AZ-500 Q&As

Microsoft Azure Security Technologies

Pass Microsoft AZ-500 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.lead4pass.com/az-500.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

SIMULATION

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. See the below.

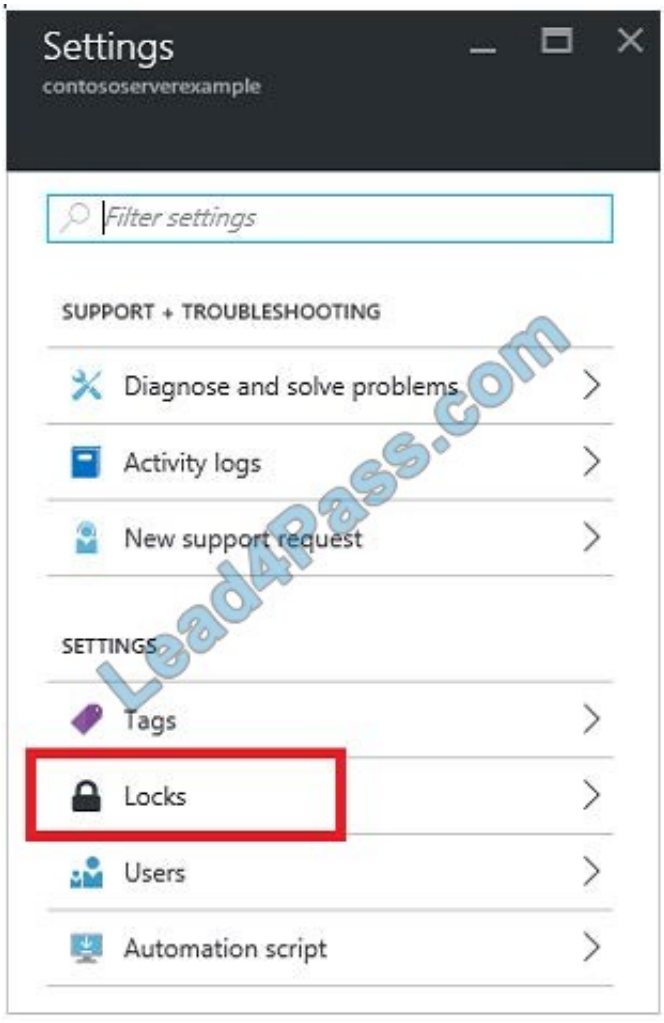
Correct Answer: A

Explanation:

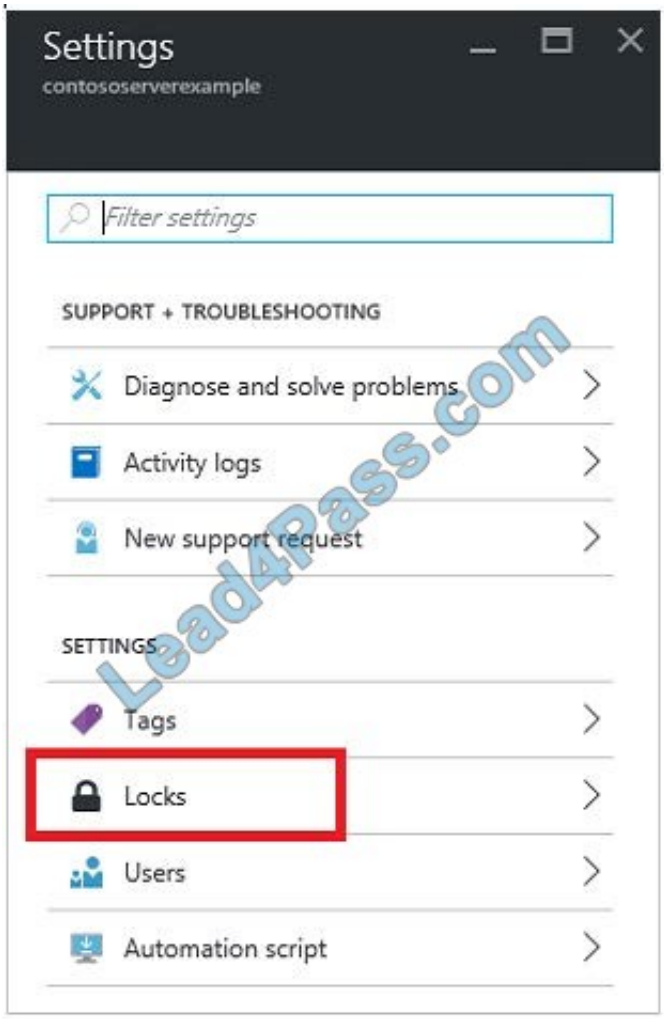
Locking prevents other users in your organization from accidentally deleting or modifying critical resources, such as Azure subscription, resource group, or resource.

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.



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 2

HOTSPOT

You have an Azure subscription that contains an Azure Sentinel workspace.

Azure Sentinel is configured to ingest logs from several Azure workloads. A third-party service management platform is used to manage incidents.

You need to identify which Azure Sentinel components to configure to meet the following requirements:

1.

When Azure Sentinel identifies a threat, an incident must be created.

2.

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel.

Which component should you identify for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Correct Answer:

Reference: https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

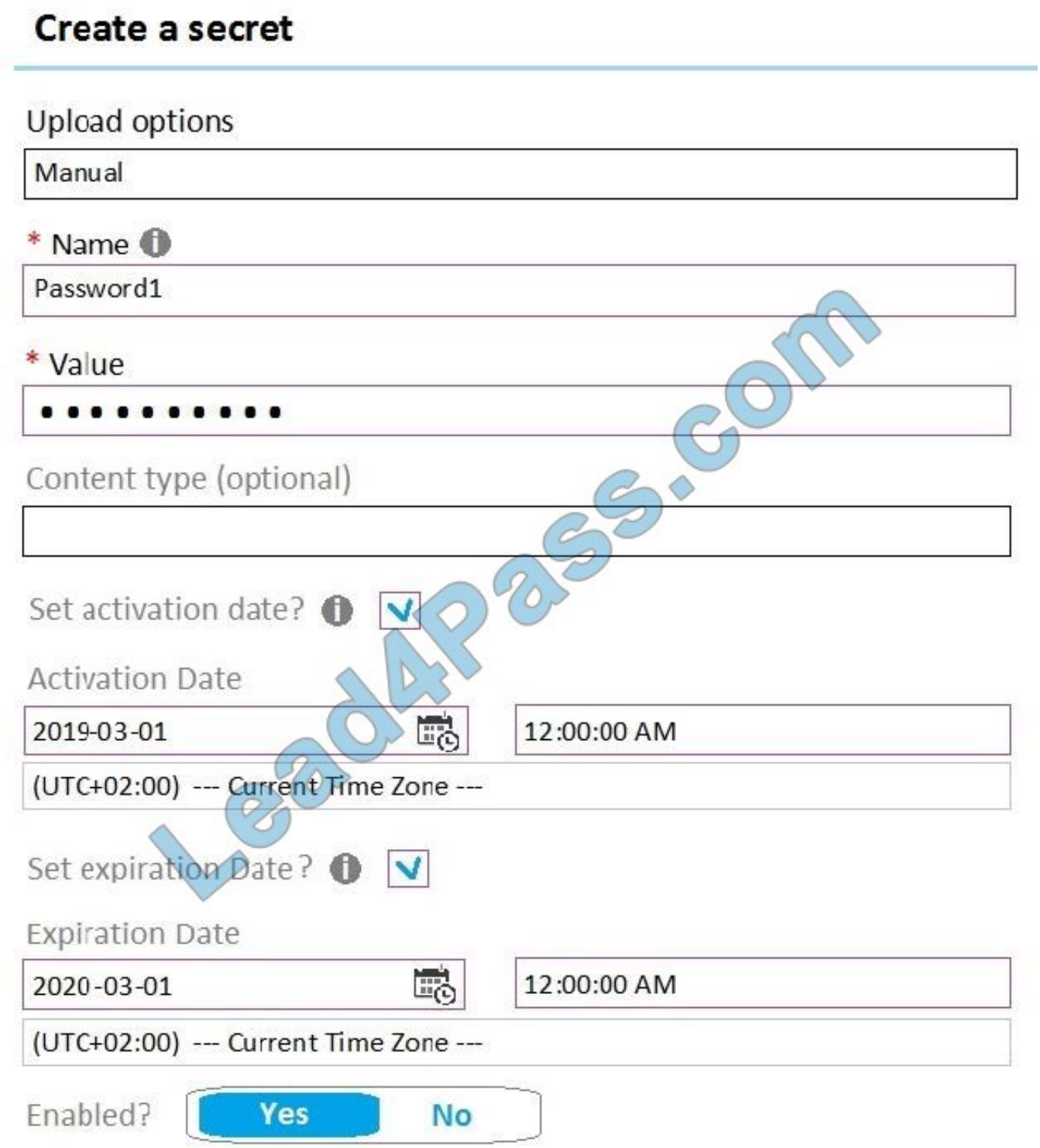
QUESTION 3

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

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

User1 is a member of Group1. Group1 and User2 are assigned the Key Vault Contributor role for Vault1.

On January 1, 2019, you create a secret in Vault1. The secret is configured as shown in the exhibit. (Click the Exhibit tab.)



User2 is assigned an access policy to Vault1. The policy has the following configurations:

Key Management Operations: Get, List, and Restore Cryptographic Operations: Decrypt and Unwrap Key Secret Management Operations: Get, List, and Restore

Group1 is assigned an access to Vault1. The policy has the following configurations:

Key Management Operations: Get and Recover Secret Management Operations: List, Backup, and Recover

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

Hot Area:

Correct Answer:

QUESTION 4

You are collecting events from Azure virtual machines to an Azure Log Analytics workspace.

You plan to create alerts based on the collected events.

You need to identify which Azure services can be used to create the alerts.

Which two services should you identify? Each correct answer presents a complete solution

NOTE: Each correct selection is worth one point.

A. Azure Monitor

B. Azure Security Center

C. Azure Analytics Services

D. Azure Sentinel

E. Azure Advisor

Correct Answer: AD

QUESTION 5

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.)

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	○	○

Correct Answer:

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	○	○

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.

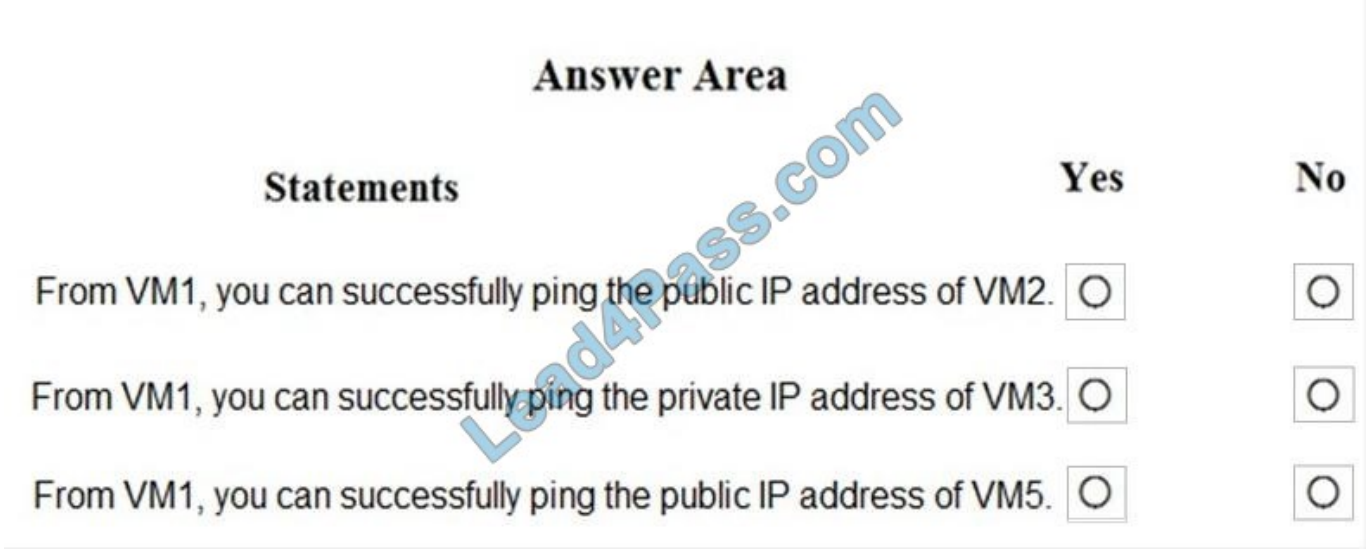
References:

https://www.cayosoft.com/difference-enabling-enforcing-mfa/

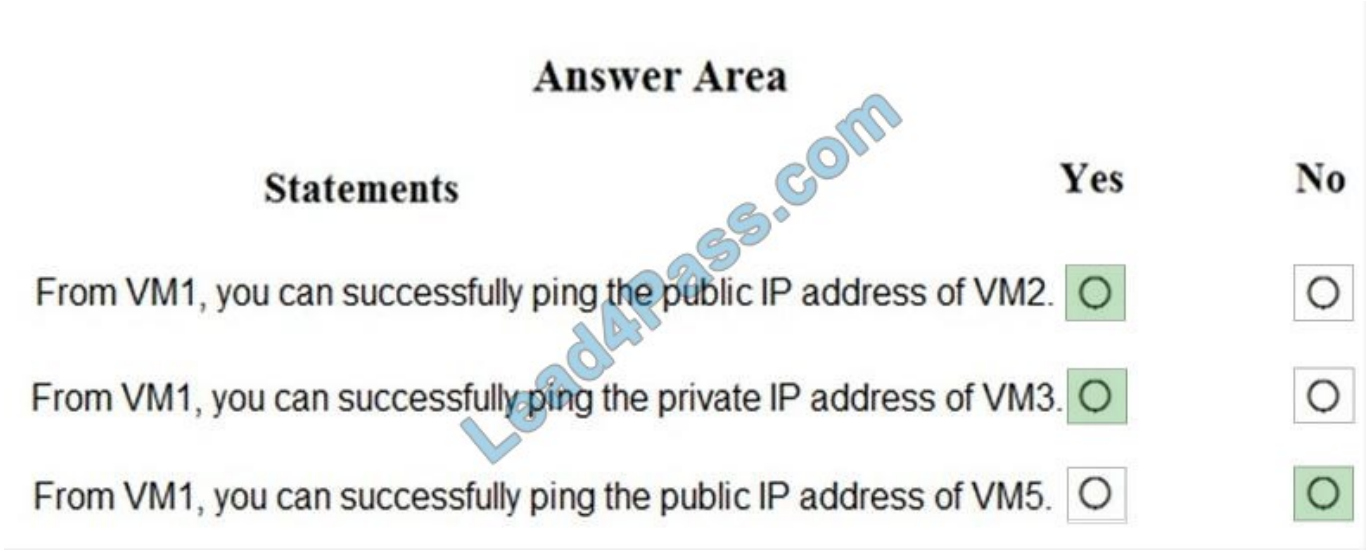
QUESTION 6

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:



Correct Answer:



Box 1: Yes

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

Box 2: Yes

Box 3: No

Note:

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

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

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

QUESTION 7

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

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

QUESTION 8

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

Correct Answer: A

Note: Create a workspace

1.

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.

2.

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 9

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:

1.

Assignments: Include Group1, exclude Group2

2.

Conditions: Sign-in risk level: Medium and above

3.

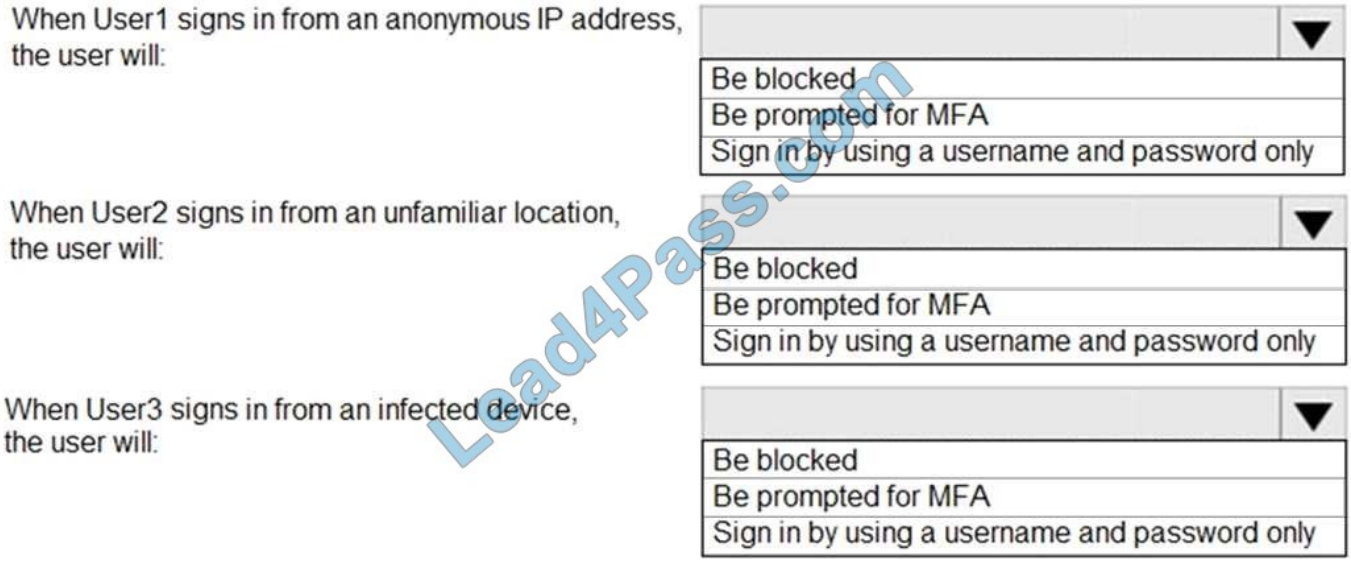
Access Allow access, Require multi-factor authentication

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

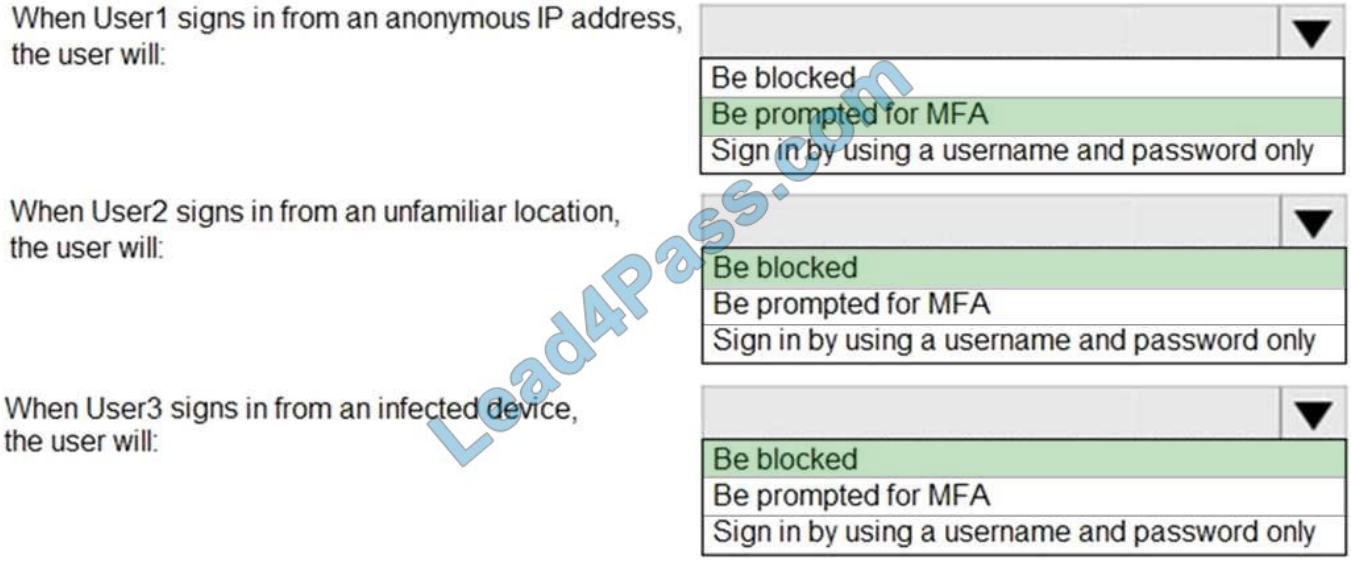
What should you identify for each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



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

QUESTION 10

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.

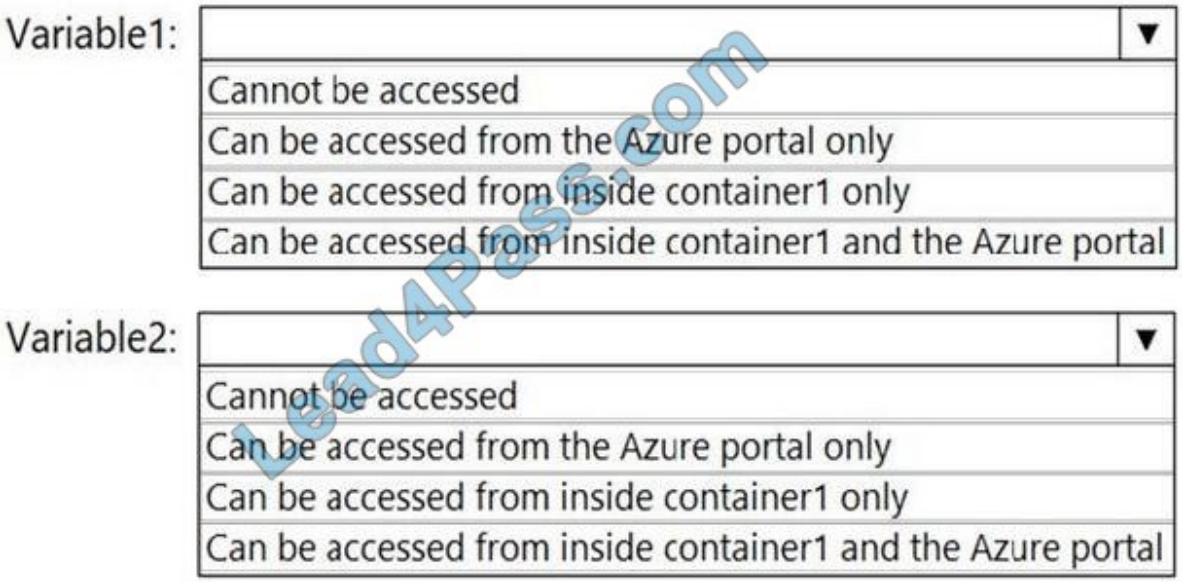
You need to identify where you can access the values of Variable1 and Variable2.

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

NOTE: Each correct selection is worth one point.

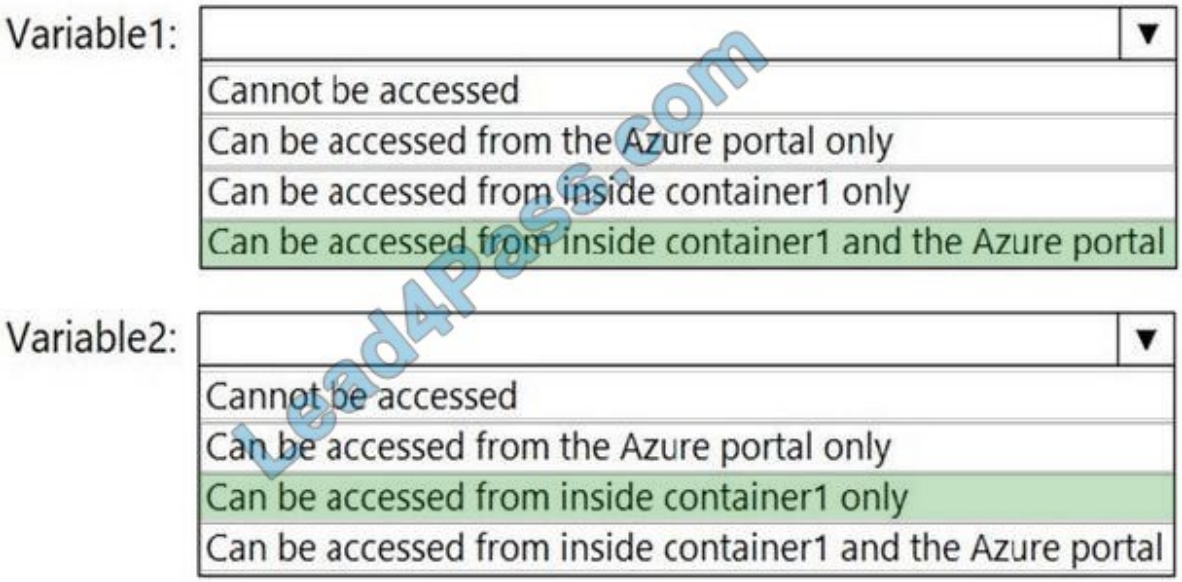
Hot Area:

Answer Area



Correct Answer:

Answer Area



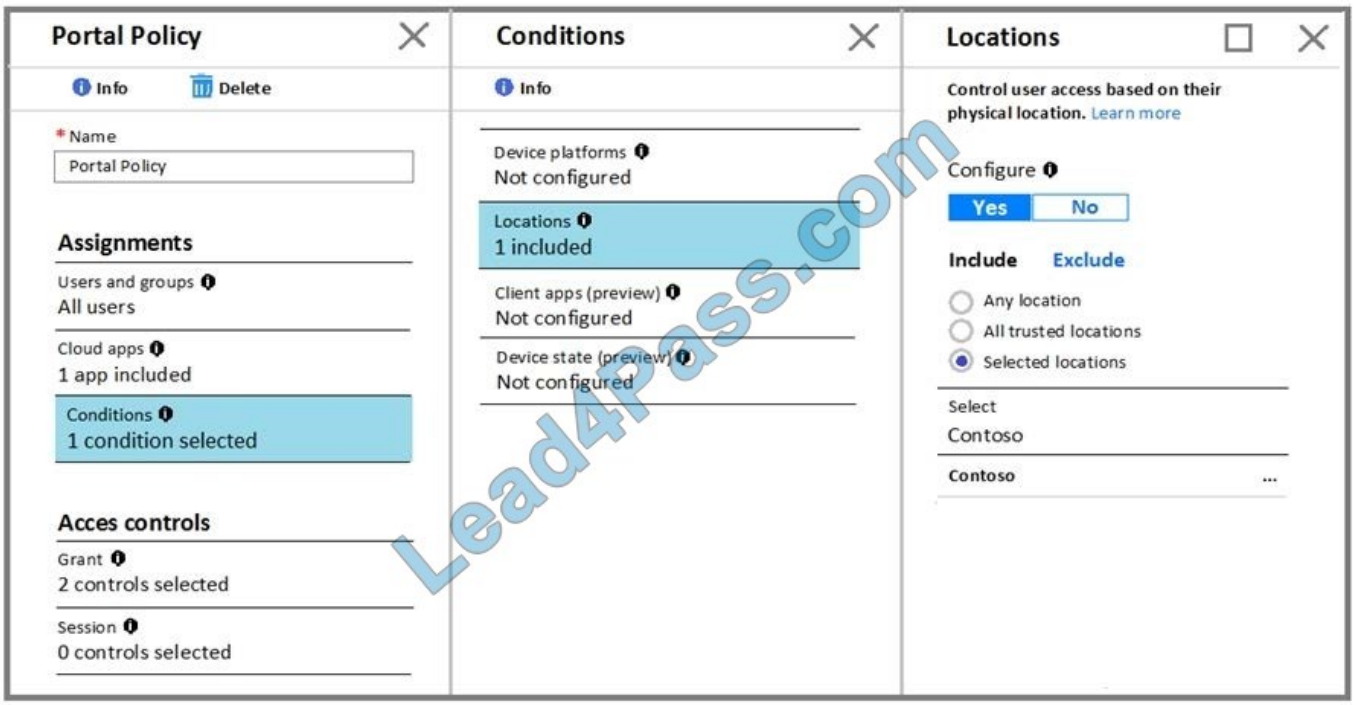
Reference: https://docs.microsoft.com/en-us/azure/container-instances/container-instances-environment-variables

QUESTION 11

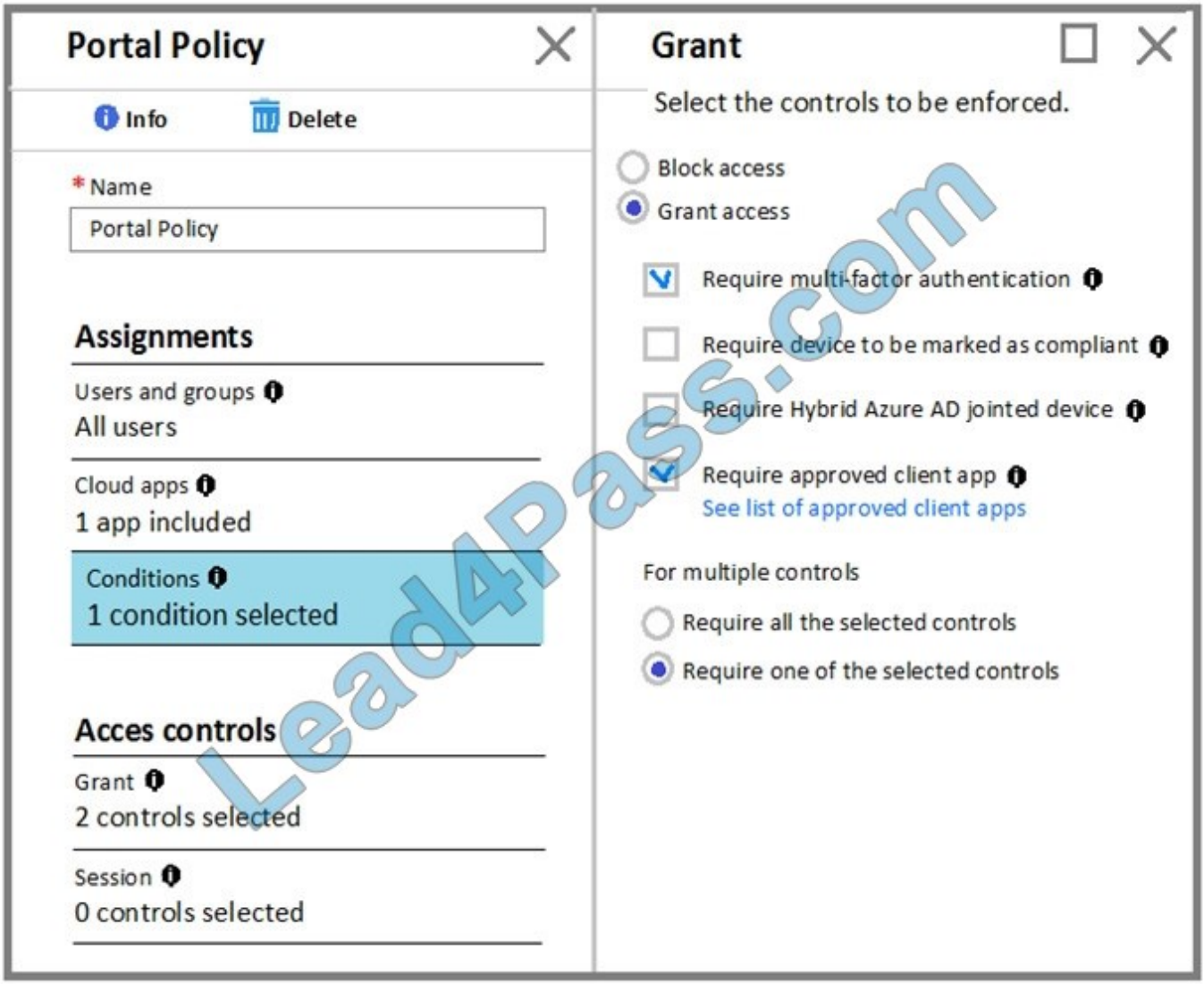
You create a new Azure subscription that is associated to a new Azure Active Directory (Azure AD) tenant.

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.)



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



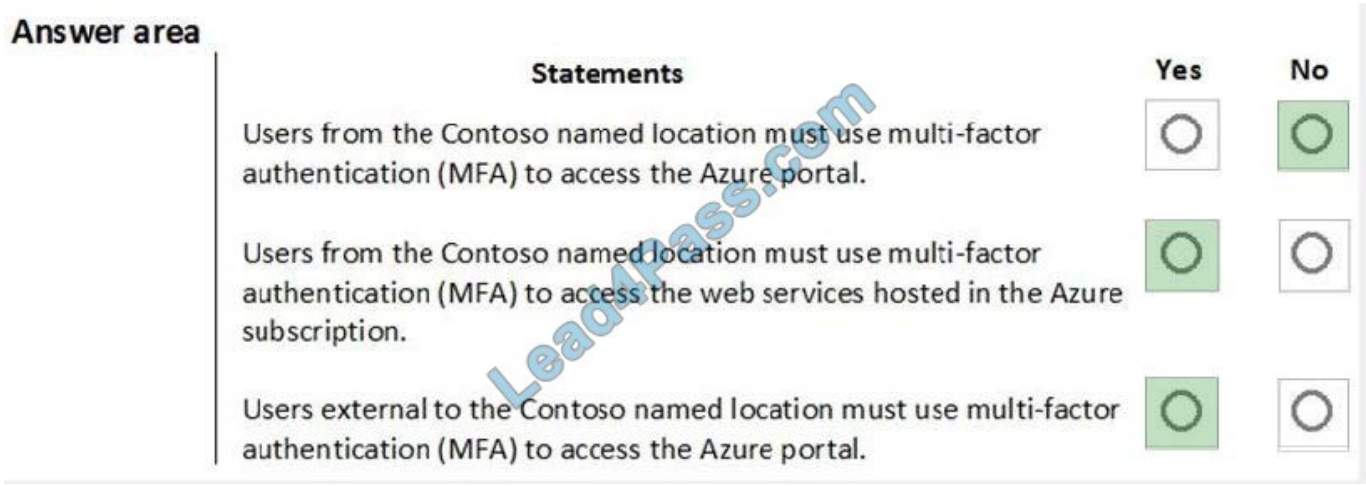
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

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.	○	○

Correct Answer:



Box 1: No The Contoso location is excluded Box 2: Yes

Box 3: Yes Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

QUESTION 12

You have a web app named WebApp1.

You create a web application firewall (WAF) policy named WAF1.

You need to protect WebApp1 by using WAF1.

What should you do first?

A. Deploy an Azure Front Door.

B. Add an extension to WebApp1.

C. Deploy Azure Firewall.

Correct Answer: A

References: https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door

QUESTION 13

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

References: https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal