Microsoft

AZ-500 Exam

Microsoft Azure Security Technologies

Product Questions: 203/3Case Study Version: 19.0

Case Study: 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: 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 Office 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.

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: 2

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.

Answer: A

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:

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: 3

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

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

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: 4

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

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

Answer: BE

Explanation:
Refer https://docs.microsoft.com/en-us/azure/app-service/app-service-web-configure-tls-mutual-auth

Question: 5

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

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

"Microsoft.Compute/	disks/*",
"Microsoft.Resources/	storageAccounts/*",
"Microsoft.Storage/	virtualMachines/disks/*",

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

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

```
                  ]
}
```

Answer:

1) Microsoft.Compute/
2) disks
3) /subscription/{subscriptionId}/resourceGroups/{Resource Group Id}

Explanation:

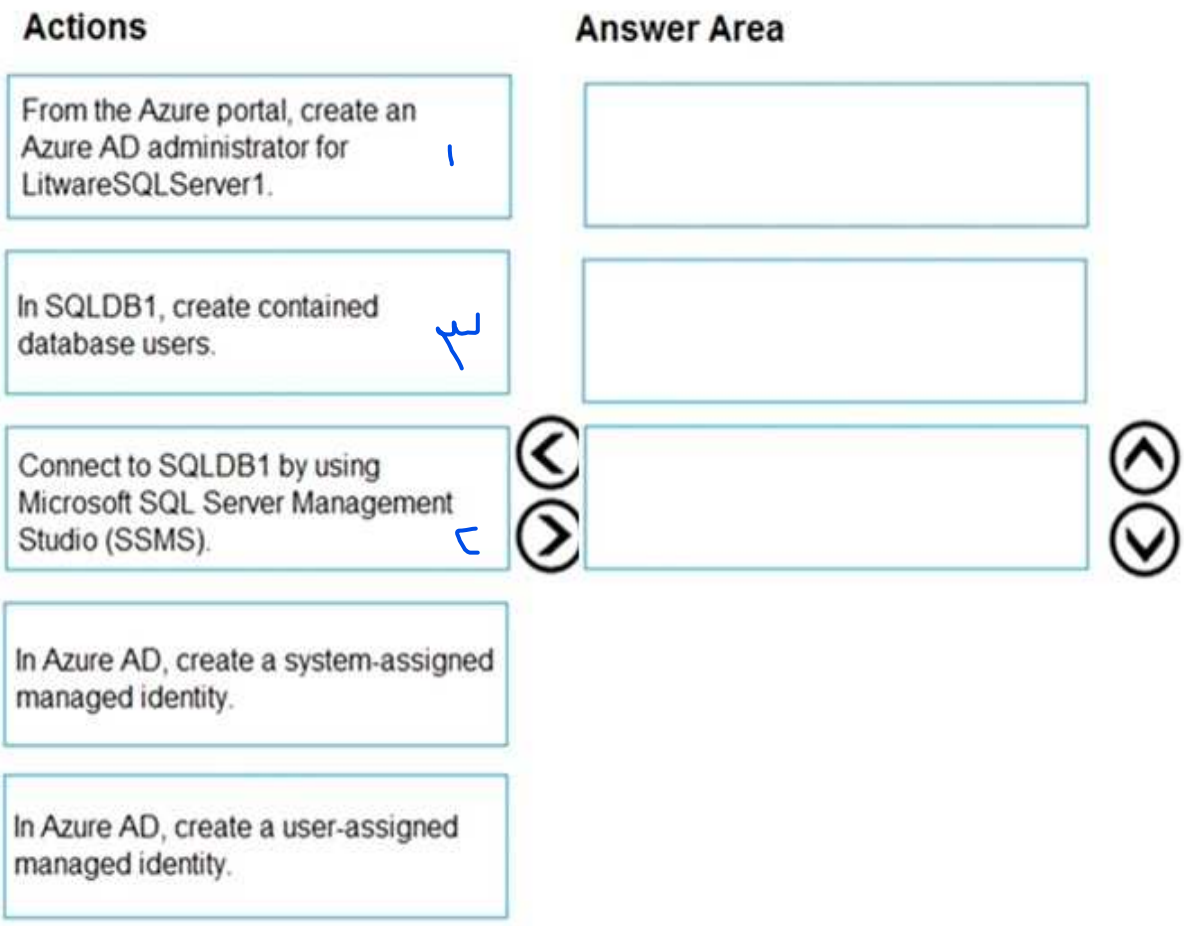
A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

Question: 6

DRAG DROP

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

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



Answer:

From the Azure portal, create an Azure AD administrator for LitwareSQLServer1

Connect to SQLDB1 by using SSMS

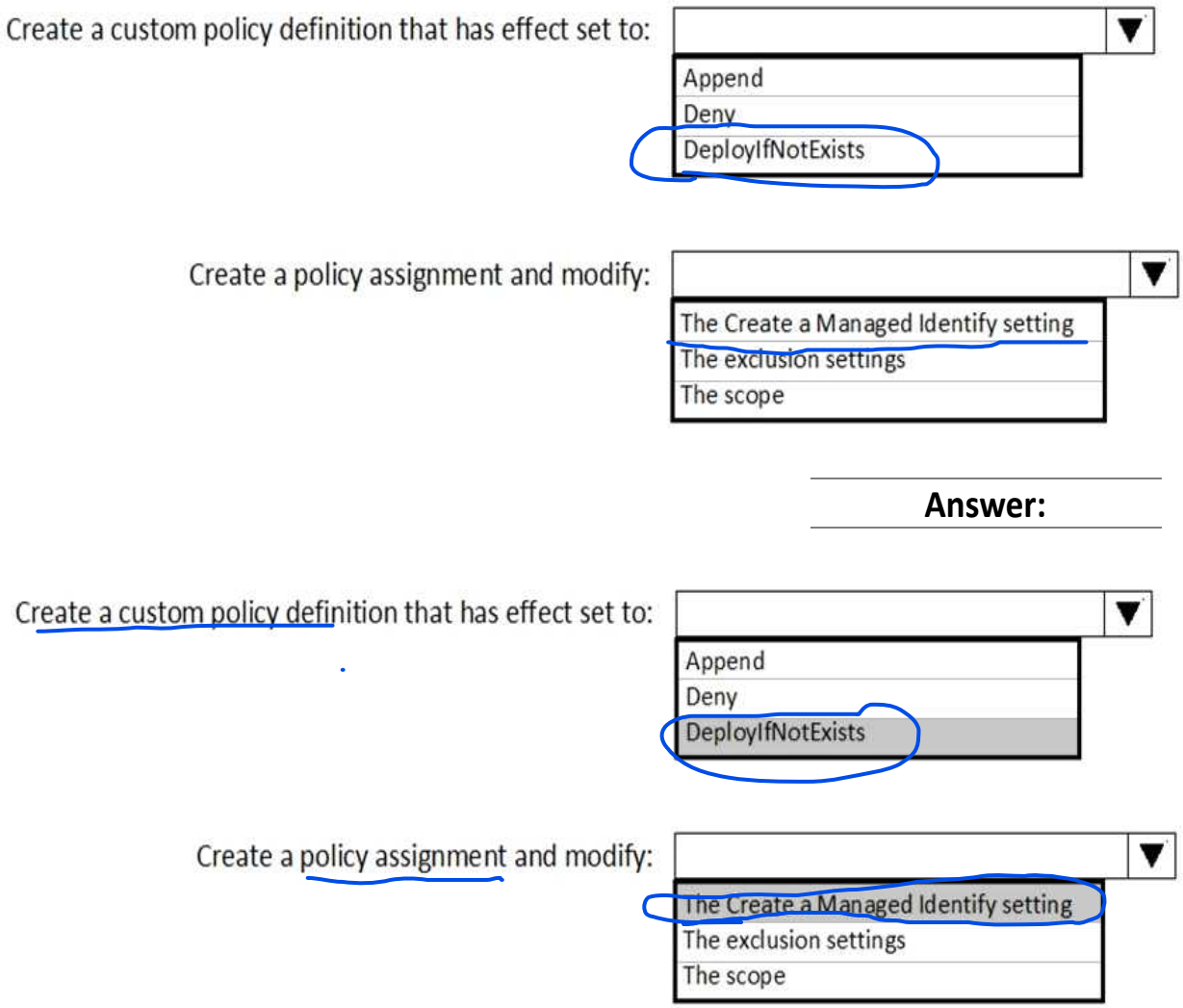
In SQLDB1, create contained database users

Explanation:
https://www.youtube.com/watch?v=pEPyPsGEevw

Question: 7

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.



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

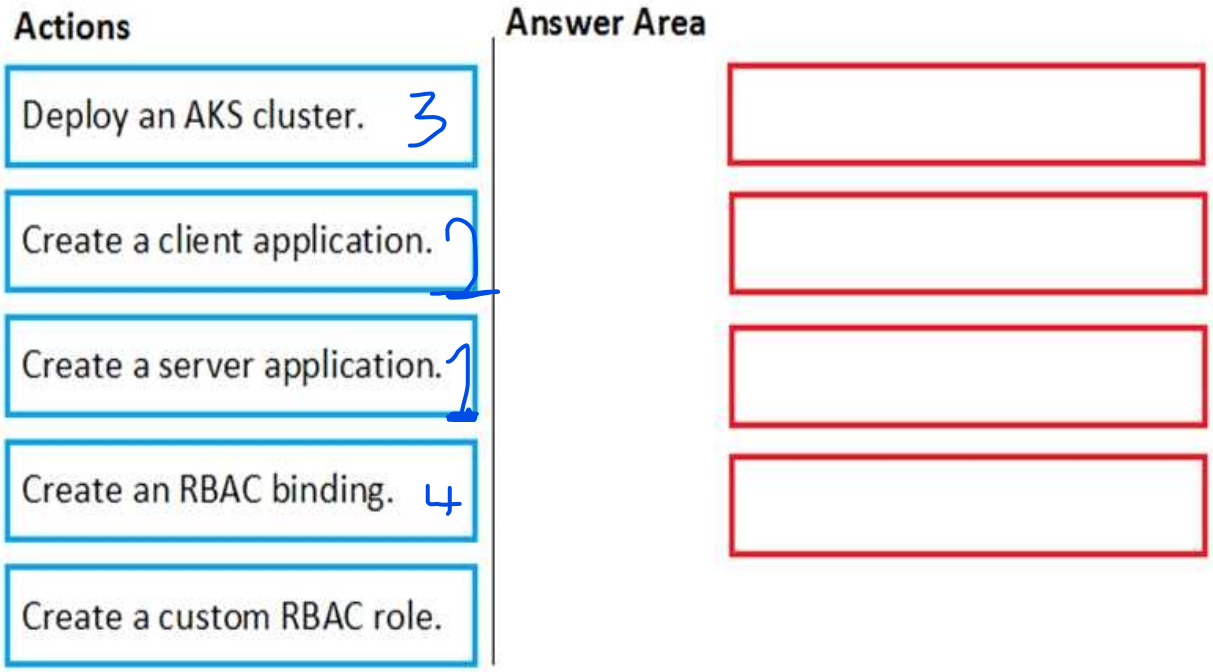
Question: 8

DRAG DROP

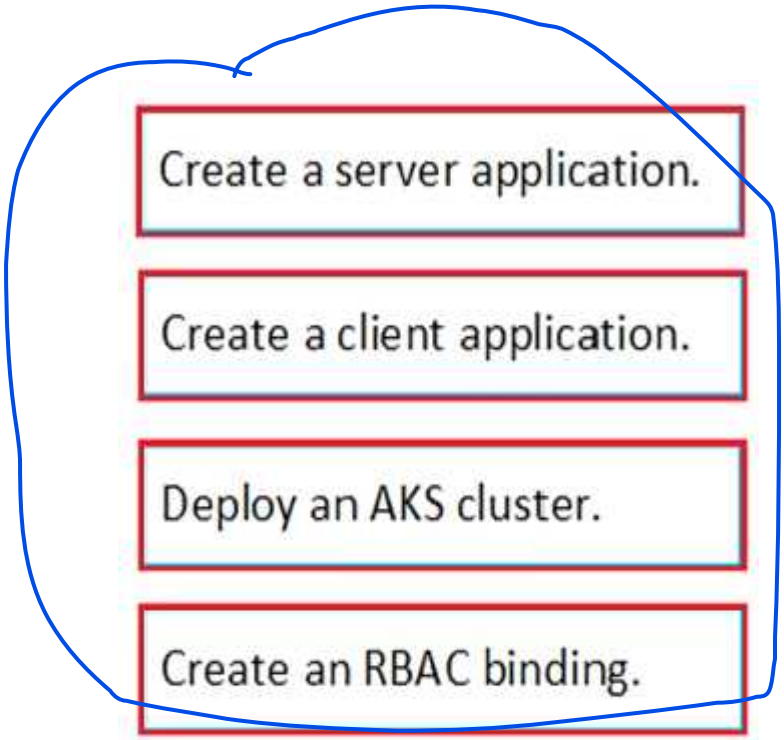
You need to deploy AKS1 to meet the platform protection requirements.

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.



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: 9

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.

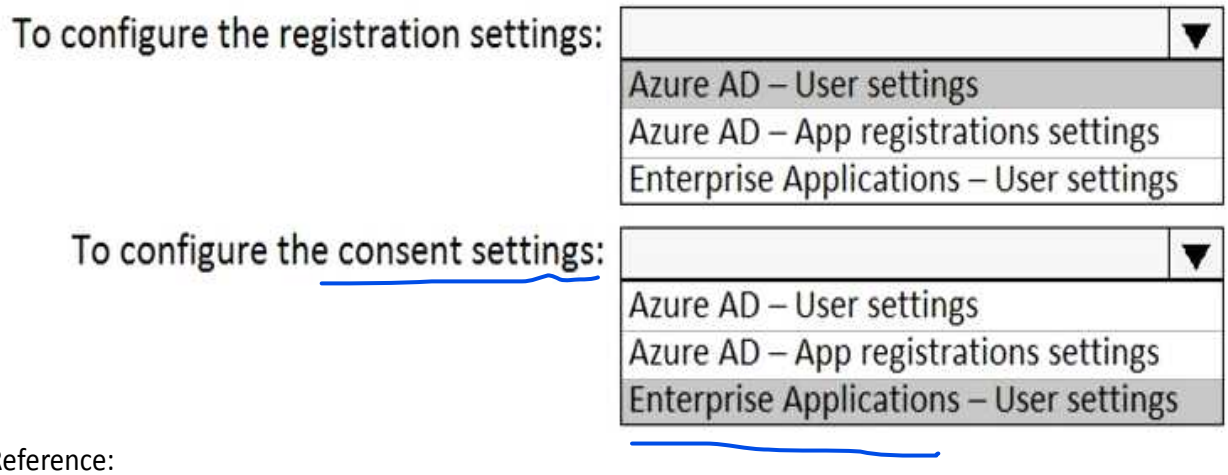
To configure the registration settings:

- 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:



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

Case Study: 2

Contoso

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab{s) and all
Please note that once you submit your work by clicking the Next button within a lab.
Task 1:
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.
Task 2:
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.
Task 3:
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.
Task 4:
The developers at your company plan to create a web app named App103178O6 and to publish the app to htlps://www.contoso.com.
You need to perform the following tasks:

- Ensure that App10317806 is registered lo Azure Active Directory (Azure AD).
- Generate a password for App10317806.

Task 5:
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.

Task 6:
You need to ensure that a user named user2103l7806 can manage the properties of the virtual machines in the RG1lod10317806 resource group. The solution must use the principle of least privilege.
Task 7:
You need to ensure that only devices connected to a 131.107.0.0/16 subnet can access data in the railod10317806 Azure Storage account,
Task 8:
You need to email an alert to a user named admin1@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes.
Task 9:
You need to collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account.
To complete this task, sign in to the Azure portal.
This task might take several minutes to complete. You can perform other tasks while the task completes.
Task 10:
You need to prevent HTTP connections to the rg1lodl03l7806n1 Azure Storage account.
Task 11:
You need to ensure that the rg1lod10317806n1 Azure Storage account is encrypted by using a key stored in the KeyVault10317806 Azure key vault.
Task 12:
You need to create a new Azure Active Directory (Azure AD) directory named
10317806.onmicrosoft.com. The new directory must contain a user named
userl103l7806.onmicrosoft.com who is configured to sign in by using Azure Multi-Factor Authentication (MFA).
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: 10

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

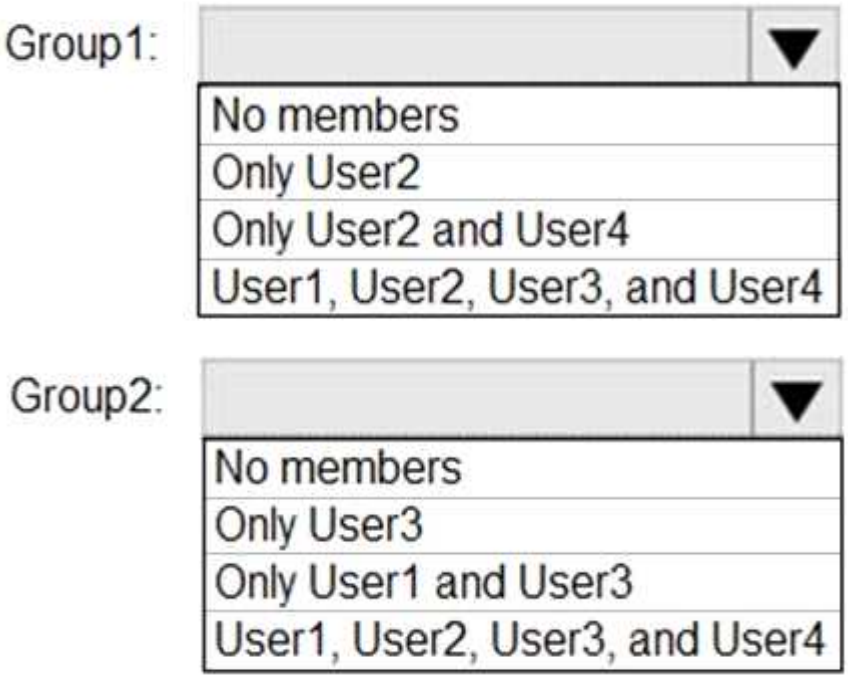
A. Assign User2 the Global administrator role.
B. Configure authentication methods for contoso.com.
C. Configure the identity secure score for contoso.com.
D. Enable multi-factor authentication (MFA) for User2.

Answer: D

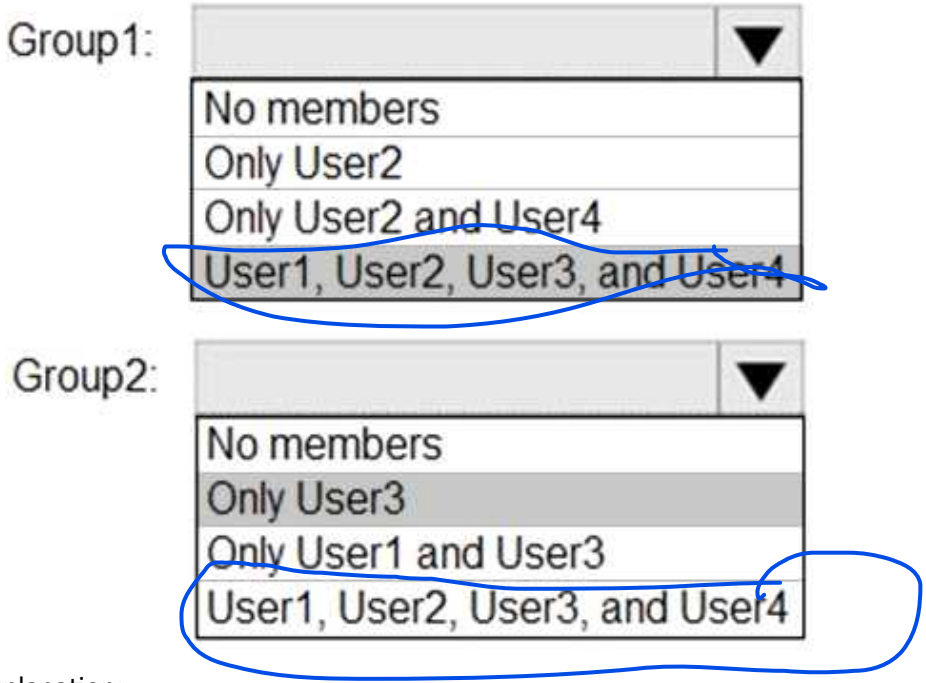
Explanation:
To start using PIM in your directory, you must first enable PIM.
1. Sign in to the Azure portal as a Global Administrator of your directory.
You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com),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

Question: 11

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.



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: 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: 12

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.

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:

No,
Yes,
Yes

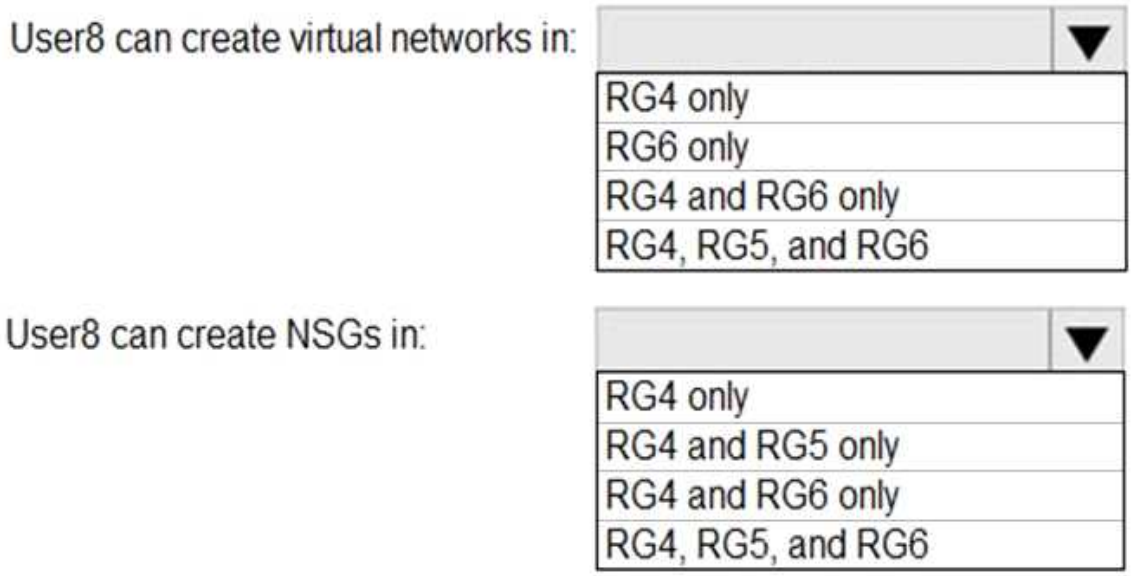
Question: 13

HOTSPOT

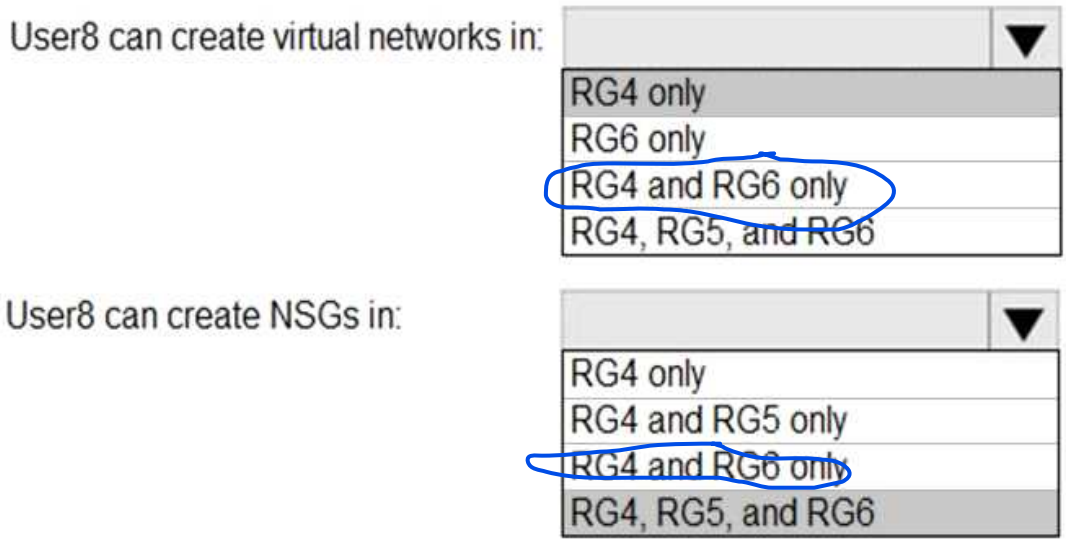
You assign User8 the Owner role for RG4, RG5, and RG6.

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.



Answer:



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

Question: 14

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.

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:

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

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: 15

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.

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:
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: 16

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.

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

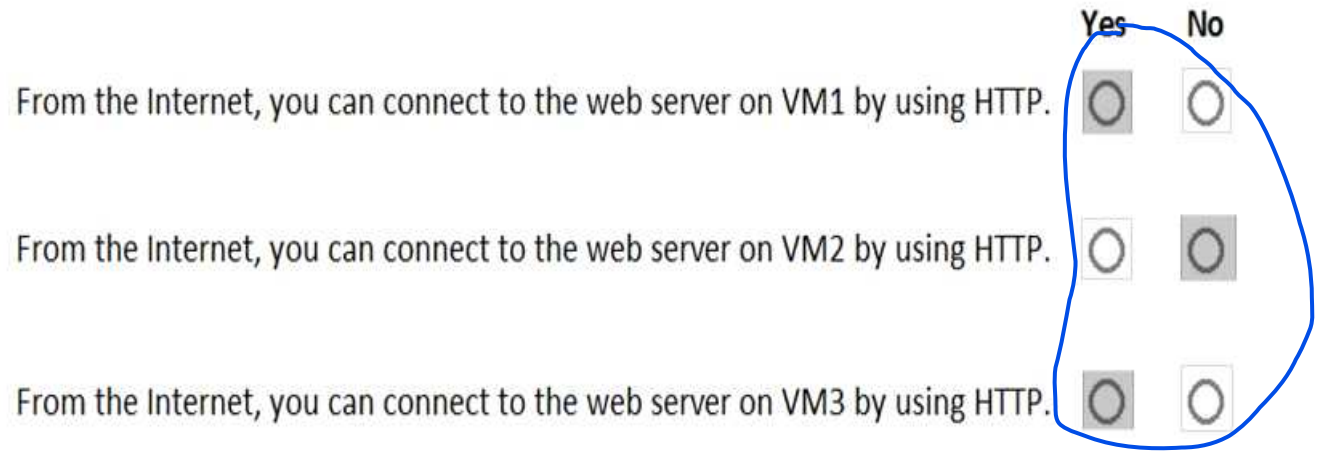
Question: 17

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.

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:



Case Study: 3

Mix Questions

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 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

Answer: B

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: 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 create a new stored access policy.
Does this meet the goal?

A. Yes
B. No

Answer: A

Shared access signatures provides access to a particular resource such as blog. Stored access policies are a group of Shared Access Signatures (SAS). In order to revoke access to a SAS you can either:
1. Rotate the Key1 or Key 2, that is the access keys used to sign the SAS. Rotating the access keys used to sign the SAS, invalidates any previously signed SAS hence revoking the SAS issued before
2. Remove the stored access policy which an SAS is linked to. If a Stored Access Policy is removed, it also invalidates the SASs liked to the Stored Access Policy.

Question: 20

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

Answer: B

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: 21

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

Answer: A

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
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

Question: 22

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)

Answer: C

Explanation:
1. Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant
>> Pass-Through Authentication enforce on-premises user account states, password policies, and sign-in hours.
2. Minimizes the number of servers required for the solution.
>> Pass-through needs a lightweight agent to be installed one (or more) on-premises servers.
>> PW Hash also require installing Azure AD Connect on your existing DC.

Question: 23

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

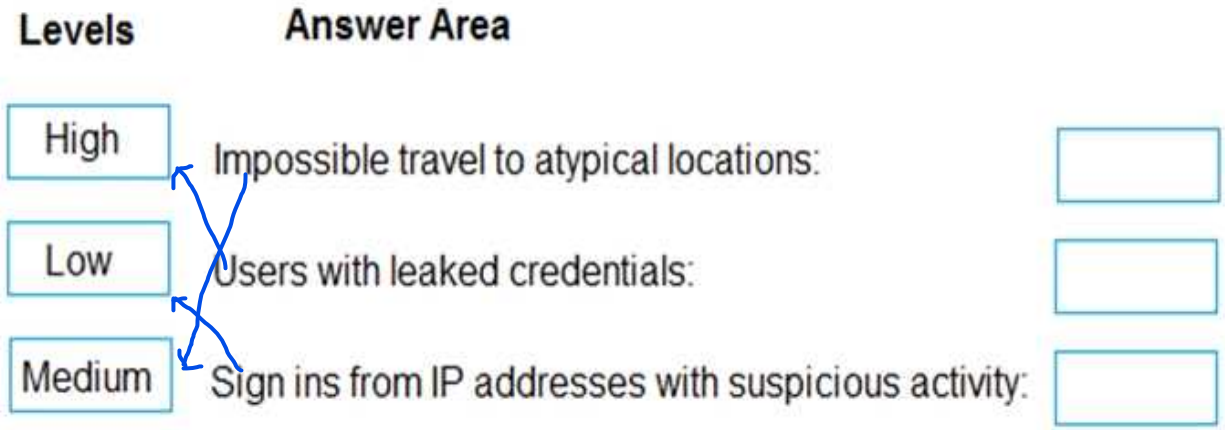
Answer: A

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: 24

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.



Answer:

Medium
High
Medium

Explanation:

Refer https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events#sign-ins-from-ip-addresses-with-suspicious-activity

Question: 25

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.

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:

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.	○	○

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:

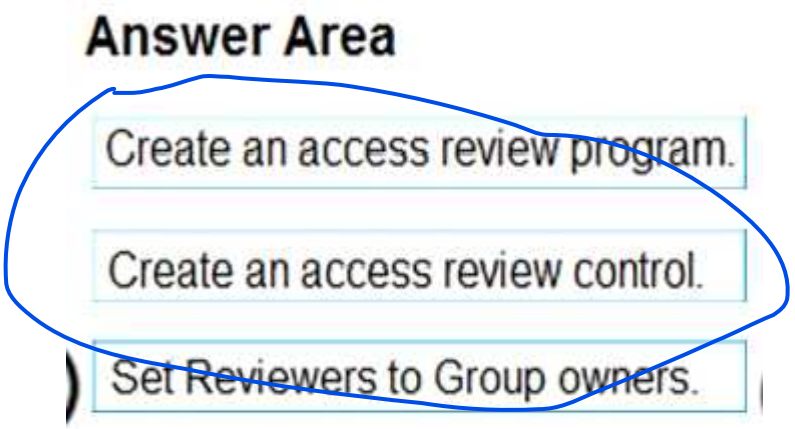
Sign-in Activity	Risk Level
Users with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from IP addresses with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium

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: 26

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.

Answer:



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.

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

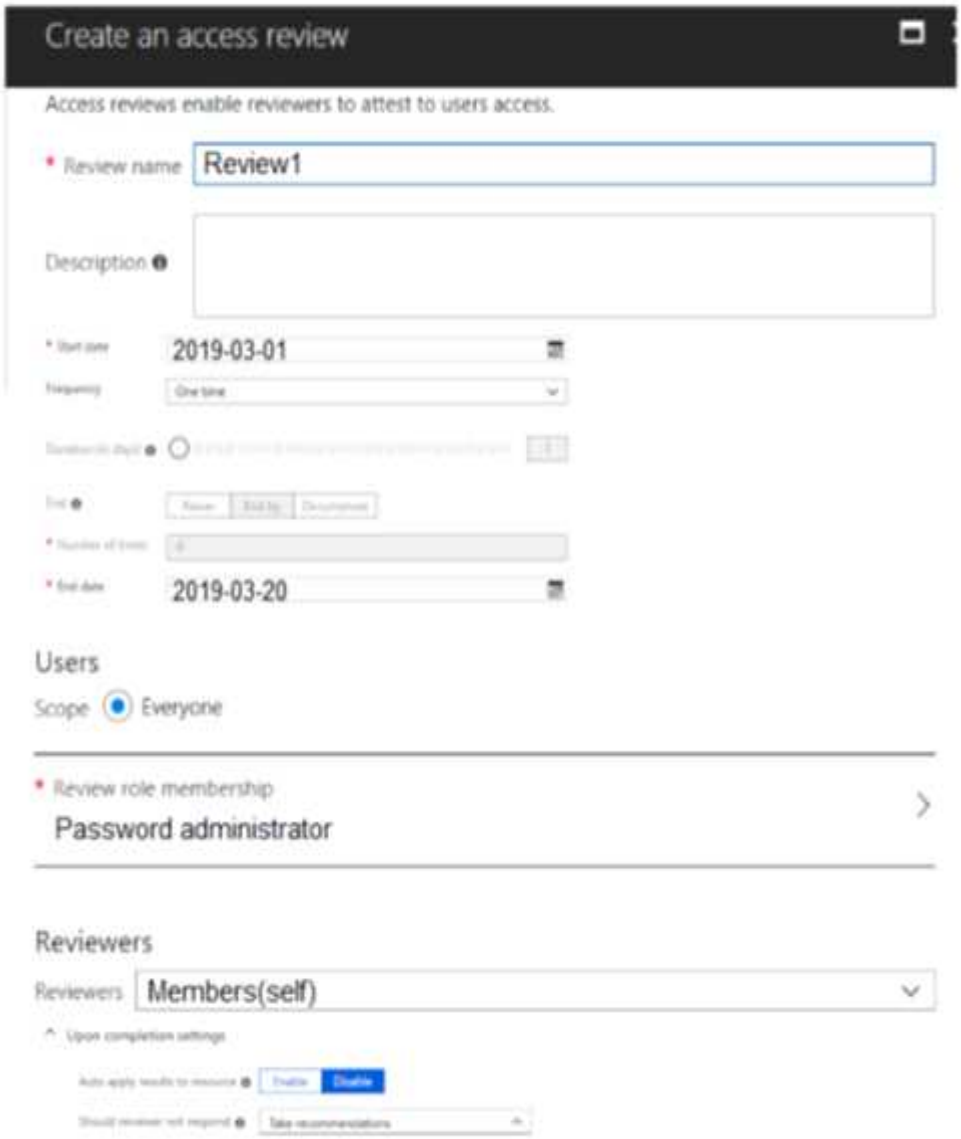
Question: 27

HOTSPOT

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

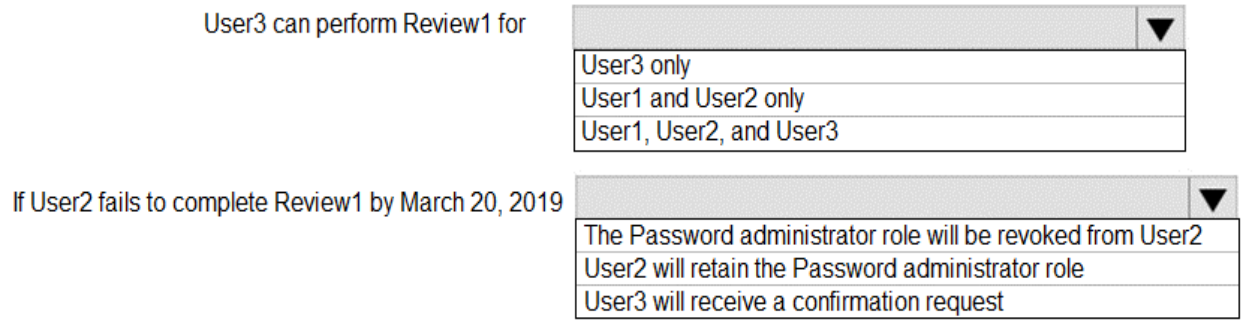
Name	Role	Sign in frequency
User1	Password administrator	Sign in every work day
User2	Password administrator	Sign in bi-weekly
User3	Global administrator, Password administrator	Signs in every month

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

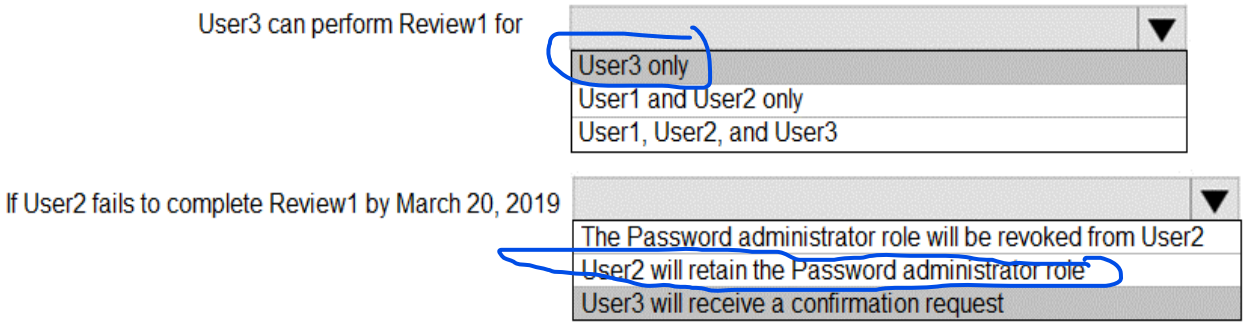


Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



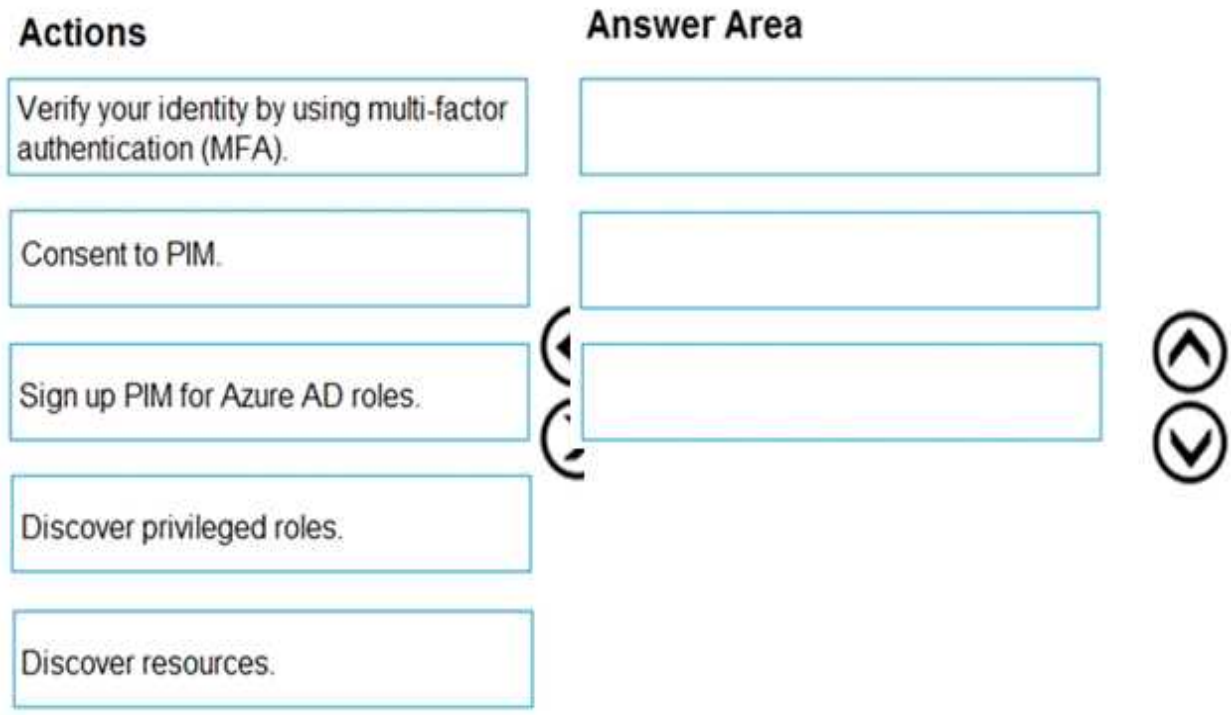
Answer:



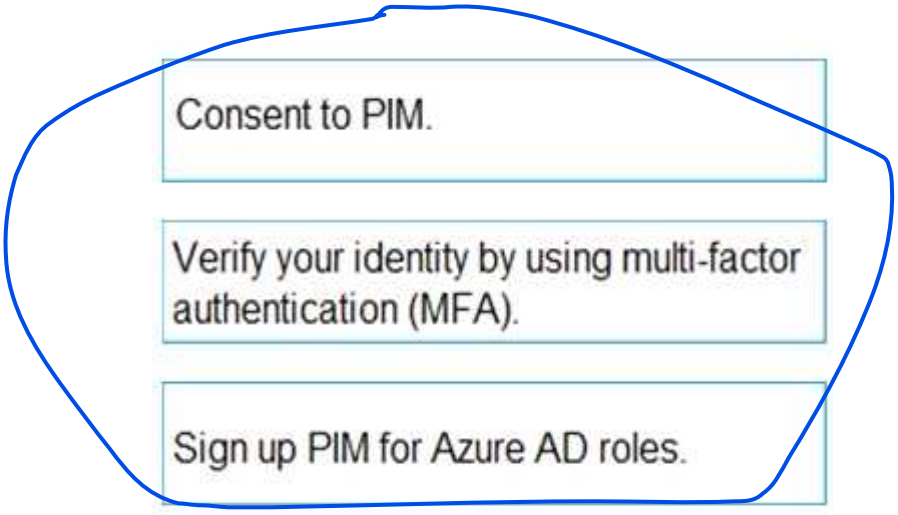
Explanation:
Box 1: User3 only
Use the Members (self) option to have the users review their own role assignments.
Box 2: User3 will receive a confirmation request
Use the Should reviewer not respond list to specify what happens for users that are not reviewed by the reviewer within the review period. 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: 28

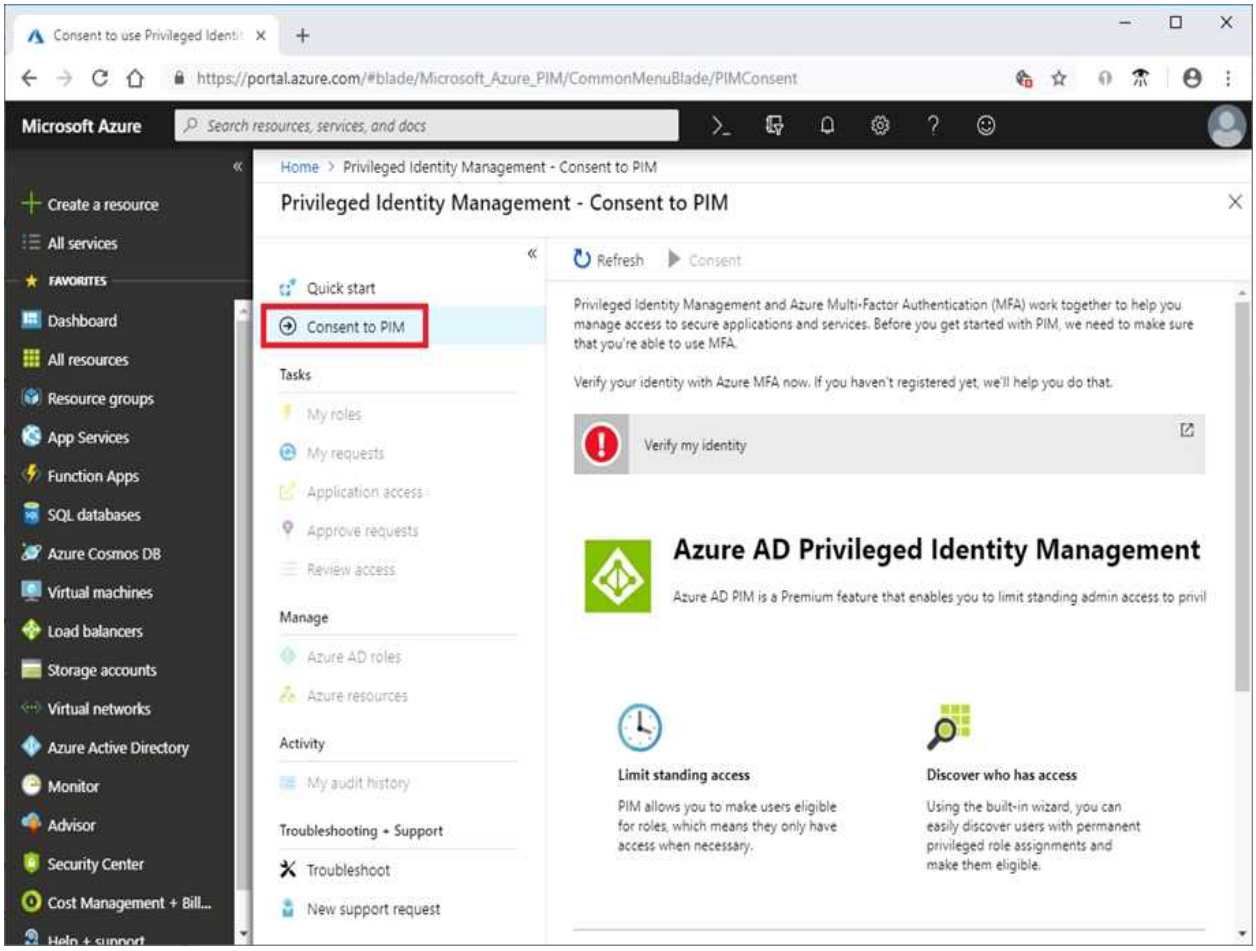
DRAG DROP
You create an Azure subscription.
You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure AD roles.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:
Step 1: Consent to PIM



Step: 2 Verify your identity by using multi-factor authentication (MFA)
Click Verify my identity to verify your identity with Azure MF
A. 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.
References:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

Question: 29

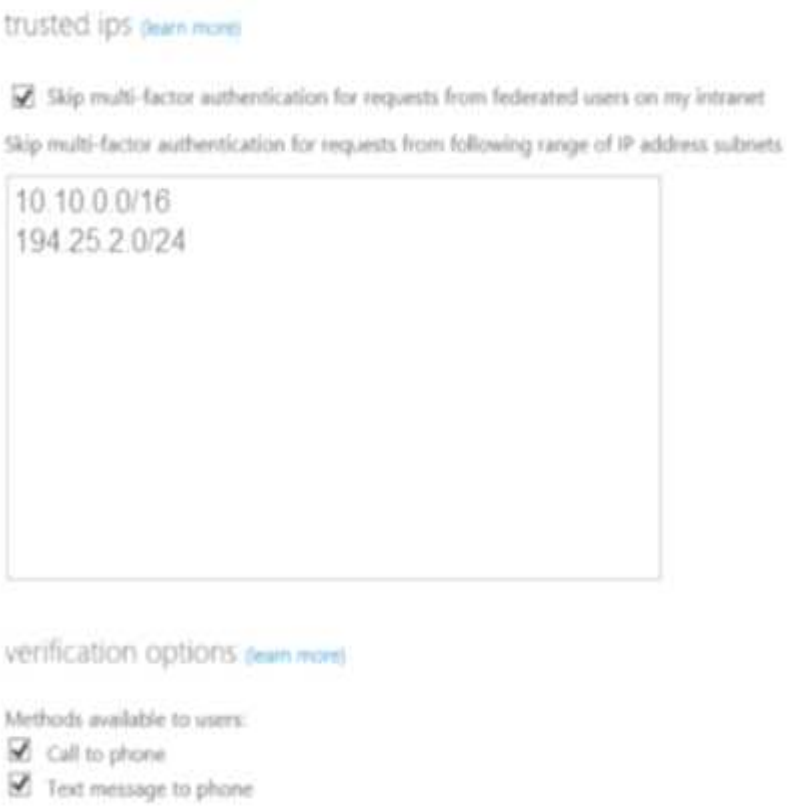
HOTSPOT
Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.

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.)



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

	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:

	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	○	○

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: 30

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 Blueprints
C. Azure AD Privileged Identity Management (PIM)
D. Azure Policy

Answer: B

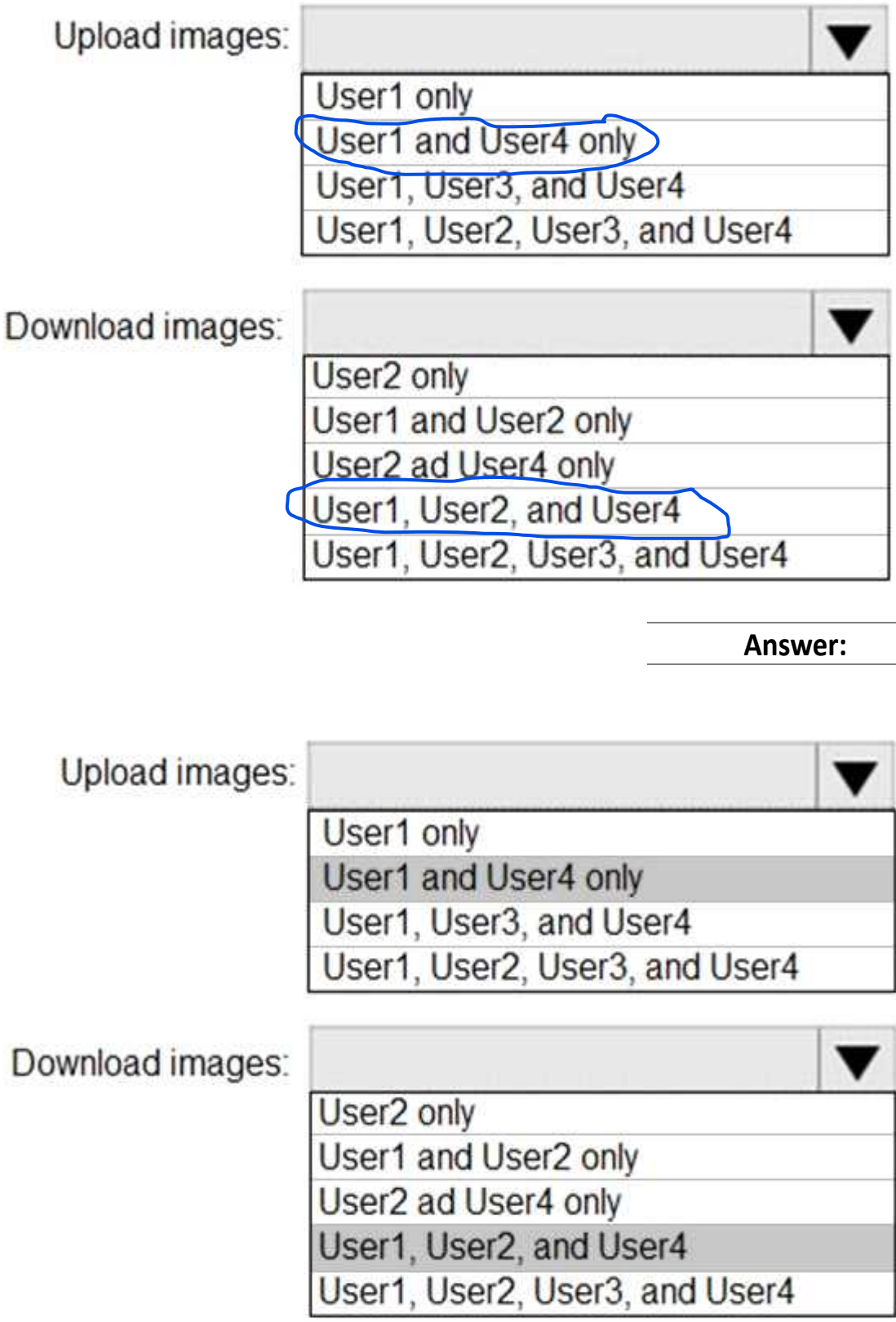
Explanation:
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview#blueprint-definition
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

Question: 31

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.



Answer:

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: 32

You have an Azure subscription.
You create an Azure web app named Contoso1812 that uses an S1 App service plan.
You create a DNS record for www.contoso.com that points to the IP address of 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

Answer: BF

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

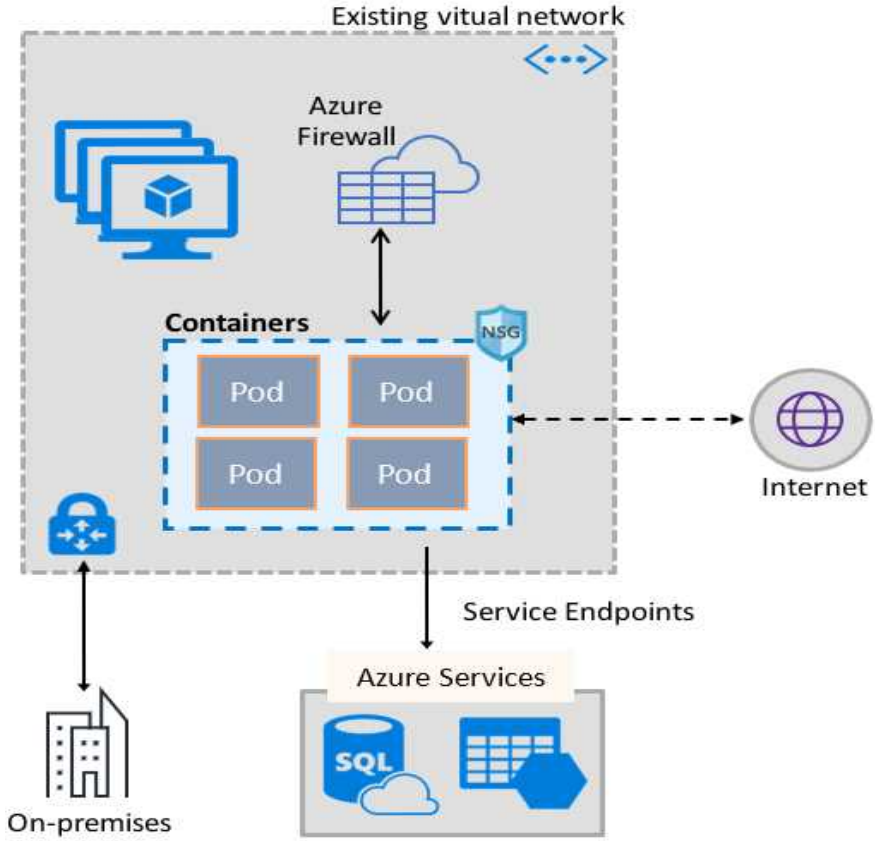
Question: 33

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.

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.

Answer: C

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: 34

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 DSCService 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

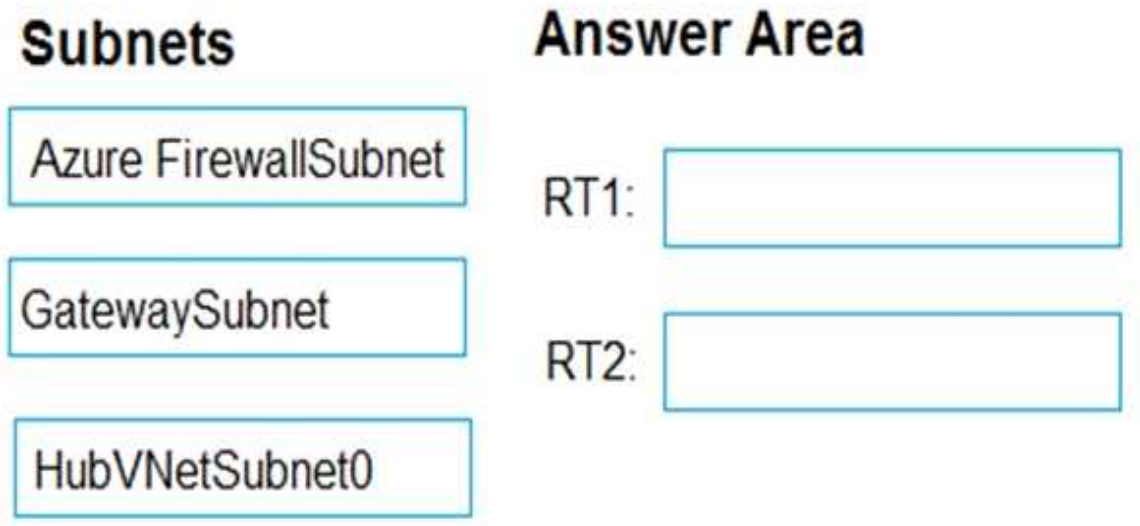
Question: 35

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

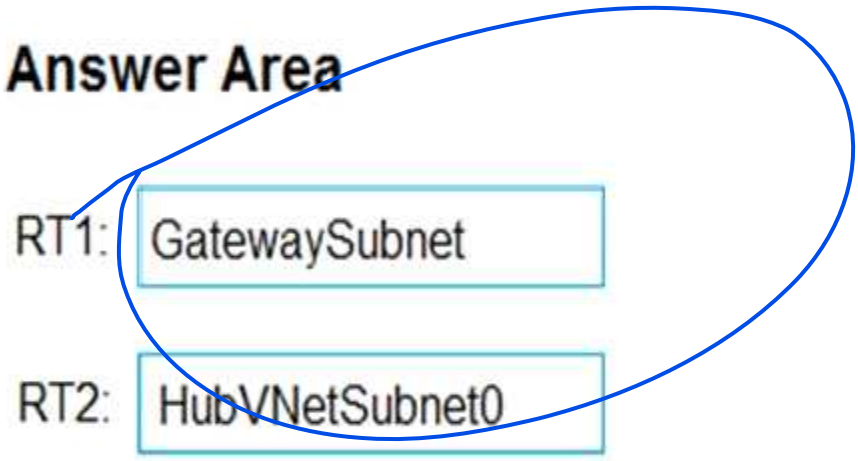
Name	Region	Description
HubVNet	East US	HubVNet is a virtual network connected to the on-premises network by using a site-to-site VPN that has BGP route propagation enabled. HubVNet contains a subnet named HubVNetSubnet0.
SpokeVNet	East US	SpokeVNet is a virtual network connected to HubVNet by using 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.



Answer:



Question: 36

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.

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

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

Answer:

```
    },
    "then" : {
        "effect" : "[ Append / Deny / DeployIfNotExists ]",

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

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: 37

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

Answer: B

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: 38

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.

Answer Area

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

Answer:

Answer Area

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

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

Question: 39

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.

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:

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

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: 40

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

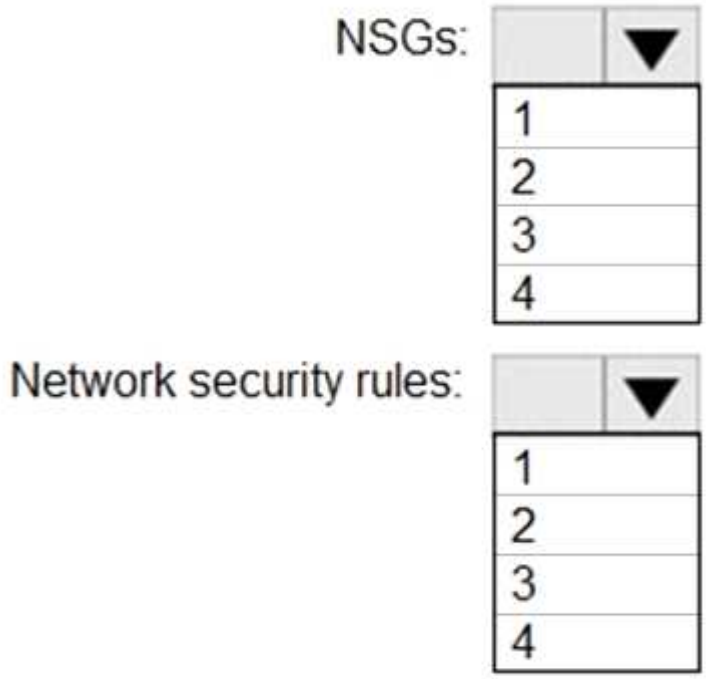
Currently, you have not provisioned any network security groups (NSGs).

You need to implement network security to meet the following requirements:

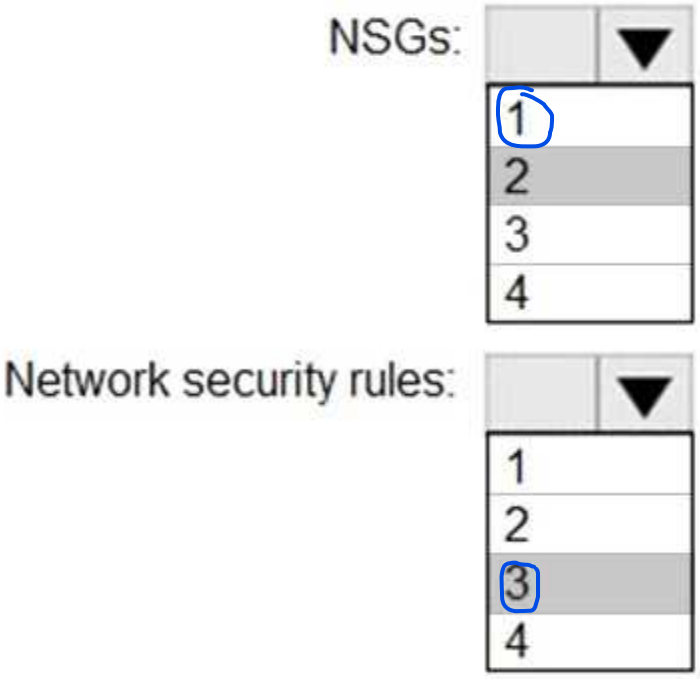
- Allow traffic to VM4 from VM3 only.
- Allow traffic from the Internet to VM1 and VM2 only.
- Minimize the number of NSGs and network security rules.

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.



Answer:



Explanation:
NSGs: 1
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: 41

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.

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:

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

Explanation:

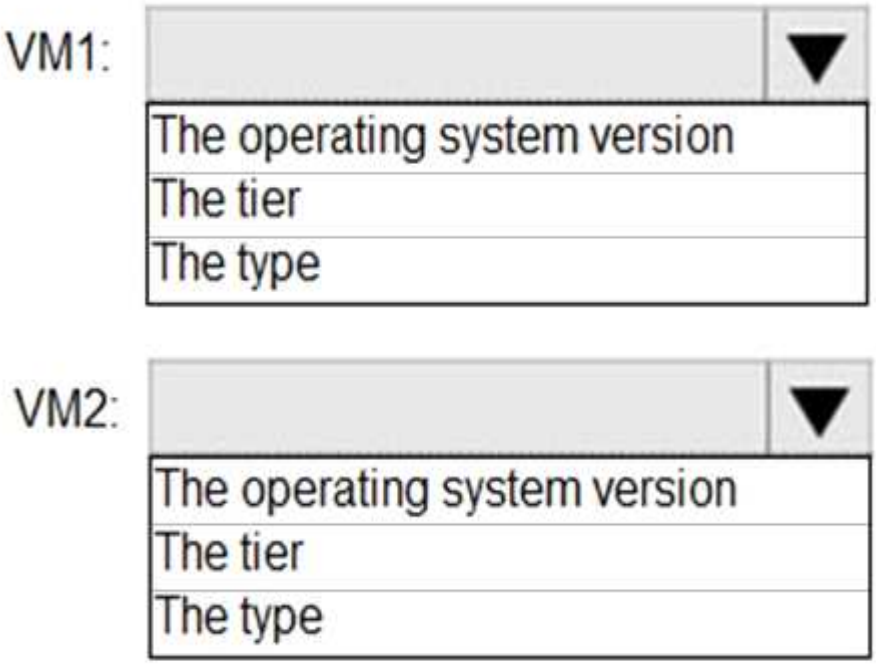
User1: RBAC
RBAC is used as the Key Vault access control mechanism for the management plane. It would allow a user with the proper identity to:
• set Key Vault access policies
• create, read, update, and delete key vaults
• set Key Vault tags
Note: Role-based access control (RBAC) is a system that provides 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: 42

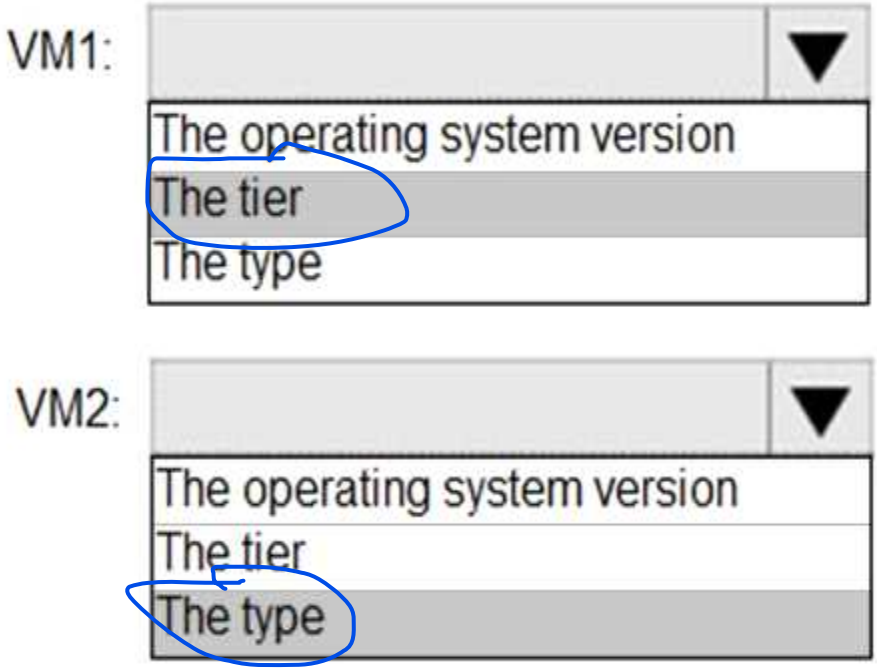
HOTSPOT
You have two Azure virtual machines in the East US2 region as shown in the following table.

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.



Answer:



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 operating system
References:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/generation-2#generation-1-vs-generation-2-capabilities

Question: 43

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: C

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: 44

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	1.1 1.5
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.

Answer: A

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: 45

HOTSPOT
You plan to use Azure Log Analytics to collect logs from 200 servers that run Windows Server 2016.
You need to automate the deployment of the Microsoft Monitoring Agent to all the servers by using an Azure Resource Manager template.
How should you complete the template? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

```
{
    "type" : "Microsoft.Compute/virtualMachines/extensions",
    "name" : "[concat(parameter('vmname'), /OMSExtension]",
    "apiVersion" : "[variables('apiVersion')]",
    "location" : "[resourceGroup().location]",
    "dependsOn" : [
        "[concat('Microsoft.Compute/virtualMachines/", parameters('vmName'))]"
    ],
    "properties" : {
        "publisher" : "Microsoft.EnterpriseCloud.Monitoring",
        "type" :  "MicrosoftMonitoringAgent",
        "typeHandlerVersion" : "1.0",
        "autoUpgradeMinorVersion" : true,
        "settings" : {
            [ ▼ ] : "[variable('var1')]"
        },
        "protectedSettings" : {
            [ ▼ ] : "[variable ('var2')]"
        }
    }
}
```

"AzureADApplicationID"
"WorkspaceID"
"WorkspaceName"
"WorkspaceURL"

"AzureADApplicationSecret"
"StorageAccountKey"
"WorkspaceID"
"WorkspaceKey"

Answer:

```
],
"properties" : {
    "publisher" : "Microsoft.EnterpriseCloud.Monitoring",
    "type" :  "MicrosoftMonitoringAgent",
    "typeHandlerVersion" : "1.0",
    "autoUpgradeMinorVersion" : true,
    "settings" : {
        [ ▼ ] : "[variable('var1')]"
            "AzureADApplicationID"
            "WorkspaceID"
            "WorkspaceName"
            "WorkspaceURL"
    },
        "protectedSettings" : {
        [ ▼ ] : "[variable ('var2')]"
            "AzureADApplicationSecret"
            "StorageAccountKey"
            "WorkspaceID"
            "WorkspaceKey"
    }
  }
}
```

Explanation:

References:

https://blogs.technet.microsoft.com/manageabilityguys/2015/11/19/enabling-the-microsoft-monitoring-agent-in-windows-json-templates/

Question: 46

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You are assigned the Global administrator role for the tenant. You are responsible for managing Azure Security Center settings.

You need to create a custom sensitivity label.

What should you do first?

A. Create a custom sensitive information type.

B. Elevate access for global administrators in Azure AD.

C. Upgrade the pricing tier of the Security Center to Standard.

D. Enable integration with Microsoft Cloud App Security.

Answer: A

Explanation:

First, you need to create a new sensitive information type because you can't directly modify the default rules.

References:

https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-type

Question: 47

HOTSPOT
You suspect that users are attempting to sign in to resources to which they have no access.
You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than five failed sign-in attempts.
How should you configure the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AcccountType == 'User' and [ ▼ ] ==4625
```

ActivityID
DataType
EventID
QuantityUnit

```
| Summarie failed_login_attempts= [ ▼ ]
```

Count(),
Countif(),
Makeset(),
Split(),

```
    latest_failed_login=arg_max(TimeGenerated by Account
| where failed login attempts > 5
```

Answer:

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AcccountType == 'User' and [ ▼ ] ==4625
```

ActivityID
DataType
EventID
QuantityUnit

```
| Summarie failed_login_attempts= [ ▼ ]
```

Count(),
Countif(),
Makeset(),
Split(),

```
    latest_failed_login=arg_max(TimeGenerated by Account
| where failed login attempts > 5
```

Explanation:
The following example identifies user accounts that failed to log in more than five times in the last day, and when they last attempted to log in.
let timeframe = 1d;
SecurityEvent
| where TimeGenerated > ago(1d)
| where AccountType == 'User' and EventID == 4625 // 4625 - failed log in
| summarize failed_login_attempts=count(), latest_failed_login=arg_max(TimeGenerated, Account) by Account
| where failed_login_attempts > 5
| project-away Account1
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples

Question: 48

You have an Azure subscription named Sub1.
In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.
You need to modify Play1 to send email messages to a distribution group named Alerts.
What should you use to modify Play1?

A. Azure DevOps
B. Azure Application Insights
C. Azure Monitor
D. Azure Logic Apps Designer

Answer: D

Explanation:

You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up.
References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks

Question: 49

You create a new Azure subscription.
You need to ensure that you can create custom alert rules in Azure Security Center.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Onboard Azure Active Directory (Azure AD) Identity Protection.
B. Create an Azure Storage account.
C. Implement Azure Advisor recommendations.
D. Create an Azure Log Analytics workspace.
E. Upgrade the pricing tier of Security Center to Standard.

Answer: BD

Explanation:
D: You need write permission in the workspace that you select to store your custom alert.
References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-custom-alert

Question: 50

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.
You have 100 on-premises servers that run Windows Server 2012 R2 and Windows Server 2016. The servers connect to LAW1. LAW1 is configured to collect security-related performance counters from the connected servers.
You need to configure alerts based on the data collected by LAW1. The solution must meet the following
requirements:
• Alert rules must support dimensions.
• The time it takes to generate an alert must be minimized.
• Alert notifications must be generated only once when the alert is generated and once when the alert is
• resolved.
Which signal type should you use when you create the alert rules?

A. Log
B. Log (Saved Query)
C. Metric
D. Activity Log

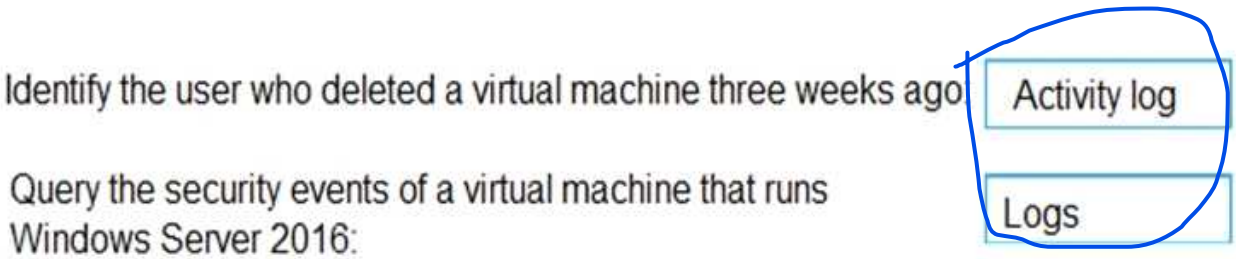
Answer: C

Explanation:
Metric alerts in Azure Monitor provide a way to get notified when one of your metrics cross a threshold. Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights standard and custom metrics.
Note: Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric

Question: 51

DRAG DROP
You have an Azure subscription that contains 100 virtual machines. Azure Diagnostics is enabled on all the virtual machines.
You are planning the monitoring of Azure services in the subscription.
You need to retrieve the following details:
• Identify the user who deleted a virtual machine three weeks ago.
• Query the security events of a virtual machine that runs Windows Server 2016.
What should you use in Azure Monitor? To answer, drag the appropriate configuration settings to the correct details. Each configuration setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Answer:



Explanation:
Box1: Activity log
Azure activity logs provide insight into the operations that were performed on resources in your subscription. Activity logs were previously known as “audit logs” or “operational logs,” because they report control-plane events for your subscriptions.
Activity logs help you determine the “what, who, and when” for write operations (that is, PUT, POST, or DELETE).
Box 2: Logs
Log Integration collects Azure diagnostics from your Windows virtual machines, Azure activity logs, Azure Security Center alerts, and Azure resource provider logs. This integration provides a unified dashboard for all your assets, whether they're on-premises or in the cloud, so that you can aggregate, correlate, analyze, and alert for security events.
References:
https://docs.microsoft.com/en-us/azure/security/azure-log-audit

Question: 52

Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
The company develops an application named App1. App1 is registered in Azure AD.
You need to ensure that App1 can access secrets in Azure Key Vault on behalf of the application users.
What should you configure?

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

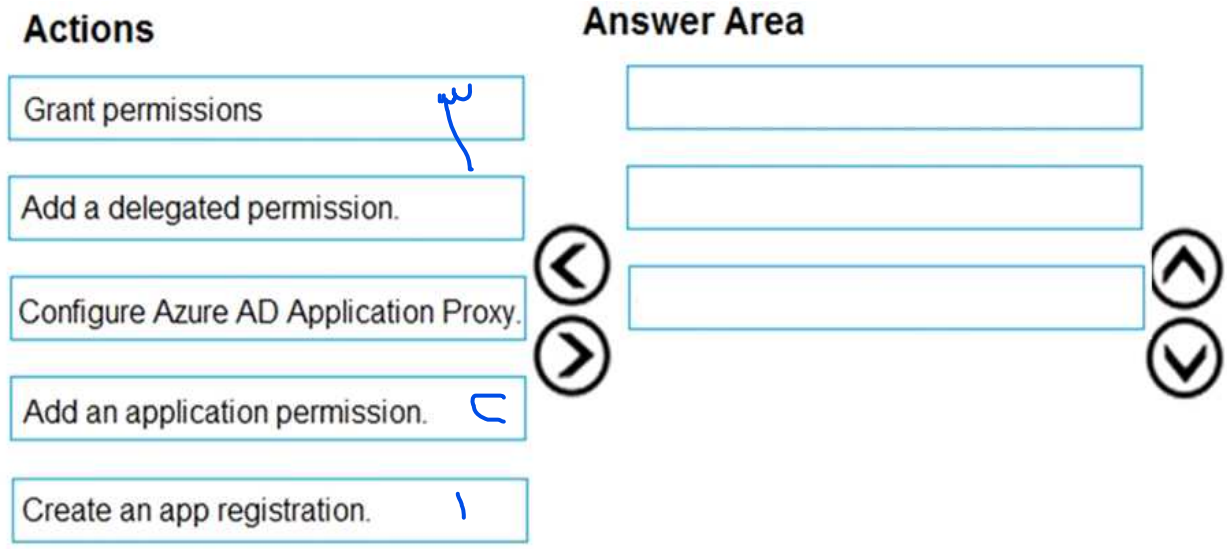
Answer: B

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

Question: 53

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.



Answer:

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

Question: 54

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

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

Answer: A

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

Question: 55

From the Azure portal, you are configuring an Azure policy.
You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects.
Which effect requires a managed identity for the assignment?

A. AuditIfNotExist
B. Append
C. DeployIfNotExist
D. Deny

Answer: C

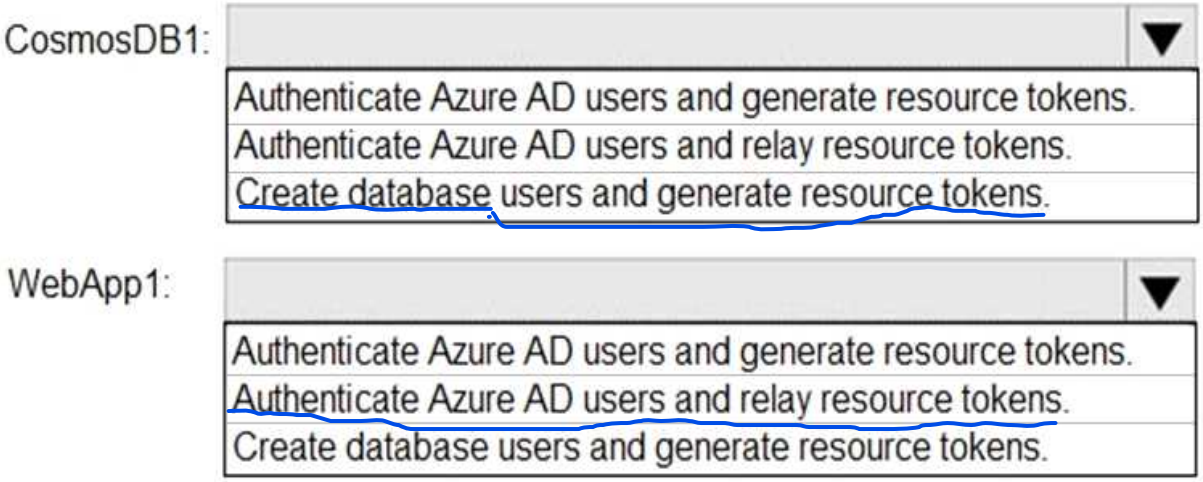
Explanation:
When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.
References:
https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources

Question: 56

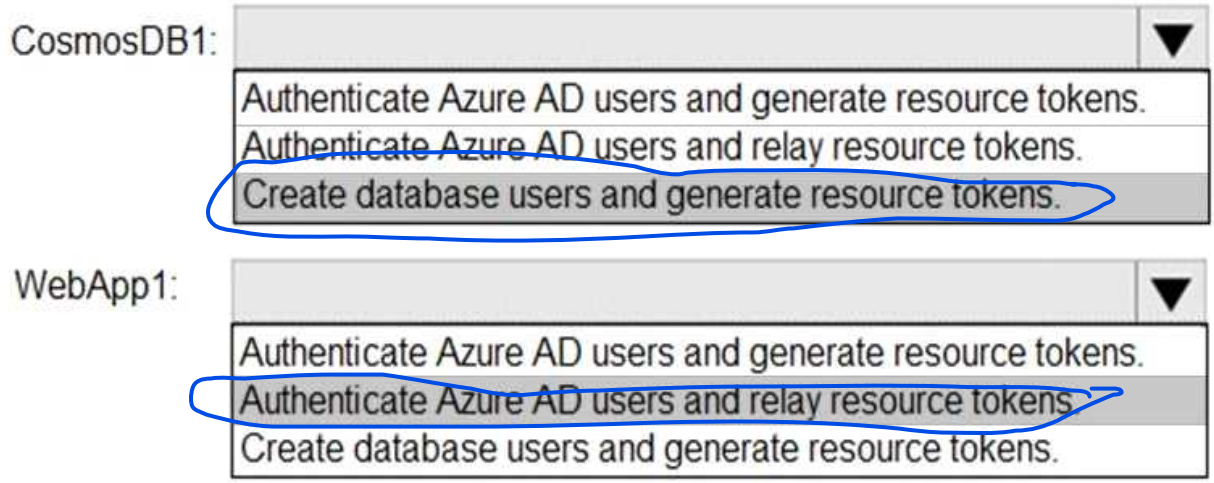
HOTSPOT
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
You plan to implement an application that will consist of the resources shown in the following table.

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

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

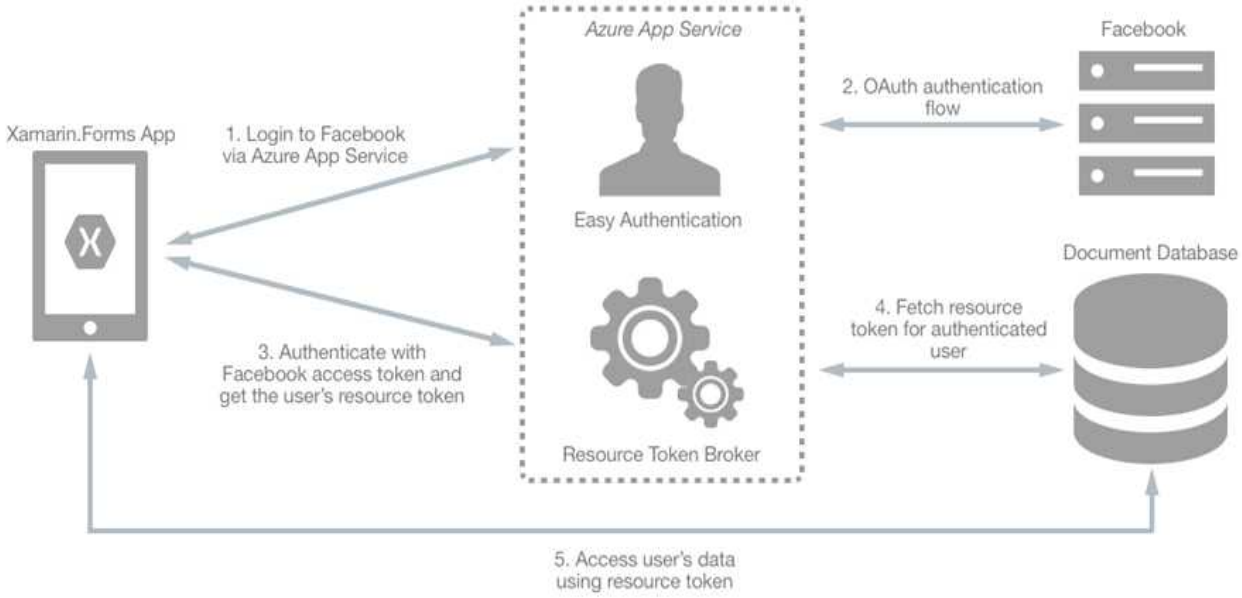


Answer:



Explanation:
CosmosDB1: Create database users and generate resource tokens.
Azure Cosmos DB resource tokens provide a safe mechanism for allowing clients to read, write, and delete specific resources in an Azure Cosmos DB account according to the granted permissions.

WebApp1: Authenticate Azure AD users and relay resource tokens
A typical approach to requesting, generating, and delivering resource tokens to a mobile application is to use a resource token broker. The following diagram shows a high-level overview of how the sample application uses a resource token broker to manage access to the document database data:



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

Question: 57

HOTSPOT
You need to create an Azure key vault. The solution must ensure that any object deleted from the key vault be retained for 90 days.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

```
New-AzureRmKeyVault  -VaultName 'KeyVault1' -ResourceGroupName 'RG1'
    -Location 'East US'  [ ▼ ]  [ ▼ ]
```

-EnabledForDeployment	-Confirm
-EnablePurgeProtection	-DefaultProfile
-Tag	-EnableSoftDelete
	-SKU

Answer:

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

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

-EnabledForDeployment	-Confirm
-EnablePurgeProtection	-DefaultProfile
-Tag	-EnableSoftDelete
	-SKU

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

Question: 58

You have an Azure subscription that contains an Azure key vault named Vault1.
In Vault1, you create a secret named Secret1.
An application developer registers an application in Azure Active Directory (Azure AD).
You need to ensure that the application can use Secret1.
What should you do?

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

Answer: C

Explanation:
"You may need to configure the target resource to allow access from your application. For example, if you request a token to Key Vault, you need to make sure you have added an access policy that includes your application's identity. Otherwise, your calls to Key Vault will be rejected, even if they include the token" https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet

Question: 59

You have an Azure SQL database.
You implement Always Encrypted.
You need to ensure that application developers can retrieve and decrypt data in the database.
Which two pieces of information should you provide to the developers? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Answer: CE

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

Question: 60

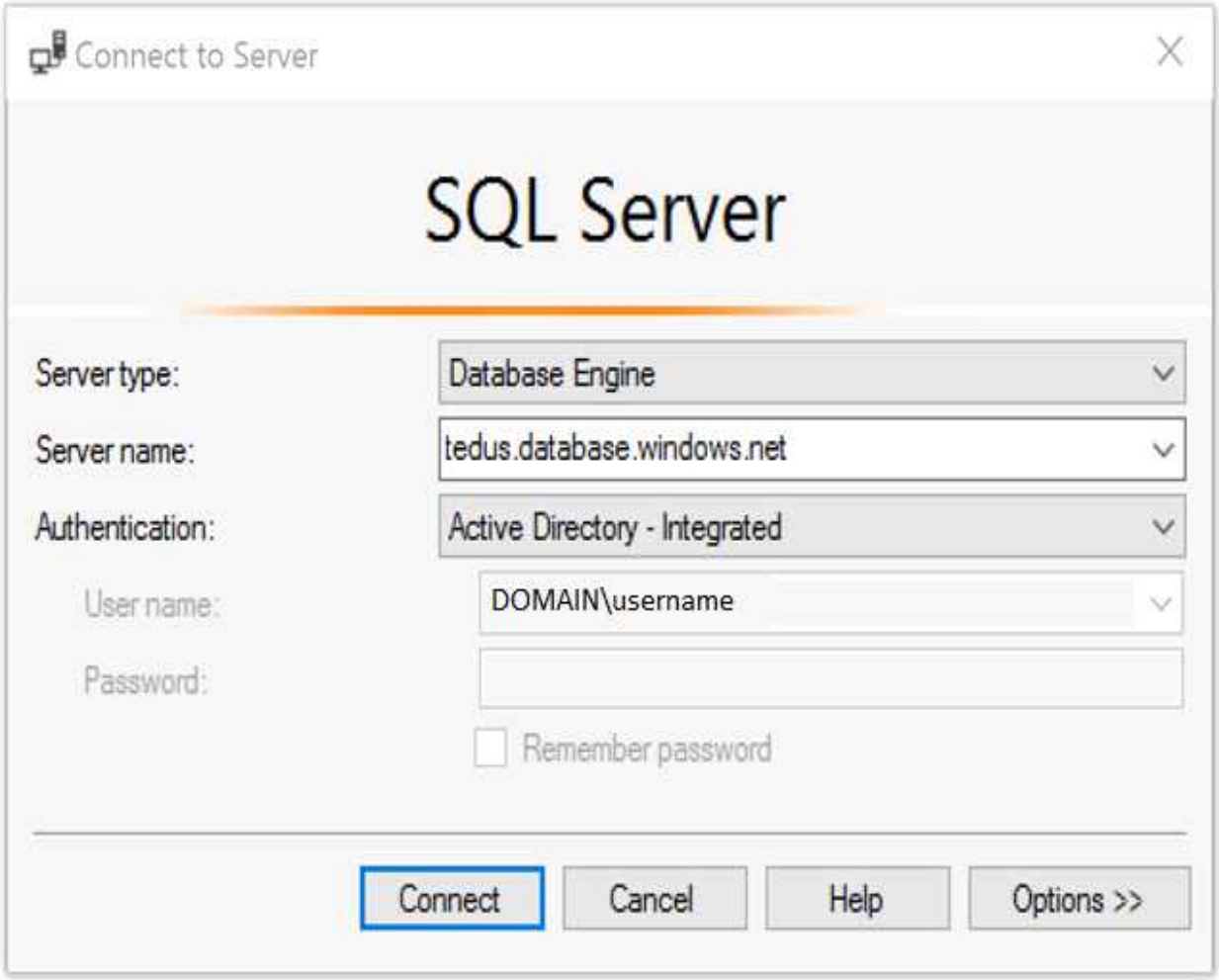
You have a hybrid configuration of Azure Active Directory (Azure AD).
All users have computers that run Windows 10 and are hybrid Azure AD joined.
You have an Azure SQL database that is configured to support Azure AD authentication.
Database developers must connect to the SQL database by using Microsoft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

A. SQL Login
B. Active Directory – Universal with MFA support
C. Active Directory – Integrated
D. Active Directory – Password

Answer: C

Explanation:
Azure AD can be the initial Azure AD managed domain. Azure AD can also be an on-premises Active Directory Domain Services that is federated with the Azure AD.
Using an Azure AD identity to connect using SSMS or SSDT
The following procedures show you how to connect to a SQL database with an Azure AD identity using SQL Server Management Studio or SQL Server Database Tools.
Active Directory integrated authentication
Use this method if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

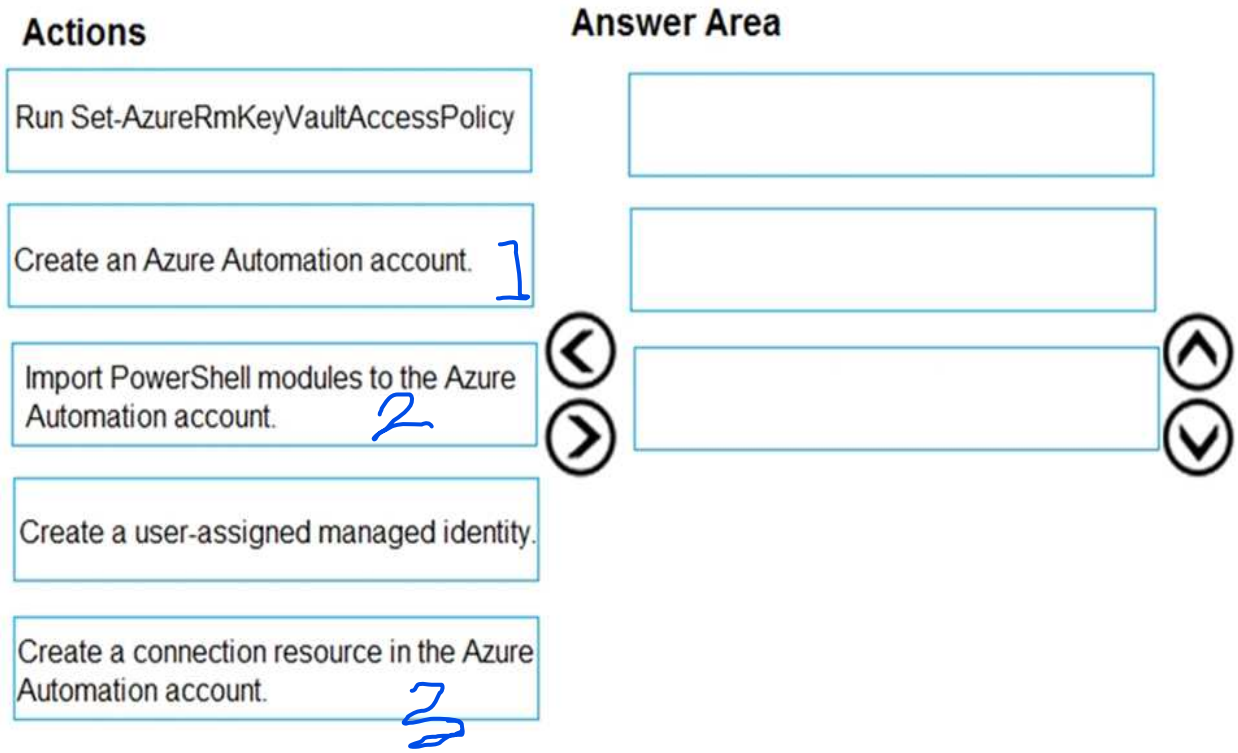
1. Start Management Studio or Data Tools and in the Connect to Server (or Connect to Database Engine) dialog box, in the Authentication box, select Active Directory - Integrated. No password is needed or can be entered because your existing credentials will be presented for the connection.



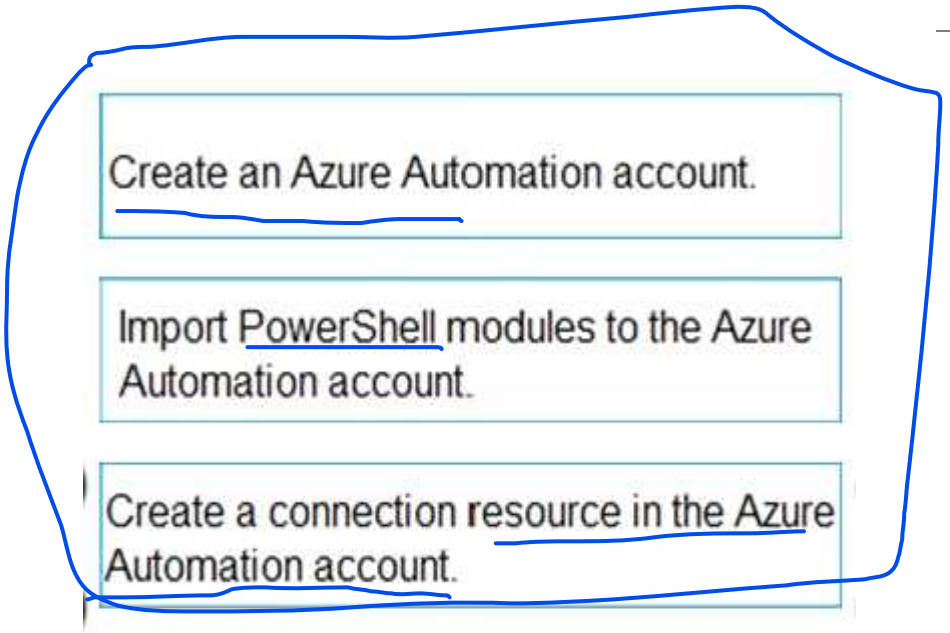
2. Select the Options button, and on the Connection Properties page, in the Connect to database box, type the name of the user database you want to connect to. (The AD domain name or tenant ID" option is only supported for Universal with MFA connection options, otherwise it is greyed out.)
References: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

Question: 61

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



Answer:



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

authentication code, run the same code above to get all the keys from the vault.

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

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

Question: 62

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

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

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: 63

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

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

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

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

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

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

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

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

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

Answer:

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

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

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

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

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

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

Question: 64

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=azuredevops&viewFallbackFrom=vsts

Question: 65

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

Answer: B

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: 66

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

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-configure-using-azure-adds

Question: 67

Your network contains an Active Directory forest named contoso.com. You have an Azure 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.

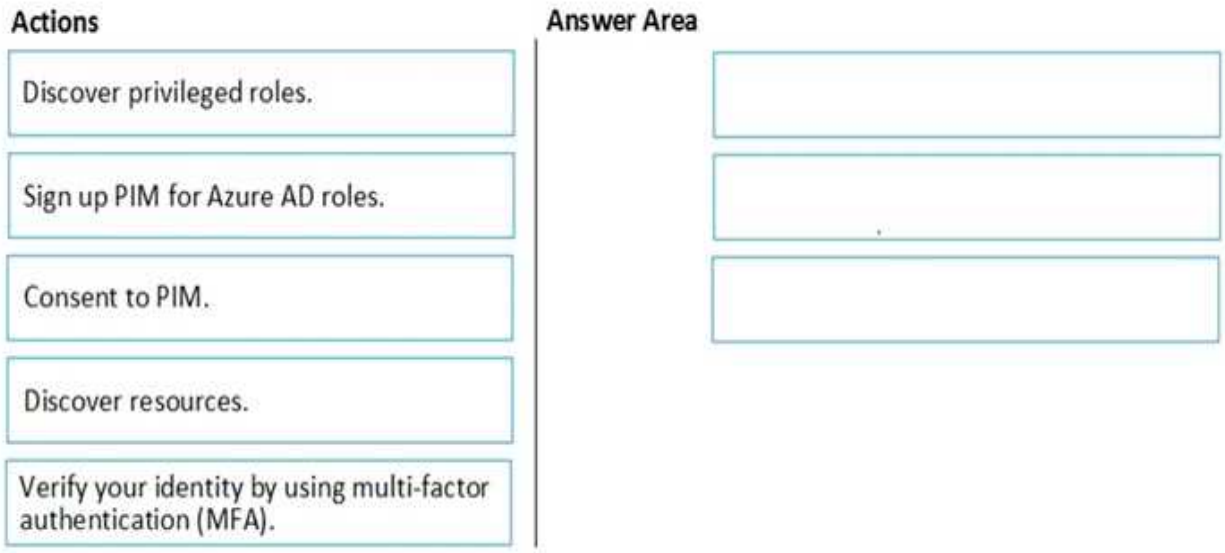
A. the Domain Admins group in Active Directory
B. the Security administrator role in Azure AD
C. the Global administrator role in Azure AD
D. the User administrator role in Azure AD
E. the Enterprise Admins group in Active Directory

Answer: CE

Explanation:
References:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

Question: 68

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.



Answer:

1. Verify your identity with MFA
2. Consent to PIM
3. Sign up PIM for AAD Roles

Question: 69

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 use Azure Security Center for the centralized policy management of three Azure subscriptions.
You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a policy definition and assignments that are scoped to resource groups.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
References:
https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/

Question: 70

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 use Azure Security Center for the centralized policy management of three Azure subscriptions.
You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a resource graph and an assignment that is scoped to a management group.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
References:
https://docs.microsoft.com/en-us/azure/governance/management-groups/create

Question: 71

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

Answer: A

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: 72

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

Answer: B

Explanation:

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

Question: 73

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.

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups

Question: 74

HOTSPOT
You create an alert rule that has the following settings:
- Resource: RG1
- Condition: All Administrative operations
- Actions: Action groups configured for this alert rule: ActionGroup1
- Alert rule name: Alert1

You create an action rule that has the following settings:
- Scope: VM1
- Filter criteria: Resource Type = "Virtual Machines"
- Define on this scope: Suppression
- Suppression config: From now (always)
- Name: ActionRule1

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

Statements	Yes	No
If you start VM1, an alert is triggered.	○	○
If you start VM2, an alert is triggered.	○	○
If you add a tag to RG1, an alert is triggered.	○	○

Answer:

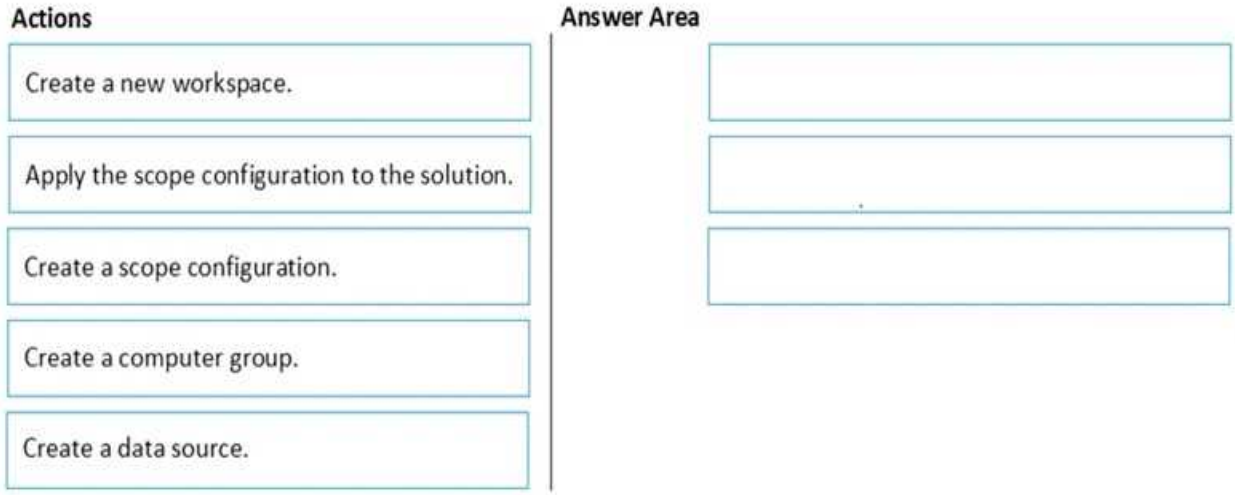
Statements	Yes	No
If you start VM1, an alert is triggered.	○	●
If you start VM2, an alert is triggered.	●	○
If you add a tag to RG1, an alert is triggered.	○	●

Explanation:
Box 1:
The scope for the action rule is set to VM1 and is set to suppress alerts indefinitely.
Box 2:
The scope for the action rule is not set to VM2.
Box 3:
Adding a tag is not an administrative operation.
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-action-rules

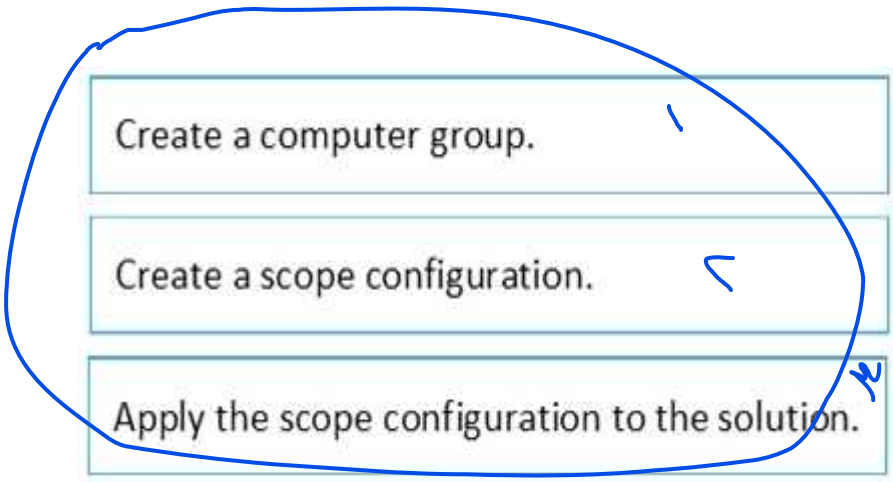
Question: 75

DRAG DROP
You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named

LAW1.
You have 500 Azure virtual machines that run Windows Server 2016 and are enrolled in LAW1.
You plan to add the System Update Assessment solution to LAW1.
You need to ensure that System Update Assessment-related logs are uploaded to LAW1 from 100 of the virtual machines only.
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.



Answer:

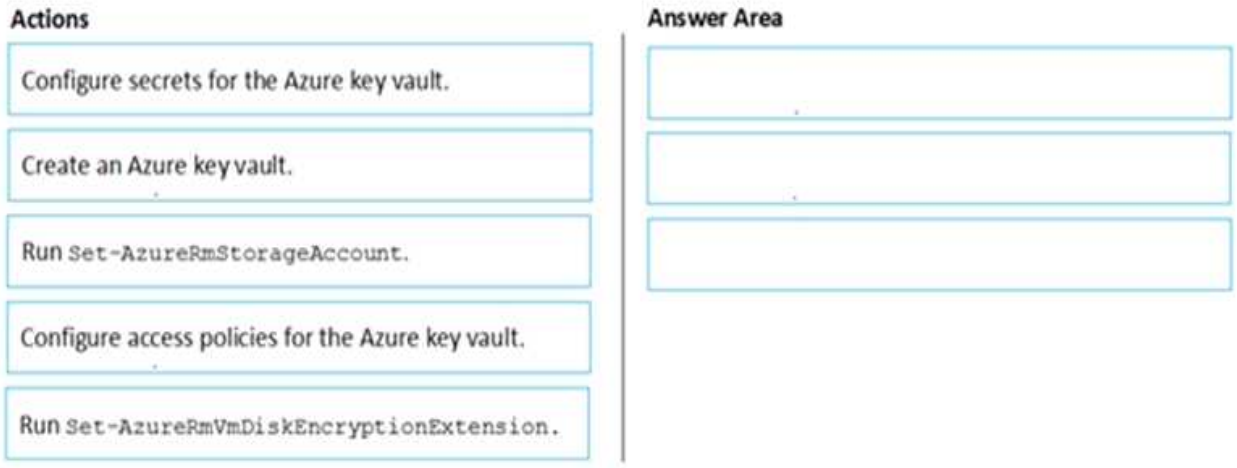


Explanation:
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solution-targeting

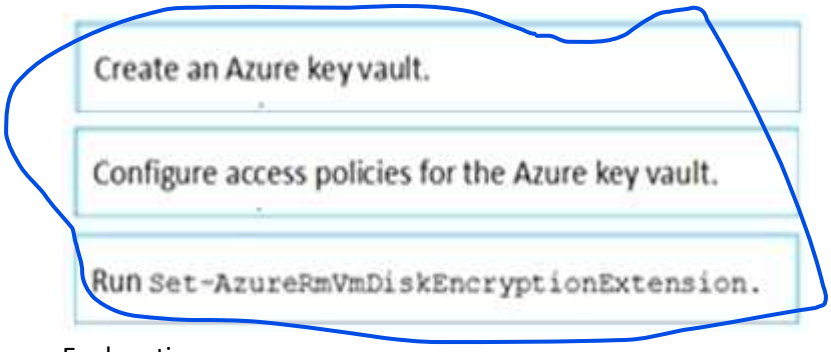
Question: 76

DRAG DROP
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Subscription named Sub1. Sub1 contains an Azure virtual machine named VM1 that runs Windows Server 2016.
You need to encrypt VM1 disks by using Azure Disk Encryption.

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



Answer:



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

Question: 77

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

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

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

Question: 78

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

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

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

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

Answer: A

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

Question: 79

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 rt 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 Sal by using several shared access signatures {SASs) and stored access policies.
You discover that unauthorized users accessed both the rile service and the blob service.
You need to revoke all access to Sa1.
Solution: You regenerate the access keys.
Does this meet the goal?

A. Yes
B. No

Answer: A

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 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: 80

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 use Azure Security Center for the centralized policy management of three Azure subscriptions.
You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a policy initiative and assignments that are scoped to resource groups.
Does this meet the goal?

A. Yes
B. No

Answer: A

Question: 81

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. security policies in Azure Security Center
B. Azure Logic Apps
C. an Azure Desired State Configuration (DSC) virtual machine extension
D. Azure Advisor

Answer: C

Question: 82

You have an Azure subscription named Sub1 that contains the Azure key vaults shown in the following table.

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

In Sub1, you create a virtual machine that has the following configurations:

- Name:VM1
- Size: DS2v2
- Resource group: RG1
- Region: West Europe
- Operating system: Windows Server 2016

You plan to enable Azure Disk Encryption on VM1.
In which key vaults can you store the encryption key for VM1?

A. Vault1 or Vault3 only
B. Vault1, Vault2, Vault3, or Vault4
C. Vault1 only
D. Vault1 or Vault2 only

Answer: D A

Question: 83

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

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

Answer: B

Question: 84

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

Answer: B

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: 85

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.

Statements	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 activate the Password Administrator role, the user can approve their own request.	○	○

Answer:

Statements	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 activate the Password Administrator role, the user can approve their own request.	○	○

Reference:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-resource-roles-assign-roles

Question: 86

You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure SQL Database
instance that is configured to support Azure AD authentication.
Database developers must connect to the database instance 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

Answer: D

Explanation:
References:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

Question: 87

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?

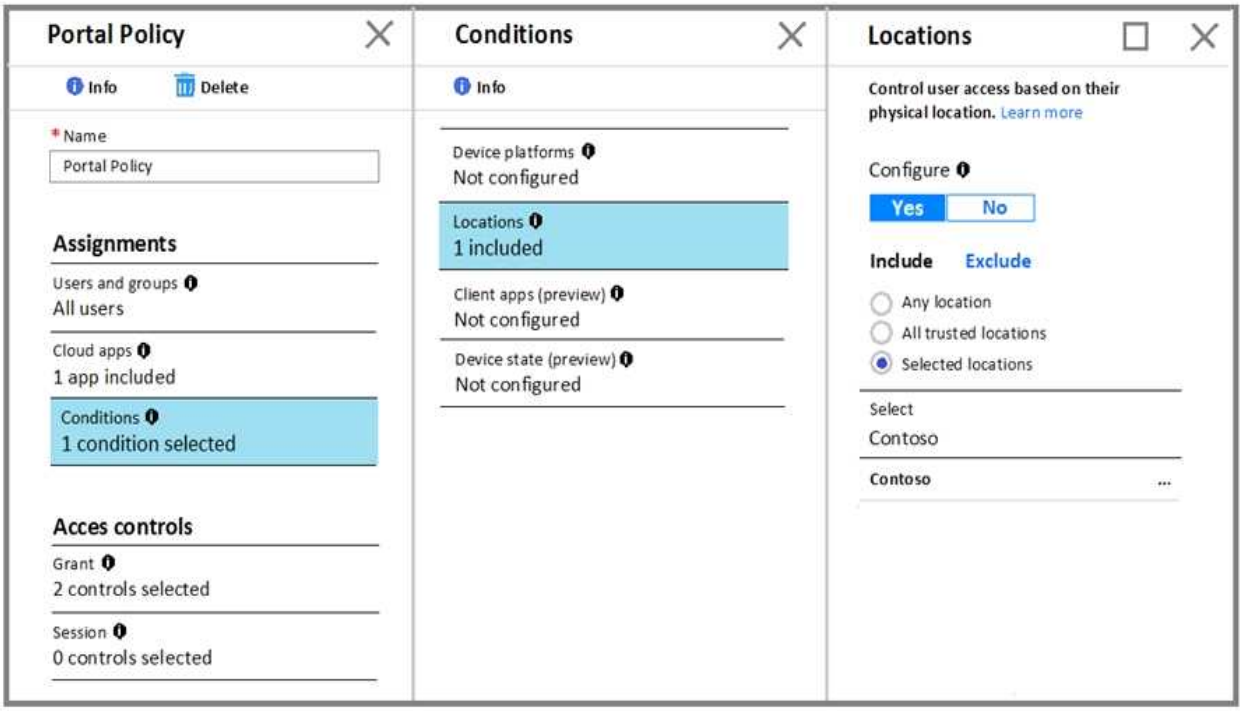
A. a key vault access policy
B. a linked template
C. a parameters file
D. an automation account

Answer: B C

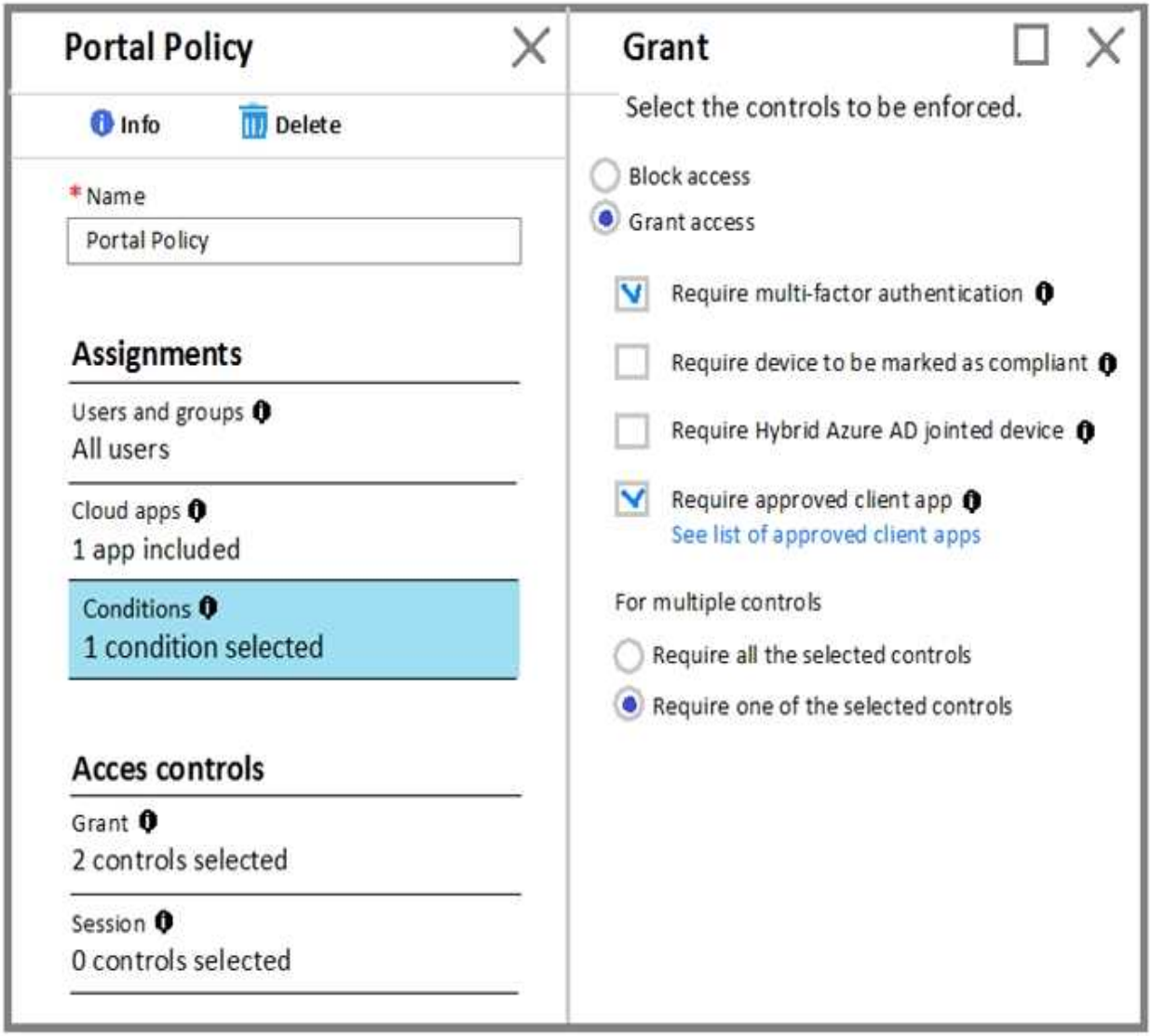
Explanation:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli#reference-secrets-with-dynamic-id

Question: 88

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.)



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.

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:

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.	●	○

Explanation:

Box 1: No
The Contoso location is excluded
Box 2: NO
Box 3: NO
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Question: 89

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

Answer: C

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-anaccount-in-another-azure-ad-tenant

Question: 90

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

Answer: D

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: 91

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

Answer: C

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: 92

HOTSPOT
You have a network security group (NSG) bound to an Azure subnet.
You run Get-AzureRmNetworkSecurityRuleConfig 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.

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:

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

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: 93

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

Answer: C

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: 94

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.

Answer: B

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: 95

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 deployedtogether. 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

Answer: D

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: 96

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.

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:

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.	●	○

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: 97

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 use Azure Security Center for the centralized policy management of three Azure subscriptions.
You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a policy initiative and assignments that are scoped to resource groups.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead use a management group.
Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously.
Reference:
https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-managementgroups/

Question: 98

You have an Azure subscription named Sub1 that contains the virtual machines shown in the following table.

Name	Resource group
VM1	RG1
VM2	RG2
VM3	RG1
VM4	RG2

You need to ensure that the virtual machines in RG1 have the Remote Desktop port closed until an authorized user requests access.
What should you configure?

A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
B. an application security group
C. Azure Active Directory (Azure AD) conditional access
D. just in time (JIT) VM access

Answer: D

Explanation:
Just-in-time (JIT) virtual machine (VM) access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.
Note: When just-in-time is enabled, Security Center locks down inbound traffic to your Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the just-in-time solution.
When a user requests access to a VM, Security Center checks that the user has Role-Based Access Control (RBAC) permissions that permit them to successfully request access to a VM. If the request is approved, Security Center automatically configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the amount of time that was specified. After the time has expired, Security Center restores the NSGs to their previous states. Those connections that are already established are not being interrupted, however.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

Question: 99

You have 10 virtual machines on a single subnet that has a single network security group (NSG).
You need to log the network traffic to an Azure Storage account.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Install the Network Performance Monitor solution.
B. Enable Azure Network Watcher.
C. Enable diagnostic logging for the NSG.
D. Enable NSG flow logs.
E. Create an Azure Log Analytics workspace.

Answer: BD

Explanation:
A network security group (NSG) enables you to filter inbound traffic to, and outbound traffic from, a virtual
machine (VM). You can log network traffic that flows through an NSG with Network Watcher's NSG flow log capability. Steps include:
• Create a VM with a network security group
• Enable Network Watcher and register the Microsoft.Insights provider
• Enable a traffic flow log for an NSG, using Network Watcher's NSG flow log capability
• Download logged data

• View logged data
Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal

Question: 100

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

Name	Operating system
VM1	Windows Server 2016
VM2	Ubuntu Server 18.04 LTS

From Azure Security Center, you turn on Auto Provisioning.
You deploy the virtual machines shown in the following table.

Name	Operating system
VM3	Windows Server 2016
VM4	Ubuntu Server 18.04 LTS

On which virtual machines is the Log Analytics agent installed?

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

Answer: D

Explanation:
When automatic provisioning is On, Security Center provisions the Log Analytics Agent on all supported Azure VMs and any new ones that are created.
Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

Question: 101

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

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

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

A. Vault1 or Vault3 only
B. Vault1, Vault2, Vault3, or Vault4
C. Vault1 only
D. Vault1 or Vault2 only

Answer: A

Explanation:
In order to make sure the encryption secrets don't cross regional boundaries, Azure Disk Encryption needs the Key Vault and the VMs to be co-located in the same region. Create and use a Key Vault that is in the same region as the VM to be encrypted.
Reference:
https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites

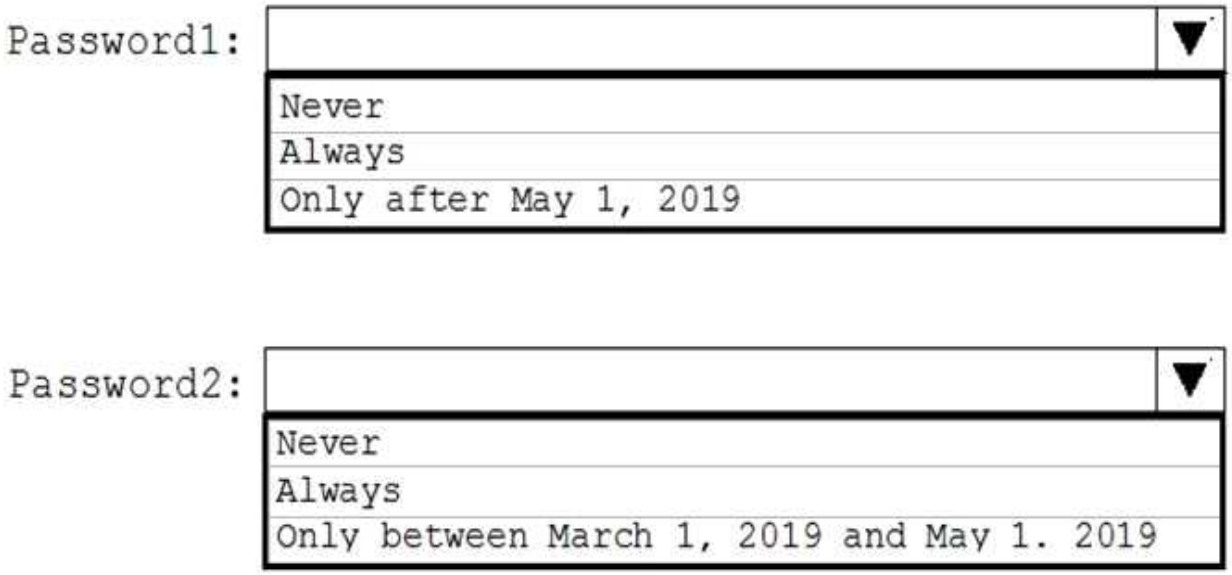
Question: 102

HOTSPOT
You have an Azure subscription that contains an Azure key vault named Vault1.
On January 1, 2019, Vault1 stores the following secrets.

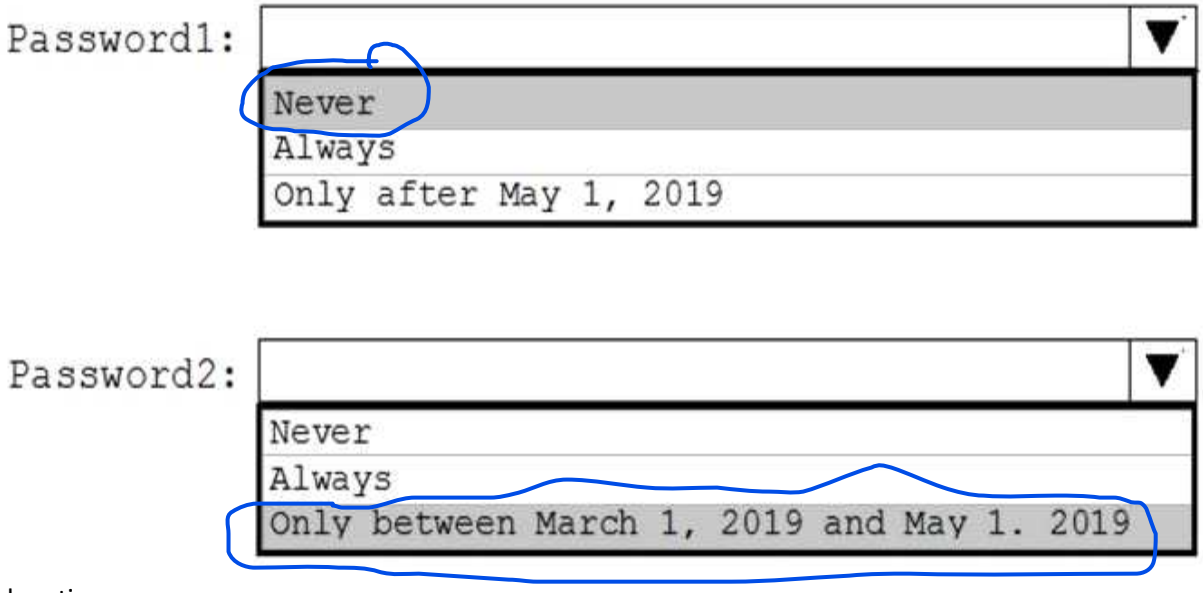
```
Enabled      : False
Expires      :
NotBefore    : 5/1/19 12:00:00 AM
Created      : 12/20/18 2:55:00 PM
Updated      : 12/20/18 2:55:00 PM
ContentType  :
Tags         :
TagTable     :
VaultName    : vault1
Name         : Password1
Version      :
Id           : https://vault1.vault.azure.net:443/secrets/Password1

Enabled      : True
Expires      : 5/1/19 12:00:00 AM
NotBefore    : 3/1/19 12:00:00 AM
Created      : 12/20/18 3:00:00 PM
Updated      : 12/20/18 3:00:00 PM
ContentType  :
Tags         :
TagsTable    :
VaultName    : vault1
Name         : Password2
Version      :
Id           : https://vault1.vault.azure.net:443/secrets/Password2
```

Which can each secret be used by an application? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



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

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

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

Question: 103

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

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

Answer: B

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

Question: 104

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 use Azure Security Center for the centralized policy management of three Azure subscriptions.
You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create an initiative and an assignment that is scoped to a management group.
Does this meet the goal?

A. Yes
B. No

Answer: A

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

Question: 105

You are troubleshooting a security issue for an Azure Storage account.
You enable the diagnostic logs for the storage account. What should you use to retrieve the diagnostics logs?

A. the Security & Compliance admin center
B. SQL query editor in Azure
C. File Explorer in Windows
D. AzCopy

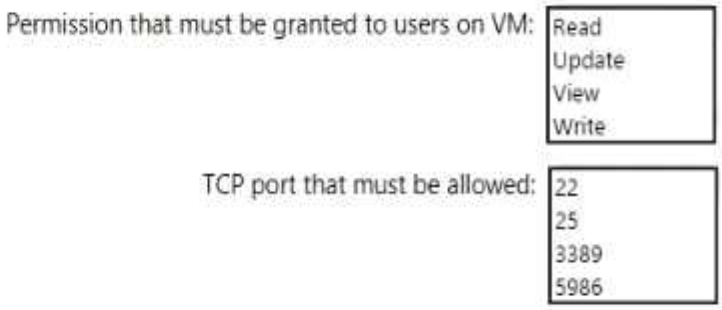
Answer: D

References:
https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-logging?toc=%2fazure%2fstorage%2fblobs%2ftoc.json

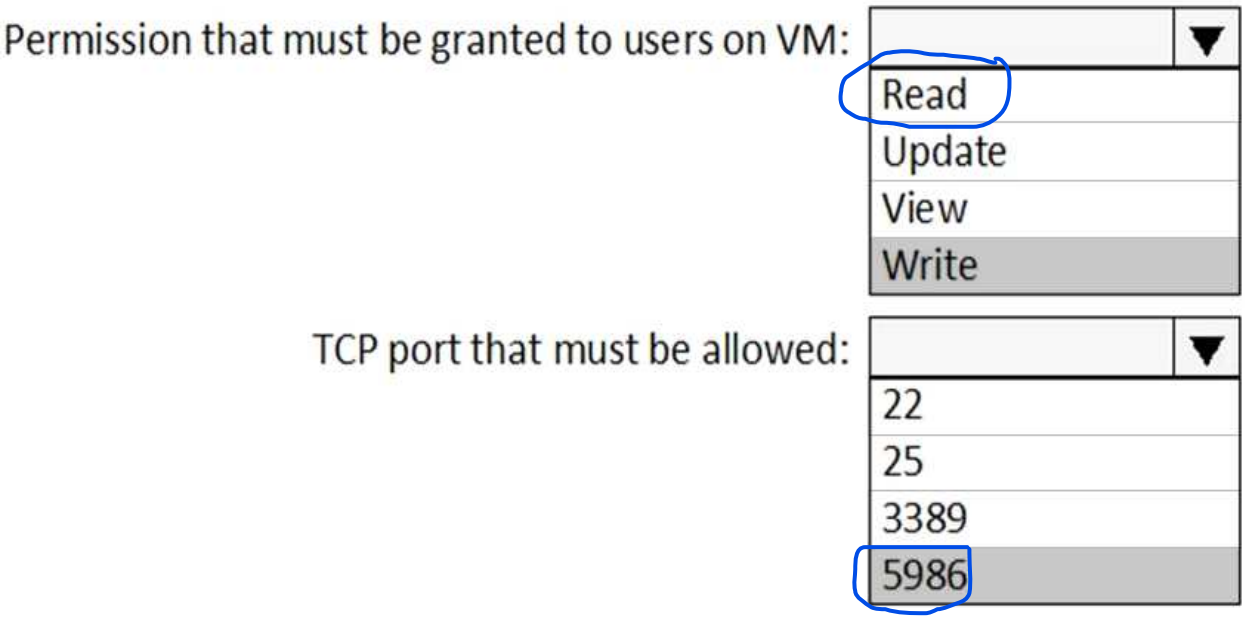
Question: 106

HOTSPOT
You are configuring just in time (JIT) VM access to a set of Azure virtual machines.
You need to grant users PowerShell access to the virtual machine by using JIT VM access.
What should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:



Question: 107

HOTSPOT

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

Name	Type	Region	Resource group
SQL1	Azure SQL database	East US	RG1
Analytics1	Azure Log Analytics workspace	East US	RG1
Analytics2	Azure Log Analytics workspace	East US	RG2
Analytics3	Azure Log Analytics workspace	West Europe	RG1

You create the Azure Storage accounts shown in the following table.

Name	Region	Resource group	Storage account type	Access tier (default)
Storage1	East US	RG1	Blob	Cool
Storage2	East US	RG2	General purpose V1	*Not applicable*
Storage3	West Europe	RG1	General purpose V2	Hot

You need to configure auditing for SQL1.

Which storage accounts and Log Analytics workspaces can you use as the audit log destination? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Storage accounts that can be used as the audit log destination:
- Storage1 only
- Storage2 only
- Storage1 and Storage2 only
- Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:
- Analytics1 only
- Analytics1 and Analytics2 only
- Analytics1 and Analytics3 only
- Analytics1, Analytics2, and Analytics3

Answer:

Storage accounts that can be used as the audit log destination:
- Storage1 only
- Storage2 only
- Storage1 and Storage2 only
- Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:
- Analytics1 only
- Analytics1 and Analytics2 only
- Analytics1 and Analytics3 only
- Analytics1, Analytics2, and Analytics3

Question: 108

HOTSPOT

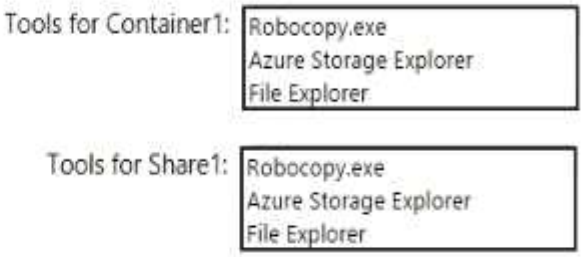
You have an Azure subscription named Sub1. Sub1 has an Azure Storage account named Storage1 that contains the resources shown in the following table.

Name	Type
Container1	Blob container
Share1	File share

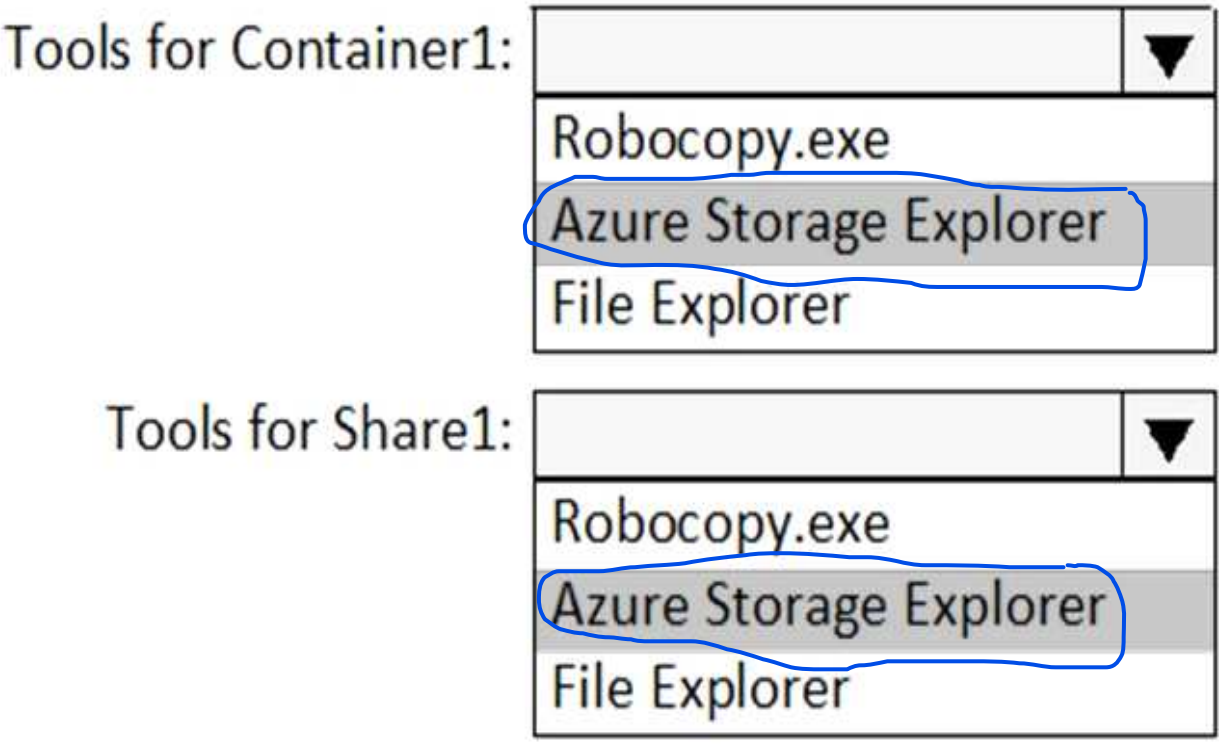
You generate a shared access signature (SAS) to connect to the blob service and the file service.

Which tool can you use to access the contents in Container1 and Share! by using the SAS? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:



Question: 109

You have an Azure Storage account named storage1 that has a container named container1. You need to prevent the blobs in container1 from being modified. What should you do?

A. From container1, change the access level.
B. From container1 add an access policy.
C. From container1, modify the Access Control (1AM) settings.
D. From storage1 , enable soft delete for blobs.

Answer: B

Explanation:
References:
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage?tabs=azure-portal

Question: 110

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	Block 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.

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:

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.	○	○

Question: 111

DRAG DROP

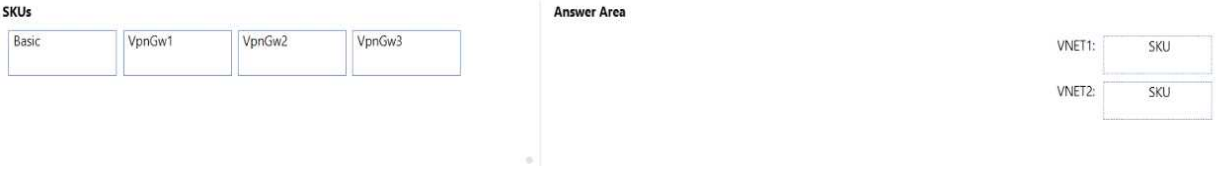
You are configuring network connectivity for two Azure virtual networks named VNET1 and VNET2.

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 SKI) 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



Answer:

Explanation:

References:

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

Question: 112

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 use?

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

Answer: B

Question: 113

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 ?2 license.
You plan lo 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
Answer Area

Users who can onboard Azure AD Identity Protection:
- User1 only
- User1 and User2 only
- User1, User 2, and User3 only
- User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:
- User1 and User2 only
- User1 and User3 only
- User1, User 2, and User3 only
- User1, User 2, User3, and User 4

Answer:

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

Question: 114

HOTSPOT

You ate 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.

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 private 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 private IP address of VM5.	○	○

Question: 115

You have an Azure subscription that contains a user named User1 and an Azure Container Registry named ConReg1.
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.

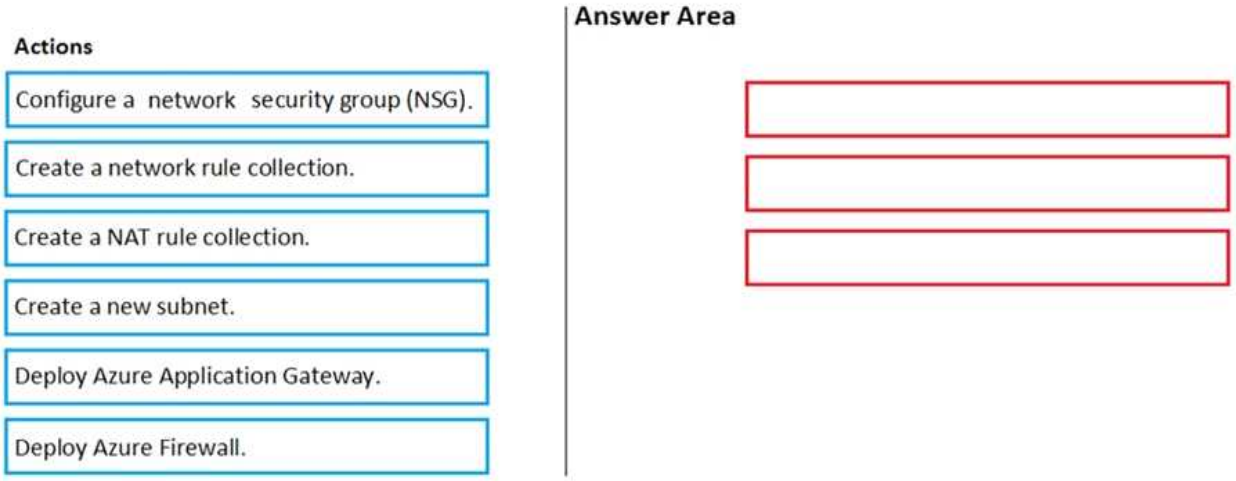
A. AcrQuarantineReader
B. Contributor
C. AcrPush
D. AcrImageSigner
E. AcrQuarantineWriter

Answer: CD

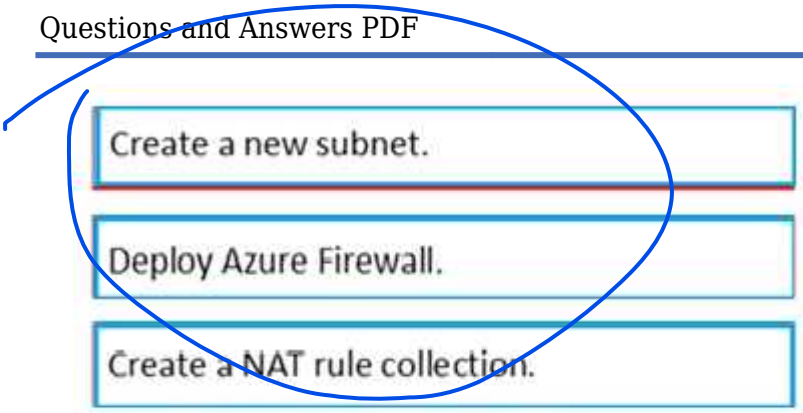
Explanation:
References:
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles

Question: 116

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.



Answer:



Question: 117

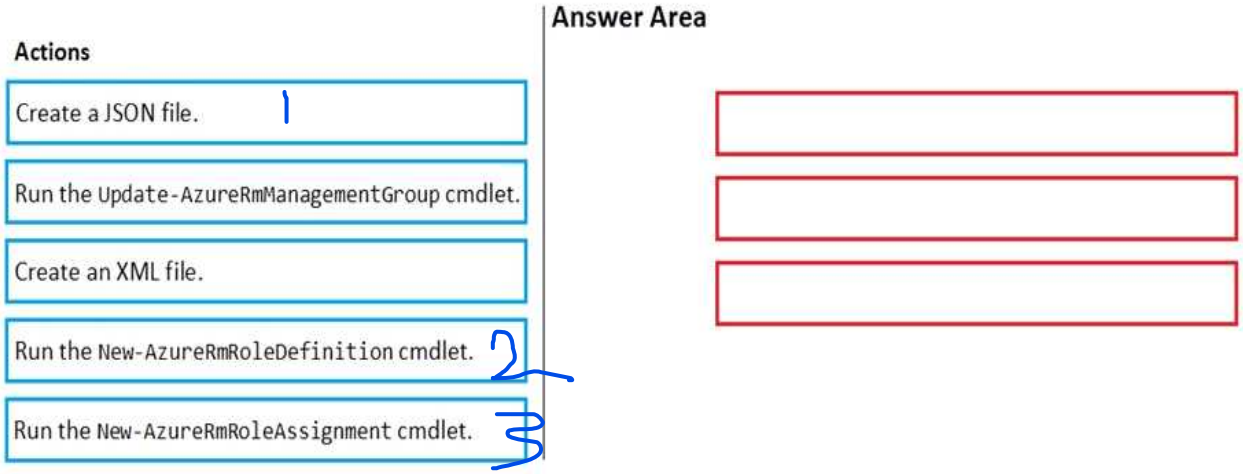
DRAG DROP

You have an Azure subscription named Sub1.

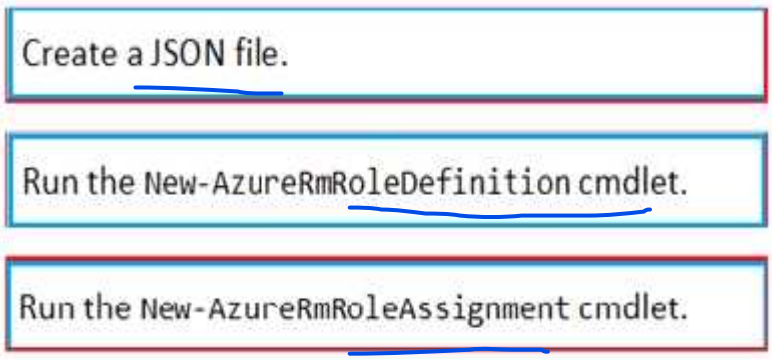
You have an Azure Active Directory (Azure AD) group named Group1 that contains all the members of your IT team.

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.



Answer:



Explanation:

References:

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

Question: 118

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

Name	Operating system	State
VM1	Windows Server 2008 R2 Service Pack 1 (SP1)	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

Answer: C

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

Question: 119

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

Answer: B

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

Question: 120

You company has an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to create several security alerts by using Azure Monitor.
You need to prepare the Azure subscription for the alerts.
What should you create first?

A. An Azure Storage account
B. an Azure Log Analytics workspace
C. an Azure event hub
D. an Azure Automation account

Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-create-workspace

Question: 121

You company has an Azure subscription named Sub1. Sub1 contains an Azure web app named WebApp1 that uses Azure Application Insights. WebApp1 requires users to authenticate by using OAuth 2.0 client secrets.
Developers at the company plan to create a multi-step web test app that preforms synthetic transactions emulating user traffic to Web App1.
You need to ensure that web tests can run unattended.
What should you do first?

A. In Microsoft Visual Studio, modify the .webtest file.
B. Upload the .webtest file to Application Insights.
C. Register the web test app in Azure AD.
D. Add a plug-in to the web test app.

Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep

Question: 122

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

Name	Operating system
VM1	Windows Server 2016
VM2	Ubuntu Server 18.04 LTS

From Azure Security Center, you turn on Auto Provisioning.
You deploy the virtual machines shown in the following table.

Name	Operating system
VM3	Windows Server 2016
VM4	Ubuntu Server 18.04 LTS

On which virtual machines is the Microsoft Monitoring agent installed?

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

Answer: D

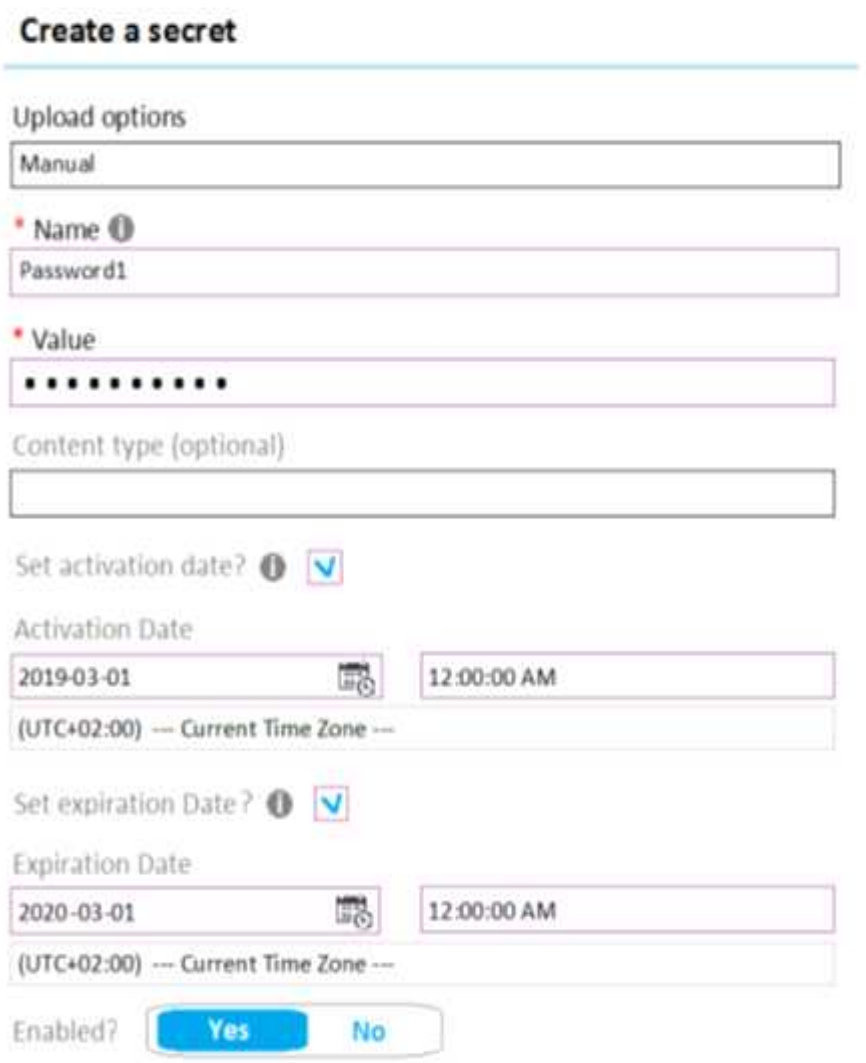
Explanation:
When automatic provisioning is enabled, Security Center provisions the Microsoft Monitoring Agent on all supported Azure VMs and any new ones that are created.
Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803.
References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-faq

Question: 123

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

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

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



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.

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

Answer:

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

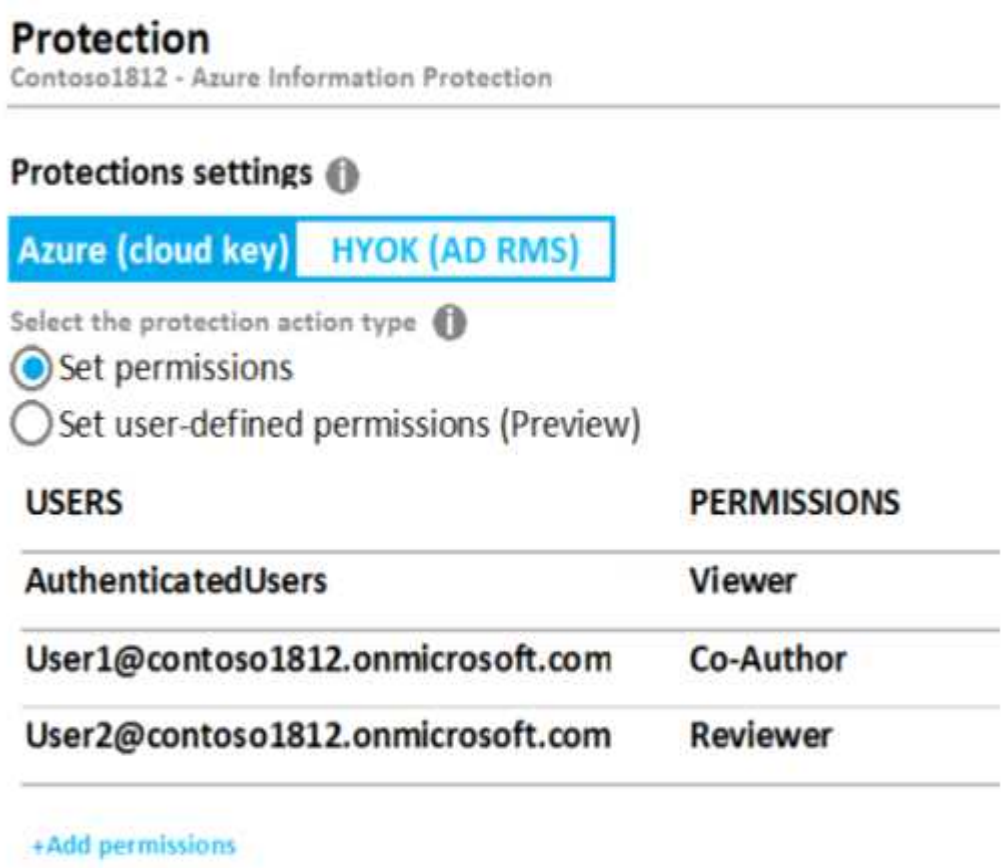
Question: 124

HOTSPOT

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

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

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



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

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

Answer:

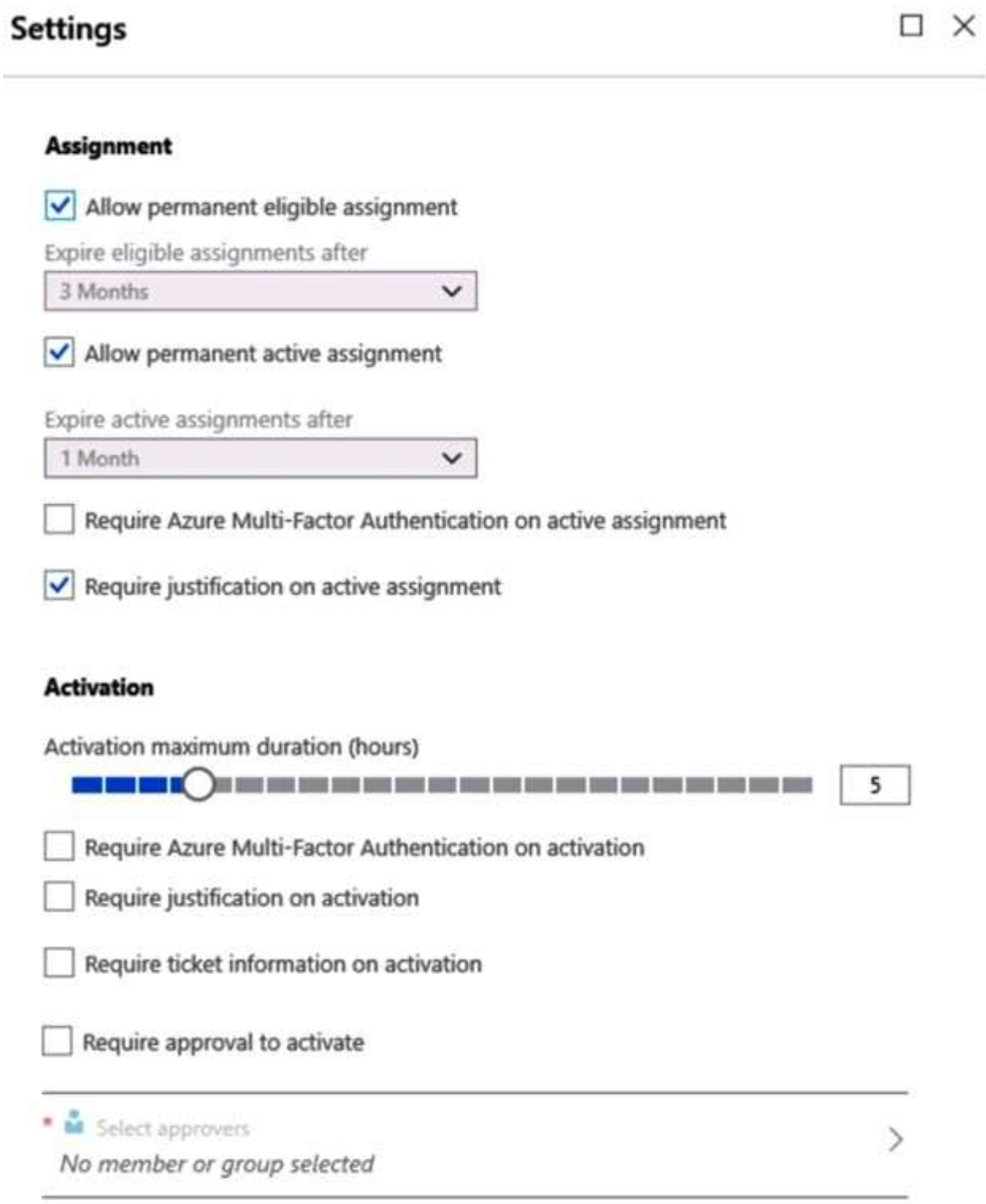
Question: 125

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.



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.

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:

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.	○	○

Explanation:
Box 1: Yes
Eligible Type: A role assignment that requires a user to perform one or more actions to use the role. If a user has been made eligible for a role, that means they can activate the role when they need to perform privileged tasks. There's no difference in the access given to someone with a permanent versus an eligible role assignment. The only difference is that some people don't need that access all the time.
You can choose from two assignment duration options for each assignment type (eligible and active) when you configure settings for a role. These options become the default maximum duration when a user is assigned to the role in Privileged Identity Management.
Use the Activation maximum duration slider to set the maximum time, in hours, that a role stays active before it expires. This value can be from one to 24 hours.
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: Yes
User3 is member of Group2.
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: 126

HOTSPOT

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

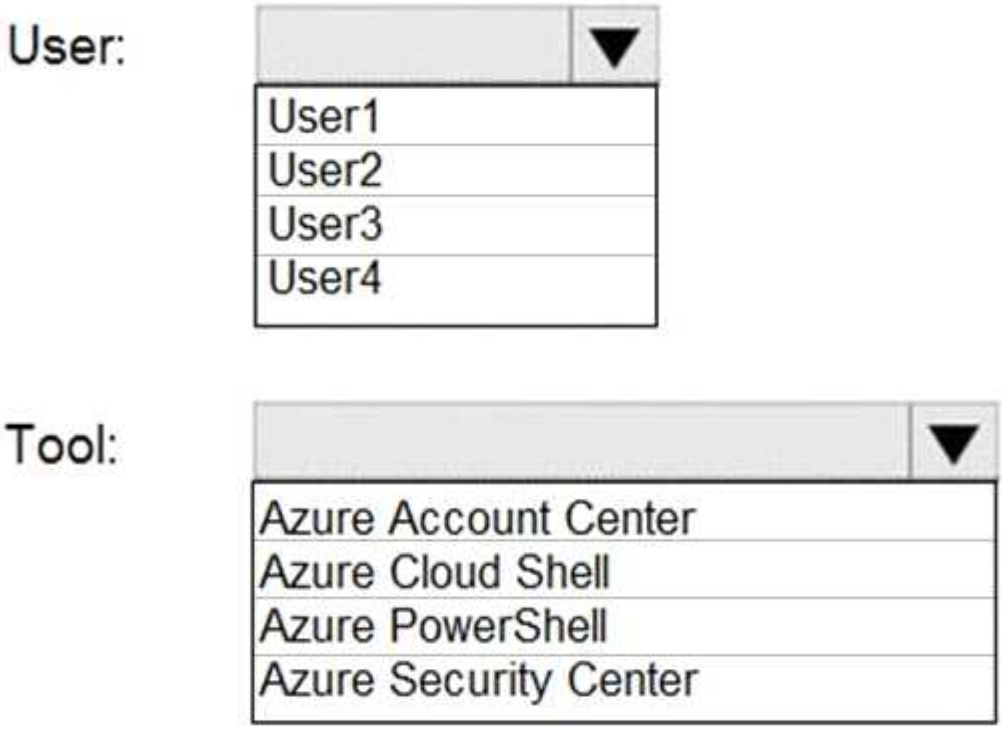
Name	Role
User1	Global administrator
User2	Billing administrator
User3	Owner
User4	Account Admin

The company is sold to a new owner.

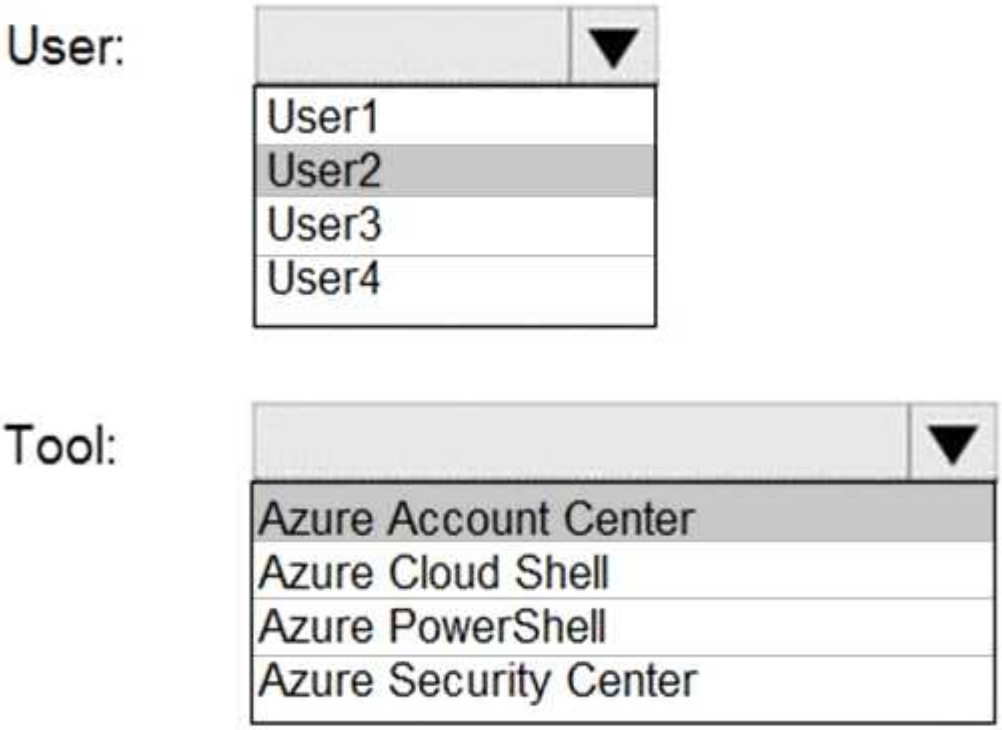
The company needs to transfer ownership of Subscription1.

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.



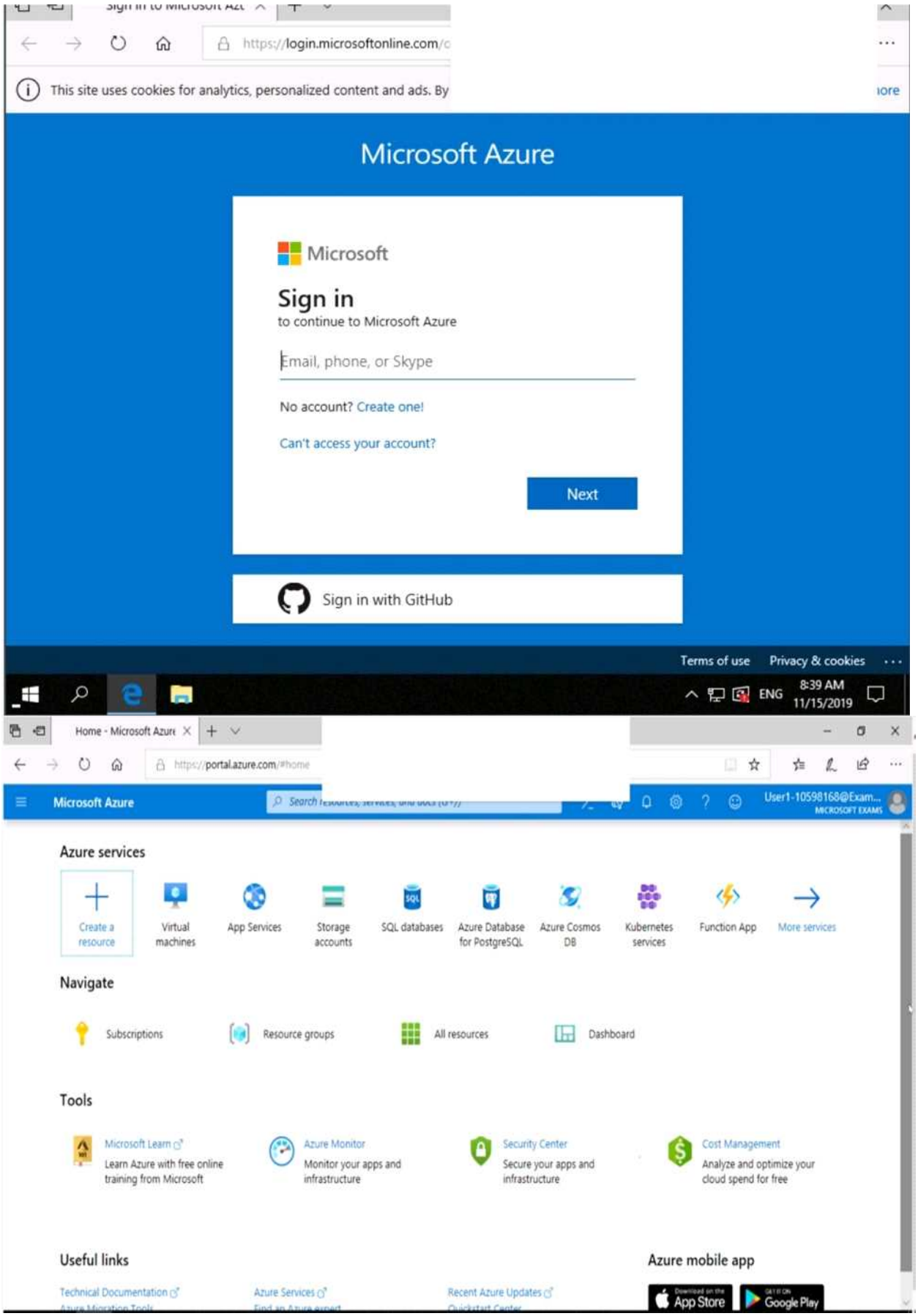
Answer:

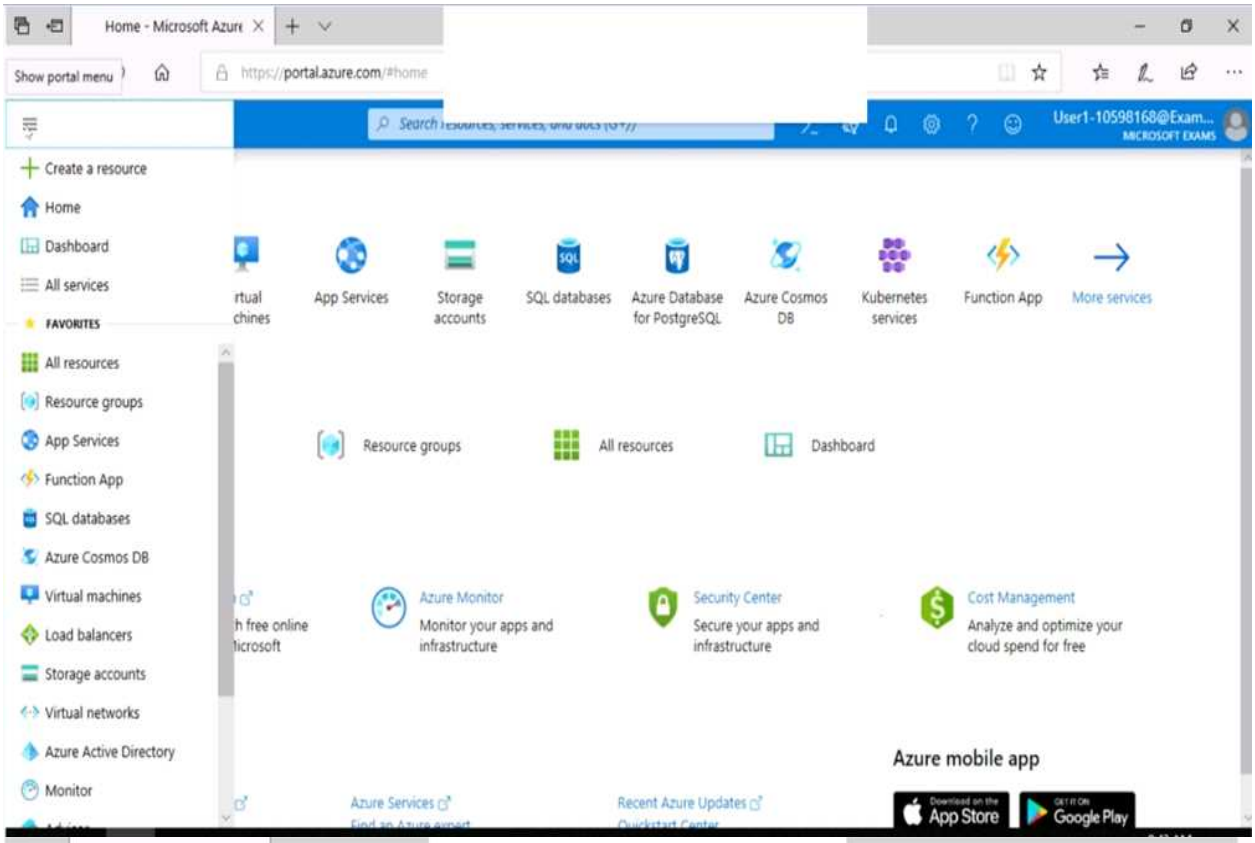


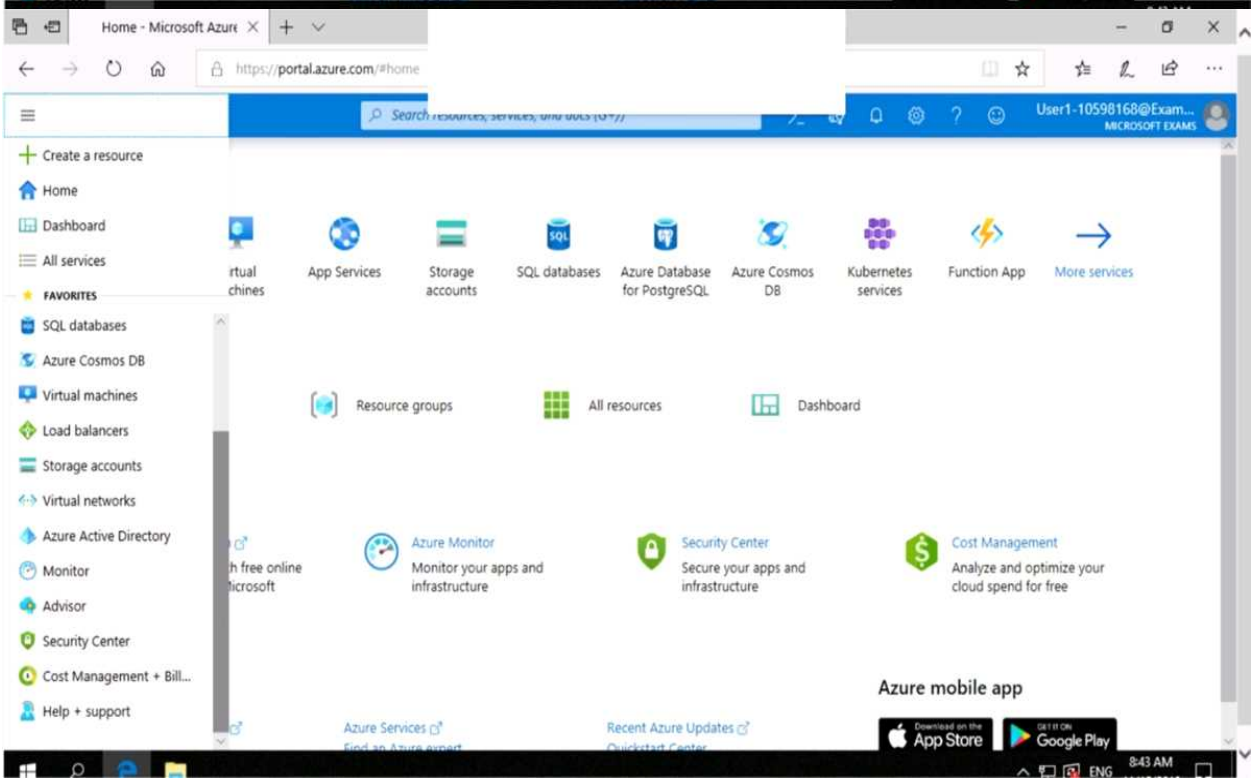
Explanation:
Box 1; User2
Billing Administrator
Select Transfer billing ownership for the subscription that you want to transfer.
Enter the email address of a user who's a billing administrator of the account that will be the new owner for the subscription.
Box 2: Azure Account Center
Azure Account Center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

Question: 127

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
Home - Microsoft Azure
https://portal.azure.com/#home
Microsoft Azure
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 Services
Recent Azure Updates
Azure mobile app
App Store
Google Play





The developers at your company plan to create a web app named App10598168 and to publish the app to https://www.contoso.com.

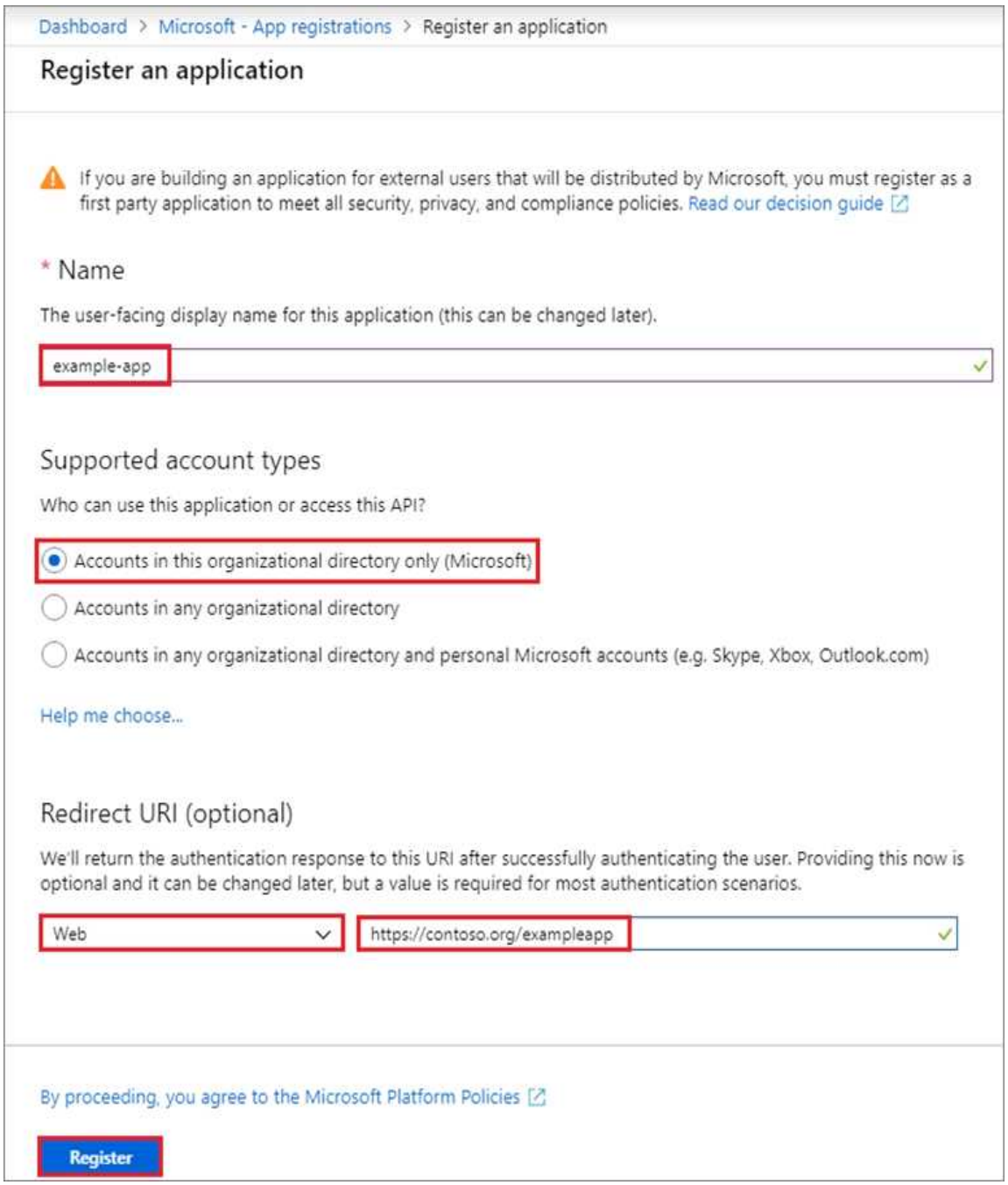
You need to perform the following tasks:

- 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.

Answer:

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.

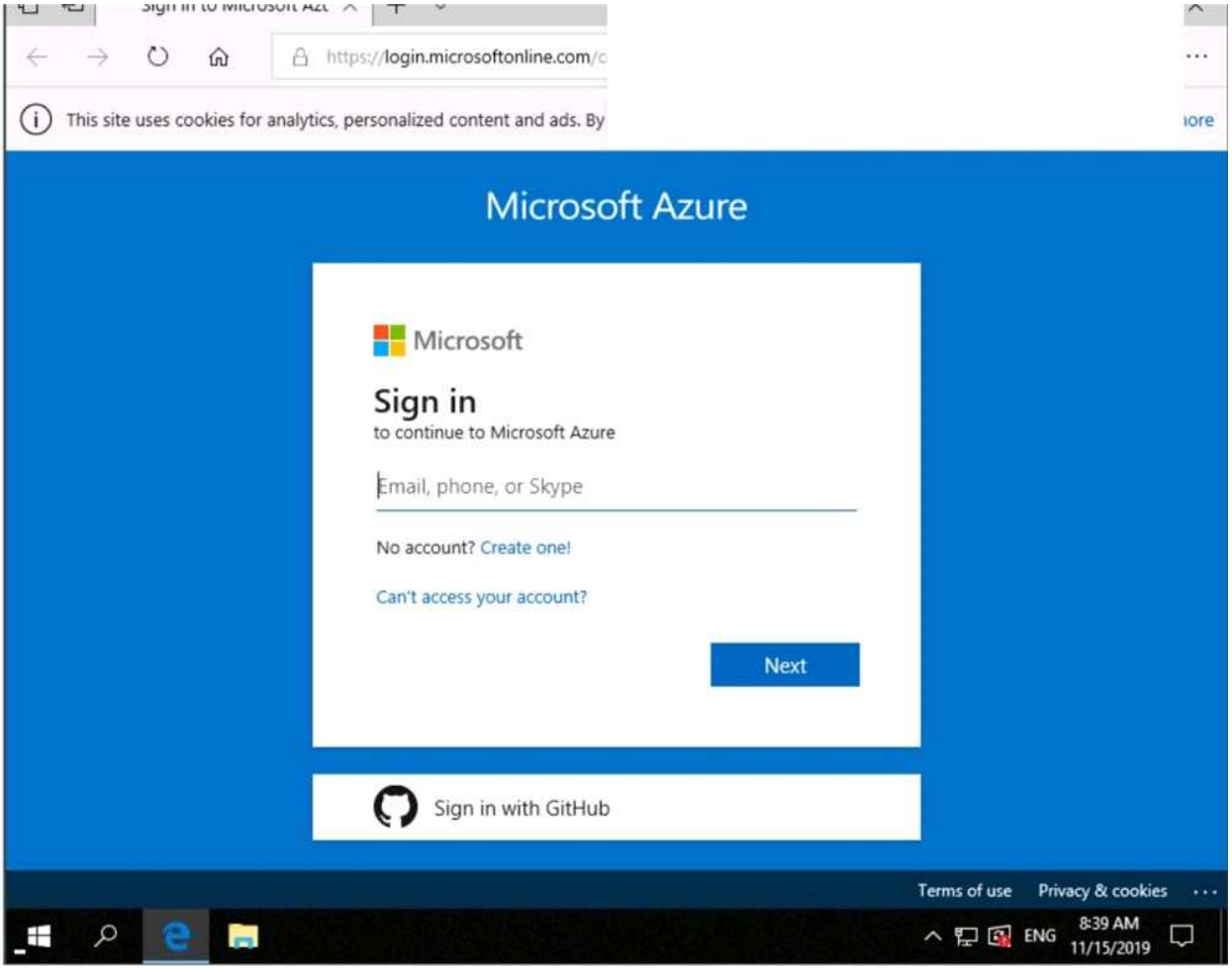


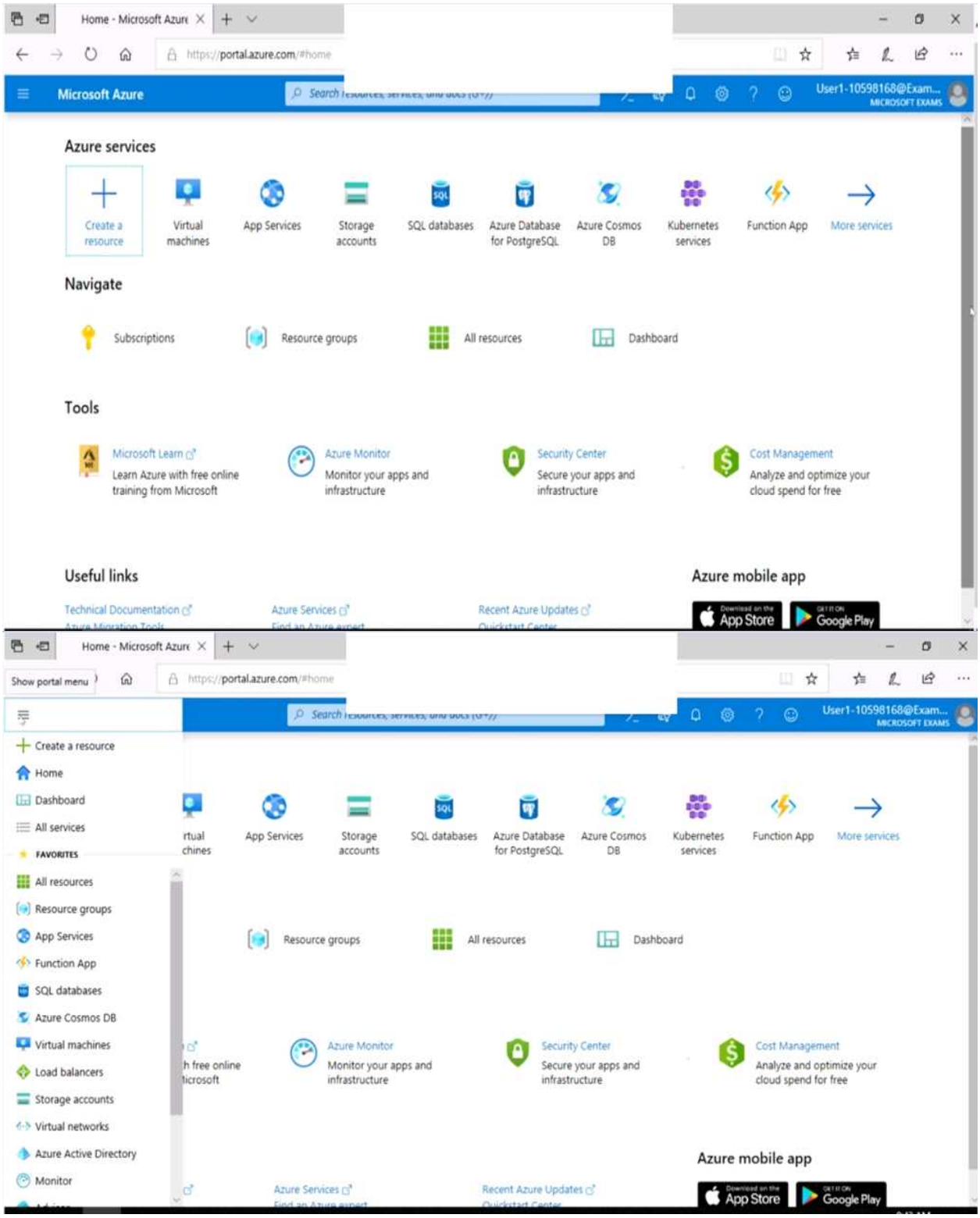
6. Click Register
Step 2: Create a new application secret

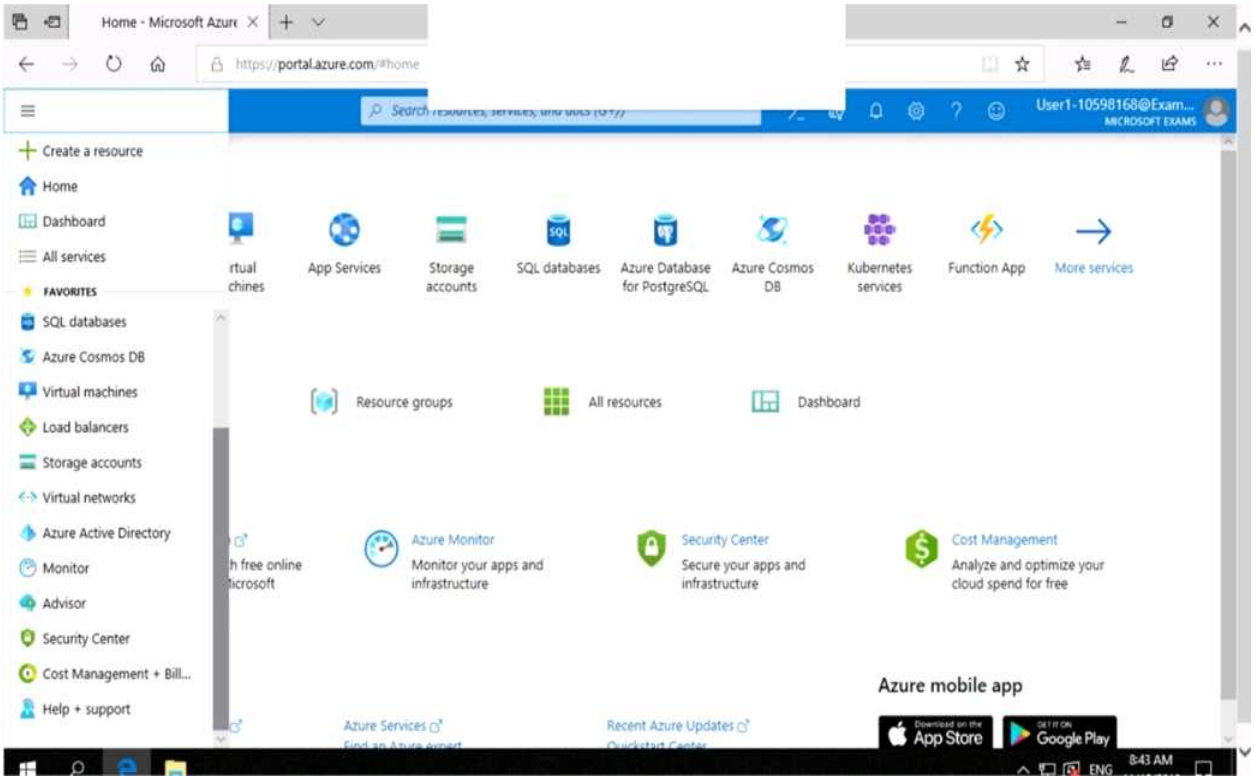
If you choose not to use a certificate, you can create a new application secret.
7 Select Certificates & secrets.
8. Select Client secrets -> New client secret.
9. Provide a description of the secret, and a duration. When done, select Add.
After saving the client secret, the value of the client secret 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: 128

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







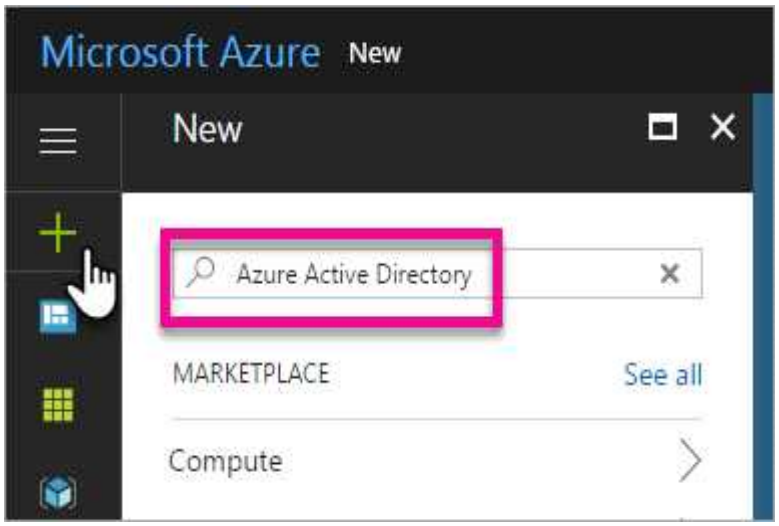
You need to create a new Azure Active Directory (Azure AD) directory named 10598168.onmicrosoft.com. The new directory must contain a user named user1@10598168.onmicrosoft.com who is configured to sign in by using Azure Multi-Factor Authentication (MFA).

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

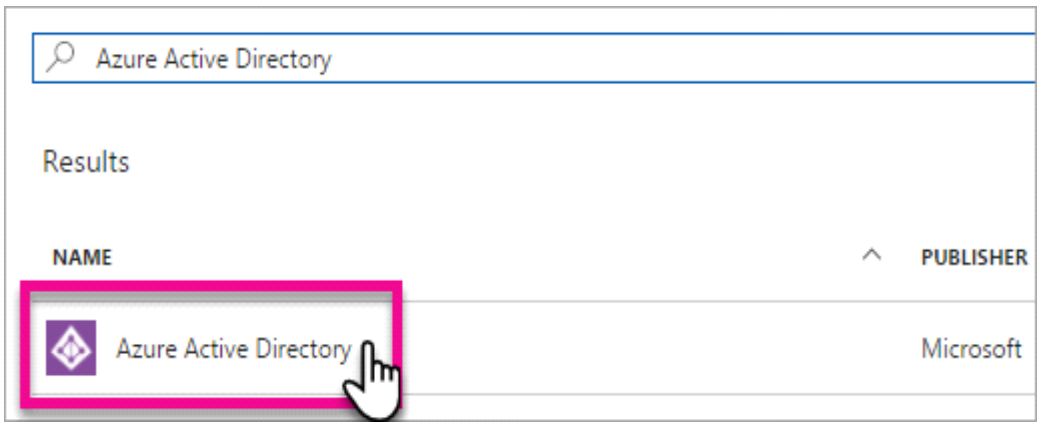
Answer:

Step 1: Create an Azure Active Directory tenant

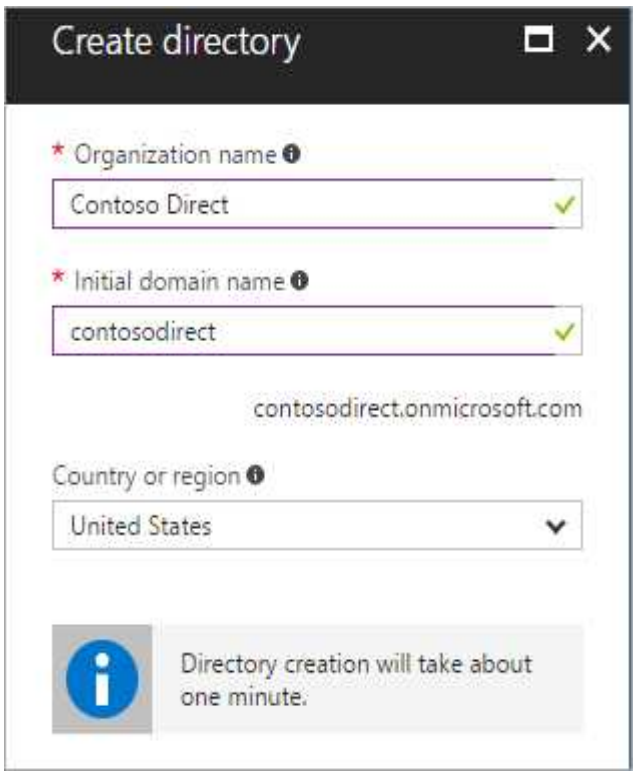
1. Browse to the Azure portal and sign in with an account that has an Azure subscription.
2. Select the plus icon (+) and search for Azure Active Directory.



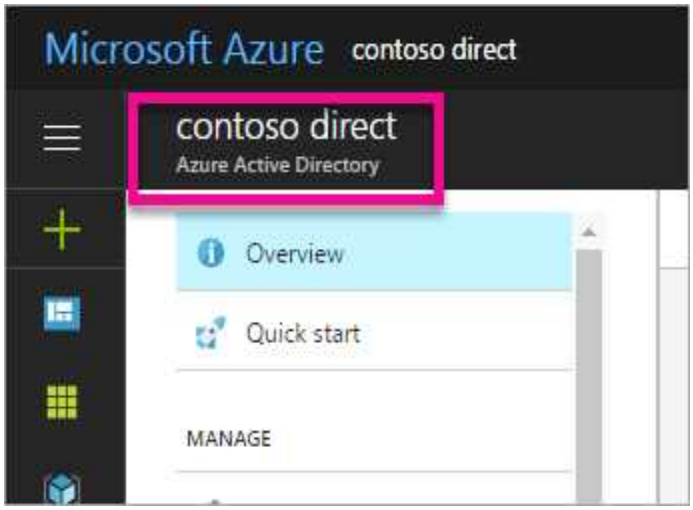
3. Select Azure Active Directory in the search results.



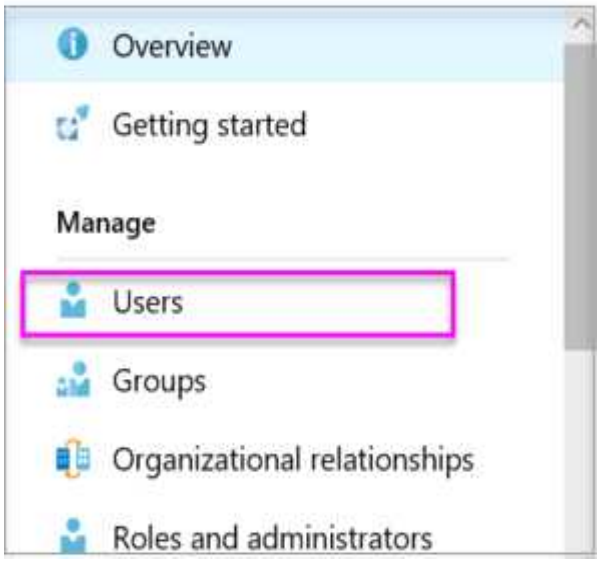
4. Select Create.
5. Provide an Organization name and an Initial domain name (10598168). Then select Create. Your directory is created.



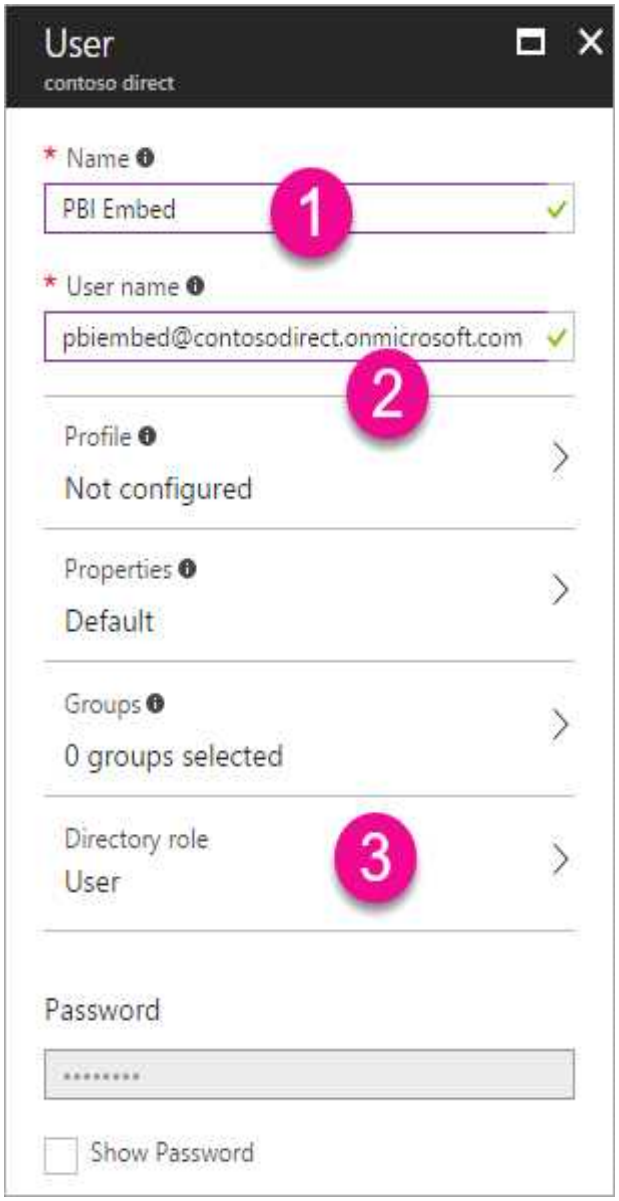
6. After directory creation is complete, select the information box to manage your new directory. Next, you're going to add tenant users.
Step 2: Create an Azure Active Directory tenant user
7. In the Azure portal, make sure you are on the Azure Active Directory fly out.



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@10598168.onmicrosoft.com



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

Question: 129

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
image2	Image was pushed with client content trust enabled.
image3	Image was pushed with client content trust disabled.

Which images are trusted images?

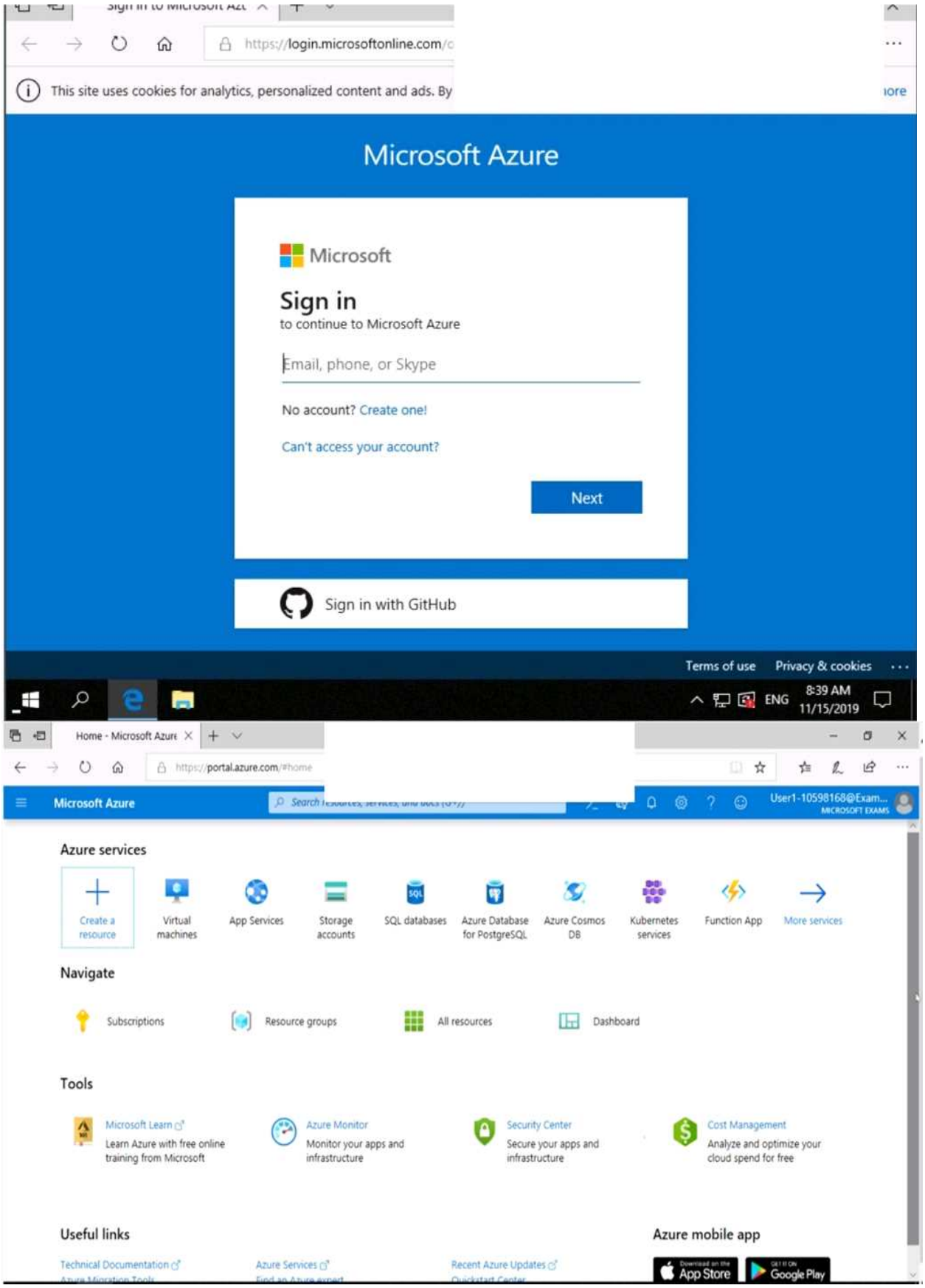
A. image1 and image2 only
B. image2 only
C. image1, image2, and image3

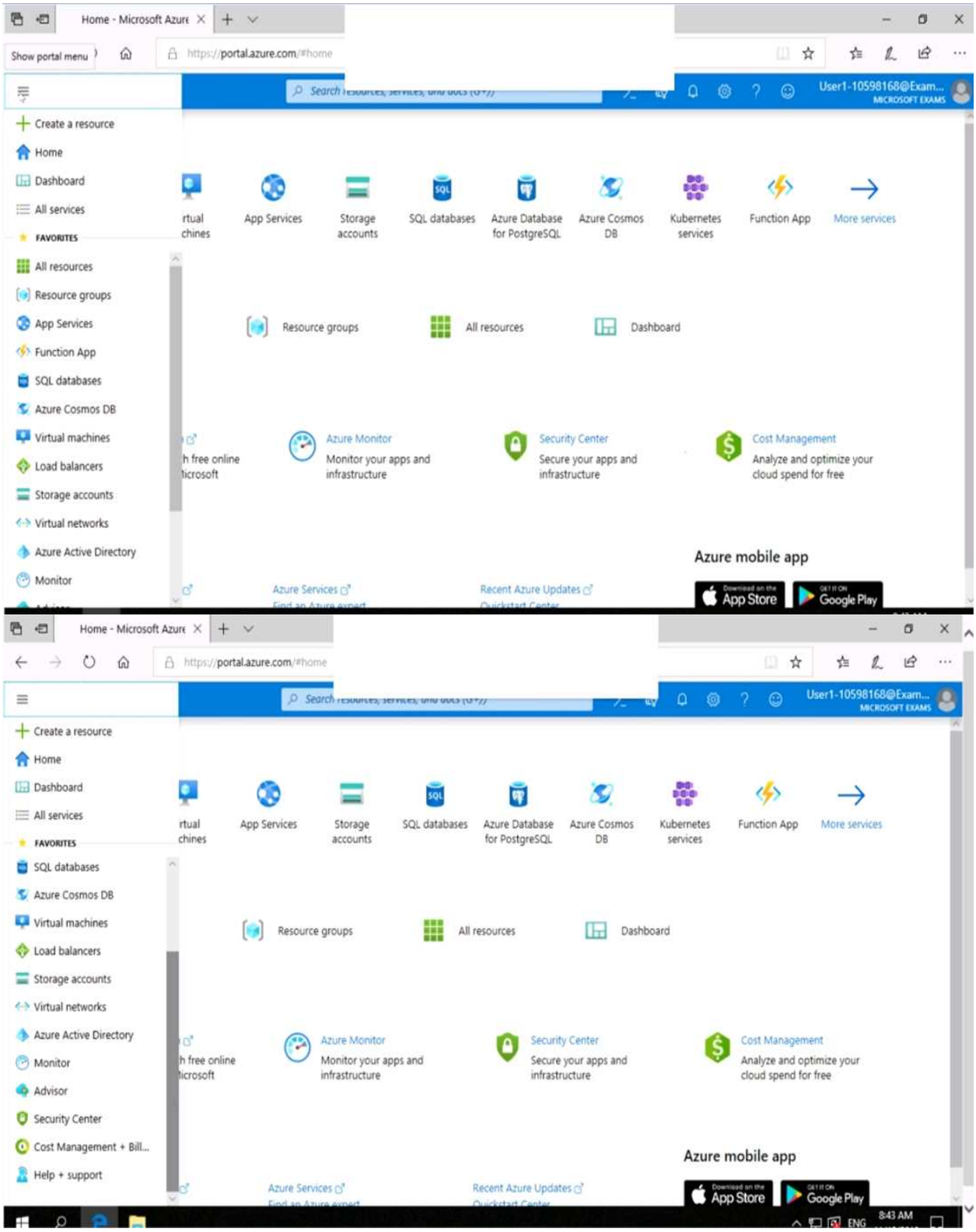
Answer: B

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: 130

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





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.

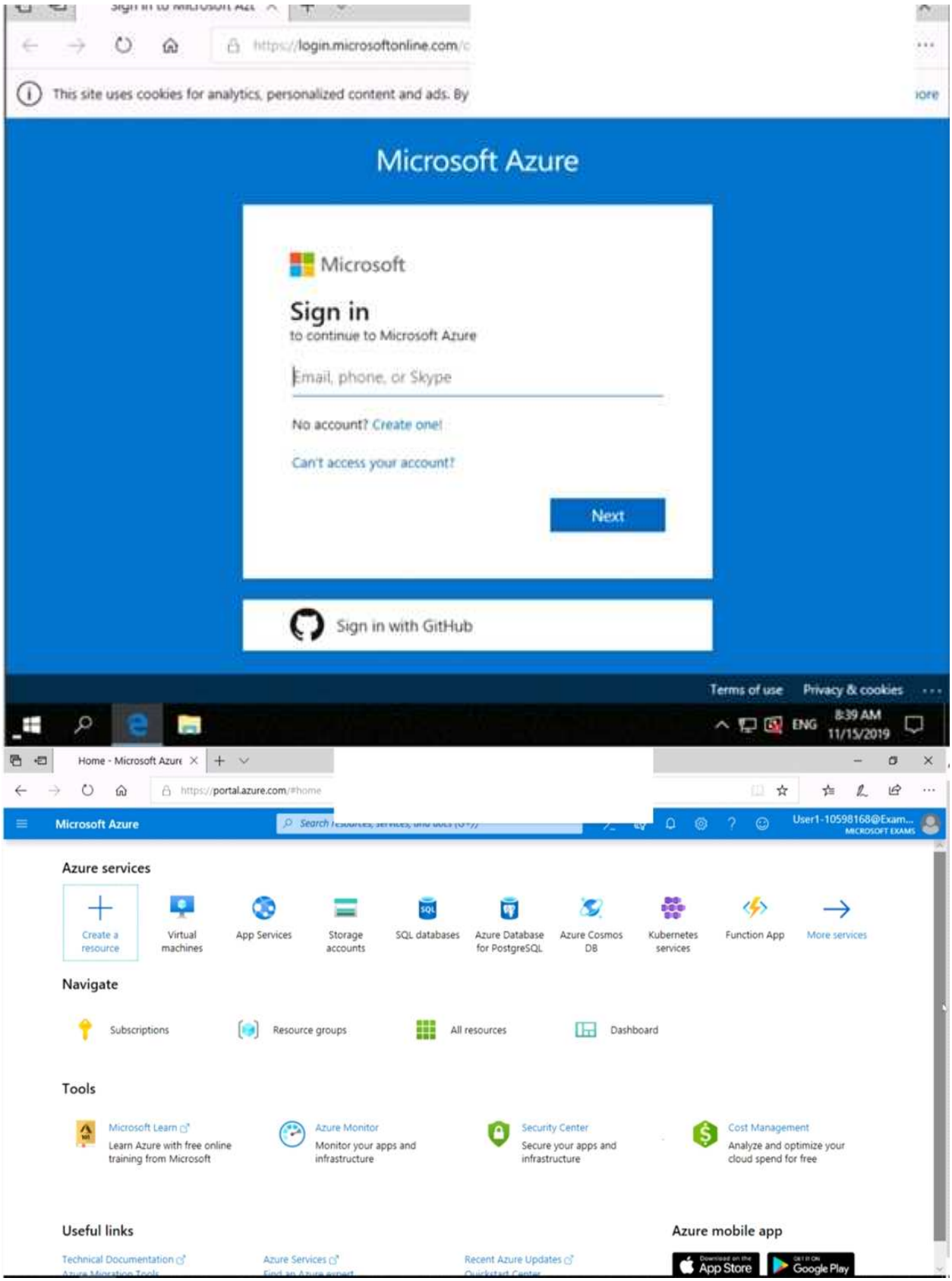
Answer:

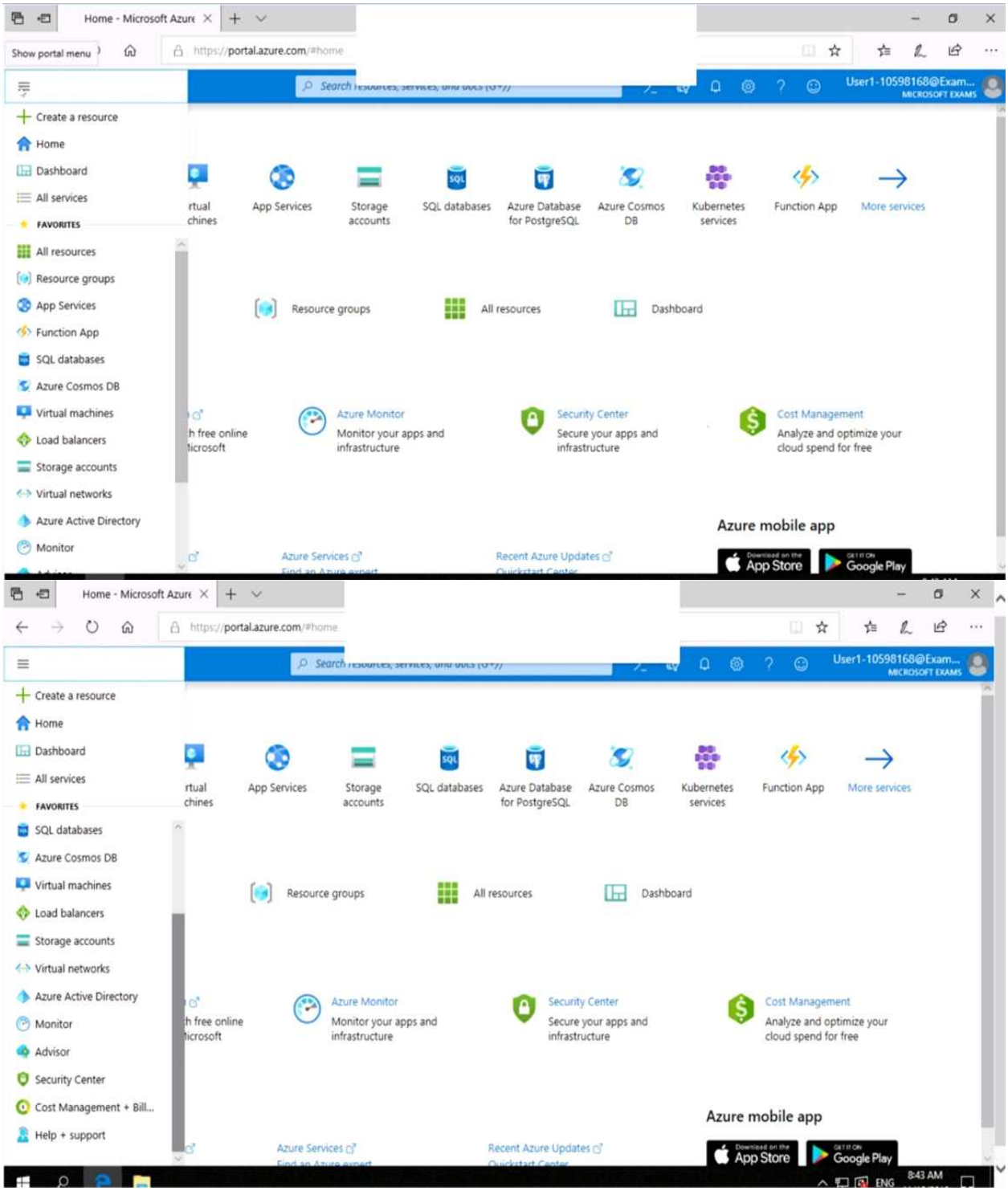
To enable the RDP port in an NSG, follow these steps:
• Sign in to the Azure portal.

• In Virtual Machines, select VM1
• In Settings, select Networking.
• 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: 131

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





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.

Answer:

• 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.

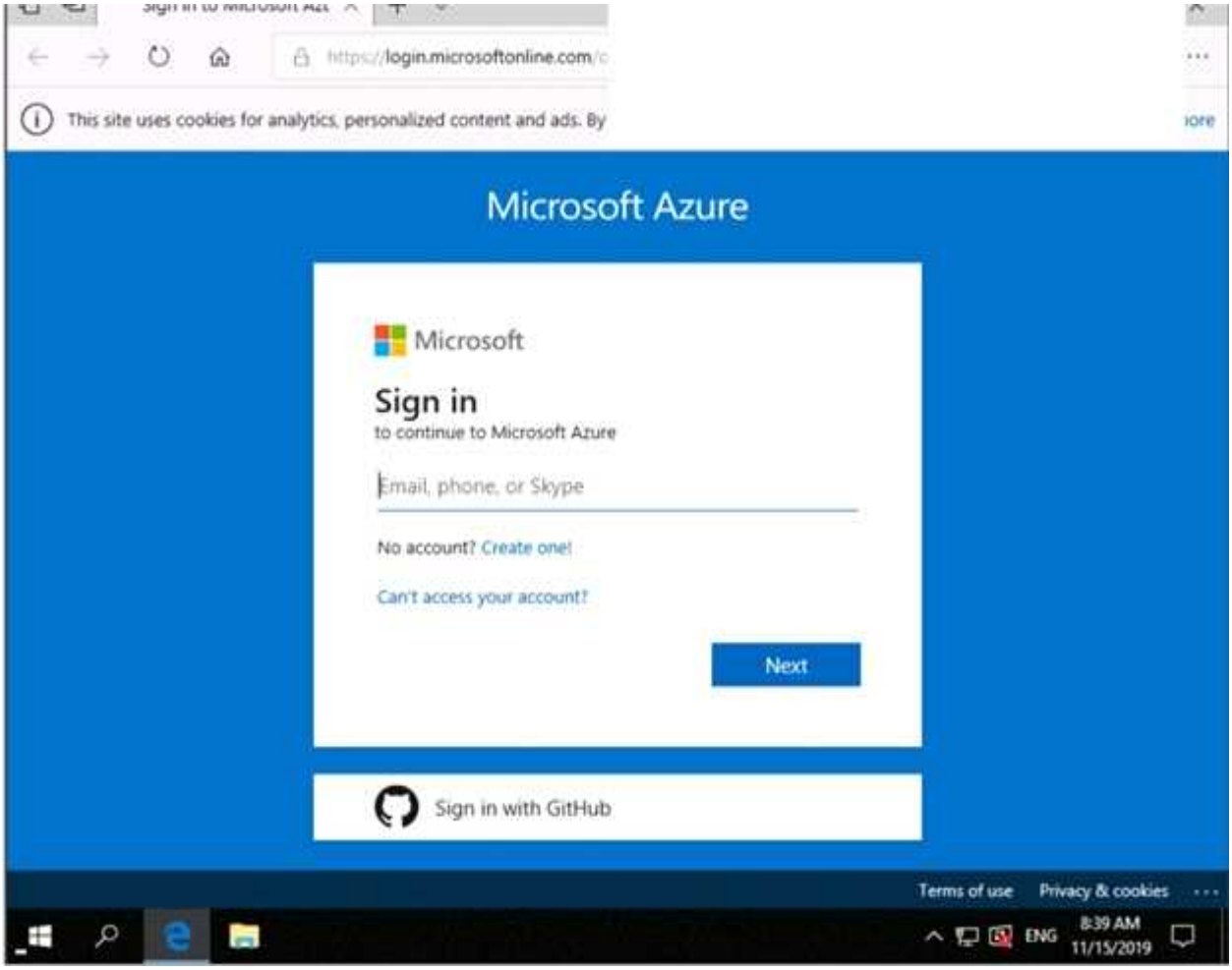
• When the name of your VM appears in the search results, select it.

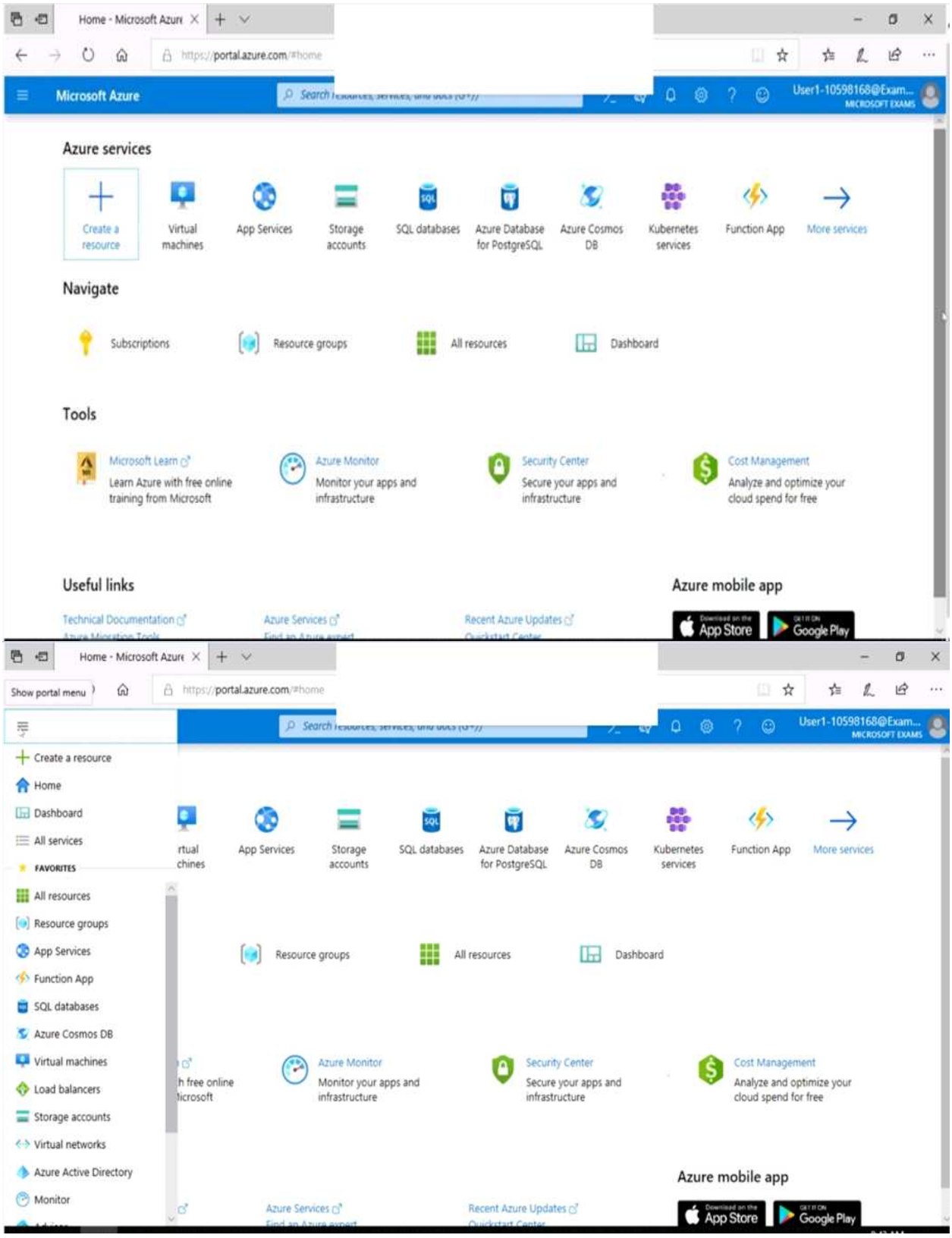
• Under SETTINGS, select Networking. Select Configure the application security groups, select the

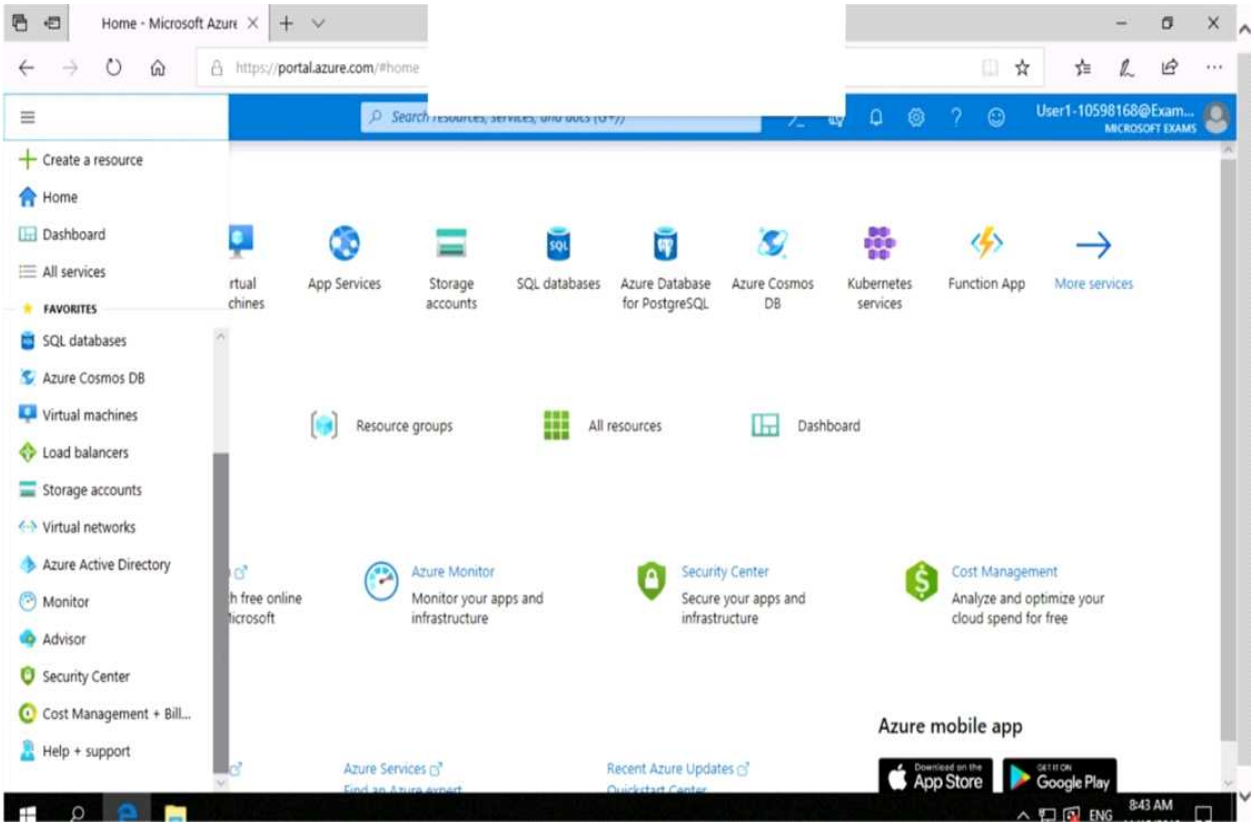
application security groups that you want to add the network interface to, or unselect the application security groups that you want to remove the network interface from, and then select Save.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface

Question: 132

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



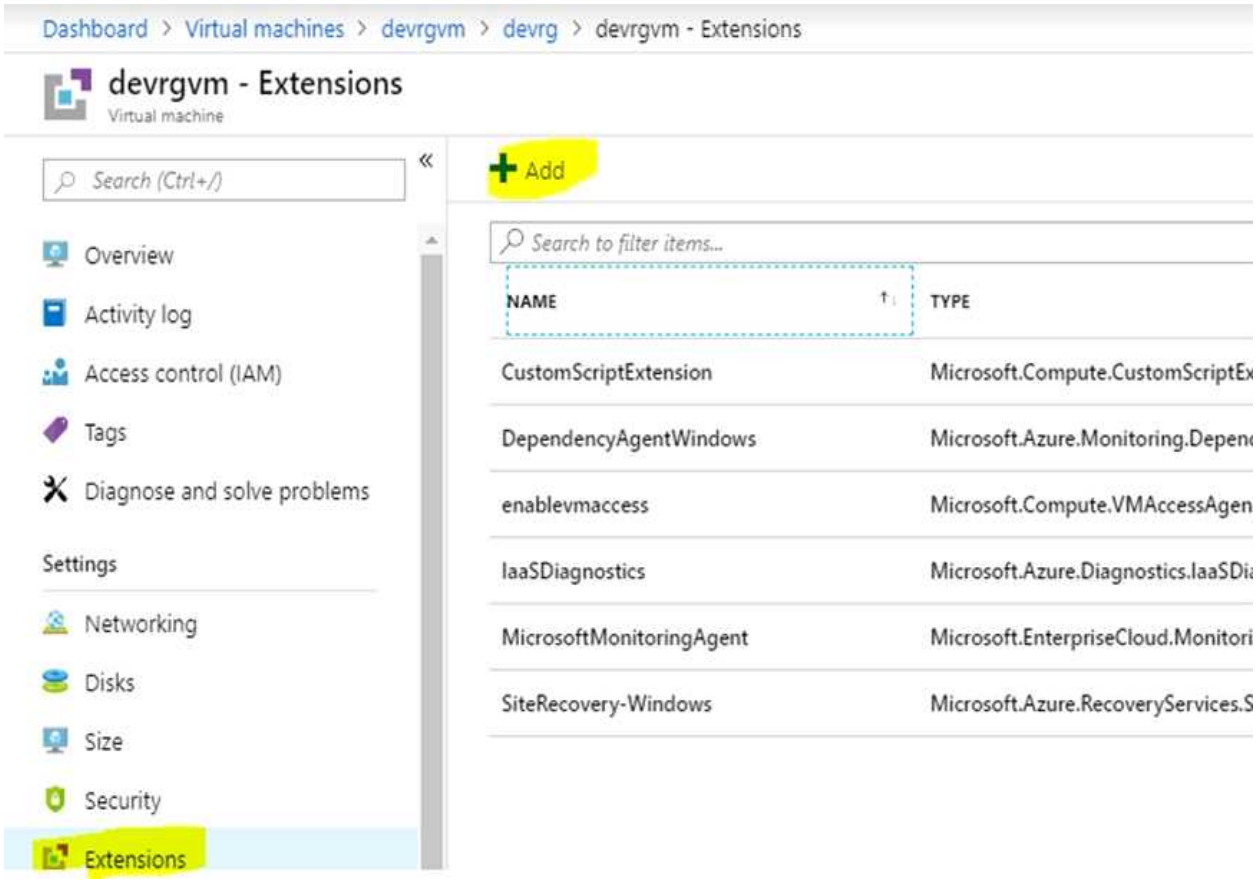




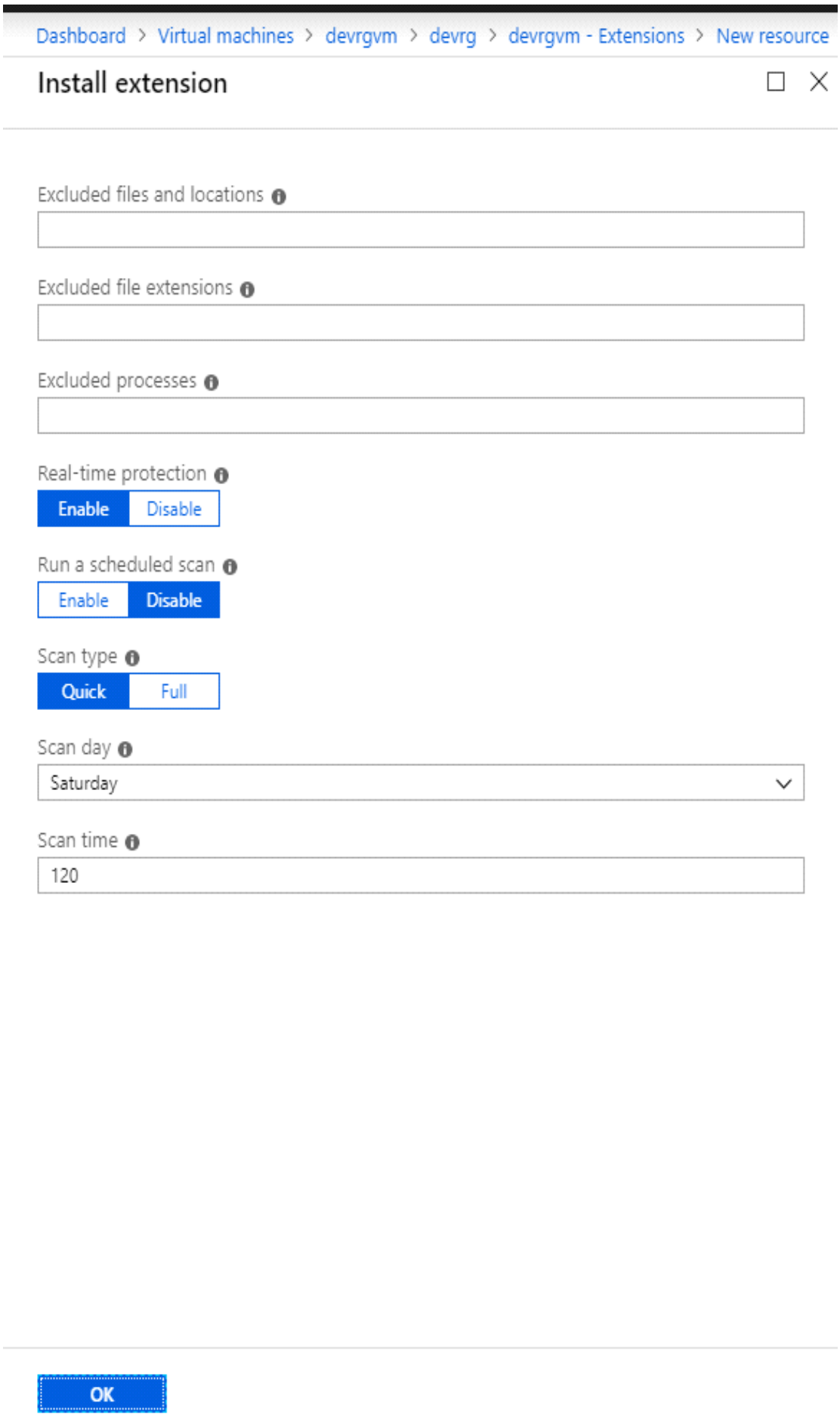
You need to perform a full malware scan every Sunday at 02:00 on a virtual machine named VM1 by using Microsoft Antimalware for Virtual Machines.
To complete this task, sign in to the Azure portal.

Answer:

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.



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



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

Question: 133

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.

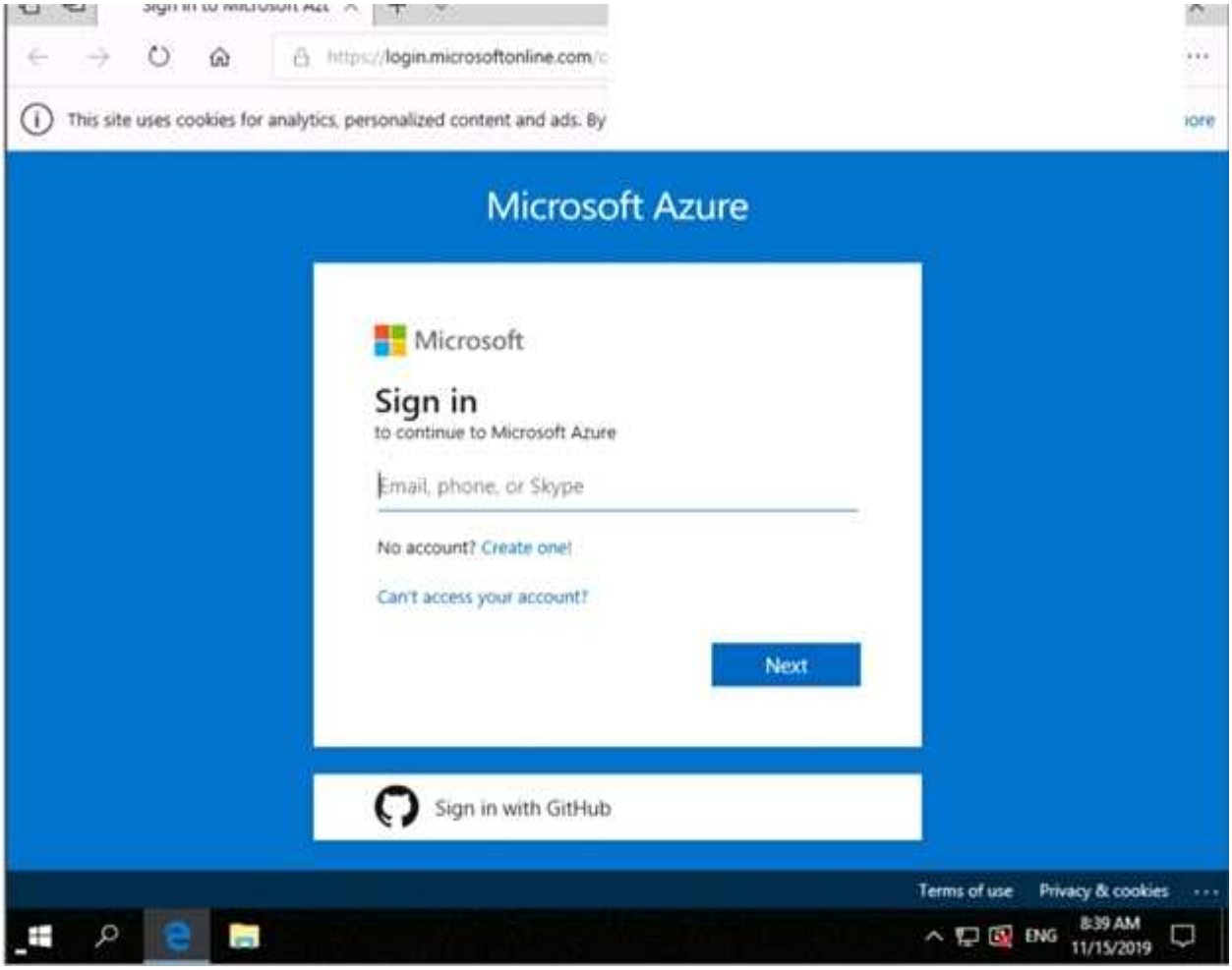
To enter your password, place your cursor in the Enter password box and click on the password below.

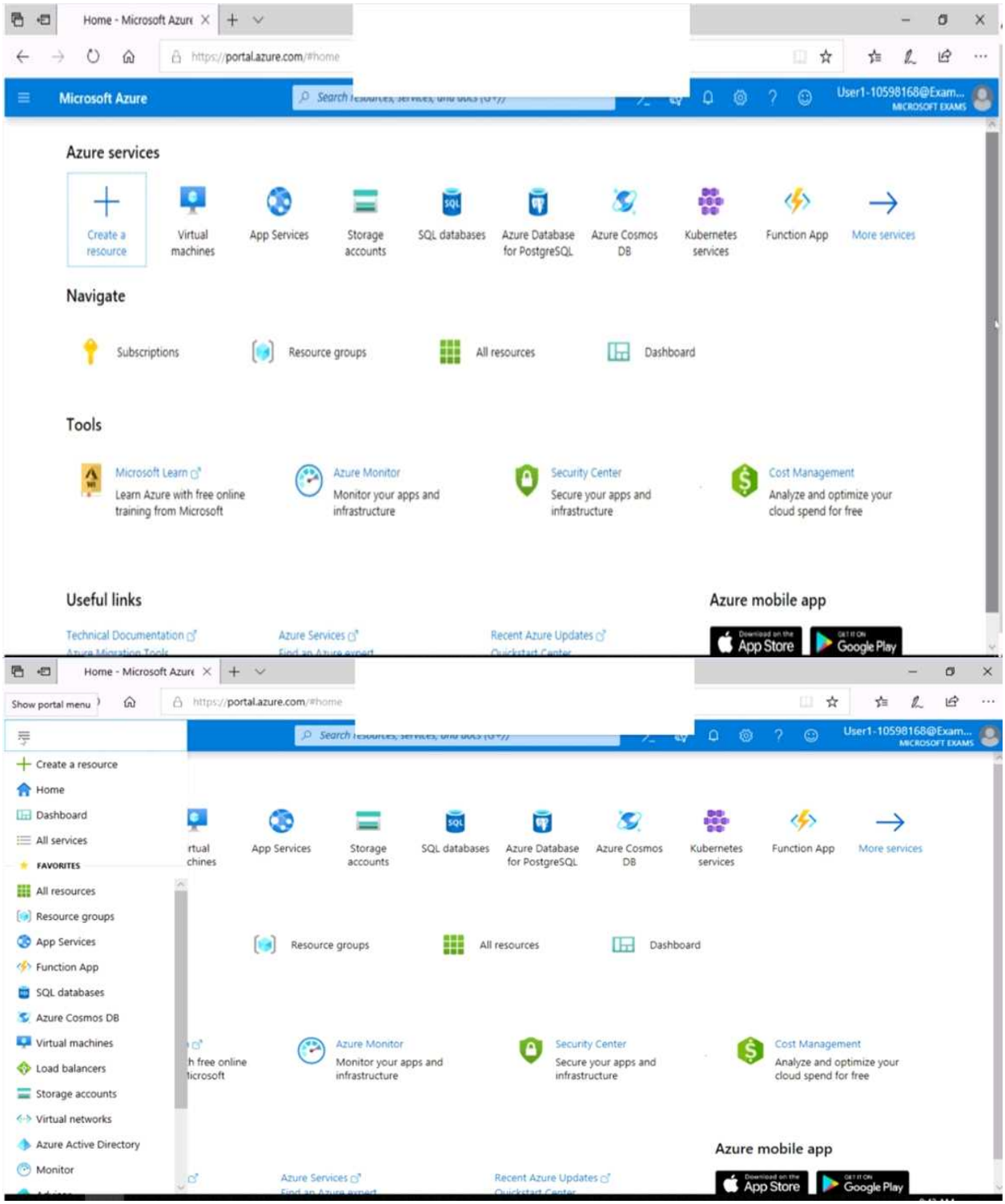
Azure Username: User1-10598168@ExamUsers.com

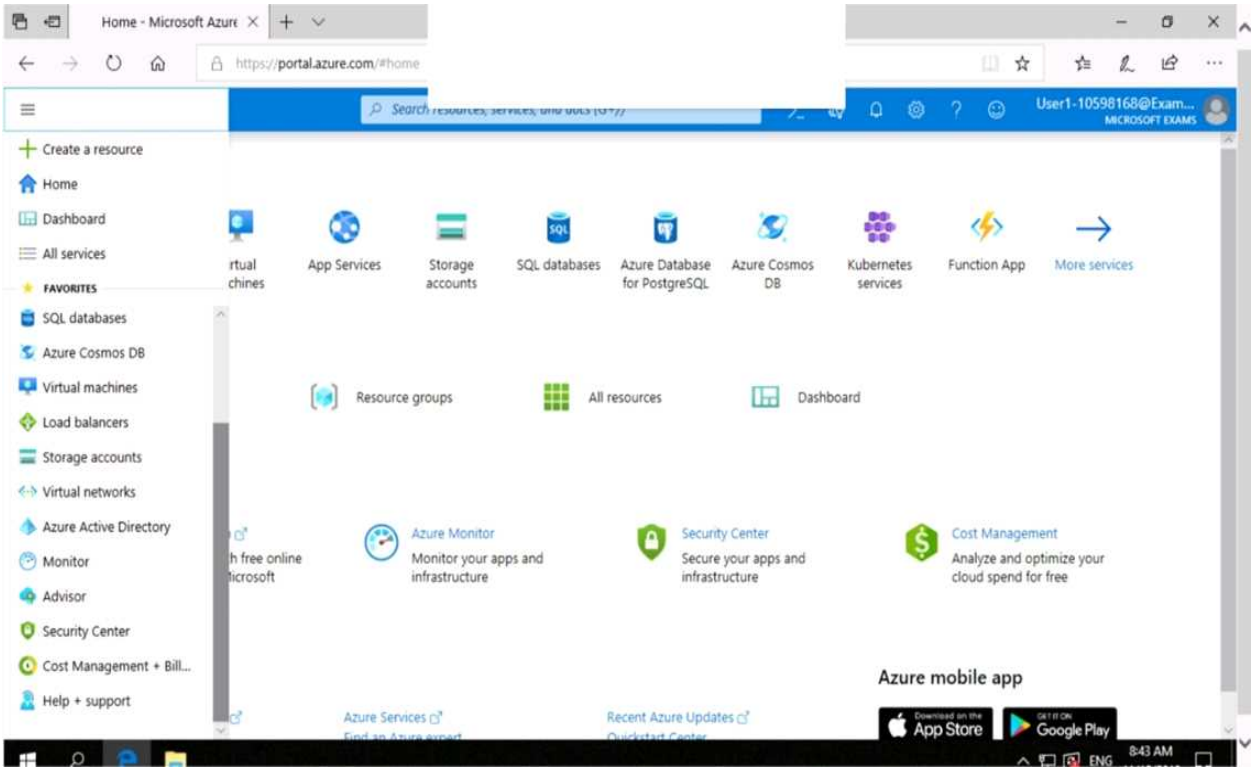
Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168



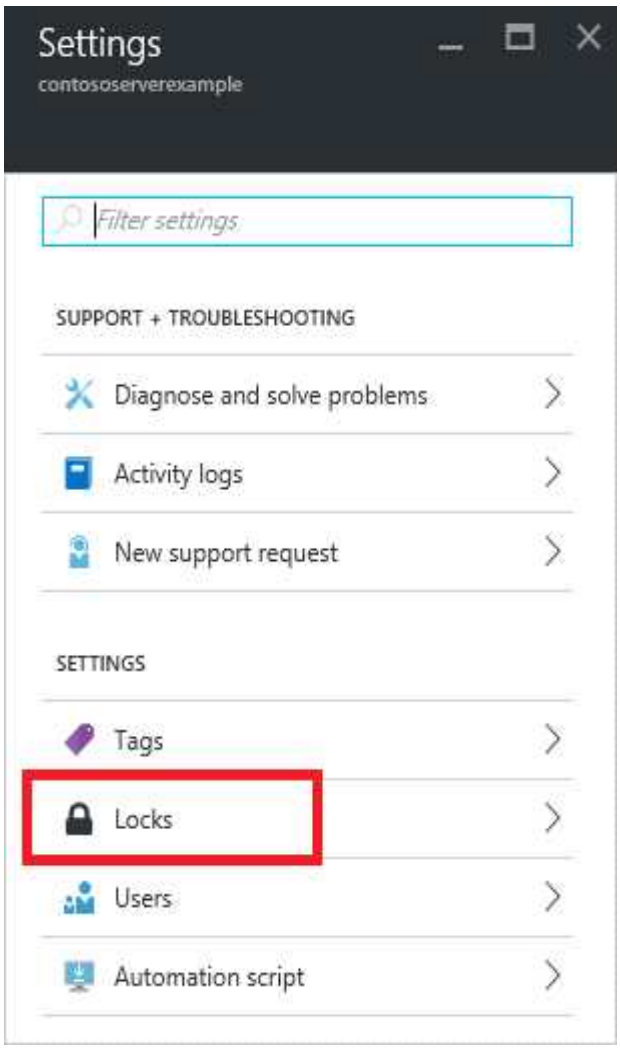




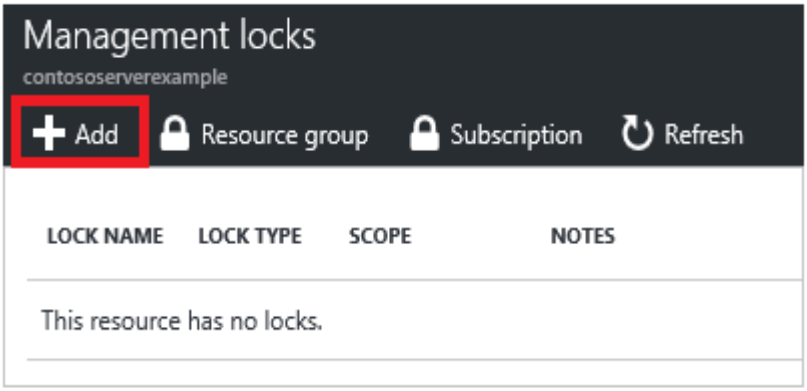
You need to prevent administrative users from accidentally deleting a virtual network named VNET1. The administrative users must be allowed to modify the settings of VNET1.
To complete this task, sign in to the Azure portal.

Answer:

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: 134

SIMULATION

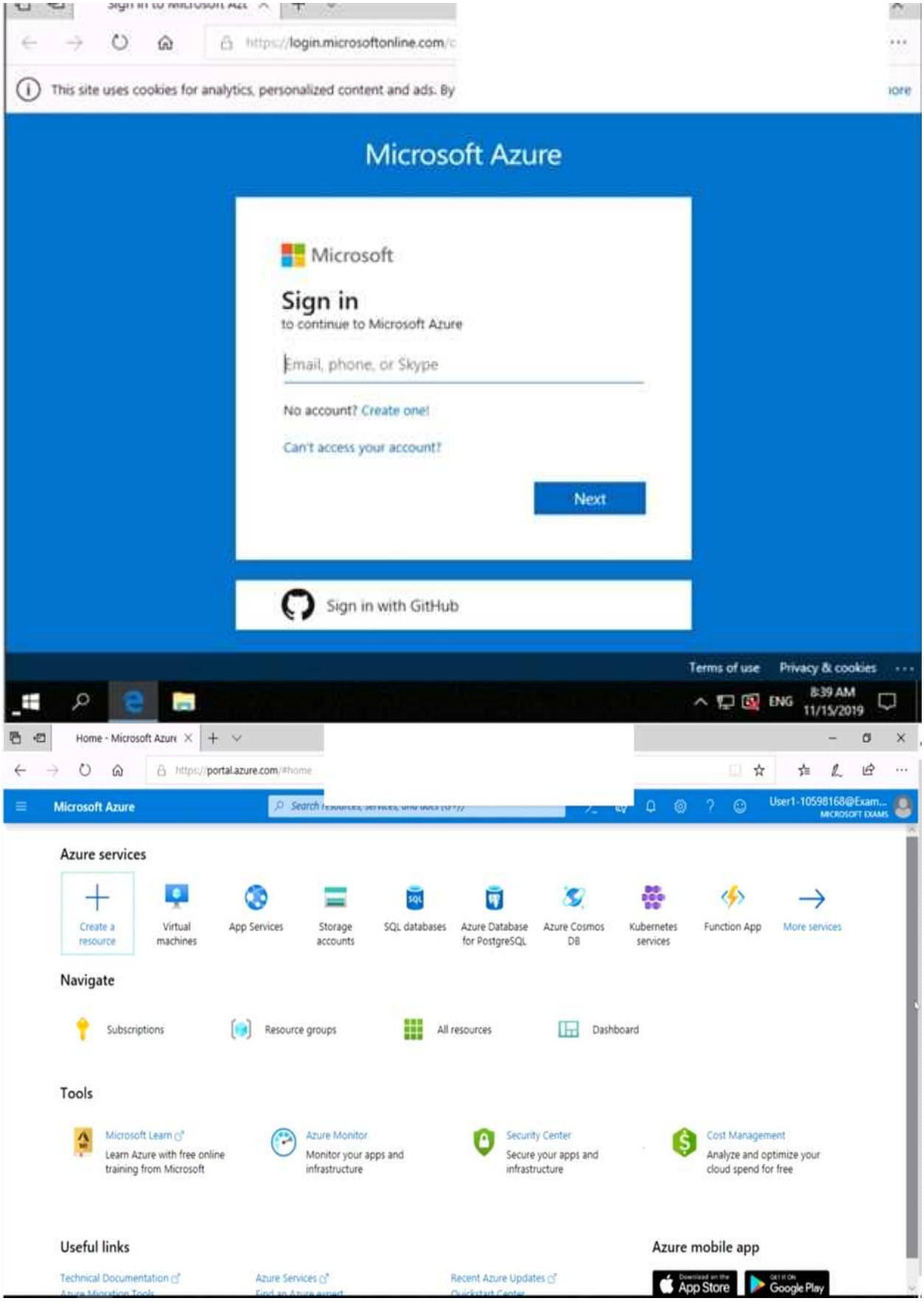
Use the following login credentials as needed:

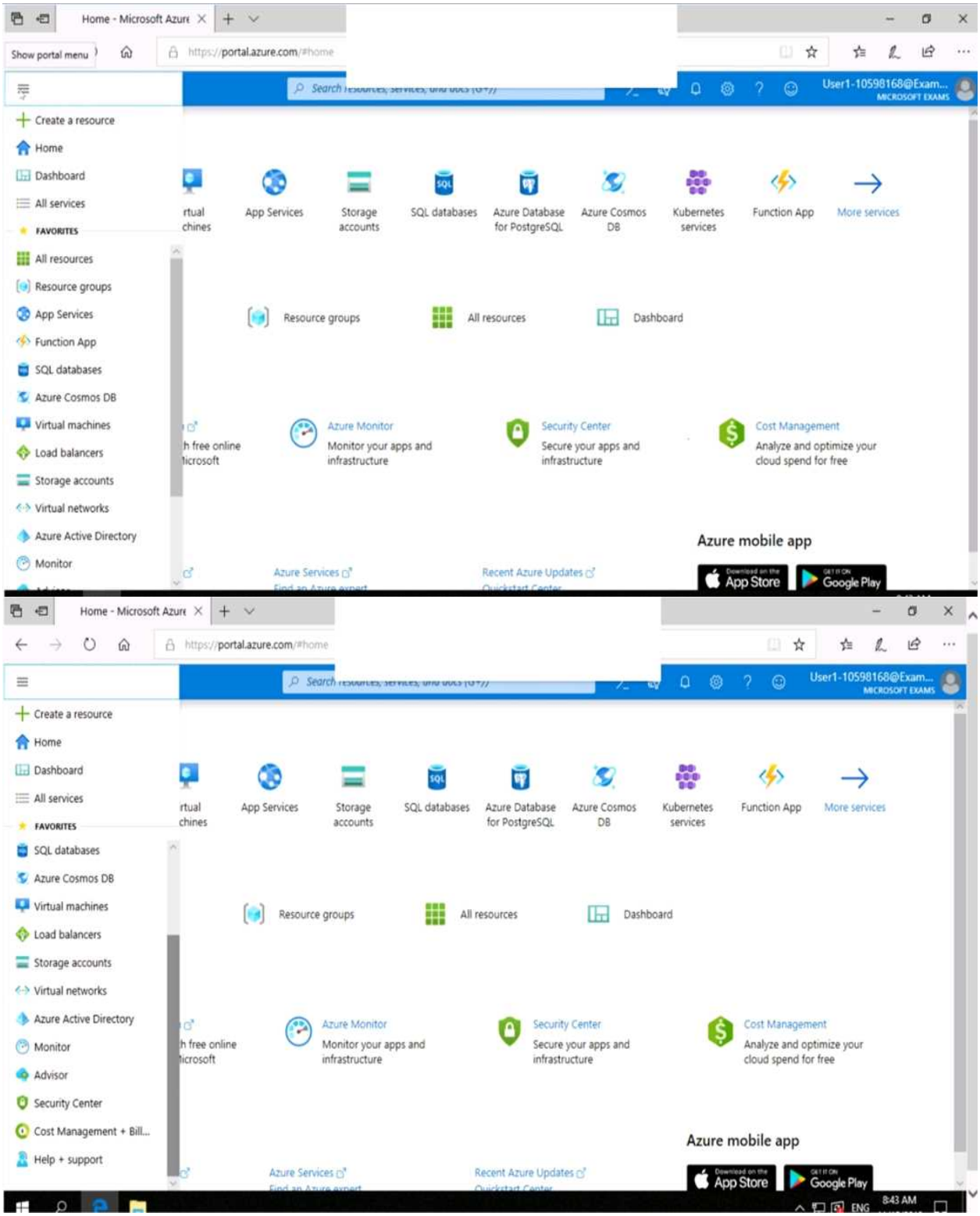
To enter your username, place your cursor in the Sign in box and click on the username below.

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





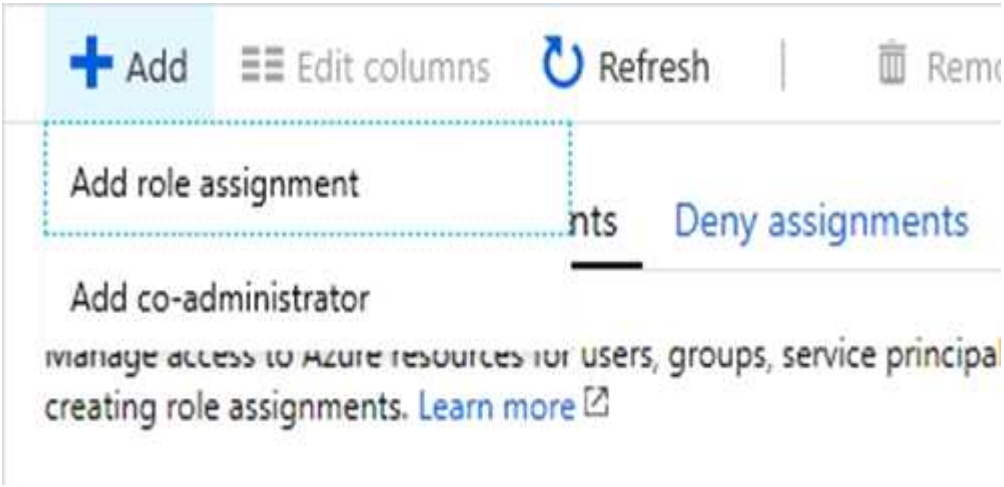
You need to ensure that a user named user21059868 can manage the properties of the virtual machines in the RG1lod10598168 resource group. The solution must use the principle of least privilege.

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

Answer:

1. In Azure portal, locate and select the RG1lod10598168 resource group.
2. Click Access control (IAM).

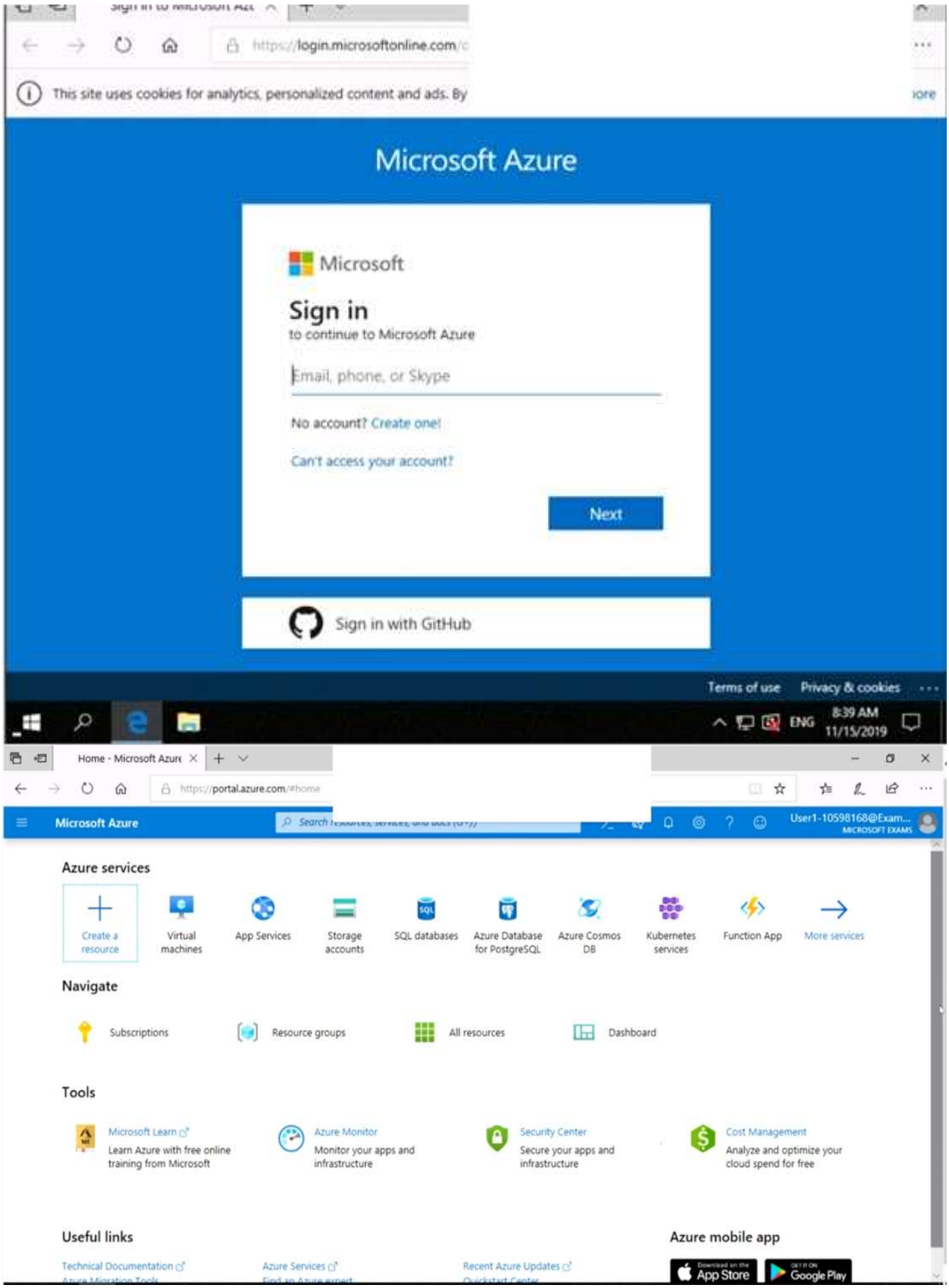
3. Click the Role assignments tab to view all the role assignments at this scope.
4. Click Add > Add role assignment to open the Add role assignment pane.

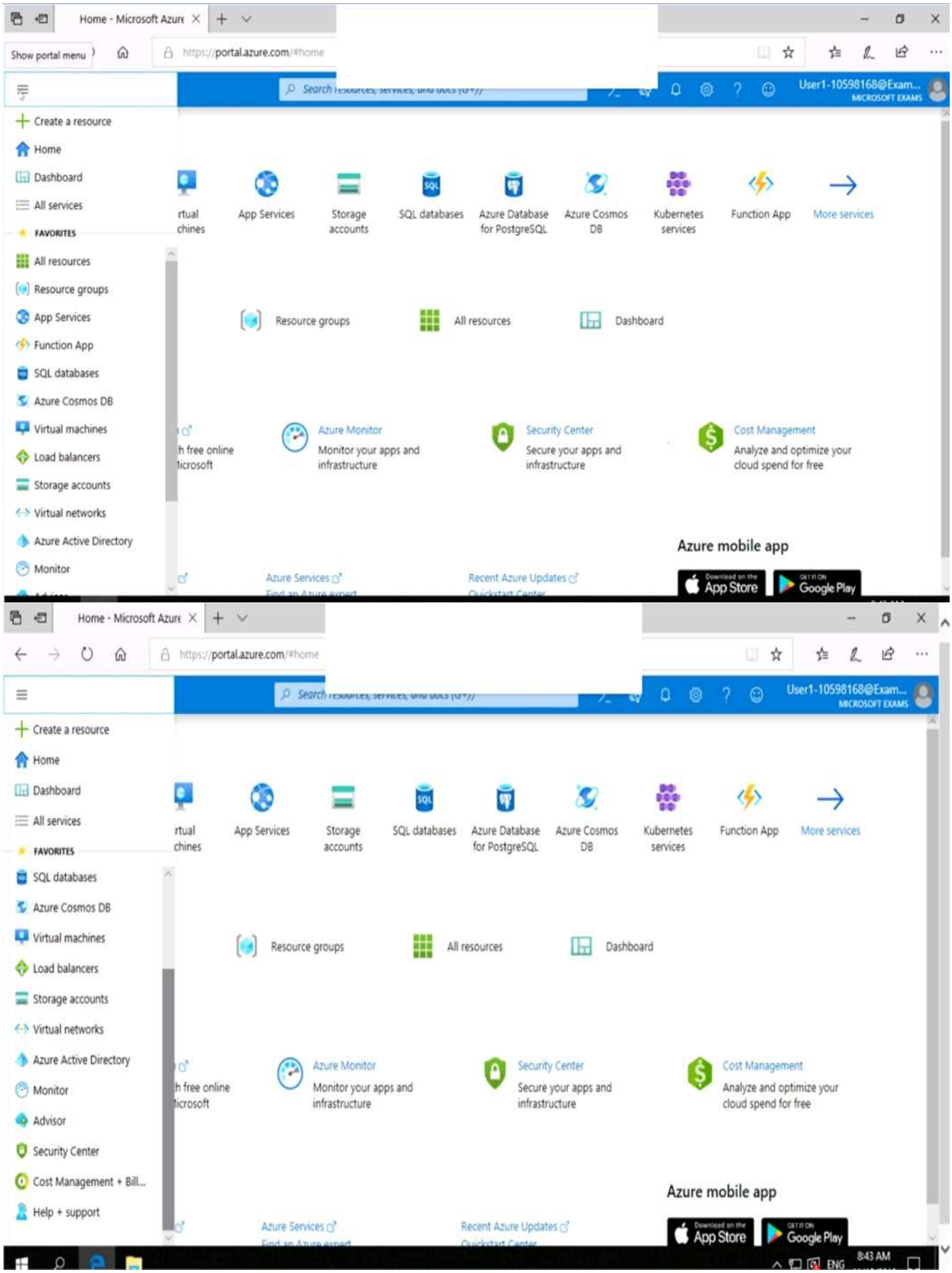


5. In the Role drop-down list, select the role Virtual Machine Contributor. Virtual Machine Contributor lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.
6. In the Select list, select user user21059868
7. Click Save to assign 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: 135

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
Home - Microsoft Azure
https://portal.azure.com/#home
Microsoft Azure
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 Services
Recent Azure Updates
Azure mobile app
App Store
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.

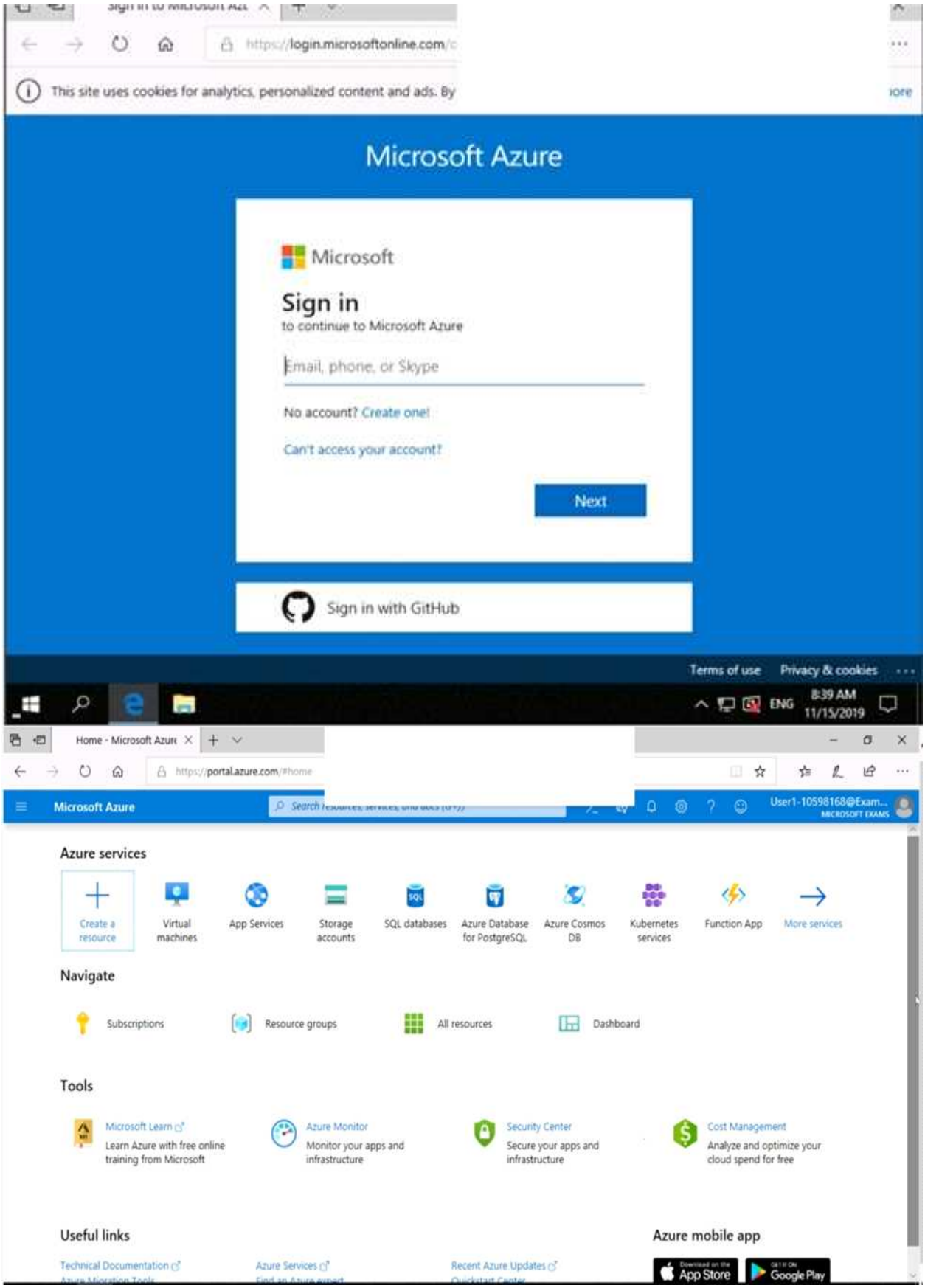
To complete this task, sign in to the Azure portal.

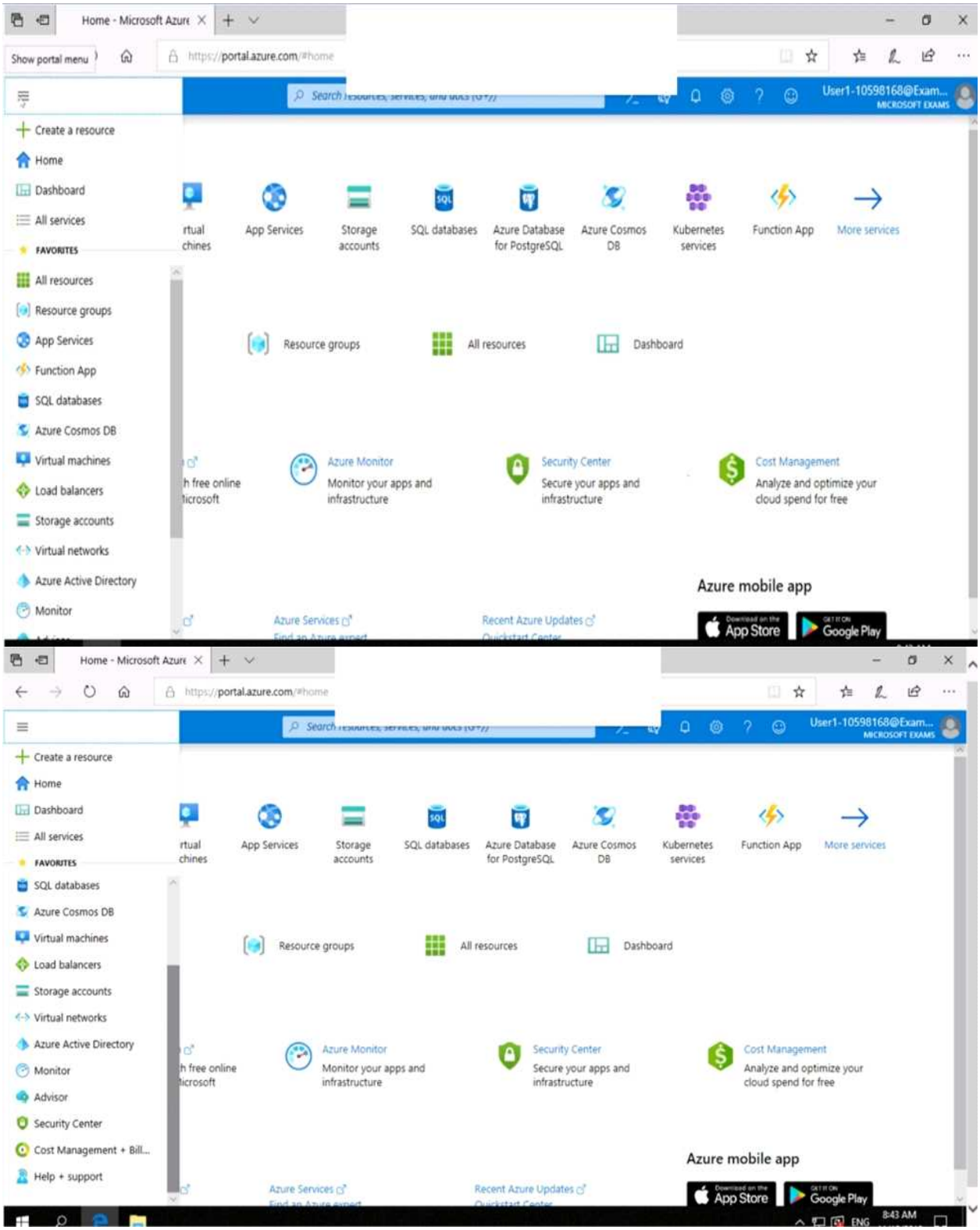
Answer:

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: 136

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





You need to email an alert to a user named admin1@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes.
To complete this task, sign in to the Azure portal.

Answer:

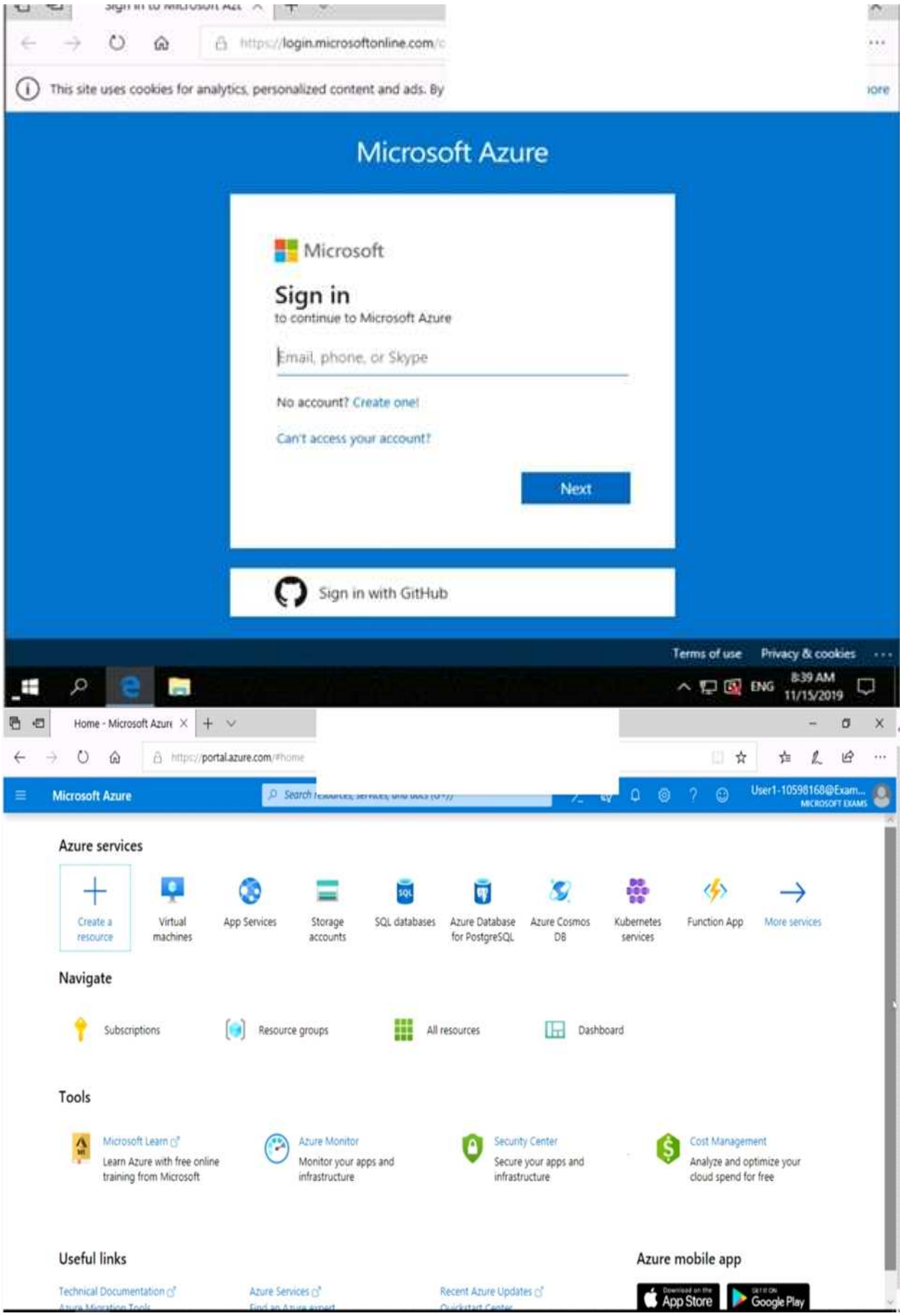
Create an alert rule on a metric with the Azure portal
1. In the portal, locate the resource, here VM1, you are interested in monitoring and select it.

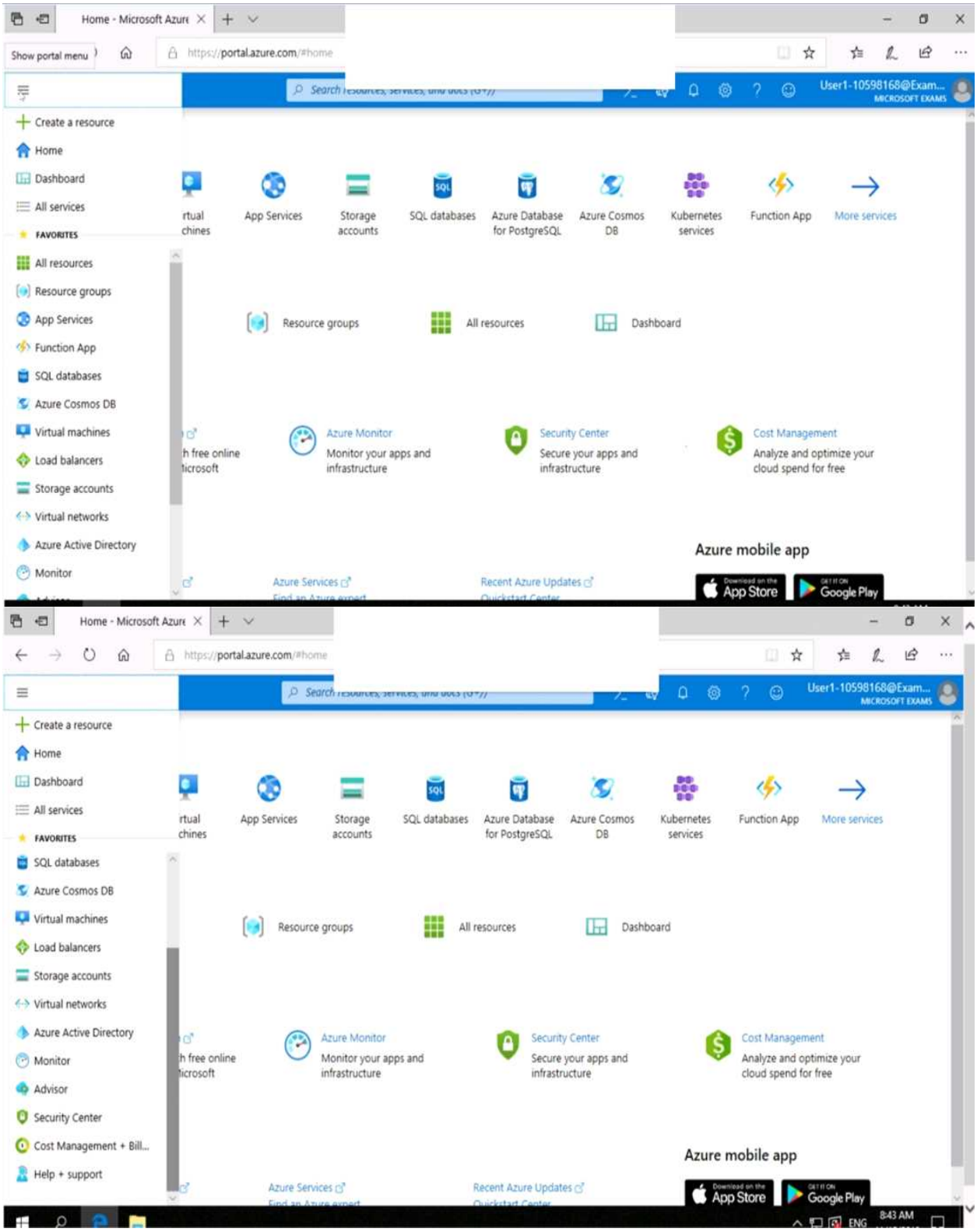
2. Select Alerts (Classic) under the MONITORING section. The text and icon may vary slightly for different resources.
3. Select the Add metric alert (classic) button and fill in the fields as per below, and click OK.
Metric: CPU Percentage
Condition: Greater than
Period: Over last 15 minutes
Notify via: email
Additional administrator email(s): admin1@contoso.com

Reference:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-insights-alerts-portal

Question: 137

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





You need to collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account.

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

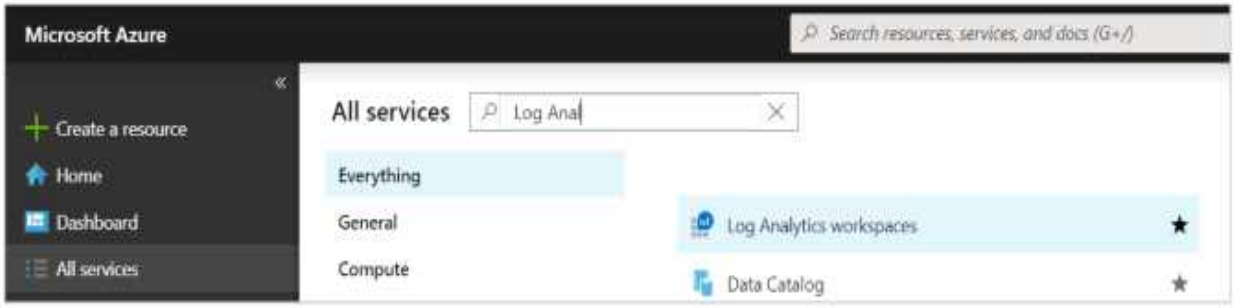
This task might take several minutes to complete You can perform other tasks while the task completes.

Answer:

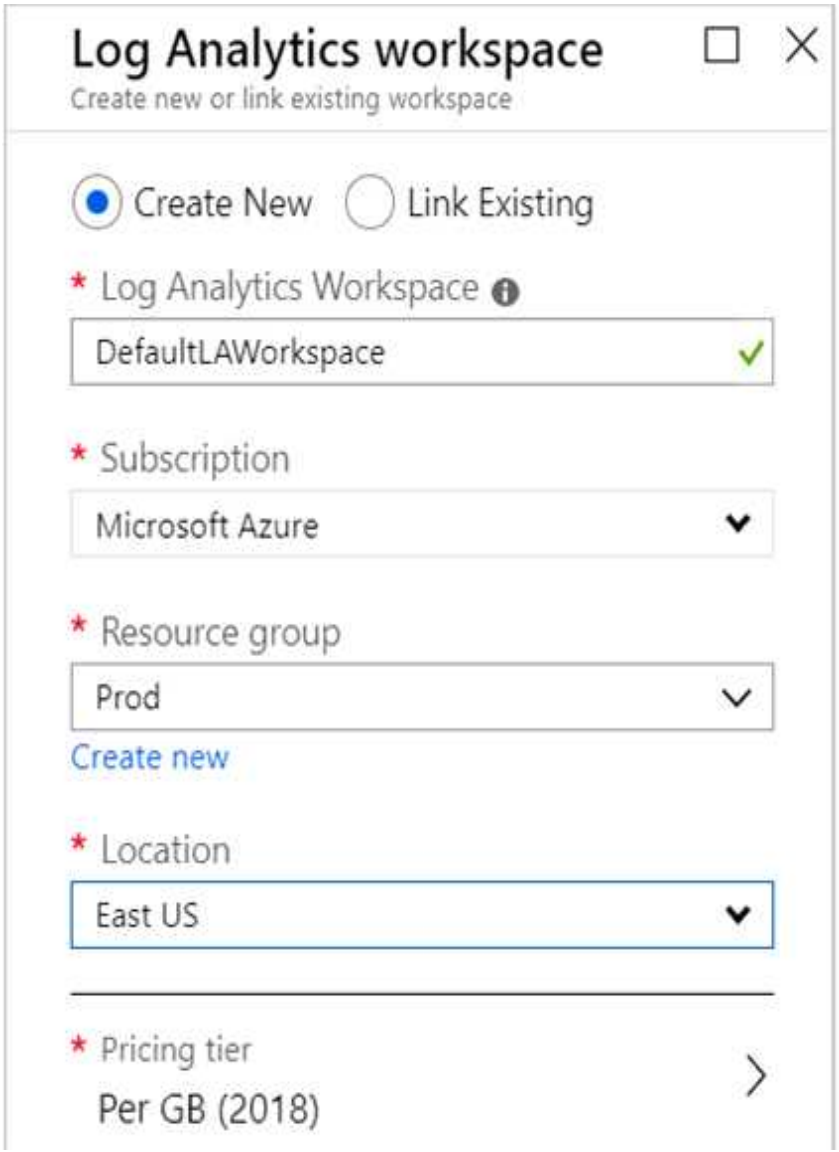
Step 1: Create a workspace

Azure Monitor can collect data directly from your Azure virtual machines into a Log Analytics workspace for detailed analysis and correlation.

1. In the Azure portal, select All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics workspaces.



2. Select Create, and then select choices for the following items:



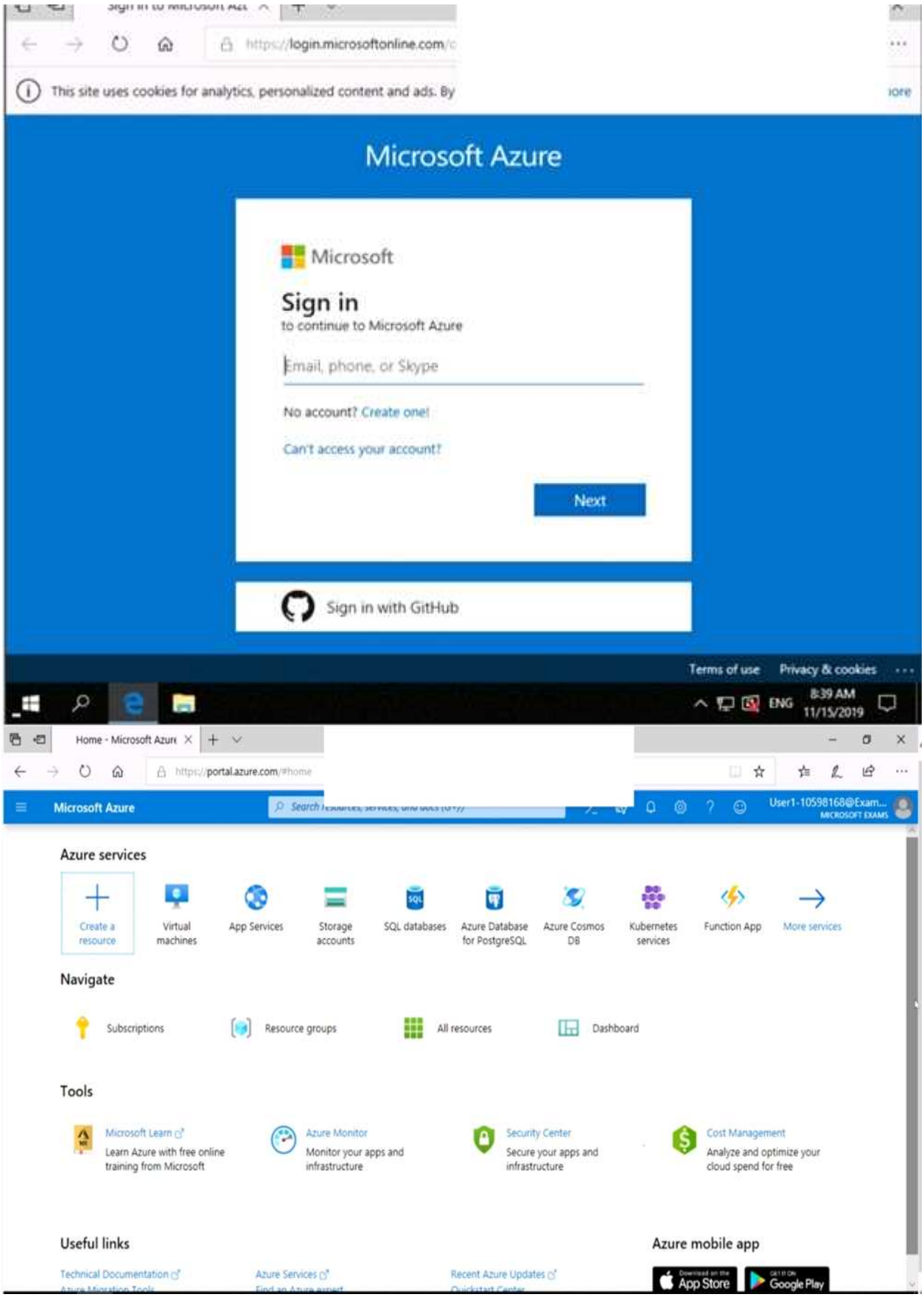
3. After providing the required information on the Log Analytics workspace pane, select OK.

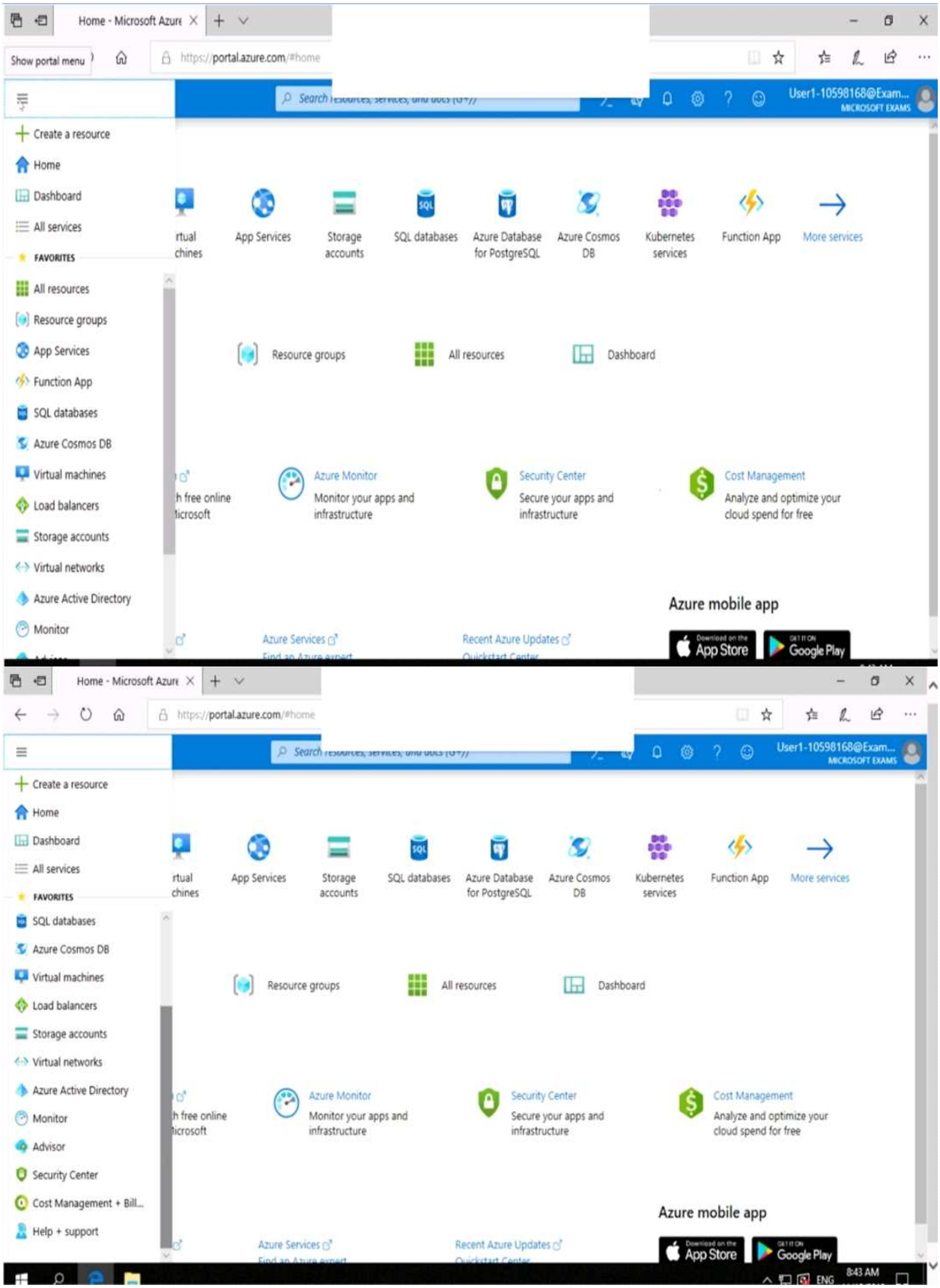
While the information is verified and the workspace is created, you can track its progress under Notifications from the menu.

Step 2: Enable the Log Analytics VM Extension
Installing the Log Analytics VM extension for Windows and Linux allows Azure Monitor to collect data from your Azure VMs.
1. In the Azure portal, select All services found in the upper left-hand corner. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics workspaces.
2. In your list of Log Analytics workspaces, select DefaultWorkspace (the name you created in step 1).
3. On the left-hand menu, under Workspace Data Sources, select Virtual machines.
4. In the list of Virtual machines, select a virtual machine you want to install the agent on. Notice that the Log Analytics connection status for the VM indicates that it is Not connected.
5. In the details for your virtual machine, select Connect. The agent is automatically installed and configured for your Log Analytics workspace. This process takes a few minutes, during which time the Status shows Connecting.
After you install and connect the agent, the Log Analytics connection status will be updated with This workspace.
Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm

Question: 138

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



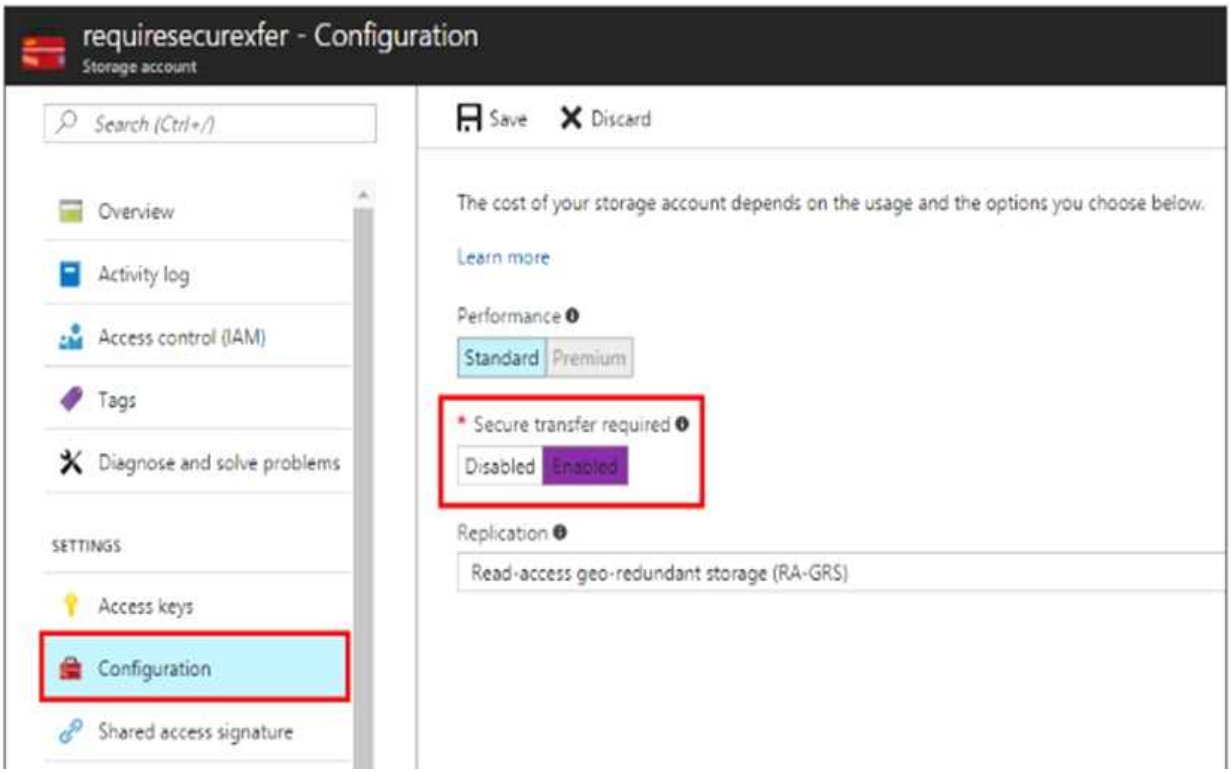


You need to prevent HTTP connections to the rg1lod10598168n1 Azure Storage account.
To complete this task, sign in to the Azure portal.

Answer:

The "Secure transfer required" feature is now supported in Azure Storage account. This feature enhances the security of your storage account by enforcing all requests to your account through a secure connection. This feature is disabled by default.

1. In Azure Portal select you Azure Storage account rg1lod10598168n1.
2. Select Configuration, and Secure Transfer required.



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

Question: 139

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.

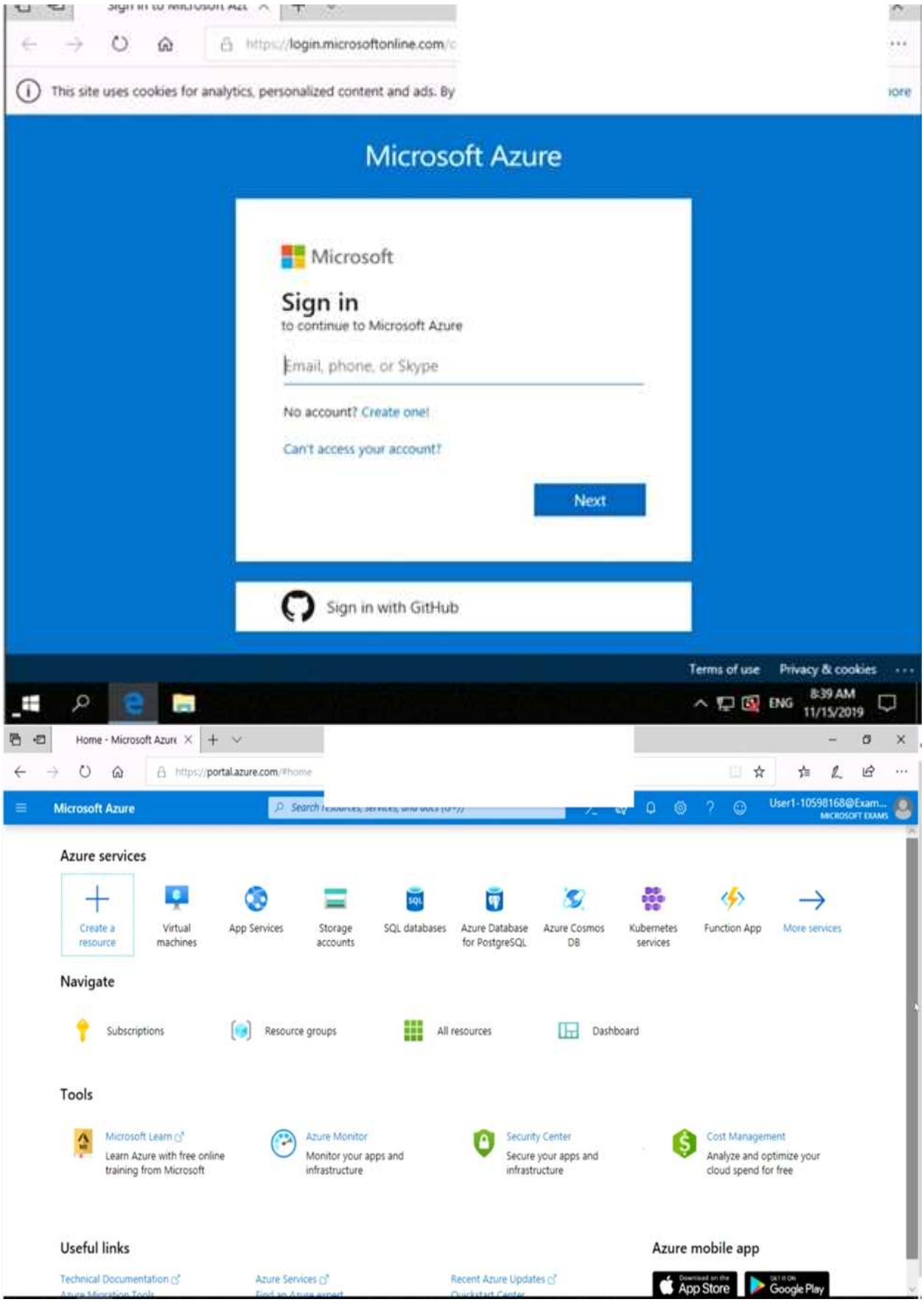
To enter your password, place your cursor in the Enter password box and click on the password below.

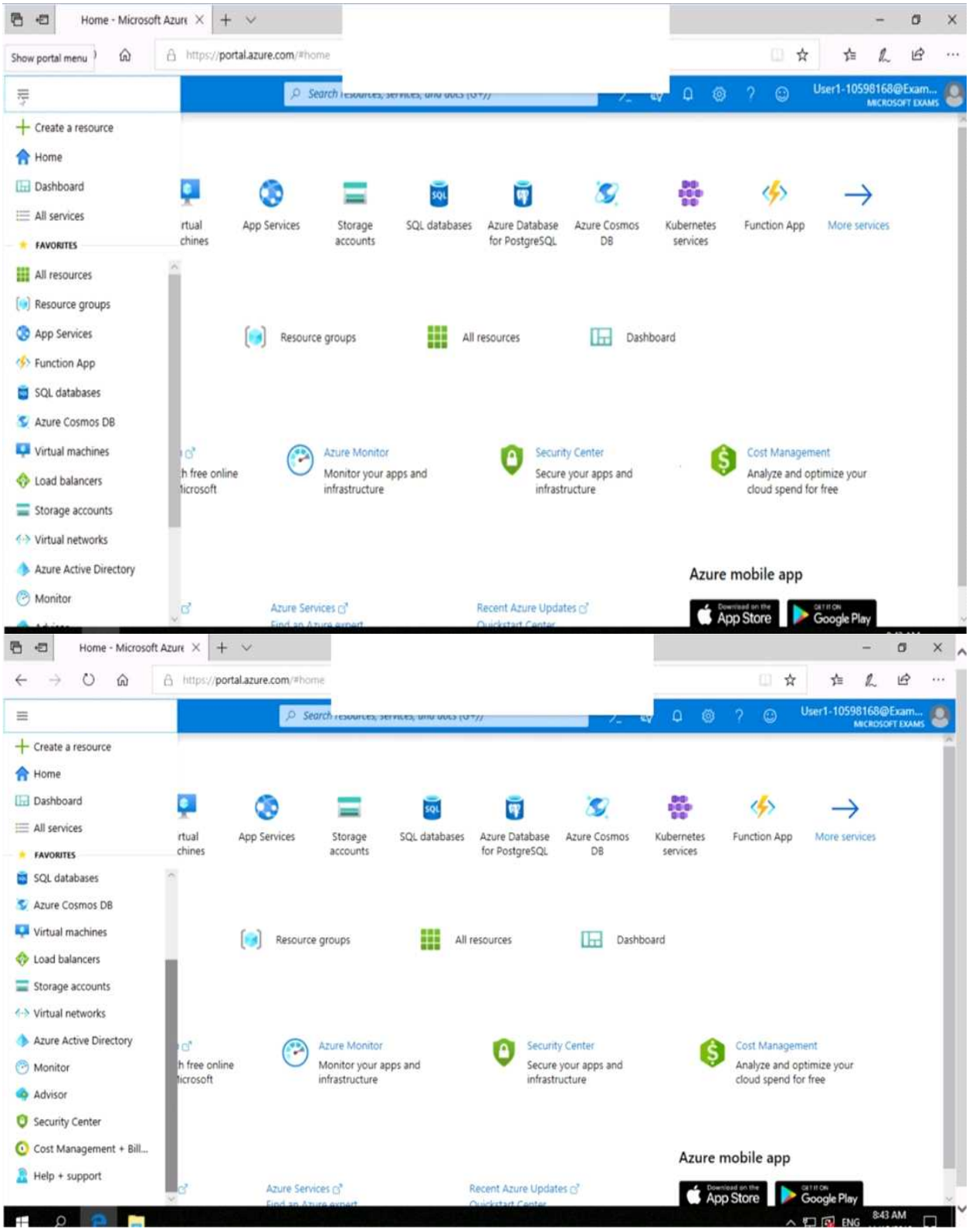
Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168



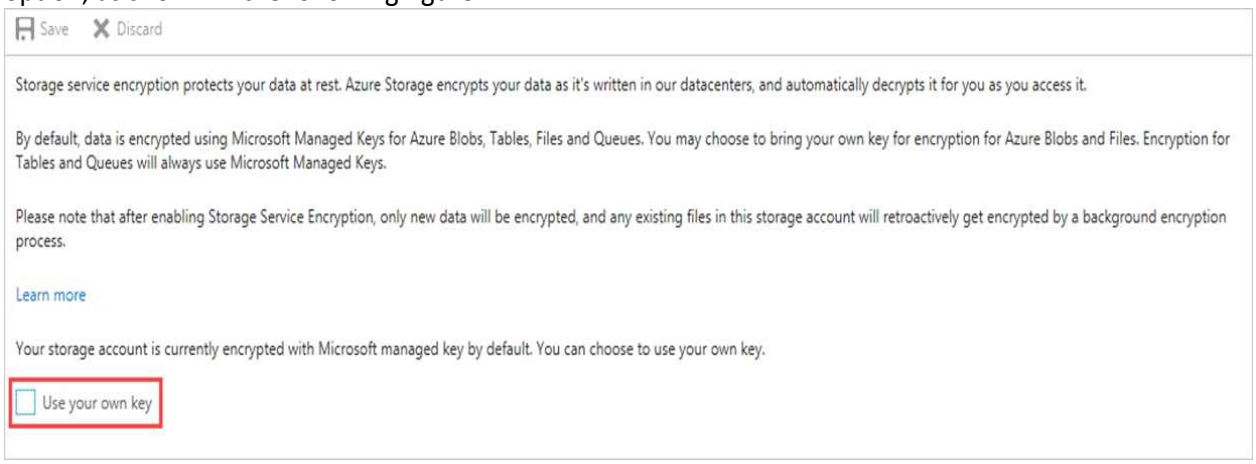


You need to ensure that the rg1lod10598168n1 Azure Storage account is encrypted by using a key stored in the KeyVault10598168 Azure key vault.
To complete this task, sign in to the Azure portal.

Answer:

Step 1: To enable customer-managed keys in the Azure portal, follow these steps:
1. Navigate to your storage account rg1lod10598168n1

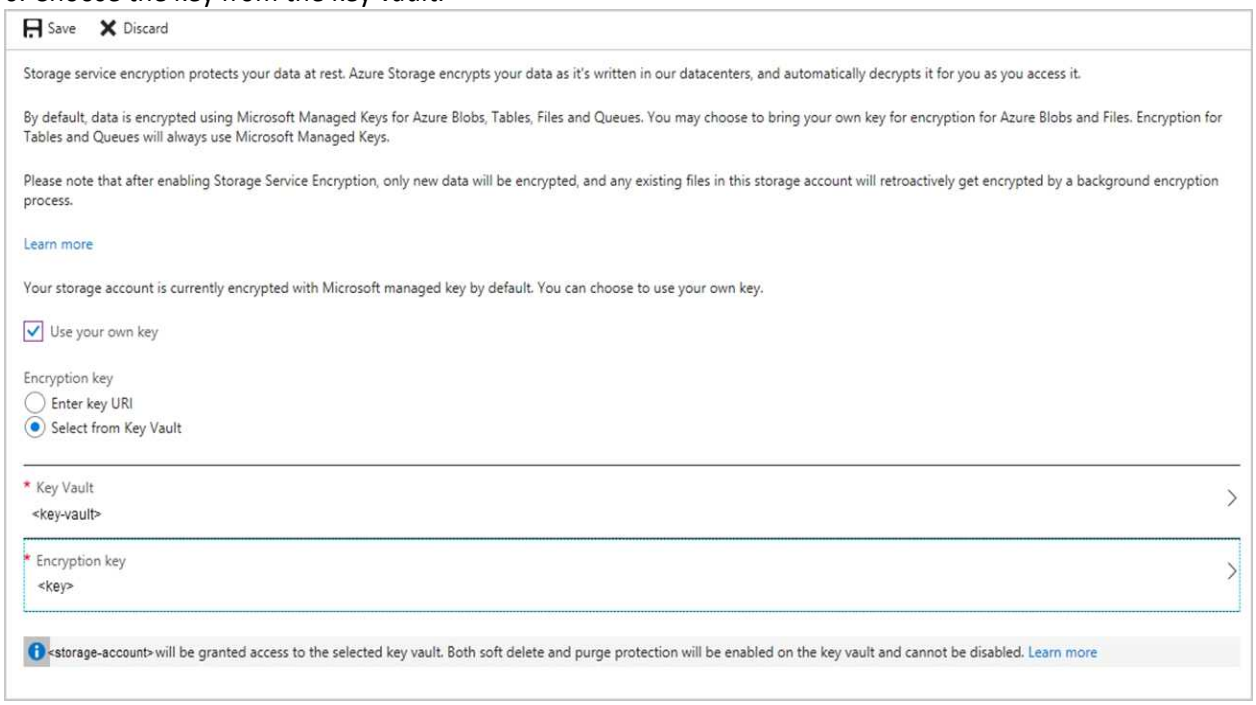
2. On the Settings blade for the storage account, click Encryption. Select the Use your own key option, as shown in the following figure.



Step 2: Specify a key from a key vault

To specify a key from a key vault, first make sure that you have a key vault that contains a key. To specify a key from a key vault, follow these steps:

4. Choose the Select from Key Vault option.
5. Choose the key vault KeyVault10598168 containing the key you want to use.
6. Choose the key from the key vault.



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

Question: 140

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.

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:

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

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

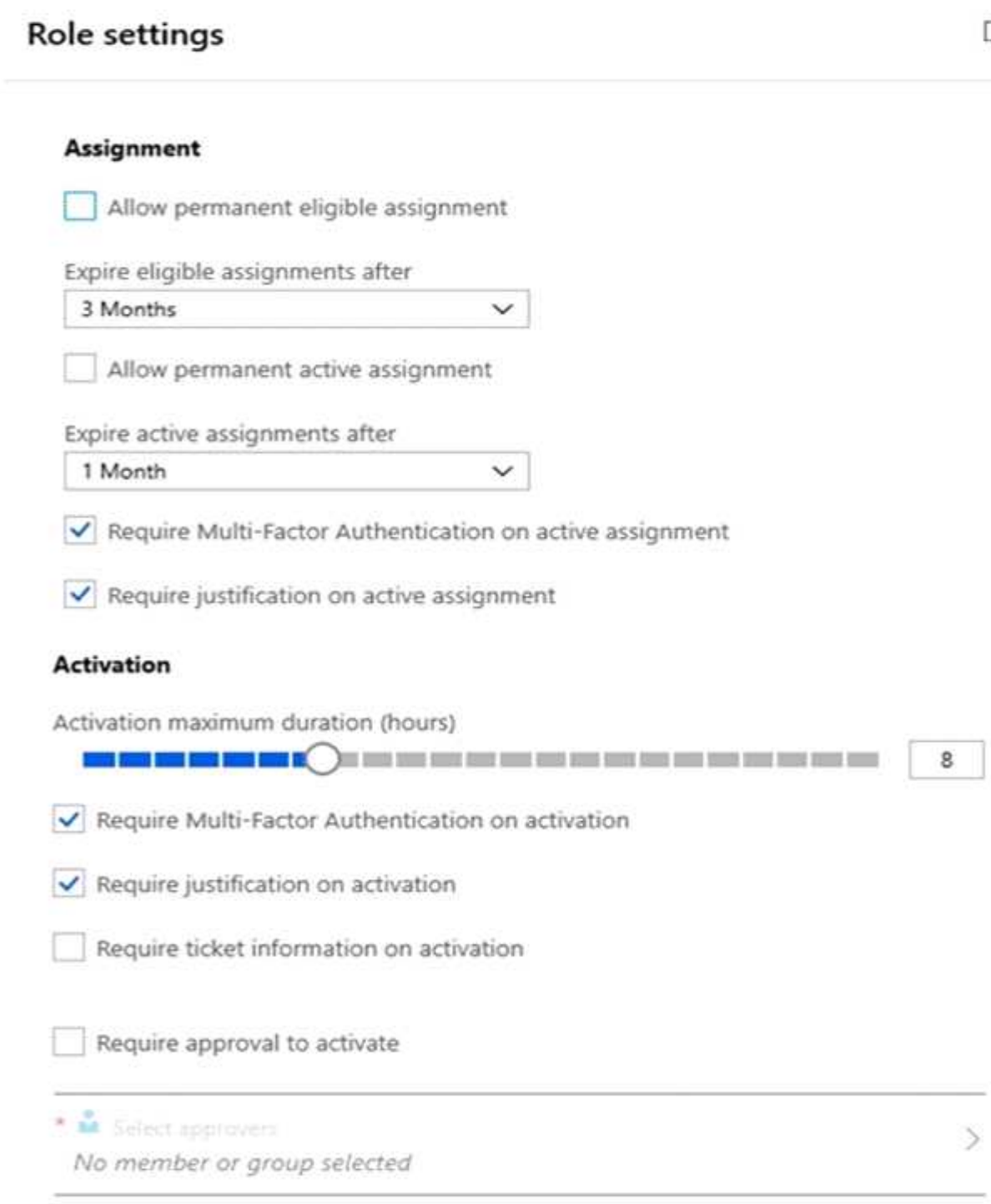
Question: 141

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.)



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.

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.	○	○

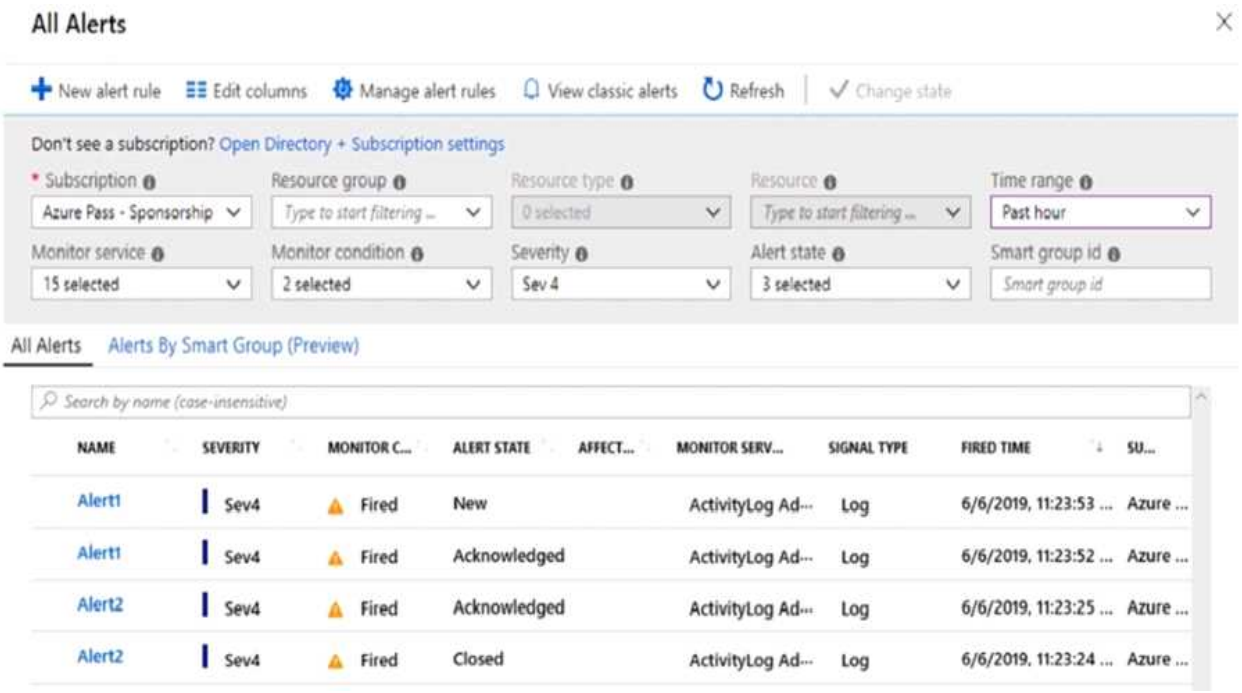
Answer:

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.	○	○

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

Question: 142

HOTSPOT
You have an Azure subscription that contains the alerts shown in the following exhibit.



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.

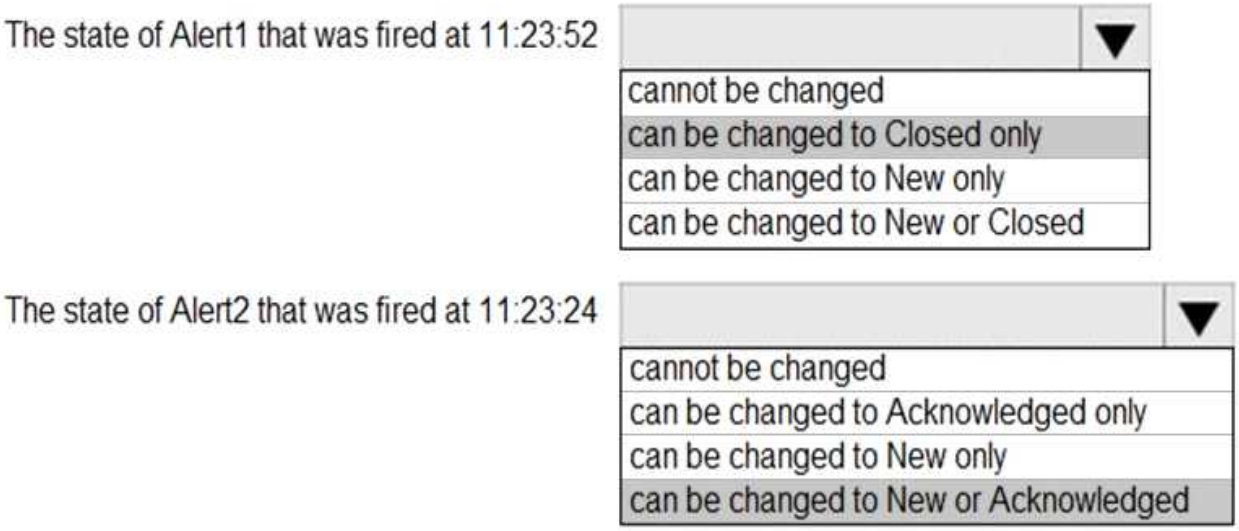
The state of Alert1 that was fired at 11:23:52

- cannot be changed
- can be changed to Closed only
- can be changed to New only
- can be changed to New or Closed

The state of Alert2 that was fired at 11:23:24

- cannot be changed
- can be changed to Acknowledged only
- can be changed to New only
- can be changed to New or Acknowledged

Answer:



Explanation:
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-overview

Question: 143

You are troubleshooting a security issue for an Azure Storage account.
You enable the diagnostic logs for the storage account.
What should you use to retrieve the diagnostics logs?

A. Azure Storage Explorer
B. SQL query editor in Azure
C. File Explorer in Windows
D. Azure Security Center

Answer: A

Explanation:
If you want to download the metrics for long-term storage or to analyze them locally, you must use a tool or write some code to read the tables. You must download the minute metrics for analysis. The tables do not appear if you list all the tables in your storage account, but you can access them directly by name. Many storage-browsing tools are aware of these tables and enable you to view them directly (see Azure Storage Client Tools for a list of available tools).
Microsoft provides several graphical user interface (GUI) tools for working with the data in your Azure Storage account. All of the tools outlined in the following table are free.

Azure Storage client tool	Supported platforms	Block Blob	Page Blob	Append Blob	Tables	Queues	Files
Azure portal	Web	Yes	Yes	Yes	Yes	Yes	Yes
Azure Storage Explorer	Windows, OSX	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Visual Studio Cloud Explorer	Windows	Yes	Yes	Yes	Yes	Yes	No

References:
https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-metrics?toc=%2fazure%2fstorage%2fblobs%2ftoc.json
https://docs.microsoft.com/en-us/azure/storage/common/storage-explorers

Question: 144

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.

Answer: A

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

Question: 145

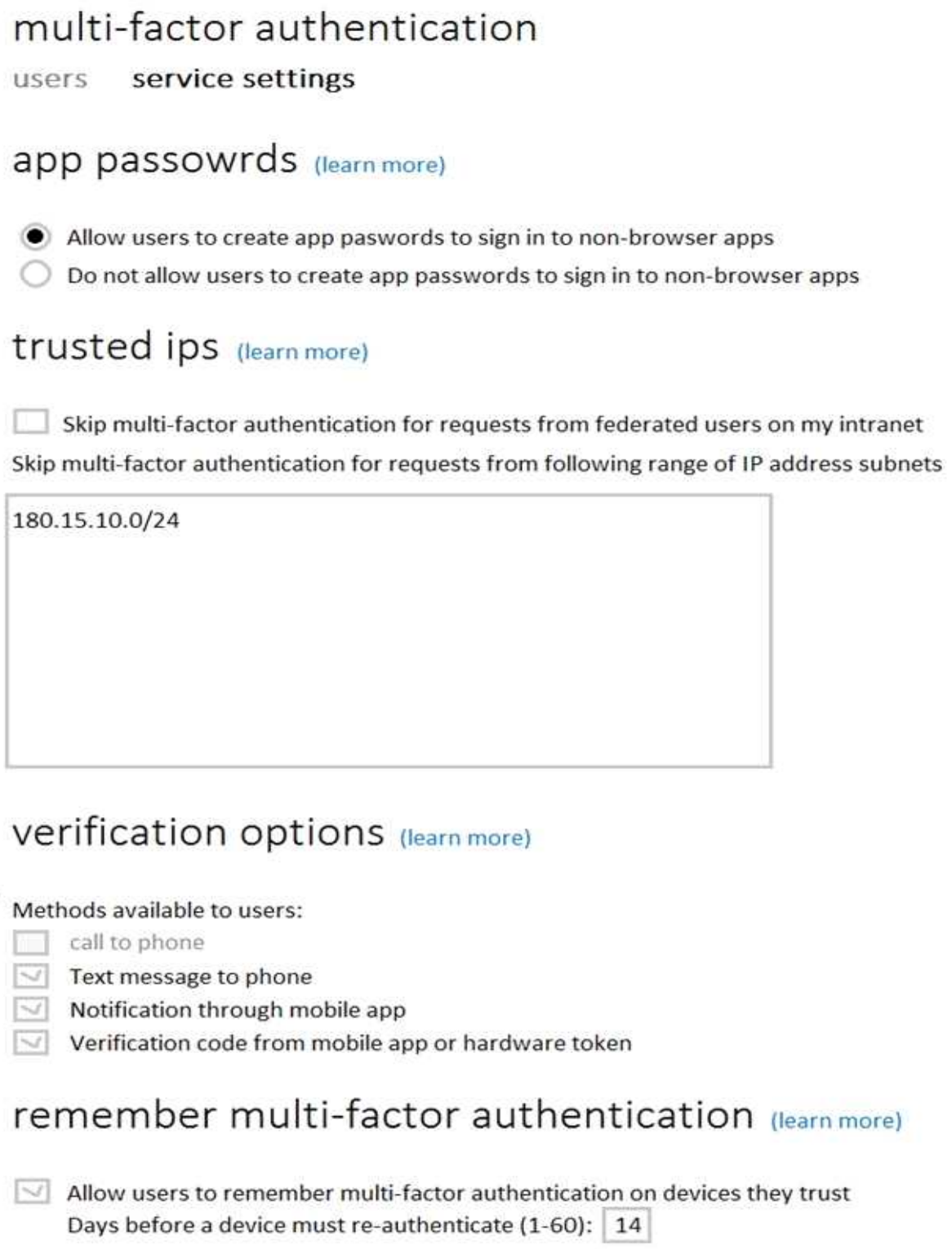
HOTSPOT
You work at a company named Contoso, Ltd. that has the offices shown in the following table.

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.



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

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:

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.	●	○

Question: 146

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.

Answer: AB

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

Question: 147

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.

Answer: C

Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/connect-logon

Question: 148

HOTSPOT
You 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 and 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.

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:

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.	○	○

Question: 149

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

Answer: A

Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines

Question: 150

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.

Answer:

You need to configure the Network Security Group that is associated with subnet0.
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.
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.
Type Network Security Groups into the search box and select the Network Security Group associated with Subnet0.
In the properties of the Network Security Group, click on Inbound Security Rules.
Click the Add button to add a new rule.
In the Source field, select Service Tag.
In the Source Service Tag field, select Internet.
Leave the Source port ranges and Destination field as the default values (* and All).
In the Destination port ranges field, enter 7777.
Change the Protocol to TCP.
Leave the Action option as Allow.
Change the Priority to 100.
Change the Name from the default Port_8080 to something more descriptive such as Allow_TCP_7777_from_Internet. The name cannot contain spaces.
Click the Add button to save the new rule.

Question: 151

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.

Answer:

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.
• 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.
• In the properties of the app service plan, click on Locks.
• Click the Add button to add a new lock.
• Enter a name in the Lock name field. It doesn't matter what name you provide for the exam.
• For the Lock type, select Read-only.
• Click OK to save the changes.

Question: 152

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.

Answer:

You need to provision an Azure AD Admin for the SQL Server.
• 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.
• In the SQL Server properties page, click on Active Directory Admin.
• Click the Set Admin button.
• In the Add Admin window, search for and select Danny11597200.
• Click the Select button to add Danny11597200.
• 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: 153

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.

Answer:

You need to allow access to Azure services and configure a virtual network rule for the SQL Server.
• 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.
• In the properties of the SQL Server, click Firewalls and virtual networks.
• In the Virtual networks section, click on Add existing. This will open the Create/Update virtual network rule window.

• Give the rule a name such as Allow_VNET01-Subnet0 (it doesn't matter what name you enter for the exam).
• In the Virtual network box, select VNET01.
• In the Subnet name box, select Subnet0.
• Click the OK button to save the rule.
• Back in the Firewall / Virtual Networks window, set the Allow access to Azure services option to On.

Question: 154

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

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.
Reference:
https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started

Question: 155

SIMULATION
You need to ensure that web11597200 is protected from malware by using Microsoft Antimalware for Virtual Machines and is scanned every Friday at 01:00.
To complete this task, sign in to the Azure portal.

Answer:

You need to install and configure the Microsoft Antimalware extension on the virtual machine named web11597200.
• In the Azure portal, type Virtual Machines in the search box, select Virtual Machines from the search results then select web11597200. Alternatively, browse to Virtual Machines in the left navigation pane.
• In the properties of web11597200, click on Extensions.

• Click the Add button to add an Extension.
• Scroll down the list of extensions and select Microsoft Antimalware.
• Click the Create button. This will open the settings pane for the Microsoft Antimalware Extension.
• In the Scan day field, select Friday.
• In the Scan time field, enter 60. The scan time is measured in minutes after midnight so 60 would be 01:00, 120 would be 02:00 etc.
• Click the OK button to save the configuration and install the extension.

Question: 156

SIMULATION
You need to ensure that the events in the NetworkSecurityGroupRuleCounter log of the VNET01-Subnet0-NSG network security group (NSG) are stored in the logs11597200 Azure Storage account for 30 days.
To complete this task, sign in to the Azure portal.

Answer:

You need to configure the diagnostic logging for the NetworkSecurityGroupRuleCounter log.
• In the Azure portal, type Network Security Groups in the search box, select Network Security Groups from the search results then select VNET01-Subnet0-NSG. Alternatively, browse to Network Security Groups in the left navigation pane.
• In the properties of the Network Security Group, click on Diagnostic Settings.
• Click on the Add diagnostic setting link.
• Provide a name in the Diagnostic settings name field. It doesn't matter what name you provide for the exam.
• In the Log section, select NetworkSecurityGroupRuleCounter.
• In the Destination details section, select Archive to a storage account.
• In the Storage account field, select the logs11597200 storage account.
• In the Retention (days) field, enter 30.
• Click the Save button to save the changes.

Question: 157

SIMULATION
A user named Debbie has the Azure app installed on her mobile device.
You need to ensure that debbie@contoso.com is alerted when a resource lock is deleted.
To complete this task, sign in to the Azure portal.

Answer:

You need to configure an alert rule in Azure Monitor.
• Type Monitor into the search box and select Monitor from the search results.
• Click on Alerts.
• Click on +New Alert Rule.
• In the Scope section, click on the Select resource link.
• In the Filter by resource type box, type locks and select Management locks (locks) from the filtered results.

• Select the subscription then click the Done button.
• In the Condition section, click on the Select condition link.
• Select the Delete management locks condition the click the Done button.
• In the Action group section, click on the Select action group link.
• Click the Create action group button to create a new action group.
• Give the group a name such as Debbie Mobile App (it doesn't matter what name you enter for the exam) then click the Next: Notifications > button.
• In the Notification type box, select the Email/SMS message/Push/Voice option.
• In the Email/SMS message/Push/Voice window, tick the Azure app Push Notifications checkbox and enter debbie@contoso.com in the Azure account email field.
• Click the OK button to close the window.
• Enter a name such as Debbie Mobile App in the notification name box.
• Click the Review & Create button then click the Create button to create the action group.
• Back in the Create alert rule window, in the Alert rule details section, enter a name such as Management lock deletion in the Alert rule name field.
• Click the Create alert rule button to create the alert rule.

Question: 158

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

Answer:

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

Question: 159

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

Answer:

You need to configure an option in the Advanced Access Policy of the key vault.
• In the Azure portal, type Azure Key Vault in the search box, select Azure Key Vault from the search

results then select the key vault named KV11597200. Alternatively, browse to Azure Key Vault in the left navigation pane.
• In the properties of the key vault, click on Advanced Access Policies.
• Tick the checkbox labelled Enable access to Azure Resource Manager for template deployment.
• Click Save to save the changes.

Question: 160

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

Answer:

You need to enable the Web Application Firewall on the Application Gateway.
• In the Azure portal, type Application gateways in the search box, select Application gateways from the search results then select the gateway named Homepage-AGW. Alternatively, browse to Application Gateways in the left navigation pane.
• In the properties of the application gateway, click on Web application firewall.
• For the Tier setting, select WAF V2.
• In the Firewall status section, click the slider to switch to Enabled.
• In the Firewall mode section, click the slider to switch to Prevention.
• Click Save to save the changes.

Question: 161

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

Answer:

• In the Azure portal, type App services in the search box and select App services from the search results.
• Click the Create app service button to create a new app service.
• In the Resource Group section, click the Create new link to create a new resource group.
• Give the resource group a name such as Intranet11597200RG and click OK.
• In the Instance Details section, enter Intranet11597200 in the Name field.
• In the Runtime stack field, select any runtime stack such as .NET Core 3.1.
• Click the Review + create button.
• Click the Create button to create the web app.
• Click the Go to resource button to open the properties of the new web app.
• In the Settings section, click on Authentication / Authorization.
• Click the App Service Authentication slider to set it to On.
• In the Action to take when request is not authentication box, select Log in with Azure Active

Directory.

• Click Save to save the changes.

Question: 162

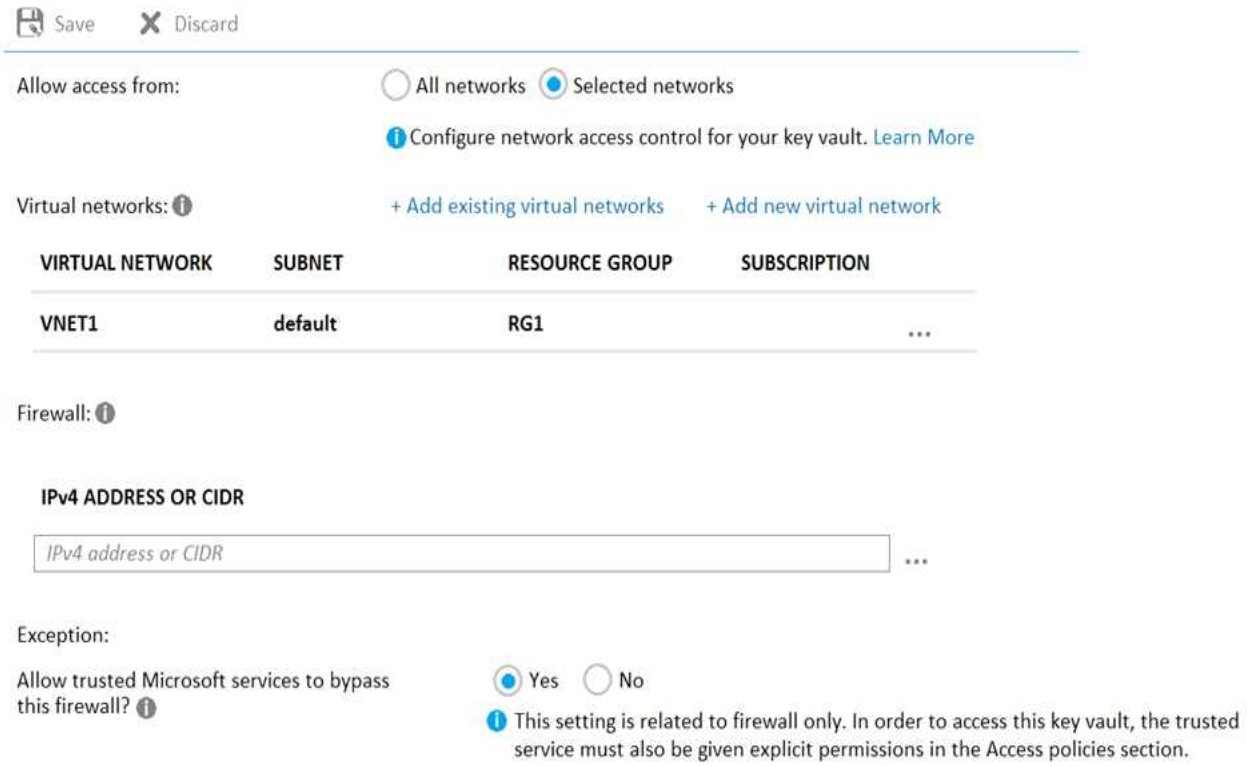
HOTSPOT

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

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

You set the Key Vault access policy to Enable access to Azure Disk Encryption for volume encryption.

KeyVault1 is configured as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

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

Answer:

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

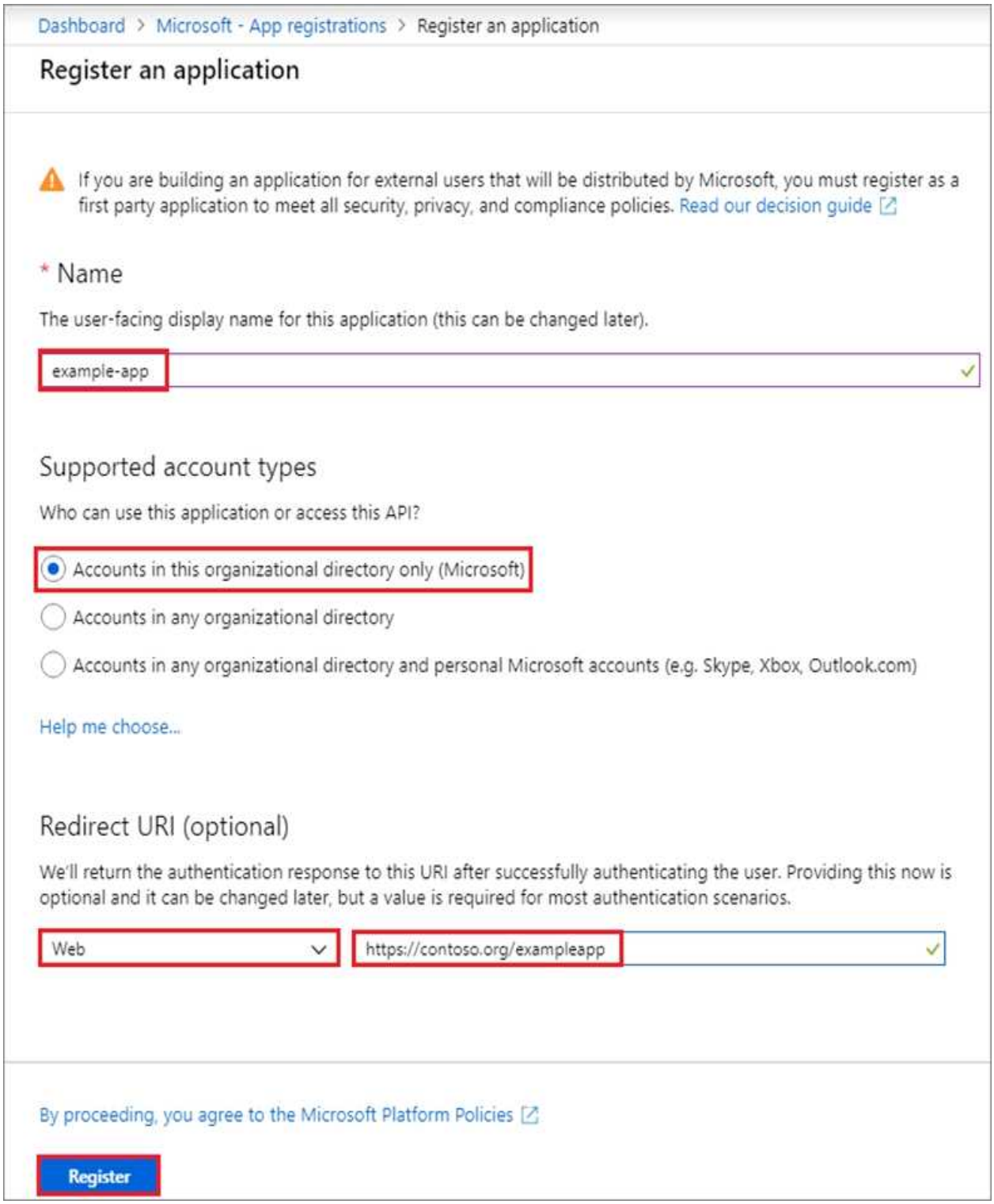
Question: 163

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.

Answer:

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.



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

Question: 164

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.

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

Answer:

NO
NO
NO

Explanation:
1.) cannot perform write operation because following scope(s) are locked: 'subscriptions/xxxx/resourceGroups/xxx' Please remove the lock and try again.
2.) When creating a VM in a resource group with a Read Only lock an error is shown: "The selected resource group is read only"
3.) Because of the read only lock virtual machines cannot be started nor stopped when the lock is added after the machine started. (not part of this use case, but still good to know.

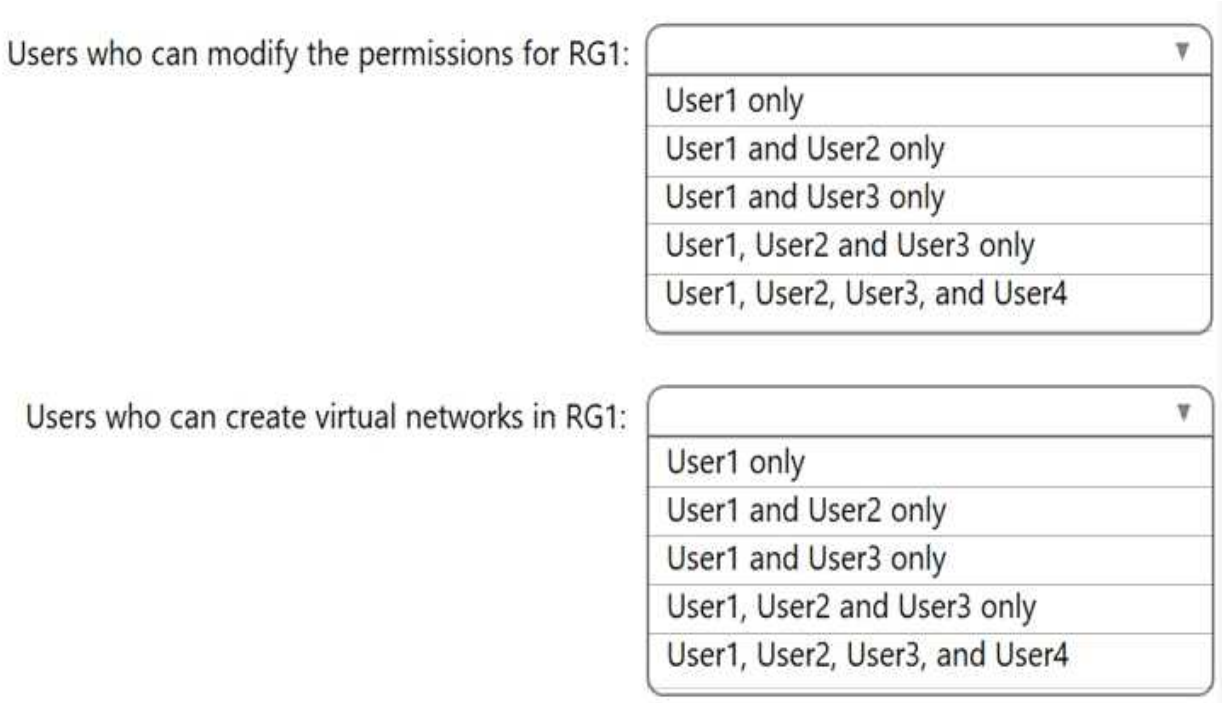
The article referenced in the answer states different because that is scoped to blueprints.
In the Lock Resources pages is states the following regarding starting VMs:
"A ReadOnly lock on a resource group that contains a virtual machine prevents all users from starting or restarting the virtual machine. These operations require a POST request."
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

Question: 165

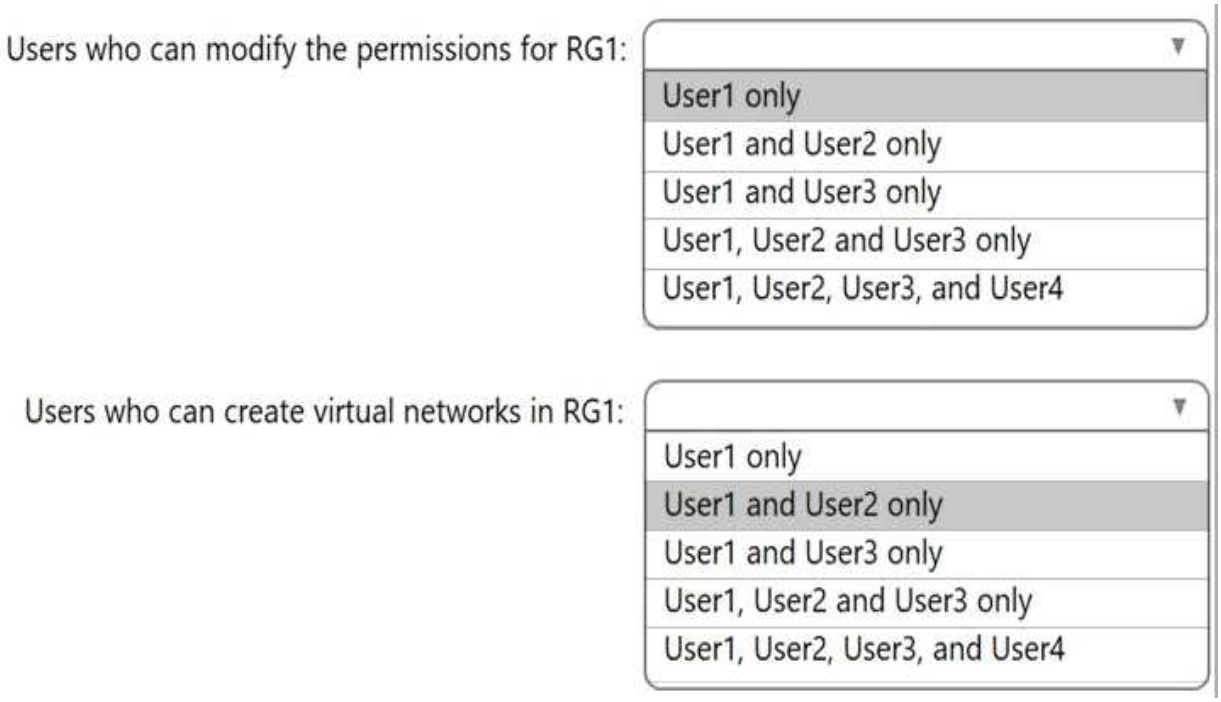
HOTSPOT
You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

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.



Answer:



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: 166

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.

Answer:

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: 167

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.

Answer:

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.
• 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.
• In the Overview section, note the Location (region) and Resource Group of the virtual network. We'll need these when we add the firewall.
• Click on Subnets.
• Click on + Subnet to add a new subnet.
• Enter AzureFirewallSubnet in the Name box. The subnet must be named AzureFirewallSubnet.
• Enter an appropriate IP range for the subnet in the Address range box.
• Click the OK button to create the subnet.
Add the Azure Firewall.
• In the settings of VNET3 click on Firewall.
• Click the Click here to add a new firewall link.
• The Resource group will default to the VNET3 resource group. Leave this default.
• Enter a name for the firewall in the Name box.
• In the Region box, select the same region as VNET3.
• 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.
• Click the Review + create button.
• 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

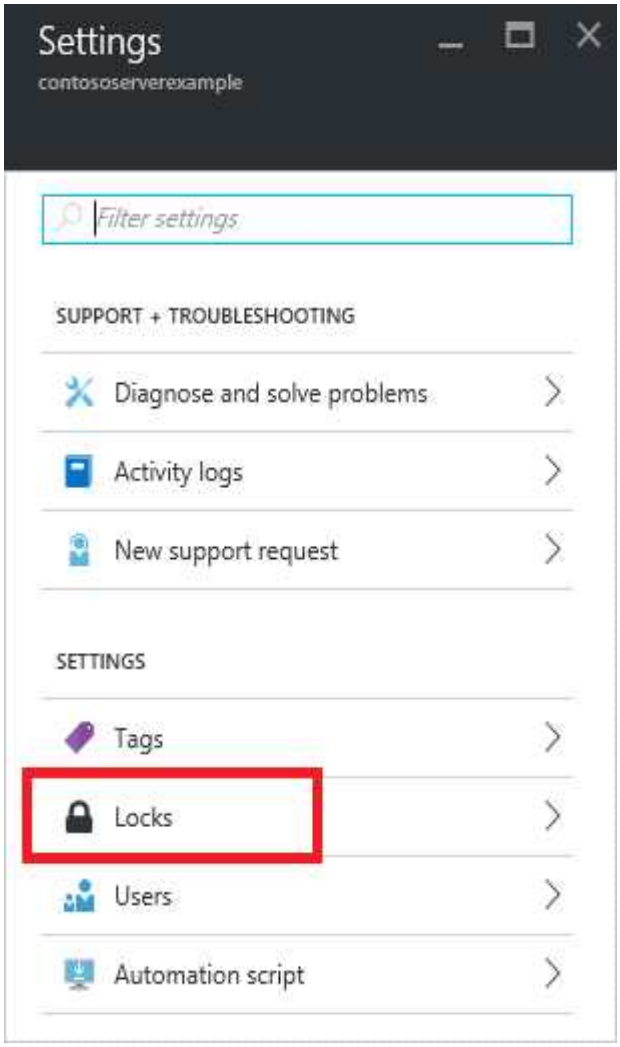
Question: 168

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.

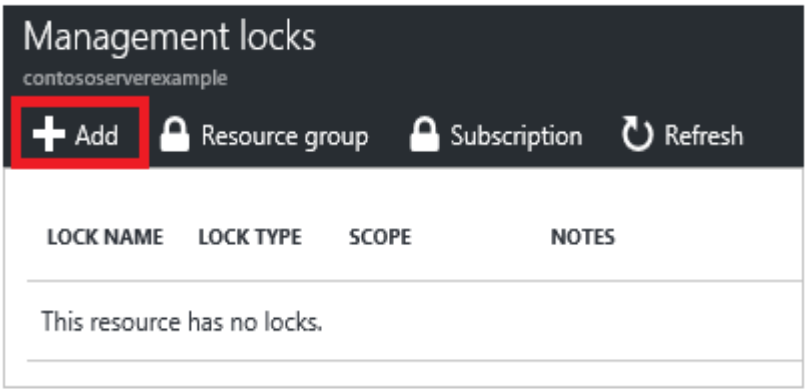
To complete this task, sign in to the Azure portal and modify the Azure resources.

Answer:

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.



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: 169

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).

Answer: A

Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-endpoint-protection

Question: 170

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.

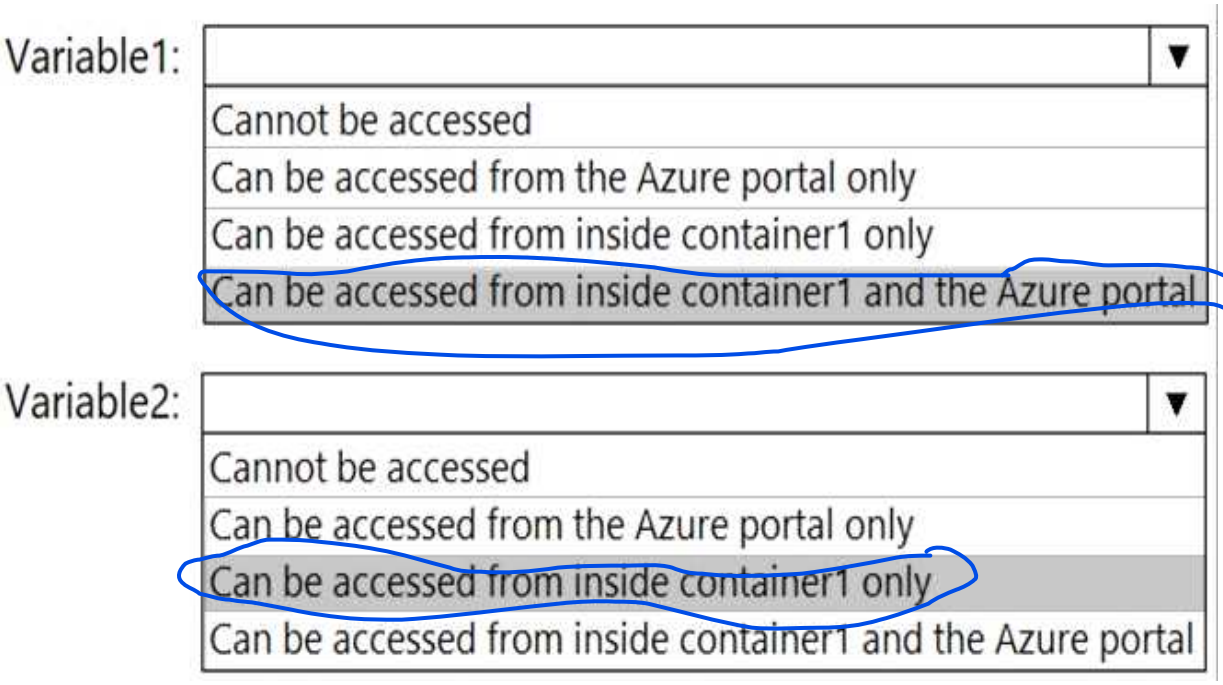
Variable1:

- 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:



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

Question: 171

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

Answer: C

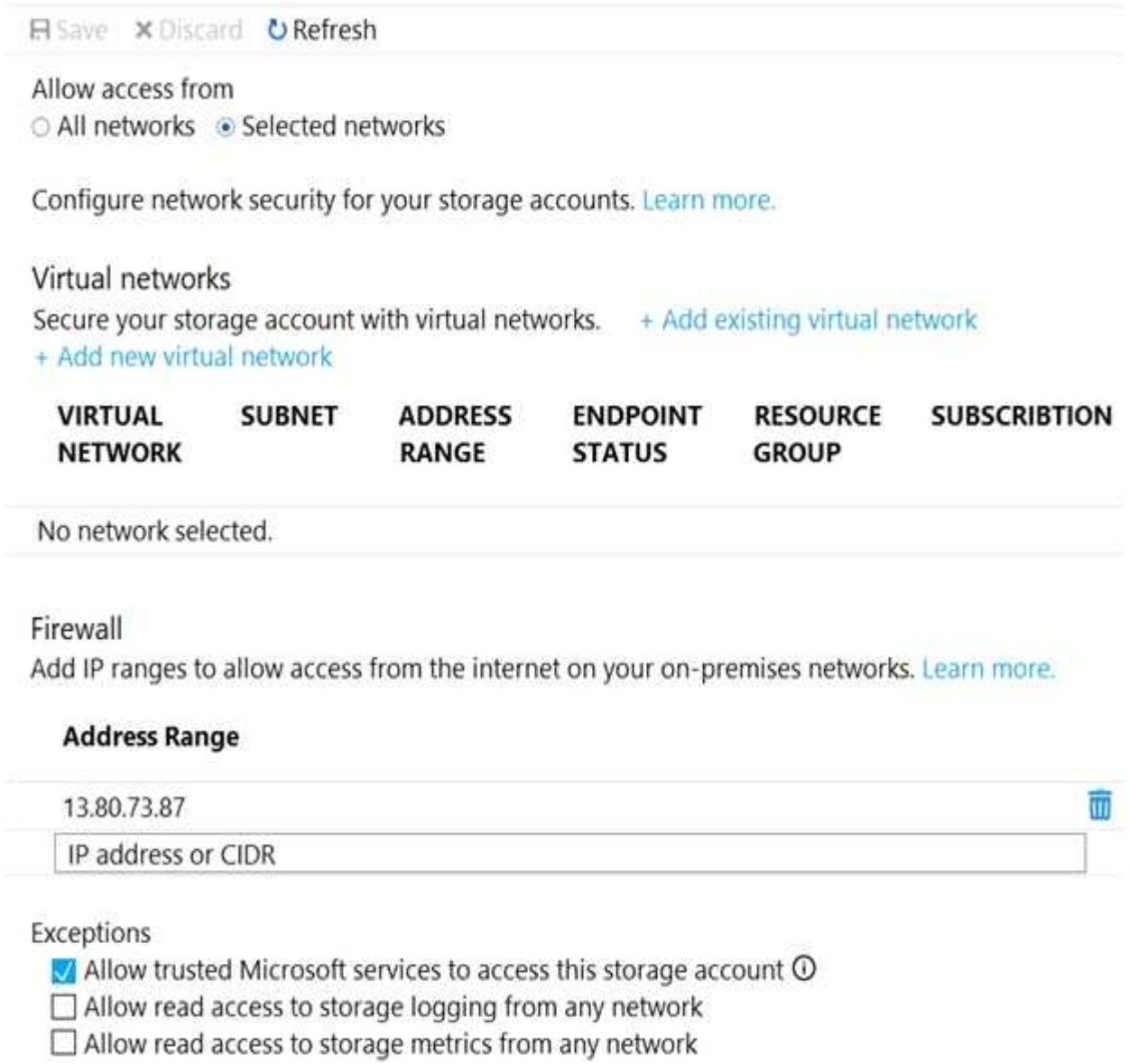
Explanation:
An NSG needs to be enabled, either at the VM level or the subnet level.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

Question: 172

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.



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

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:

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.	○	○

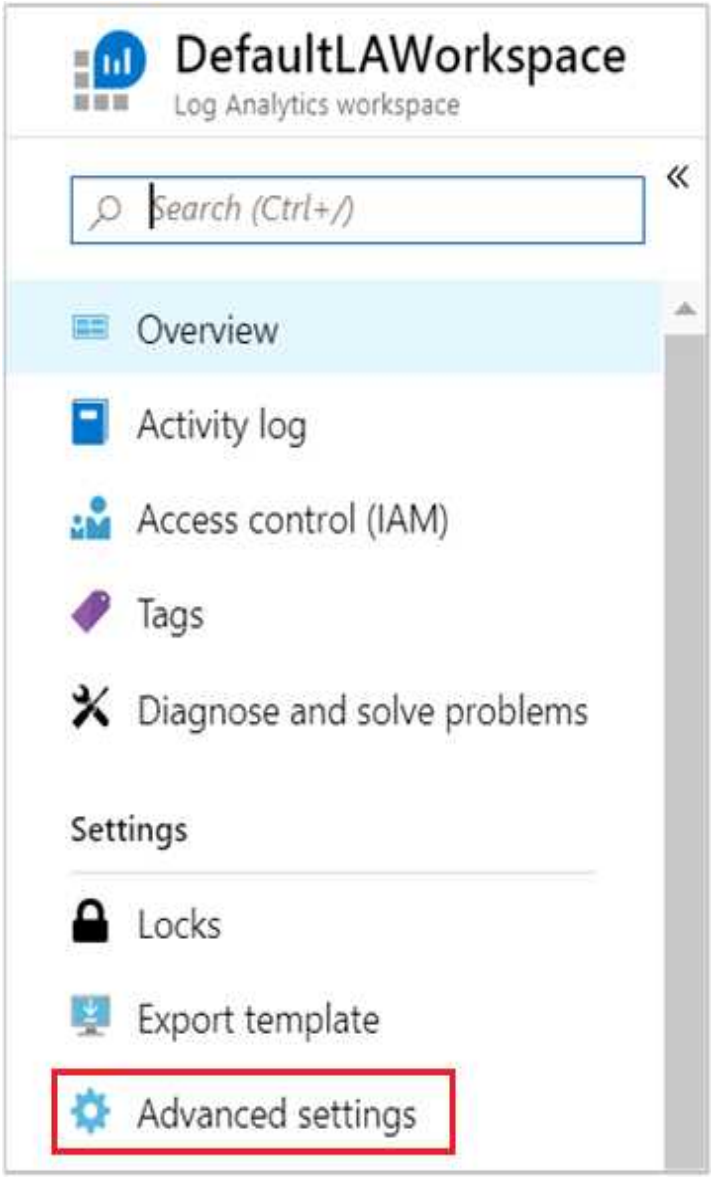
Explanation:
Box 1: Yes
The public IP of VM1 is allowed through the firewall.
Box 2: No
The allowed virtual network list is empty so VM2 cannot access storageacc1 directly. The public IP address of VM2 is not in the allowed IP list so VM2 cannot access storageacc1 over the Internet.
Box 3: No
The allowed 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: 173

SIMULATION
You plan to connect several Windows servers to the WS11641655 Azure Log Analytics workspace.
You need to ensure that the events in the System event logs are collected automatically to the workspace after you connect the Windows servers.
To complete this task, sign in to the Azure portal and modify the Azure resources.

Answer:

Azure Monitor can collect events from the Windows event logs or Linux Syslog and performance counters that you specify for longer term analysis and reporting, and take action when a particular condition is detected. Follow these steps to configure collection of events from the Windows system log and Linux Syslog, and several common performance counters to start with.
Data collection from Windows VM
1. In the Azure portal, locate the WS11641655 Azure Log Analytics workspace then select Advanced settings.



2. Select Data, and then select Windows Event Logs.
3. You add an event log by typing in the name of the log. Type System and then select the plus sign +.
4. In the table, check the severities Error and Warning. (for this question, select all severities to ensure that ALL logs are collected).
5. Select Save at the top of the page to save the configuration.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm

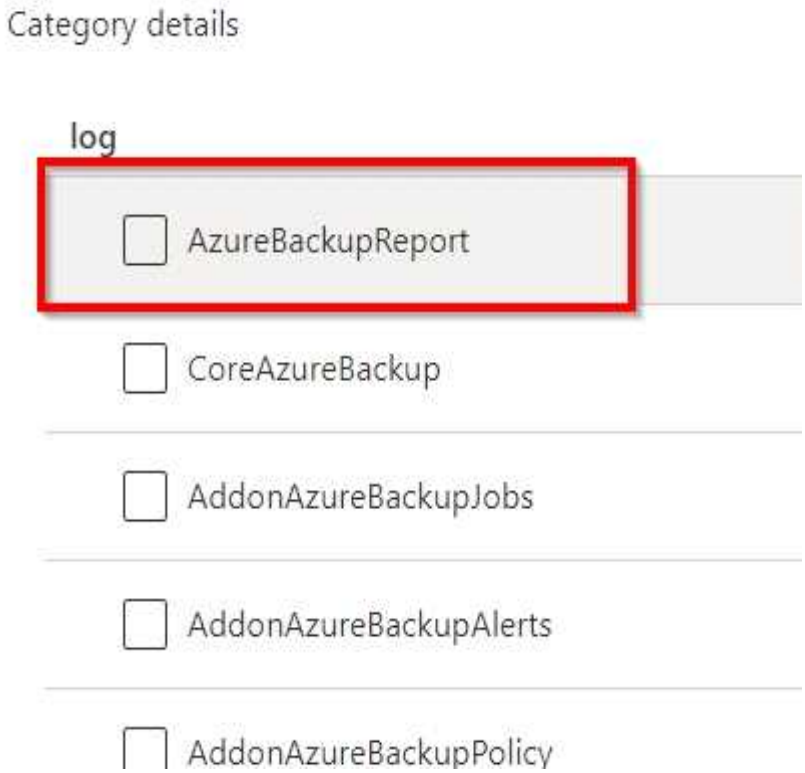
Question: 174

SIMULATION
You need to ensure that the AzureBackupReport log for the Vault1 Recovery Services vault is stored in the WS11641655 Azure Log Analytics workspace.
To complete this task, sign in to the Azure portal and modify the Azure resources.

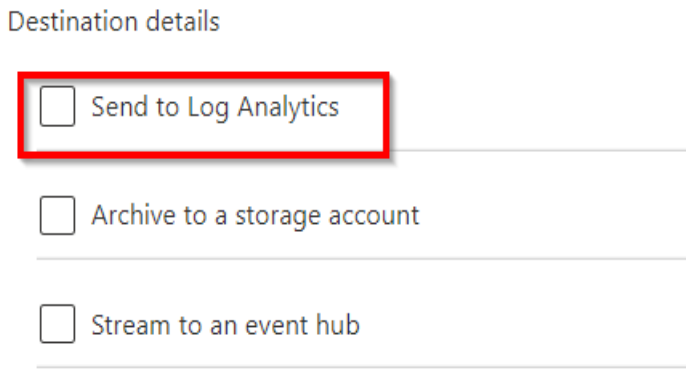
Answer:

1. In the Azure portal, type Recovery Services Vaults in the search box, select Recovery Services

Vaults from the search results then select Vault1. Alternatively, browse to Recovery Services Vaults in the left navigation pane.
2. In the properties of Vault1, scroll down to the Monitoring section and select Diagnostic Settings.
3. Click the Add a diagnostic setting link.
4. Enter a name in the Diagnostic settings name box.
5. In the Log section, select AzureBackupReport.



6. In the Destination details section, select Send to log analytics



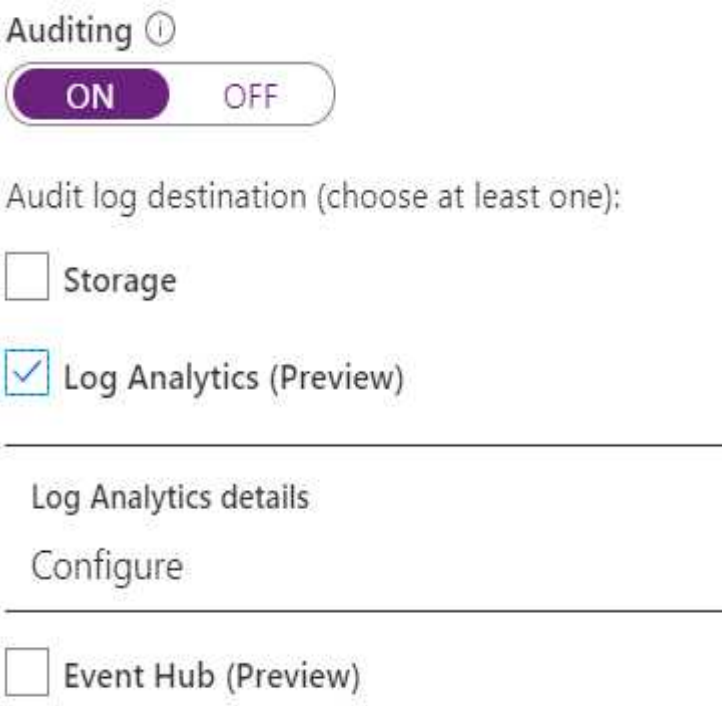
7. Select the WS11641655 Azure Log Analytics workspace.
8. Click the Save button to save the changes.
Reference:
https://docs.microsoft.com/en-us/azure/backup/backup-azure-diagnostic-events

Question: 175

SIMULATION
You need to ensure that the audit logs from the SQLdb1 Azure SQL database are stored in the WS11641655 Azure Log Analytics workspace.
To complete this task, sign in to the Azure portal and modify the Azure resources.

Answer:

1. In the Azure portal, type SQL in the search box, select SQL databases from the search results then select SQLdb1. Alternatively, browse to SQL databases in the left navigation pane.
2. In the properties of SQLdb1, scroll down to the Security section and select Auditing.
3. Turn auditing on if it isn't already, tick the Log Analytics checkbox then click on Configure.



4. Select the WS11641655 Azure Log Analytics workspace.
5. Click Save to save the changes.

Question: 176

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

Answer:

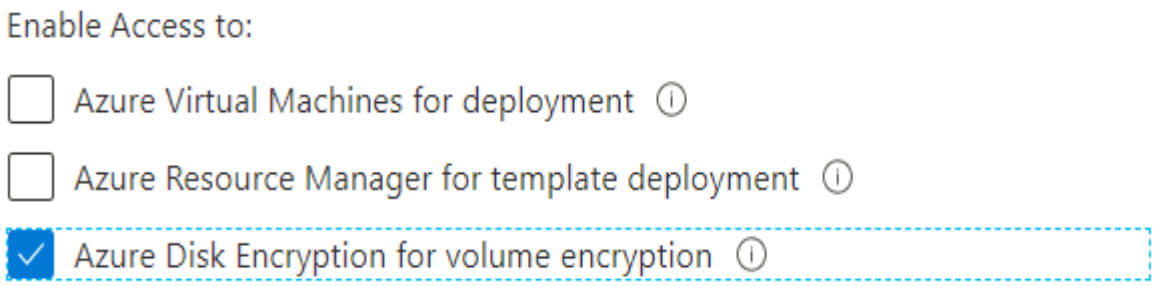
• In the Azure portal, type SQL in the search box, select SQL databases from the search results then select SQLdb1. Alternatively, browse to SQL databases in the left navigation pane.
• In the properties of SQLdb1, scroll down to the Security section and select Advanced data security.
• Click on the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

Question: 177

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

Answer:

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



4. Click Save to save the changes.

Question: 178

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

Answer:

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

Question: 179

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

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

Answer: B

Reference:
https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate-in-code

Question: 180

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

Name	Location	Azure subscription name
KV1	West US	Subscription1
KV2	West US	Subscription1
KV3	East US	Subscription1
KV4	West US	Subscription2
KV5	East US	Subscription2

KV1 stores a secret named Secret1 and a key for a managed storage account named Key1.
You back up Secret1 and Key1.
To which key vaults can you restore each backup? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

You can restore the Secret1 backup to:

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

You can restore the Key1 backup to:

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

Answer:

You can restore the Secret1 backup to:

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

You can restore the Key1 backup to:

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

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

Question: 181

You onboard Azure Sentinel. You connect Azure Sentinel to Azure Security Center.
You need to automate the mitigation of incidents in Azure Sentinel. The solution must minimize administrative effort.
What should you create?

A. an alert rule
B. a playbook
C. a function app
D. a runbook

Answer: B

Question: 182

You have an Azure subscription named Subscription1.
You deploy a Linux virtual machine named VM1 to Subscription1.
You need to monitor the metrics and the logs of VM1.
D18912E1457D5D1DDCBD40AB3BF70D5D
What should you use?

A. the AzurePerformanceDiagnostics extension
B. Azure HDInsight
C. Linux Diagnostic Extension (LAD) 3.0
D. Azure Analysis Services

Answer: C

Question: 183

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.

Answer: D

Question: 184

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.
D18912E1457D5D1DDCBD40AB3BF70D5D

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

Answer: B,C E

Question: 185

You have an Azure subscription that contains a resource group named RG1 and a security group serverless RG1 contains 10 virtual machine, a virtual network VNET1, and a network security group (NSG) named NSG1. ServerAdmins can access the virtual machines by using RDP.
You need to ensure that NSG1 only RDP connections to the virtual for a maximum of 60 minutes when a member of ServerAdmins requests access.
What should you configure?

A. an Azure Active Directory (Azure AD) Privileged identity Management (PIM) role assignment.
B. a just in time (JIT) VM access policy in Azure Security Center
C. an azure policy assigned to RG1.
D. an Azure Bastion host on VNET1.

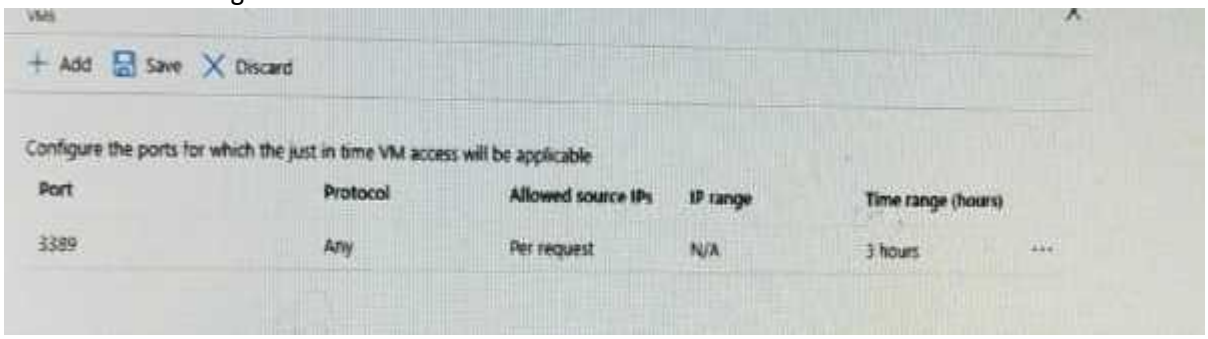
Answer: A B

Question: 186

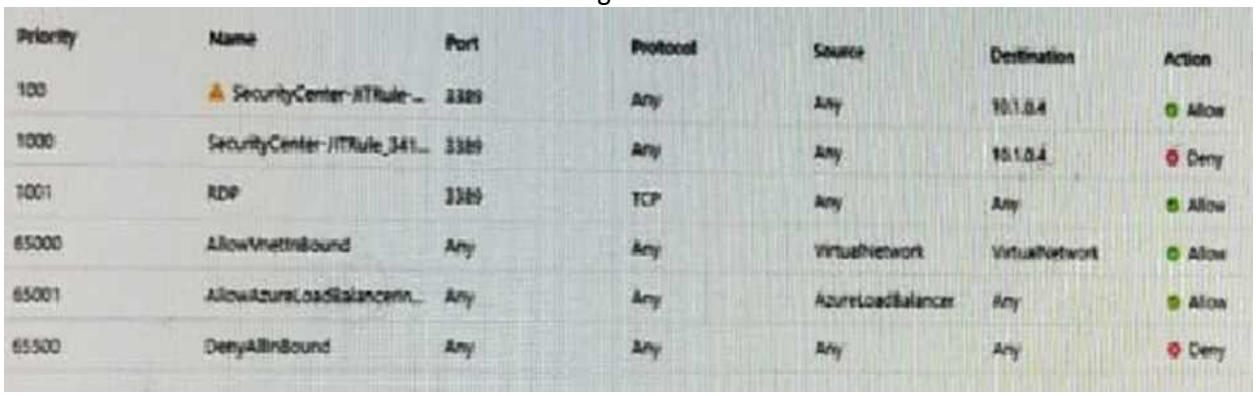
HOTSPOT
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Attached to	NSG
NSG1	Network security group (NSG)	VM5	Not applicable
NSG2	Network security group (NSG)	Subnet1	Not applicable
Subnet1	Subnet	Not applicable	Not applicable
VM5	Virtual machine	Subnet1	NSG1

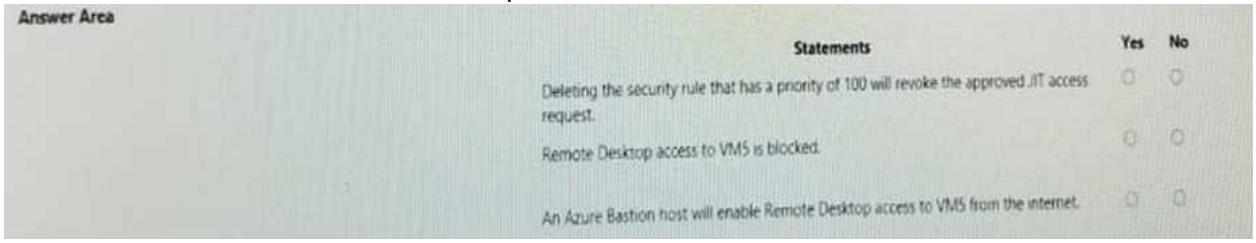
An IP address of 10.10.4 is assigned to VM5. VM5 does not have a public IP address.
VM5 has just in the (JIT) VM access configured as shown in the following exhibit.
JIT VM access configuration.



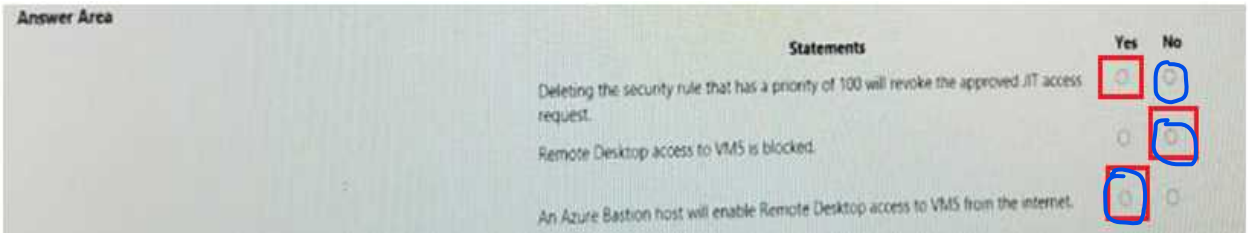
You enable JIT VM access for VM5.
NSG1 has the inbound rules shown in the following exhibit.



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



Answer:



Question: 187

DRAG DROP

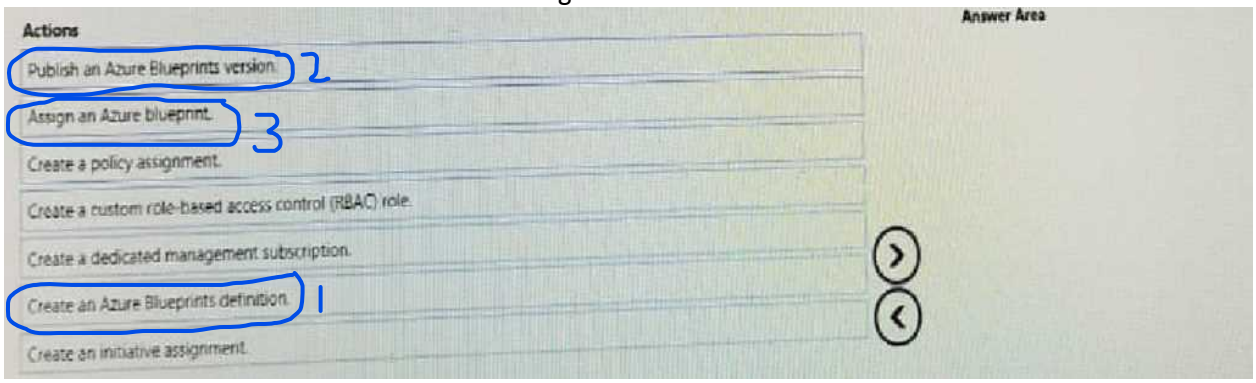
You have five Azure subscriptions linked to a single Azure Active Directory (Azure AD) tenant.

You create an Azure Policy initiative named securityPolicyinitive1

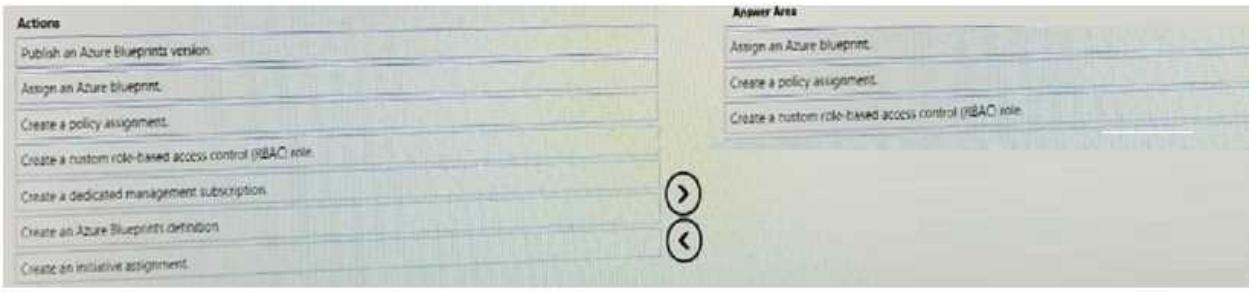
You identify which standard role assignments must be configured on all new resource groups.

You need to enforce SecurityPolicyinvitative1 and the role assignments when anew resource group is created

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.



Answer:



Question: 188

You have an Azure subscription that contains an Azure key vault and an Azure Storage account. The key vault contains customer-managed keys. The storage account is configured to use the customer-managed keys stored In the key vault.

You plan to store data in Azure by using the following services:

* Azure Files
* Azure Blob storage
* Azure Log Analytics
* Azure Table storage
* Azure Queue storage

Which two services data encryption by using the keys stored in the key vault? Each correct answer present a complete solution.
NOTE: Each correct selection is worth one point.

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

Answer: A, D

Question: 189

You have an Azure Active Directory (Azure AD) tenant named Contoso.com and an Azure 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 Kubermetes.
C. From Azure AD, implement Azure AD Premium.
D. From Azure AD, configure the User settings

Answer: A

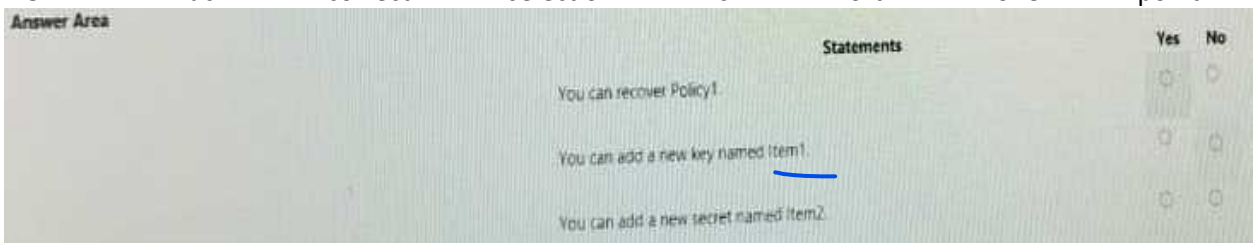
Question: 190

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

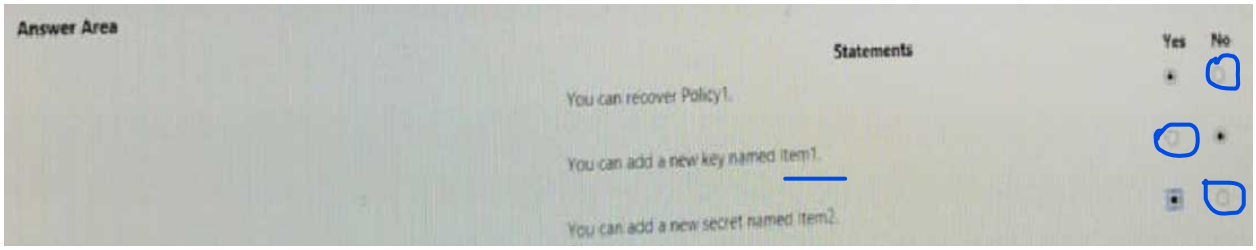
Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

In KeyVault, the following events occur in sequence:
- Item is deleted
- An administrator enables soft delete.
- Item2 and Policy1 are deleted.

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



Answer:



Question: 191

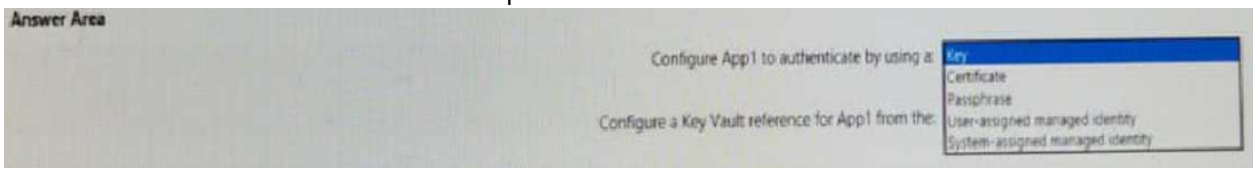
You have a Azure subscription that contains an Azure Container Registry named Registry1. The subscription uses the Standard use tier of Azure Security Center.
You upload several container images to Register1.
You discover that vulnerability security scans were not performed
You need to ensured that the 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

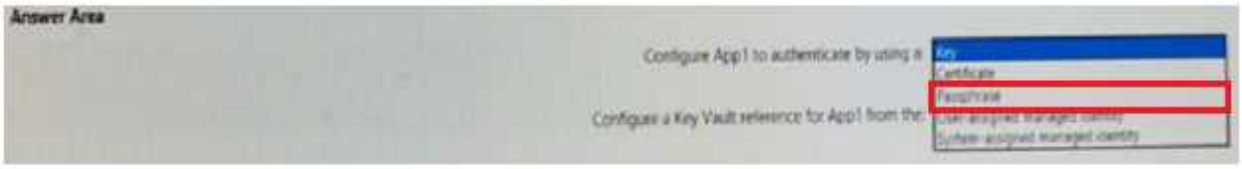
Answer: A

Question: 192

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



Answer:



Question: 193

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

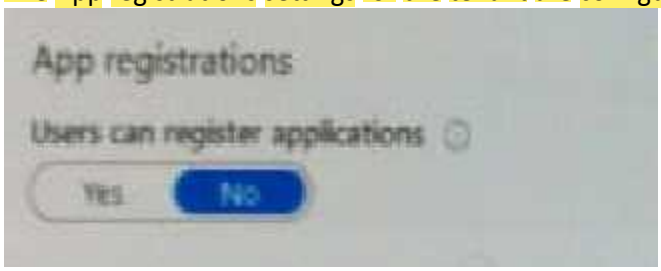
You need to ensure that ServerAdmins can perform the following tasks:
Create virtual machine to the existing virtual network in RG2 only.
The solution must use the principle of least privilege.
Which two role-based access control (RBAC) roles should you assign to ServerAdmins? Each correct answer presents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

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

Answer: B, F

Question: 194

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.



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.

Answer: B D

Question: 195

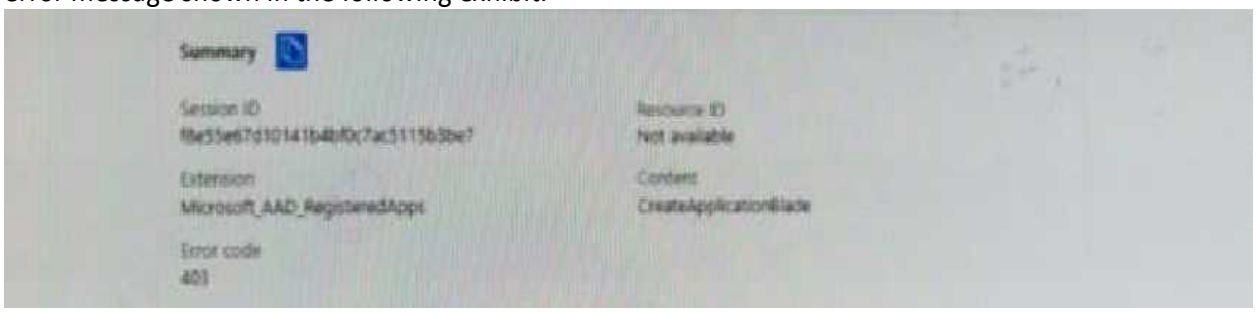
You have an Azure subscription named Subcription1 that contains an Azure Active Directory (Azure AD) tenant named contosos.com and a resource group named RG1.
You create a custom role named Role1 for contoso.com.
You need to identify where you can use Role1 for permission delegation.
What should you identify?

A. contoso.com only
B. contoso.com and RGT only
C. contoso.com and Subscription1 only
D. contoso.com, RG1, and Subcription1

Answer: B A

Question: 196

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant.
When a developer attempts to register an app named App1 in the tenant, the developer receive the error message shown in the following exhibit.



A. Modify the User settings
B. Set Enable Security default to Yes.
C. Modify the Directory properties.
D. Configure the Consent and permissions settings for enterprise applications.

Answer: B A

Question: 197

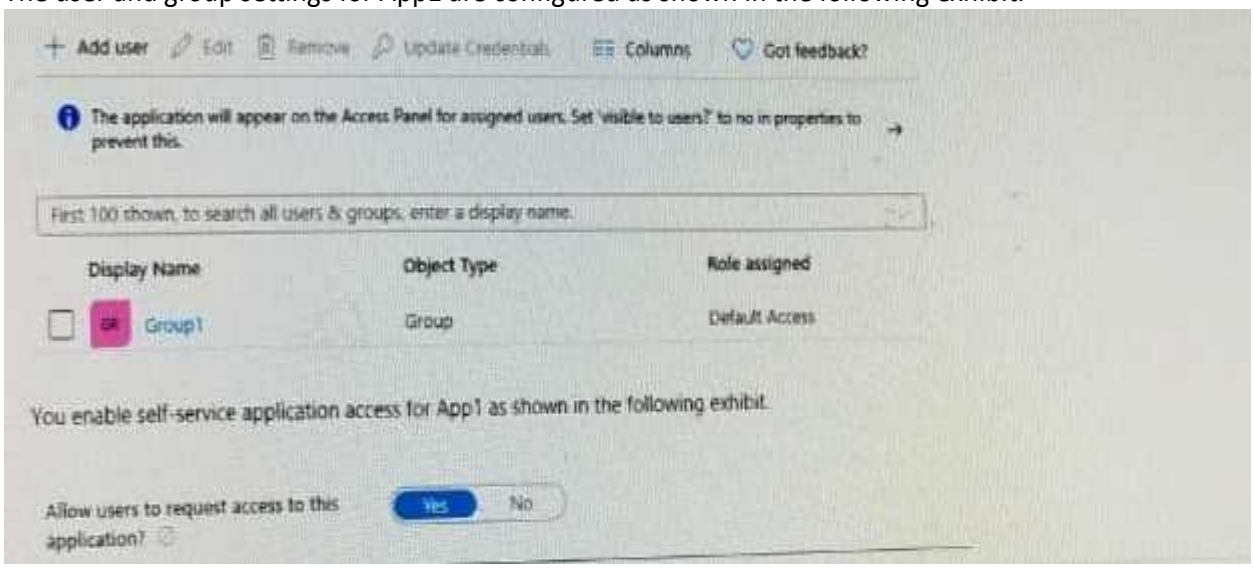
HOTSPOT

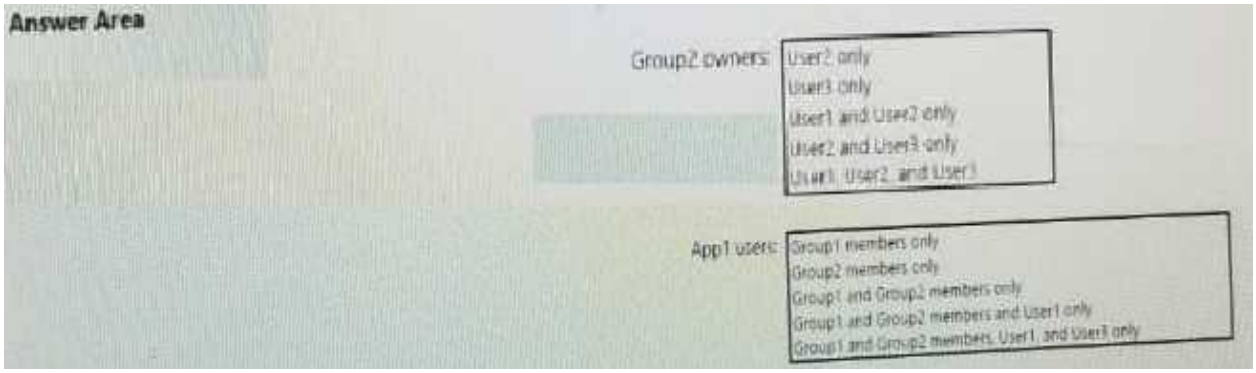
You have an azure active Directory (Azure AD) tenant that contains the resources shown in the following table.

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

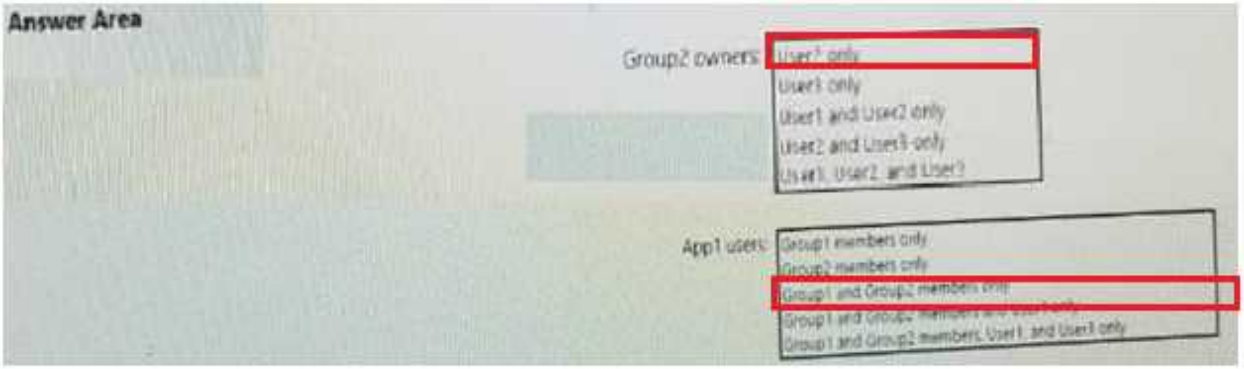
User2 is the owner of Group2.

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





Answer:



Question: 198

You have three on-premises servers named Server1, Server2, and Server3 that run Windows Server1 and Server2 and located on the Internal network. Server3 is located on the premises network. All servers have access to Azure.
From Azure Sentinel, you install a Windows firewall data connector.
You need to collect Microsoft Defender Firewall data from the servers for Azure Sentinel.
What should you do?

A. Create an event subscription from Server1, Server2 and Server3
B. Install the On-premises data gateway on each server.
C. Install the Microsoft Agent on each server.
D. Install the Microsoft Agent on Server1 and Server2 install the on-premises data gateway on Server3.

Answer: C

Question: 199

You have an Azure subscription that contains several Azure SQL databases and an Azure sentinel workspace.
You need to create a saved query in the workspace to find event reported by Advanced. Threat protection for Azure SQL Database.
What should you do?

A. From Azure CLI run the Get-AzOperationalInsightsworkspace cmdlet.
B. From the Azure SQL Database query editor, create a Transact-SQL query.
C. From the Azure Sentinel workspace, create a Custom query languages query.
D. From Microsoft SQL Server Management Studio (SSMS), create a Transact-SQL query.

Answer: C

Question: 200

HOTSPOT

You have an Azure subscription named Subcription1 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
storage1	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.

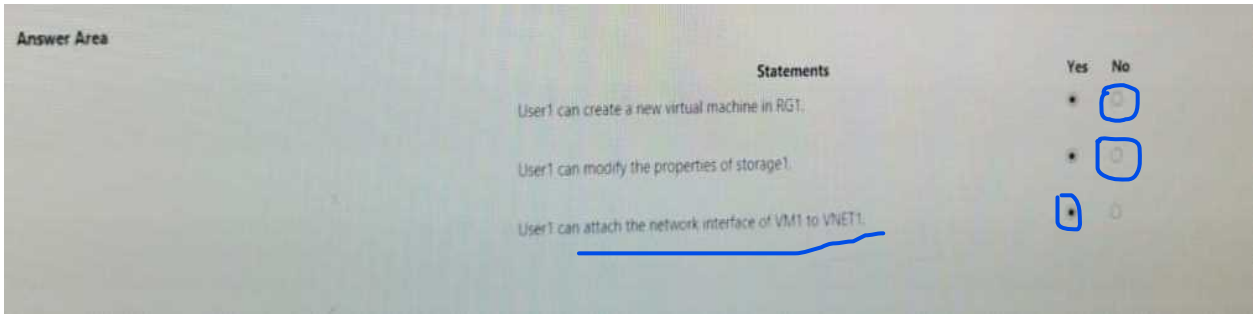
For each of the following statement, select Yes if the statement is true. Otherwise, select No.

Note: Each correct selection is worth one point.

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:



Question: 201

HOTSPOT

You have an Azure subscription named Subcription1 that contains the resources shown in the following table.

Name	Type	Description
EventHub1	Azure Event Hubs	Not applicable
Adf1	Azure Data Factory	Not applicable
NVA1	Network virtual appliance (NVA)	The NVA sends security event messages in the Common Event Format (CEF).

You have an Azure subscription named Subcription2 that contains the following resources:

- An Azure Sentinel workspace
- An Azure Event Grid instance

You need to ingest the CEF messages from the NVAs to Azure Sentinel.

NOTE: Each correct selection is worth one point.

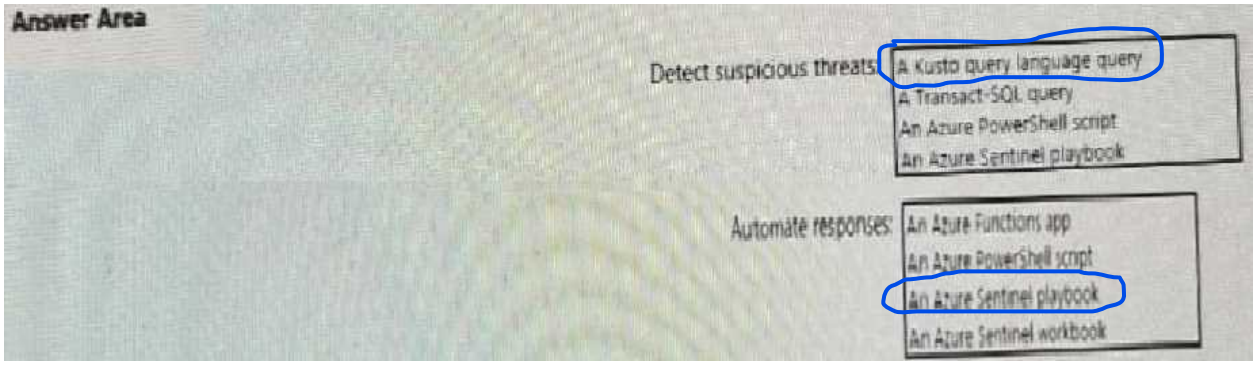
Answer:

Question: 202

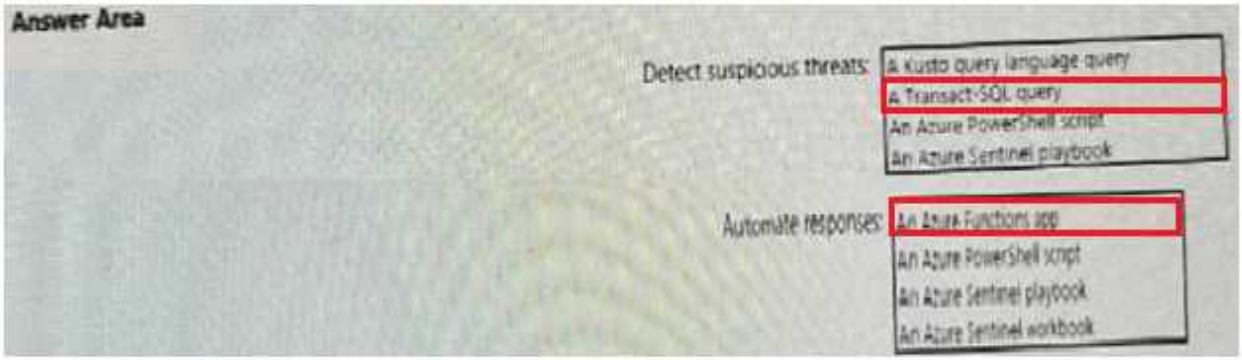
HOTSPOT

You plan to use Azure Sentinel to create an analytic rule that will detect suspicious Threats and automate responses. Which components are required for the rule? To answer, select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.



Answer:



Question: 203

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

Answer: B, C A D