

Microsoft.AZ-500.vJun-2024.by.Any.158q

Number: AZ-500  
Passing Score: 800  
Time Limit: 120  
File Version: 12.0

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



## 01 - Manage identity and access

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Overview

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

Existing Environment

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

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD

Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

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



The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com.
RG1	Resource group	RG1 is a resource group that contains VNet1, VM0, and VM1.
RG2	Resource group	RG2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Standard tier.

Requirements

Planned Changes

Litware plans to deploy the Azure resources shown in the following table.

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

#### Identity and Access Requirements

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.

The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment.

Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

#### Platform Protection Requirements

Litware identifies the following platform protection requirements:

Microsoft Antimalware must be installed on the virtual machines in RG1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.

#### Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

#### Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

WebApp1 must enforce mutual authentication.

#### General Requirements

Litware identifies the following general requirements:

Whenever possible, administrative effort must be minimized.

Whenever possible, use of automation must be maximized.



### QUESTION 1

#### HOTSPOT

You need to ensure that the Azure AD application registration and consent configurations meet the identity and access requirements. What should you use in the Azure portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

#### Hot Area:

##### Answer Area

To configure the registration settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

To configure the consent settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

#### Answer Area:

## Answer Area

To configure the registration settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

To configure the consent settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

### Section:

### Explanation:

Reference:

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

### QUESTION 2

You need to meet the identity and access requirements for Group1.

What should you do?

- A. Add a membership rule to Group1.
- B. Delete Group1. Create a new group named Group1 that has a membership type of Microsoft 365. Add users and devices to the group.
- C. Modify the membership rule of Group1.
- D. Change the membership type of Group1 to Assigned. Create two groups that have dynamic memberships. Add the new groups to Group1.

### Correct Answer: D

### Section:

### Explanation:

When you create dynamic groups, they can either contain users or devices. Hence here we need to create two separate dynamic groups and assign those groups to an Assigned group. Incorrect Answers:

A, C: You can create a dynamic group for devices or for users, but you can't create a rule that contains both users and devices.

D: For assigned group you can only add individual members.

Scenario:

Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1.

The tenant currently contain this group:

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

References:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership>

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal>

## 02 - Manage identity and access

### Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company hosts its entire server infrastructure in Azure.

Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

Existing Environment

Azure AD

Contoso.com contains the users shown in the following table.

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	None
User9	Sydney	Owner

Contoso.com contains the security groups shown in the following table.

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	user.city -contains "ON"
Group2	Dynamic user	user.city -match "*on"

Sub1

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

User9 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

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

Sub1 contains the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2

Sub2 contains the virtual networks shown in the following table.



Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

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

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

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

Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

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

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

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

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

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

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG4 has the inbound security rules shown in the following table.

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

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

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

Technical requirements

Contoso identifies the following technical requirements:

Deploy Azure Firewall to VNetwork1 in Sub2.

Register an application named App2 in contoso.com.



Whenever possible, use the principle of least privilege.  
Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

#### QUESTION 1

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

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

**Correct Answer: A**

**Section:**

**Explanation:**

To start using PIM in your directory, you must first enable PIM.

1. Sign in to the Azure portal as a Global Administrator of your directory.

You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory. Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com

References:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started>

#### 01 - Implement platform protection

This is a case study.

Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

General Overview

Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.

Existing Environment

Network Environment

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

The network contains an on-premises Active Directory domain named Fabrikam.com. The domain contains two organizational units (OUs) named OU1 and OU2. Azure AD Connect cloud sync syncs only OU1.

The Azure resources hierarchy is shown in the following exhibit.



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

Name	Type	Directory-synced	Role	Delegated to
User1	User	Yes	User	<b>None</b>
Admin1	User	No	User Access Administrator	Tenant Root Group
Admin2	User	No	Security administrator	MG1
Admin3	User	No	Contributor	Subscription1
Admin4	User	No	Owner	RG1
Group1	Group	No	<b>Not applicable</b>	<b>None</b>

Azure AD contains the resources shown in the following table.



Name	Type	Setting
CAPolicy1	Conditional access policy	Users in the finance department must use multi-factor authentication (MFA) when accessing Microsoft SharePoint Online
Sentinel1	Azure Sentinel workspace	<b>Not applicable</b>
SecPol1	Azure Policy definition	Security configuration for virtual machines

Subscription1 Resources

Subscription1 contains the virtual networks shown in the following table.

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

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

Name	Location
NSG2	West US
NSG3	Central US
NSG4	West US

Subscription1 contains the virtual machines shown in the following table.

Name	Operating system	Location	Connected to	Associated NSG
VM1	Windows Server 2019	West US	VNET1/Subnet1	<b>None</b>
VM2	CentOS-based 8.2	West US	VNET1/Subnet2	NSG2
VM3	Windows Server 2016	Central US	VNET2/Subnet1	NSG3
VM4	Ubuntu Server 18.04 LTS	West US	VNET3/Subnet1	NSG4

Subscription1 contains the Azure key vaults shown in the following table.

Name	Location	Pricing tier	Private endpoint
KeyVault1	West US	Standard	VNET1/Subnet1
KeyVault2	Central US	Premium	<b>None</b>
KeyVault3	East US	Premium	VNET1/Subnet1, VNET2/Subnet1, VNET3/Subnet1

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

Planned Changes and Requirements

Planned Changes

Fabrikam plans to implement the following changes:

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



Name	Location
ASG1	West US
ASG2	Central US

Associate the network interface of VM1 to ASG1.

Deploy SecPol1 by using Azure Security Center.

Deploy a third-party app named App1. A version of App1 exists for all available operating systems.

Create a resource group named RG2.

Sync OU2 to Azure AD.

Add User1 to Group1.

Technical Requirements

Fabrikam identifies the following technical requirements:

The finance department users must reauthenticate after three hours when they access SharePoint Online. Storage1 must be encrypted by using customer-managed keys and automatic key rotation.

From Sentinel1, you must ensure that the following notebooks can be launched:

- Entity Explorer – Account

- Entity Explorer – Windows Host

- Guided Investigation Process Alerts

VM1, VM2, and VM3 must be encrypted by using Azure Disk Encryption.

Just in time (JIT) VM access for VM1, VM2, and VM3 must be enabled.

App1 must use a secure connection string stored in KeyVault1.

KeyVault1 traffic must NOT travel over the internet.

#### QUESTION 1

You plan to implement JIT VM access.

Which virtual machines will be supported?

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

**Correct Answer: C**

**Section:**

#### QUESTION 2

You plan to configure Azure Disk Encryption for VM4.

Which key vault can you use to store the encryption key?

- A. KeyVault1
- B. KeyVault2
- C. KeyVault3

**Correct Answer: A**

**Section:**

**Explanation:**

The key vault needs to be in the same subscription and same region as the VM.

VM4 is in West US. KeyVault1 is the only key vault in the same region as the VM.

Reference: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault>



**QUESTION 3**

You need to encrypt storage1 to meet the technical requirements.  
Which key vaults can you use?

- A. KeyVault2 and KeyVault3 only
- B. KeyVault1 only
- C. KeyVault1 and KeyVault3 only
- D. KeyVault1, KeyVault2, and KeyVault3

**Correct Answer: A**

**Section:**

**Explanation:**

**QUESTION 4**

HOTSPOT

You implement the planned changes for ASG1 and ASG2.

In which NSGs can you use ASG1, and the network interfaces of which virtual machines can you assign to ASG2?

**Hot Area:**

**Answer Area**

NSGs:  ▼

NSG2 only
NSG2 and NSG4 only
NSG2, NSG3, and NSG4

Virtual machines:  ▼

VM3 only
VM2 and VM4 only
VM1, VM2, and VM4 only
VM2, VM3, and VM4 only
VM1, VM2, VM3, and VM4

**Answer Area:**



**Answer Area**

NSGs:  ▼

- NSG2 only
- NSG2 and NSG4 only
- NSG2, NSG3, and NSG4

Virtual machines:  ▼

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

**Section:**

**Explanation:**

**02 - Implement platform protection**

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Overview

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

Existing Environment

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

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

The tenant contains the groups shown in the following table.

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

The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com.
RG1	Resource group	RG1 is a resource group that contains VNet1, VM0, and VM1.
RG2	Resource group	RG2 is a resource group that contains shared IT resources.

#### Identity and Access Requirements

Azure Security Center is set to the Standard tier.

#### Requirements

#### Planned Changes

Litware plans to deploy the Azure resources shown in the following table.



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

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.

The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment. Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

#### Platform Protection Requirements

Litware identifies the following platform protection requirements:

Microsoft Antimalware must be installed on the virtual machines in RG1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access. A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.

#### Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center. Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

WebApp1 must enforce mutual authentication.

General Requirements

Litware identifies the following general requirements:

Whenever possible, administrative effort must be minimized.

Whenever possible, use of automation must be maximized.

**QUESTION 1**

**HOTSPOT**

You need to deploy Microsoft Antimalware to meet the platform protection requirements.

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

NOTE: Each correct selection is worth one point.

**Hot Area:**

**Answer Area**

Create a custom policy definition that has effect set to:

▼

Append
Deny
DeployIfNotExists

Create a policy assignment and modify:

▼

The Create a Managed Identify setting
The exclusion settings
The scope

**Answer Area:**

**Answer Area**

Create a custom policy definition that has effect set to:

▼

Append
Deny
DeployIfNotExists

Create a policy assignment and modify:

▼

The Create a Managed Identify setting
The exclusion settings
The scope

**Section:**

**Explanation:**

Scenario: Microsoft Antimalware must be installed on the virtual machines in RG1.

RG1 is a resource group that contains Vnet1, VM0, and VM1.

Box 1: DeployIfNotExists

DeployIfNotExists executes a template deployment when the condition is met.

Azure policy definition Antimalware

Incorrect Answers:

Append:

Append is used to add additional fields to the requested resource during creation or update. A common example is adding tags on resources such as costCenter or specifying allowed IPs for a storage resource.

Deny:

Deny is used to prevent a resource request that doesn't match defined standards through a policy definition and fails the request.

Box 2: The Create a Managed Identity setting

When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity. Azure Policy creates a managed identity for each assignment, but must have details about what roles to grant the managed identity.

Reference:

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

## QUESTION 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.

**Correct Answer: A**

**Section:**

**Explanation:**

Azure Firewall has the following known issue:

Conflict with Azure Security Center (ASC) Just-in-Time (JIT) feature.

If a virtual machine is accessed using JIT, and is in a subnet with a user-defined route that points to Azure Firewall as a default gateway, ASC JIT doesn't work. This is a result of asymmetric routing – a packet comes in via the virtual machine public IP (JIT opened the access), but the return path is via the firewall, which drops the packet because there is no established session on the firewall.

Solution: To work around this issue, place the JIT virtual machines on a separate subnet that doesn't have a user-defined route to the firewall.

Scenario:

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

DRAG DROP

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

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

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

**Select and Place:**

**Actions**

- Deploy an AKS cluster.
- Create a client application.
- Create a server application.
- Create an RBAC binding.
- Create a custom RBAC role.

**Answer Area**

**Correct Answer:**

**Actions**

- 
- 
- 
- 
- Create a custom RBAC role.

**Answer Area**

Create a server application.

Create a client application.

Deploy an AKS cluster.

Create an RBAC binding.



**Section:**

**Explanation:**

Scenario: Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.

Litewire plans to deploy AKS1, which is a managed AKS (Azure Kubernetes Services) cluster.

Step 1: Create a server application

To provide Azure AD authentication for an AKS cluster, two Azure AD applications are created. The first application is a server component that provides user authentication.

Step 2: Create a client application

The second application is a client component that's used when you're prompted by the CLI for authentication. This client application uses the server application for the actual authentication of the credentials provided by the client.

Step 3: Deploy an AKS cluster.

Use the az group create command to create a resource group for the AKS cluster.

Use the az aks create command to deploy the AKS cluster.

Step 4: Create an RBAC binding.

Before you use an Azure Active Directory account with an AKS cluster, you must create role-binding or cluster role-binding. Roles define the permissions to grant, and bindings apply them to desired users. These assignments can be applied to a given namespace, or across the entire cluster.



Reference:

<https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration>

### 03 - Implement platform protection

#### Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

#### Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company hosts its entire server infrastructure in Azure.

Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

#### Existing Environment

##### Azure AD

Contoso.com contains the users shown in the following table.

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	None
User9	Sydney	Owner

Contoso.com contains the security groups shown in the following table.

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	<code>user.city -contains "ON"</code>
Group2	Dynamic user	<code>user.city -match "*on"</code>

##### Sub1

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

User9 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

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

Sub1 contains the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2

Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

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

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

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

Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

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



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

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

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

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

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG4 has the inbound security rules shown in the following table.

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

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

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

Technical requirements

Contoso identifies the following technical requirements:

Deploy Azure Firewall to VNetwork1 in Sub2.

Register an application named App2 in contoso.com.

Whenever possible, use the principle of least privilege.

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

## QUESTION 1

HOTSPOT

You are evaluating the security of the network communication between the virtual machines in Sub2.

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

NOTE: Each correct selection is worth one point.

Hot Area:



### Answer Area

#### Statements

Yes

No

From VM1, you can successfully ping the public IP address of VM2.

From VM1, you can successfully ping the private IP address of VM3.

From VM1, you can successfully ping the public IP address of VM5.

Answer Area:



### Answer Area

#### Statements

Yes

No

From VM1, you can successfully ping the public IP address of VM2.

From VM1, you can successfully ping the private IP address of VM3.

From VM1, you can successfully ping the public IP address of VM5.

Section:

Explanation:

Box 1: Yes. All traffic is allowed out to the Internet so you can ping the public IP.

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

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

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

dumps

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

Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

Box 3: No (because VM5 is in a separate VNet).

Note: Sub2 contains the virtual machines shown in the following table.

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

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21



## QUESTION 2

### HOTSPOT

You are evaluating the effect of the application security groups on the network communication between the virtual machines in Sub2.

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

NOTE: Each correct selection is worth one point.

### Hot Area:

Answer area	Statements	Yes	No
	From VM1, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input type="radio"/>
	From VM2, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input type="radio"/>
	From VM1, you can connect to the web server on VM4.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer area	Statements	Yes	No
	From VM1, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input checked="" type="radio"/>
	From VM2, you can successfully ping the private IP address of VM4.	<input checked="" type="radio"/>	<input type="radio"/>
	From VM1, you can connect to the web server on VM4.	<input checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

Box 1: No. VM4 is in Subnet13 which has NSG3 attached to it.

VM1 is in ASG1. NSG3 would only allow ICMP pings from ASG2 but not ASG1. Only TCP traffic is allowed from ASG1.

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

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

Box 2: Yes.

VM2 is in ASG2. Any protocol is allowed from ASG2 so ICMP ping would be allowed.

Box3. VM1 is in ASG1. TCP traffic is allowed from ASG1 so VM1 could connect to the web server as connections to the web server would be on ports TCP 80 or TCP 443.

### QUESTION 3

You need to meet the technical requirements for VNetwork1.

What should you do first?

- A. Create a new subnet on VNetwork1.
- B. Remove the NSGs from Subnet11 and Subnet13.
- C. Associate an NSG to Subnet12.
- D. Configure DDoS protection for VNetwork1.

Correct Answer: A

**Section:**

**Explanation:**

From scenario: Deploy Azure Firewall to VNetwork1 in Sub2.

Azure firewall needs a dedicated subnet named AzureFirewallSubnet.

References:

<https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal>

**QUESTION 4**

**HOTSPOT**

You are evaluating the security of VM1, VM2, and VM3 in Sub2.

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

NOTE: Each correct selection is worth one point.

**Hot Area:**

**Answer area**

	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	<input type="radio"/>	<input type="radio"/>
From the Internet, you can connect to the web server on VM2 by using HTTP.	<input type="radio"/>	<input type="radio"/>
From the Internet, you can connect to the web server on VM3 by using HTTP.	<input type="radio"/>	<input type="radio"/>

**Answer Area:**

**Answer area**

	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	<input checked="" type="radio"/>	<input type="radio"/>
From the Internet, you can connect to the web server on VM2 by using HTTP.	<input type="radio"/>	<input checked="" type="radio"/>
From the Internet, you can connect to the web server on VM3 by using HTTP.	<input checked="" type="radio"/>	<input type="radio"/>

**Section:**

**Explanation:**

VM1: Yes. NSG2 applies to VM1 and this allows inbound traffic on port 80.

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

**QUESTION 5**

HOTSPOT

What is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Group1: 

	▼
No members	
Only User2	
Only User2 and User4	
User1, User2, User3, and User4	

Group2: 

	▼
No members	
Only User3	
Only User1 and User3	
User1, User2, User3, and User4	

Answer Area:

Answer Area

Group1: 

	▼
No members	
Only User2	
Only User2 and User4	
User1, User2, User3, and User4	

Group2: 

	▼
No members	
Only User3	
Only User1 and User3	
User1, User2, User3, and User4	

Section:

Explanation:

Box 1: User1, User2, User3, User4

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

Box 2: Only User3

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

Scenario:

Contoso.com contains the users shown in the following table.





Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	None

Contoso.com contains the security groups shown in the following table.

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	user.city -contains "ON"
Group2	Dynamic user	user.city -match "*on"

References:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership>

#### 04 - Implement platform protection

##### QUESTION 1

HOTSPOT

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

 Vdumps

**Answer Area**

Update1:  ▼

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

Update2:  ▼

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

Answer Area:

**Answer Area**

Update1:  ▼

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

Update2:  ▼

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

Section:  
Explanation:



Update1: VM1 and VM2 only

VM3: Windows Server 2016 West US RG2

Update2: VM4 and VM5 only

VM6: CentOS 7.5 East US RG1

For Linux, the machine must have access to an update repository. The update repository can be private or public.

References:

<https://docs.microsoft.com/en-us/azure/automation/automation-update-management>

## QUESTION 2

### HOTSPOT

You have an Azure subscription named Sub1.

You create a virtual network that contains one subnet. On the subnet, you provision the virtual machines shown in the following table.

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

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

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

Allow traffic to VM4 from VM3 only.

Allow traffic from the Internet to VM1 and VM2 only.

Minimize the number of NSGs and network security rules.

How many NSGs and network security rules should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



NSGs:

1
2
3
4

Network security rules:

1
2
3
4

Answer Area:

NSGs:

	▼
1	
2	
3	
4	



Network security rules:

	▼
1	
2	
3	
4	



**Section:**

**Explanation:**

NSGs: 2

Network security rules: 3

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

References:

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



**QUESTION 3**

**HOTSPOT**

You have an Azure key vault.

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

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

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

Use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

**Hot Area:**

**Answer Area**  
CEplus.com

User1:  ▼

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

User2:  ▼

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



Answer Area:

User1:  ▼

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

User2:  ▼

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



**Section:**

**Explanation:**

User1: RBAC

RBAC is used as the Key Vault access control mechanism for the management plane. It would allow a user with the proper identity to:

- set Key Vault access policies
- create, read, update, and delete key vaults
- set Key Vault tags

Note: Role-based access control (RBAC) is a system that provides fine-grained access management of Azure resources. Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs.

User2: A key vault access policy

A key vault access policy is the access control mechanism to get access to the key vault data plane. Key Vault access policies grant permissions separately to keys, secrets, and certificates.

References:

<https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault>

**QUESTION 4**

You have an Azure virtual machine named VM1.

From Azure Security Center, you get the following high-severity recommendation: "Install endpoint protection solutions on virtual machine".

You need to resolve the issue causing the high-severity recommendation.

What should you do?

- A. Add the Microsoft Antimalware extension to VM1.
- B. Install Microsoft System Center Security Management Pack for Endpoint Protection on VM1.
- C. Add the Network Watcher Agent for Windows extension to VM1.
- D. Onboard VM1 to Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

**Correct Answer: A**

**Section:**

**Explanation:**

Reference:

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

**QUESTION 5**

HOTSPOT

You have a file named File1.yaml that contains the following contents.

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

You create an Azure container instance named container1 by using File1.yaml.

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

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

NOTE: Each correct selection is worth one point.

**Hot Area:**



## Answer Area

Variable1: 

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

Variable2: 

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

Answer Area:

## Answer Area

Variable1: 

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

Variable2: 

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

Section:

Explanation:

Reference:

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

### QUESTION 6

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



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

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

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

You enable just in time (JIT) VM access for all the virtual machines.

You need to identify which virtual machines are protected by JIT.

Which virtual machines should you identify?

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

**Correct Answer: C**

**Section:**

**Explanation:**

An NSG needs to be enabled, either at the VM level or the subnet level.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time>



## QUESTION 7

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.

Save Discard Refresh

Allow access from

All networks Selected networks

Configure network security for your storage accounts. [Learn more.](#)

Virtual networks

Secure your storage account with virtual networks. [+ Add existing virtual network](#)

[+ Add new virtual network](#)

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIPTION
-----------------	--------	---------------	-----------------	----------------	--------------

No network selected.

Firewall

Add IP ranges to allow access from the internet on your on-premises networks. [Learn more.](#)

Address Range

13.80.73.87



IP address or CIDR

Exceptions

Allow trusted Microsoft services to access this storage account ⓘ

Allow read access to storage logging from any network

Allow read access to storage metrics from any network

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

Hot Area:

**Answer Area**

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>
From VM2, you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>
From VM3 , you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>

Answer Area:



## Answer Area

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
From VM2, you can upload a blob to storageacc1.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
From VM3 , you can upload a blob to storageacc1.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

### Section:

### Explanation:

Box 1: Yes

The public IP of VM1 is allowed through the firewall.

Box 2: No

The allowed virtual network list is empty so VM2 cannot access storageacc1 directly. The public IP address of VM2 is not in the allowed IP list so VM2 cannot access storageacc1 over the Internet.

Box 3: No

The allowed virtual network list is empty so VM3 cannot access storageacc1 directly. VM3 does not have a public IP address so it cannot access storageacc1 over the Internet.

Reference:

<https://docs.microsoft.com/en-gb/azure/storage/common/storage-network-security>

### QUESTION 8

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

You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.

What should you use?

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

**Correct Answer: B**

### Section:

### Explanation:

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

### QUESTION 9

#### HOTSPOT

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

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

You deploy and configure an Azure Key vault.

You need to ensure that you can enable Azure Disk Encryption on VM1 and VM2.

What should you modify on each virtual machine? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

VM1:  ▼

The operating system version
The tier
The type

VM2:  ▼

The operating system version
The tier
The type

Answer Area:

**Answer Area**

VM1:  ▼

The operating system version
The tier
The type

VM2:  ▼

The operating system version
The tier
The type

Section:

Explanation:

VM1: The Tier

The Tier needs to be upgraded to standard.



Disk Encryption for Windows and Linux IaaS VMs is in General Availability in all Azure public regions and Azure Government regions for Standard VMs and VMs with Azure Premium Storage.

VM2: The type

Need to change the VMtype to any of A, D, DS, G, GS, F, and so on, series IaaS VMs.

Not the operating system version: Ubuntu 16.04 is supported.

References:

<https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview>

[https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-faq#bkmk\\_LinuxOSSupport](https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-faq#bkmk_LinuxOSSupport)

#### QUESTION 10

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.

You need to deploy Microsoft Antimalware to the virtual machines.

Solution: You add an extension to each virtual machine.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: A**

**Section:**

**Explanation:**

You can use Visual Studio to enable and configure the Microsoft Antimalware service. This entails selecting Microsoft Antimalware extension from the dropdown list under Installed Extensions and click Add to configure with default antimalware configuration.

References:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware>

#### QUESTION 11

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.

You need to deploy Microsoft Antimalware to the virtual machines.

Solution: You connect to each virtual machine and add a Windows feature.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

**Section:**

**Explanation:**

Microsoft Antimalware is deployed as an extension and not a feature.

References:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware>

#### QUESTION 12

You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1. You create a service endpoint for Subnet1.

Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 18.04.

You need to deploy Docker containers to VM1. The containers must be able to access Azure Storage resources and Azure SQL databases by using the service endpoint. What should you do on VM1 before you deploy the container?

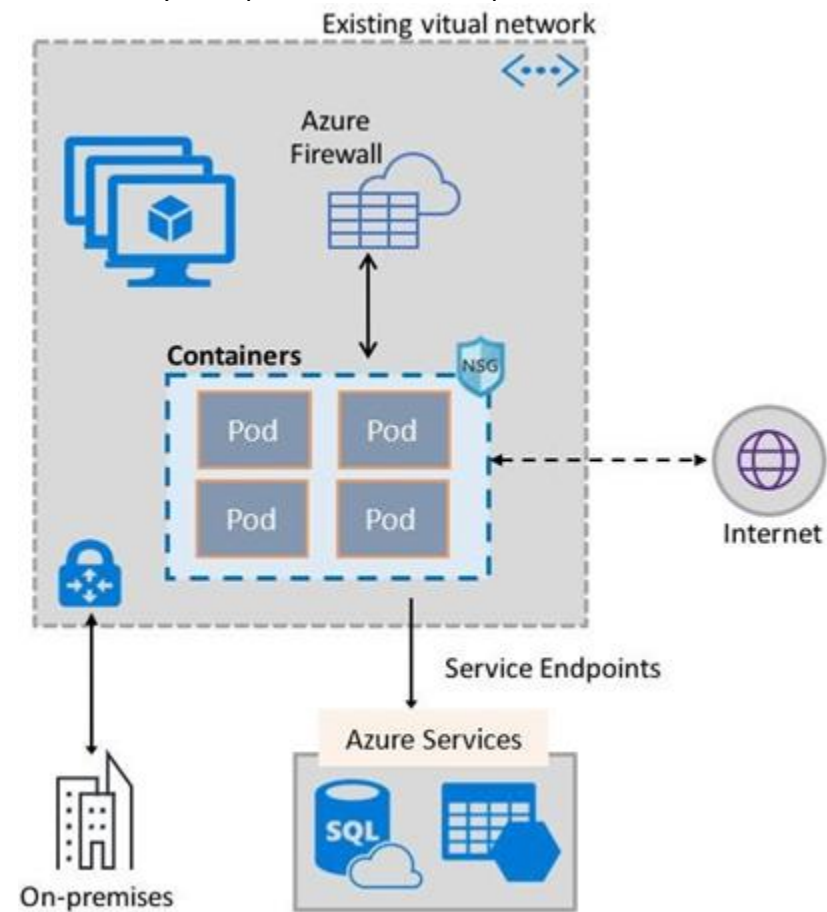
- A. Create an application security group and a network security group (NSG).
- B. Edit the docker-compose.yml file.
- C. Install the container network interface (CNI) plug-in.

**Correct Answer: C**

**Section:**

**Explanation:**

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



References:

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

### QUESTION 13

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

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

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



**Correct Answer: B**

**Section:**

**Explanation:**

The primary use case for the Azure Desired State Configuration (DSC) extension is to bootstrap a VM to the Azure Automation State Configuration (DSC) service. The service provides benefits that include ongoing management of the VM configuration and integration with other operational tools, such as Azure Monitoring. Using the extension to register VM's to the service provides a flexible solution that even works across Azure subscriptions.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview>

**QUESTION 14**

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

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

**Correct Answer: B**

**Section:**

**Explanation:**

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



**QUESTION 15**

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

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

You create an Azure Log Analytics workspace named Analytics1 in RG1 in the East US region.

Which virtual machines can be enrolled in Analytics1?

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

**Correct Answer: A**

**Section:**

**Explanation:**

Note: Create a workspace

In the Azure portal, click All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics. Click Create, and then select choices for the following items:

Provide a name for the new Log Analytics workspace, such as DefaultLAWorkspace. OMS workspaces are now referred to as Log Analytics workspaces. Select a Subscription to link to by selecting from the drop-down list if the default selected is not appropriate. For Resource Group, select an existing resource group that contains one or more Azure virtual machines. Select the Location your VMs are deployed to. For additional information, see

which regions Log Analytics is available in. Incorrect Answers:

B, C: A Log Analytics workspace provides a geographic location for data storage. VM2 and VM3 are at a different location. D: VM4 is a different resource group.

References: <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-access>

#### QUESTION 16

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.



**Correct Answer: A**

**Section:**

**Explanation:**

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

#### QUESTION 17

DRAG DROP

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

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

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

You plan to deploy an Azure firewall to HubVNet.



You create the following two routing tables:

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

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

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

NOTE: Each correct selection is worth one point.

Select and Place:

**Subnets**

AzureFirewallSubnet

GatewaySubnet

SpokeVNetSubnet0

**Answer Area**

RT1:

RT2:

Correct Answer:

**Subnets**

AzureFirewallSubnet

**Answer Area**

RT1:

RT2:

**Section:**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/firewall/tutorial-hybrid-portal#create-the-routes>

**QUESTION 18**

HOTSPOT

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

Hot Area:

Answer Area

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

Append  
Deny  
DeployIfNotExists

existenceCondition  
resources  
template

Answer Area:

**Answer Area**

CEplus.com

```

{
  "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           |


            ": {
          }
        }
      }
    }
  }
}

```

CEplus.com

Q&A dumps

CEplus.com

**Section:**

**Explanation:**

Box 1: DeployIfNotExists

DeployIfNotExists executes a template deployment when the condition is met.

Box 2: Template

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

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

References:

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

**QUESTION 19**

HOTSPOT

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

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

You create the Azure policies shown in the following table.

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

You create the resource locks shown in the following table.

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

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



NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
You can start VM1.	<input type="radio"/>	<input type="radio"/>
You can start VM2.	<input type="radio"/>	<input type="radio"/>
You can create a virtual machine in RG2.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Statements	Yes	No
You can start VM1. 	<input type="radio"/>	<input checked="" type="radio"/>
You can start VM2.	<input checked="" type="radio"/>	<input type="radio"/>
You can create a virtual machine in RG2. 	<input checked="" type="radio"/>	<input type="radio"/>

**Section:**

**Explanation:**

References:

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

#### QUESTION 20

From Azure Security, you create a custom alert rule.

You need to configure which users will receive an email message when the alert is triggered.

What should you do?

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

**Correct Answer: A**

**Section:**

**Explanation:**

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups>

#### QUESTION 21

You are configuring and securing a network environment.

You deploy an Azure virtual machine named VM1 that is configured to analyze network traffic.

You need to ensure that all network traffic is routed through VM1.

What should you configure?

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

**Correct Answer: C**

**Section:**

**Explanation:**

Although the use of system routes facilitates traffic automatically for your deployment, there are cases in which you want to control the routing of packets through a virtual appliance. You can do so by creating user defined routes that specify the next hop for packets flowing to a specific subnet to go to your virtual appliance instead, and enabling IP forwarding for the VM running as the virtual appliance.

Note: User Defined Routes

For most environments you will only need the system routes already defined by Azure. However, you may need to create a route table and add one or more routes in specific cases, such as:

Force tunneling to the Internet via your on-premises network.

Use of virtual appliances in your Azure environment.

In the scenarios above, you will have to create a route table and add user defined routes to it.

Reference:

<https://github.com/uglide/azure-content/blob/master/articles/virtual-network/virtual-networks-udr-overview.md>

#### QUESTION 22

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

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

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

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

On NIC1, you configure an application security group named ASG1.

On which other network interfaces can you configure ASG1?

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

**Correct Answer: C**

**Section:**

**Explanation:**

Only network interfaces in VNET1, 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 23

You have 15 Azure virtual machines in a resource group named RG1.

All virtual machines run identical applications.

You need to prevent unauthorized applications and malware from running on the virtual machines.

What should you do?



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

**Correct Answer: B**

**Section:**

**Explanation:**

Adaptive application control is an intelligent, automated end-to-end application whitelisting solution from Azure Security Center. It helps you control which applications can run on your Azure and non-Azure VMs (Windows and Linux), which, among other benefits, helps harden your VMs against malware. Security Center uses machine learning to analyze the applications running on your VMs and helps you apply the specific whitelisting rules using this intelligence.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application>

**QUESTION 24**

You plan to deploy Azure container instances.

You have a containerized application that validates credit cards. The application is comprised of two containers: an application container and a validation container.

The application container is monitored by the validation container. The validation container performs security checks by making requests to the application container and waiting for responses after every transaction.

You need to ensure that the application container and the validation container are scheduled to be deployed together. The containers must communicate to each other only on ports that are not externally exposed.

What should you include in the deployment?

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



**Correct Answer: D**

**Section:**

**Explanation:**

Azure Container Instances supports the deployment of multiple containers onto a single host using a container group. A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process.

Reference:

<https://docs.microsoft.com/en-us/azure/container-instances/container-instances-container-groups>

**QUESTION 25**

**HOTSPOT**

You create resources in an Azure subscription as shown in the following table.

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

VNET1 contains two subnets named Subnet1 and Subnet2. Subnet1 has a network ID of 10.0.0.0/24. Subnet2 has a network ID of 10.1.1.0/24.

Contoso1901 is configured as shown in the exhibit. (Click the Exhibit tab.)

```
PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet
ByPass          : Logging, Metrics
DefaultAction   : Deny
IpRules         : [193.77.0.0/16,...]
VirtualNetworkRules : [/subscriptions/a90c8c8f-d8bc-4112-abfb-
                    dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/
                    virtualNetworks/VNET1/subnets/Subnet1,...]

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

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRules
Action VirtualNetworkResourceId          State
-----
Allow  /subscriptions/a90c8c8f-d8bc-4112-abfb dac4906573dd/resourceGroups/
                    RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1 Succeeded

PS C:\> _
```

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

Hot Area:

Answer area

Statements	Yes	No
An Azure virtual machine on Subnet1 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>
An Azure virtual machine on Subnet2 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>

Answer Area:



**Answer area**

Statements	Yes	No
An Azure virtual machine on Subnet1 can access data in Contoso1901.	<input checked="" type="radio"/>	<input type="radio"/>
An Azure virtual machine on Subnet2 can access data in Contoso1901.	<input type="radio"/>	<input checked="" type="radio"/>
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	<input checked="" type="radio"/>	<input type="radio"/>

**Section:**

**Explanation:**

Box 1: Yes

Access from Subnet1 is allowed.

Box 2: No

No access from Subnet2 is allowed.

Box 3: Yes

Access from IP address 193.77.10.2 is allowed.



**QUESTION 26**

**DRAG DROP**

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

You need to implement VPN gateways for the virtual networks to meet the following requirements:

VNET1 must have six site-to-site connections that use BGP.

VNET2 must have 12 site-to-site connections that use BGP.

Costs must be minimized.

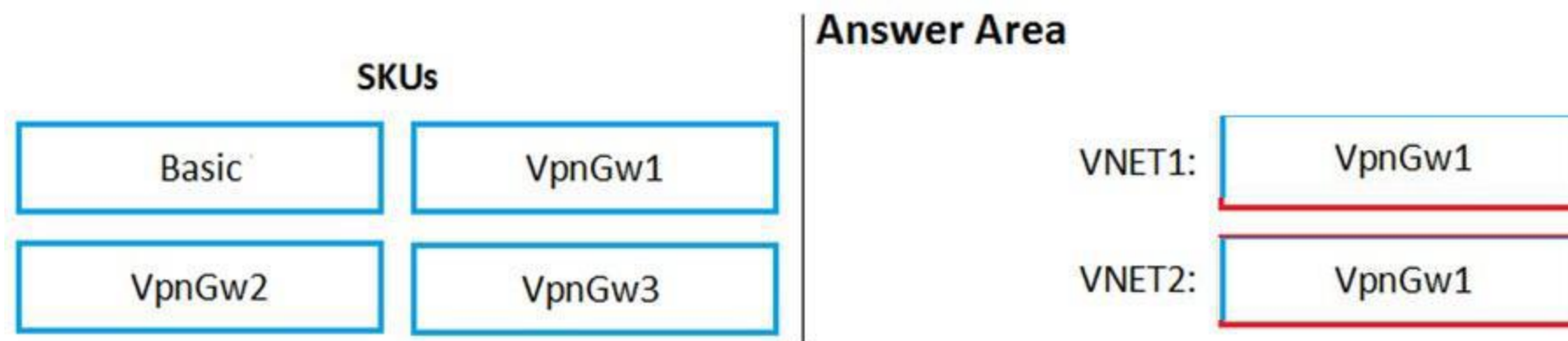
Which VPN gateway SKU should you use for each virtual network? To answer, drag the appropriate SKUs to the correct networks. Each SKU may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

**Select and Place:**

SKUs		Answer Area
Basic	VpnGw1	VNET1: <input type="text"/>
VpnGw2	VpnGw3	VNET2: <input type="text"/>

**Correct Answer:**



**Section:**

**Explanation:**

References:

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

**QUESTION 27**

You are securing access to the resources in an Azure subscription.

A new company policy states that all the Azure virtual machines in the subscription must use managed disks.

You need to prevent users from creating virtual machines that use unmanaged disks.

What should you do?

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

**Correct Answer: B**

**Section:**

**QUESTION 28**

You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.

You need to use automatically generated service principal for the AKS cluster to authenticate to the Azure Container Registry.

What should you create?

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

**Correct Answer: B**

**Section:**

**Explanation:**

References:

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

**QUESTION 29**

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



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

For which virtual machine can you enable Update Management?

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

**Correct Answer: C**

**Section:**

**Explanation:**

References:

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

**QUESTION 30**

DRAG DROP

You have an Azure subscription named Sub1.

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

You need to ensure that the members of Group1 can stop, start, and restart the Azure virtual machines in Sub1. The solution must use the principle of least privilege.

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

**Select and Place:**

**Actions**

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

**Answer Area**

**Correct Answer:**

**Actions**

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

**Answer Area**

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

**Section:**

**Explanation:**

References:

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

**QUESTION 31**

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 them in the correct order.



**Select and Place:**

**Actions**

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

**Answer Area**

- 
- 
- 

**Correct Answer:**

**Actions**

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

**Answer Area**

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

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

**QUESTION 32**

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

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

**Correct Answer: C, D**

**Section:**

**Explanation:**

References:

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust>

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles>

**QUESTION 33**

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

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

Which images are trusted images?

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

**Correct Answer: B**

**Section:**

**Explanation:**

Azure Container Registry implements Docker's content trust model, enabling pushing and pulling of signed images.

To push a trusted image tag to your container registry, enable content trust and push the image with docker push.

To work with trusted images, both image publishers and consumers need to enable content trust for their Docker clients. As a publisher, you can sign the images you push to a content trust-enabled registry.

Reference:

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust>

#### **QUESTION 34**

##### **SIMULATION**

Use the following login credentials as needed:

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

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

Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168




Sign in to Microsoft Azure

https://login.microsoftonline.com/

This site uses cookies for analytics, personalized content and ads. By [more](#)

# Microsoft Azure



## 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

8:39 AM 11/15/2019 ENG

Home - Microsoft Azure x + v

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

Microsoft Azure Search resources, services, and more (0/???) 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 <sup>o</sup>  
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

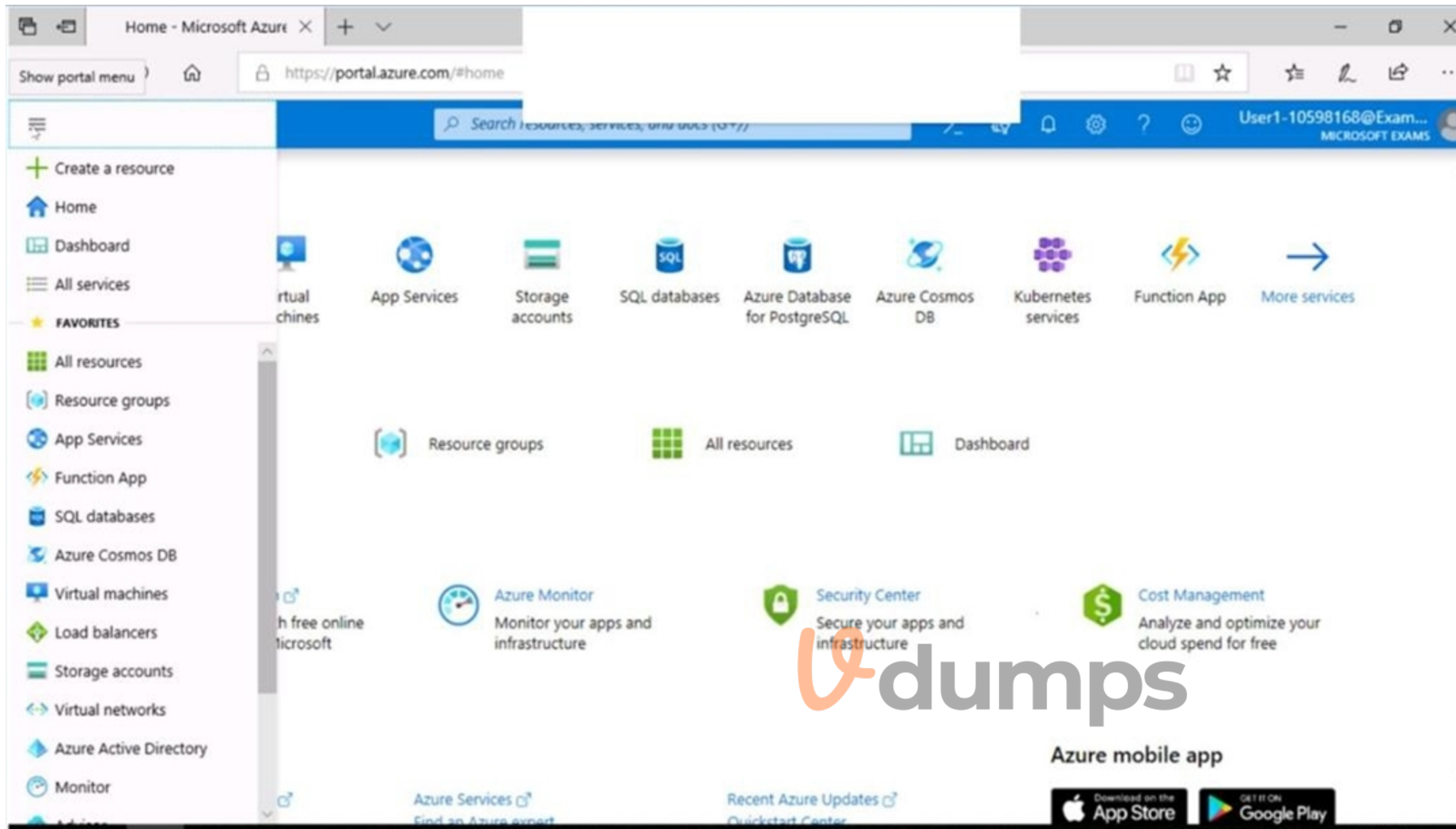
- Technical Documentation <sup>o</sup>
- Azure Migration Tools
- Azure Services <sup>o</sup>  
Find an Azure expert
- Recent Azure Updates <sup>o</sup>  
Quickstart Center

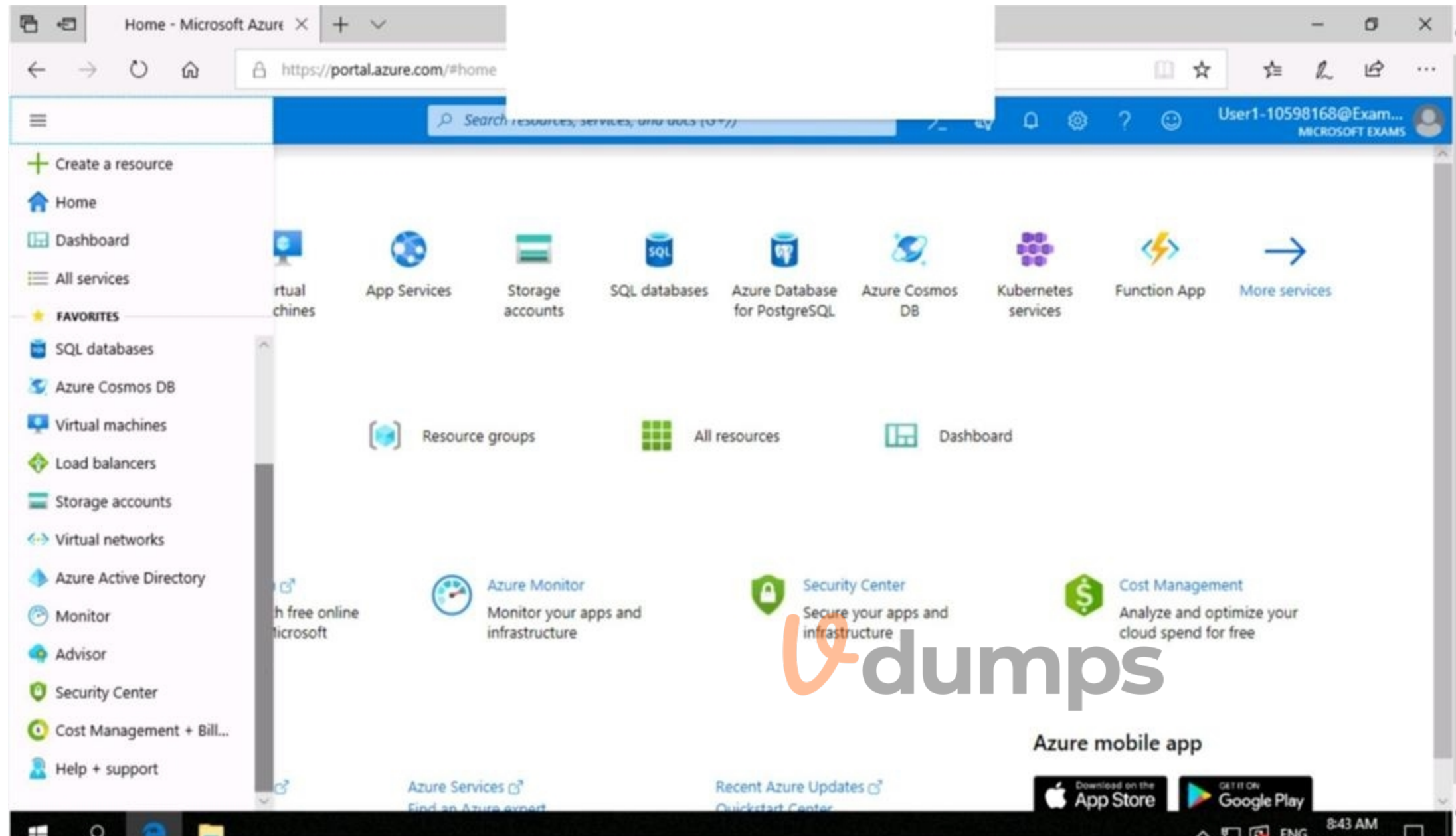
Azure mobile app

Download on the App Store | GET IT ON Google Play









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

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

To enable the RDP port in an NSG, follow these steps:

1. Sign in to the Azure portal.
2. In Virtual Machines, select VM1
3. In Settings, select Networking.
4. In Inbound port rules, check whether the port for RDP is set correctly. The following is an example of the configuration:

Priority: 300

Name: Port\_3389

Port(Destination): 3389

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

### QUESTION 35

#### 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.

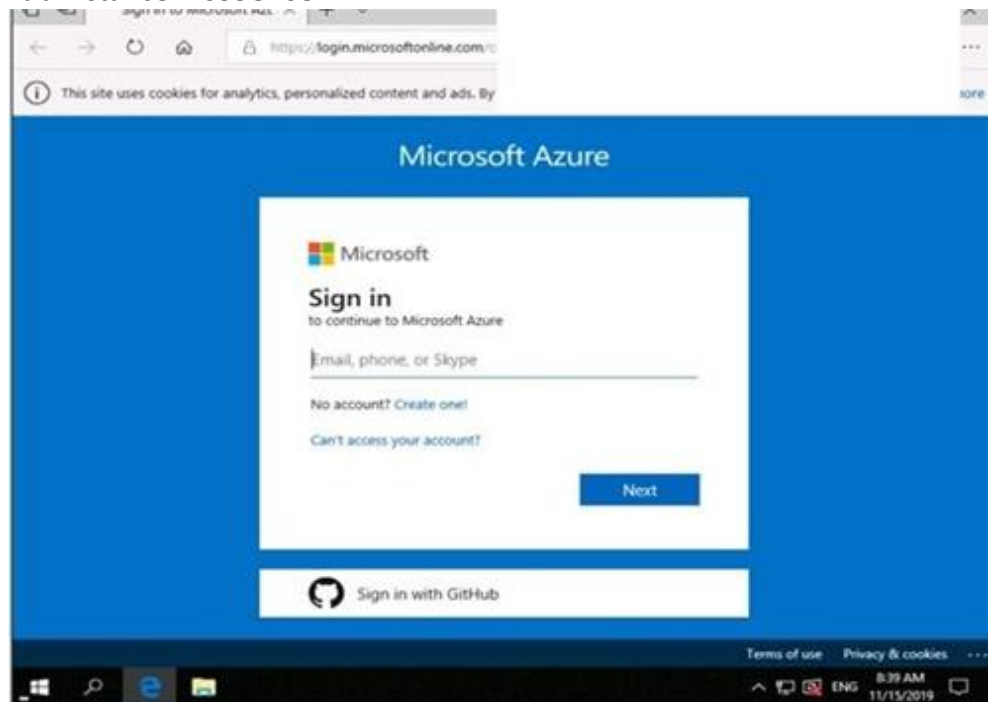
To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168



 **vdumps**

Home - Microsoft Azure x + v

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

Microsoft Azure Search Resources, services, and more (0/??)

User1-10598168@Exam... MICROSOFT EXAMS

### Azure services

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

### Navigate

- Subscriptions
- Resource groups
- All resources
- Dashboard

### Tools


- Microsoft Learn [Learn Azure with free online training from Microsoft](#)
- Azure Monitor [Monitor your apps and infrastructure](#)
- Security Center [Secure your apps and infrastructure](#)
- Cost Management [Analyze and optimize your cloud spend for free](#)

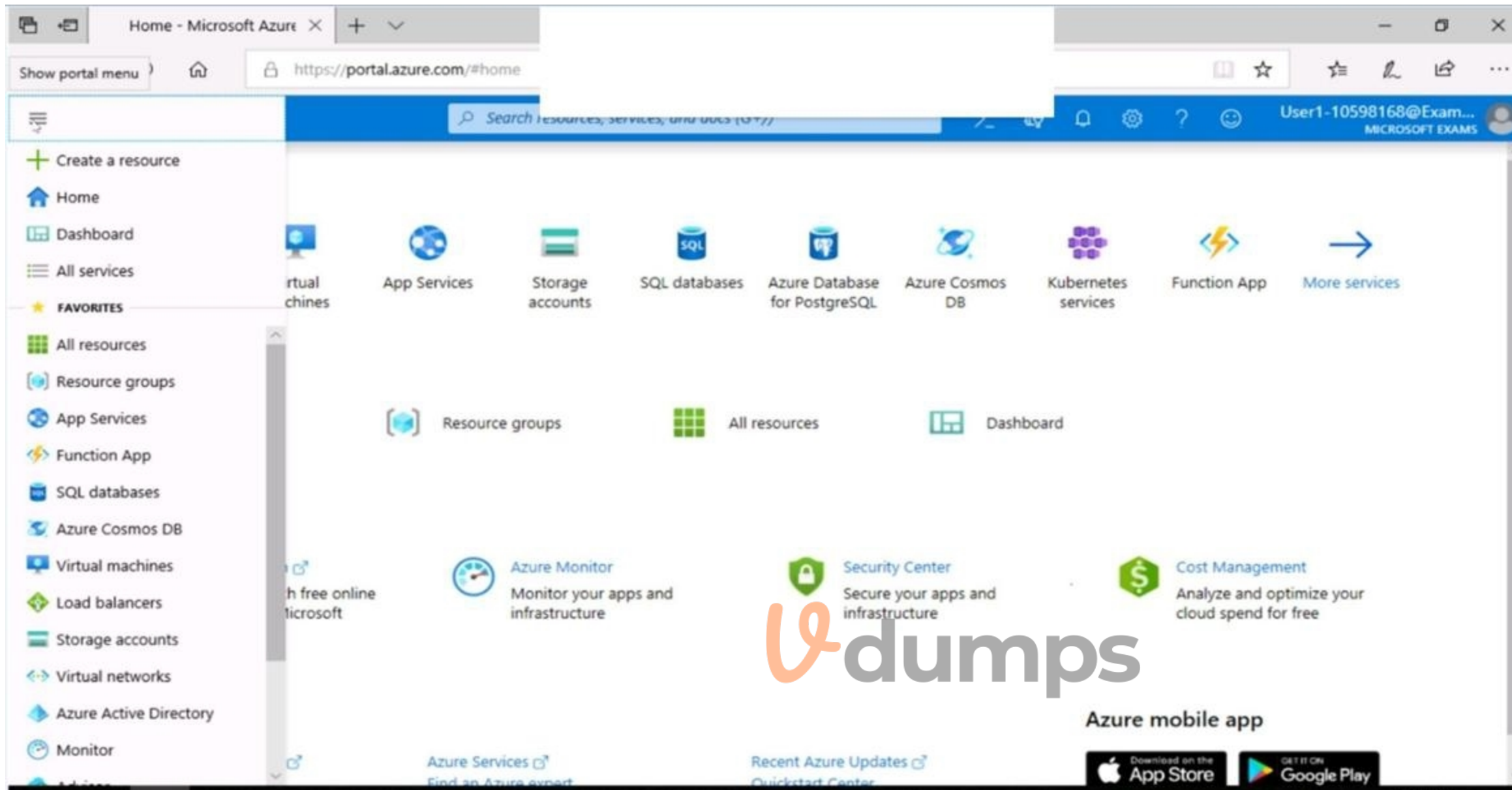
### Useful links

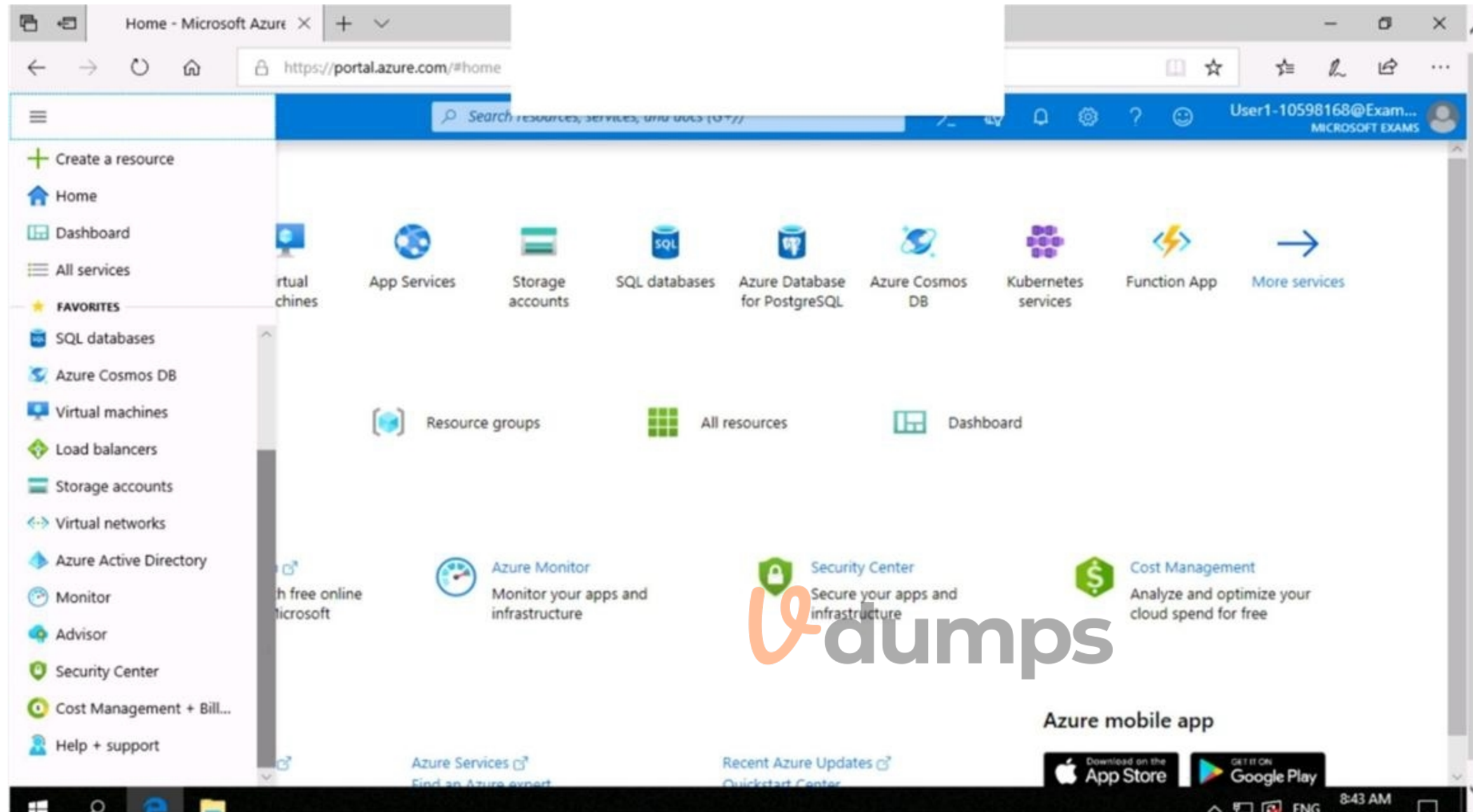
- Technical Documentation [Azure Migration Tools](#)
- Azure Services [Find an Azure expert](#)
- Recent Azure Updates [Quickstart Center](#)

Azure mobile app

Download on the App Store | GET IT ON Google Play







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

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

1. In the Search resources, services, and docs box at the top of the portal, begin typing the name of a virtual machine, VM1 that has a network interface that you want to add to, or remove from, an application security group.
2. When the name of your VM appears in the search results, select it.
3. Under SETTINGS, select Networking. Select Configure the application security groups, select the application security groups that you want to add the network interface to, or unselect the application security groups that you want to remove the network interface from, and then select Save.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

### QUESTION 36

#### 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.

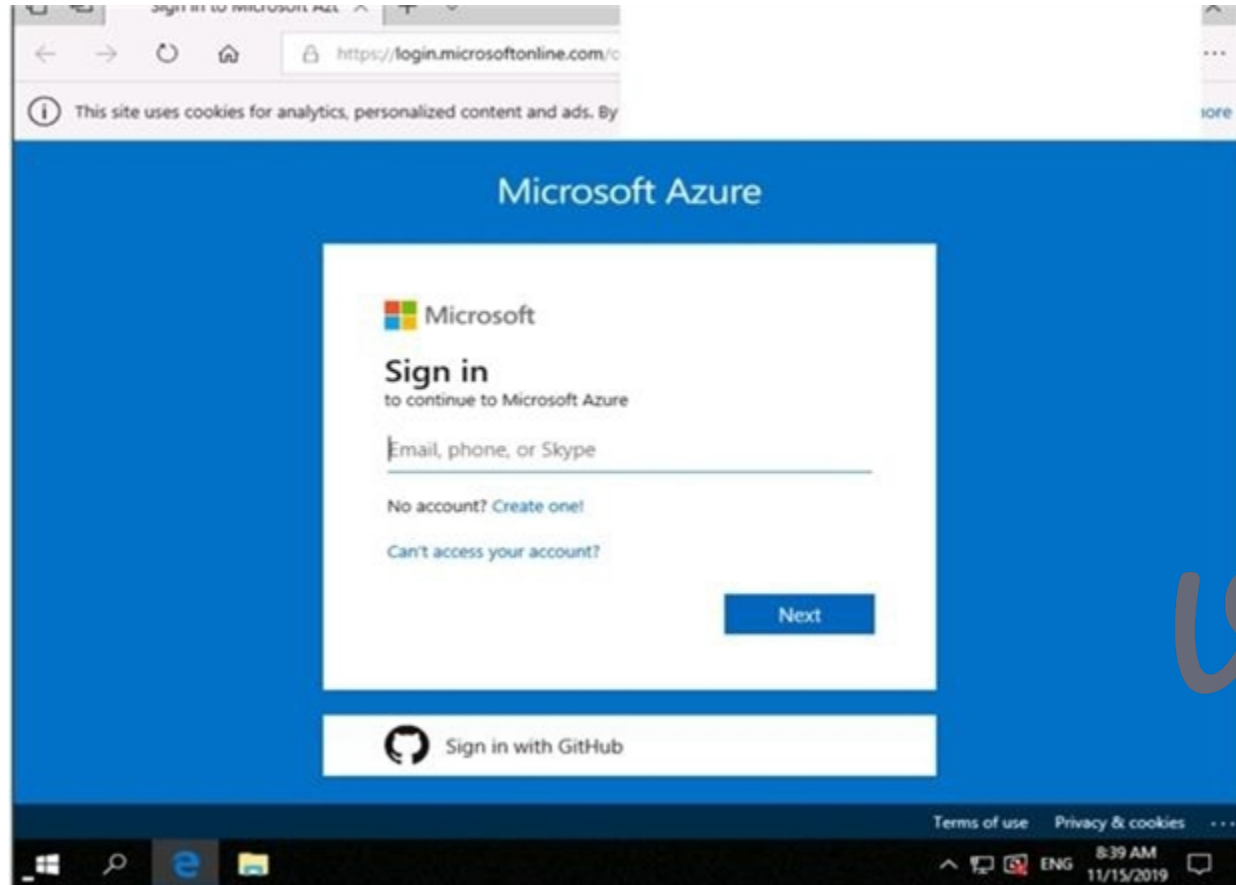
To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168



Vdumps

Home - Microsoft Azure x + v

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

Microsoft Azure Search Resources, services, and tools (0/??)

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

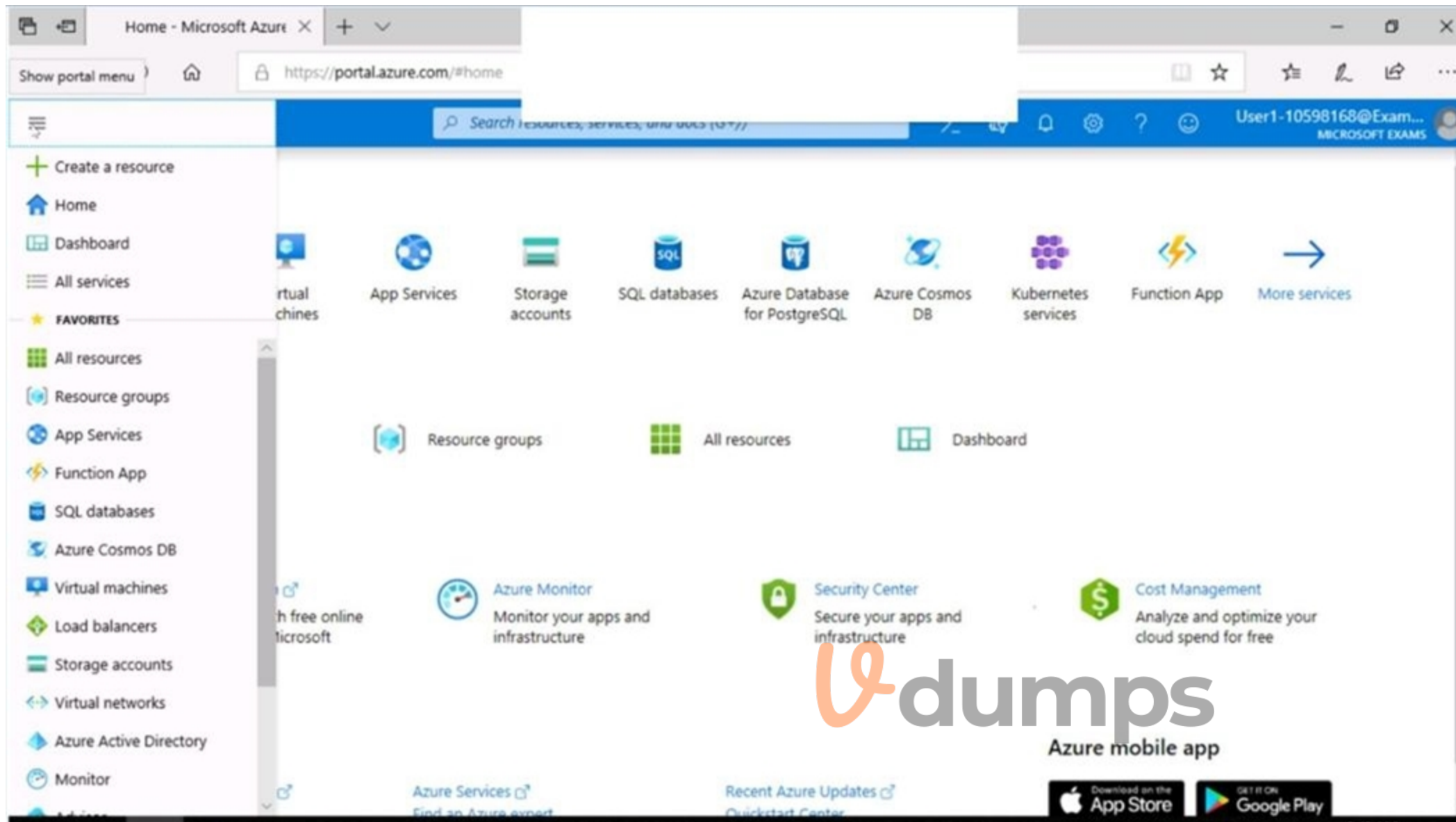
### Useful links

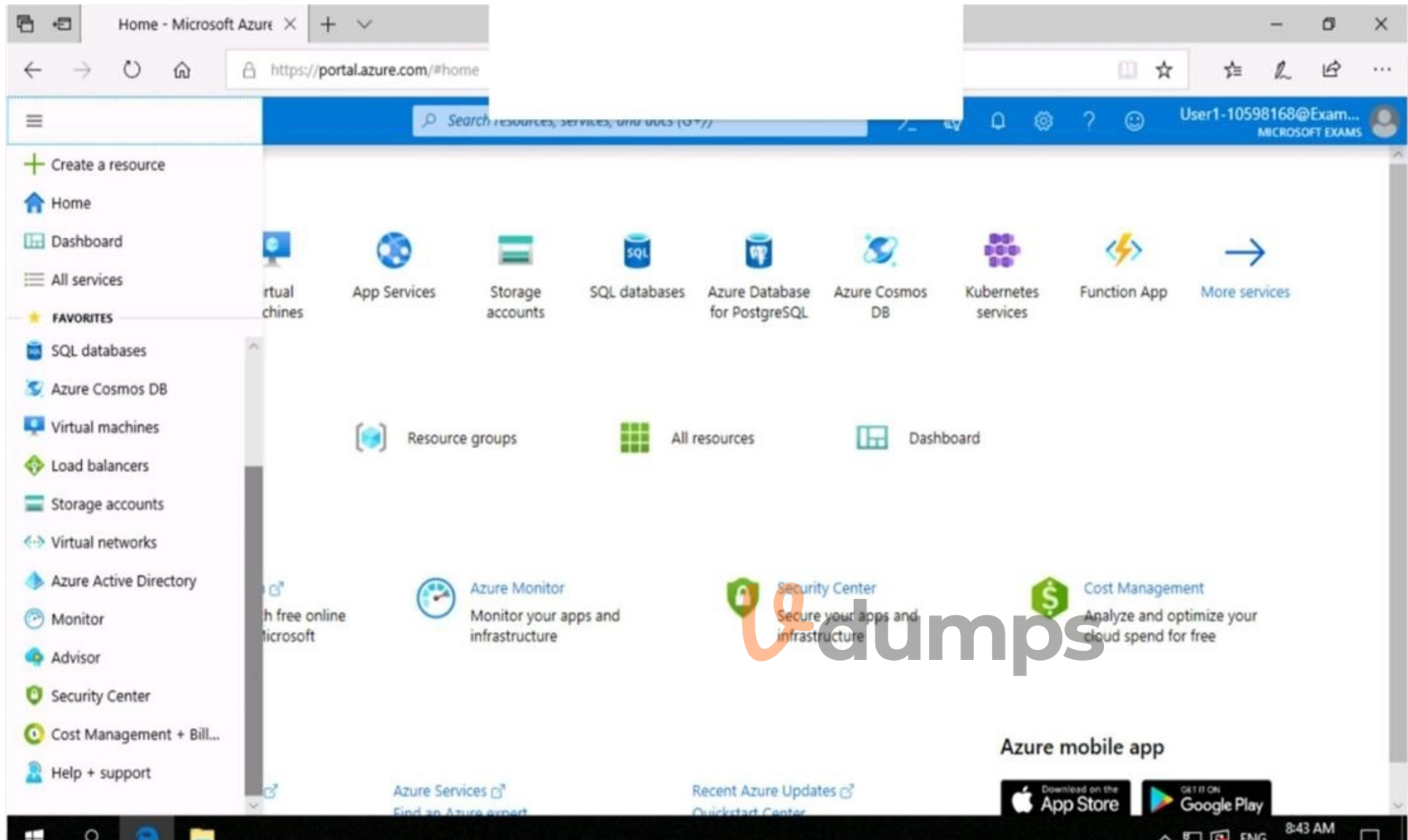
- Technical Documentation
- Azure Services
- Recent Azure Updates

Azure mobile app

Download on the App Store | Get it on Google Play







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

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

Deploy the Microsoft Antimalware Extension using the Azure Portal for single VM deployment

1. In Azure Portal, go to the Azure VM1's blade, navigate to the Extensions section and press Add.

## devrgvm - Extensions

Virtual machine

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
- Networking
- Disks
- Size
- Security
- Extensions**

+ Add

Search to filter items...

NAME	TYPE
CustomScriptExtension	Microsoft.Compute.CustomScriptEx
DependencyAgentWindows	Microsoft.Azure.Monitoring.Depend
enablevmaccess	Microsoft.Compute.VMAccessAgen
IaaS.Diagnostics	Microsoft.Azure.Diagnostics.IaaS
MicrosoftMonitoringAgent	Microsoft.EnterpriseCloud.Monitori
SiteRecovery-Windows	Microsoft.Azure.RecoveryServices.S



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

## Install extension



Excluded files and locations ⓘ

Excluded file extensions ⓘ

Excluded processes ⓘ

Real-time protection ⓘ

Run a scheduled scan ⓘ

Scan type ⓘ

Scan day ⓘ

Scan time ⓘ

OK

Reference:

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

QUESTION 37



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

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

**Correct Answer: B, E**

**Section:**

**Explanation:**

Only Linux images are scanned. Windows images are not scanned.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/azure-container-registry-integration>

### QUESTION 38

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

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

All the virtual networks are peered.

You deploy Azure Bastion to VNET2.

Which virtual machines can be protected by the bastion host?

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

**Correct Answer: A**

**Section:**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/bastion/vnet-peering>

### QUESTION 39

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

You discover that AKS1 cannot be accessed by using accounts from Contoso.com.

You need to ensure AKS1 can be accessed by using accounts from Contoso.com. The solution must minimize administrative effort. What should you do first?

- A. From Azure recreate AKS1.
- B. From AKS1, upgrade the version of Kubernetes.
- C. From Azure AD, implement Azure AD Premium.
- D. From Azure AD, configure the User settings.

**Correct Answer: A**

**Section:**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli>

#### QUESTION 40

You have an Azure subscription that contains an Azure Container Registry named Registry1. Azure Defender is enabled in the subscription. You upload several container images to Register1.

You discover that vulnerability security scans were not performed.

You need to ensure that the container images are scanned for vulnerabilities when they are uploaded to Registry1.

What should you do?

- A. From the Azure portal modify the Pricing tier settings.
- B. From Azure CLI, lock the container images.
- C. Upload the container images by using AzCopy.
- D. Push the container images to Registry1 by using Docker

**Correct Answer: A**

**Section:**

**Explanation:**

Reference:

<https://charbelnemnom.com/scan-container-images-in-azure-container-registry-with-azure-security-center/>

#### QUESTION 41

SIMULATION

You need to ensure that connections from the Internet to VNET1\subnet0 are allowed only over TCP port 7777. The solution must use only currently deployed resources.

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

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

You need to configure the Network Security Group that is associated with subnet0.

1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET1. Alternatively, browse to Virtual Networks in the left navigation pane.
2. In the properties of VNET1, click on Subnets. This will display the subnets in VNET1 and the Network Security Group associated to each subnet. Note the name of the Network Security Group associated to Subnet0.
3. Type Network Security Groups into the search box and select the Network Security Group associated with Subnet0.
4. In the properties of the Network Security Group, click on Inbound Security Rules.



5. Click the Add button to add a new rule.
6. In the Source field, select Service Tag.
7. In the Source Service Tag field, select Internet.
8. Leave the Source port ranges and Destination field as the default values (\* and All).
9. In the Destination port ranges field, enter 7777.
10. Change the Protocol to TCP.
11. Leave the Action option as Allow.
12. Change the Priority to 100.
13. Change the Name from the default Port\_8080 to something more descriptive such as Allow\_TCP\_7777\_from\_Internet. The name cannot contain spaces.
14. Click the Add button to save the new rule.

#### QUESTION 42

##### SIMULATION

You need to prevent administrators from performing accidental changes to the Homepage app service plan.

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

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

You need to configure a 'lock' for the app service plan. A read-only lock ensures that no one can make changes to the app service plan without first deleting the lock.

1. In the Azure portal, type App Service Plans in the search box, select App Service Plans from the search results then select Homepage. Alternatively, browse to App Service Plans in the left navigation pane.
2. In the properties of the app service plan, click on Locks.
3. Click the Add button to add a new lock.
4. Enter a name in the Lock name field. It doesn't matter what name you provide for the exam.
5. For the Lock type, select Read-only.
6. Click OK to save the changes.

#### QUESTION 43

##### SIMULATION

You need to ensure that a user named Danny11597200 can sign in to any SQL database on a Microsoft SQL server named web11597200 by using SQL Server Management Studio (SSMS) and Azure Active Directory (Azure AD) credentials.

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

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

You need to provision an Azure AD Admin for the SQL Server.

1. In the Azure portal, type SQL Server in the search box, select SQL Server from the search results then select the server named web11597200. Alternatively, browse to SQL Server in the left navigation pane.
2. In the SQL Server properties page, click on Active Directory Admin.
3. Click the Set Admin button.
4. In the Add Admin window, search for and select Danny11597200.
5. Click the Select button to add Danny11597200.
6. Click the Save button to save the changes.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?tabs=azure-powershell>

#### QUESTION 44

##### SIMULATION

You need to deploy an Azure firewall to a virtual network named VNET3.

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

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

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

To add an Azure firewall to a VNET, the VNET must first be configured with a subnet named AzureFirewallSubnet (if it doesn't already exist).

Configure VNET3.

1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET3. Alternatively, browse to Virtual Networks in the left navigation pane.
2. In the Overview section, note the Location (region) and Resource Group of the virtual network. We'll need these when we add the firewall.
3. Click on Subnets.
4. Click on + Subnet to add a new subnet.
5. Enter AzureFirewallSubnet in the Name box. The subnet must be named AzureFirewallSubnet.
6. Enter an appropriate IP range for the subnet in the Address range box.
7. Click the OK button to create the subnet.

Add the Azure Firewall.

1. In the settings of VNET3 click on Firewall.
2. Click the Click here to add a new firewall link.
3. The Resource group will default to the VNET3 resource group. Leave this default.
4. Enter a name for the firewall in the Name box.
5. In the Region box, select the same region as VNET3.
6. In the Public IP address box, select an available public IP address if one exists, or click Add new to add a new public IP address.
7. Click the Review + create button.
8. Review the settings and click the Create button to create the firewall.

Reference:

<https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal>

#### QUESTION 45

##### SIMULATION

You need to configure a virtual network named VNET2 to meet the following requirements:

Administrators must be prevented from deleting VNET2 accidentally.

Administrators must be able to add subnets to VNET2 regularly.

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

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A



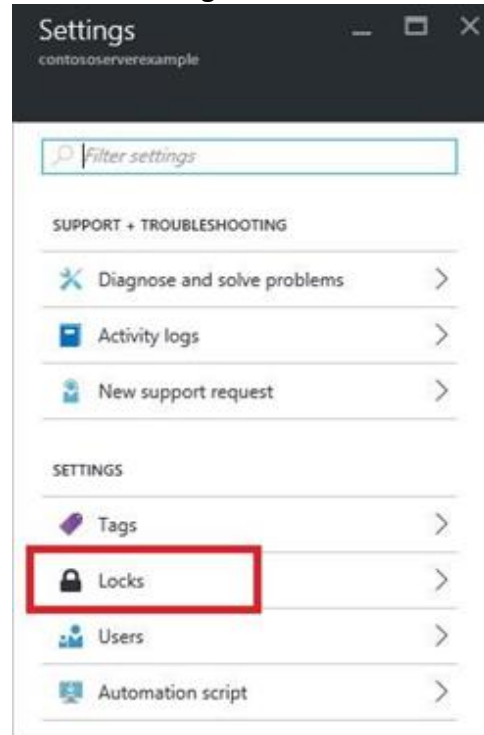


Explanation:

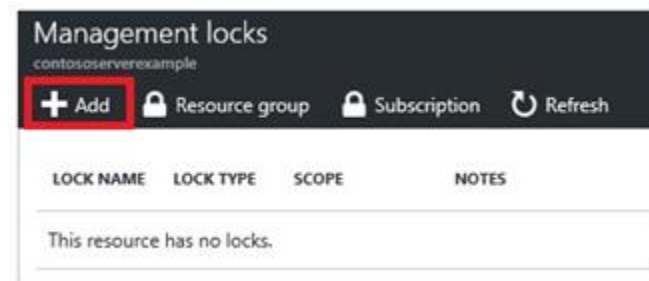
Locking prevents other users in your organization from accidentally deleting or modifying critical resources, such as Azure subscription, resource group, or resource.

Note: In Azure, the term resource refers to an entity managed by Azure. For example, virtual machines, virtual networks, and storage accounts are all referred to as Azure resources.

1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET2. Alternatively, browse to Virtual Networks in the left navigation pane.
2. In the Settings blade for virtual network VNET2, select Locks.



3. To add a lock, select Add.



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

Reference:

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

#### QUESTION 46

HOTSPOT

You have a network security group (NSG) bound to an Azure subnet.

You run Get-AzNetworkSecurityRuleConfig and receive the output shown in the following exhibit.



```

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

Name : StorageEA2Allow
ProvisioningState : Succeeded
Description :
Protocol : *
SourcePortRange : (*)
DestinationPortRange : {443}
SourceAddressPrefix : (*)
DestinationAddressPrefix : {Storage.EastUS2}
SourceApplicationSecurityGroups : []
DestinationApplicationSecurityGroups : []
Access : Allow
Priority : 104
Direction : Outbound

Name : Contoso_FTP
Description :
Protocol : TCP
SourcePortRange : (*)
DestinationPortRange : {21}
SourceAddressPrefix : {1.2.3.4/32}
DestinationAddressPrefix : {10.0.0.5/32}
SourceApplicationSecurityGroups : []
DestinationApplicationSecurityGroups : []
Access : Allow
Priority : 504
Direction : Inbound

```



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

NOTE: Each correct selection is worth one point.

**Hot Area:**

Answer Area

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

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


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

	▼
allowed	
dropped	
forwarded	

Answer Area:

Answer Area

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



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

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

	▼
allowed	
dropped	
forwarded	

Section:

Explanation:

Box 1: able to connect to East US 2

The StorageEA2Allow has DestinationAddressPrefix {Storage/EastUS2}

Box 2: allowed

TCP Port 21 controls the FTP session. Contoso\_FTP has SourceAddressPrefix {1.2.3.4/32} and DestinationAddressPrefix {10.0.0.5/32}

Note:

The Get-AzureRmNetworkSecurityRuleConfig cmdlet gets a network security rule configuration for an Azure network security group. Security rules in network security groups enable you to filter the type of network traffic that can flow in and out of virtual network subnets and network interfaces.

Reference:

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

#### QUESTION 47

You have a web app hosted on an on-premises server that is accessed by using a URL of <https://www.contoso.com>.

You plan to migrate the web app to Azure. You will continue to use <https://www.contoso.com>.

You need to enable HTTPS for the Azure web app.

What should you do first?

- A. Export the public key from the on-premises server and save the key as a P7b file.
- B. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using TripleDES.
- C. Export the public key from the on-premises server and save the key as a CER file.
- D. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using AES256.

**Correct Answer: B**

**Section:**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate#private-certificate-requirements>

#### QUESTION 48

HOTSPOT

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



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

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

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

You configure the following Firewall and virtual networks settings for storage1:

Allow access from: Selected networks

Virtual networks: VNET3\Subnet3

Firewall – Address range: 52.233.129.0/24

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

NOTE: Each correct selection is worth one point.

**Hot Area:**

### Answer Area

Statements	Yes	No
VM1 can connect to storage1.	<input type="radio"/>	<input type="radio"/>
VM2 can connect to storage1.	<input type="radio"/>	<input type="radio"/>
VM3 can connect to storage1.	<input type="radio"/>	<input type="radio"/>

Answer Area:

### Answer Area

Statements	Yes	No
VM1 can connect to storage1.	<input type="radio"/>	<input checked="" type="radio"/>
VM2 can connect to storage1.	<input checked="" type="radio"/>	<input type="radio"/>
VM3 can connect to storage1.	<input type="radio"/>	<input checked="" type="radio"/>

Vdumps

**Section:**

**Explanation:**

Box 1: No

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

Box 2: Yes

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

Box 3: No

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

### QUESTION 49

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

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

Save Discard Upload Download

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

```
1 {
2   "id": "d6b00db3-7ef4-4f3c-b1e7-8346f0a59546",
3   "acceptMappedClaims": null,
4   "accessTokenAcceptedVersion": null,
5   "addIns": [],
6   "allowPublicClient": null,
7   "appId": "88137405-6a75-4c20-903a-f7b18ff7d496",
8   "appRoles": [],
9   "oauth2AllowUrlPathMatching": false,
10  "createdDateTime": "2019-07-15T21:09:20Z",
11  "groupMembershipClaims": null,
12  "identifierUris": [],
13  "informationalUrls": {
14    "termsOfService": null,
15    "support": null,
16    "privacy": null,
17    "marketing": null
18  },
19  "keyCredentials": [],
20  "knownClientApplications": [],
21  "logoUrl": null,
22  "logoutUrl": null,
23  "name": "AKSAzureADServer",
24  "oauth2AllowIdTokenImplicitFlow": false,
25  "oauth2AllowImplicitFlow": false,
26  "oauth2Permissions": [],
27  "oauth2RequirePostResponse": false,
28  "optionalClaims": null,
29  "orgRestrictions": [],
30  "parentalControlSettings": {
```



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

- A. accessTokenAcceptedVersion
- B. keyCredentials
- C. groupMembershipClaims
- D. acceptMappedClaims

**Correct Answer: C**

**Section:**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli>

<https://www.codeproject.com/Articles/3211864/Operation-and-Maintenance-of-AKS-Applications>

## QUESTION 50

### 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.

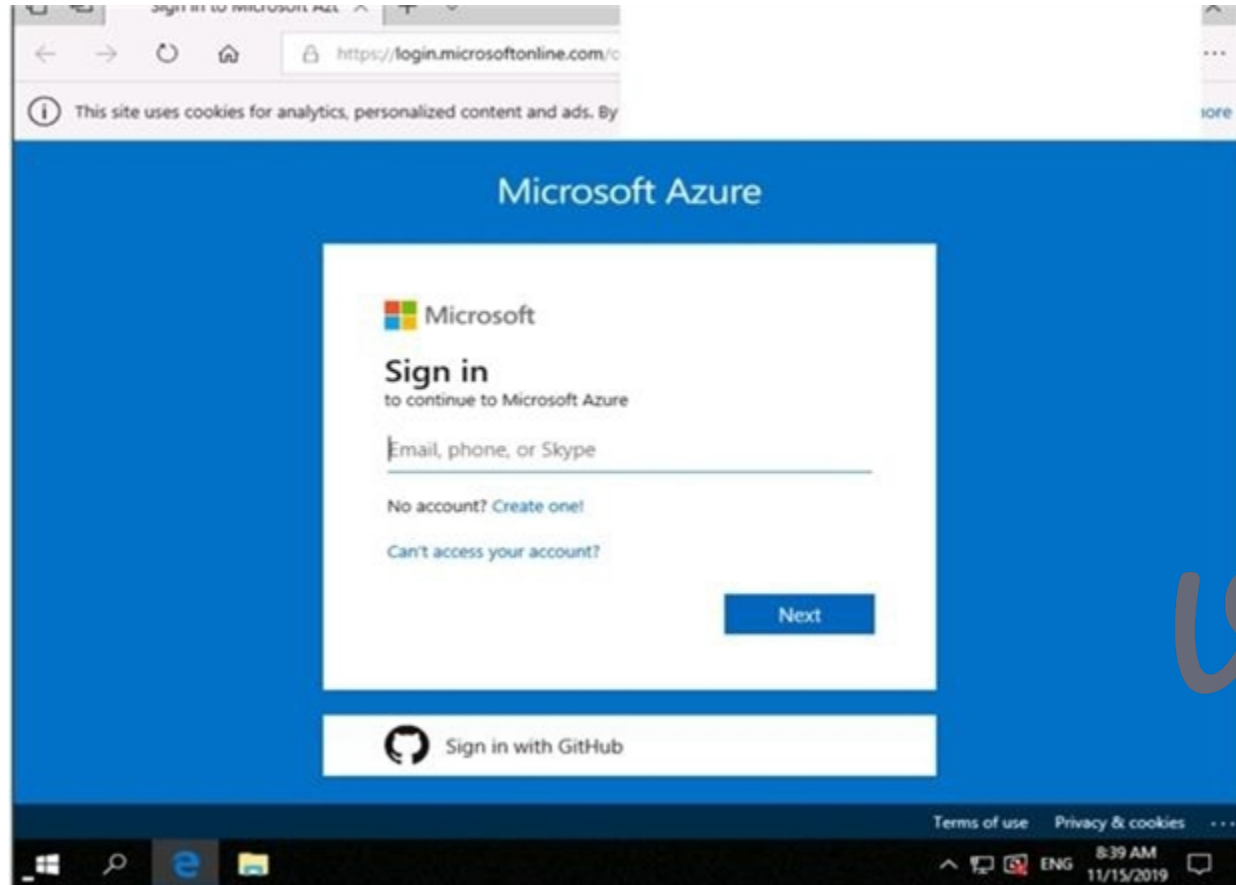
To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User1-10598168@ExamUsers.com

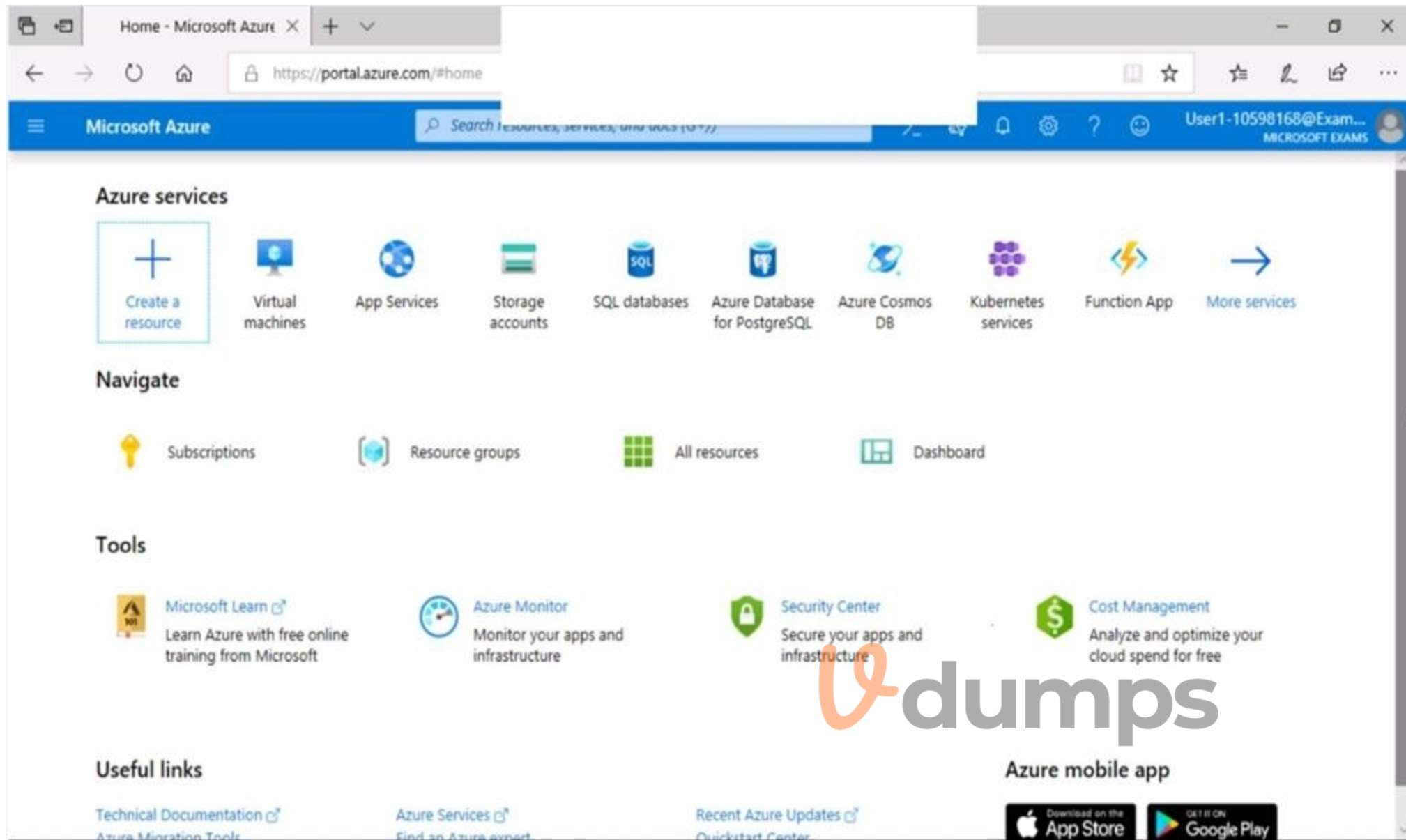
Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

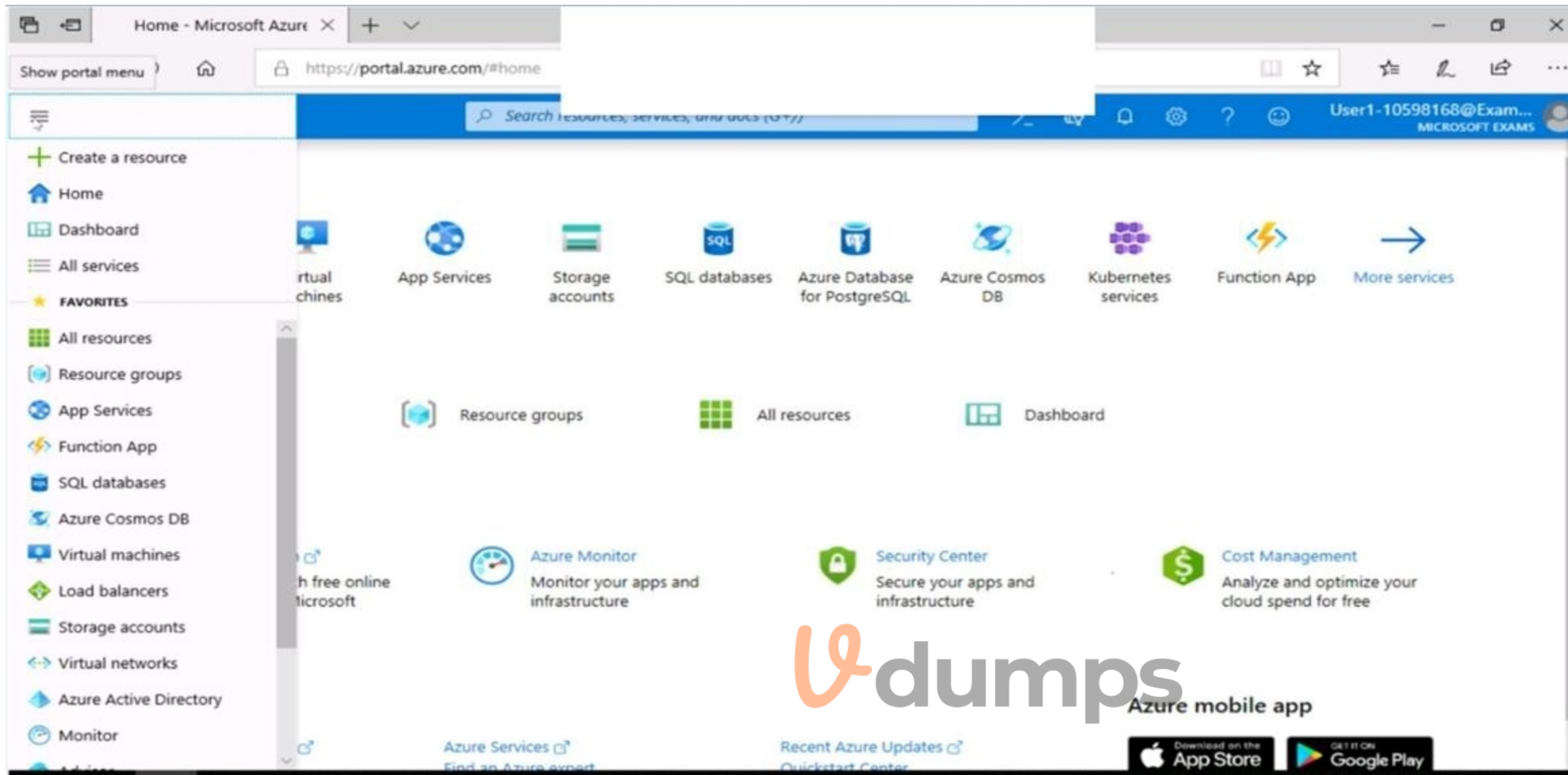
Lab Instance: 10598168

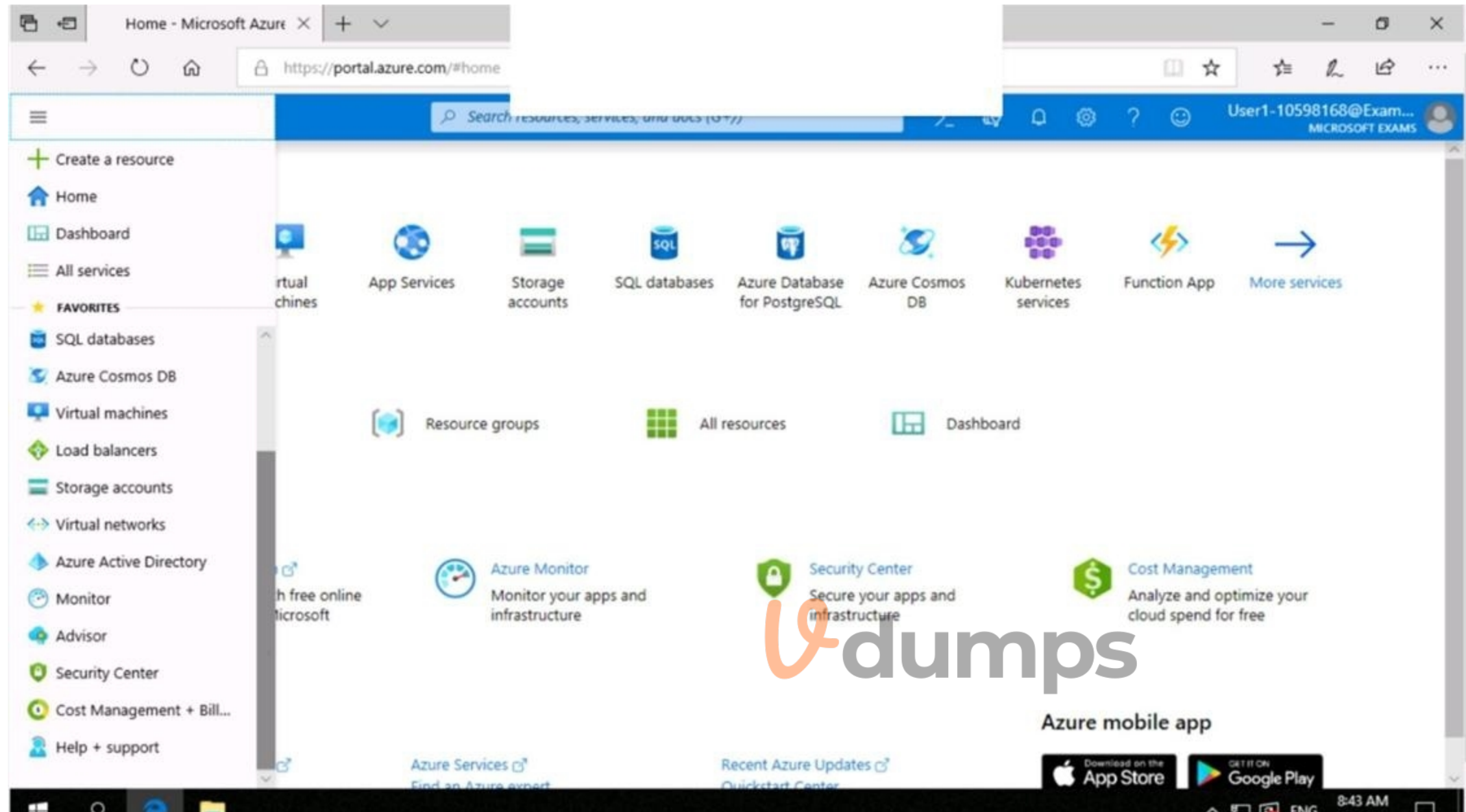


Vdumps









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

A.

**Correct Answer: A**

**Section:**

**Explanation:**

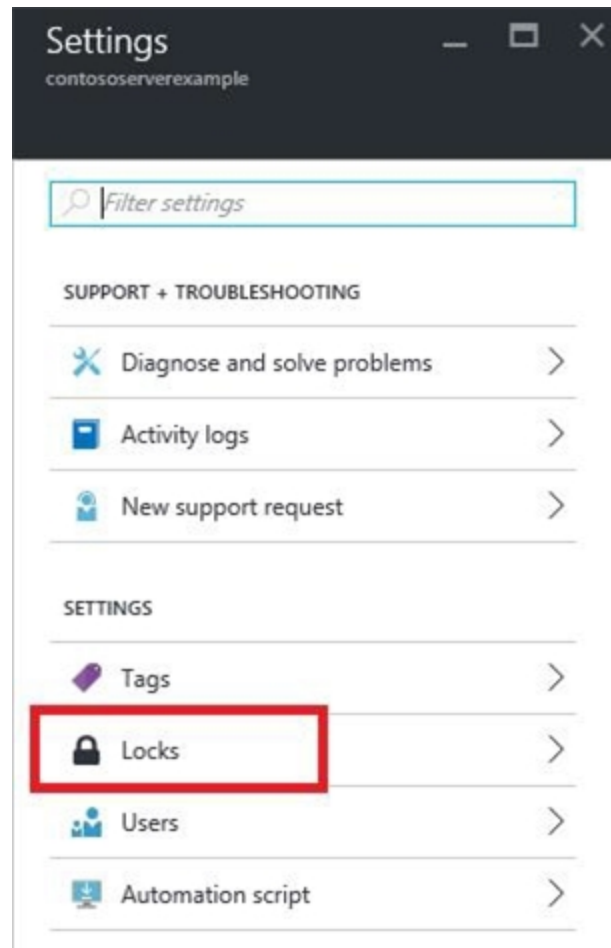
Answer: A

Explanation:

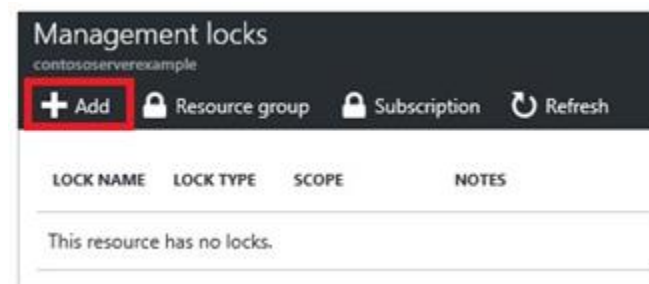
Locking prevents other users in your organization from accidentally deleting or modifying critical resources, such as Azure subscription, resource group, or resource.

Note: In Azure, the term resource refers to an entity managed by Azure. For example, virtual machines, virtual networks, and storage accounts are all referred to as Azure resources.

1. In the Settings blade for virtual network VNET, select Locks.



2. To add a lock, select Add.



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 51

#### 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.

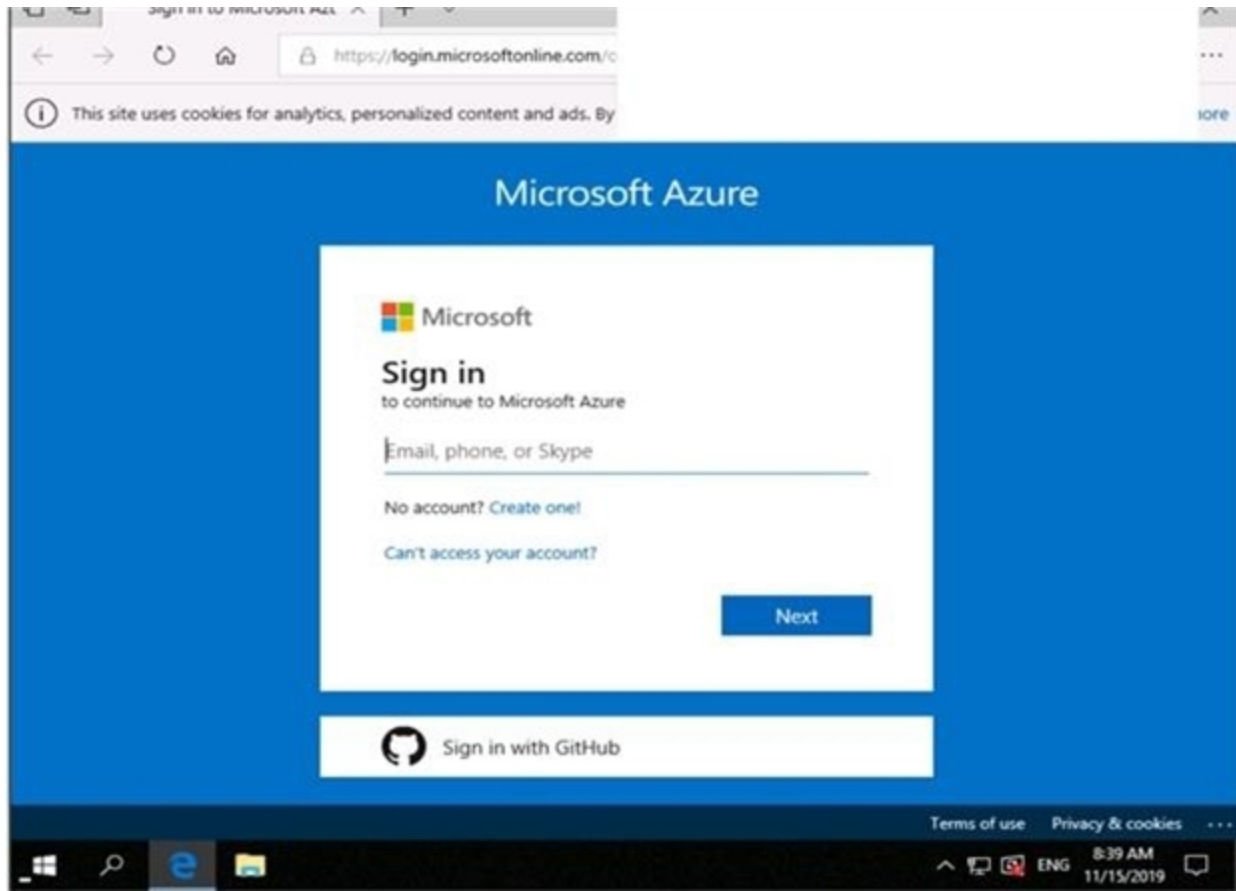
To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168



 **vdumps**

Home - Microsoft Azure X + v

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

Microsoft Azure Search resources, services, and docs (0/7)

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 <sup>o</sup>  
Learn Azure with free online training from Microsoft
- Azure Monitor <sup>o</sup>  
Monitor your apps and infrastructure
- Security Center <sup>o</sup>  
Secure your apps and infrastructure
- Cost Management <sup>o</sup>  
Analyze and optimize your cloud spend for free

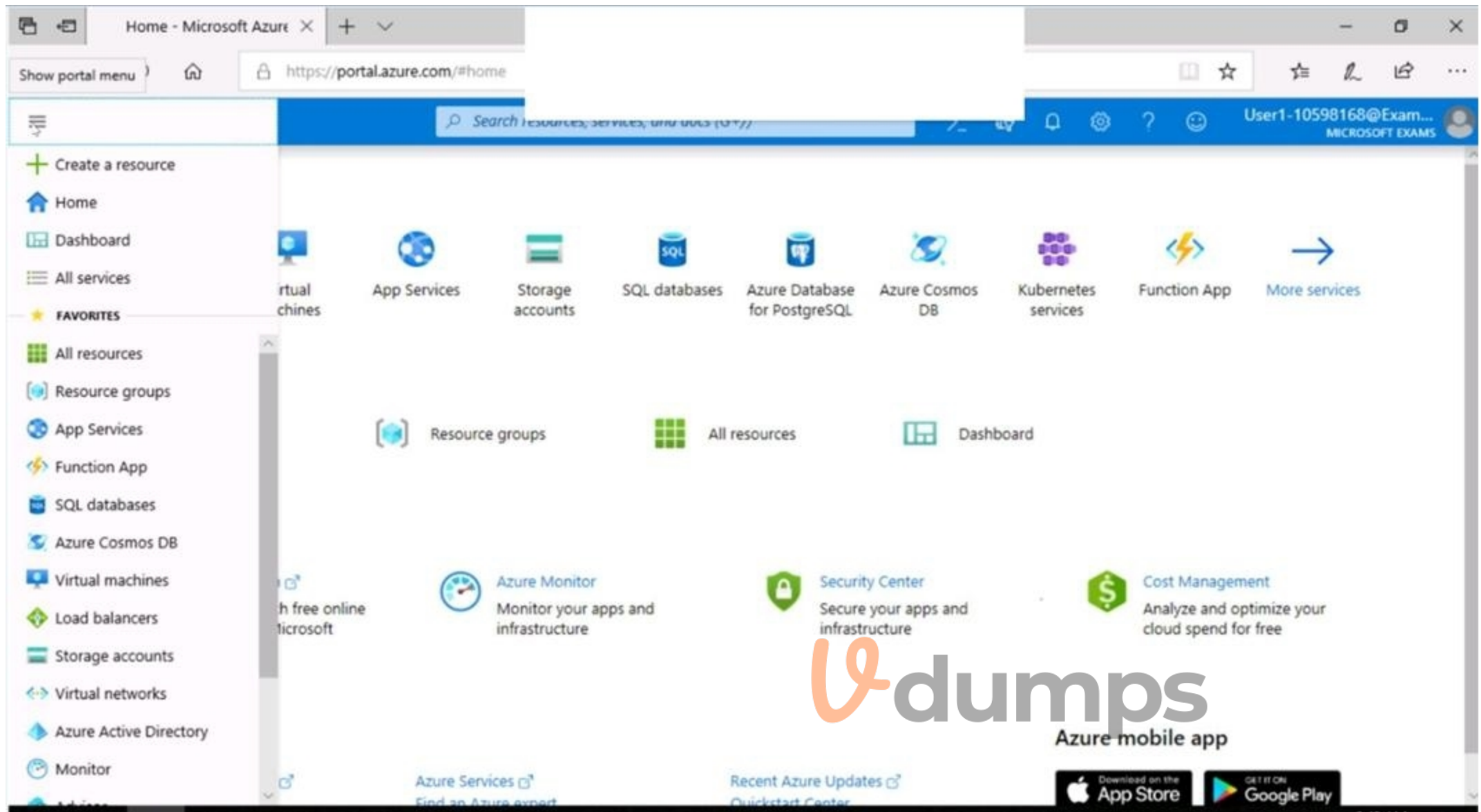
### Useful links

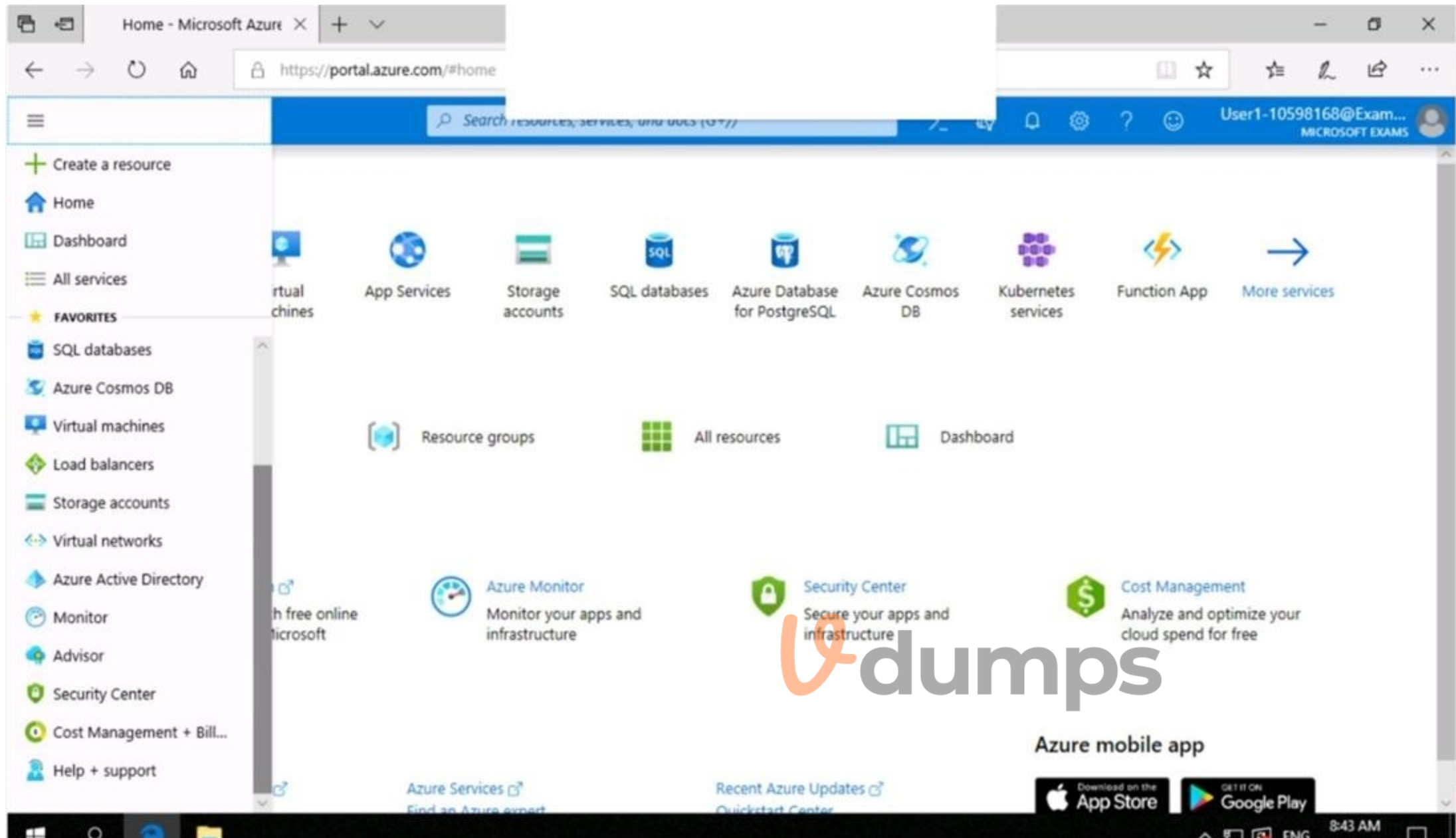
- Technical Documentation <sup>o</sup>
- Azure Services <sup>o</sup>
- Recent Azure Updates <sup>o</sup>

Azure mobile app

Download on the App Store | GET IT ON Google Play







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

A.

**Correct Answer: A**

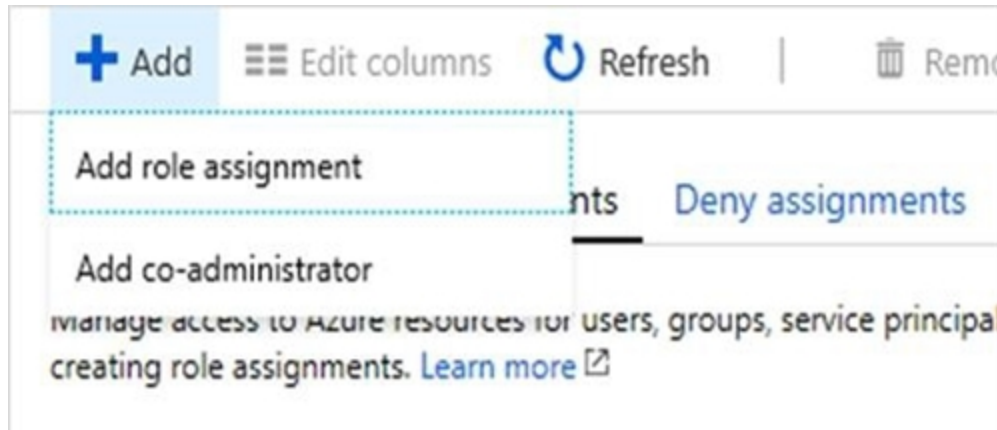
**Section:**

**Explanation:**

Answer: A

Explanation:

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



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 52

### 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.

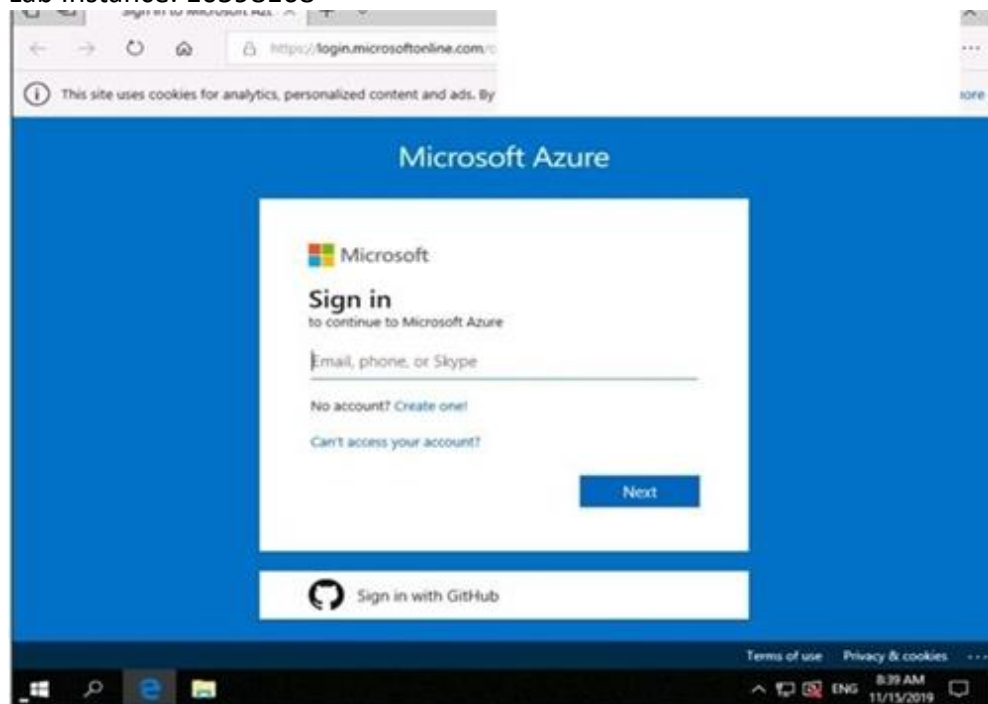
Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168

The logo for 'Vdumps' features a stylized orange 'V' followed by the word 'dumps' in a grey, sans-serif font.





Home - Microsoft Azure x + v

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

Microsoft Azure Search [resources, subscriptions, azure portal (0/177)] 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 <sup>o</sup>  
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

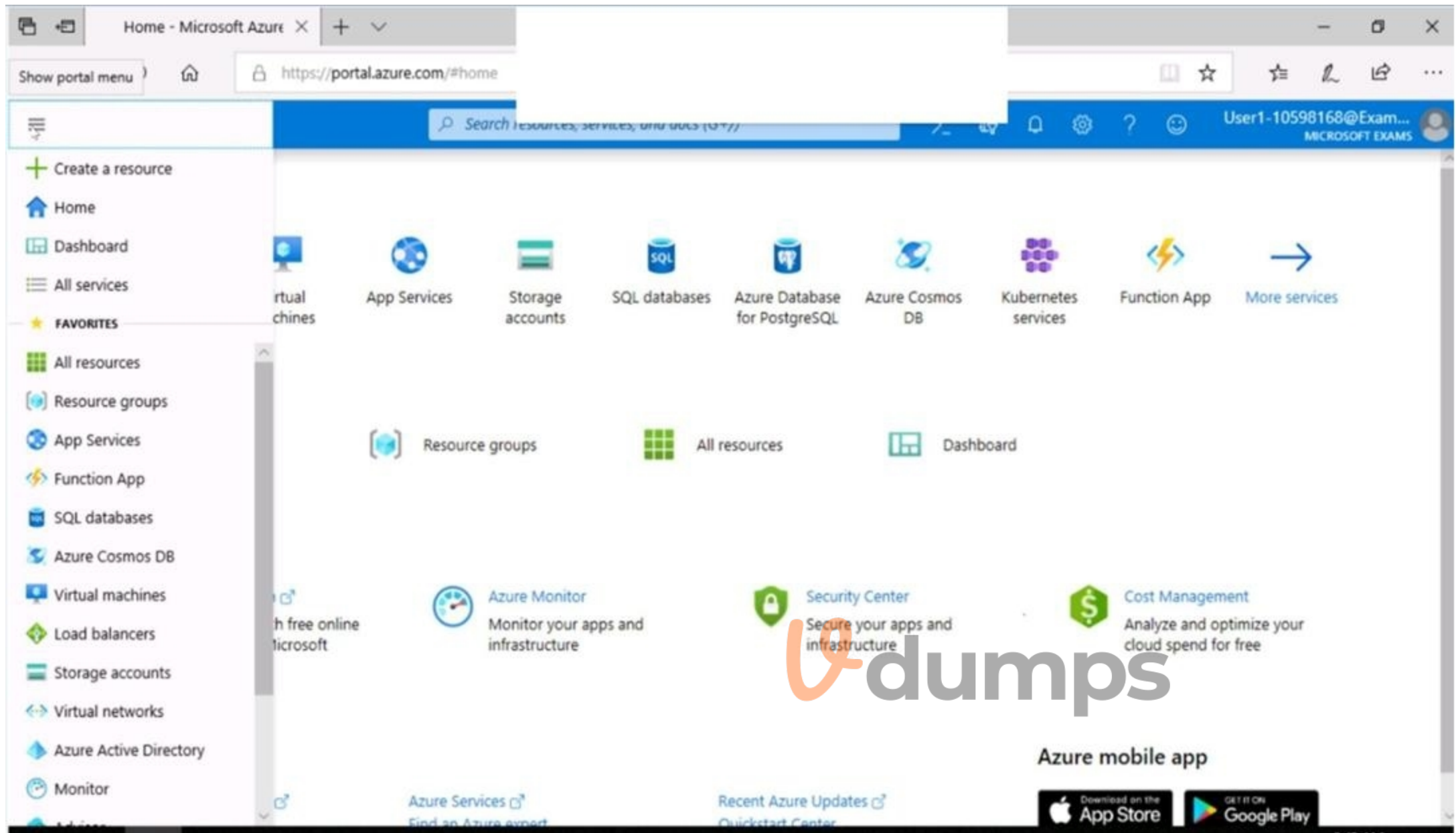
### Useful links

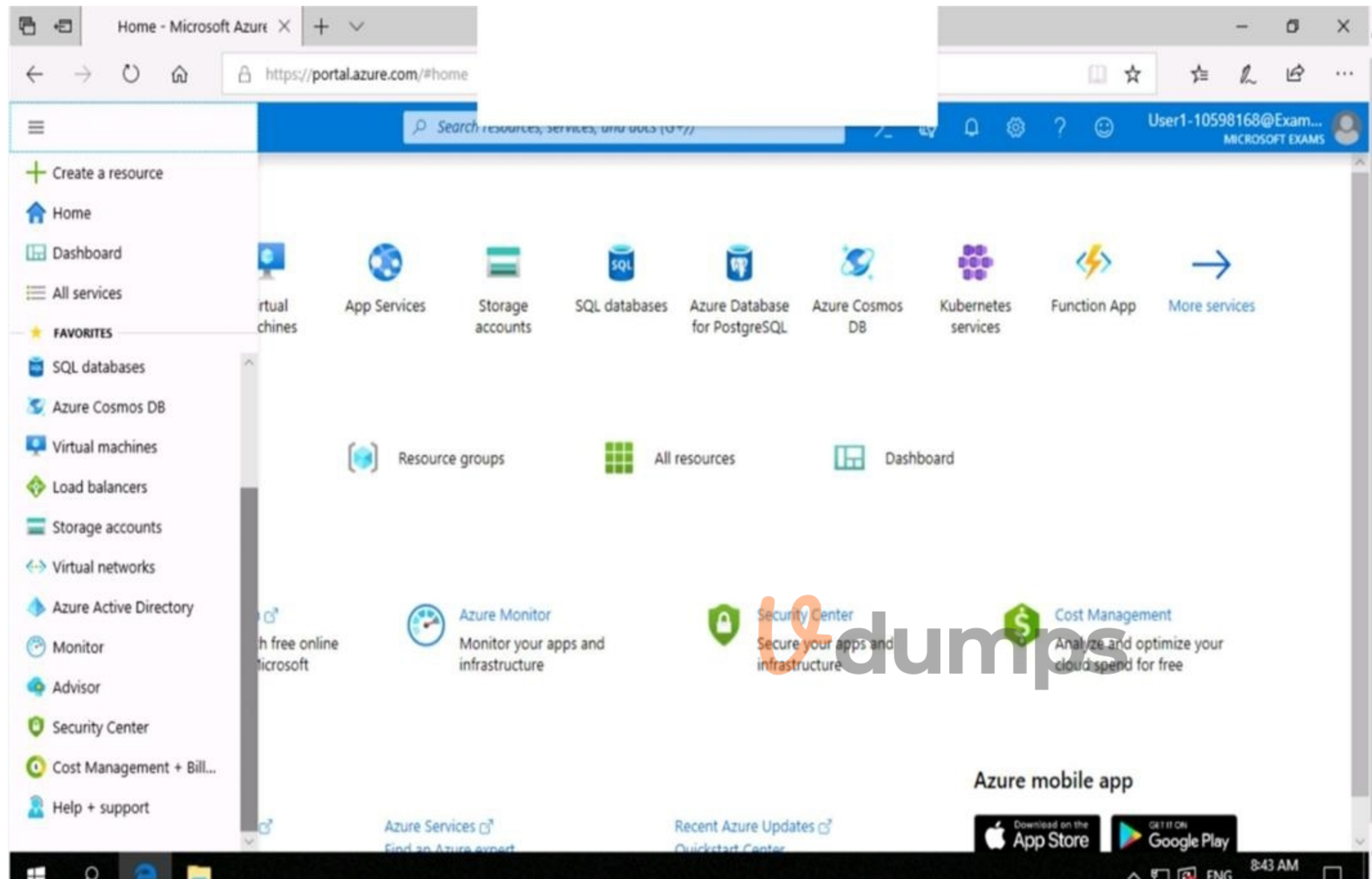
- Technical Documentation <sup>o</sup>
- Azure Migration Tools
- Azure Services <sup>o</sup>  
Find an Azure expert
- Recent Azure Updates <sup>o</sup>  
Quickstart Center

Azure mobile app

Download on the App Store | GET IT ON Google Play

**Vdumps**





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

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

Step 1:

1. In Azure portal go to the storage account you want to secure. Here: rg1lod10598168

2. Click on the settings menu called Firewalls and virtual networks.

3. To deny access by default, choose to allow access from Selected networks. To allow traffic from all networks, choose to allow access from All networks.

4. Click Save to apply your changes.

Step 2:

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

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security>

### QUESTION 53

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

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

**Correct Answer: B**

**Section:**

**Explanation:**

You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines.

Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSC-Service so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.

Reference:

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

### QUESTION 54

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

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

You create an MDM Security Baseline profile named Profile1.

You need to identify to which virtual machines Profile1 can be applied.

Which virtual machines should you identify?

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

Correct Answer: A

Section:

Explanation:

Reference:

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

### QUESTION 55

HOTSPOT

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

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

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

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

The firewalls on all the virtual machines allow ping traffic.

NSG1 is configured as shown in the following exhibit.

Inbound security rules

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

Outbound security rules

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Statements	Yes	No
VM1 can ping VM3 successfully.	<input type="radio"/>	<input type="radio"/>
VM2 can ping VM4 successfully.	<input type="radio"/>	<input type="radio"/>
VM3 can be accessed by using Remote Desktop from the internet.	<input type="radio"/>	<input type="radio"/>

Answer Area:

### Answer Area

Statements	Yes	No
VM1 can ping VM3 successfully.	<input checked="" type="radio"/>	<input type="radio"/>
VM2 can ping VM4 successfully.	<input type="radio"/>	<input checked="" type="radio"/>
VM3 can be accessed by using Remote Desktop from the internet.	<input checked="" type="radio"/>	<input type="radio"/>

**Section:**

**Explanation:**

Box 1: Yes

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

Box 2: No

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

Box 3: Yes

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

### QUESTION 56

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

You are implementing Update Management in Azure Automation.

You plan to create a new update deployment named Update1.

You need to ensure that Update1 meets the following requirements:

Automatically applies updates to VM1 and VM2.

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

What should you include in Update1?

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

**Correct Answer: C**

**Section:**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/automation/update-management/configure-groups>

#### QUESTION 57

You have multiple development teams that will create apps in Azure.

You plan to create a standard development environment that will be deployed for each team.

You need to recommend a solution that will enforce resource locks across the development environments and ensure that the locks are applied in a consistent manner.

What should you include in the recommendation?

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

**Correct Answer: D**

**Section:**

**Explanation:**

Reference:

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



#### QUESTION 58

SIMULATION

You need to configure a Microsoft SQL server named Web11597200 only to accept connections from the Subnet0 subnet on the VNET01 virtual network.

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

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

You need to allow access to Azure services and configure a virtual network rule for the SQL Server.

1. In the Azure portal, type SQL Server in the search box, select SQL Server from the search results then select the server named web11597200. Alternatively, browse to SQL Server in the left navigation pane.
2. In the properties of the SQL Server, click Firewalls and virtual networks.
3. In the Virtual networks section, click on Add existing. This will open the Create/Update virtual network rule window.
4. Give the rule a name such as Allow\_VNET01-Subnet0 (it doesn't matter what name you enter for the exam).
5. In the Virtual network box, select VNET01.
6. In the Subnet name box, select Subnet0.
7. Click the OK button to save the rule.
8. Back in the Firewall / Virtual Networks window, set the Allow access to Azure services option to On.

**QUESTION 59**

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

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

**Correct Answer: B**

**Section:**

**Explanation:**

The primary use case for the Azure Desired State Configuration (DSC) extension is to bootstrap a VM to the Azure Automation State Configuration (DSC) service. The service provides benefits that include ongoing management of the VM configuration and integration with other operational tools, such as Azure Monitoring. Using the extension to register VM's to the service provides a flexible solution that even works across Azure subscriptions.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview>

**QUESTION 60**

HOTSPOT

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

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



You create a resource group named RG1.

Which users can modify the permissions for RG1 and which users can create virtual networks in RG1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Hot Area:**



## Answer Area

Users who can modify the permissions for RG1:

▼
User1 only
User1 and User2 only
User1 and User3 only
User1, User2 and User3 only
User1, User2, User3, and User4

Users who can create virtual networks in RG1:

▼
User1 only
User1 and User2 only
User1 and User3 only
User1, User2 and User3 only
User1, User2, User3, and User4

Answer Area:

## Answer Area

Users who can modify the permissions for RG1:

▼
User1 only
User1 and User2 only
User1 and User3 only
User1, User2 and User3 only
User1, User2, User3, and User4

Users who can create virtual networks in RG1:

▼
User1 only
User1 and User2 only
User1 and User3 only
User1, User2 and User3 only
User1, User2, User3, and User4

Section:

Explanation:

Box 1: Only an owner can change permissions on resources.

Box 2: A Contributor can create/modify/delete anything in the subscription but cannot change permissions.

QUESTION 61

SIMULATION

You need to configure network connectivity between a virtual network named VNET1 and a virtual network named VNET2. The solution must ensure that virtual machines connected to VNET1 can communicate with virtual machines connected to VNET2.

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

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

You need to configure VNet Peering between the two networks. The question 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>

### 01 - Manage security operations

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

General Overview

Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.

Existing Environment

Network Environment

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

The network contains an on-premises Active Directory domain named Fabrikam.com. The domain contains two organizational units (OUs) named OU1 and OU2. Azure AD Connect cloud sync syncs only OU1.

The Azure resources hierarchy is shown in the following exhibit.



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

Name	Type	Directory-synced	Role	Delegated to
User1	User	Yes	User	None
Admin1	User	No	User Access Administrator	Tenant Root Group
Admin2	User	No	Security administrator	MG1
Admin3	User	No	Contributor	Subscription1
Admin4	User	No	Owner	RG1
Group1	Group	No	<b>Not applicable</b>	<b>None</b>

Azure AD contains the resources shown in the following table.

Name	Type	Setting
CAPolicy1	Conditional access policy	Users in the finance department must use multi-factor authentication (MFA) when accessing Microsoft SharePoint Online
Sentinel1	Azure Sentinel workspace	<b>Not applicable</b>
SecPol1	Azure Policy definition	Security configuration for virtual machines

Subscription1 Resources

Subscription1 contains the virtual networks shown in the following table.

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

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

Name	Location
NSG2	West US
NSG3	Central US
NSG4	West US

Subscription1 contains the virtual machines shown in the following table.

Name	Operating system	Location	Connected to	Associated NSG
VM1	Windows Server 2019	West US	VNET1/Subnet1	None
VM2	CentOS-based 8.2	West US	VNET1/Subnet2	NSG2
VM3	Windows Server 2016	Central US	VNET2/Subnet1	NSG3
VM4	Ubuntu Server 18.04 LTS	West US	VNET3/Subnet1	NSG4

Subscription1 contains the Azure key vaults shown in the following table.

Name	Location	Pricing tier	Private endpoint
KeyVault1	West US	Standard	VNET1/Subnet1
KeyVault2	Central US	Premium	None
KeyVault3	East US	Premium	VNET1/Subnet1, VNET2/Subnet1, VNET3/Subnet1

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

Planned Changes and Requirements

Planned Changes

Fabrikam plans to implement the following changes:

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

Name	Location
ASG1	West US
ASG2	Central US

Associate the network interface of VM1 to ASG1.

Deploy SecPol1 by using Azure Security Center.

Deploy a third-party app named App1. A version of App1 exists for all available operating systems.

Create a resource group named RG2.

Sync OU2 to Azure AD.

Add User1 to Group1.

Technical Requirements

Fabrikam identifies the following technical requirements:

The finance department users must reauthenticate after three hours when they access SharePoint Online. Storage1 must be encrypted by using customer-managed keys and automatic key rotation.

From Sentinel1, you must ensure that the following notebooks can be launched:

- Entity Explorer – Account
- Entity Explorer – Windows Host
- Guided Investigation Process Alerts

VM1, VM2, and VM3 must be encrypted by using Azure Disk Encryption.

Just in time (JIT) VM access for VM1, VM2, and VM3 must be enabled.

App1 must use a secure connection string stored in KeyVault1.

KeyVault1 traffic must NOT travel over the internet.

#### QUESTION 1

From Azure Security Center, you need to deploy SecPol1.

What should you do first?

- A. Enable Azure Defender.
- B. Create an Azure Management group.
- C. Create an initiative.
- D. Configure continuous export.

**Correct Answer: C**

**Section:**

**Explanation:**

Reference:

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/security-center/custom-security-policies.md>

<https://zimmergren.net/create-custom-security-center-recommendation-with-azure-policy/>



#### QUESTION 2

HOTSPOT

You need to configure support for Azure Sentinel notebooks to meet the technical requirements.

What is the minimum number of Azure container registries and Azure Machine Learning workspaces required?

**Hot Area:**

**Answer Area**

Container registries:

	▼
0	
1	
2	
3	

Workspaces:

	▼
0	
1	
2	
3	

Answer Area:

**Answer Area**

Container registries:

	▼
0	
1	
2	
3	

Workspaces:

	▼
0	
1	
2	
3	

Section:



**Explanation:**

Reference:

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

**02 - Manage security operations**

Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company hosts its entire server infrastructure in Azure.

Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

Existing Environment

Azure AD

Contoso.com contains the users shown in the following table.

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	None
User9	Sydney	Owner

Contoso.com contains the security groups shown in the following table.

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	user.city -contains "ON"
Group2	Dynamic user	user.city -match "*on"

Sub1

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

User9 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

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

Sub1 contains the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2

Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

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

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

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

Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

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





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

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

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

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

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG4 has the inbound security rules shown in the following table.

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

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

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

Technical requirements

Contoso identifies the following technical requirements:

Deploy Azure Firewall to VNetwork1 in Sub2.

Register an application named App2 in contoso.com.

Whenever possible, use the principle of least privilege.

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

### QUESTION 1

Which virtual networks in Sub1 can User9 modify and delete in their current state? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Virtual networks that User9 can modify:

▼
VNET4 only
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

Virtual networks that User9 can delete:

▼
VNET4 only
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

Answer Area:

## Answer Area

Virtual networks that User9 can modify:

▼
VNET4 only
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

Virtual networks that User9 can delete:

▼
VNET4 only
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

**Section:**

**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:

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

User9 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

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

Reference:

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

## QUESTION 2

You assign User8 the Owner role for RG4, RG5, and RG6. In which resource groups can User8 create virtual networks and NSGs? You must be able to connect virtual machines to deployed virtual networks. To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

User8 can create virtual networks in:

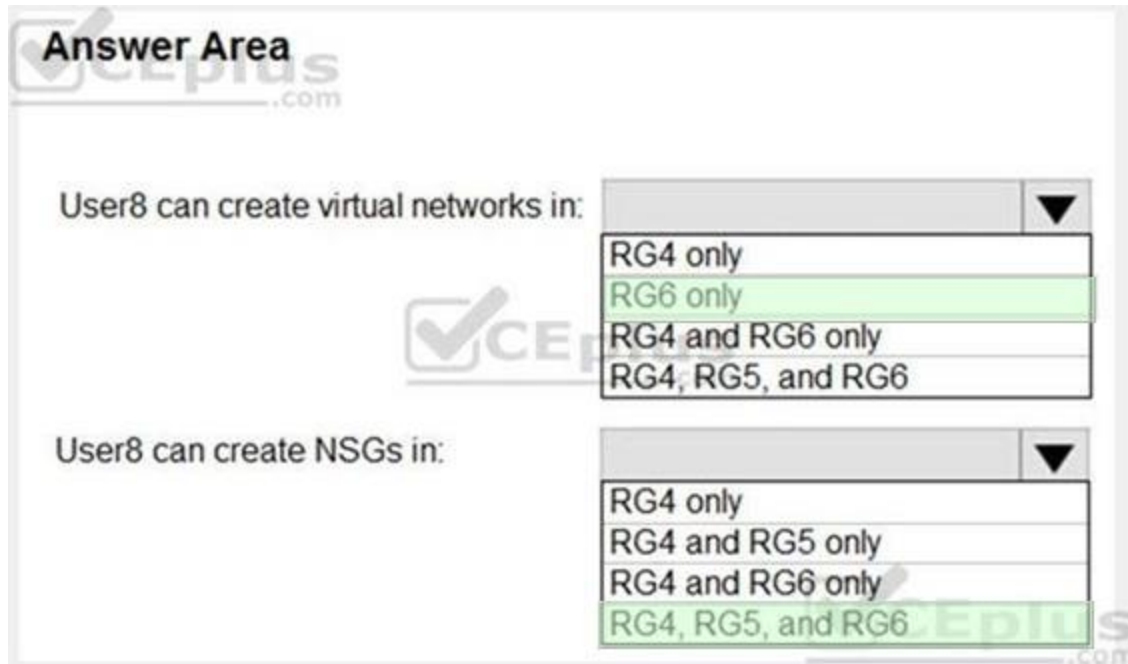
- RG4 only
- RG6 only
- RG4 and RG6 only
- RG4, RG5, and RG6

User8 can create NSGs in:

- RG4 only
- RG4 and RG5 only
- RG4 and RG6 only
- RG4, RG5, and RG6

Answer Area:

 Vdumps



**Section:**

**Explanation:**

Box 1: RG6 only

The policy does not allow the creation of virtual networks/subnets in RG5. Only NSGs can be created in RG4.B

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>

**01 - Secure data and applications**

**QUESTION 1**

You need to recommend which virtual machines to use to host App1. The solution must meet the technical requirements for KeyVault1.

Which virtual machines should you use?

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

**Correct Answer: D**

**Section:**



**Explanation:**

**02 - Secure data and applications**

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

**Overview**

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

**Existing Environment**

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

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

The tenant contains the groups shown in the following table.

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

The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://www.litwareinc.com and http://www.litwareinc.com.
RG1	Resource group	RG1 is a resource group that contains VNet1, VM0, and VM1.
RG2	Resource group	RG2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Standard tier.

Requirements

Planned Changes

Litware plans to deploy the Azure resources shown in the following table.

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

Identity and Access Requirements

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.

The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment. Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

Platform Protection Requirements

Litware identifies the following platform protection requirements:

Microsoft Antimalware must be installed on the virtual machines in RG1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access. A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.

Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center. Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

WebApp1 must enforce mutual authentication.

General Requirements

Litware identifies the following general requirements:

Whenever possible, administrative effort must be minimized.

Whenever possible, use of automation must be maximized.

### QUESTION 1

You need to 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.

**Correct Answer: A, C**

**Section:**

**Explanation:**

A: To configure Certificates for use in Azure Websites Applications you need to upload a public Certificate.

C: Over time, multiple versions of TLS have been released to mitigate different vulnerabilities. TLS 1.2 is the most current version available for apps running on Azure App Service.

Incorrect Answers:

B: We need support the http url as well.



Note:

WebApp1 is an Azure web app that is accessible by using <https://litwareinc.com> and <http://www.litwareinc.com>.

References:

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

<https://azure.microsoft.com/en-us/updates/app-service-and-functions-hosted-apps-can-now-update-tls-versions/>

## QUESTION 2

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.

Hot Area:

Answer Area

```
{
  "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 Area:

### Answer Area



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

Microsoft.Compute/ Microsoft.Resources/ Microsoft.Storage/	▼	disks/*, storageAccounts/*, virtualMachines/disks/*	▼
--	---	---	---

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



#### Section:

#### Explanation:

Scenario: A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.

Azure RBAC template managed disks "Microsoft.Storage/"

Reference:

<https://blogs.msdn.microsoft.com/azureedu/2017/02/11/new-managed-disk-storage-option-for-your-azure-vms/>

<https://blogs.msdn.microsoft.com/azure4fun/2016/10/21/custom-azure-rbac-roles-and-how-to-extend-existing-role-definitions-scope/>

#### QUESTION 3

#### 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.

#### Select and Place:



Actions	Answer Area
From the Azure portal, create a managed identity.	
Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS).	
In Azure AD, enable authentication method policy.	
In SQLDB1, create contained database users.	
From the Azure portal, create an Azure AD administrator for LitwareSQLServer1.	

Correct Answer:

Actions	Answer Area
From the Azure portal, create a managed identity.	From the Azure portal, create an Azure AD administrator for LitwareSQLServer1.
	Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS).
In Azure AD, enable authentication method policy.	In SQLDB1, create contained database users.

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-gb/azure/azure-sql/database/authentication-aad-overview>

### 03 - Secure data and applications

#### QUESTION 1

DRAG DROP

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

The company is developing an application named App1. App1 will run as a service on server that runs Windows Server 2016. App1 will authenticate to contoso.com and access Microsoft Graph to read directory data.

You need to delegate the minimum required permissions to App1.

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

Select and Place:

**Actions**

- Grant permissions
- Add a delegated permission.
- Configure Azure AD Application Proxy.
- Add an application permission.
- Create an app registration.

**Answer Area**

Navigation icons: Left arrow, Right arrow, Up arrow, Down arrow.

CEplus.com watermark

Correct Answer:

**Actions**

- 
- Add a delegated permission.
- Configure Azure AD Application Proxy.
- 
- 

**Answer Area**

- Create an app registration.
- Add an application permission.
- Grant permissions

Navigation icons: Left arrow, Right arrow, Up arrow, Down arrow.

CEplus.com watermark

**Section:**

**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 2

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.

Hot Area:

Answer Area



CosmosDB1:

	▼
Authenticate Azure AD users and generate resource tokens.	
Authenticate Azure AD users and relay resource tokens.	
Create database users and generate resource tokens.	

WebApp1:

	▼
Authenticate Azure AD users and generate resource tokens.	
Authenticate Azure AD users and relay resource tokens.	
Create database users and generate resource tokens.	

Answer Area:

CosmosDB1:  ▼

Authenticate Azure AD users and generate resource tokens.  
 Authenticate Azure AD users and relay resource tokens.  
 Create database users and generate resource tokens.

WebApp1:  ▼

Authenticate Azure AD users and generate resource tokens.  
 Authenticate Azure AD users and relay resource tokens.  
 Create database users and generate resource tokens.

**Section:**

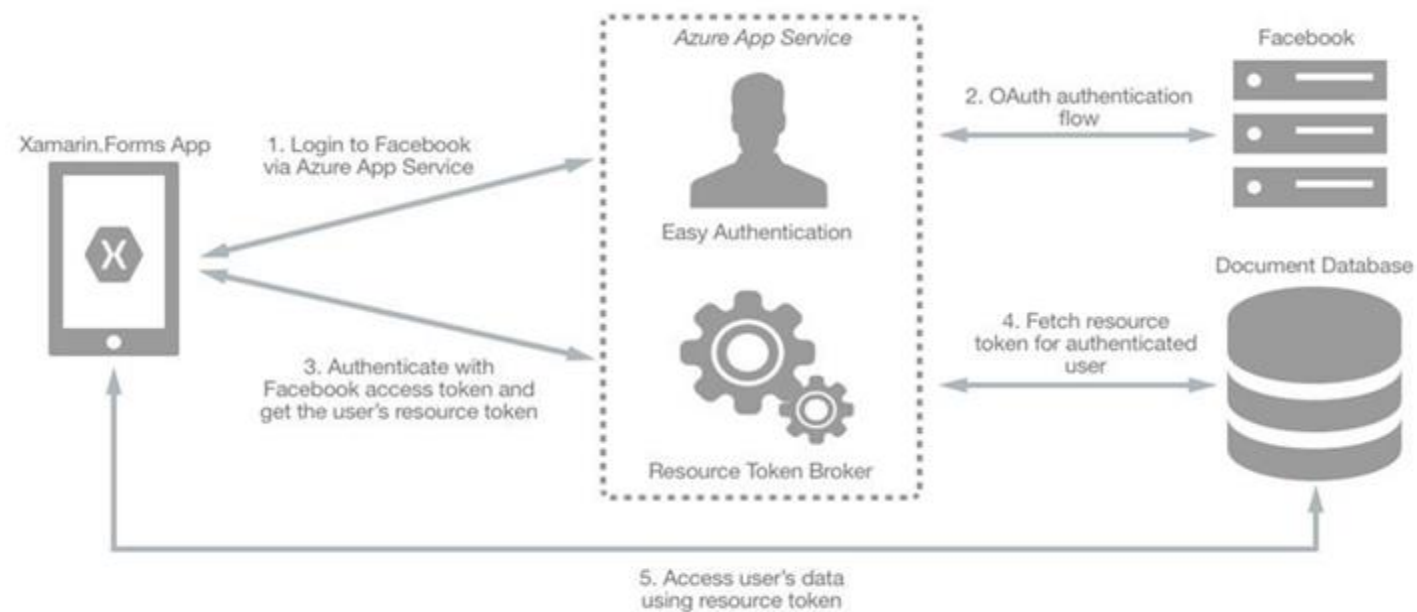
**Explanation:**

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 3**

**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.

Select and Place:

### Actions

Run Set-AzureRmKeyVaultAccessPolicy

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a user-assigned managed identity.

Create a connection resource in the Azure Automation account.

### Answer Area



Correct Answer:

### Actions

Run Set-AzureRmKeyVaultAccessPolicy

Create a user-assigned managed identity.

### Answer Area

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a connection resource in the Azure Automation account.

**Section:**

**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 4**



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.

**Correct Answer: B**

**Section:**

**Explanation:**

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

#### QUESTION 5

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.

**Select and Place:**

Actions	Answer Area
Configure secrets for the Azure key vault.	
Create an Azure key vault.	
Run Set-AzureRmStorageAccount.	
Configure access policies for the Azure key vault.	
Run Set-AzureRmVmDiskEncryptionExtension.	

**Correct Answer:**

Actions	Answer Area
Configure secrets for the Azure key vault.	Create an Azure key vault.
	Configure access policies for the Azure key vault.
Run Set-AzureRmStorageAccount.	Run Set-AzureRmVmDiskEncryptionExtension.

**Section:**

**Explanation:**

References:

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

#### QUESTION 6

You have a web app named WebApp1.

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

You need to protect WebApp1 by using WAF1.

What should you do first?

- A. Deploy an Azure Front Door.
- B. Add an extension to WebApp1.
- C. Deploy Azure Firewall.

**Correct Answer: A**

**Section:**

**Explanation:**

References:

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

#### QUESTION 7

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.

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

You need to configure the backup policy for the Azure SQL database.

1. 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.





2. Select the server hosting the Homepage database and click on Manage backups.
3. Click on Configure policies.
4. Ensure that the Weekly Backups option is ticked.
5. Configure the How long would you like weekly backups to be retained option to 8 weeks.
6. Click Apply to save the changes.

#### QUESTION 8

##### 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.

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

You need to configure an option in the Advanced Access Policy of the key vault.

1. 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.
2. In the properties of the key vault, click on Advanced Access Policies.
3. Tick the checkbox labelled Enable access to Azure Resource Manager for template deployment.
4. Click Save to save the changes.

#### QUESTION 9

##### 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.

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

You need to enable the Web Application Firewall on the Application Gateway.

1. 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.
2. In the properties of the application gateway, click on Web application firewall.
3. For the Tier setting, select WAF V2.
4. In the Firewall status section, click the slider to switch to Enabled.
5. In the Firewall mode section, click the slider to switch to Prevention.
6. Click Save to save the changes.

#### QUESTION 10

##### 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.

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

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

### QUESTION 11

#### 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.

Save Discard

Allow access from:  All networks  Selected networks

[Configure network access control for your key vault. Learn More](#)

Virtual networks: [+ Add existing virtual networks](#) [+ Add new virtual network](#)

VIRTUAL NETWORK	SUBNET	RESOURCE GROUP	SUBSCRIPTION
VNET1	default	RG1	...

Firewall: [?](#)

IPv4 ADDRESS OR CIDR

...

Exception:

Allow trusted Microsoft services to bypass this firewall?  Yes  No

[?](#) This setting is related to firewall only. In order to access this key vault, the trusted service must also be given explicit permissions in the Access policies section.

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Statements	Yes	No
From VM1, users can manage the keys and secrets stored in KeyVault1.	<input type="radio"/>	<input type="radio"/>
From VM2, users can manage the keys and secrets stored in KeyVault1.	<input type="radio"/>	<input type="radio"/>
VM2 can use KeyVault for Azure Disk Encryption	<input type="radio"/>	<input type="radio"/>

Answer Area:

## Answer Area

Statements	Yes	No
From VM1, users can manage the keys and secrets stored in KeyVault1.	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, users can manage the keys and secrets stored in KeyVault1.	<input checked="" type="radio"/>	<input type="radio"/>
VM2 can use KeyVault for Azure Disk Encryption	<input checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

### QUESTION 12

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.

**Correct Answer: A**

**Section:**

**Explanation:**

Azure Key Vault provides a way to securely store credentials and other keys and secrets, but your code needs to authenticate to Key Vault to retrieve them. Managed identities for Azure resources overview makes solving this problem simpler, by giving Azure services an automatically managed identity in Azure Active Directory (Azure AD). You can use this identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without having any credentials in your code. Example: How a system-assigned managed identity works with an Azure VM

After the VM has an identity, use the service principal information to grant the VM access to Azure resources. To call Azure Resource Manager, use role-based access control (RBAC) in Azure AD to assign the appropriate role to the VM service principal. To call Key Vault, grant your code access to the specific secret or key in Key Vault. References: <https://docs.microsoft.com/en-us/azure/key-vault/quick-create-net> <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

### QUESTION 13

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

**Correct Answer: C, E**

**Section:**

**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 14

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

**Correct Answer: C**

**Section:**

**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.

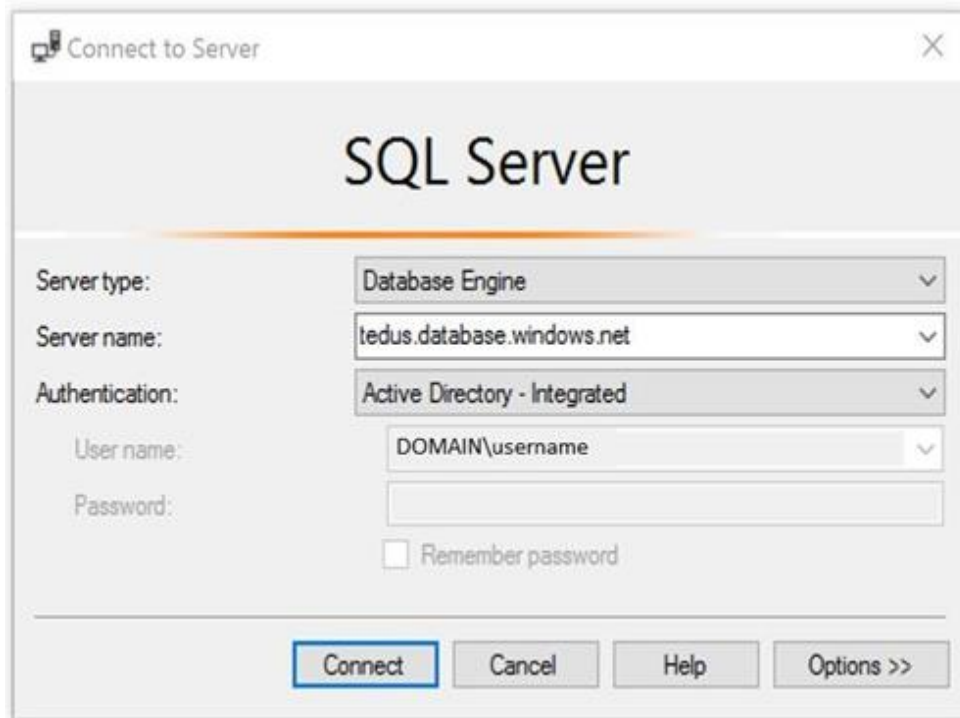
Using an Azure AD identity to connect using SSMS or SSDT

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 15

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.

**Correct Answer: B**

**Section:**

**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 16

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

**Correct Answer: C**

**Section:**

**Explanation:**

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

**QUESTION 17**

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.

Hot Area:

Answer Area

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

```
-Location 'East US'
```

<ul style="list-style-type: none"> <li>-EnabledForDeployment</li> <li>-EnablePurgeProtection</li> <li>-Tag</li> </ul>	<ul style="list-style-type: none"> <li>-Confirm</li> <li>-DefaultProfile</li> <li>-EnableSoftDelete</li> <li>-SKU</li> </ul>
---	--

Answer Area:

Answer Area

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

```
-Location 'East US'
```

<ul style="list-style-type: none"> <li>-EnabledForDeployment</li> <li style="background-color: #e0ffe0;">-EnablePurgeProtection</li> <li>-Tag</li> </ul>	<ul style="list-style-type: none"> <li>-Confirm</li> <li>-DefaultProfile</li> <li style="background-color: #e0ffe0;">-EnableSoftDelete</li> <li>-SKU</li> </ul>
--	---

**Section:**

**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/azurermskeyvault/new-azurermskeyvault>

#### QUESTION 18

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

**Correct Answer: A**

**Section:**

**Explanation:**

References:

<https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault>



#### QUESTION 19

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.)

## Create a secret

### Upload options

Manual

### \* Name ?

Password1

### \* Value

••••••••••

### Content type (optional)

Set activation date? ?

### Activation Date

2019-03-01  12:00:00 AM

(UTC+02:00) --- Current Time Zone ---

Set expiration date? ?

### Expiration Date

2020-03-01  12:00:00 AM

(UTC+02:00) --- Current Time Zone ---

Enabled?

Yes

No

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 policy 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.

NOTE: Each correct selection is worth one point.

Hot Area:



## Answer Area

Statements	Yes	No
On January 1, 2019, User1 can view the value of Password1.	<input type="radio"/>	<input type="radio"/>
On June 1, 2019, User2 can view the value of Password1.	<input type="radio"/>	<input type="radio"/>
On June 1, 2019, User1 can view the value of Password1.	<input type="radio"/>	<input type="radio"/>

Answer Area:

## Answer Area

Statements	Yes	No
On January 1, 2019, User1 can view the value of Password1.	<input type="radio"/>	<input checked="" type="radio"/>
On June 1, 2019, User2 can view the value of Password1.	<input checked="" type="radio"/>	<input type="radio"/>
On June 1, 2019, User1 can view the value of Password1.	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

### QUESTION 20

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.)

## Protection

Contoso1812 - Azure Information Protection

### Protections settings ⓘ

Azure (cloud key) **HYOK (AD RMS)**

Select the protection action type ⓘ

- Set permissions
- Set user-defined permissions (Preview)

USERS	PERMISSIONS
AuthenticatedUsers	Viewer
User1@contoso1812.onmicrosoft.com	Co-Author
User2@contoso1812.onmicrosoft.com	Reviewer

[+Add permissions](#)

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.



Hot Area:

### Answer Area

Statements	Yes	No
User1 can print File1.	<input type="radio"/>	<input type="radio"/>
User3 can read File1.	<input type="radio"/>	<input type="radio"/>
User4 can print File1.	<input type="radio"/>	<input type="radio"/>

Answer Area:

## Answer Area

Statements	Yes	No
User1 can print File1.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can read File1.	<input checked="" type="radio"/>	<input type="radio"/>
User4 can print File1.	<input type="radio"/>	<input checked="" type="radio"/>

**Section:**

**Explanation:**

### QUESTION 21

SIMULATION

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

A.

**Correct Answer: A**

**Section:**

**Explanation:**

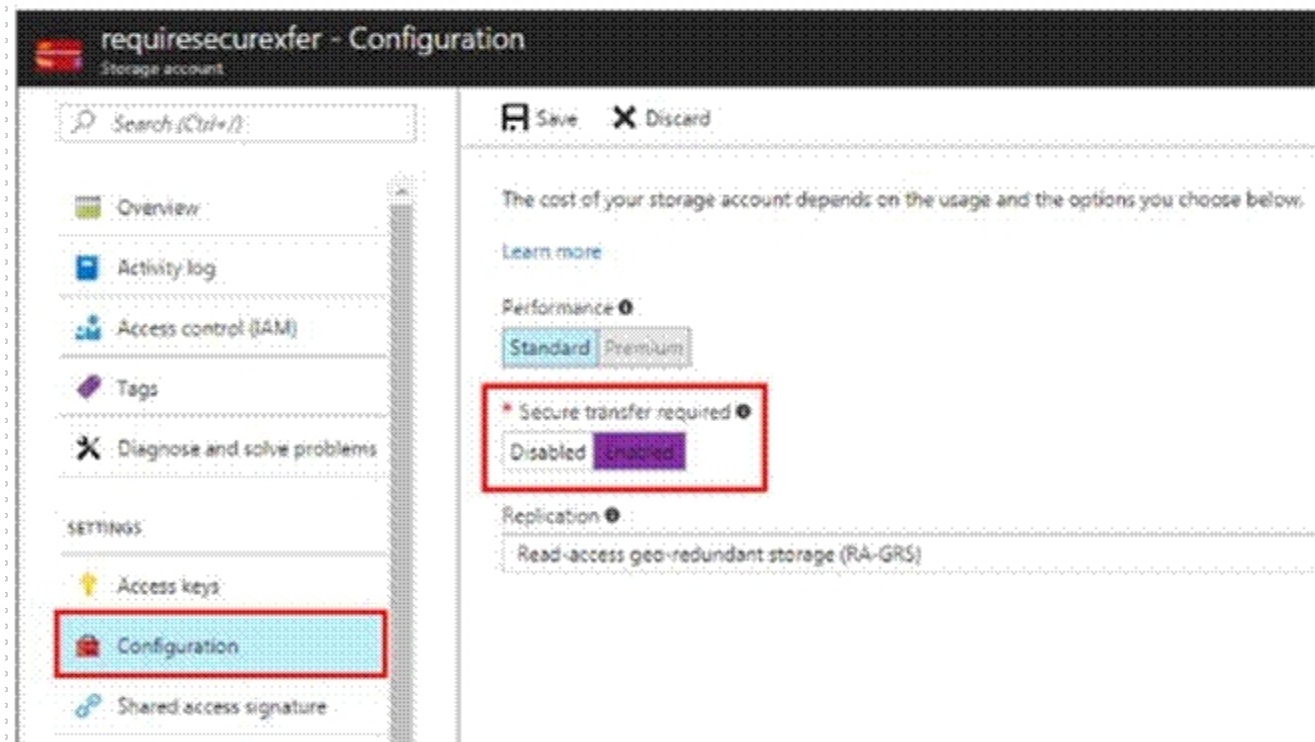
Answer: A

Explanation:

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 22

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

**Correct Answer: C**

**Section:**

**Explanation:**

#### QUESTION 23

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         :
TagsTable    :
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
```

When 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.

Hot Area:

Answer Area



Password1:

	▼
Never	
Always	
Only after May 1, 2019	

Password2:

	▼
Never	
Always	
Only between March 1, 2019 and May 1. 2019	

Answer Area:

## Answer Area

Password1:

- Never
- Always
- Only after May 1, 2019

Password2:

- Never
- Always
- Only between March 1, 2019 and May 1, 2019

### Section:

#### 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 24

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

**Correct Answer: B**

#### Section:

#### 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 25

#### 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	Use condition	Label is applied
Label1	Condition1	Automatically
Label2	Condition2	Automatically

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

Name	Applies to	Use label	Set the default label
Global	<i>Not applicable</i>	<i>None</i>	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.

Hot Area:

**Answer Area**  


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 Area:

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	

**Section:**

**Explanation:**

Box 1: Label 2 only

How multiple conditions are evaluated when they apply to more than one label

1. 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).
2. The most sensitive label is applied.
3. 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 26**

**HOTSPOT**

You have an Azure Storage account that contains a blob container named container1 and a client application named App1.

You need to enable App1 access to container1 by using Azure Active Directory (Azure AD) authentication.

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

NOTE: Each correct selection is worth one point.

**Hot Area:**



**Answer Area**

From Azure AD:  ▼

- Register App1.
- Create an access package.
- Implement an application proxy.
- Modify the authentication methods.

From the storage account:  ▼

- Add a private endpoint.
- Regenerate the access key.
- Configure Access control (IAM).
- Generate a shared access signature (SAS).

Answer Area:

**Answer Area**

From Azure AD:  ▼

- Register App1.
- Create an access package.
- Implement an application proxy.
- Modify the authentication methods.

From the storage account:  ▼

- Add a private endpoint.
- Regenerate the access key.
- Configure Access control (IAM).
- Generate a shared access signature (SAS).



**Section:**

**Explanation:**

Reference:

<https://azure.microsoft.com/en-in/blog/announcing-the-preview-of-aad-authentication-for-storage/>

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/storage/common/storage-auth-aad-rbac-portal.md>

**QUESTION 27**

HOTSPOT

You have an Azure subscription that contains an Azure key vault named ContosoKey1.

You create users and assign them roles as shown in the following table.

Name	Subscription role assignment	ContosoKey1 role assignment
User1	Owner	None
User2	Security Admin	None
User3	None	User Access Administrator
User4	None	Key Vault Contributor

You need to identify which users can perform the following actions:

Delegate permissions for ContosoKey1.

Configure network access to ContosoKey1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Delegate permissions for ContosoKey1:

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

Configure network access to ContosoKey1:

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

Answer Area:

## Answer Area

Delegate permissions for ContosoKey1:

▼
User1 only
User1 and User2 only
User1 and User3 only
User1 and User4 only
User1, User2, and User3 only
User1, User2, User3, and User4

Configure network access to ContosoKey1:

▼
User1 only
User1 and User2 only
User1 and User3 only
User1 and User4 only
User1, User2, and User3 only
User1, User2, User3, and User4

**Section:**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-gb/azure/key-vault/general/rbac-guide>



### QUESTION 28

You have an Azure subscription that contains four Azure SQL managed instances.

You need to evaluate the vulnerability of the managed instances to SQL injection attacks.

What should you do first?

- A. Create an Azure Sentinel workspace.
- B. Enable Advanced Data Security.
- C. Add the SQL Health Check solution to Azure Monitor.
- D. Create an Azure Advanced Threat Protection (ATP) instance.

**Correct Answer: B**

**Section:**

### QUESTION 29

DRAG DROP

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains a user named User1.

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains an Azure Storage account named storage1. Storage1 contains an Azure file share named share1.

Currently, the domain and the tenant are not integrated.

You need to ensure that User1 can access share1 by using his domain credentials.

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

Select and Place:

**Actions**

- Create a private link to storage1.
- Enable Active Directory Domain Services (AD DS) authentication on storage1.
- Implement Azure AD Connect.
- Create a service endpoint to storage1.
- Assign share-level permissions for share1.

**Answer Area**

Correct Answer:

**Actions**

- Create a private link to storage1.
- 
- 
- Create a service endpoint to storage1.
- 

**Answer Area**

- Implement Azure AD Connect.
- Enable Active Directory Domain Services (AD DS) authentication on storage1.
- Assign share-level permissions for share1.

**Section:**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-enable>

**QUESTION 30**

You have an Azure subscription that contains an Azure SQL database named sql1.

You plan to audit sql1.

You need to configure the audit log destination. The solution must meet the following requirements:  
Support querying events by using the Kusto query language.  
Minimize administrative effort.  
What should you configure?

- A. an event hub
- B. a storage account
- C. a Log Analytics workspace

**Correct Answer: C**

**Section:**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-log-analytics-wizard>

**QUESTION 31**

HOTSPOT

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

Name	Performance	Account kind	Azure Data Lake Storage Gen2
storage1	Standard	BlobStorage	Enabled
storage2	Premium	BlockBlobStorage	Disabled
storage3	Standard	Storage	Disabled
storage4	Premium	FileStorage	Disabled
storage5	Standard	StorageV2	Enabled

You enable Azure Defender for Storage.

Which storage services of storage5 are monitored by Azure Defender for Storage, and which storage accounts are protected by Azure Defender for Storage? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Hot Area:**

**Answer Area**

Monitored storage5 services:

- File services only
- Data Lake Storage only
- File services and table services only
- File service and Data Lake Storage only
- Data Lake Storage, file services, and table services

Protected storage accounts:

- storage3 and storage5 only
- storage1, storage2, and storage5 only
- storage1, storage4, and storage5 only
- storage1, storage2, storage3, storage4, and storage5

Answer Area:

**Answer Area**

Monitored storage5 services:

- File services only
- Data Lake Storage only
- File services and table services only
- File service and Data Lake Storage only
- Data Lake Storage, file services, and table services

Protected storage accounts:

- storage3 and storage5 only
- storage1, storage2, and storage5 only
- storage1, storage4, and storage5 only
- storage1, storage2, storage3, storage4, and storage5

**Section:**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/azure-defender-storage-configure?tabs=azure-security-center>

**QUESTION 32**

You have an Azure subscription that contains as 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 support data encryption by using the keys stored in the key vault? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

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

**Correct Answer: B, C**

**Section:**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption>

### QUESTION 33

DRAG DROP

You have an Azure subscription.

You plan to create a storage account.

You need to use customer-managed keys to encrypt the tables in the storage account.

From Azure Cloud Shell, which three cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.

Select and Place:

#### Cmdlets

New-AzStorageAccountKey

New-AzStorageTable

Register-AzProviderFeature

New-AzStorageAccount

Register-AzResourceProvider



Answer Area 



**Correct Answer:**

### Cmdlets

Register-AzProviderFeature
Register-AzResourceProvider



### Answer Area

New-AzStorageAccount
New-AzStorageAccountKey
New-AzStorageTable



**Section:**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-key-vault?tabs=powershell>

**QUESTION 34**

**HOTSPOT**

You have an Azure subscription that contains the following resources:

An Azure key vault

An Azure SQL database named Database1

Two Azure App Service web apps named AppSrv1 and AppSrv2 that are configured to use system-assigned managed identities and access Database1

You need to implement an encryption solution for Database1 that meets the following requirements:

The data in a column named Discount in Database1 must be encrypted so that only AppSrv1 can decrypt the data. AppSrv1 and AppSrv2 must be authorized by using managed identities to obtain cryptographic keys.

How should you configure the encryption settings for Database1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Hot Area:**



## Answer Area

To configure the encryption of Database1:

- Always Encrypted by using Azure Key Vault.
- Always Encrypted by using the Windows Certificate Store.
- Transparent Data Encryption (TDE) by using Azure Key Vault integration.
- Transparent Data Encryption (TDE) by using Bring Your Own Key (BYOK).

To obtain the cryptographic keys:

- Create an access policy in Azure Key Vault.
- Generate a key on an HSM device.
- Import App Service certificates to AppSrv1 and AppSrv2.
- Register an enterprise application in Azure AD.

Answer Area:

## Answer Area



To configure the encryption of Database1:

- Always Encrypted by using Azure Key Vault.
- Always Encrypted by using the Windows Certificate Store.
- Transparent Data Encryption (TDE) by using Azure Key Vault integration.
- Transparent Data Encryption (TDE) by using Bring Your Own Key (BYOK).

To obtain the cryptographic keys:

- Create an access policy in Azure Key Vault.
- Generate a key on an HSM device.
- Import App Service certificates to AppSrv1 and AppSrv2.
- Register an enterprise application in Azure AD.

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/always-encrypted-azure-key-vault-configure?tabs=azure-powershell>

QUESTION 35

DRAG DROP

You have an Azure Storage account named storage1 and an Azure virtual machine named VM1. VM1 has a premium SSD managed disk.

You need to enable Azure Disk Encryption for VM1.

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

Select and Place:

### Actions

Run the `Set-AzVMDiskEncryptionExtension` cmdlet.

Set the Key Vault access policy to **Enable access to Azure Virtual Machines for deployment**.

Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption**.

Generate a key vault certificate.

Create an Azure key vault.

Configure storage1 to use a customer-managed key.

Correct Answer:

### Actions

Set the Key Vault access policy to **Enable access to Azure Virtual Machines for deployment**.

Generate a key vault certificate.

Configure storage1 to use a customer-managed key.

Section:

Explanation:

### Answer Area



### Answer Area

Create an Azure key vault.

Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption**.

Run the `Set-AzVMDiskEncryptionExtension` cmdlet.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault>

### QUESTION 36

#### 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.

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

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 Advanced data security.
3. Click on the Settings icon.
4. Tick the Enable Advanced Data Security at the database level checkbox.
5. Click Yes at the confirmation prompt.
6. In the Storage account select a storage account if one isn't selected by default.
7. Under Advanced Threat Protection Settings, enter User1@contoso.com in the Send alerts to box.
8. Click the Save button to save the changes.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/advanced-data-security>



### QUESTION 37

#### 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.

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

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

Enable Access to:

- Azure Virtual Machines for deployment ⓘ
- Azure Resource Manager for template deployment ⓘ
- Azure Disk Encryption for volume encryption ⓘ

4. Click Save to save the changes.

### QUESTION 38

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

**Correct Answer: B**

**Section:**

**Explanation:**

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 39

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



**Correct Answer: A**

**Section:**

**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 40

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

**Correct Answer: C**

**Section:**

**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 41**

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.

Hot Area:

**Answer Area**

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 Area:

## Answer Area

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	

**Section:**

**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 42**

HOTSPOT

You have an Azure subscription that contains a web app named 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.

**Hot Area:**

**Answer Area**

Configure App1 to authenticate by using a:

Key
Certificate
Passphrase
User-assigned managed identity
System-assigned managed identity

Configure a Key Vault reference for App1 from the:

Extensions blade
General settings tab
TLS/SSL settings blade
Application settings tab

Answer Area:

**Answer Area**



Configure App1 to authenticate by using a:

Key
Certificate
Passphrase
User-assigned managed identity
System-assigned managed identity

Configure a Key Vault reference for App1 from the:

Extensions blade
General settings tab
TLS/SSL settings blade
Application settings tab

**Section:**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet>

**QUESTION 43**

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 KeyVault1, the following events occur in sequence:

Item1 is deleted.

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.

Hot Area:

**Answer Area**

Statements	Yes	No
You can recover Policy1.	<input type="radio"/>	<input type="radio"/>
You can add a new key named Item1.	<input type="radio"/>	<input type="radio"/>
You can recover Item2.	<input type="radio"/>	<input type="radio"/>

Answer Area:



## Answer Area

Statements	Yes	No
You can recover Policy1.	<input type="radio"/>	<input checked="" type="radio"/>
You can add a new key named Item1.	<input type="radio"/>	<input checked="" type="radio"/>
You can recover Item2.	<input checked="" type="radio"/>	<input type="radio"/>

### Section:

### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview>

### QUESTION 44

#### SIMULATION

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.

A.

### Correct Answer: A

### Section:

### Explanation:

Answer: A

Explanation:

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.

Vdumps

Save X Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data is encrypted using Microsoft Managed Keys for Azure Blobs, Tables, Files and Queues. You may choose to bring your own key for encryption for Azure Blobs and Files. Encryption for Tables and Queues will always use Microsoft Managed Keys.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

[Learn more](#)

Your storage account is currently encrypted with Microsoft managed key by default. You can choose to use your own key.

Use your own key

**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.

Save X Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data is encrypted using Microsoft Managed Keys for Azure Blobs, Tables, Files and Queues. You may choose to bring your own key for encryption for Azure Blobs and Files. Encryption for Tables and Queues will always use Microsoft Managed Keys.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

[Learn more](#)

Your storage account is currently encrypted with Microsoft managed key by default. You can choose to use your own key.

Use your own key

Encryption key

Enter key URI

Select from Key Vault

---

\* Key Vault >

<key-vault>

\* Encryption key >

<key>

**i** <storage-account> will be granted access to the selected key vault. Both soft delete and purge protection will be enabled on the key vault and cannot be disabled. [Learn more](#)

Reference:

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

**QUESTION 45**

**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.

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

You need to assign the user the Key Vault Secrets Officer role.

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, select Access control (IAM).
3. In the Add a role assignment section, click the Add button.
4. In the Role box, select the Key Vault Secrets Officer role from the drop-down list.
5. In the Select box, start typing User2-11641655 and select User2-11641655 from the search results.
6. Click the Save button to save the changes.

#### QUESTION 46

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.

**Correct Answer: B**

**Section:**

**Explanation:**

Reference:

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

#### Exam L

#### QUESTION 1

You have an Azure subscription.

You plan to create a workflow automation in Azure Security Center that will automatically remediate a security vulnerability. What should you create first?

- A. an automation account
- B. a managed identity
- C. an Azure logic app
- D. an Azure function app
- E. an alert rule

**Correct Answer: C**

**Section:**

**Explanation:**

Reference: <https://docs.microsoft.com/en-us/azure/security-center/workflow-automation>



**QUESTION 2**

**HOTSPOT**

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

Name	Type
storage1	Azure Blob storage
storage2	Azure Files SMB
storage3	Azure Table storage

You need to configure authorization access.

Which authorization types can you use for each storage account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

storage1:  Shared Key only  
 Shared access signature (SAS) only  
 Azure Active Directory (Azure AD) only  
 Shared Key and shared access signature (SAS) only  
 Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

storage2:  Shared Key only  
 Shared access signature (SAS) only  
 Shared Key and shared access signature (SAS)

storage3:  Shared Key only  
 Shared access signature (SAS) only  
 Azure Active Directory (Azure AD) only  
 Shared Key and shared access signature (SAS) only  
 Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

Answer Area:

## Answer Area

storage1:

Shared Key only
Shared access signature (SAS) only
Azure Active Directory (Azure AD) only
Shared Key and shared access signature (SAS) only
Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

storage2:

Shared Key only
Shared access signature (SAS) only
Shared Key and shared access signature (SAS)

storage3:

Shared Key only
Shared access signature (SAS) only
Azure Active Directory (Azure AD) only
Shared Key and shared access signature (SAS) only
Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

**Section:**

**Explanation:**

Reference: <https://docs.microsoft.com/en-us/azure/storage/common/authorize-data-access> 0CB84EF020870C137158A568970423A4

### QUESTION 3

You have an Azure Active Directory (Azure AD) tenant. The tenant contains users that are assigned Azure AD Premium Plan 2 licenses. You have a partner company that has a domain named The fabrikam.com domain contains a user named user1. User1 has an email address of user1@fabrikam.com. You to provide User1 with to the resources in the tenant The solution must meet the following requirements: user1 must be able to sign in by using the user1@fabrikam.com credentials You must be able to grant User1 access to the resources in the tenant Administrative effort must be minimized. What should you do?

- A. Create a user account for user1.
- B. Create an invite for User1.
- C. To the tenant add fabrikamcom as a custom domain
- D. Set Enable guest self-service sign up via user flows to Yes for the tenant.

**Correct Answer: B**

**Section:**

### QUESTION 4

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

Name	Type
storage1	Storage account
Vault1	Azure Key vault
Vault2	Azure Key vault

You plan to deploy the virtual machines shown in the following table.

Name	Role
VM1	<ul style="list-style-type: none"> <li>Storage Blob Data Reader for storage1</li> <li>Key Vault Reader for Vault1</li> </ul>
VM2	<ul style="list-style-type: none"> <li>Storage Blob Data Reader for storage1</li> <li>Key Vault Reader for Vault1</li> </ul>
VM3	<ul style="list-style-type: none"> <li>Storage Blob Data Reader for storage1</li> <li>Key Vault Reader for Vault1</li> <li>Key Vault Reader for Vault2</li> </ul>
VM4	<ul style="list-style-type: none"> <li>Storage Blob Data Reader for storage1</li> <li>Key Vault Reader for Vault1</li> <li>Key Vault Reader for Vault2</li> </ul>

You need to assign managed identities to the virtual machines. The solution must meet the following requirements:  
 Assign each virtual machine the required roles. Use the principle of least privilege.  
 What is the minimum number of managed identities required?

- A. 1
- B. 2
- C. 3
- D. 4

**Correct Answer: B**

**Section:**

**Explanation:**

We have two different sets of required permissions. VM1 and VM2 have the same permission requirements. VM3 and VM4 have the same permission requirements.

A user-assigned managed identity can be assigned to one or many resources. By using user-assigned managed identities, we can create just two managed identities: one with the permission requirements for VM1 and VM2 and the other with the permission requirements for VM3 and VM4.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

**QUESTION 5**

## SIMULATION

You need to ensure that a user named user2-12345678 can manage the properties of the virtual machines in the RG1lod12345678 resource group. The solution must use the principle of least privilege. To complete this task, sign in to the Azure portal.

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

1. Sign in to the Azure portal.
2. Browse to Resource Groups.
3. Select the RG1lod12345678 resource group.
4. Select Access control (IAM).
5. Select Add > role assignment.
6. Select Virtual Machine Contributor (you can filter the list of available roles by typing 'virtual' in the search box) then click Next.
7. Select the +Select members option and select user2-12345678 then click the Select button.
8. Click the Review + assign button twice.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal?tabs=current>

## QUESTION 6

### 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: User1-28681041@ExamUsers.com

Azure Password: GpOAe4@IDg

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab. The following information is for technical support purposes only:

Lab Instance: 28681041

Task 10

You need to create a new Azure AD directory named 28681041.onmicrosoft.com. The new directory must contain a new user named user1@28681041.onmicrosoft.com.

A.

**Correct Answer: A**

**Section:**

**Explanation:**

Answer: A

Explanation:

The first step is to create the Azure Active Directory tenant.

To create a new Azure AD directory named 28681041.onmicrosoft.com that contains a new user named user1@28681041.onmicrosoft.com, you can follow these steps:

In the Azure portal, search for and select Azure Active Directory.

In the left pane, select Domains.

Select Add domain.

In the Add a custom domain pane, enter the following information:

Domain name: Enter the domain name you want to use. For example, 28681041.onmicrosoft.com.

Add domain: Select Add domain.

In the left pane, select Users.

Select New user.

In the New user pane, enter the following information:

User name: Enter the user name you want to use. For example, user1@28681041.onmicrosoft.com.

Name: Enter the name of the user.

Password: Enter a password for the user.

Groups: Select the groups you want the user to be a member of.

Select Create.

You can find more information on these topics in the following Microsoft documentation:

Add a custom domain name to Azure Active Directory

Create a new user in your organization - Azure Active Directory

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant> <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory>

#### QUESTION 7

You have an Azure Active Directory (Azure AD) tenant that contains a group named Group1. You need to ensure that the members of Group1 sign in by using passwordless authentication. What should you do?

- A. Configure the Microsoft Authenticator authentication method policy.
- B. Configure the certificate-based authentication (CBA) policy.
- C. Configure the sign-in risk policy.
- D. Create a Conditional Access policy.

**Correct Answer: A**

**Section:**

#### QUESTION 8

You have an Azure subscription that contains a web app named App1.

Users must be able to select between a Google identity or a Microsoft identity when authenticating to App1. You need to add Google as an identity provider in Azure AD.

Which two pieces of information should you configure? Each correct answer presents part of the solution. Each correct selection is worth one point.

- A. a tenant name
- B. a tenant ID
- C. the endpoint URL of an application
- D. a client ID
- E. a client secret

**Correct Answer: D, E**

**Section:**

**Explanation:**

<https://learn.microsoft.com/en-us/azure/app-service/configure-authentication-provider-google>

#### QUESTION 9

You have an Azure key vault named Vault1 that stores the resources shown in the following table.

Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

Which resources support the creation of a rotation policy?



- A. Key1 Only
- B. Cert1 only
- C. Key1 and Secret1 only
- D. Key1 and Cert1 only
- E. Secret1 and Cert1 only
- F. Key1, Secret1, and Cert1

**Correct Answer: C**

**Section:**

#### QUESTION 10

You have an Azure subscription that contains a  
You need to grant user1 access to blob1. The solution must ensure that the access expires after six days. What should you use?

- A. a shared access policy
- B. a shared access signature (SAS)
- C. role-based access control (RBAC)
- D. a managed identity

**Correct Answer: C**

**Section:**

**Explanation:**

Depending on how you want to authorize access to blob data in the Azure portal, you'll need specific permissions. In most cases, these permissions are provided via Azure role-based access control (Azure RBAC). For more information about Azure RBAC, see [What is Azure role-based access control \(Azure RBAC\)?](#).

<https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal>

#### QUESTION 11

HOTSPOT

You have an Azure subscription that contains an Azure SQL database named SQL1.

You plan to deploy a web app named App1.

You need to provide App1 with read and write access to SQL1. The solution must meet the following requirements:

Provide App1 with access to SQL1 without storing a password.

Use the principle of least privilege. Minimize administrative effort.

Which type of account should App1 use to access SQL1, and which database roles should you assign to App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Hot Area:**

**Answer area**

Account type:

Azure Active Directory User
Managed identity
Service Principal

Roles:

db_datawriter only
db_datareader and db_datawriter
db owner only

Answer Area:



**Answer area**

Account type:

Azure Active Directory User
Managed identity
Service Principal

Roles:

db_datawriter only
db_datareader and db_datawriter
db owner only

Section:

**Explanation:**

<https://docs.microsoft.com/en-us/azure/app-service/tutorial-connect-msi-sql-database?tabs=windowsclient%2Cdotnet>

**QUESTION 12**

**HOTSPOT**

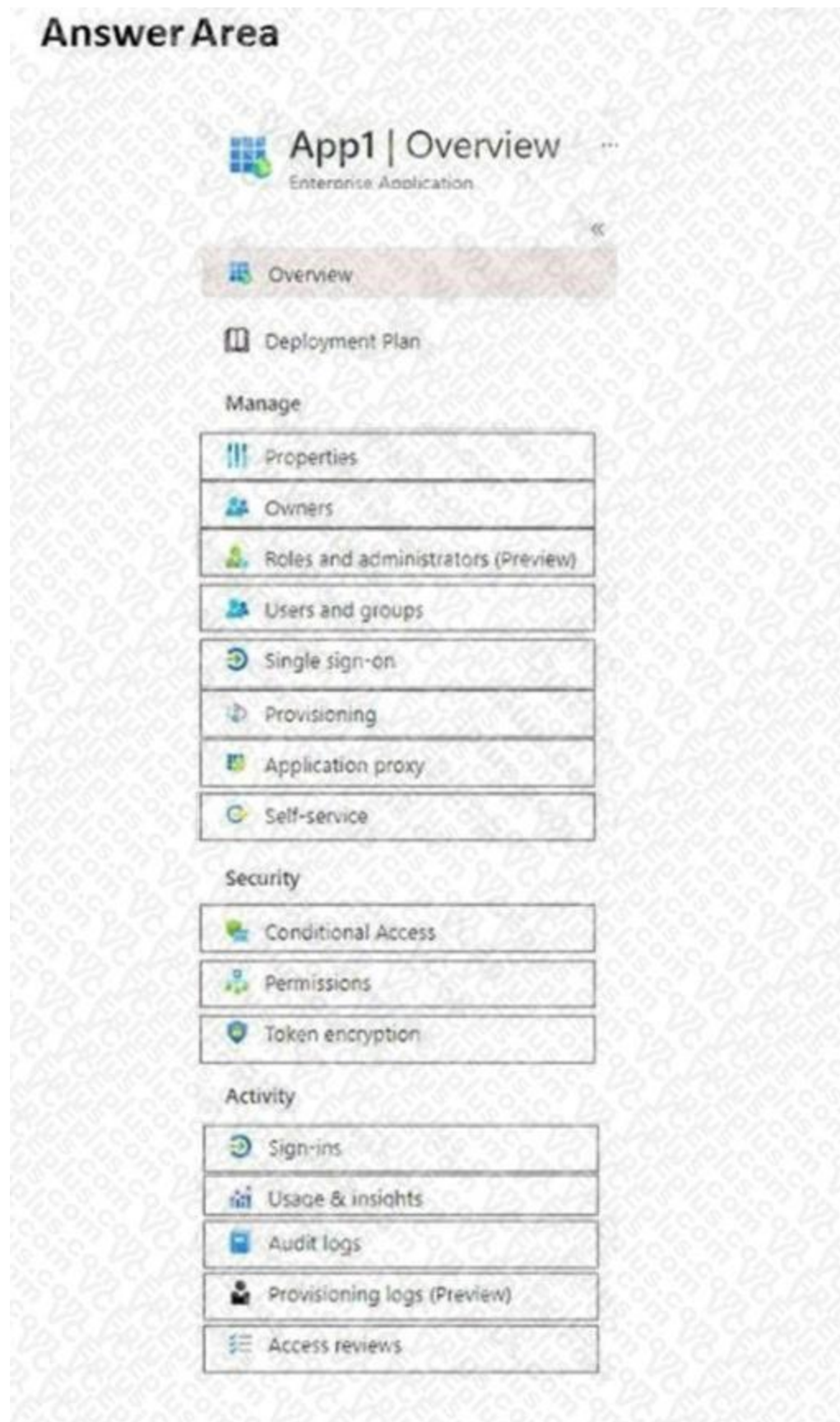
You have an Azure Active Directory (Azure AD) tenant that contains two users named User1 and User2 and a registered app named App1. You create an app-specific role named Role1. You need to assign Role1 to User1 and enable User2 to request access to App1.

Which two settings should you modify? To answer, select the appropriate settings in the answer area. NOTE: Each correct selection is worth one point.

**Hot Area:**

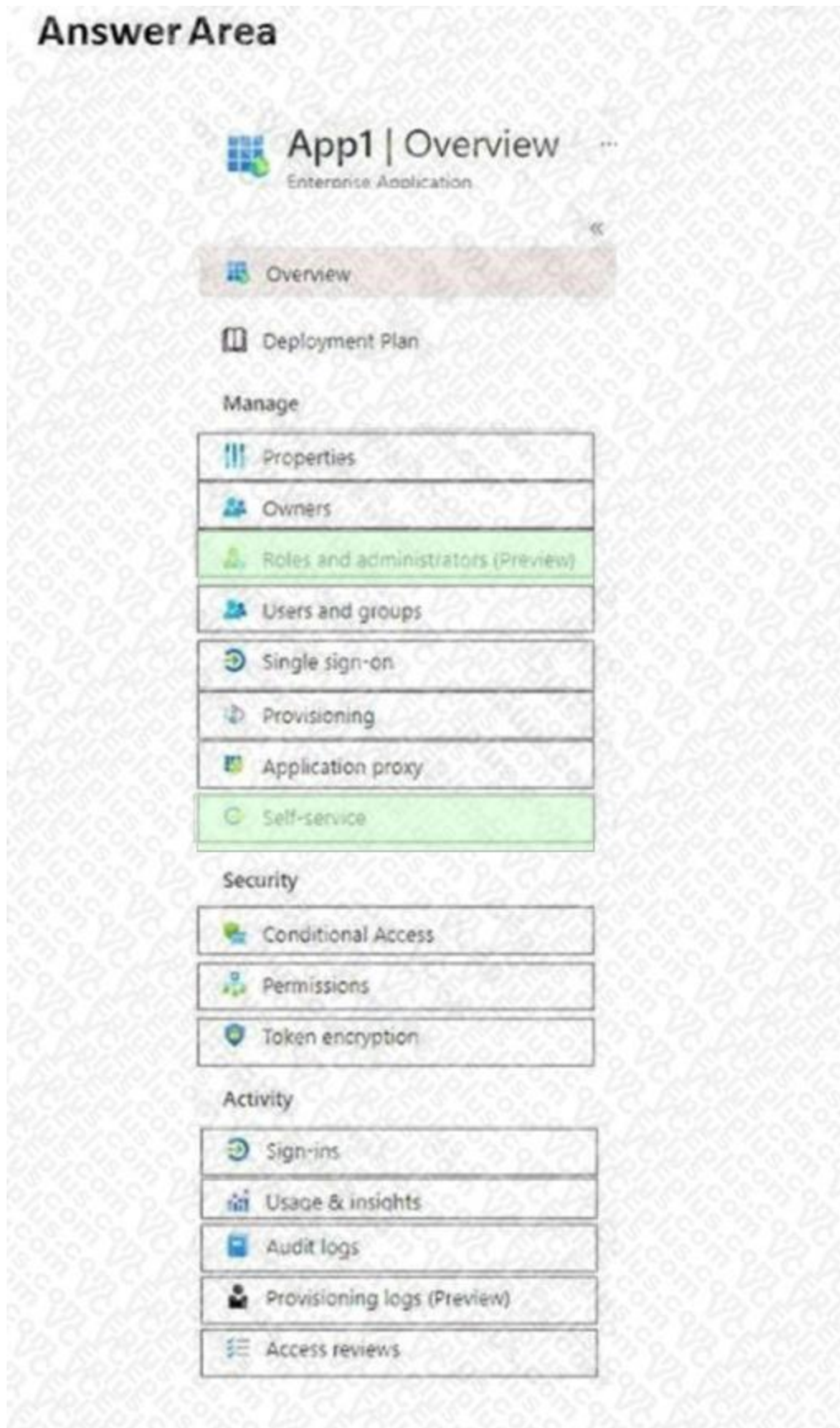


# Answer Area



Answer Area:





**Section:**

**Explanation:**

Box 1: Roles and administrators

Here you will find Role1 and be able to assign User1 to the role.

Box 2: Self Service

Under Self Service, there is an option to "Allow users to request access to this application".



**QUESTION 13**

**HOTSPOT**

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

Name	Member of group	Multi-factor authentication (MFA) status
User1	Group1, Group2	Enabled
User2	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: Low and above

Access: Allow access, Require multi-factor authentication

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

What should you identify for each user? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Hot Area:**

**Answer Area**

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

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

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

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

**Answer Area:**

**Answer Area**

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

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

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

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

**Section:**

**Explanation:**

Reference: <http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-accesspolicies/> <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protectionpolicies> <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protectionrisks>

#### QUESTION 14

You have an Azure subscription name Sub1 that contains an Azure Policy definition named Policy1. Policy1 has the following settings:

Definition location: Tenant Root Group

Category: Monitoring

You need to ensure that resources that are noncompliant with Policy1 are listed in the Azure Security Center dashboard. What should you do first?

- A. Change the Category of Policy1 to Security Center.
- B. Add Policy1 to a custom initiative.
- C. Change the Definition location of Policy1 to Sub1.
- D. Assign Policy1 to Sub1.

**Correct Answer: D**

**Section:**

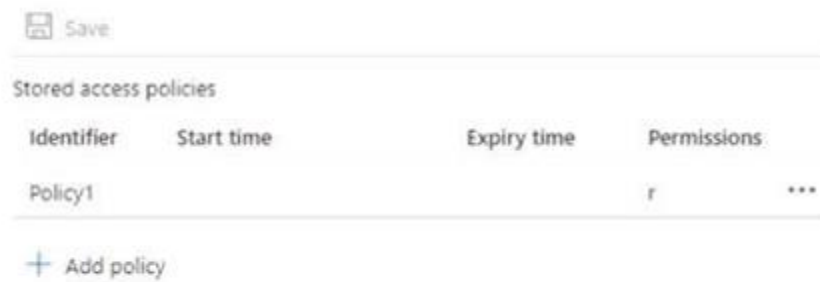
**Explanation:**

Reference: <https://docs.microsoft.com/en-us/azure/governance/policy/overview>

#### QUESTION 15

HOTSPOT

You have an Azure subscription that contains a blob container named cont1. Cont1 has the access policies shown in the following exhibit.



The screenshot shows a table titled "Stored access policies" with a "Save" button at the top and an "Add policy" button at the bottom. The table has four columns: "Identifier", "Start time", "Expiry time", and "Permissions". There is one row with the identifier "Policy1", an empty "Start time" and "Expiry time" field, and "r" in the "Permissions" column. A three-dot menu icon is visible to the right of the "Permissions" cell.

Identifier	Start time	Expiry time	Permissions
Policy1			r ***

The logo for "Vdumps" features a stylized orange "V" followed by the word "dumps" in a grey, lowercase, sans-serif font.

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

**Hot Area:**

The maximum number of additional stored access policies that you can add to cont1 is [answer choice].

  
  
1  
2  
4  
7  
15

The maximum number of additional immutable blob storage policies that you can add to cont1 is [answer choice].

  
  
1  
2  
4  
7  
15

**Answer Area:**

The maximum number of additional stored access policies that you can add to cont1 is [answer choice].

  
  
1  
2  
4  
7  
15

**Vdumps**

The maximum number of additional immutable blob storage policies that you can add to cont1 is [answer choice].

  
  
1  
2  
4  
7  
15

**Section:**

**Explanation:**

**QUESTION 16**

You have an Azure environment.



You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001:2013 standards. What should you use?

- A. Azure Active Directory (Azure AD) Identity Protection
- B. Microsoft Defender for Cloud
- C. Microsoft Defender for Identity
- D. Microsoft Sentinel

**Correct Answer: B**

**Section:**

#### QUESTION 17

You have an Azure subscription that contains an Azure SQL database named DB1 in the East US Azure region. You create the storage accounts shown in the following table.

Name	Location	Performance	Premium account type
storage1	East US	Standard	<i>Not applicable</i>
storage2	East US	Premium	Block blobs
storage3	East US	Premium	File shares
storage4	East US 2	Standard	<i>Not applicable</i>

You plan to enable auditing for DB1.

Which storage accounts can you use as the auditing destination for DB1?

- A. storage1 only
- B. storage1 and storage4 only
- C. Storage2 and storage3 only
- D. storage1, storage2 and storage3 only

**Correct Answer: C**

**Section:**

#### QUESTION 18

You have an Azure subscription that contains an Azure Files share named share1 and a user named User1. Identity-based authentication is configured for share1. User1 attempts to access share1 from a Windows 10 device by using SMB.

Which type of token will Azure Files use to authorize the request?

- A. OAuth 2.0
- B. JSON Web Token (JWT)
- C. Kerberos
- D. SAML

**Correct Answer: C**

**Section:**

#### QUESTION 19

You have an Azure subscription that contains an Azure key vault.

You need to configure maximum number of days for Which new keys are valid. The solution must minimize administrative effort. What should you use?

- A. Key Vault properties
- B. Azure Policy



- C. Azure Purview
- D. Azure Blueprints

**Correct Answer: B**

**Section:**

**QUESTION 20**

You have an Azure key vault named Vault1 that stores the resources shown in the following table.

Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

Which resources support the creation of a rotation policy?

- A. Key 1 only
- B. Cert1 only
- C. Key1 and Secret1 only
- D. Key1 and Cert1 only
- E. Secret1 and Cert1 only
- F. Key1, Secret1, and Cert1

**Correct Answer: A**

**Section:**

**QUESTION 21**

HOTSPOT

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



Name	Type	Resource group
RG1	Resource group	Not applicable
RG2	Resource group	Not applicable
RG3	Resource group	Not applicable
SQL1	Azure SQL Database	RG3

Transparent Data Encryption (TDE) is disabled on SQL1.

You assign policies to the resource groups as shown in the following table.

Name	Condition	Effect if condition is false	Assignment
Policy1	TDE enabled	Deny	RG1, RG2
Policy2	TDE enabled	DeployIfNotExists	RG2, RG3
Policy3	TDE enabled	Audit	RG1

You plan to deploy Azure SQL databases by using an Azure Resource Manager (ARM) template. The databases will be configured as shown in the following table.

Name	Resource group	TDE
SQL2	RG2	Disabled
SQL3	RG1	Disabled

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Statements	Yes	No
SQL1 will have TDE enabled automatically.	<input type="checkbox"/>	<input type="checkbox"/>
The deployment of SQL2 will fail.	<input type="checkbox"/>	<input type="checkbox"/>
SQL3 will be deployed and marked as noncompliant.	<input type="checkbox"/>	<input type="checkbox"/>

Answer Area:

**Answer Area**

Statements	Yes	No
SQL1 will have TDE enabled automatically.	<input type="radio"/>	<input checked="" type="radio"/>
The deployment of SQL2 will fail.	<input checked="" type="radio"/>	<input type="radio"/>
SQL3 will be deployed and marked as noncompliant.	<input checked="" type="radio"/>	<input type="radio"/>

**Section:**

**Explanation:**

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

**QUESTION 22**

HOTSPOT

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

Name	Type	Resource group	Location
RG1	Resource group	<b>Not applicable</b>	West US
Managed1	Managed identity	RG1	West US

The subscription is linked to an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Usage location
User1	United States
User2	Germany

You create the groups shown in the following table.

Name	Type	Membership type
Group1	Security	Dynamic User
Group2	Microsoft 365	Dynamic User

The membership rules for Group1 and Group2 are configured as shown in the following exhibit.

 Vdumps

## Dynamic membership rules

Save | Discard | Got feedback?

**Configure Rules** | Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value
	accountEnabled	Equals	true
Or	usageLocation	Equals	US

+ Add expression | + Get custom extension properties

**Rule syntax** [Edit](#)

```
(user.accountEnabled -eq true) or (user.usageLocation - eq "US")
```

**Vdumps**

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

Hot Area:

**Answer Area**

Statements	Yes	No
User1 is a member of Group1 and Group2.	<input type="radio"/>	<input type="radio"/>
User2 is a member of Group2 only.	<input type="radio"/>	<input type="radio"/>
Managed1 is a member of Group1 and Group2.	<input type="radio"/>	<input type="radio"/>

Answer Area:

**Answer Area**

Statements	Yes	No
User1 is a member of Group1 and Group2.	<input checked="" type="radio"/>	<input type="radio"/>
User2 is a member of Group2 only.	<input type="radio"/>	<input checked="" type="radio"/>
Managed1 is a member of Group1 and Group2.	<input type="radio"/>	<input checked="" type="radio"/>

**Section:**

**Explanation:**

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership>

**QUESTION 23**

You have a Microsoft 365 tenant that uses an Azure Active Directory (Azure AD) tenant. The Azure AD tenant syncs to an on-premises Active Directory domain by using an instance of Azure AD Connect.

You create a new Azure subscription.

You discover that the synced on-premises user accounts cannot be assigned roles in the new subscription. You need to ensure that you can assign Azure and Microsoft 365 roles to the synced Azure AD user accounts. What should you do first?

- A. Configure the Azure AD tenant used by the new subscription to use pass-through authentication.
- B. Configure the Azure AD tenant used by the new subscription to use federated authentication.
- C. Change the Azure AD tenant used by the new subscription.
- D. Configure a second instance of Azure AD Connect.

**Correct Answer: C**

**Section:**

**QUESTION 24**

You have an Azure subscription that contains an app named App1. App1 has the app registration shown in the following table.

API	Permission	Type	Admin consent required	Status
Microsoft.Graph	User.Read	Delegated	No	None
Microsoft.Graph	Calendars.Read	Delegated	No	None

You need to ensure that App1 can read all user calendars and create appointments. The solution must use the principle of least privilege. What should you do?

- A. Add a new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.
- B. Add a new Application API permission for Microsoft.Graph Calendars.ReadWrite.
- C. Select Grant admin consent.
- D. Add new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.Shared.

**Correct Answer: A**

**Section:**

**Explanation:**

Reference: <https://docs.microsoft.com/en-us/graph/permissions-reference#calendars-permissions>

**QUESTION 25**

**HOTSPOT**

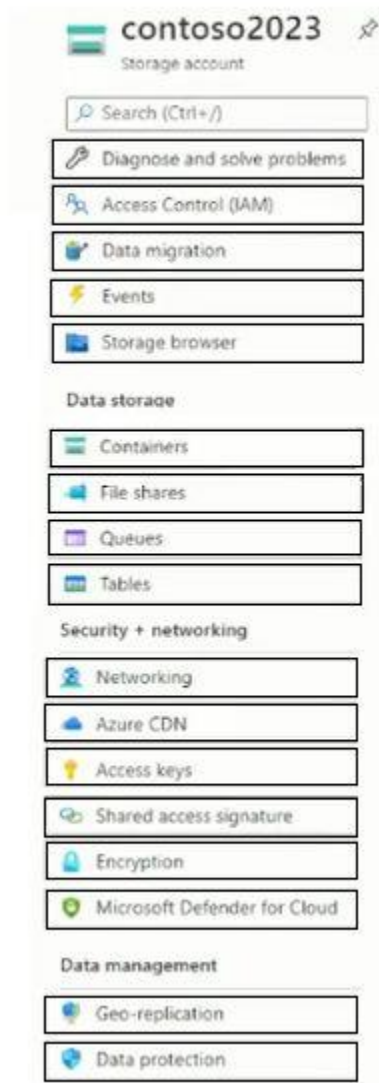
You have an Azure subscription that contains a storage account named contoso2023. You need to perform the following tasks:

- \* Verify that identity-based authentication over SMB is enabled.
- \* Only grant users access to contoso2023 in the year 2023.

Which two settings should you use? To answer, select the appropriate settings in the answer area NOTE: Each correct selection is worth one point.

**Hot Area:**

**Answer Area**



**Answer Area:**



## Answer Area



**Section:**

**Explanation:**

### QUESTION 26

HOTSPOT

You have an Azure Storage account that contains a blob container named container1 and a client application named App1. You need to enable App1 access to container1 by using Microsoft Entra authentication. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Hot Area:**

 **vdumps**



Answer Area

From Microsoft Entra: Register App1. Register App1. Create an access package. Implement an application proxy. Modify the authentication methods.

From the storage account: Configure Access control (IAM). Add a private endpoint. Regenerate the access key. Configure Access control (IAM). Generate a shared access signature (SAS).

Answer Area:

Answer Area

From Microsoft Entra: Register App1. Register App1. Create an access package. Implement an application proxy. Modify the authentication methods.

From the storage account: Configure Access control (IAM). Add a private endpoint. Regenerate the access key. Configure Access control (IAM). Generate a shared access signature (SAS).

Section:

Explanation:

QUESTION 27

HOTSPOT

You have an Azure subscription that contains an Azure key vault and an Azure SQL database named SQL1.

You generate a key named Key1.

You need to enable Transparent Data Encryption (TDE) for SQL1 by using Key1.

Which two settings should you modify for Key1? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

81cb93e71e7e401095f37bb5841417dd Key Version

Save Discard changes Download public key

Key type	RSA
RSA key size	2048
Created	4/24/2023, 7:39:34 PM
Updated	4/24/2023, 7:39:34 PM
Key Identifier	<a href="https://nk230424.vault.azure.net/keys/Key2/81cb93e71e7e401095f37...">https://nk230424.vault.azure.net/keys/Key2/81cb93e71e7e401095f37...</a>

Set expiration date

Expiration date    
(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

Enabled  Yes  No

Tags

Permitted operations

- Encrypt
- Decrypt
- Sign
- Verify
- Wrap Key
- Unwrap Key

Answer Area:

Answer Area

81cb93e71e7e401095f37bb5841417dd Key Version

Save Discard changes Download public key

Key type	RSA
RSA key size	2048
Created	4/24/2023, 7:39:34 PM
Updated	4/24/2023, 7:39:34 PM
Key Identifier	<a href="https://nk230424.vault.azure.net/keys/Key2/81cb93e71e7e401095f37...">https://nk230424.vault.azure.net/keys/Key2/81cb93e71e7e401095f37...</a>

Set expiration date

Expiration date    
(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

Enabled  Yes  No

Tags

Permitted operations

- Encrypt
- Decrypt
- Sign
- Verify
- Wrap Key
- Unwrap Key



Section:

Explanation:

QUESTION 28

You have an Azure subscription named Sub1 that has Security defaults disabled. The subscription contains the following users:

- \* Five users that have owner permissions for Sub1.

- \* Ten users that have owner permissions for Azure resources.

None of the users have multi-factor authentication (MFA) enabled.

Sub1 has the secure score as shown in the Secure Score exhibit. (Click the Secure Score tab.)

You plan to enable MFA for the following users:

- \* Five users that have owner permissions for Sub1.

- \* Five users that have owner permissions for Azure resources.

By how many points will the secure score increase after you perform the planned changes?

- A. 0
- B. 5
- C. 7.5
- D. 10
- E. 14

**Correct Answer: C**

**Section:**

