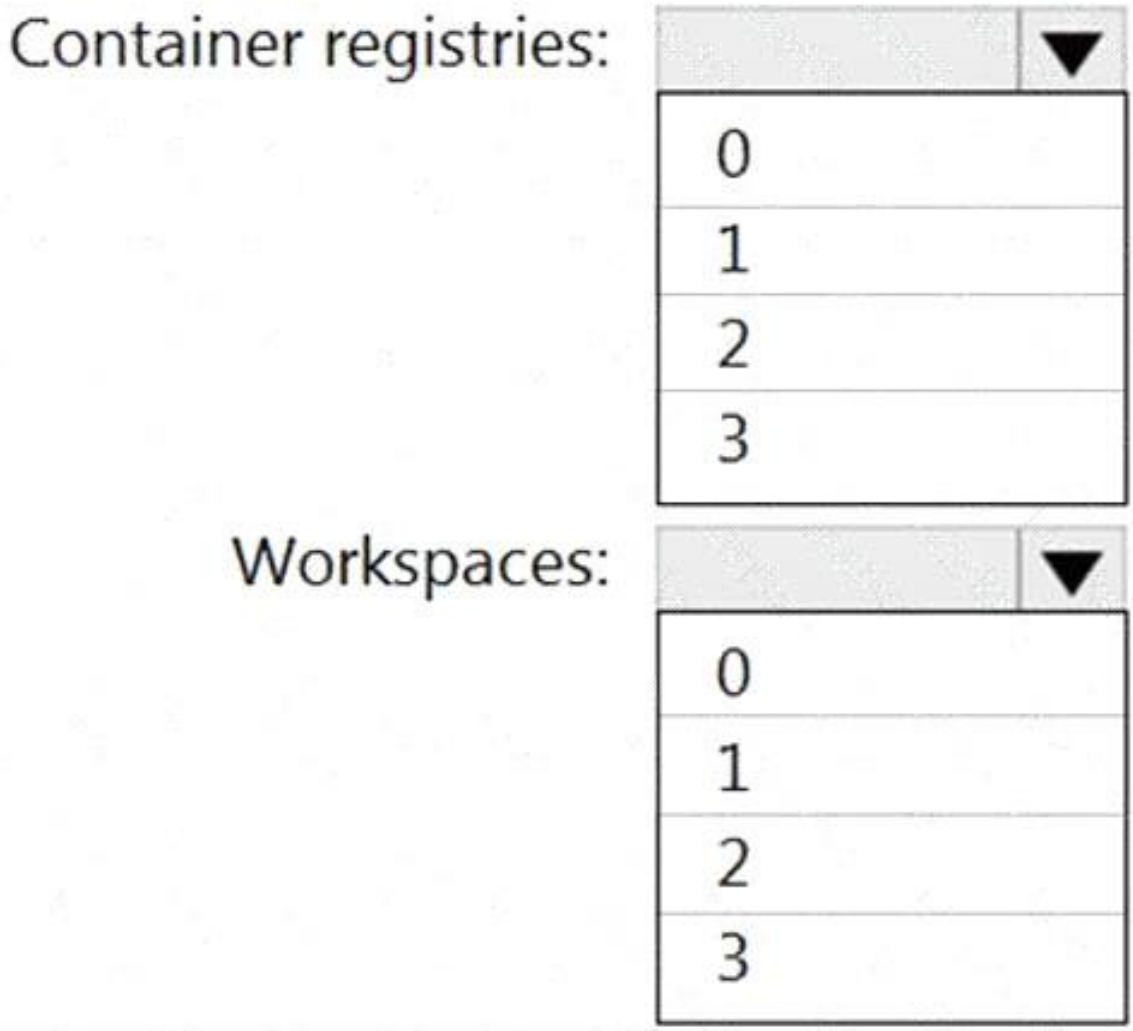


Explanation:
Graphical user interface, text, application, chat or text message Description automatically generated

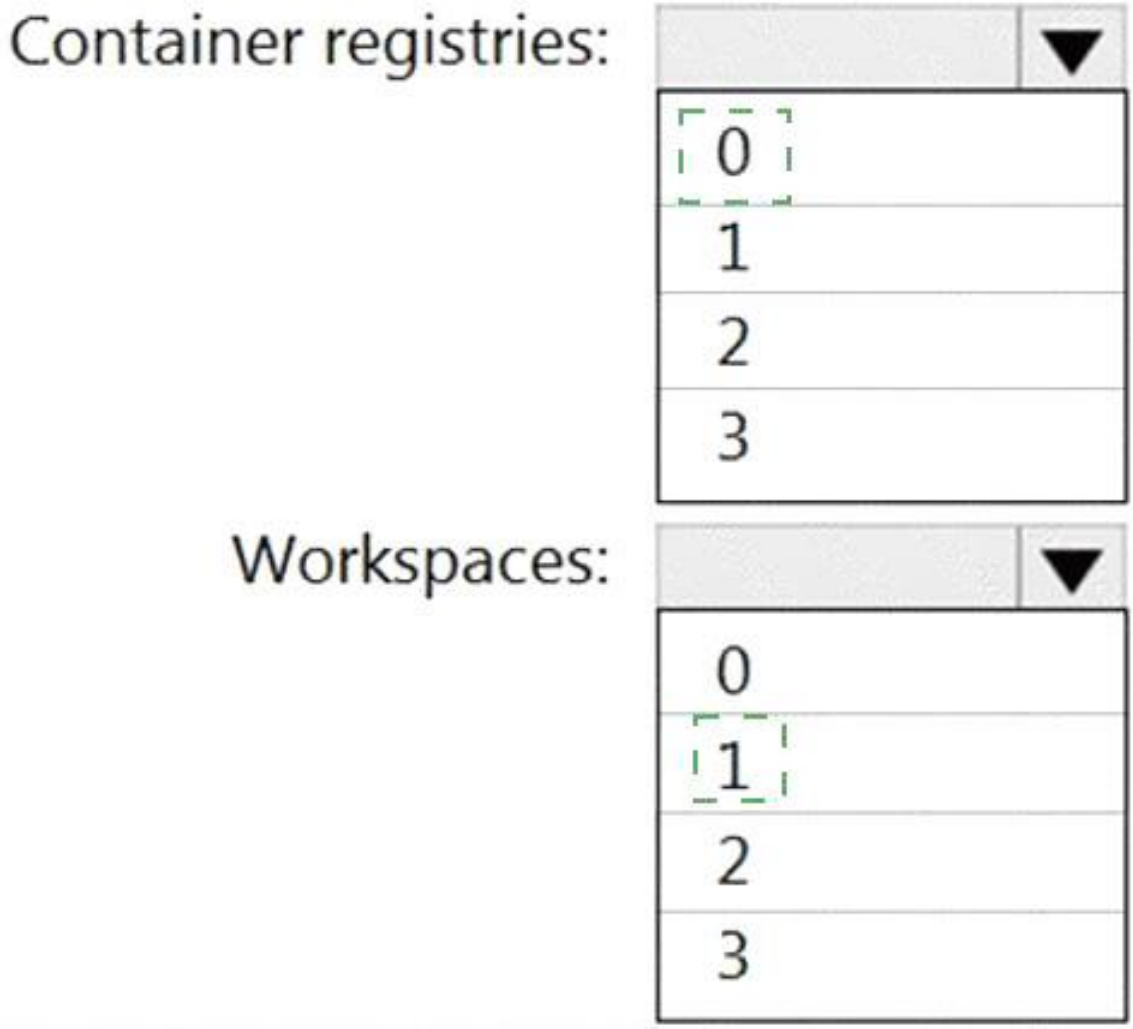


Box 1: Admin3 only
The Contributor role has the necessary write permissions to create the resource group.
Box 2: Admin4 only
You need Owner level access to be able to manage permissions. The Contributor role can do most things but cannot modify permissions on existing objects.

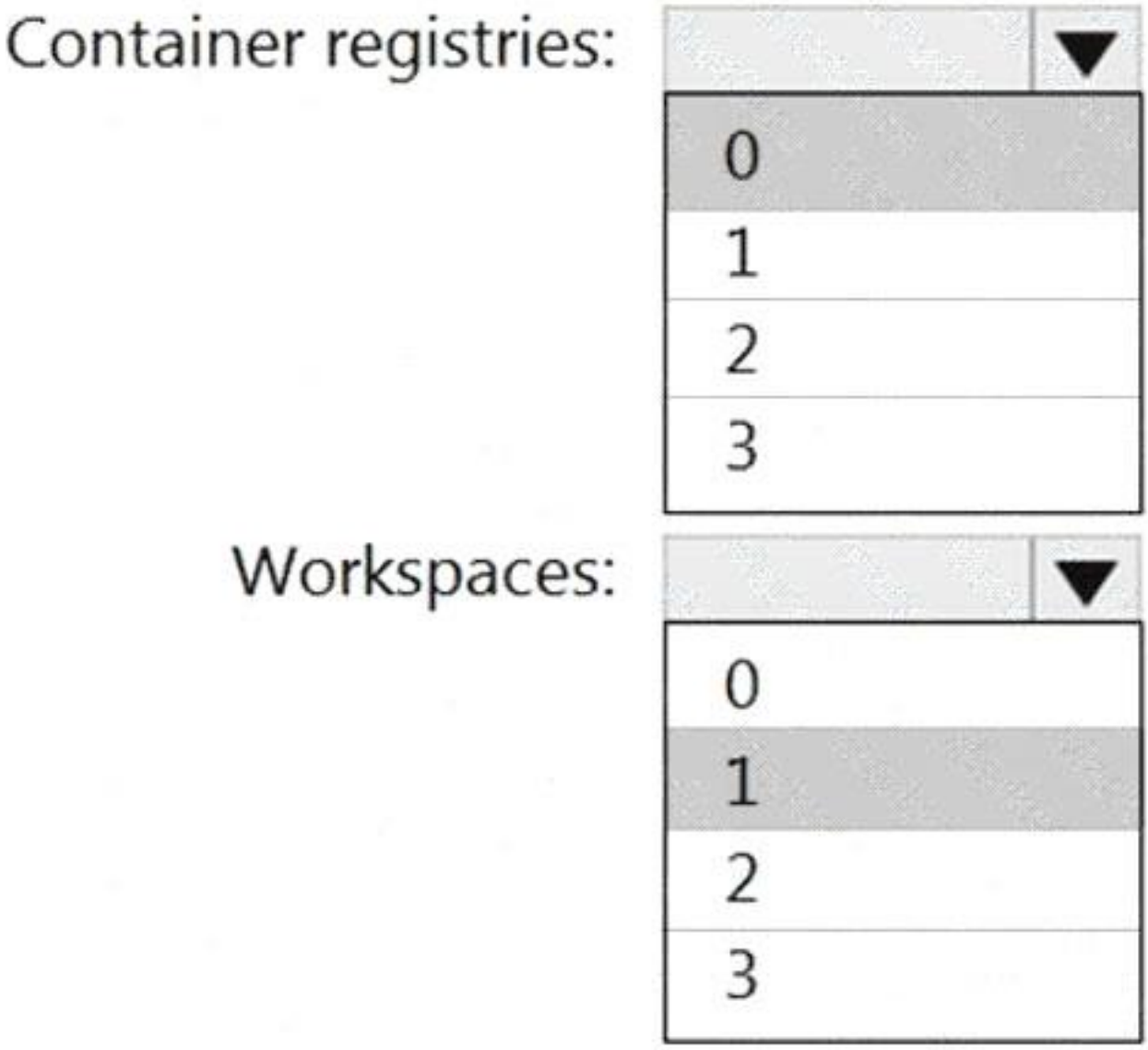
QUESTION NO: 22
技術的な要件を満たすには、AzureSentinelノートブックのサポートを構成する必要があります。
必要なAzureコンテナーレジストリとAzureMachine Learningワークスペースの最小数はいくつですか？



Answer:

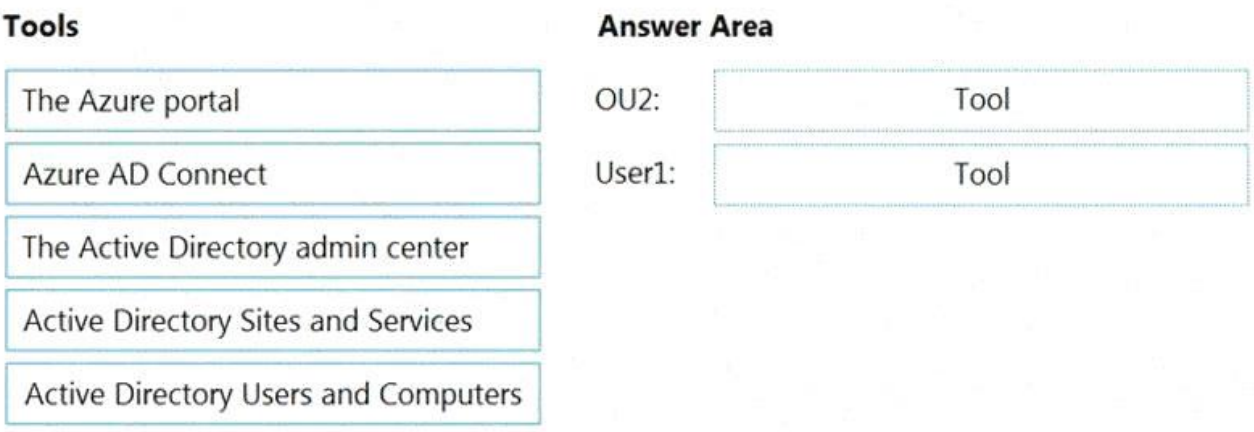


Explanation:
Table Description automatically generated with medium confidence

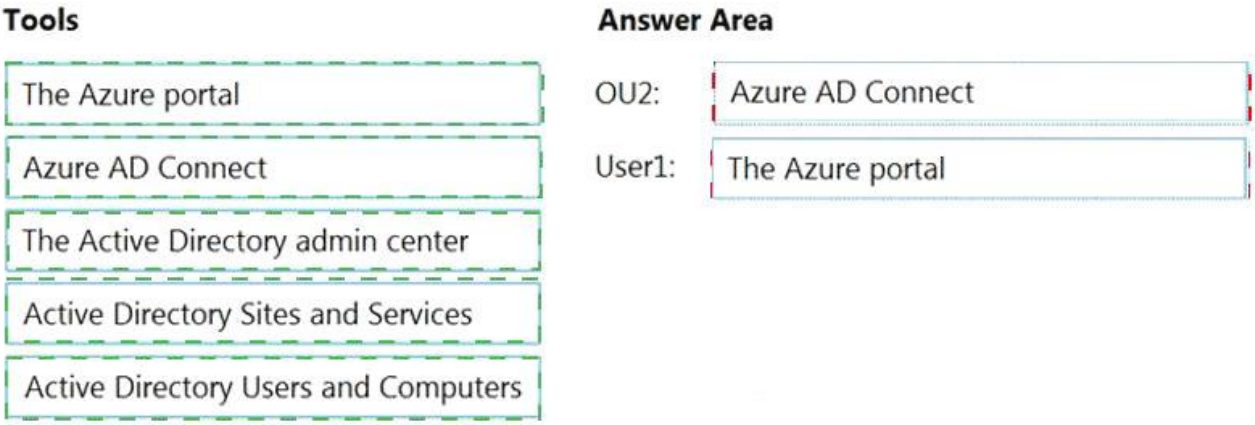


Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

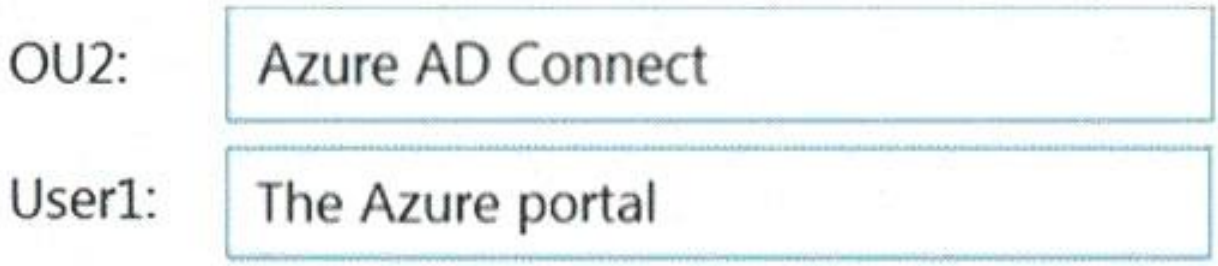
QUESTION NO: 23
OU2とUser1に対して計画された変更を実行する必要があります。
どのツールを使用する必要がありますか？答えるには、適切なツールを正しいリソースにドラッグします。各ツールは、1回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、分割バーをペイン間でドラッグするか、スクロールする必要がある場合があります。
注：正しい選択はそれぞれ1ポイントの価値があります。



Answer:



Explanation:
Table Description automatically generated



QUESTION NO: 24
VM4用にAzureDisk
Encryptionを構成する予定です。暗号化キーを格納するために使用できるキーボールトはどれですか？
A.KeyVault1
B.KeyVault3
C.KeyVault2
Answer: A
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 NO: 25
財務部門のユーザーの技術要件を満たす必要があります。
どのCAPolicy1設定を変更する必要がありますか？
A.クラウドアプリまたはアクション
B.条件
C.付与
D.セッション
Answer: D
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session- lifetime

QUESTION NO: 26
Azure Security Centerから、SecPol1をデプロイする必要があります。
あなたは最初に何をすべきですか？
A.AzureDefenderを有効にします。
B.Azure管理グループを作成します。
C.イニシアチブを作成します。
D.継続的なエクスポートを構成します。
Answer: B
Reference:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/security-center/custom-security-policies.md
https://zimmergren.net/create-custom-security-center-recommendation-with-azure-policy/
Topic 4, Fabrikam, Inc.
Case Study
Overview
Existing Environment
Network Environment
Cloud Environment
Sub1 Resources
Fabrikam, Inc. is a consulting company. The company has a main office in New York City and branch offices in Amsterdam and Singapore.
The on-premises network contains a datacenter in each office.
Fabtikam has two Azure subscriptions named Sub1 and Sub2 and a Microsoft 365 subscription that includes Microsoft 365 E5 licenses.
All the subscriptions are linked to a Microsoft Entra tenant named fabrikam.com that contains the identities shown in the following table.

Name	Type	Microsoft Entra role	Azure role assignment for Sub1
Admin1	User	Privileged Authentication Administrator	Resource Policy Contributor
Admin2	User	Compliance Administrator	User Access Administrator
Admin3	User	Authentication Administrator	Contributor
Admin4	User	Global Administrator	*None*
User1	User	*None*	Reader
AKS1	System-assigned managed identity	*None*	*None*
ID1	User-assigned managed identity	*None*	*None*

The tenant contains the groups shown in the following table.

Name	Type	Role assignments allowed
Group1	Security	Yes
Group2	Security	No
Group3	Microsoft 365	Yes
Group4	Microsoft 365	No

All devices are enrolled in Microsoft Intune.
Sub2 Resources
Sub1 contains a resource group named RG1 that contains the resources shown in the following table.

Name	Description	Location
SQLServer1	Azure SQL Database logical server	East US
SQLdb1	Database on SQLServer1	East US
VM1	Virtual machine	East US
AKS1	Azure Kubernetes Service (AKS) cluster	East US
Registry1	Azure container registry	East US
storage1	Storage account	East US
AKV1	Azure key vault	East US

SQLServer1 uses Microsoft SQL Server authentication.
Sub1 has an Azure Web Application Firewall (WAF) named WAF1 that has the following types of rule sets:
* Bot Manager 1.1
* Azure-managed Default Rule Set (DRS)
Sub1 has the following compliance standards assigned in Microsoft Defender for Cloud:

* MIST SP 800-53 Rev. 4
* Microsoft cloud security benchmark (MCSB)
* System and Organization Controls (SOC) 2 Type 2

Planned Changes and Requirements

Planned Changes

Sub2 contains a resource group named RG2.

Fabtikam plans to implement the following changes:

* Deploy the following key vaults to RG1:
o AKV2 in the West Europe Azure region
o AKV3 in the Central US Azure region
o AKV4 in the East US Azure region
* Deploy the following key vaults to RG2:
o AKV5 in the East US region
* Configure VM1 to read data from storage1.
* Create function apps that have the following hosting plans:
o Fa1: Flex Consumption hosting plan
o Fa2: Consumption hosting plan
o Fa3: Dedicated hosting plan
* For WAF1, implement rate limiting rules based on the request location.
* Enable the NIST SP 800-53 Rev. 5 compliance standard in Defender for Cloud.
* Create a new storage account named storage2 that supports Azure Table storage.
* Enforce multifactor authentication (MFA) when database administrators access SQLdbl.
* Implement ExpressRoute circuits to the on-premises network as shown in the following table.

Name	Location	Deployment type
ER1	West Europe	ExpressRoute with a connectivity provider
ER2	West Europe	ExpressRoute Metro with a connectivity provider
ER3	East US	ExpressRoute Direct
ER4	Southeast Asia	ExpressRoute Metro Direct

* For RG1. create a new Privileged Identity Management (PIM) eligible role assignment that assigns the Contributor role to supported groups.

Technical Requirements

Fabrikam has the following technical requirements:

* If VM1 is deleted, the permissions for VM1 must be removed automatically.
* The AKS1 managed identity must only be able to pull images from Registry1.
* The ID1 managed identity must be able to push images to and pull images from Registry 1.
* All the data in the storage accounts must be encrypted by using Fabrikam-managed keys.
* All outbound traffic from the function apps to the on-premises network must use ExpressRoute circuits.
* ExpressRoute connectivity between the on-premises network and the Azure environment must be encrypted by using Layer 2 or Layer 3 encryption.

QUESTION NO: 27

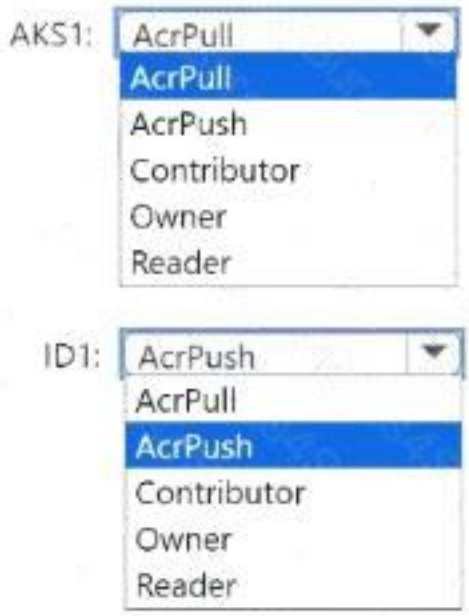
Defender for Cloud
の計画された変更を実装するには、ユーザーに委任する必要があります。
ソリューションは最小権限の原則に従う必要があります。
どのユーザーを選択すべきでしょうか?
A. 管理者1
B. 管理者2
C. 管理者3
D. 管理者4
Answer: B

QUESTION NO: 28
WAF1 に対して計画された変更を実装する必要があります。
ソリューションは管理の手間を最小限に抑える必要がある
何をすべきでしょうか?
A. Azure ポリシーを作成します。
B. Azure 管理の DRS を変更します。
C. カスタムルールを追加します。
D. Bot Manager 1.1 ルール セットを変更します。
Answer: C

QUESTION NO: 29
SQLdb1 に対して計画された変更を実装する必要があります。
実行すべき 2
つのアクションはどれですか。それぞれの正解は解決策の一部を示しています。
注意: 正しい選択ごとに 1 ポイントが付与されます。
A. コンプライアンス ポリシーを作成します。
B. SQLServer1 の Microsoft Entra 認証を構成します。
C. 条件付きアクセス ポリシーを作成します。
D. SQLdb1 のユーザー割り当てマネージド ID を構成します。
E. SQLdb1 のフェデレーション クライアント ID を構成します。
Answer: B C

QUESTION NO: 30
技術要件を満たすには、AKS1 および ID1 マネージド ID
を構成する必要があります。ソリューションは、最小権限の原則に従う必要があります。
各 ID にどのロールを割り当てる必要がありますか?
回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area

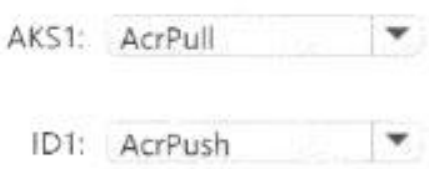


Answer:

Answer Area

Explanation:

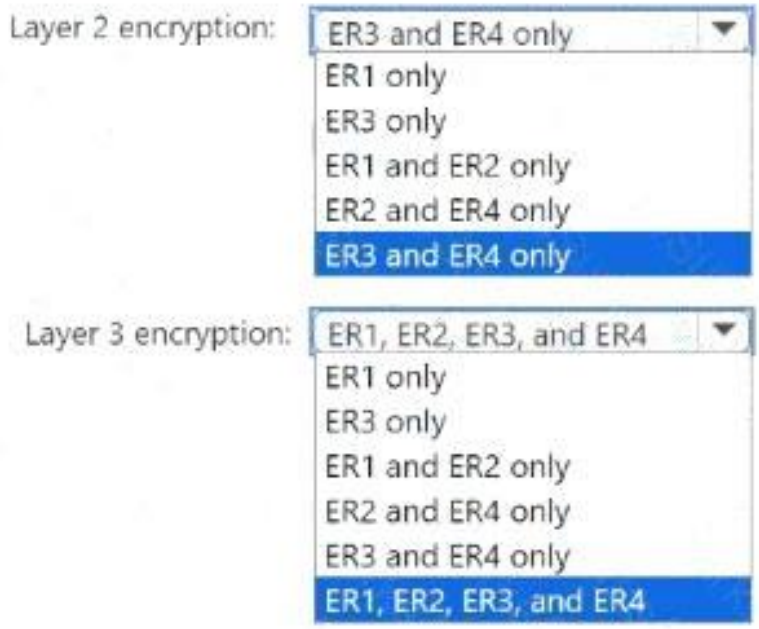
Answer Area



QUESTION NO: 31
VM1 が storage1 にアクセスできるように、計画された変更を実装する必要があります。
ソリューションは技術要件を満たしている必要があります。
まず何をすべきでしょうか?
A. VM1 でシステム割り当てマネージド ID を構成します。
B. ID1 のフェデレーション ID 資格情報を構成します。
C. ストレージ 1 にストレージ BLOB データ リーダー ロールを割り当てます。
D. VM1にID1を割り当てます。
E. storage1 にロール割り当て条件を追加します。
Answer: A

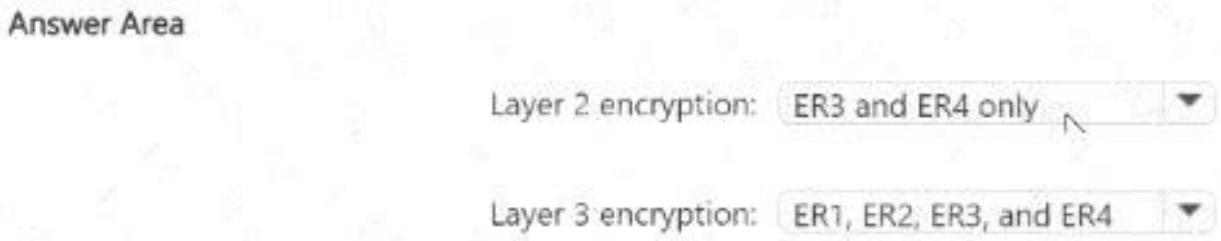
QUESTION NO: 32
計画中のExpressRoute実装に適した暗号化ソリューションを推奨する必要があります。ソリューションは技術要件を満たす必要があります。
各暗号化の種類ごとにどの ExpressRoute 回線を推奨すればよいですか?
回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area



Answer:

Explanation:



QUESTION NO: 33
キー コンテナーに対して計画された変更を実装します。
AKV1 バックアップをどのキー コンテナーに復元できますか?
A. AKV4のみ
B. AKV3とAKV4のみ
C. AKV4とAKV5のみ
D. AKV2、AKV3、AKV4のみ
E. AKV2、AKV3、AKV4、およびAKV5
Answer: C

QUESTION NO: 34
SQL1という名前のAzure SQL Databaseサーバーがあります。
SQL1のAdvanced Threat
Protectionを有効にして、すべての脅威検出タイプを検出する予定です。
Advanced Threat Protectionは脅威としてどのアクションを検出しますか？
A. A user updates more than 50 percent of the records in a table.
B. A user attempts to sign as select * from table1.

C. A user is added to the db_owner database role.

D. A user deletes more than 100 records from the same table.

Answer: B

Explanation:

Advanced Threat Protection can detect potential SQL injections: This alert is triggered when an active exploit happens against an identified application vulnerability to SQL injection. This means the attacker is trying to inject malicious SQL statements using the vulnerable application code or stored procedures.

References:

https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview

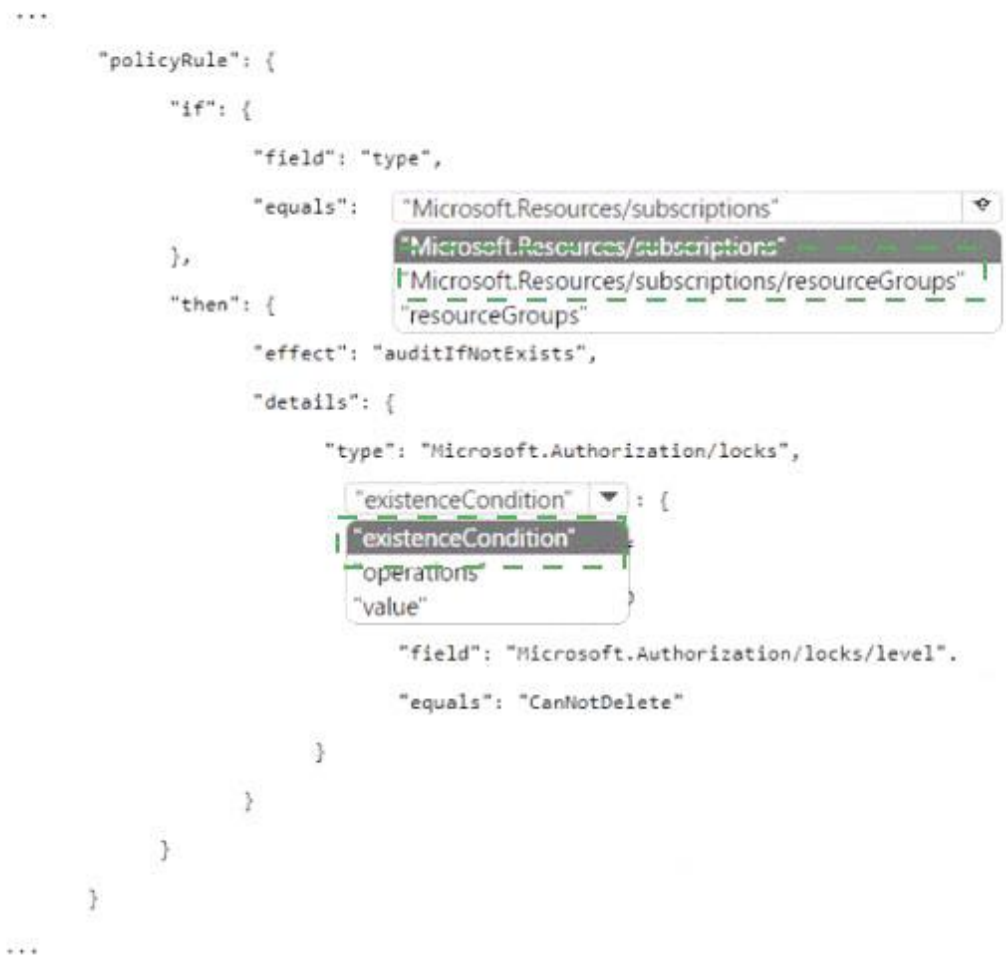
QUESTION NO: 35

Microsoft Defender for Cloud のカスタム ポリシー イニシアチブを展開する予定です。
削除ロックを持つすべてのリソース グループを識別する必要があります。
ポリシー定義はどのように完了すればよいでしょうか?
回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Answer:

Answer Area



Explanation:
A screenshot of a computer Description automatically generated

Answer Area


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