Exam Questions az-500

Microsoft Azure Security Technologies

https://www.2passeasy.com/dumps/az-500/

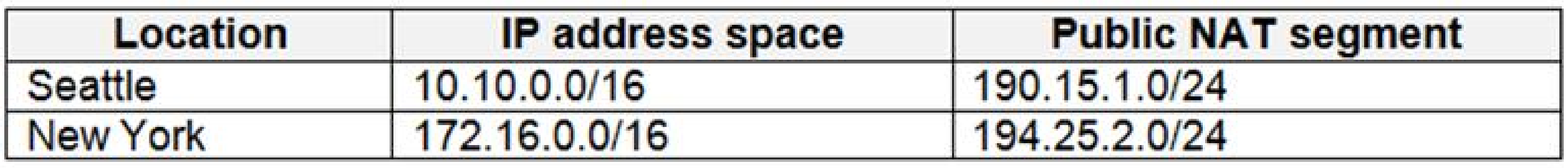
NEW QUESTION 1
You need to ensure that User2 can implement PIM.
What should you do first?

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.

Answer: A

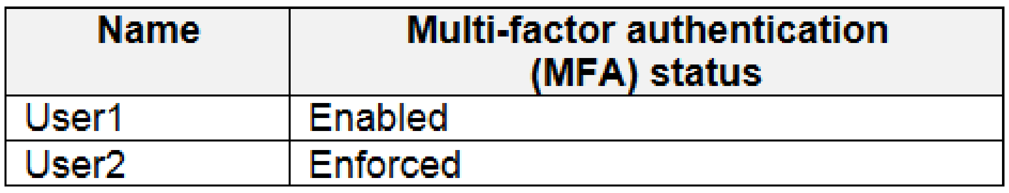
Explanation:
To start using PIM in your directory, you must first enable PIM.
1. Sign in to the Azure portal as a Global Administrator of your directory.
You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com),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

NEW QUESTION 2
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.



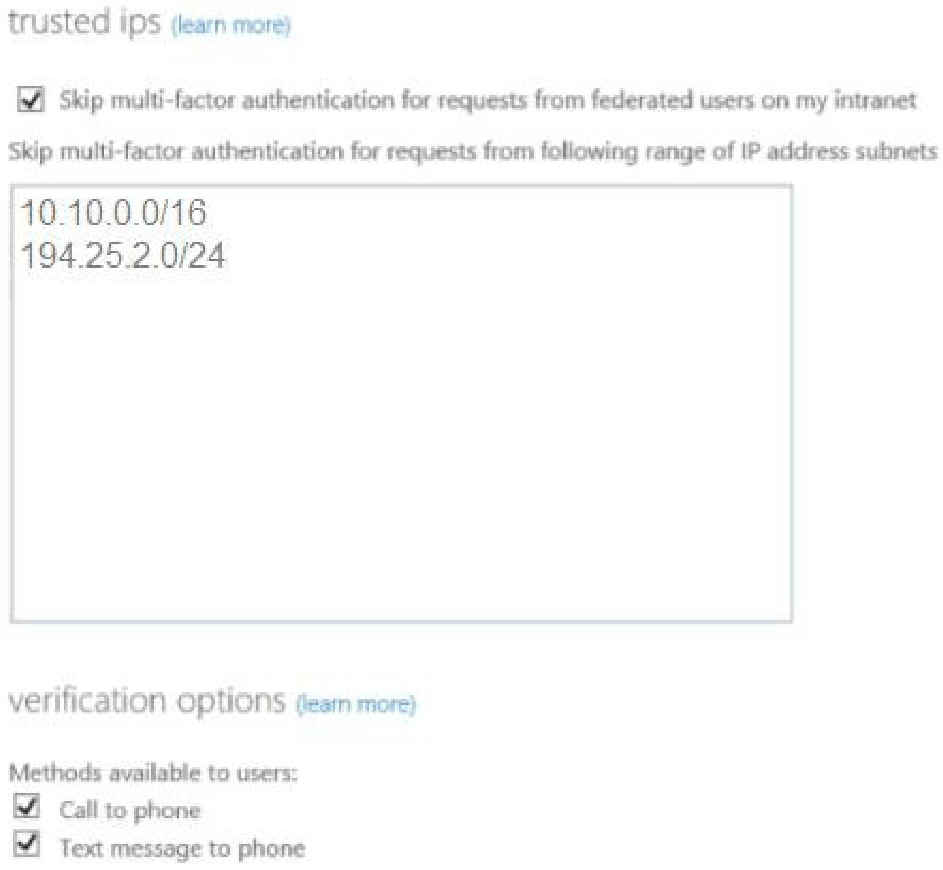
Location	IP address space	Public NAT segment
Seattle	10.10.0.0/16	190.15.1.0/24
New York	172.16.0.0/16	194.25.2.0/24

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

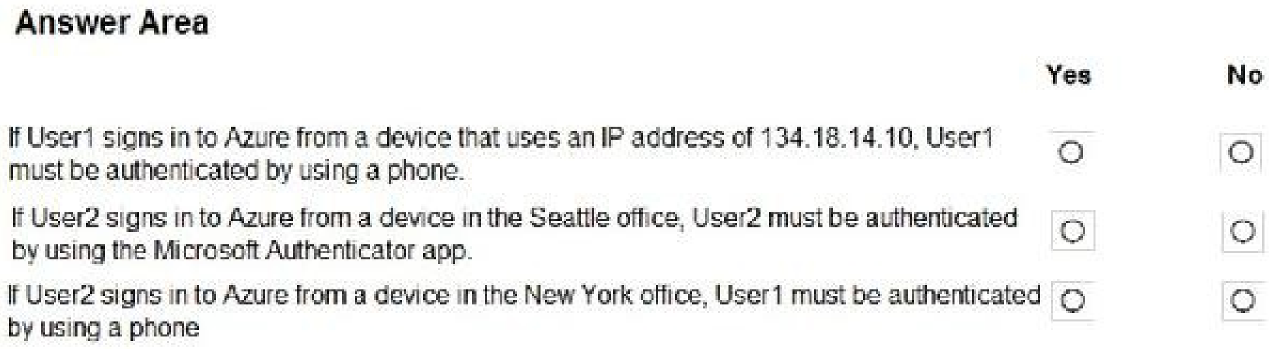
Skip multi-factor authentication for requests from following range of IP address subnets

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

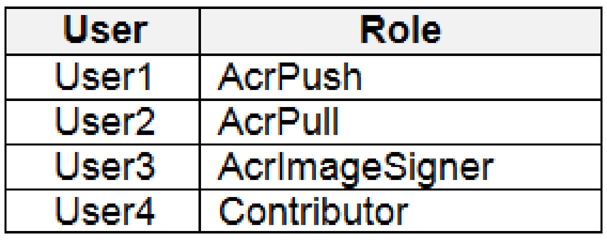
	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	○	○
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	○	○
If User2 signs in to Azure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

A. Mastered
B. Not Mastered

Answer: A

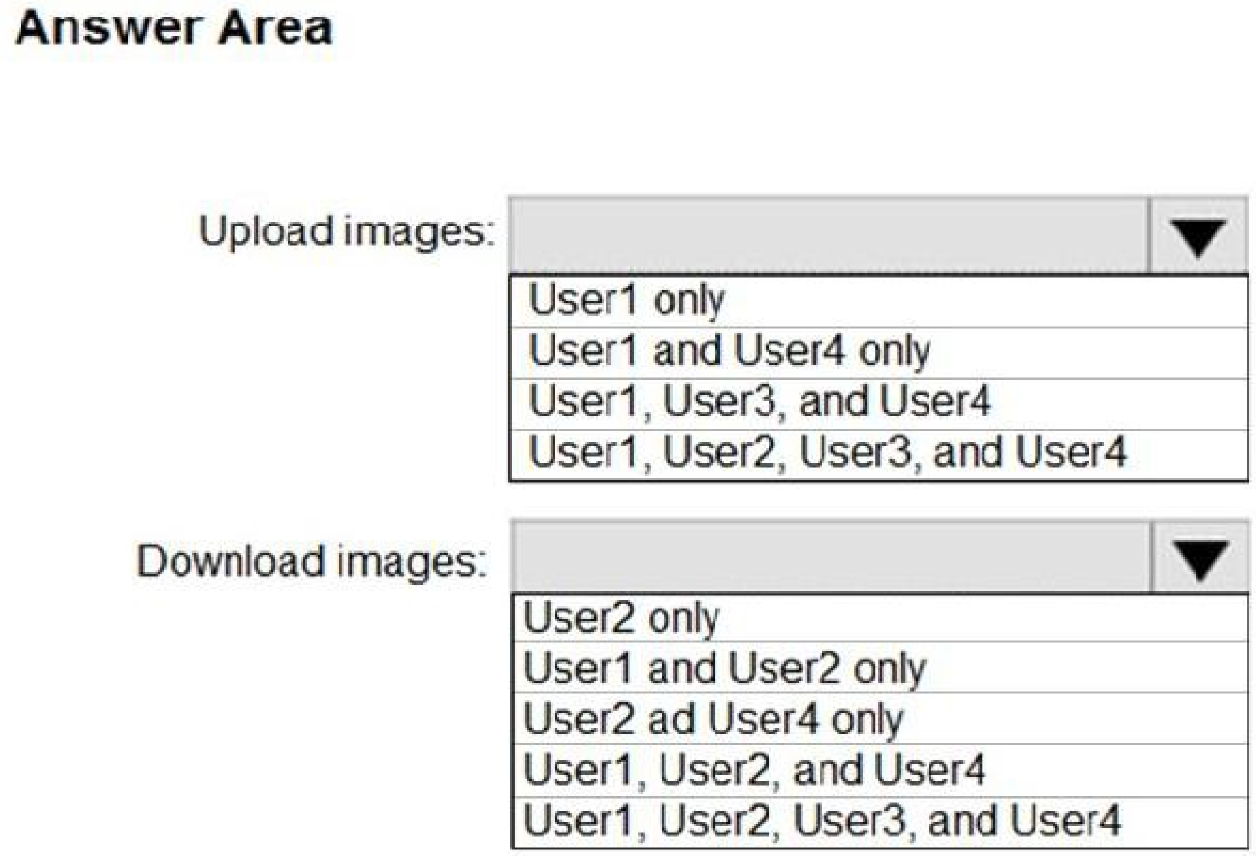
Explanation:
Box 2: No
Use of Microsoft Authenticator is not required.
Note: Microsoft Authenticator is a multifactor app for mobile devices that generates time-based codes used during the Two-Step Verification process. Box 3: No
The New York IP address subnet is included in the "skip multi-factor authentication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

NEW QUESTION 3
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

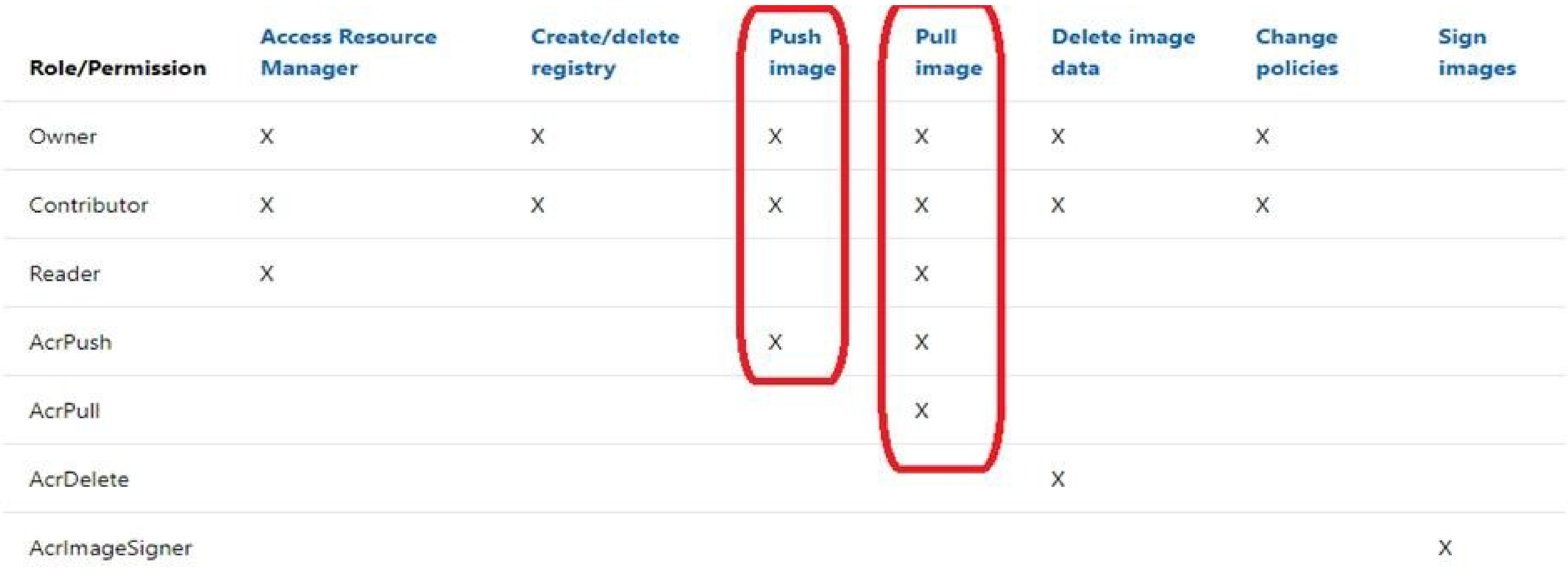
Upload images:
- User1 only
- User1 and User4 only
- User1, User3, and User4
- User1, User2, User3, and User4

Download images:
- User2 only
- User1 and User2 only
- User2 ad User4 only
- User1, User2, and User4
- User1, User2, User3, and User4

A. Mastered
B. Not Mastered

Answer: A

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

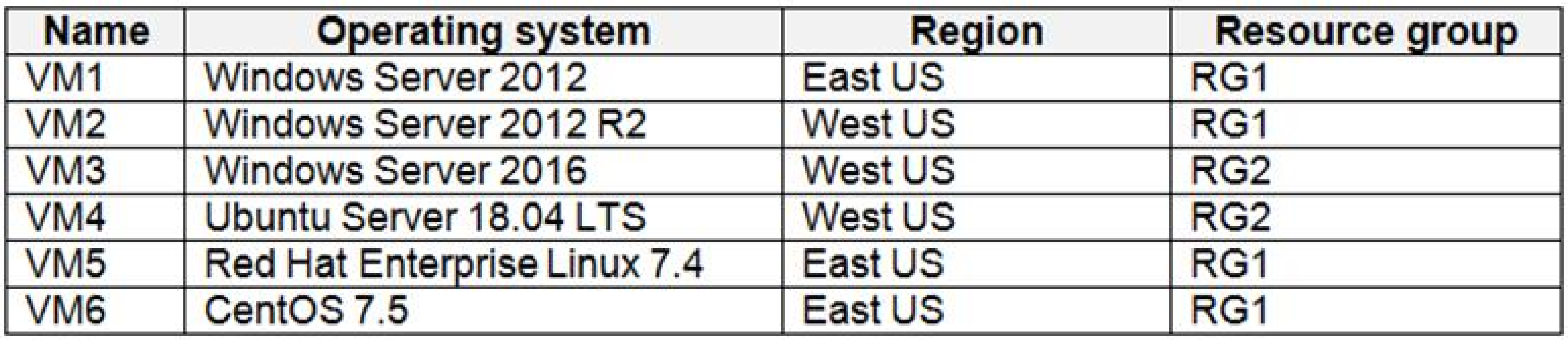
NEW QUESTION 4
You have Azure Resource Manager templates that you use to deploy Azure virtual machines.
You need to disable unused Windows features automatically as instances of the virtual machines are provisioned. What should you use?

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

Answer: B

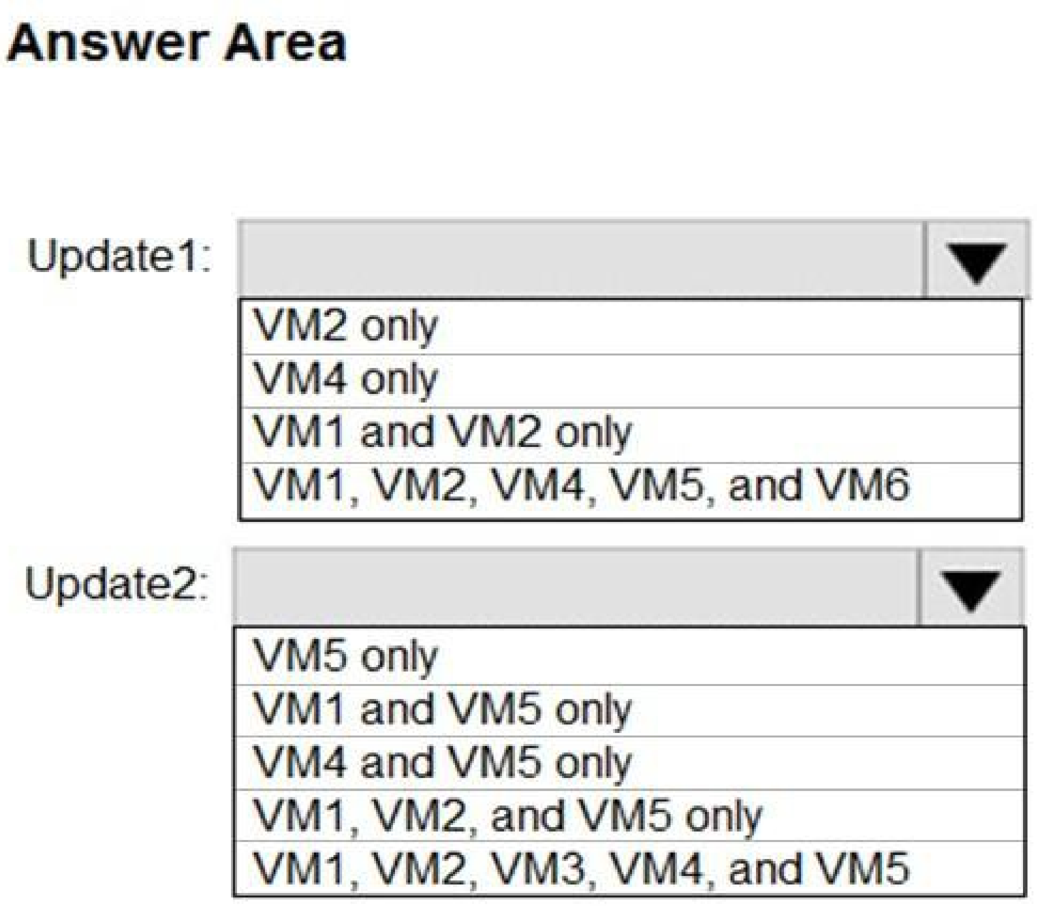
Explanation:
You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines.
Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSC-Service 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.
References:
https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started

NEW QUESTION 5
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

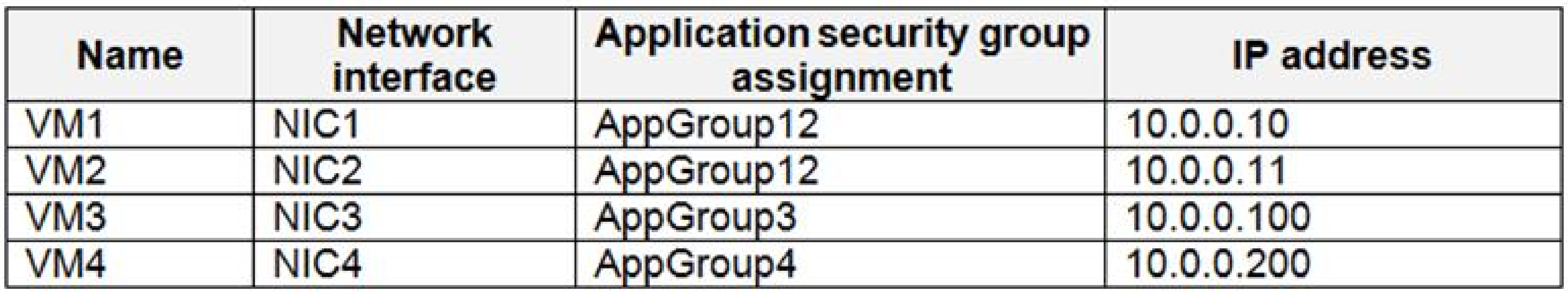
Update2:
- VM5 only
- VM1 and VM5 only
- VM4 and VM5 only
- VM1, VM2, and VM5 only
- VM1, VM2, VM3, VM4, and VM5

A. Mastered
B. Not Mastered

Answer: A

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

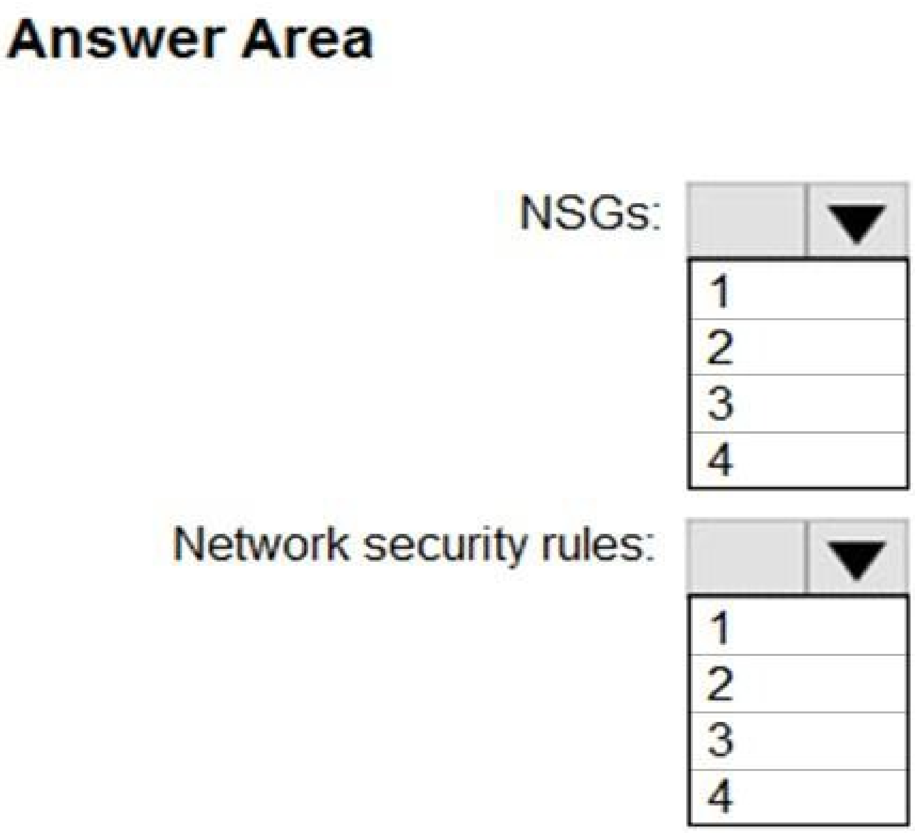
NEW QUESTION 6
HOTSPOT
You have an Azure subscription named Sub1.
You create a virtual network that contains one subnet. On the subnet, you provision the virtual machines shown in the following table.



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:



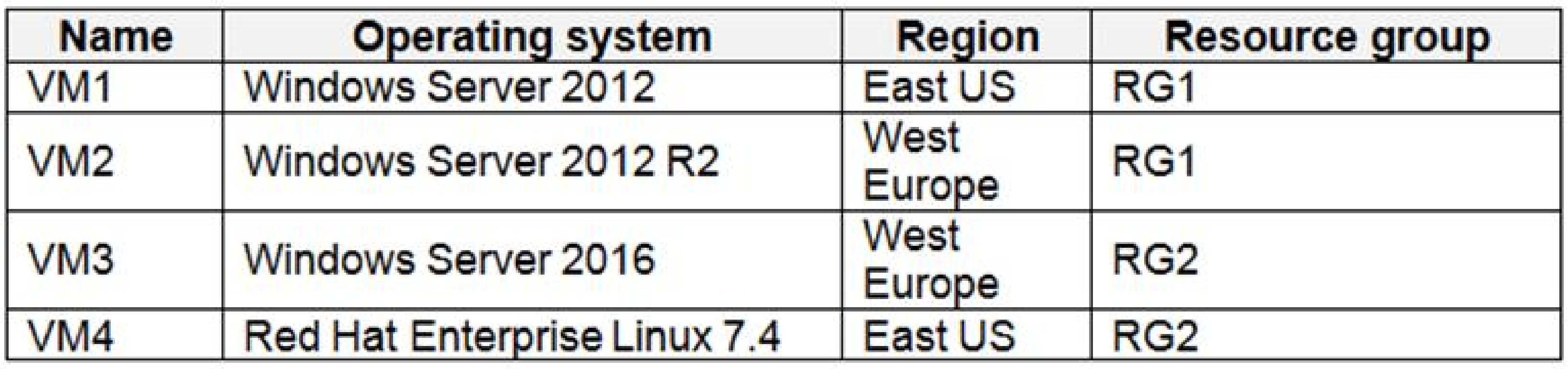
Answer Area

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 7
You have an 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

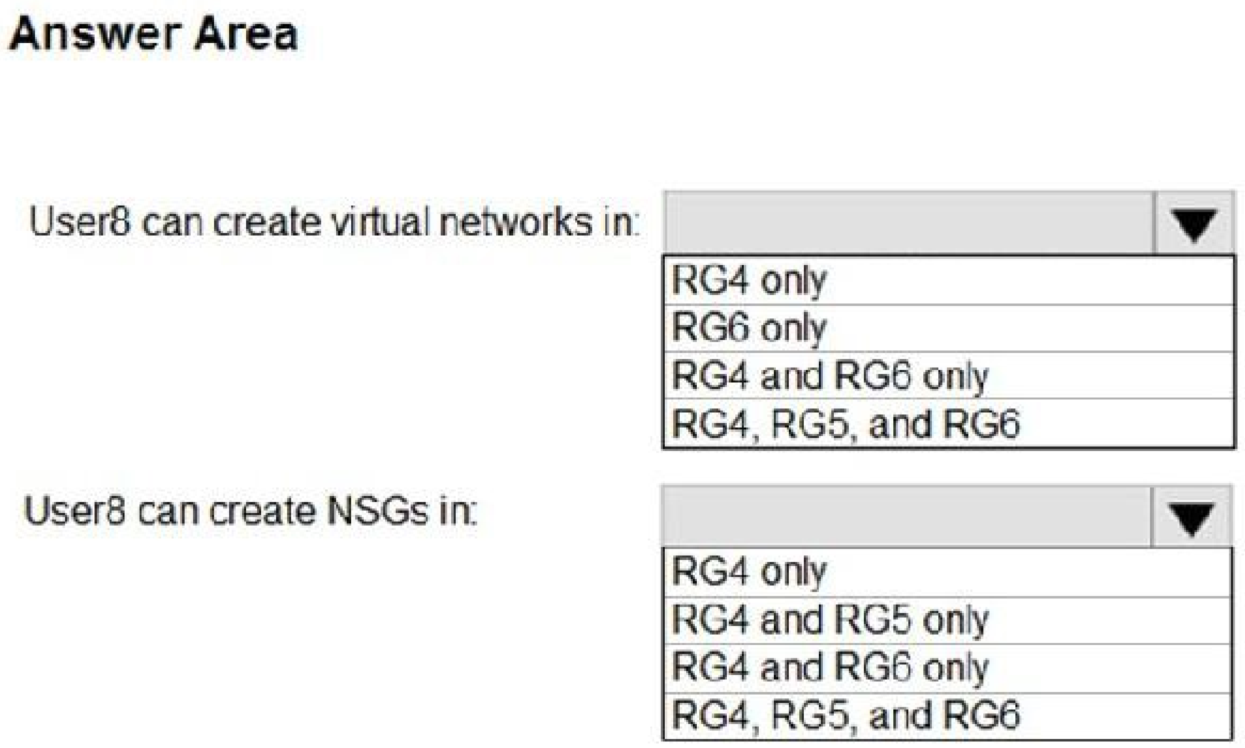
You create an Azure Log Analytics workspace named Analytics1 in RG1 in the East US region. Which virtual machines can be enrolled in Analytics1?

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

Answer: A

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

NEW QUESTION 8
HOTSPOT
You assign User8 the Owner role for RG4, RG5, and RG6.
In which resource groups can User8 create virtual networks and NSGs? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

User8 can create virtual networks in:
- RG4 only
- RG6 only
- RG4 and RG6 only
- RG4, RG5, and RG6

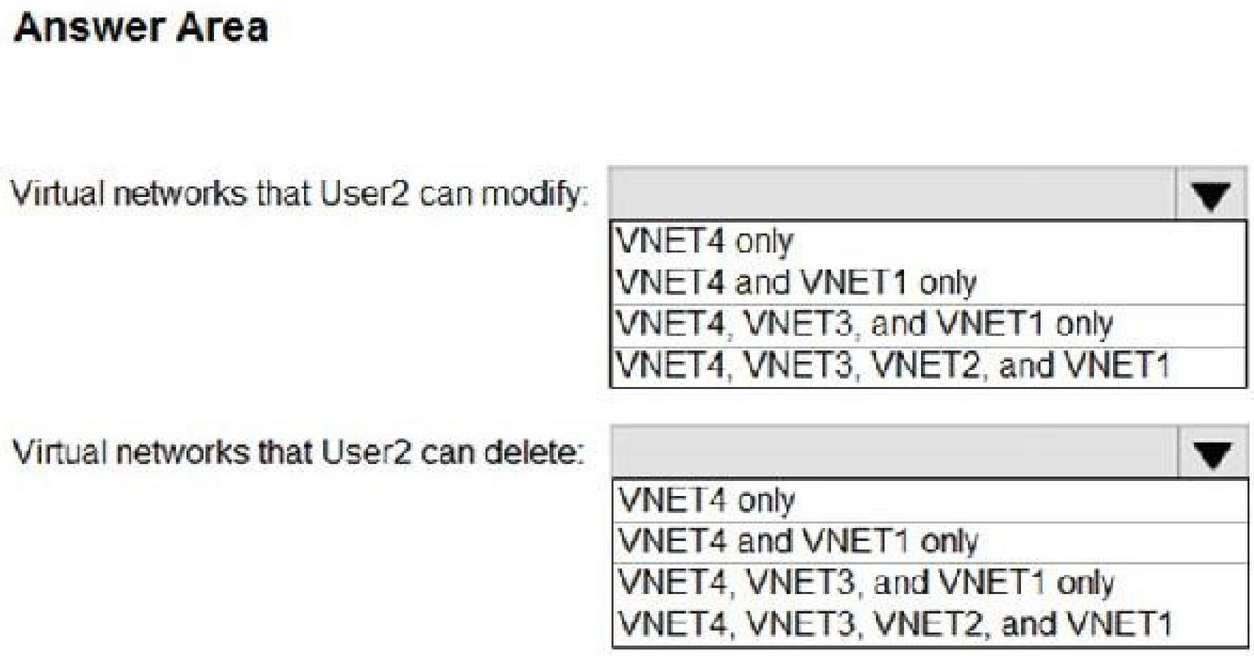
User8 can create NSGs in:
- RG4 only
- RG4 and RG5 only
- RG4 and RG6 only
- RG4, RG5, and RG6

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: RG4 only
Virtual Networks are not allowed for Rg5 and Rg6.
Box 2: Rg4,Rg5, and Rg6 Scenario:
Contoso has two Azure subscriptions named Sub1 and Sub2.
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6. You assign User8 the Owner role for RG4, RG5, and RG6
User8 city Sidney, Role:None
Note: A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager).
References:
https://docs.microsoft.com/en-us/azure/governance/policy/overview

NEW QUESTION 9
HOTSPOT
Which virtual networks in Sub1 can User2 modify and delete in their current state? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

Virtual networks that 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

A. Mastered
B. Not Mastered

Answer: A

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

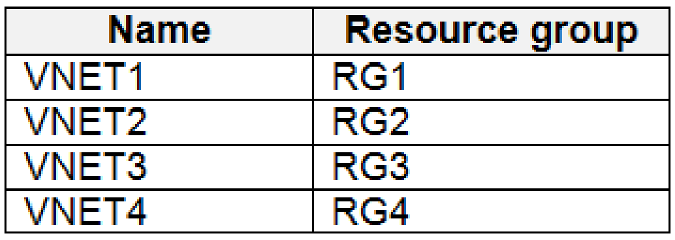
users to the permissions granted by the Reader role.

Scenario:

User2 is a Security administrator.

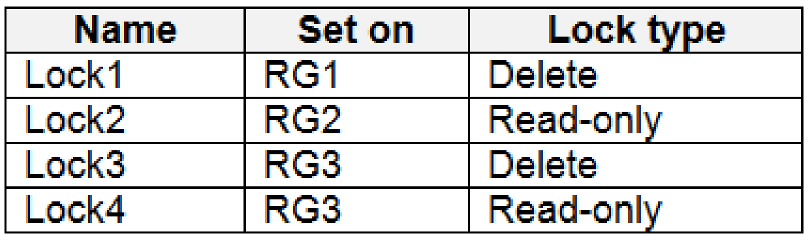
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

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

Testlet 2

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

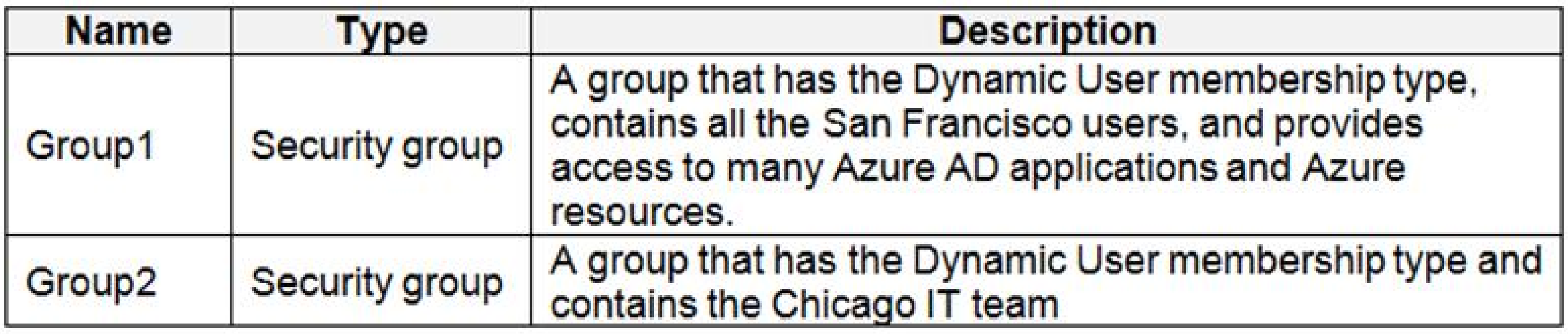
Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment

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

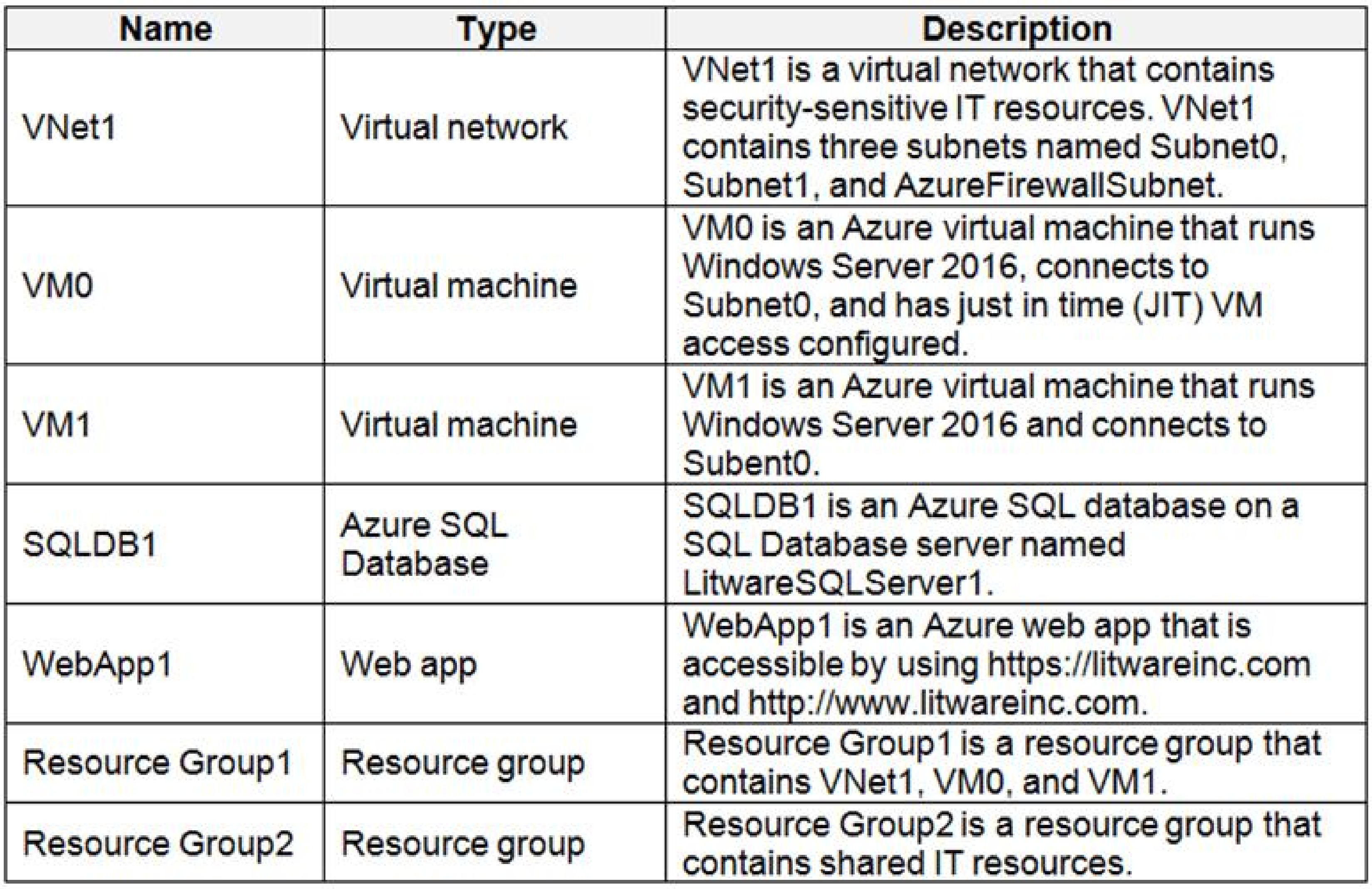
Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.



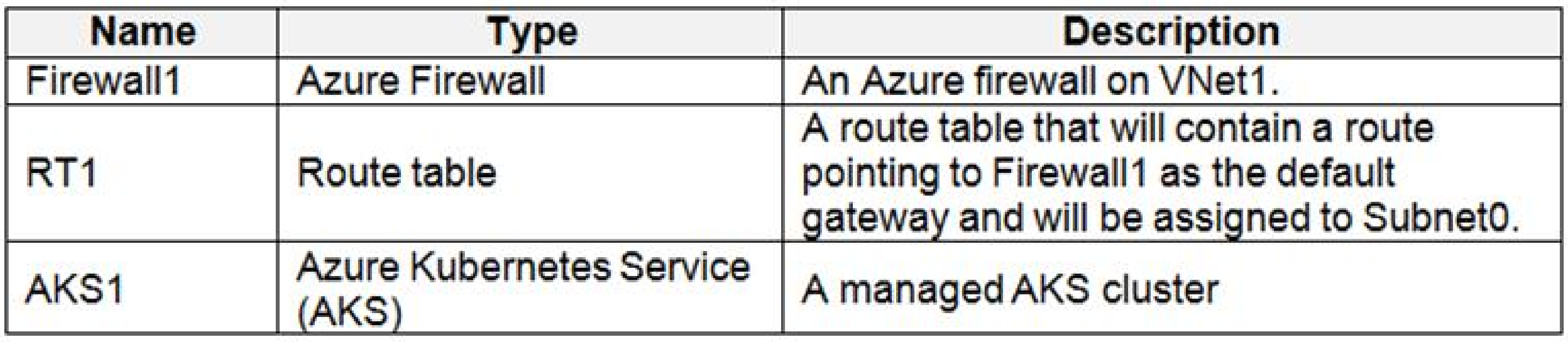
Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago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

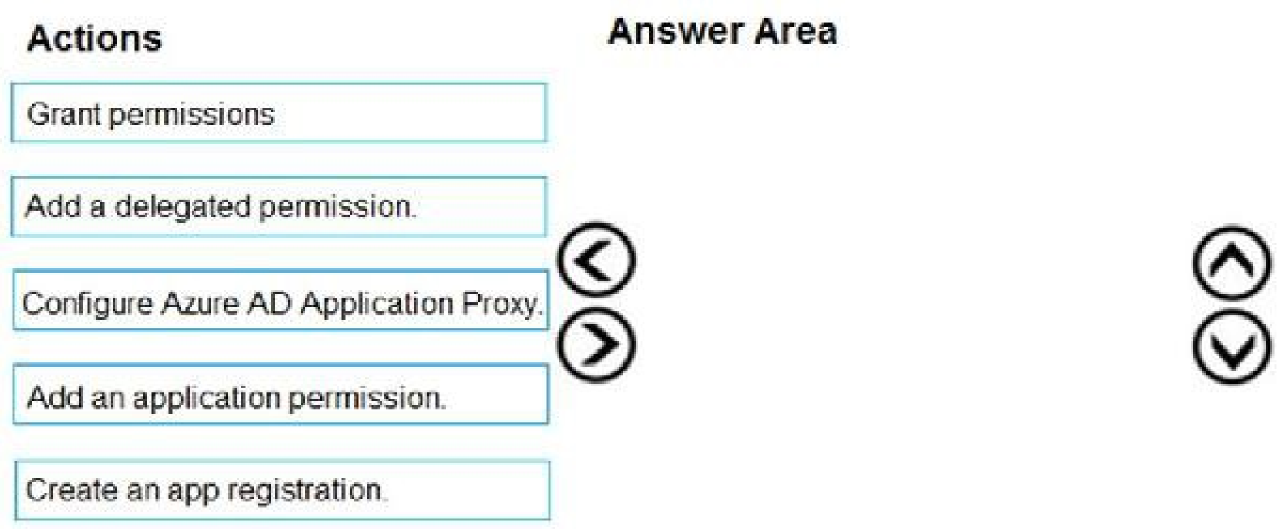
Azure Security Center is set to the Free tier.
Planned changes
Litware plans to deploy the Azure resources shown in the following table.



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.

NEW QUESTION 10
DRAG DROP
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.
The company is developing an application named App1. App1 will run as a service on server that runs Windows Server 2016. App1 will authenticate to contoso.com and access Microsoft Graph to read directory data.
You need to delegate the minimum required permissions to App1.
Which three actions should you perform in sequence from the Azure portal? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select and Place:



Actions

Grant permissions

Add a delegated permission.

Configure Azure AD Application Proxy.

Add an application permission.

Create an app registration.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 10
Your company uses Azure DevOps.
You need to recommend a method to validate whether the code meets the company’s quality standards and code review standards. What should you recommend implementing in Azure DevOps?

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

Answer: C

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

NEW QUESTION 12
......