

Microsoft.AZ-500.v2024-03-29.q215

Exam Code:	AZ-500
Exam Name:	Microsoft Azure Security Technologies
Certification Provider:	Microsoft
Free Question Number:	215
Version:	v2024-03-29
# of views:	404
# of Questions views:	2150
https://www.freepdfdumps.com/Microsoft.AZ-500.v2024-03-29.q215.html	

NEW QUESTION: 1

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

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

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

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

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

On which other network interfaces can you configure ASG1?

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

Answer: (SHOW ANSWER)

Explanation

Only network interfaces in NVET1, which consists of Subnet11 and Subnet12, can be configured in ASG1, as all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.

Reference:

<https://azure.microsoft.com/es-es/blog/applicationsecuritygroups/>

NEW QUESTION: 2

You have an Azure subscription that contains the following resources:

- A network virtual appliance (NVA) that runs non-Microsoft firewall software and routes all outbound traffic from the virtual machines to the internet
- An Azure function that contains a script to manage the firewall rules of the NVA
- Azure Security Center standard tier enabled for all virtual machines
- An Azure Sentinel workspace
- 30 virtual machines

You need to ensure that when a high-priority alert is generated in Security Center for a virtual machine, an incident is created in Azure Sentinel and then a script is initiated to configure a firewall rule for the NVA.

How should you configure Azure Sentinel to meet the requirements? To answer, drag the appropriate components to the correct requirements. Each component 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.

Components

- A data connector for Security Center
- A data connector for the firewall software
- A playbook
- A rule
- A Security Events connector
- A workbook

Answer Area

- Enable alert notifications from Security Center: Component
- Create an incident: Component
- Initiate a script to configure the firewall rule: Component

Microsoft

Answer:

Components

- A data connector for Security Center
- A data connector for the firewall software
- A playbook
- A rule
- A Security Events connector
- A workbook

Answer Area

- Enable alert notifications from Security Center: A data connector for Security Center
- Create an incident: A rule
- Initiate a script to configure the firewall rule: A playbook

Microsoft

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts>

<https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center>

NEW QUESTION: 3

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

Name	Member of	Multi-factor authentication (MFA) status
User1	None	Disabled
User2	Group1	Disabled
user3	Group1	Enforced

Azure AD Privileged Identity Management (PIM) is enabled for the tenant.

In PIM, the Password Administrator role has the following settings:

Maximum activation duration (hours): 2

Send email notifying admins of activation: Disable

Require incident/request ticket number during activation: Disable

Require Azure Multi-Factor Authentication for activation: Enable

Require approval to activate this role: Enable

Selected approver: Group1

You assign users the Password Administrator role as shown in the following table.

Name	Assignment type
User1	Active
User2	Eligible
user3	Eligible

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	<input type="radio"/>	<input type="radio"/>
User2 can request to activate the Password Administrator role.	<input type="radio"/>	<input type="radio"/>
If User3 wants to activate the Password Administrator role, the user can approve their own request.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can request to activate the Password Administrator role.	<input checked="" type="radio"/>	<input type="radio"/>
If User3 wants to activate the Password Administrator role, the user can approve their own request.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

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

NEW QUESTION: 4

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	AllowAzureLoadBalanc	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.

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:

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"/>

NEW QUESTION: 5

Your network contains an Active Directory forest named contoso.com. The forest contains a single domain.

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

You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant.

You need to recommend an integration solution that meets the following requirements:

- * Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant
- * Minimizes the number of servers required for the solution.

Which authentication method should you include in the recommendation?

- A. federated identity with Active Directory Federation Services (AD FS)
- B. password hash synchronization with seamless single sign-on (SSO)
- C. pass-through authentication with seamless single sign-on (SSO)

Answer: B (LEAVE A REPLY)

Password hash synchronization requires the least effort regarding deployment, maintenance, and infrastructure. This level of effort typically applies to organizations that only need their users to sign in to Office

365, SaaS apps, and other Azure AD-based resources. When turned on, password hash synchronization is

part of the Azure AD Connect sync process and runs every two minutes.

Incorrect Answers:

A: A federated authentication system relies on an external trusted system to authenticate users. Some

companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.

C: For pass-through authentication, you need one or more (we recommend three) lightweight agents installed on existing servers. These agents must have access to your on-premises Active Directory Domain Services, including your on-premises AD domain controllers. They need outbound access to the Internet and access to your domain controllers. For this reason, it's not supported to deploy the agents in a perimeter network.

Pass-through Authentication requires unconstrained network access to domain controllers. All network traffic is encrypted and limited to authentication requests.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta>

NEW QUESTION: 6

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

Name	Multi-factor authentication (MFA) status
User1	Disabled
User2	Disabled
User3	Enforced

In Azure AD Privileged Identity Management (PIM), the Role settings for the Contributor role are configured as shown in the exhibit. (Click the Exhibit tab.)

Assignment

Allow permanent eligible assignment

Expire eligible assignments after

3 Months

Allow permanent active assignment

Expire active assignments after

1 Month

Require Multi-Factor Authentication on active assignment

Require justification on active assignment

Activation

Activation maximum duration (hours)



Require Multi-Factor Authentication on activation

Require justification on activation

Require ticket information on activation

Require approval to activate



* Select approvers

No member or group selected



You assign users the Contributor role on May 1, 2019 as shown in the following table.

Name	Assignment type
User1	Eligible
User2	Active
User3	Active

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
On May 15, 2019, User1 can activate the Contributor role.	<input type="radio"/>	<input type="radio"/>
On May 15, 2019, User2 can use the Contributor role.	<input type="radio"/>	<input type="radio"/>
On June 15, 2019, User3 can activate the Contributor role.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
On May 15, 2019, User1 can activate the Contributor role.	<input checked="" type="radio"/>	<input type="radio"/>
On May 15, 2019, User2 can use the Contributor role.	<input type="radio"/>	<input type="radio"/>
On June 15, 2019, User3 can activate the Contributor role.	<input type="radio"/>	<input type="radio"/>

Reference:

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

NEW QUESTION: 7

You have a Azure subscription that contains an Azure Container Registry named Registry1. The subscription uses the Standard use tier of Azure Security Center.

You upload several container images to Register1.

You discover that vulnerability security scans were not performed

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

What should you do?

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

Answer: A (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 8

You have an Azure AD tenant named contoso.com that has Azure AD Premium P1 licenses. You need to create a group named Group1 that will be assigned the Global reader role. Which portal should you use to create Group1 and which type of group should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Portal:
The Azure Active Directory admin center only
The Microsoft 365 admin center only
The Azure Active Directory admin center or the Microsoft 365 admin center

Group type:
Security only
Microsoft 365 only
Security or mail-enabled security only
Security or Microsoft 365 only
Security, Microsoft 365, or mail-enabled security

Answer:

Portal:
The Azure Active Directory admin center only
The Microsoft 365 admin center only
The Azure Active Directory admin center or the Microsoft 365 admin center

Group type:
Security only
Microsoft 365 only
Security or mail-enabled security only
Security or Microsoft 365 only
Security, Microsoft 365, or mail-enabled security


<https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-create-eligible>

NEW QUESTION: 9

You are configuring just in time (JIT) VM access to a set of Azure virtual machines. You need to grant users PowerShell access to the virtual machine by using JIT VM access. What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Microsoft

Permission that must be granted to users on VM:

- Read
- Update
- View
- Write

TCP port that must be allowed:

- 22
- 25
- 3389
- 5986

Answer:
Answer Area

Permission that must be granted to users on VM:

- Read
- Update
- View
- Write

TCP port that must be allowed:

- 22
- 25
- 3389
- 5986



Microsoft

NEW QUESTION: 10

You are implementing conditional access policies.

You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.

You need to identify the risk level of the following risk events:

Users with leaked credentials

Impossible travel to atypical locations

Sign ins from IP addresses with suspicious activity


Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Levels

Answer Area

High



Low

Impossible travel to atypical locations:

Users with leaked credentials:

Medium

Sign ins from IP addresses with suspicious activity:

Answer:

Levels	Answer Area	
High	Impossible travel to atypical locations:	Medium
Low	Users with leaked credentials:	High
Medium	Sign ins from IP addresses with suspicious activity:	Medium

NEW QUESTION: 11

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?

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:

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

NEW QUESTION: 12

You have an Azure subscription that is linked to an Azure AD tenant and contains the virtual machines shown in the following table.

Name	Connects to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.5	20.224.219.170
VM2	VNET1/Subnet2	10.1.2.5	20.224.219.230
VM3	VNET2/Subnet1	10.11.1.5	40.122.155.212

The subnets of the virtual networks have the service endpoints shown in the following table.

Subnet	Service endpoint
VNET1/Subnet1	Microsoft.Storage
VNET1/Subnet2	Microsoft.KeyVault
VNET2/Subnet1	Microsoft.Storage, Microsoft.KeyVault

You create the resources shown in the following table.

Name	Type
storage1	Azure Storage account
Vault1	Azure Key Vault

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

NOTE: Each correct selection is worth one point.

Answer Area



Statements

Connections from VM1 to storage1 always use IP address 10.1.1.5. Yes No

Connections from VM2 to Vault1 always use IP address 20.224.219.230. Yes No

Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212. Yes No

Answer:

Answer Area



Statements

Connections from VM1 to storage1 always use IP address 10.1.1.5. Yes No

Connections from VM2 to Vault1 always use IP address 20.224.219.230. Yes No

Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212. Yes No

NEW QUESTION: 13

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

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

You have an Azure Subscription named Sub1.

You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service.

You need to revoke all access to Sa1.

Solution: You create a new stored access policy.

Does this meet the goal?

A. No

B. Yes

Answer: A (LEAVE A REPLY)

NEW QUESTION: 14

You plan to implement an Azure function named Function1 that will create new storage accounts for containerized application instances.

You need to grant Function1 the minimum required privileges to create the storage accounts. The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Assign role to:

A group account
A system-assigned managed identity
A user account
A user-assigned managed identity

Role assignment to create:

Built-in role assignment
Classic administrator role assignment
Custom role-based access control (RBAC) role assignment

Answer:

Assign role to:

A group account
A system-assigned managed identity
A user account
A user-assigned managed identity

Role assignment to create:

Built-in role assignment
Classic administrator role assignment
Custom role-based access control (RBAC) role assignment

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/howto-assign-access-portal>

NEW QUESTION: 15

Use the following login credentials as needed:

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

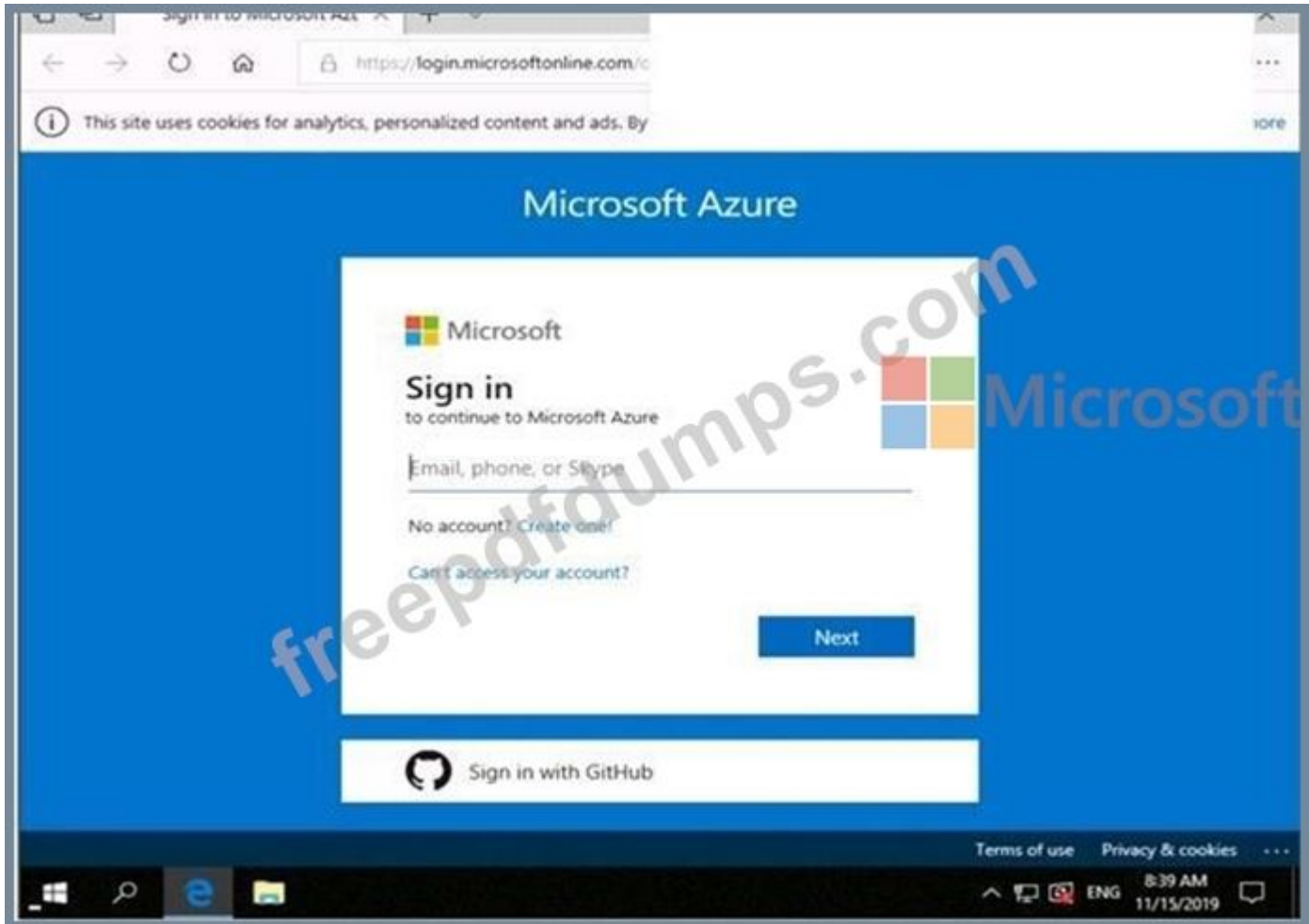
To enter your password, place your cursor in the Enter password box and click on the password below.

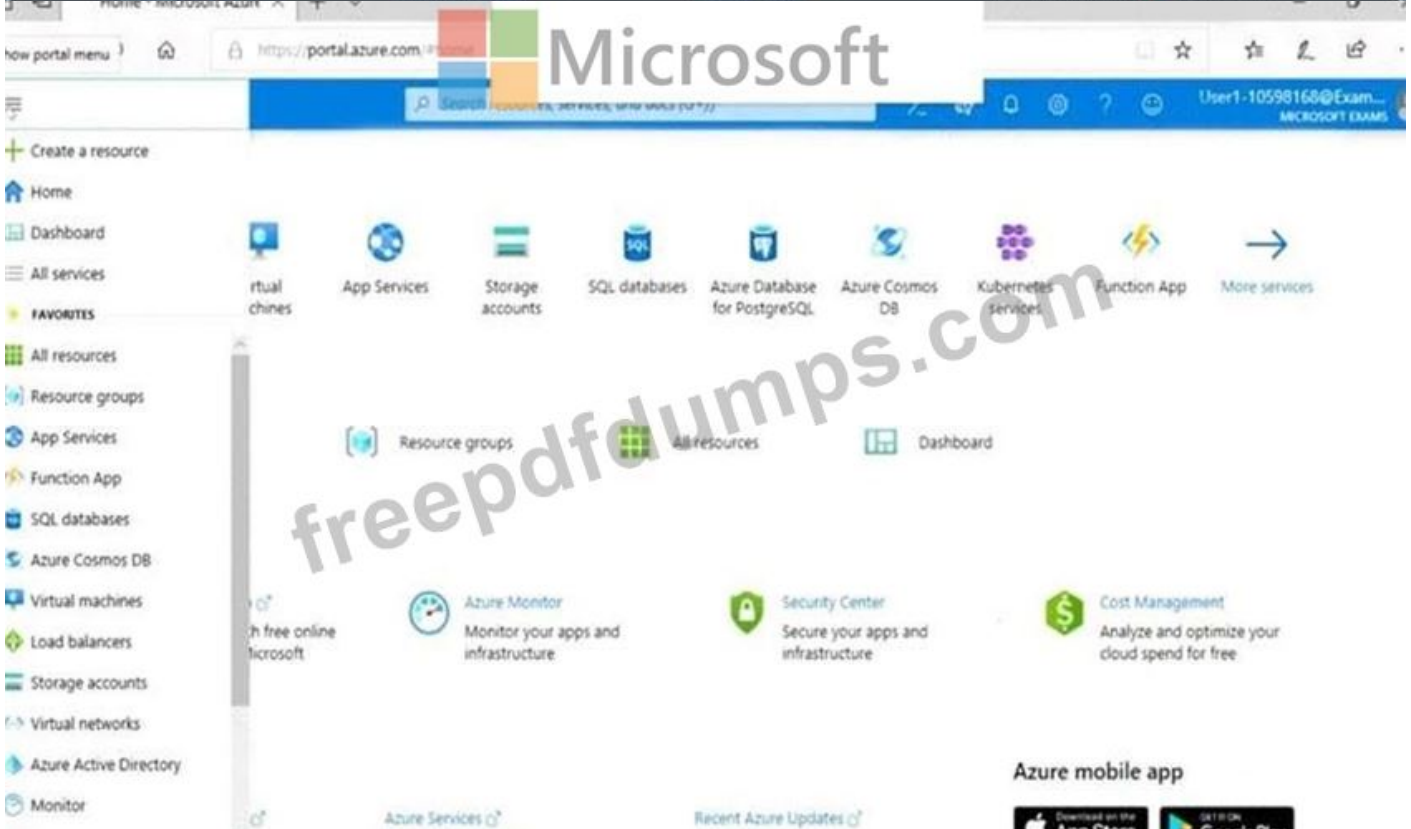
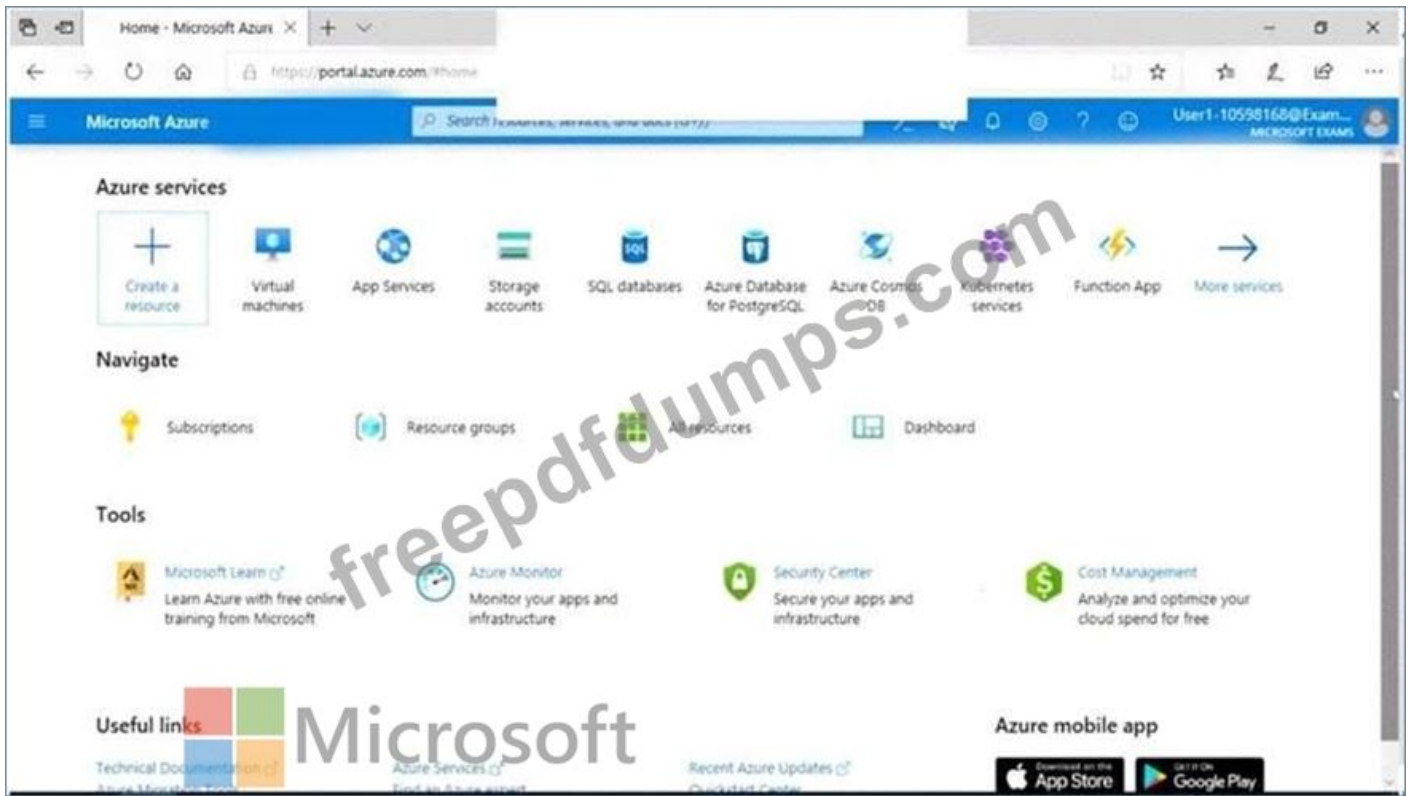
Azure Username: User1-10598168@ExamUsers.com

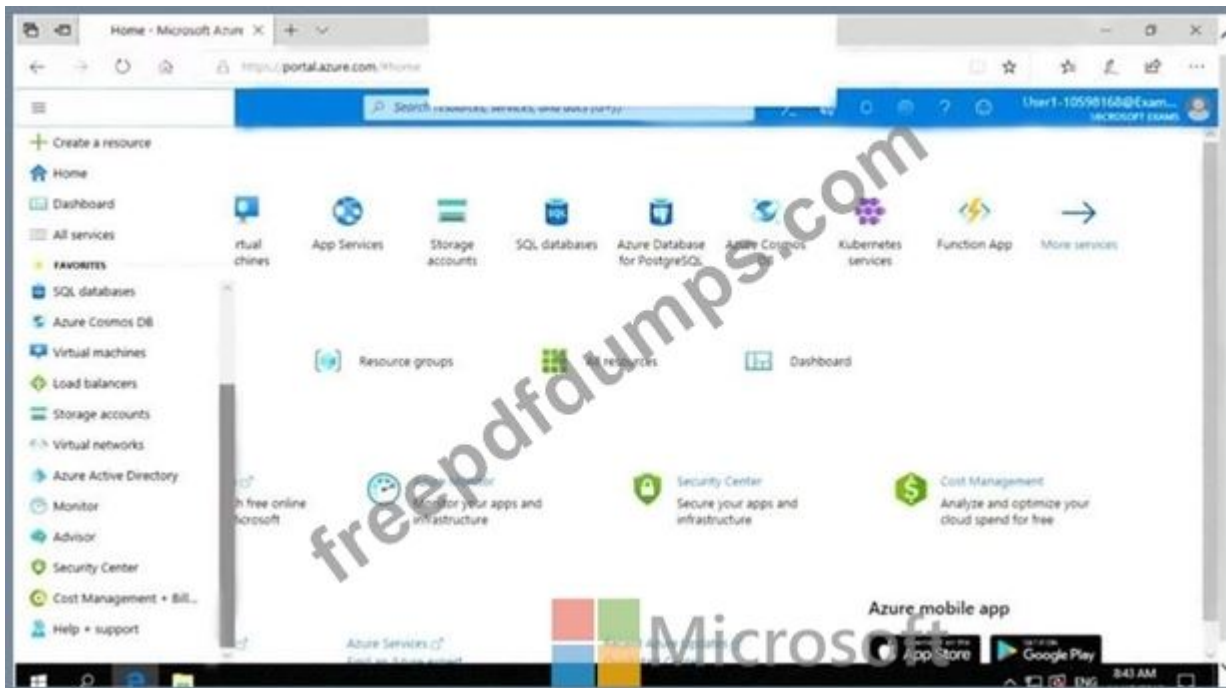
Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168







You need to ensure that the rg1lod10598168n1 Azure Storage account is encrypted by using a key stored in the KeyVault10598168 Azure key vault.

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

Answer:

See the explanation below.

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.



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.

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>

 **Microsoft**

 <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>

NEW QUESTION: 16

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

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

NOTE: Each correct selection is worth one point.


Answer Area

Statements	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	<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"/>

 **Microsoft**

Answer:

Statements	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"/>

 **Microsoft**

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-synched	Role	Delegated to
User1	User	Yes	User	None
Admin1	User	No	User Access Administrator	Tenant Root Group
Admin2	User	No	Security administrator	MG1
Admin3	User	No	Contributor	Subscription1
Admin4	User	No	Owner	RG1
Group1	Group	No	Not applicable	None

Azure AD contains the resources shown in the following table.

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

Subscription1 Resources

Subscription1 contains the virtual networks shown in the following table.

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

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

Name	Location
NSG2	West US
NSG3	Central US
NSG4	West US

Subscription1 contains the virtual machines shown in the following table.

Name	Operating system	Location	Connected 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.

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!

Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (**460** Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 17

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD).

The Azure AD tenant contains the users shown in the following table.

You configure the Authentication methods - Password Protection settings for adatum.com as shown in the following exhibit.

Custom smart lockout

Lockout threshold ⓘ ✓

Lockout duration in seconds ⓘ ✓

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ ✓

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit

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

Microsoft Statements	Yes	No
User1 will be prompted to change the password on the next sign-in.	<input type="radio"/>	<input type="radio"/>
User2 can change the password to @d@tum_C0mpleX123.	<input type="radio"/>	<input type="radio"/>
User3 can change the password to Adatum123!.	<input type="radio"/>	<input type="radio"/>

Answer:

Microsoft Statements	Yes	No
User1 will be prompted to change the password on the next sign-in.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can change the password to @d@tum_C0mpleX123.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can change the password to Adatum123!.	<input checked="" type="radio"/>	<input type="radio"/>

Reference:

- <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>
- <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad>

NEW QUESTION: 18

On Monday, you configure an email notification in Azure Security Center to email notifications to user1@contoso.com.

On Tuesday, Security Center generates the security alerts shown in the following table.

Time	Description	Severity
01:00	Failed RDP brute force attack	Medium
01:01	Successful RDP brute force attack	High
06:10	Suspicious process executed	High
09:00	Malicious SQL activity	High
11:15	Network communication with a malicious machine detected	Low
13:30	Suspicious process executed	High
14:00	Failed RDP brute force attack	Medium
16:01	Successful RDP brute force attack	High
23:20	Possible outgoing spam activity detected	Low
23:25	Modified system binary discovered in dump file	High
23:30	Malicious SQL activity	High

How many email notifications will user1@contoso.com receive on Tuesday? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Total number of Security Center email notifications about an RDP brute force attack on Tuesday:

	▼
1	
2	
3	
4	

Total number of Security Center email notifications on Tuesday:

	▼
3	
4	
6	
9	
11	

Answer:

Total number of Security Center email notifications about an RDP brute force attack on Tuesday:

Total number of Security Center email notifications on Tuesday:

▼

1

2

3

4

▼

3

4

6

9

11

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>

NEW QUESTION: 19

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

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

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

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

You need to identify how Azure Information Protection will label files.

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

NOTE: Each correct selection is worth one point.

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



	▼
No label	
Label1 only	
Label2 only	
Label1 and Label2	

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

	▼
No label	
Label1 only	
Label2 only	
Label1 and Label2	

Answer:

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



	▼
No label	
Label1 only	
Label2 only	
Label1 and Label2	

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

	▼
No label	
Label1 only	
Label2 only	
Label1 and Label2	

Explanation

<p>If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:</p>	<table border="1"><tr><td></td><td>▼</td></tr><tr><td colspan="2">No label</td></tr><tr><td colspan="2">Label1 only</td></tr><tr><td colspan="2">Label2 only</td></tr><tr><td colspan="2">Label1 and Label2</td></tr></table>		▼	No label		Label1 only		Label2 only		Label1 and Label2	
	▼										
No label											
Label1 only											
Label2 only											
Label1 and Label2											
<p>If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:</p>	<table border="1"><tr><td></td><td>▼</td></tr><tr><td colspan="2">No label</td></tr><tr><td colspan="2">Label1 only</td></tr><tr><td colspan="2">Label2 only</td></tr><tr><td colspan="2">Label1 and Label2</td></tr></table>		▼	No label		Label1 only		Label2 only		Label1 and Label2	
	▼										
No label											
Label1 only											
Label2 only											
Label1 and Label2											

Box 1: Label 2 only

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

- * The labels are ordered for evaluation, according to their position that you specify in the policy: The label positioned first has the lowest position (least sensitive) and the label positioned last has the highest position (most sensitive).
- * The most sensitive label is applied.

* The last sublabel is applied.

Box 2: No Label

Automatic classification applies to Word, Excel, and PowerPoint when documents are saved, and apply to Outlook when emails are sent. Automatic classification does not apply to Microsoft Notepad.

References:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

NEW QUESTION: 20

Use the following login credentials as needed:

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

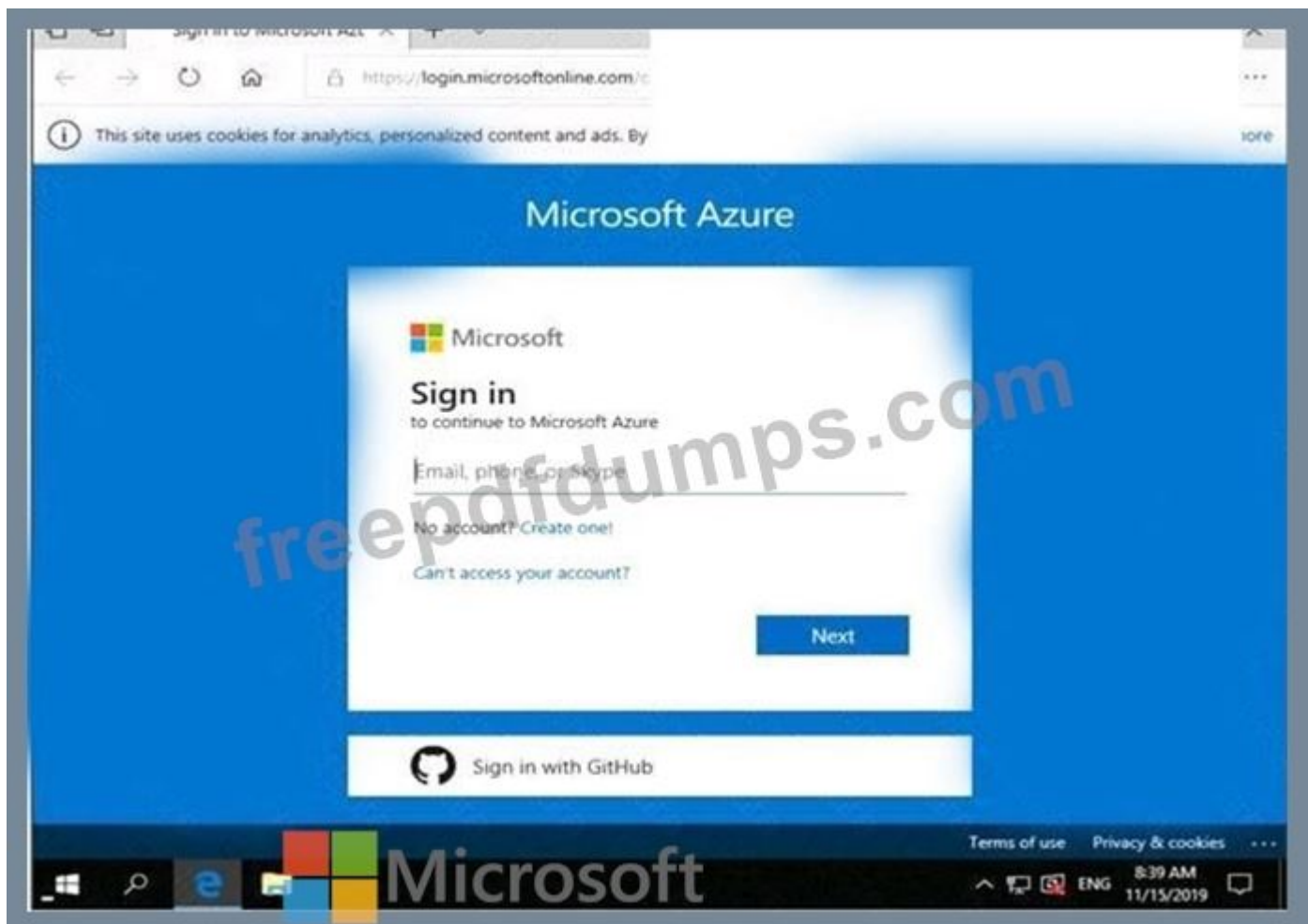
To enter your password, place your cursor in the Enter password box and click on the password below.

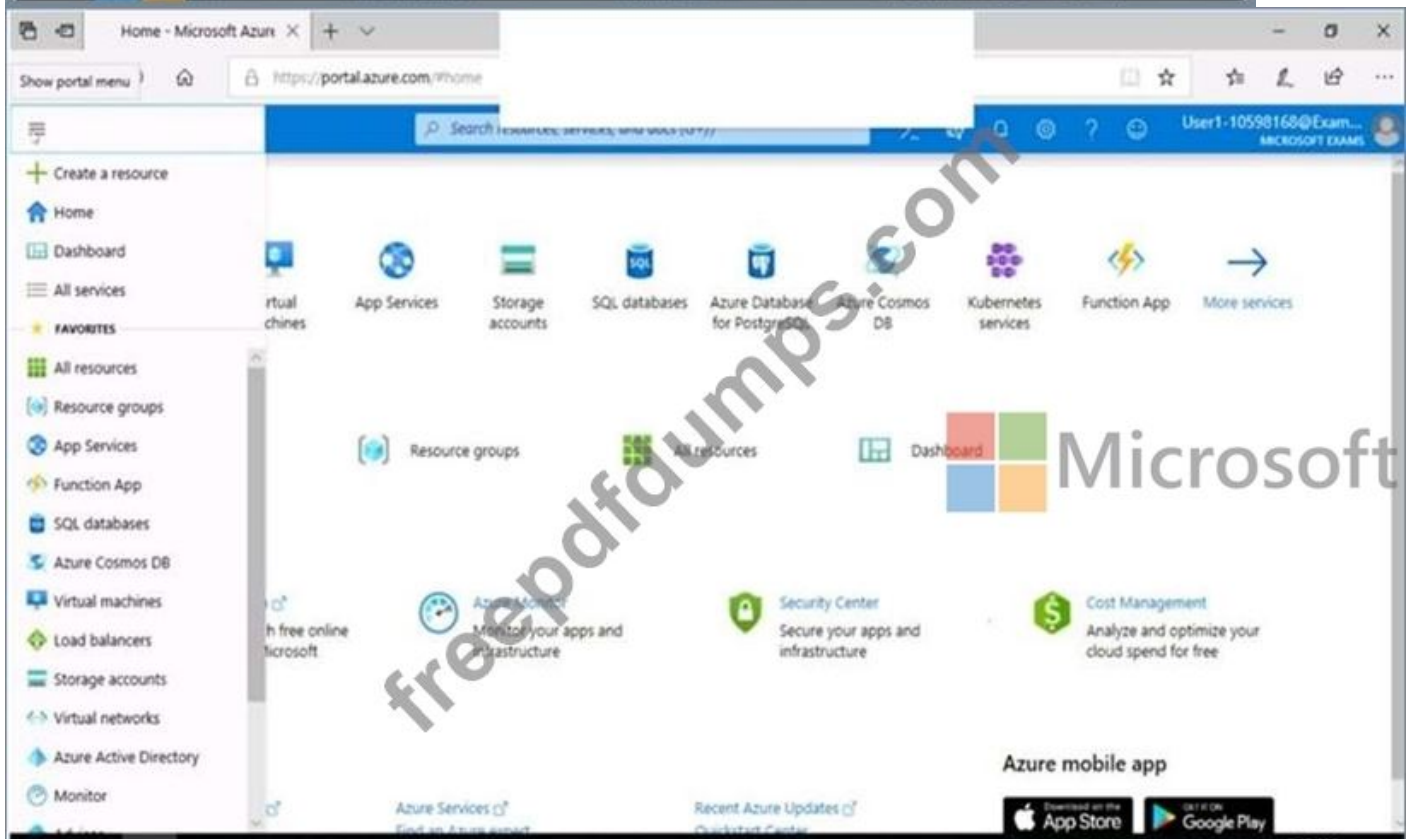
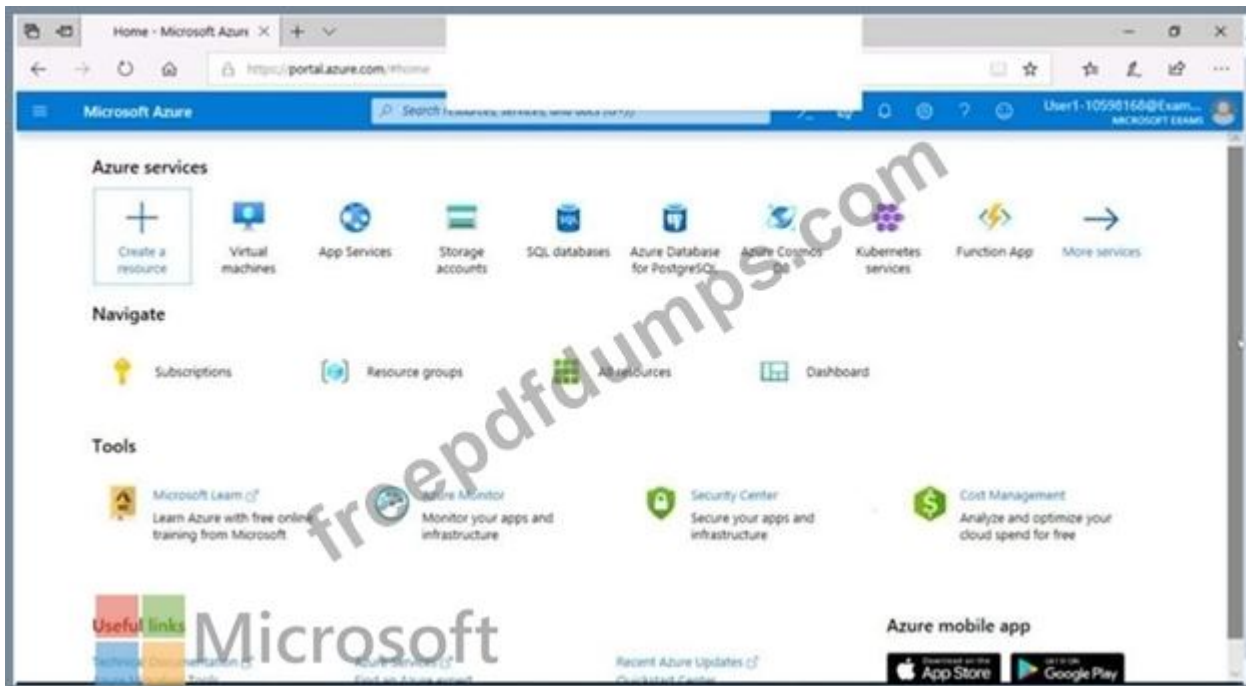
Azure Username: User1-10598168@ExamUsers.com

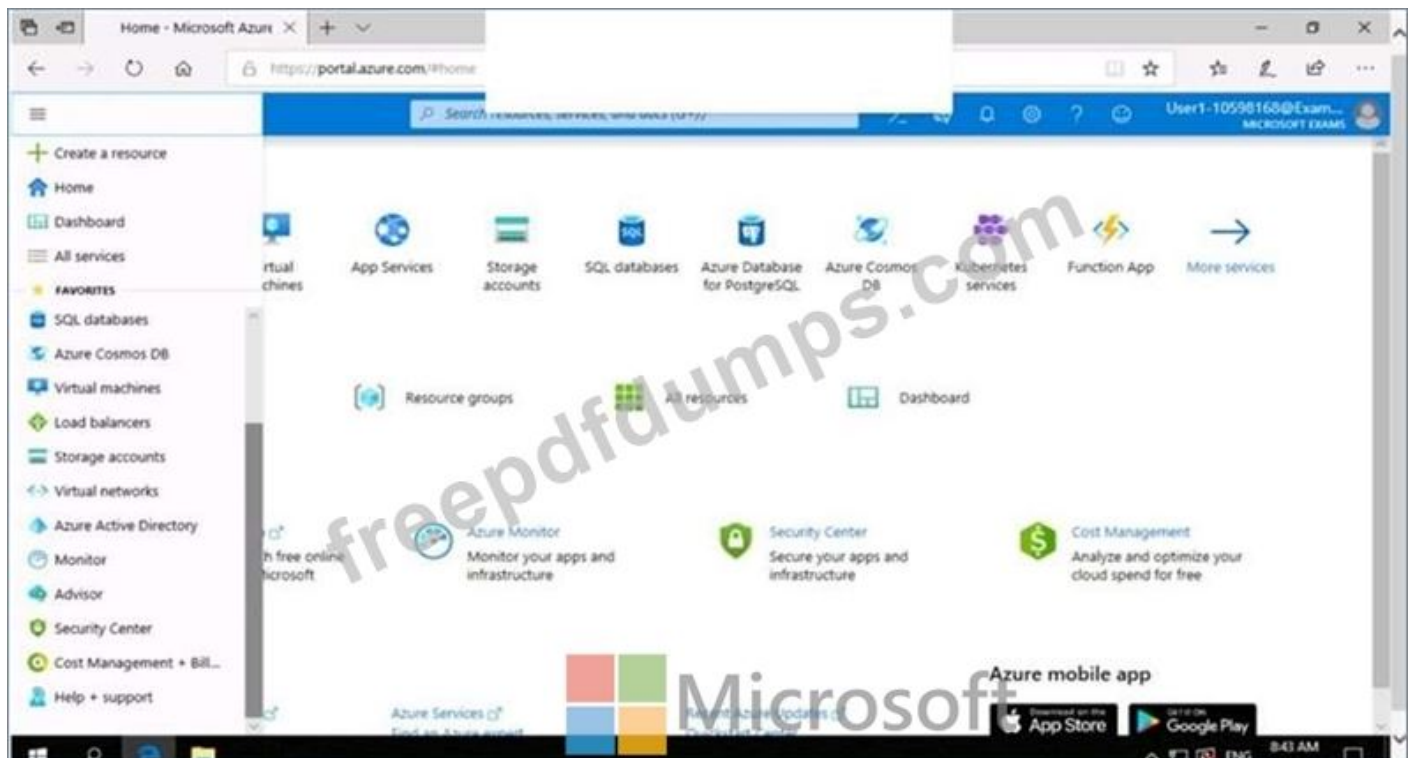
Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168







You need to email an alert to a user named admin1@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes.

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

Answer:

See the explanation below.

Explanation

Create an alert rule on a metric with the Azure portal

1. In the portal, locate the resource, here VM1, you are interested in monitoring and select it.
2. Select Alerts (Classic) under the MONITORING section. The text and icon may vary slightly for different resources.
3. Select the Add metric alert (classic) button and fill in the fields as per below, and click OK.

Metric: CPU Percentage

Condition: Greater than

Period: Over last 15 minutes

Notify via: email

Additional administrator email(s): admin1@contoso.com

Condition

Greater than

* Threshold

60

Period ⓘ

Over the last 5 minutes

Notify via

Email owners, contributors, and readers

Additional administrator email(s)

admin@contoso.com

Webhook ⓘ

http://www.contoso.com/dowork?param

Reference:

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

NEW QUESTION: 21

You have an Azure subscription that contains 100 virtual machines. Azure Diagnostics is enabled on all the virtual machines.

You are planning the monitoring of Azure services in the subscription.

You need to retrieve the following details:

- * Identify the user who deleted a virtual machine three weeks ago.
- * Query the security events of a virtual machine that runs Windows Server 2016.

What should you use in Azure Monitor? To answer, drag the appropriate configuration settings to the correct details. Each configuration setting may be used once, more than once, or not at all.

You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Settings **Answer Area**

Activity log

Logs

Metrics

Service Health

Identify the user who deleted a virtual machine three weeks ago:

Query the security events of a virtual machine that runs Windows Server 2016:



Answer:

Settings **Answer Area**

Activity log


Logs

Metrics

Service Health

Identify the user who deleted a virtual machine three weeks ago:


Query the security events of a virtual machine that runs Windows Server 2016:



Explanation

Identify the user who deleted a virtual machine three weeks ago:

Query the security events of a virtual machine that runs Windows Server 2016:



Box 1: Activity log

Azure activity logs provide insight into the operations that were performed on resources in your subscription.

Activity logs were previously known as "audit logs" or "operational logs," because they report control-plane events for your subscriptions.

Activity logs help you determine the "what, who, and when" for write operations (that is, PUT, POST, or DELETE).

Box 2: Logs

Log Integration collects Azure diagnostics from your Windows virtual machines, Azure activity logs, Azure Security Center alerts, and Azure resource provider logs. This integration provides a unified dashboard for all your assets, whether they're on-premises or in the cloud, so that you can aggregate, correlate, analyze, and alert for security events.

References:

<https://docs.microsoft.com/en-us/azure/security/azure-log-audit>

NEW QUESTION: 22

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

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

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

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

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

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

NOTE: Each correct selection is worth one point.

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

	▼
Analytics	
Data connectors	
Playbooks	
Workbooks	

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

	▼
Analytics	
Data connectors	
Playbooks	
Workbooks	

Answer:

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

	▼
Analytics	
Data connectors	
Playbooks	
Workbooks	

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

	▼
Analytics	
Data connectors	
Playbooks	
Workbooks	

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

NEW QUESTION: 23

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

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

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

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

On which virtual machines is the Log Analytics agent installed?

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

Answer: ([SHOW ANSWER](#))

Explanation

When automatic provisioning is On, Security Center provisions the Log Analytics Agent on all supported Azure VMs and any new ones that are created.

Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection>

NEW QUESTION: 24

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.

The screenshot shows an 'Answer Area' with a table for evaluating statements. The table has three rows of statements and two columns for 'Yes' and 'No' responses. Each row has a radio button in the 'Yes' column and an empty radio button in the 'No' column. A large watermark 'freepdfdumps.com' is overlaid on the table, and a Microsoft logo is visible at the bottom.

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	<input type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the private IP address of VM3.	<input type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the private IP address of VM5.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area



Microsoft

Statements

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	<input type="radio"/>	<input checked="" type="radio"/>
From VM1, you can successfully ping the private IP address of VM3.	<input checked="" type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the private IP address of VM5.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION: 25

You have an Azure subscription that contains a user named Admin1 and a resource group named RG1.

In Azure Monitor, you create the alert rules shown in the following table.

Name	Resource	Condition
Rule1	RG1	All security operations
Rule2	RG1	All administrative operations
Rule3	Azure subscription	All security operations by Admin1
Rule4	Azure subscription	All administrative operations by Admin1

Admin1 performs the following actions on RG1:

- * Adds a virtual network named VNET1
- * Adds a Delete lock named Lock1

Which rules will trigger an alert as a result of the actions of Admin1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Adding VNET1:

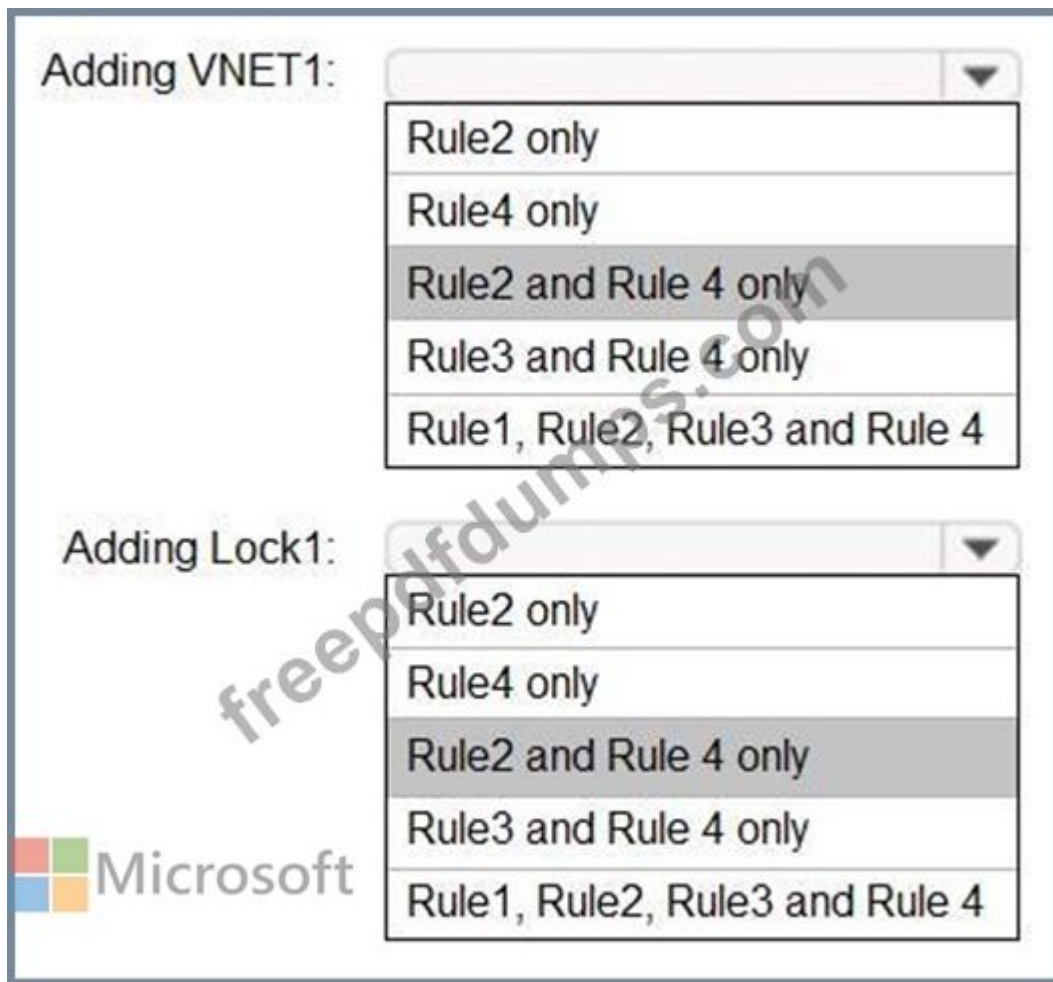
- Rule2 only
- Rule4 only
- Rule2 and Rule 4 only
- Rule3 and Rule 4 only
- Rule1, Rule2, Rule3 and Rule 4

Adding Lock1:

- Rule2 only
- Rule4 only
- Rule2 and Rule 4 only
- Rule3 and Rule 4 only
- Rule1, Rule2, Rule3 and Rule 4

Answer:

Explanation



NEW QUESTION: 26

You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) data connector.

You are threat hunting suspicious traffic from a specific IP address.

You need to annotate an intermediate event stored in the workspace and be able to reference the IP address when navigating through the investigation graph.

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.

Actions

Answer Area



Add the query to Favorites.

From the Azure Sentinel workspace, run an Azure Log Analytics query.

In a Jupyter notebook, create a reference to the IP address.

Add a bookmark and assign a tag.

Add a bookmark and map an entity.

From Azure Monitor, run an Azure Log Analytics query.

Select a query result.



Answer:

Answer Area

From the Azure Sentinel workspace, run an Azure Log Analytics query.

Select a query result.

Add a bookmark and map an entity.

1 - From the Azure Sentinel workspace, run an Azure Log Analytics query.

2 - Select a query result.

3 - Add a bookmark and map an entity.

Reference:

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

NEW QUESTION: 27

Use the following login credentials as needed:

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

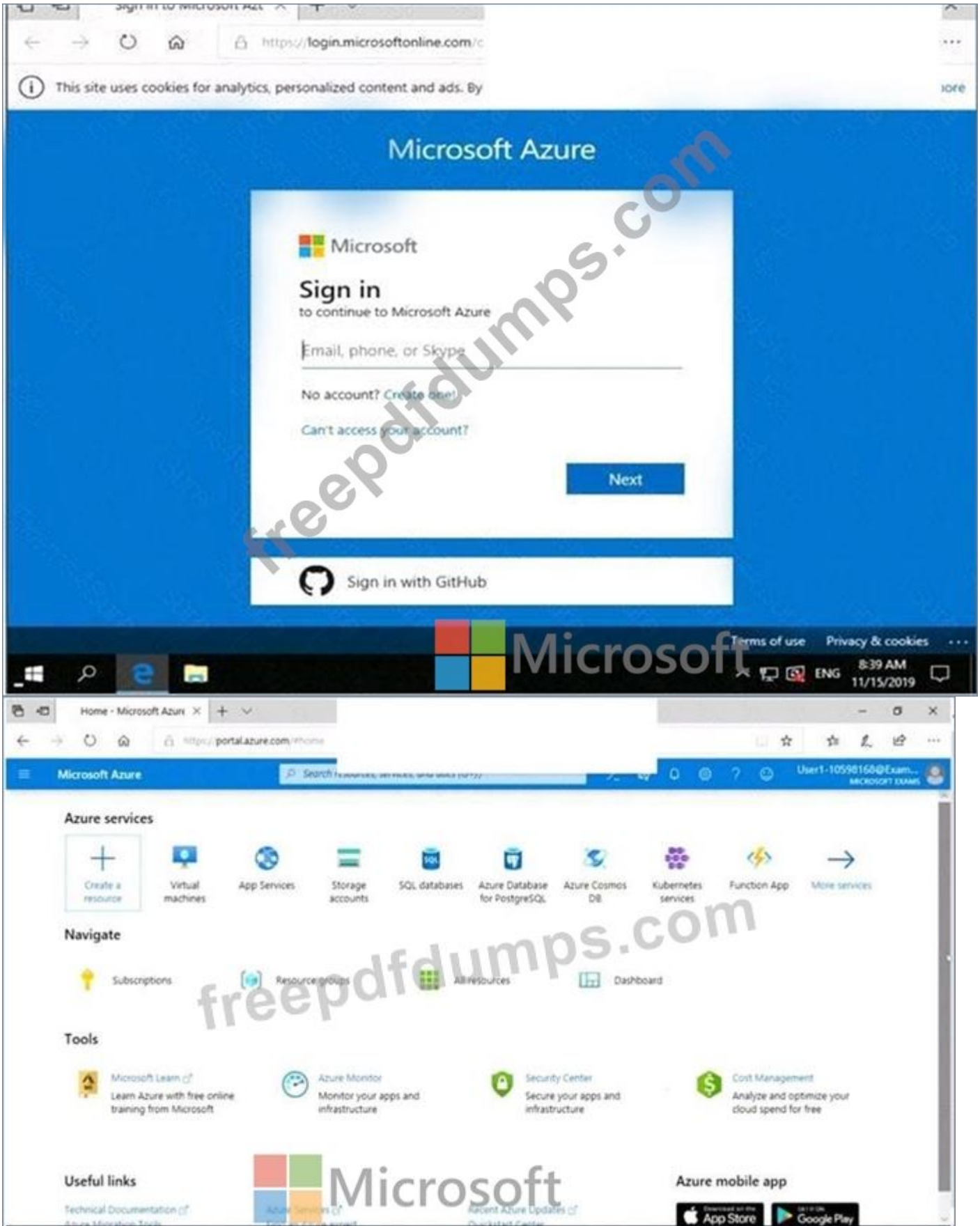
To enter your password, place your cursor in the Enter password box and click on the password below.

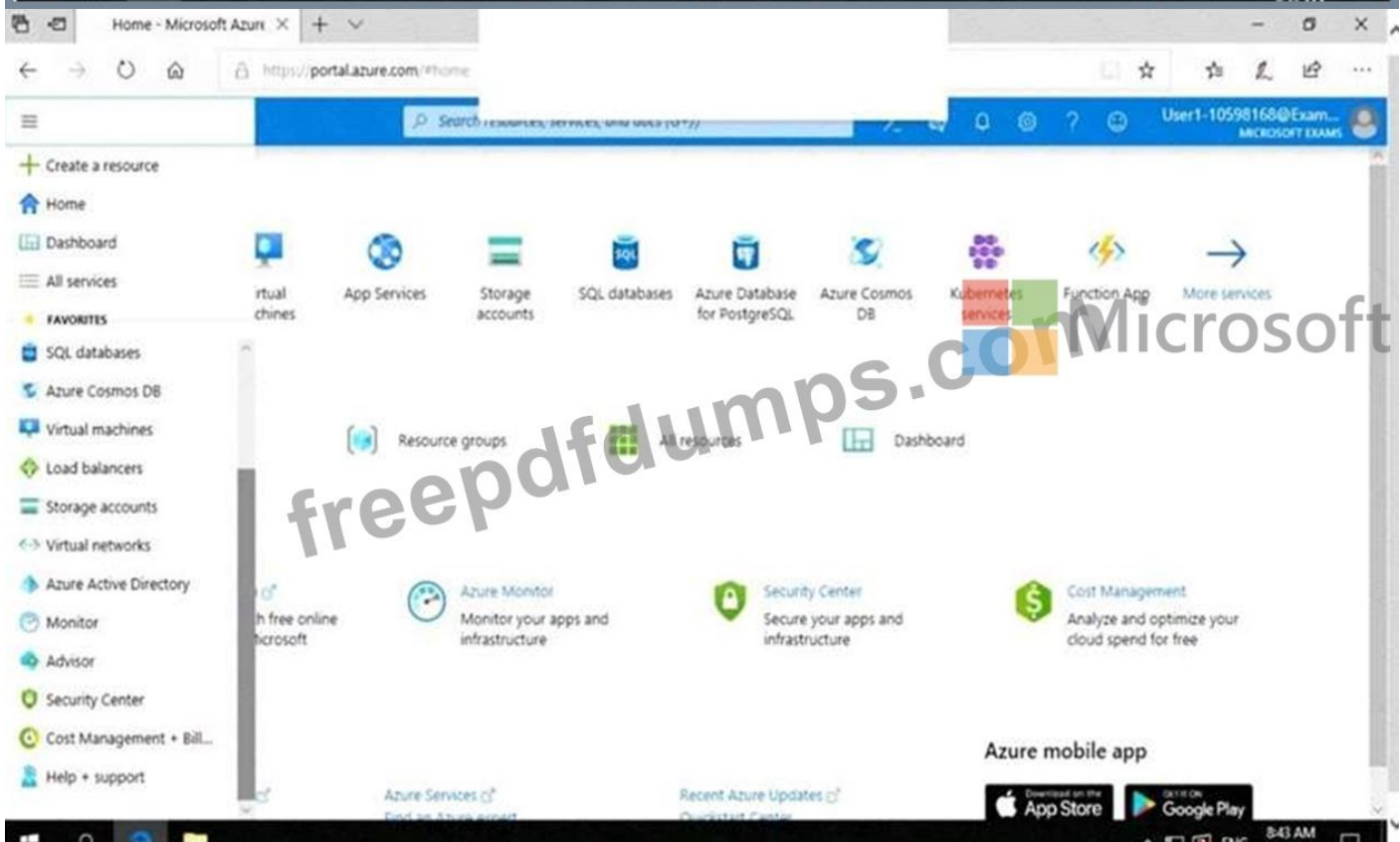
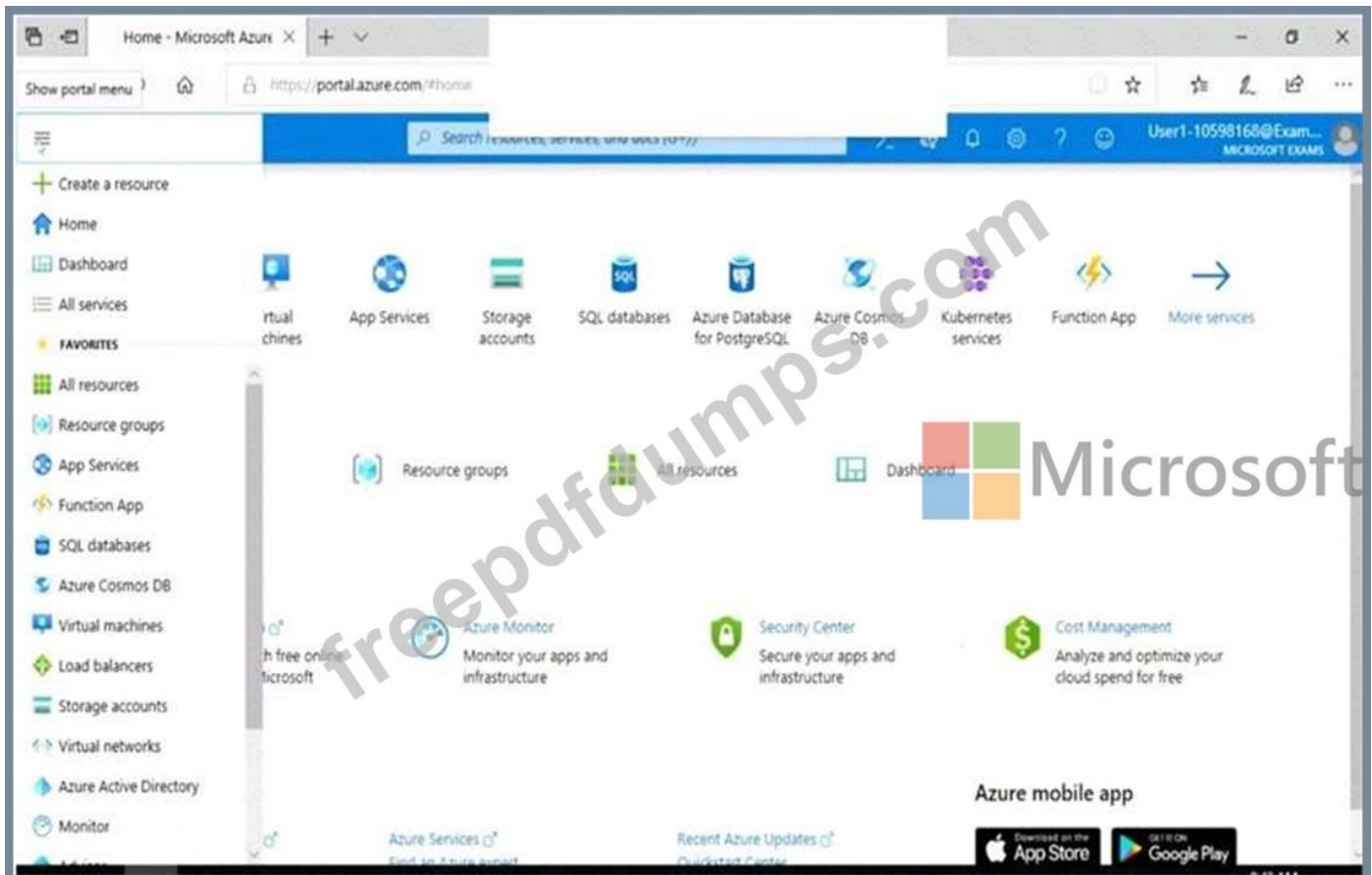
Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168





You need to prevent HTTP connections to the rg1lod10598168n1 Azure Storage account.

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

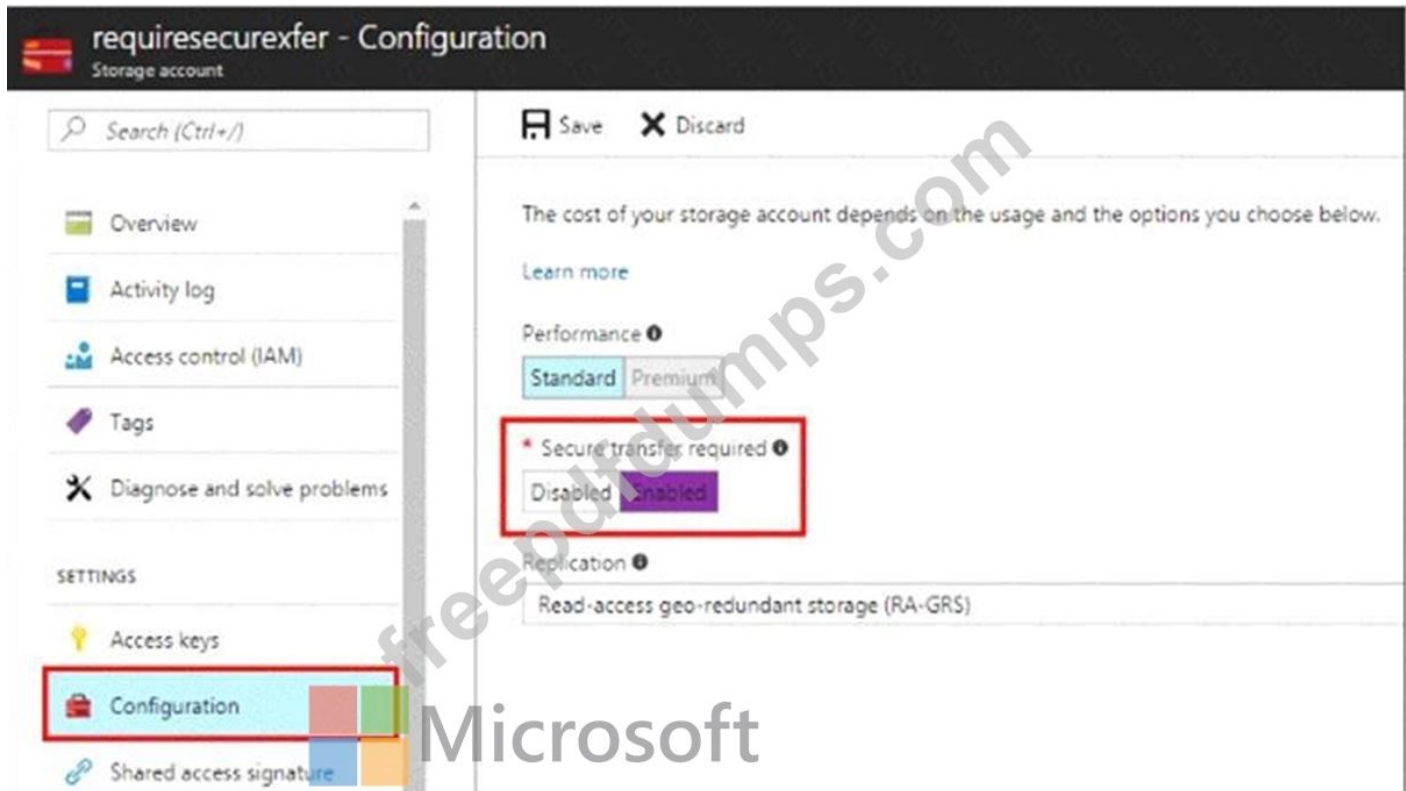
See the explanation below.

Answer:

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>

NEW QUESTION: 28

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	In resource group
8372f433-2dcd-4361-b5ef-5b188fed87d0	Subscription ID	Not applicable
RG1	Resource group	Not applicable
VM1	Virtual machine	RG1
VNET1	Virtual network	RG1
storage	Storage account	RG1
User1	User account	Not applicable

You create an Azure role by using the following JSON file.

```

{
  "properties":{
    "roleName": "Role1",
    "description": "",
    "assignableScopes": [
      "/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0",
      "/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG1"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Compute/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}

```

You assign Role1 to User1 for RG1.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can create a new virtual machine in RG1.	<input type="radio"/>	<input type="radio"/>
User can modify the properties of storage1.	<input type="radio"/>	<input type="radio"/>
User1 can attach the network interface of VM1 to VNET1.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can create a new virtual machine in RG1.	<input type="radio"/>	<input checked="" type="radio"/>
User can modify the properties of storage1.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can attach the network interface of VM1 to VNET1.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#compute>

NEW QUESTION: 29

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.

Actions

- 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.

Answer Area

Three empty boxes for the answer.

Answer:

Actions

- 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.

Answer Area

- Create an Azure key vault.
- Configure access policies for the Azure key vault.
- Run Set-AzureRmVmDiskEncryptionExtension.

Explanation

- Create an Azure key vault.
- Configure access policies for the Azure key vault.
- Run Set-AzureRmVmDiskEncryptionExtension.

References:

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

NEW QUESTION: 30

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

You create one active conditional access policy named Portal Policy. Portal Policy is used to provide access to the Microsoft Azure Management cloud app.

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

The screenshot displays three panels from the Azure portal:

- Portal Policy:** Shows the policy name 'Portal Policy' and summary statistics under 'Assignments':
 - Users and groups: All users
 - Cloud apps: 1 app included
 - Conditions: 1 condition selected
 - Access controls: Grant (2 controls selected), Session (0 controls selected)
- Conditions:** Shows configuration options:
 - Device platforms: Not configured
 - Locations: 1 included
 - Client apps (preview): Not configured
 - Device state (preview): Not configured
- Locations:** Shows configuration options for user access based on physical location:
 - Configure: Yes (selected), No
 - Include/Exclude: Selected locations (selected)
 - Select: Contoso

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

Portal Policy

Info **Delete**

*** Name**
Portal Policy

Assignments

Users and groups
All users

Cloud apps
1 app included

Conditions
1 condition selected

Access controls

Grant
2 controls selected

Session
0 controls selected

Grant

Select the controls to be enforced.

Block access

Grant access

Require multi-factor authentication

Require device to be marked as compliant

Require Hybrid Azure AD joined device

Require approved client app
[See list of approved client apps](#)

For multiple controls

Require all the selected controls

Require one of the selected controls

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

Statements	Yes	No
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	<input type="radio"/>	<input type="radio"/>
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	<input type="radio"/>	<input type="radio"/>
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	<input type="radio"/>	<input type="radio"/>

Answer:

Explanation

Box 1: No

The Contoso location is excluded

Box 2: NO

Box 3: NO

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

NEW QUESTION: 31

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.

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:

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"/>

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!
 Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (460 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 32

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

You create a service endpoint for Subnet1.

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

You need to deploy Docker containers to VM1. The containers must be able to access Azure Storage resources and Azure SQL databases by using the service endpoint.

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

Answer: (SHOW ANSWER)

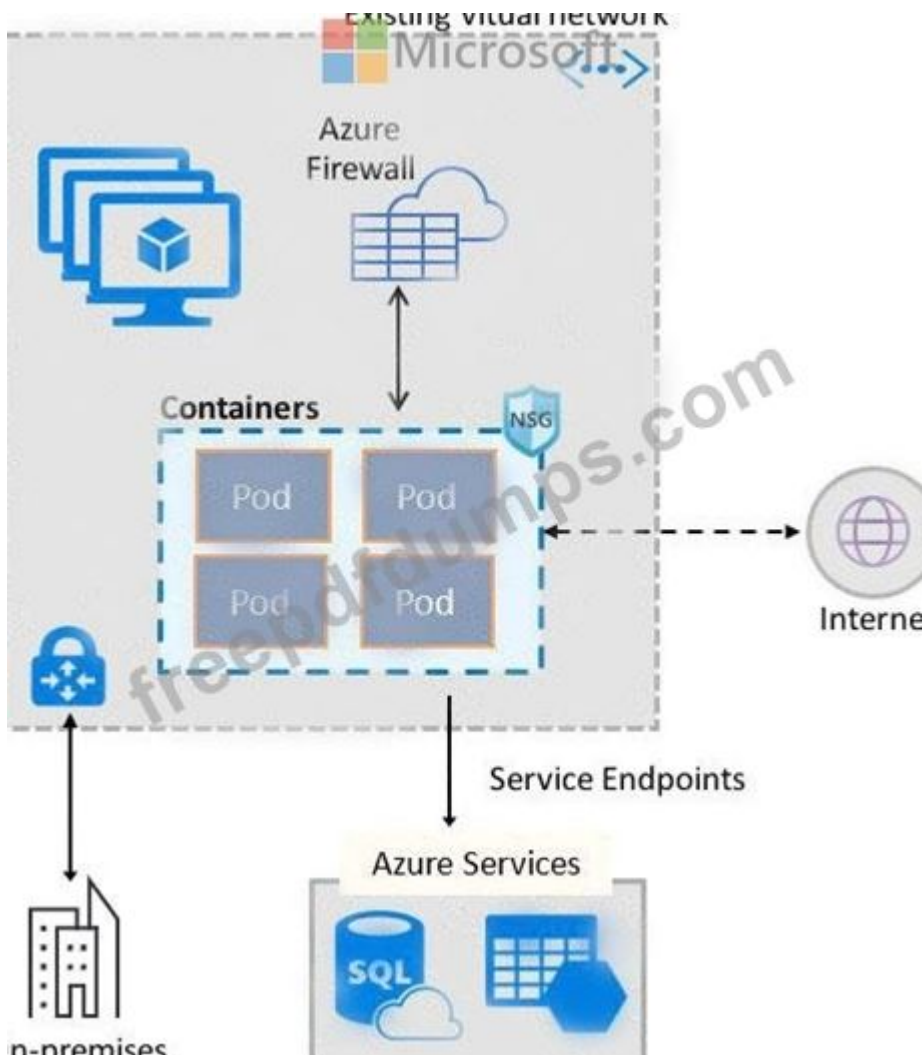
Explanation

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>

NEW QUESTION: 33

You have an Azure subscription that contains three storage accounts, an Azure SQL managed instance named SQL and three Azure SQL databases. The storage accounts are configured as shown in the following table.

SQL1 has the following settings:

- * Auditing: On
- * Audit log destination: storage1

The Azure SQL databases are configured as shown in the following table.

ANSWER AREA

Statements	Yes	No
Audit events for DB1 are written to storage1.	<input type="radio"/>	<input type="radio"/>
Audit events for DB2 are written to storage1 and storage2.	<input type="radio"/>	<input type="radio"/>
Storage3 can be used as an audit log destination for DB3.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

 **Microsoft**

Statements

Audit events for DB1 are written to storage1.	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Audit events for DB2 are written to storage1 and storage2.	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Storage3 can be used as an audit log destination for DB3.	<input type="radio"/> Yes	<input checked="" type="radio"/> No

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/auditing-configure>

<https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview>

NEW QUESTION: 34

You have an Azure Active directory tenant that syncs with an Active Directory Domain Services (AD DS) domain.

You plan to create an Azure file share that will contain folders and files.

Which identity store can you use to assign permissions to the Azure file share and folders within the share? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Azure files share:

Folders in the file share:

Answer:

Answer is as image below.

Answer Area

Azure files share:

Folders in the file share:

NEW QUESTION: 35

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

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

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

Name	Multi-factor authentication (MFA) status
User1	Enabled
User2	Enforced

The MFA service settings are configured as shown in the exhibit. (Click the Exhibit tab.)

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

- | | Yes | No |
|---|-----------------------|-----------------------|
| If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone. | <input type="radio"/> | <input type="radio"/> |
| If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app. | <input type="radio"/> | <input type="radio"/> |
| If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone | <input type="radio"/> | <input type="radio"/> |

Answer:

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 2: No

Use of Microsoft Authenticator is not required.

Note: Microsoft Authenticator is a multifactor app for mobile devices that generates time-based codes used during the Two-Step Verification process.

Box 3: No

The New York IP address subnet is included in the "skip multi-factor authentication for request.

References:

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

NEW QUESTION: 36

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

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

From Azure AD Privileged Identity Management (PIM), you configure the settings for the Security Administrator role as shown in the following exhibit.

Settings □ ×

Assignment

Allow permanent eligible assignment

Expire eligible assignments after

3 Months ▼

Allow permanent active assignment

Expire active assignments after


1 Month ▼

Require Azure Multi-Factor Authentication on active assignment

Require justification on active assignment

Activation

Activation maximum duration (hours)




5

Require Azure Multi-Factor Authentication on activation

Require justification on activation

Require ticket information on activation

Require approval to activate

*  Select approvers >

No member or group selected

From PIM, you assign the Security Administrator role to the following groups:

Group1: Active assignment type, permanently assigned

Group2: Eligible assignment type, permanently eligible

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	<input type="radio"/>	<input type="radio"/>
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	<input type="radio"/>	<input type="radio"/>
User3 can activate the Security Administrator role.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can activate the Security Administrator role.	<input checked="" type="radio"/>	<input type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

<https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings>

NEW QUESTION: 37

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains three security groups named Group1, Group2, and Group3 and the users shown in the following table.

Name	Role	Member of
User1	Application administrator	Group1
User2	Application developer	Group2
User3	Cloud application administrator	Group3

Group3 is a member of Group2.

In contoso.com, you register an enterprise application named App1 that has the following settings:

Owners: User1

Users and groups: Group2



You configure the properties of App1 as shown in the following exhibit.


Save Discard Delete Got feedback


Enabled for users to sign-in? Yes No

Name *

Homepage URL

Logo 
 

Application ID 

Object ID 

User assignment required? Yes No

Visible to users Yes No

Notes

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

Statements	Yes	No
User1 has App1 listed on his My Apps portal.	<input type="radio"/>	<input type="radio"/>
User2 has App1 listed on her My Apps portal.	<input type="radio"/>	<input type="radio"/>
User3 has App1 listed on her My Apps portal.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 has App1 listed on his My Apps portal.	<input type="radio"/>	<input type="radio"/>
User2 has App1 listed on her My Apps portal.	<input type="radio"/>	<input type="radio"/>
User3 has App1 listed on her My Apps portal.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>

NEW QUESTION: 38

You plan to deploy a custom policy initiative for Microsoft Defender for Cloud.

You need to identify all the resource groups that have a Delete lock.

How should you complete the policy definition? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

...

```

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

```

...

Answer:

ANSWER AREA



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

NEW QUESTION: 39

Your network contains an on-premises Active Directory domain named corp.contoso.com. You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. You sync all on-premises identities to Azure AD. You need to prevent users who have a givenName attribute that starts with TEST from being synced to Azure AD. The solution must minimize administrative effort. What should you use?

- A. Synchronization Rules Editor
- B. Web Service Configuration Tool
- C. the Azure AD Connect wizard
- D. Active Directory Users and Computers

Answer: A (LEAVE A REPLY)

Explanation

Use the Synchronization Rules Editor and write attribute-based filtering rule.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration>

NEW QUESTION: 40

You plan to use Azure Sentinel to create an analytic rule that will detect suspicious threats and automate responses.

Which components are required for the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Detect suspicious threats:

- A Kusto query language query
- A Transact-SQL query
- An Azure PowerShell query
- An Azure Sentinel playbook

Automate responses:

- An Azure Functions app
- An Azure PowerShell script
- An Azure Sentinel playbook
- An Azure Sentinel workbook

Answer:

Detect suspicious threats:

- A Kusto query language query
- A Transact-SQL query
- An Azure PowerShell query
- An Azure Sentinel playbook

Automate responses:

- An Azure Functions app
- An Azure PowerShell script
- An Azure Sentinel playbook
- An Azure Sentinel workbook

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

NEW QUESTION: 41

You have an Azure subscription that contains the Azure Log Analytics workspaces shown in the following table.

Name	Location	Description
Workspace1	East US	Used by Azure Sentinel
Workspace2	West US	Not applicable

You create the virtual machines shown in the following table.

Name	Location	Operating system	Connected to
VM1	East US	Windows Server 2019	None
VM2	East US	Windows Server 2019	Workspace2
VM3	West US	Windows Server 2019	None
VM4	West US	Windows Server 2019	Workspace2

You plan to use Azure Sentinel to monitor Windows Defender Firewall on the virtual machines. Which virtual machines you can connect to Azure Sentinel?

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

Answer: D (LEAVE A REPLY)

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall>

NEW QUESTION: 42

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

Microsoft Azure




Sign in

to continue to Microsoft Azure

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

Microsoft

Home - Microsoft Azure

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

Microsoft Azure





Azure services

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


Navigate

- Subscriptions
- Resource groups
- All resources
- Dashboard

Tools

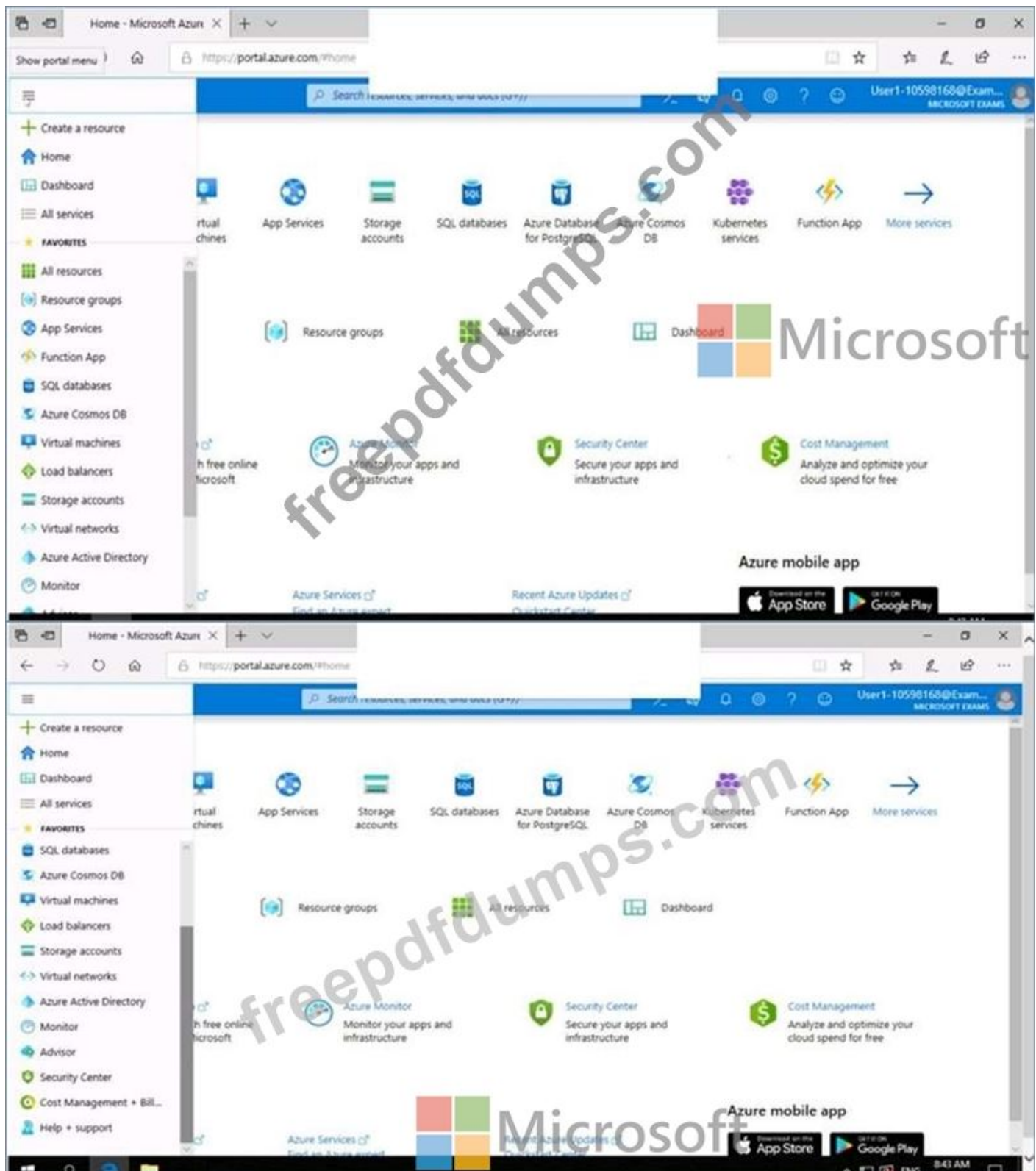
- Microsoft Learn  Learn Azure with free online training from Microsoft
- Azure Monitor  Monitor your apps and infrastructure
- Security Center  Secure your apps and infrastructure
- Cost Management  Analyze and optimize your cloud spend for free

Useful links

- Microsoft
- Recent Azure Updates 

Azure mobile app

Download on the App Store | Get it on Google Play



You need to email an alert to a user named admin1@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes.

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

Answer:

See the explanation below.

Explanation

Create an alert rule on a metric with the Azure portal

1. In the portal, locate the resource, here VM1, you are interested in monitoring and select it.

2. Select Alerts (Classic) under the MONITORING section. The text and icon may vary slightly for different resources.

3. Select the Add metric alert (classic) button and fill in the fields as per below, and click OK.

Metric: CPU Percentage

Condition: Greater than

Period: Over last 15 minutes

Notify via: email

Additional administrator email(s): admin1@contoso.com

Condition

Greater than

* Threshold

60

Period ⓘ

Over the last 5 minutes

Notify via

Email owners, contributors, and readers

Additional administrator email(s)

admin@contoso.com

Webhook ⓘ

http://www.contoso.com/dowork?param

Reference:

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

NEW QUESTION: 43

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.

Account type:

	▼
Azure Active Directory User	
Managed identity	
Service Principal	

Roles:

	▼
db_datawriter only	
db_datareader and db_datawriter	
db_owner only	

Answer:

Account type:	▼
Azure Active Directory User	
Managed identity	
Service Principal	
Roles:	▼
db_datawriter only	
db_datareader and db_datawriter	
db_owner only	

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/tutorial-connect-msi-sql-database?tabs=windowsclient%2Cdotnet>

NEW QUESTION: 44

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: [i](#)

IPv4 ADDRESS OR CIDR

...

Exception:

Allow trusted Microsoft services to **bypass** this firewall? Yes No

[i](#) 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.

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:

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

Explanation

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

NEW QUESTION: 45

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.

Actions



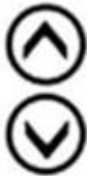
Run Set-AzureRmKeyVaultAccessPolicy

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a user-assigned managed identity.

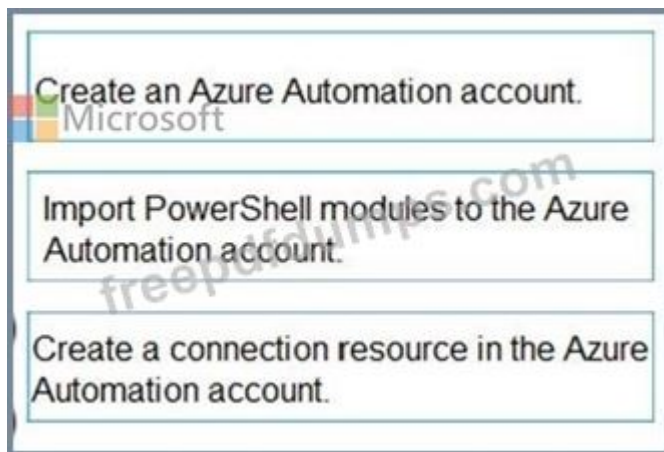
Create a connection resource in the Azure Automation account.



Answer:

Actions	Answer Area
Run Set-AzureRmKeyVaultAccessPolicy	
Create an Azure Automation account.	Create an Azure Automation account.
Import PowerShell modules to the 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.	Create a connection resource in the Azure Automation account.

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/>

NEW QUESTION: 46

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

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

From Azure AD Privileged Identity Management (PIM), you configure the settings for the Security Administrator role as shown in the following exhibit.

Settings  ⏏ ✕

Assignment

Allow permanent eligible assignment
 Expire eligible assignments after

Allow permanent active assignment
 Expire active assignments after

Require Azure Multi-Factor Authentication on active assignment

Require justification on active assignment

Activation


Activation maximum duration (hours)

Require Azure Multi-Factor Authentication on activation

Require justification on activation

Require ticket information on activation

Require approval to activate

*  Select approvers
 No member or group selected ➤

From PIM, you assign the Security Administrator role to the following groups:

- * Group1: Active assignment type, permanently assigned
- * Group2: Eligible assignment type, permanently eligible

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	<input type="radio"/>	<input type="radio"/>
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	<input type="radio"/>	<input type="radio"/>
User3 can activate the Security Administrator role.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	<input type="radio"/>	<input type="radio"/>
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	<input type="radio"/>	<input type="radio"/>
User3 can activate the Security Administrator role.	<input type="radio"/>	<input type="radio"/>

Explanation

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	<input type="radio"/>	<input type="radio"/>
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	<input type="radio"/>	<input type="radio"/>
User3 can activate the Security Administrator role.	<input type="radio"/>	<input type="radio"/>

Box 1: Yes

Eligible Type: A role assignment that requires a user to perform one or more actions to use the role. If a user has been made eligible for a role, that means they can activate the role when they need to perform privileged tasks. There's no difference in the access given to someone with a permanent versus an eligible role assignment. The only difference is that some people don't need that access all the time.

You can choose from two assignment duration options for each assignment type (eligible and active) when you configure settings for a role. These options become the default maximum duration when a user is assigned to the role in Privileged Identity Management.

Use the Activation maximum duration slider to set the maximum time, in hours, that a role stays active before it expires. This value can be from one to 24 hours.

Box 2: Yes

Active Type: A role assignment that doesn't require a user to perform any action to use the role. Users assigned as active have the privileges assigned to the role Box 3: Yes User3 is member of Group2.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

<https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource-roles>

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam! Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (460 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 47

You have a web app named WebApp1.

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

You need to protect WebApp1 by using WAF1.

What should you do first?

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

Answer: A (LEAVE A REPLY)

Explanation/Reference:

References:

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

NEW QUESTION: 48

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

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group2	Disabled

The tenant contains the named locations shown in the following table.

Name	IP address range	Trusted location
Seattle	193.77.10.0/24	Yes
Boston	154.12.18.0/24	No

You create the conditional access policies for a cloud app named App1 as shown in the following table.

Name	Include	Exclude	Condition	Grant
Policy1	Group1	Group2	Locations: Boston	Block access
Policy2	Group1	None	Locations: Any location	Grant access, Require multi-factor authentication
Policy3	Group2	Group1	Locations: Boston	Block access
Policy4	User2	None	Locations: Any location	Grant access, Require multi-factor authentication

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can access App1 from an IP address of 154.12.18.10.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 193.77.10.15.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 154.12.18.34.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can access App1 from an IP address of 154.12.18.10.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access App1 from an IP address of 193.77.10.15.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 154.12.18.34.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation

Statements	Yes	No
User1 can access App1 from an IP address of 154.12.18.10.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access App1 from an IP address of 193.77.10.15.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 154.12.18.34.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 49

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 8

You need to prevent HTTP connections to the rg1lod28681041n1 Azure Storage account.

Answer:

Check below steps in explanation for Task.

Explanation

To prevent HTTP connections to the rg1lod28681041n1 Azure Storage account, you can follow these steps:

In the Azure portal, search for and select the storage account named rg1lod28681041n1.

In the left pane, select Firewalls and virtual networks.

In the Firewalls and virtual networks pane, select Selected networks.

In the Selected networks pane, select Add existing virtual network.

In the Add existing virtual network pane, select the virtual network that does not allow HTTP connections.

Select Add.

NEW QUESTION: 50

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

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

In KeyVault, the following events occur in sequence:

Item1 is deleted

Administrator enables soft delete

Item2 and Policy1 are deleted.

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

NOTE: Each correct selection is worth one point.


Statements

- You can recover Policy1. Yes No
- You can add a new key named Item1. Yes No
- You can add a new secret named Item2. Yes No

Answer:


Statements

- You can recover Policy1. Yes No
- You can add a new key named Item1. Yes No
- You can add a new secret named Item2. Yes No

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview>

NEW QUESTION: 51

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

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

The company is sold to a new owner.

The company needs to transfer ownership of Subscription1.

Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User:

- User1
- User2
- User3
- User4

Microsoft
Tool:

- Azure Account Center
- Azure Cloud Shell
- Azure PowerShell
- Azure Security Center

Answer:

User:

	▼
User1	
User2	
User3	
User4	



Tool:

	▼
Azure Account Center	
Azure Cloud Shell	
Azure PowerShell	
Azure Security Center	

Explanation

User:	<table border="1"><tr><td></td><td>▼</td></tr><tr><td>User1</td><td></td></tr><tr><td>User2</td><td></td></tr><tr><td>User3</td><td></td></tr><tr><td>User4</td><td></td></tr></table>		▼	User1		User2		User3		User4	
	▼										
User1											
User2											
User3											
User4											
Tool:	<table border="1"><tr><td></td><td>▼</td></tr><tr><td>Azure Account Center</td><td></td></tr><tr><td>Azure Cloud Shell</td><td></td></tr><tr><td>Azure PowerShell</td><td></td></tr><tr><td>Azure Security Center</td><td></td></tr></table>		▼	Azure Account Center		Azure Cloud Shell		Azure PowerShell		Azure Security Center	
	▼										
Azure Account Center											
Azure Cloud Shell											
Azure PowerShell											
Azure Security Center											

Box 1; User2

Billing Administrator

Select Transfer billing ownership for the subscription that you want to transfer.

Enter the email address of a user who's a billing administrator of the account that will be the new owner for the subscription.

Box 2: Azure Account Center

Azure Account Center can be used.

Reference:

<https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transfer-billing-ownership-of-an-azu>

NEW QUESTION: 52

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

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

From Azure Security Center, you turn on Auto Provisioning.

You deploy the virtual machines shown in the following table.

<https://www.fast2test.com/AZ-500-practice-test.html> 64

Valid Fast2test AZ-500 Exam PDF Dumps - New AZ-500 Real Exam Questions

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

On which virtual machines is the Log Analytics Agent installed?

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

Answer: D (LEAVE A REPLY)

When automatic provisioning is On, Security Center provisions the Log Analytics Agent on all supported Azure VMs and any new ones that are created.

Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection>

NEW QUESTION: 53

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

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

You have an Azure subscription named Subscription2 that contains the following resources:


An Azure Sentinel workspace

An Azure Event Grid instance

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

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

NOTE: Each correct selection is worth one point.


Subscription1:  ▼

- An Azure Log Analytics agent on a Linux virtual machine
- A Data Factory pipeline
- An Event Hubs namespace
- An Azure Service Bus queue

Subscription2: ▼

- A new Azure Log Analytics workspace
- A new Azure Sentinel data connector
- A new Azure Sentinel playbook
- A new Event Grid resource provider

Answer:

Subscription1:  ▼

- An Azure Log Analytics agent on a Linux virtual machine
- A Data Factory pipeline
- An Event Hubs namespace
- An Azure Service Bus queue

Subscription2: ▼

- A new Azure Log Analytics workspace
- A new Azure Sentinel data connector
- A new Azure Sentinel playbook
- A new Event Grid resource provider

NEW QUESTION: 54

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. Key1 and Secret1 only
- C. Secret1 and Cert1 only
- D. Cert1 only
- E. Key1 and Cert1 only
- F. Key1, Secret1, and Cert1

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 55

You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.

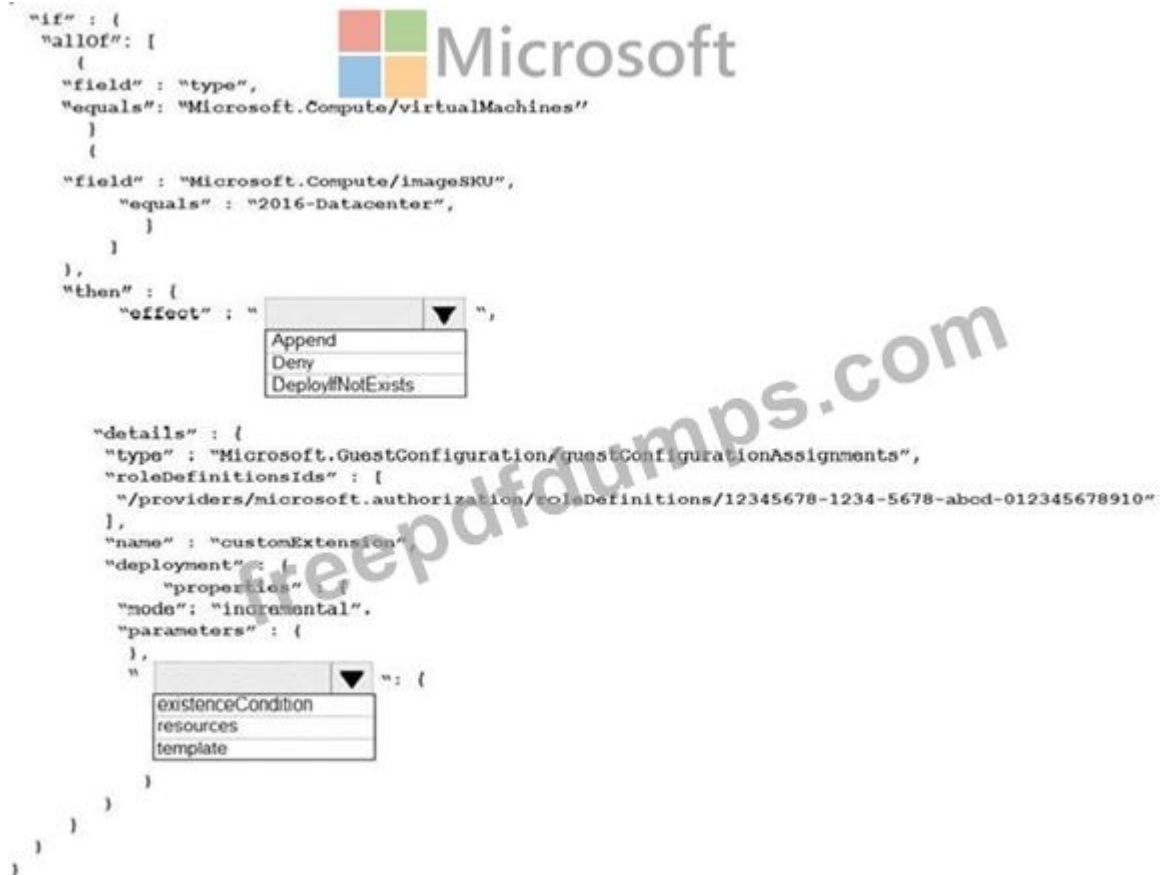
You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.

How should you complete the policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

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

```




Answer:

```

{
  "if" : {
    "allOf" : [
      {
        "field" : "type",
        "equals" : "Microsoft.Compute/virtualMachines"
      }
    ],
    "then" : {
      "effect" : "
      Append
      Deny
      DeployIfNotExists
      ",
      "details" : {
        "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
        "roleDefinitionsIds" : [
          "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
        ],
        "name" : "customExtension",
        "deployment" : {
          "properties" : {
            "mode": "incremental",
            "parameters" : {
              "
              existenceCondition
              resources
              template
              ": {
            }
          }
        }
      }
    }
  }
}

```




Explanation

```

},
"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
          ": {
        }
      }
    }
  }
}

```



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>

NEW QUESTION: 56

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

What should you do?

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

Add the new groups to Group1.

Answer: (SHOW ANSWER)

Section: [none]

Explanation:

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>

Testlet 2 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 question on this case study.

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

To start the case study

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

Overview

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

The company hosts its entire server infrastructure in Azure.

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

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.

NEW QUESTION: 57

You have an Azure subscription that contains a resource group named RG1. RG1 contains a storage account named storage1.

You have two custom Azure roles named Role1 and Role2 that are scoped to RG1.

The permissions for Role1 are shown in the following JSON code.

```

"permissions": [
  {
    "actions": [
      "Microsoft.Storage/storageAccounts/listKeys/action".
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
]

```



The permissions for Role2 are shown in the following JSON code.

```

"permissions": [
  {
    "actions": [
      "Microsoft.Storage/storageAccounts/listKeys/action",
      "Microsoft.Storage/storageAccounts/ListAccountSas/action",
      "Microsoft.Storage/storageAccounts/read"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
]

```

Answer Area

Statements

- User1 can read data in storage1.
- User2 can read data in storage1.
- User3 can restore storage1 from a backup in Azure Backup.

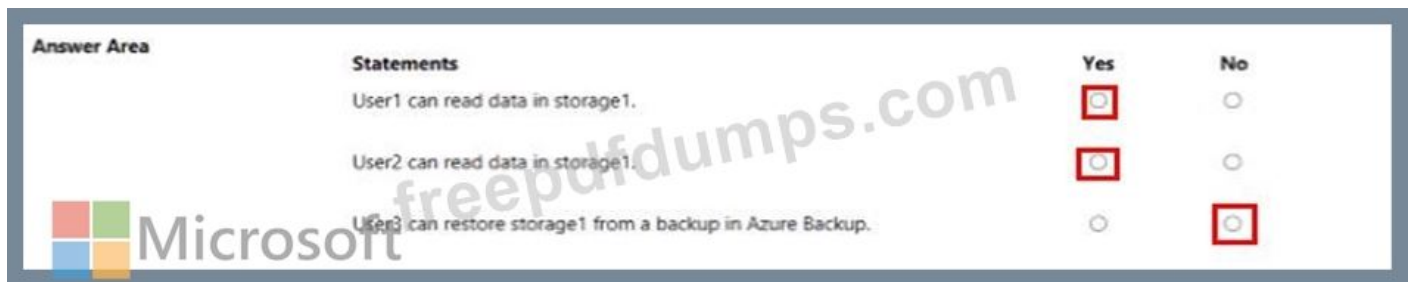
Yes

No



Microsoft

Answer:



NEW QUESTION: 58

You have an Azure subscription named Sub1.

In Azure Security Center, you have a workflow automation named WF1. WF1 is configured to send an email message to a user named User1.

You need to modify WF1 to send email messages to a distribution group named Alerts.

What should you use to modify WF1?

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

Answer: C (LEAVE A REPLY)

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/workflow-automation>

<https://docs.microsoft.com/en-us/learn/modules/resolve-threats-with-azure-security-center/6-exerciseconfigure-playbook>

NEW QUESTION: 59

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

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

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

Which virtual machines can be enrolled in Analytics1?

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

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 60

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

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Enabled
User2	Group1	Disabled
User3	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:

Assignments: Include Group1, exclude Group2

Conditions: Sign-in risk level: Medium and above

Access Allow access, Require multi-factor authentication

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

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

NOTE: Each correct selection is worth one point.

When User1 signs in from an anonymous IP address, the user will:

When User2 signs in from an unfamiliar location, the user will:

When User3 signs in from an infected device, the user will:

Answer:

When User1 signs in from an anonymous IP address, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

When User2 signs in from an unfamiliar location, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

When User3 signs in from an infected device, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

References:

<http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/>

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies>

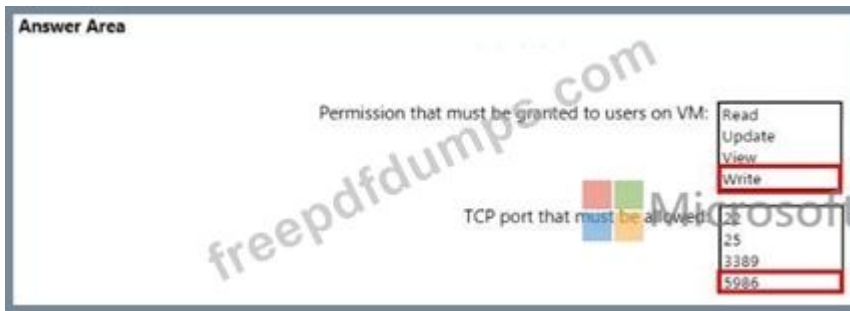
<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

NEW QUESTION: 61

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

Answer Area	
	
Permission that must be granted to users on VM:	<input type="checkbox"/> Read <input type="checkbox"/> Update <input type="checkbox"/> View <input type="checkbox"/> Write
TCP port that must be allowed:	<input type="checkbox"/> 22 <input type="checkbox"/> 25 <input type="checkbox"/> 3389 <input type="checkbox"/> 5986

Answer:



Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam! Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (460 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 62

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

Answer: (SHOW ANSWER)

NEW QUESTION: 63

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

In which resource groups can User8 create virtual networks and NSGs? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

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:

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

Explanation

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

Box2: RG4 & RG6

NEW QUESTION: 64

You plan to use Azure Sentinel to create an analytic rule that will detect suspicious threats and automate responses.

Which components are required for the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Detect suspicious threats:

- A Kusto query language query
- A Transact-SQL query
- An Azure PowerShell query
- An Azure Sentinel playbook

Automate responses:

- An Azure Functions app
- An Azure PowerShell script
- An Azure Sentinel playbook
- An Azure Sentinel workbook

Answer:

The screenshot shows the configuration interface for an Azure Sentinel analytic rule. The 'Detect suspicious threats' dropdown menu is open, and the first option, 'A Kusto query language query', is highlighted with a red box. The 'Automate responses' dropdown menu is also open, and the third option, 'An Azure Sentinel playbook', is highlighted with a red box. The Microsoft logo is visible in the top left corner of the interface.

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

NEW QUESTION: 65

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

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

User2 is the owner of Group2.

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

[+ Add user](#)
[✎ Edit](#)
[🗑 Remove](#)
[🔑 Update Credentials](#)
[☰ Columns](#)
[💙 Got feedback?](#)

📘 The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
<input type="checkbox"/> GR Group1	Group	Default Access

You enable self-service application access for App1 as shown in the following exhibit.

Allow users to request access to this application? 📘 Yes No

To which group should assigned users be added? 📘
 Select group >
 Group2

Require approval before granting access to this application? 📘 Yes No

Who is allowed to approve access to this application? 📘
 Select approvers >
 1 users selected

To which role should users be assigned in this application? 📘
 *Select a role >
 Default Access

User3 is configured to approve access to App1.

You need to identify the owners of Group2 and the users of App1.

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

NOTE: Each correct selection is worth one point.

Group2 owners: [dropdown menu]

- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

App1 users: [dropdown menu]

- Group1 members only
- Group2 members only
- Group1 and Group2 members only
- Group1 and Group2 members and User1 only
- Group1 and Group2 members, User1, and User3 only

Answer:

Group2 owners: [dropdown menu]

- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

App1 users: [dropdown menu]

- Group1 members only
- Group2 members only
- Group1 and Group2 members only
- Group1 and Group2 members and User1 only
- Group1 and Group2 members, User1, and User3 only

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access>

NEW QUESTION: 66

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

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

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

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

You need to configure auditing for SQL1.

Which storage accounts and Log Analytics workspaces can you use as the audit log destination?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Storage accounts that can be used as the audit log destination:

Log Analytics workspaces that can be used as the audit log destination:

Answer:

Answer Area

Storage accounts that can be used as the audit log destination:

Log Analytics workspaces that can be used as the audit log destination:

Explanation

Storage accounts that can be used as the audit log destination:

	▼
Storage1 only	
Storage2 only	
Storage1 and Storage2 only	
Storage1, Storage2, and Storage3	

Log Analytics workspaces that can be used as the audit log destination:

	▼
Analytics1 only	
Analytics1 and Analytics2 only	
Analytics1 and Analytics3 only	
Analytics1, Analytics2, and Analytics3	

NEW QUESTION: 67

You have an Azure subscription that contains a web app named App1. App1 provides users with product images and videos. Users access App1 by using a URL of [HTTPS://appl.contoso.com](https://appl.contoso.com). You deploy two server pools named Pool1 and Pool2. Pool1 hosts product images. Pool2 hosts product videos. You need to optimize the performance of App1. The solution must meet the following requirements:

- * Minimize the performance impact of TLS connections on Pool1 and Pool2.
- * Route user requests to the server pools based on the requested URL path.

What should you include in the solution?

- A. Azure Traffic Manager
- B. Azure Application Gateway
- C. Azure Front Door
- D. Azure Bastion

Answer: B (LEAVE A REPLY)

NEW QUESTION: 68

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

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

You have an Azure subscription named Subscription2 that contains the following resources:

- An Azure Sentinel workspace
- An Azure Event Grid instance

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

NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 69

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

The subscription is linked to an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

You create the groups shown in the following table.

The membership rules for Group1 and Group2 are configured as shown in the following exhibit.

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")
```

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

Statements	Yes	No
User1 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:

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"/>

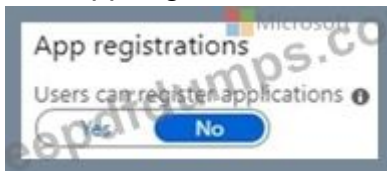
Reference:

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

NEW QUESTION: 70

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant and a user named User1.

The App registrations settings for the tenant are configured as shown in the following exhibit.



You plan to deploy an app named App1.

You need to ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.

Which role should you assign to User1?

- A. App Configuration Data Owner for the subscription
- B. Managed Application Contributor for the subscription
- C. Cloud application administrator in Azure AD
- D. Application developer in Azure AD.

Answer: ([SHOW ANSWER](#))

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task>

NEW QUESTION: 71

You need to ensure that the events in the NetworkSecurityGroupRuleCounter log of the VNET01-Subnet0-NSG network security group (NSG) are stored in the logs11597200 Azure Storage account for 30 days.

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

Answer:

See the explanation below.

Explanation

You need to configure the diagnostic logging for the NetworkSecurityGroupRuleCounter log.

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

NEW QUESTION: 72

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

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

User2 is the owner of Group2.

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



You enable self-service application access for App1 as shown in the following exhibit.

Allow users to request access to this application? ⓘ

Yes No



Microsoft

To which group should assigned users be added? ⓘ

Select group

Group2



Require approval before granting access to this application? ⓘ

Yes No

Who is allowed to approve access to this application? ⓘ

Select approvers

1 users selected



To which role should users be assigned in this application? ⓘ

*Select a role

Default Access



User3 is configured to approve access to Appl.

You need to identify the owners of Group2 and the users of Appl.

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

NOTE: Each correct selection is worth one point.

Group2 owners:

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

App1 users:

▼
Group1 members only
Group2 members only
Group1 and Group2 members only
Group1 and Group2 members and User1 only
Group1 and Group2 members, User1, and User3 only

Answer:

Group2 owners:

- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

App1 users:

- Group1 members only
- Group2 members only
- Group1 and Group2 members only
- Group1 and Group2 members and User1 only
- Group1 and Group2 members, User1, and User3 only

Explanation

Group2 owners:

- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

App1 users:

- Group1 members only
- Group2 members only
- Group1 and Group2 members only
- Group1 and Group2 members and User1 only
- Group1 and Group2 members, User1, and User3 only

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access>

NEW QUESTION: 73

You need to ensure that the Azure AD application registration and consent configurations meet the identity and access requirements.

What should you use in the Azure portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

To configure the registration settings:

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

To configure the consent settings:

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

Answer:

To configure the registration settings:	<table border="1"><tr><td></td><td>▼</td></tr><tr><td colspan="2">Azure AD – User settings</td></tr><tr><td colspan="2">Azure AD – App registrations settings</td></tr><tr><td colspan="2">Enterprise Applications – User settings</td></tr></table>		▼	Azure AD – User settings		Azure AD – App registrations settings		Enterprise Applications – User settings	
	▼								
Azure AD – User settings									
Azure AD – App registrations settings									
Enterprise Applications – User settings									
To configure the consent settings:	<table border="1"><tr><td></td><td>▼</td></tr><tr><td colspan="2">Azure AD – User settings</td></tr><tr><td colspan="2">Azure AD – App registrations settings</td></tr><tr><td colspan="2">Enterprise Applications – User settings</td></tr></table>		▼	Azure AD – User settings		Azure AD – App registrations settings		Enterprise Applications – User settings	
	▼								
Azure AD – User settings									
Azure AD – App registrations settings									
Enterprise Applications – User settings									

Reference:

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

NEW QUESTION: 74

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

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

You have an Azure subscription named Sub1.

You have an Azure Storage account named sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service.

You need to revoke all access to sa1.

Solution: You create a new stored access policy.

Does this meet the goal?

A. Yes

B. No

Answer: ([SHOW ANSWER](#))

Creating a new (additional) stored access policy will have no effect on the existing policy or the SAS's linked to it.

To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier.

Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately effects all of the shared access signatures associated with it.

Reference:

<https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy>

NEW QUESTION: 75

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

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

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

You plan to deploy an Azure firewall to HubVNet.

You create the following two routing tables:

* RT1: Includes a user-defined route that points to the private IP address of the Azure firewall as a next hop address

* RT2: Disables BGP route propagation and defines the private IP address of the Azure firewall as the default gateway You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.

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

NOTE: Each correct selection is worth one point.

Subnets



Answer Area

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

RT1:

RT2:

Answer:

Subnets	Answer Area
Azure FirewallSubnet	RT1: GatewaySubnet
GatewaySubnet	RT2: HubVNetSubnet0
HubVNetSubnet0	

Explanation

Answer Area

RT1: GatewaySubnet

RT2: HubVNetSubnet0

NEW QUESTION: 76

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.

You have 500 Azure virtual machines that run Windows Server 2016 and are enrolled in LAW1. You plan to add the System Update Assessment solution to LAW1.

You need to ensure that System Update Assessment-related logs are uploaded to LAW1 from 100 of the virtual machines only.

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

Actions	Answer Area
Create a new workspace.	
Apply the scope configuration to the solution.	
Create a scope configuration.	
Create a computer group.	
Create a data source.	

Answer:

Actions	Answer Area
Create a new workspace.	Create a computer group.
Apply the scope configuration to the solution.	Create a scope configuration.
Create a scope configuration.	Apply the scope configuration to the solution.
Create a computer group.	
Create a data source.	

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solution-targeting>

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam! Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (460 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 77

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.

You have 100 on-premises servers that run Windows Server 2012 R2 and Windows Server 2016. The servers connect to LAW1. LAW1 is configured to collect security-related performance counters from the connected servers.

You need to configure alerts based on the data collected by LAW1. The solution must meet the following requirements:

Alert rules must support dimensions.

The time it takes to generate an alert must be minimized.

Alert notifications must be generated only once when the alert is generated and once when the alert is resolved.

Which signal type should you use when you create the alert rules?

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

Answer: C (LEAVE A REPLY)

Metric alerts in Azure Monitor provide a way to get notified when one of your metrics cross a threshold. Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights standard and custom metrics.

Note: Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric>

NEW QUESTION: 78

You have an Azure subscription named Sub1.

In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.

You need to modify Play1 to send email messages to a distribution group named Alerts.

What should you use to modify Play1?

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

Answer: (SHOW ANSWER)

Section: [none]

Explanation:

You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up.

References:

NEW QUESTION: 79

You have an Azure key vault.

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

- * Provide a user named User1 with the ability to set advanced access policies for the key vault.
- * Provide a user named User2 with the ability to add and delete certificates in the key vault.
- * Use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

User1:

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

User2:

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

Answer:

User1:

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

User2:

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

Explanation:

User1: RBAC

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

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

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

User2: A key vault access policy

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

References:

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

NEW QUESTION: 80

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



Home - Microsoft Azure X +

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

Microsoft Azure Search [resources, services, what's new (1/27)] 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 ^o
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 ^o
- Azure Services ^o
- Recent Azure Updates ^o

Azure mobile app

Download on the App Store | GET IT ON Google Play

Home - Microsoft Azure X +

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

Show portal menu

Search [resources, services, what's new (1/27)] User1-10598168@Exam... MICROSOFT EXAMS

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor

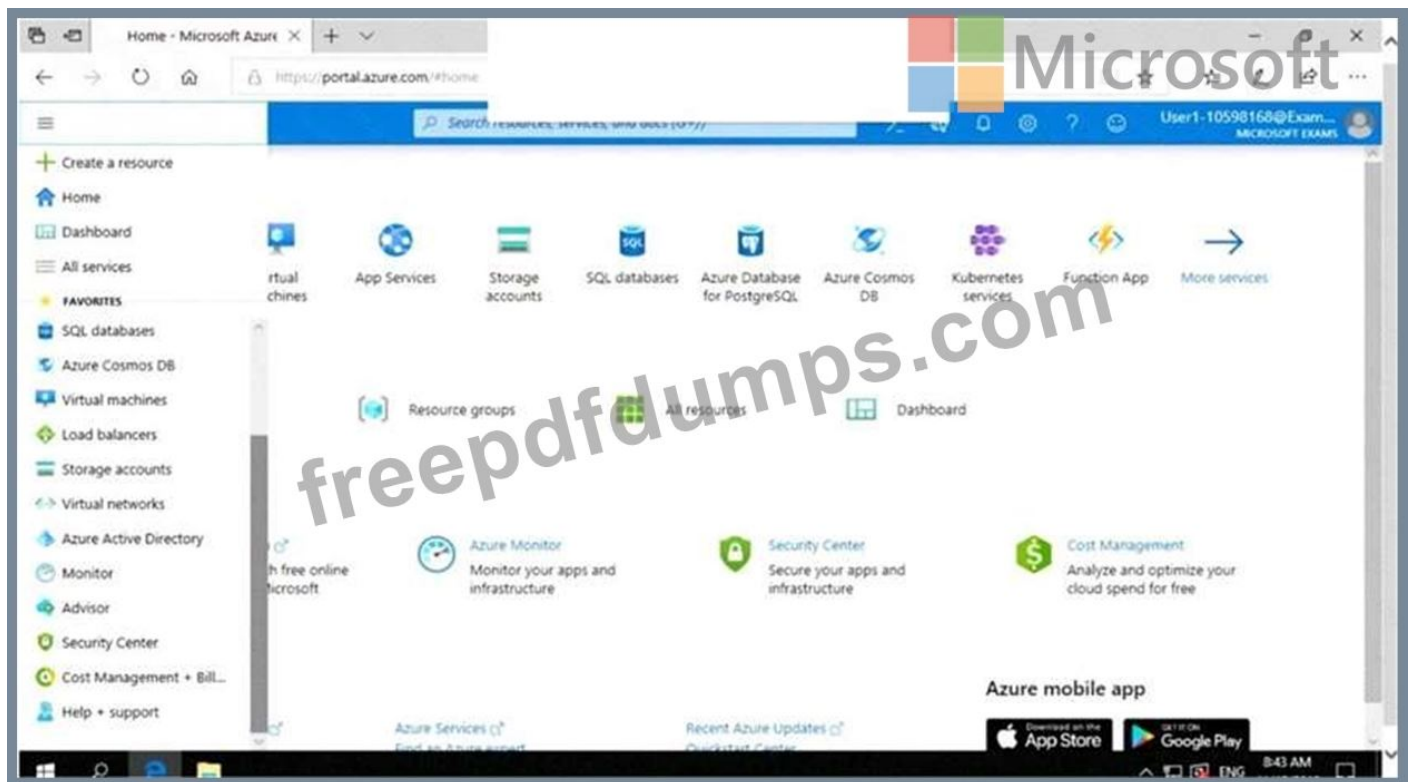
- Virtual machines
- App Services
- Storage accounts
- SQL databases
- Azure Database for PostgreSQL
- Azure Cosmos DB
- Kubernetes services
- Function App
- More services

- Resource groups
- All Resources
- Dashboard

- Microsoft Learn ^o
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

Azure mobile app

Download on the App Store | GET IT ON Google Play



The developers at your company plan to create a web app named App10598168 and to publish the app to

<https://www.contoso.com>.

You need to perform the following tasks:

- * Ensure that App10598168 is registered to Azure Active Directory (Azure AD).
- * Generate a password for App10598168.

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

See the explanation below.

Answer:


Explanation

Step 1: Register the Application

1. Sign in to your Azure Account through the Azure portal.
2. Select Azure Active Directory.
3. Select App registrations.
4. Select New registration.
5. Name the application App10598168 . Select a supported account type, which determines who can use the application. Under Redirect URI, select Web for the type of application you want to create. Enter the URI:

<https://www.contoso.com> , where the access token is sent to.

Register an application

 If you are building an application for external users that will be distributed by Microsoft, you must register as a first party application to meet all security, privacy, and compliance policies. [Read our decision guide](#)

* Name

The user-facing display name for this application (this can be changed later).

example-app

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (Microsoft)

Accounts in any organizational directory

Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

https://contoso.org/exampleapp

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

6. Click Register

Step 2: Create a new application secret

If you choose not to use a certificate, you can create a new application secret.

7 Select Certificates & secrets.

8. Select Client secrets -> New client secret.

9. Provide a description of the secret, and a duration. When done, select Add.

After saving the client secret, the value of the client secret is displayed. Copy this value because you aren't able to retrieve the key later. You provide the key value with the application ID to sign in as the application.

Store the key value where your application can retrieve it.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

NEW QUESTION: 81

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.


The screenshot shows two dropdown menus for User1 and User2. Each dropdown menu is open, displaying five options: 'A key vault access policy', 'Azure Information Protection', 'Azure Policy', 'Managed identities for Azure resources', and 'RBAC'. A Microsoft logo is visible at the bottom of the interface.

Answer:

User1:

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

User2:

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

Explanation



User1:

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

User2:

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

Explanation:

User1: RBAC

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

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

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

User2: A key vault access policy

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

References:

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

NEW QUESTION: 82

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	In resource group
cont1	Container instance	RG1
VNET1	Virtual network	RG1
App1	App Service app	RG1
VM1	Virtual machine	RG1
User1	User	Not applicable

You create a custom RBAC role in Subscription1 by using the following JSON file.

```
{
  "Name": "Role1",
  "IsCustom": true,
  "Description": "Role1 description",
  "Actions": [
    "*/Read",
    "Microsoft.Compute/*"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/subscriptions/923a419a-4358-40fb-b4a9-b8af43dd0c92/resourceGroups/RG1"
  ]
}
```

You assign Role1 to User1 on RG1.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can add VM1 to VNET1.	<input type="radio"/>	<input type="radio"/>
User1 can start and stop App1.	<input type="radio"/>	<input type="radio"/>
User1 can start and stop cont1.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements  Microsoft

	Yes	No
User1 can add VM1 to VNET1.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can start and stop App1.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can start and stop cont1.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute>

NEW QUESTION: 83

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. You need to configure VNet Peering between the two networks. The questions states, "The solution must ensure that virtual machines connected to VNET1 can communicate with virtual machines connected to VNET2". It doesn't say the VMs on VNET2 should be able to communicate with VMs on VNET1. Therefore, we need to configure the peering to allow just the one-way communication.

1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET1. Alternatively, browse to Virtual Networks in the left navigation pane.

2. In the properties of VNET1, click on Peerings.

3. In the Peerings blade, click Add to add a new peering.

4. In the Name of the peering from 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.

5. For the option Allow virtual network access from remote network to VNET1, click the slider button to Disabled.

6. Click the OK button to save the changes.

B. You need to configure VNet Peering between the two networks. The questions states, "The solution must ensure that virtual machines connected to VNET1 can communicate with virtual machines connected to VNET2". It doesn't say the VMs on VNET2 should be able to communicate with VMs on VNET1. Therefore, we need to configure the peering to allow just the one-way communication.

1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET1. Alternatively, browse to Virtual Networks in the left navigation pane.
 2. In the properties of VNET1, click on Peerings.
 3. In the Peerings blade, click Add to add a new peering.
 4. In the Name of the peering from VNET1 to remote virtual network box, enter a name such as VNET1-VNET2 (this is the name that the peering will be displayed as in VNET1)
 5. In the Virtual Network box, select VNET2.
 6. In the Name of the peering from remote virtual network to VNET1 box, enter a name such as VNET2-VNET1 (this is the name that the peering will be displayed as in VNET2).
- There is an option Allow virtual network access from VNET to remote virtual network. This should be left as Enabled.
7. For the option Allow virtual network access from remote network to VNET1, click the slider button to Disabled.
 8. Click the OK button to save the changes.

Answer: B (LEAVE A REPLY)

Reference:


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

NEW QUESTION: 84

Which virtual networks in Sub1 can User2 modify and delete in their current state? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Virtual networks that User2 can modify:

 Microsoft	
<input type="checkbox"/>	VNET4 only
<input type="checkbox"/>	VNET4 and VNET1 only
<input type="checkbox"/>	VNET4, VNET3, and VNET1 only
<input type="checkbox"/>	VNET4, VNET3, VNET2, and VNET1

Virtual networks that User2 can delete:

<input type="checkbox"/>	VNET4 only
<input type="checkbox"/>	VNET4 and VNET1 only
<input type="checkbox"/>	VNET4, VNET3, and VNET1 only
<input type="checkbox"/>	VNET4, VNET3, VNET2, and VNET1

Answer:

Virtual networks that User2 can modify:

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

Virtual networks that User2 can delete:

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



Reference:

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

NEW QUESTION: 85

You plan to use Azure Resource Manager templates to perform multiple deployments of identically configured Azure virtual machines. The password for the administrator account of each deployment is stored as a secret in different Azure key vaults.

You need to identify a method to dynamically construct a resource ID that will designate the key vault containing the appropriate secret during each deployment. The name of the key vault and the name of the secret will be provided as inline parameters.

What should you use to construct the resource ID?

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

Answer: B (LEAVE A REPLY)

Explanation

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli#re>

NEW QUESTION: 86

You have the hierarchy of Azure resources shown in the following exhibit.



You create the Azure Blueprints definitions shown in the following table.

Name	Published at
Blueprint1	Tenant Root Group
Blueprint2	Subscription1

To which objects can you assign Blueprint1 and Blueprint2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Blueprint1:

- ManagementGroup1 only
- ManagementGroup1, Subscription1, and RG1 only
- ManagementGroup1, Subscription1, RG1, and VM1
- Subscription1 only
- Tenant Root Group only
- Tenant Root Group, ManagementGroup1, and Subscription1 only

Blueprint2:

- ManagementGroup1 only
- Subscription1 and RG1 only
- Subscription1 only
- Subscription1, RG1, and VM1

Answer:



NEW QUESTION: 87

You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role
User1	Global administrator
User2	Security administrator
User3	Security reader
User4	License administrator

Each user is assigned an Azure AD Premium P2 license.

You plan to onboard and configure Azure AD Identity Protection.

Which users can onboard Azure AD Identity Protection, remediate users, and configure policies?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Answer Area

Users who can onboard Azure AD Identity Protection:

- User1 only
- User1 and User2 only
- User1, User 2, and User3 only
- User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:

- User1 and User2 only
- User1 and User3 only
- User1, User 2, and User3 only
- User1, User 2, User3, and User 4

Answer:

Create the rule and set the type to:

- Fusion
- Microsoft Security incident creation
- Scheduled

Configure the playbook to include:

- A managed connector
- A system-assigned managed identity
- A trigger
- Diagnostic settings

Explanation

Users who can onboard Azure AD Identity Protection:

- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3, and User4 only

Users who can remediate users and configure policies:

- User1 and User2 only
- User1 and User3 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

NEW QUESTION: 88

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

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

You have an Azure subscription named Subscription2 that contains the following resources:

An Azure Sentinel workspace

An Azure Event Grid instance

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

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

NOTE: Each correct selection is worth one point.

Subscription1:	<input type="text"/>
	An Azure Log Analytics agent on a Linux virtual machine
	A Data Factory pipeline
	An Event Hubs namespace
	An Azure Service Bus queue
Subscription2:	<input type="text"/>
	A new Azure Log Analytics workspace
	A new Azure Sentinel data connector
	A new Azure Sentinel playbook
	A new Event Grid resource provider

Answer:

Subscription1:	<input type="text"/>
	An Azure Log Analytics agent on a Linux virtual machine
	A Data Factory pipeline
	An Event Hubs namespace
	An Azure Service Bus queue
Subscription2:	<input type="text"/>
	A new Azure Log Analytics workspace
	A new Azure Sentinel data connector
	A new Azure Sentinel playbook
	A new Event Grid resource provider

NEW QUESTION: 89

Lab Task

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: GpO Ae4@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 5

You need to ensure that only devices connected to a 131-107.0.0/16 subnet can access data in the rg1lod28681041 Azure Storage account.

Answer:

To ensure that only devices connected to a 131-107.0.0/16 subnet can access data in the rg1lod28681041 Azure Storage account, you can follow these steps:

In the Azure portal, search for and select the storage account named rg1lod28681041.

In the left pane, select Firewalls and virtual networks.

In the Firewalls and virtual networks pane, select Selected networks.

In the Selected networks pane, select Add existing virtual network.

In the Add existing virtual network pane, select the virtual network that contains the 131-107.0.0/16 subnet.

Select Add.

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

NEW QUESTION: 90

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

In which resource groups can User8 create virtual networks and NSGs? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

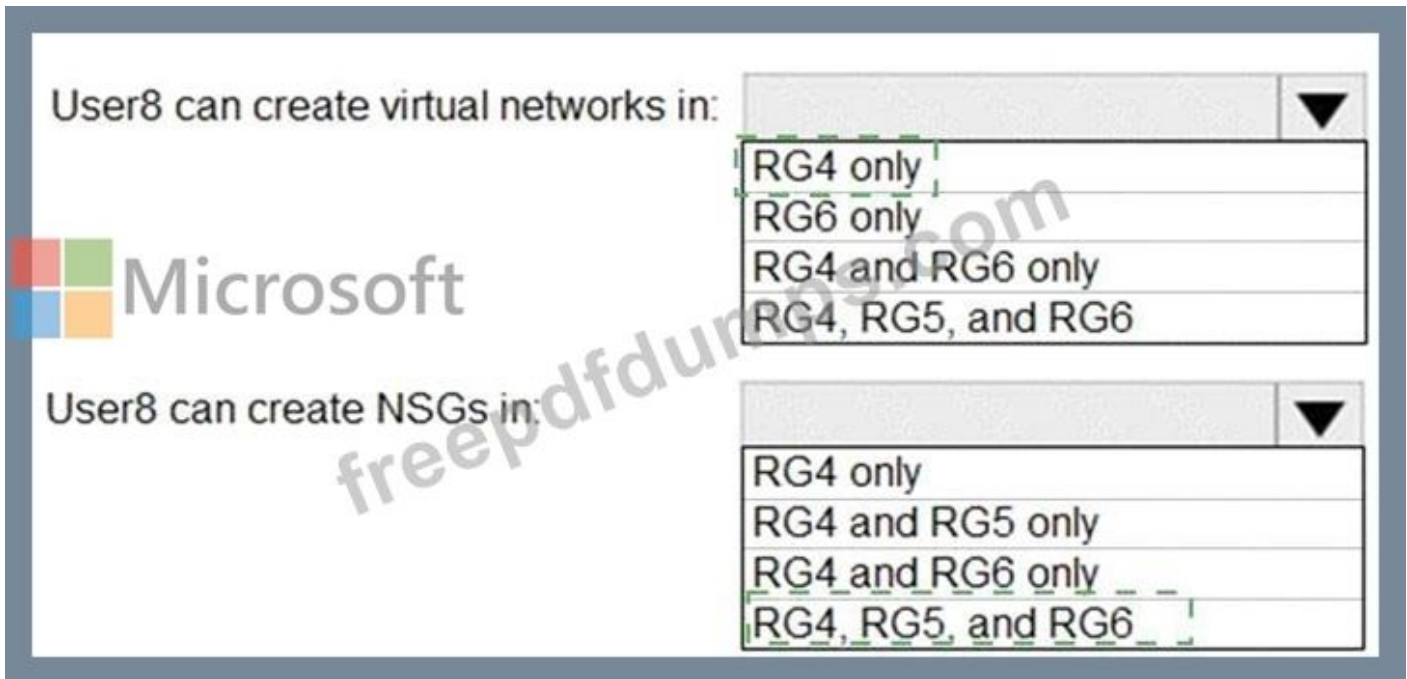
User8 can create virtual networks in:

Microsoft	▼
RG4 only	
RG6 only	
RG4 and RG6 only	
RG4, RG5, and RG6	

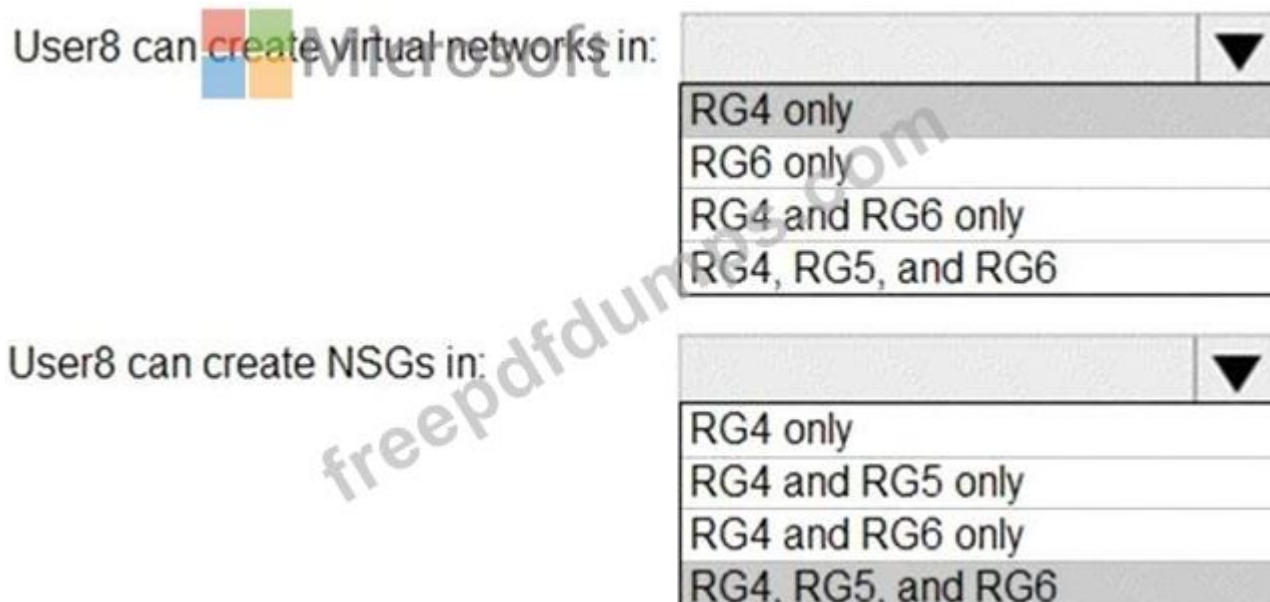
User8 can create NSGs in:

	▼
RG4 only	
RG4 and RG5 only	
RG4 and RG6 only	
RG4, RG5, and RG6	

Answer:



Explanation



Box 1: RG4 only

Virtual Networks are not allowed for Rg5 and Rg6.

Box 2: Rg4,Rg5, and Rg6

Scenario:

Contoso has two Azure subscriptions named Sub1 and Sub2.

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

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

User8 city Sidney, Role:None

Note: A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager).

References:

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

NEW QUESTION: 91

You have a hybrid configuration of Azure Active Directory (Azure AD) that has Single Sign-On (SSO) enabled.

You have an Azure SQL Database instance that is configured to support Azure AD authentication.

Database developers must connect to the database instance from the domain joined device and authenticate by using their on-premises Active Directory account.

You need to ensure that developers can connect to the instance by using Microsoft SQL Server Management Studio. The solution must minimize authentication prompts.

Which authentication method should you recommend?

- A. Active Directory - Password
- B. Active Directory - Universal with MFA support
- C. SQL Server Authentication
- D. Active Directory - Integrated

<https://www.fast2test.com/AZ-500-practice-test.html> 18

Valid Fast2test AZ-500 Exam PDF Dumps - New AZ-500 Real Exam Questions

Answer: D (LEAVE A REPLY)

Active Directory - Integrated

Azure Active Directory Authentication is a mechanism of connecting to Microsoft Azure SQL Database by using identities in Azure Active Directory (Azure AD). Use this method for connecting to SQL Database if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

Reference:

<https://docs.microsoft.com/en-us/sql/ssms/f1-help/connect-to-server-database-engine?view=sql-server-2017>

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

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!

Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (460 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 92

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

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

In KeyVault, the following events occur in sequence:

- * Item1 is deleted
- * Administrator enables soft delete
- * Item2 and Policy1 are deleted.

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

NOTE: Each correct selection is worth one point.

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 add a new secret named Item2.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
You can recover Policy1.	<input type="radio"/>	<input checked="" type="radio"/>
You can add a new key named Item1.	<input checked="" type="radio"/>	<input type="radio"/>
You can add a new secret named Item2.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation

NO. Policies cannot be recovered

YES, Item1 is permanently deleted

NO, You cannot use the same name cause Item2 is in Soft-deleted status

<https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview>

NEW QUESTION: 93

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.

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:

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

Explanation

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

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

Reference:

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

NEW QUESTION: 94

Your network contains an on-premises Active Directory domain named corp.contoso.com.

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

You sync all on-premises identities to Azure AD.

You need to prevent users who have a givenName attribute that starts with TEST from being synced to Azure AD. The solution must minimize administrative effort.

What should you use?

- A. Synchronization Rules Editor
- B. Web Service Configuration Tool
- C. Azure Portal
- D. Active Directory Users and Computers

Answer: A (LEAVE A REPLY)

Use the Synchronization Rules Editor and write attribute-based filtering rule.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration>

NEW QUESTION: 95

You are implementing conditional access policies.

You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.

You need to identify the risk level of the following risk events:

Users with leaked credentials

Impossible travel to atypical locations

Sign ins from IP addresses with suspicious activity

Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Levels	Answer Area	
High	Impossible travel to atypical locations:	<input type="text"/>
Low	Users with leaked credentials:	<input type="text"/>
Medium	Sign ins from IP addresses with suspicious activity:	<input type="text"/>

Answer:

Levels	Answer Area	
High	Impossible travel to atypical locations:	Medium
Low	Users with leaked credentials:	High
Medium	Sign ins from IP addresses with suspicious activity:	Low

Explanation:

Azure AD Identity protection can detect six types of suspicious sign-in activities:

Users with leaked credentials

Sign-ins from anonymous IP addresses

Impossible travel to atypical locations

Sign-ins from infected devices

Sign-ins from IP addresses with suspicious activity

Sign-ins from unfamiliar locations

These six types of events are categorized in to 3 levels of risks - High, Medium & Low:

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

References:

<http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/>

NEW QUESTION: 96

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.

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

Answer:

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

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



NEW QUESTION: 97

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

Name	Days to retain deleted vaults	Purge protection	Permission model
KeyVault1	10	Enabled	Azure role-based access control (Azure RBAC)
KeyVault2	15	Disabled	Azure role-based access control (Azure RBAC)

The subscription contains the users shown in the following table.

Name	Role	Assigned to
Admin1	Key Vault Contributor	KeyVault1
Admin2	Key Vault Secrets Officer	KeyVault2
Admin3	Key Vault Administrator	KeyVault1

On June 1, you perform the following actions:

- * Delete a key named key1 from KeyVault1.
- * Delete a secret named secret 1 from KeyVault2.

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

Statements

- | | Yes | No |
|--------------------------------------|-----------------------|-----------------------|
| Admin1 can recover key1 on June 5. | <input type="radio"/> | <input type="radio"/> |
| Admin2 can purge secret1 on June 12. | <input type="radio"/> | <input type="radio"/> |
| Admin3 can recover key1 on June 17. | <input type="radio"/> | <input type="radio"/> |

Answer:

Statements

Yes

No

Admin1 can recover key1 on June 5.

Admin2 can purge secret1 on June 12.

Admin3 can recover key1 on June 17.



NEW QUESTION: 98

You need to delegate the creation of RG2 and the management of permissions for RG1. Which users can perform each task? To answer select the appropriate options in the answer are a.

NOTE: Each correct selection is worth one point

Answer:

NEW QUESTION: 99

Use the following login credentials as needed:

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

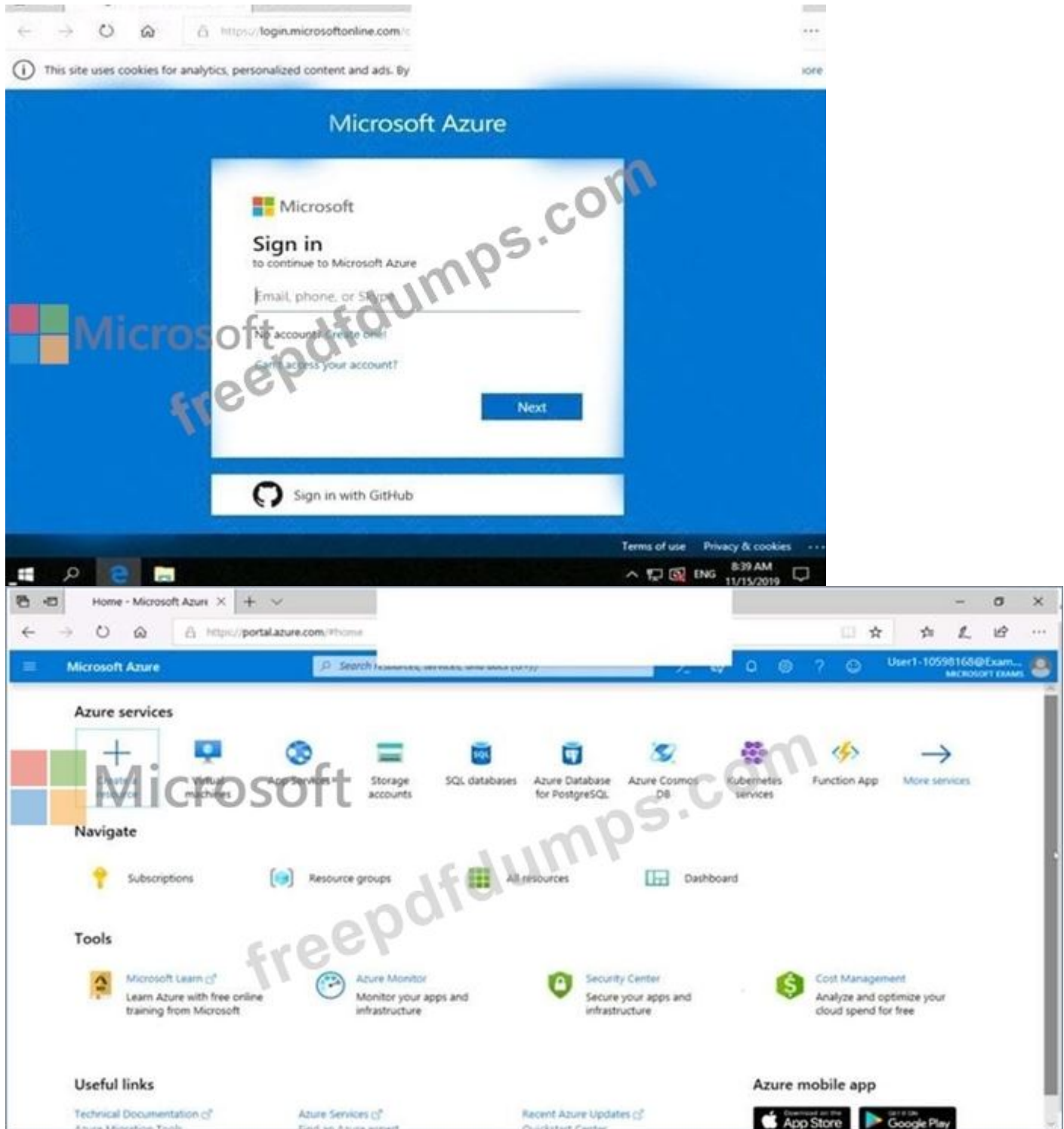
To enter your password, place your cursor in the Enter password box and click on the password below.

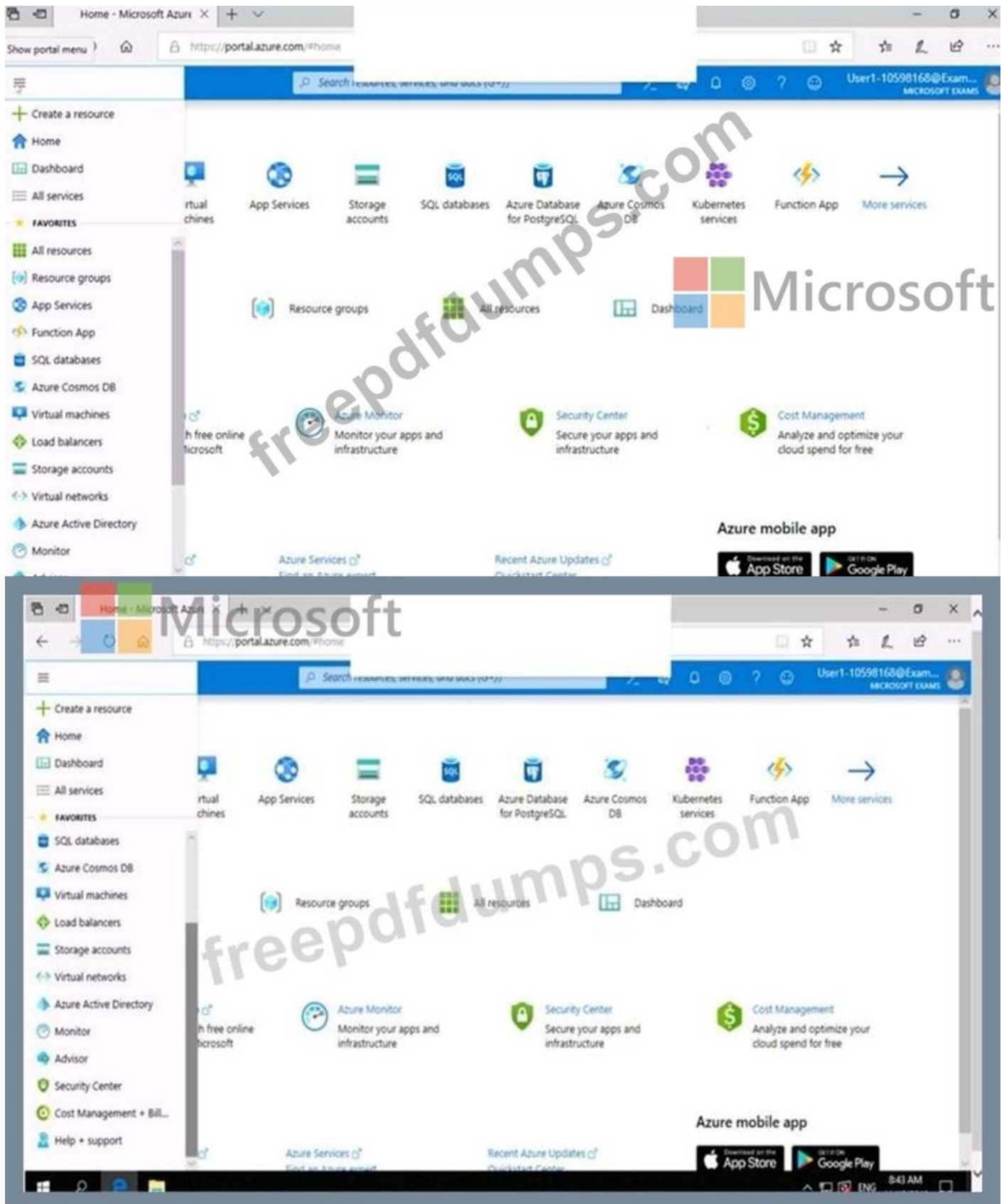
Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168





You need to ensure that only devices connected to a 131.107.0.0/16 subnet can access data in the rg1lod10598168 Azure Storage account.

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

Answer:

See the explanation below.

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>

NEW QUESTION: 100

You have an Azure key vault named Vault1 that stores the resources shown in following table.

Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

Which resources support the creation of a rotation policy?

- A. Key1 and Secret1 only
- B. Key1, Secret1, and Cert1
- C. Key1 and Cert1 only
- D. Secret1 and Cert1 only
- E. Cert1 only
- F. Key1 Only

Answer: A (LEAVE A REPLY)

NEW QUESTION: 101

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

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

The company is sold to a new owner.

The company needs to transfer ownership of Subscription1.

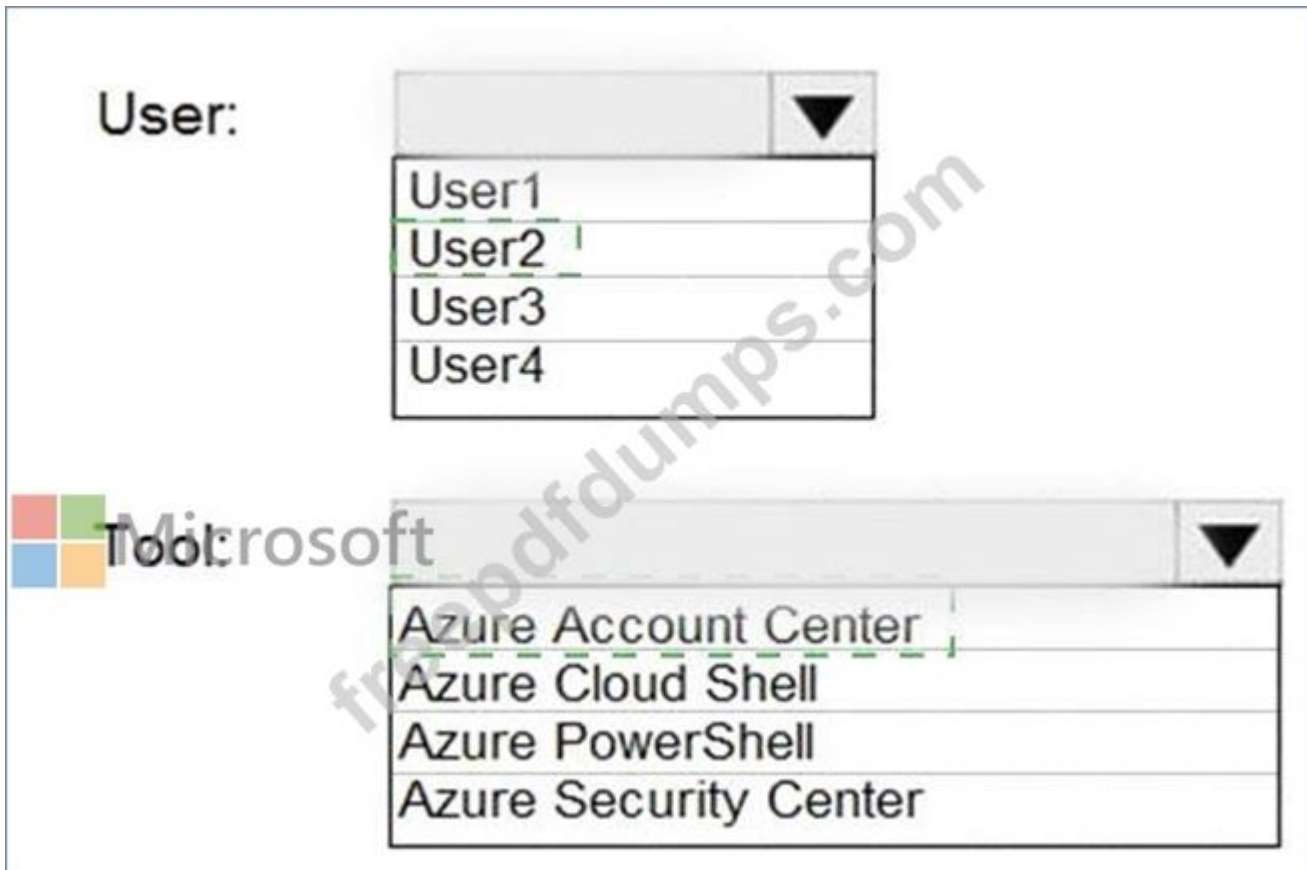
Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

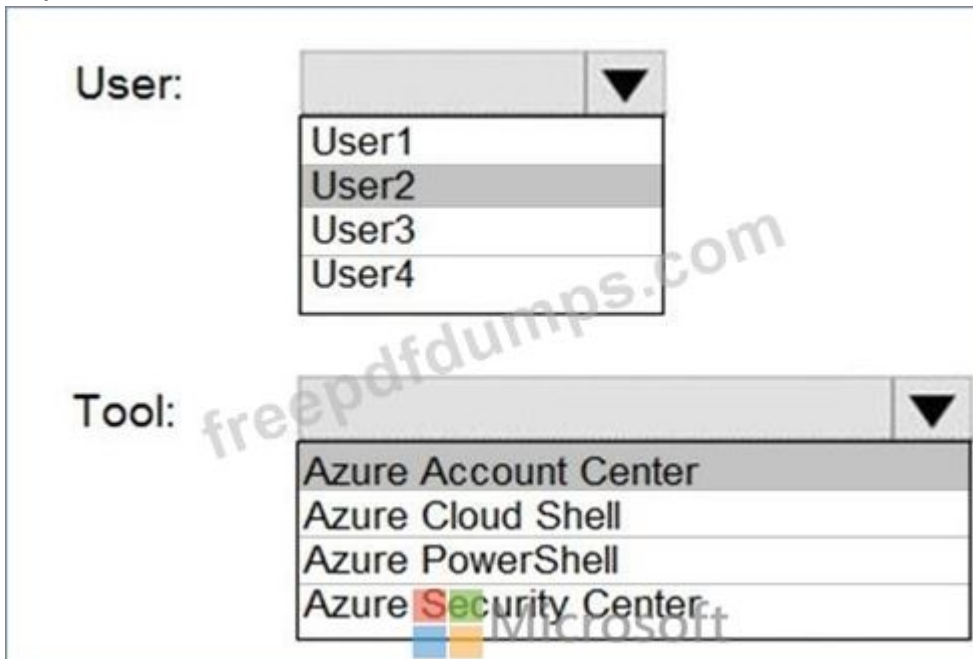
User:

Tool:

Answer:



Explanation



Box 1; User2

Billing Administrator

Select Transfer billing ownership for the subscription that you want to transfer.

Enter the email address of a user who's a billing administrator of the account that will be the new owner for the subscription.

Box 2: Azure Account Center

Azure Account Center can be used.

Reference:

<https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transfer-billing-ownership-of-an-azu>

NEW QUESTION: 102

You have an Azure Sentinel workspace that has the following data connectors:

Azure Active Directory Identity Protection

Common Event Format (CEF)

Azure Firewall

You need to ensure that data is being ingested from each connector.

From the Logs query window, which table should you query for each connector? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Azure Active Directory Identity Protection:

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

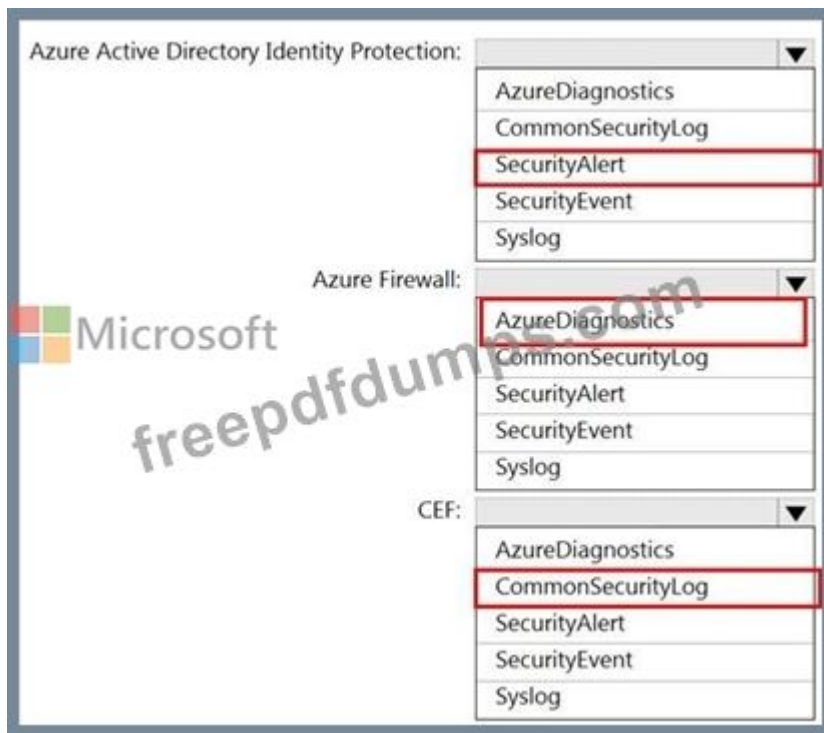
Azure Firewall:

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

CEF:

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

Answer:



NEW QUESTION: 103

You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

The User administrator role is assigned to a user named Admin1.

An external partner has a Microsoft account that uses the user1@outlook.com sign in.

Admin1 attempts to invite the external partner to sign in to the Azure AD tenant and receives the following error message: "Unable to invite user user1@outlook.com Generic authorization exception." You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant.

What should you do?

- A. From the Organizational relationships blade, add an identity provider.
- B. From the Users blade, modify the External collaboration settings.
- C. From the Roles and administrators blade, assign the Security administrator role to Admin1.
- D. From the Custom domain names blade, add a custom domain.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 104

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

Microsoft Azure



Sign in

to continue to Microsoft Azure

No account? [Create one!](#)

Can't access your account?

[Next](#)

 Sign in with GitHub

Home - Microsoft Azure x <https://portal.azure.com/#home>

Microsoft Azure Search

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

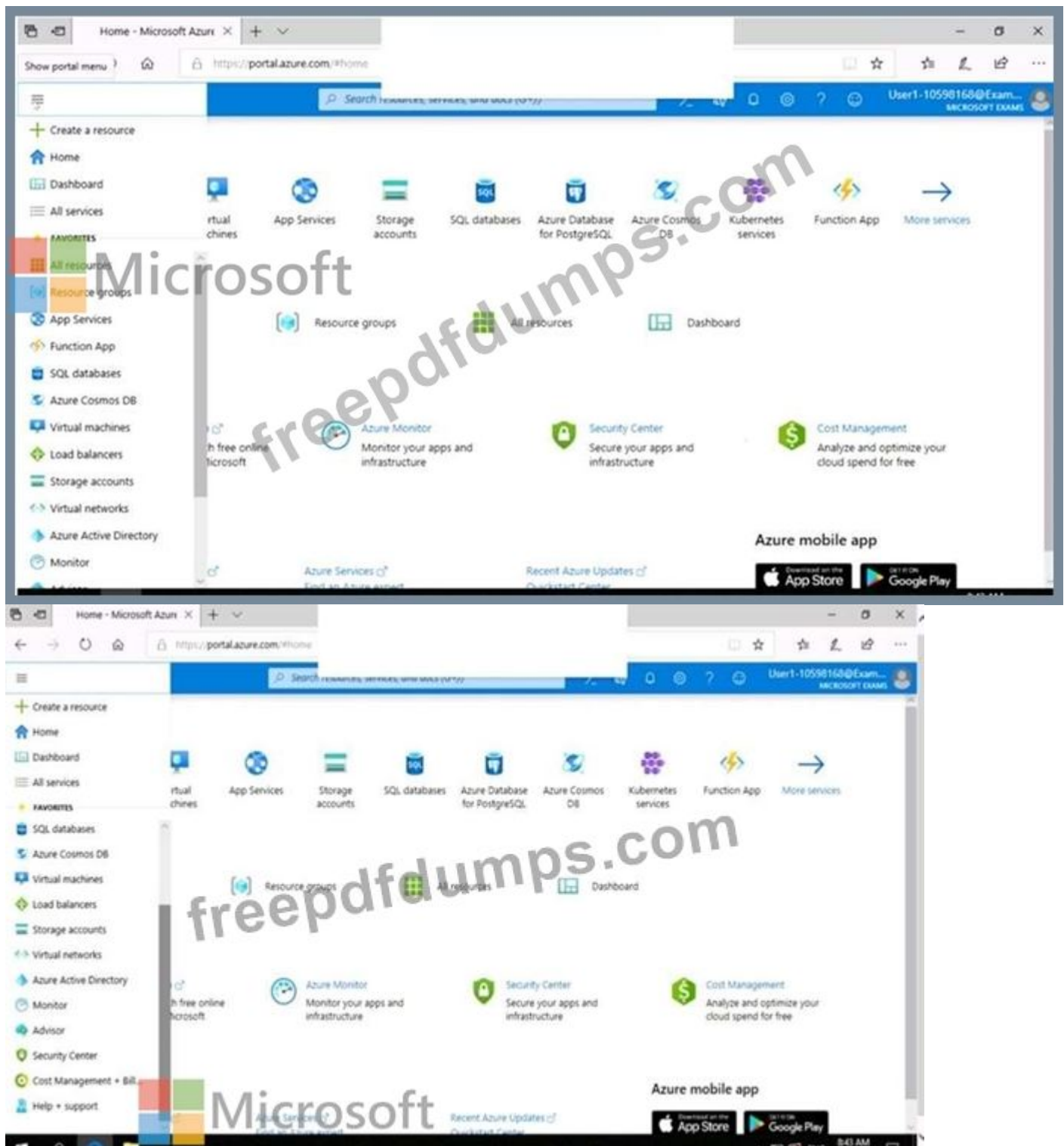
- Microsoft Learn Learn Azure with free online training from Microsoft
- Azure Monitor Monitor your apps and infrastructure
- Security Center Secure your apps and infrastructure
- Cost Management Analyze and optimize your cloud spend for free

Useful links

- Technical Documentation
- Azure Services
- Recent Azure Updates

Azure mobile app

Download on the App Store | GET IT ON Google Play



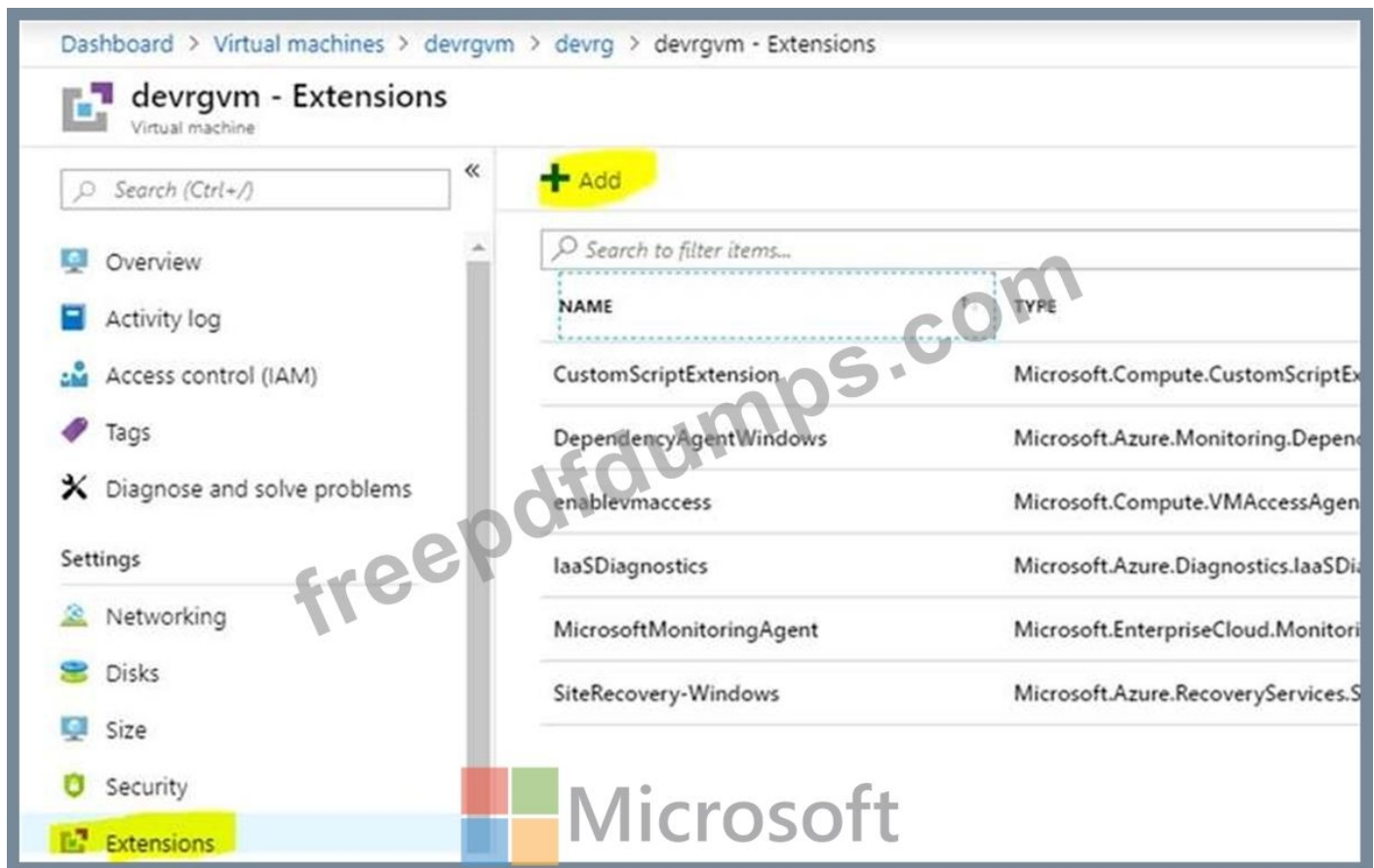
You need to perform a full malware scan every Sunday at 02:00 on a virtual machine named VM1 by using Microsoft Antimalware for Virtual Machines.

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

Answer:

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

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



2. Select the Microsoft Antimalware extension and press Create.

3. Fill the "Install extension" form as desired and press OK.

Scheduled: Enable

Scan type: Full

Scan day: Sunday

Install extension



Excluded files and locations ⓘ

Excluded file extensions ⓘ

Excluded processes ⓘ

Real-time protection ⓘ

Enable Disable

Run a scheduled scan ⓘ

Enable Disable

Scan type ⓘ

Quick Full

Scan day ⓘ

Saturday

Scan time ⓘ

120

Microsoft
freepdfdumps.com

OK

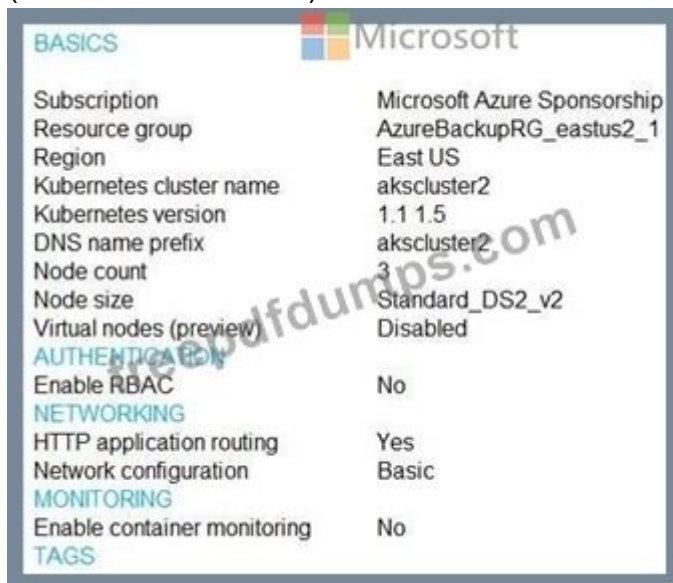
Reference:

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

NEW QUESTION: 105

You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit.

(Click the Exhibit tab.)



Microsoft	
BASIC	
Subscription	Microsoft Azure Sponsorship
Resource group	AzureBackupRG_eastus2_1
Region	East US
Kubernetes cluster name	akscluster2
Kubernetes version	1.1 1.5
DNS name prefix	akscluster2
Node count	3
Node size	Standard_DS2_v2
Virtual nodes (preview)	Disabled
AUTHENTICATION	
Enable RBAC	No
NETWORKING	
HTTP application routing	Yes
Network configuration	Basic
MONITORING	
Enable container monitoring	No
TAGS	

You plan to deploy the cluster to production. You disable HTTP application routing.

You need to implement application routing that will provide reverse proxy and TLS termination for AKS services

by using a single IP address.

What should you do?

- A. Create an AKS Ingress controller.
- B. Install the container network interface (CNI) plug-in.
- C. Create an Azure Standard Load Balancer.
- D. Create an Azure Basic Load Balancer.

Answer: A (LEAVE A REPLY)

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>

NEW QUESTION: 106

You plan to implement an Azure function named Function1 that will create new storage accounts for containerized application instances.

You need to grant Function1 the minimum required privileges to create the storage accounts. The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Assign role to:

- A group account
- A system-assigned managed identity
- A user account
- A user-assigned managed identity

Role assignment to create:

- Built-in role assignment
- Classic administrator role assignment
- Custom role-based access control (RBAC) role assignment

Answer:

Assign role to:

- A group account
- A system-assigned managed identity
- A user account
- A user-assigned managed identity

Role assignment to create:

- Built-in role assignment
- Classic administrator role assignment
- Custom role-based access control (RBAC) role assignment

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/howto-assign-access-portal>

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!
Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (460 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 107

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

Name	Role
Admin1	Global administrator
Admin2	Group administrator
Admin3	User administrator

Contoso.com contains a group naming policy. The policy has a custom blocked word list rule that includes the word Contoso.

Which users can create a group named Contoso Sales in contoso.com? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Users who can create a security group named Contoso Sales:

Microsoft

freepdfdumps.com

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3

Users who can create an Office 365 group named Contoso Sales:

Microsoft

freepdfdumps.com

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3

Answer:

Microsoft

freepdfdumps.com

Users who can create a security group named Contoso Sales:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3

Users who can create an Office 365 group named Contoso Sales:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3

Explanation



Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy>

NEW QUESTION: 108

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.



Answer:

Actions	Answer Area
Create a private link to storage1.	Implement Azure AD Connect.
Enable Active Directory Domain Services (AD DS) authentication on storage1.	Enable Active Directory Domain Services (AD DS) authentication on storage1.
Implement Azure AD Connect.	Assign share-level permissions for share1.
Create a service endpoint to storage1.	
Assign share-level permissions for share1.	

Explanation

Implement Azure AD Connect.

Enable Active Directory Domain Services (AD DS) authentication on storage1.

Assign share-level permissions for share1.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard>

NEW QUESTION: 109

You have an Azure key vault.

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

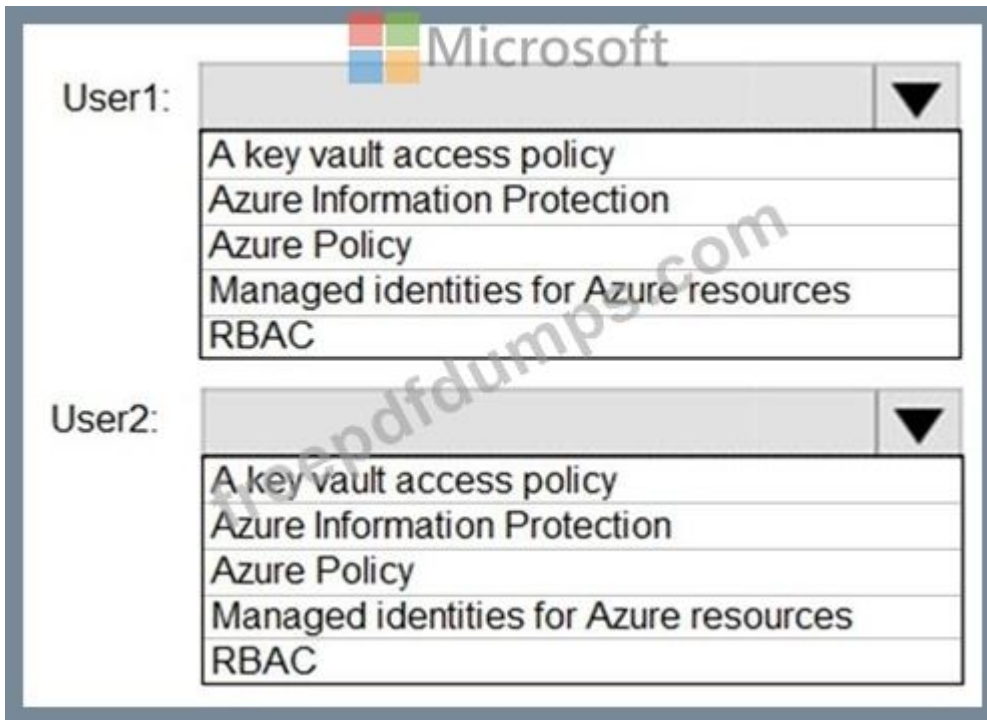
Provide a user named User1 with the ability to set advanced access policies for the key vault.

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

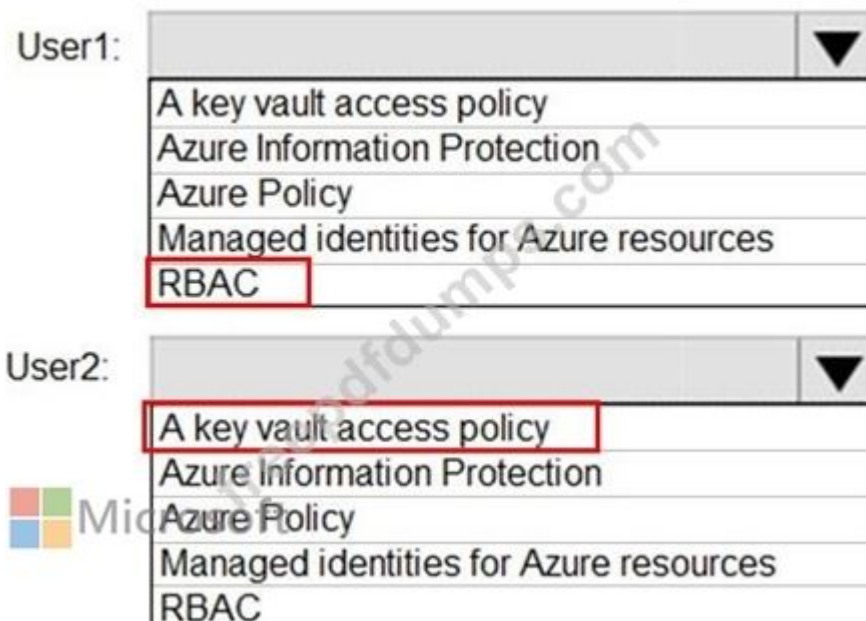
Use the principle of least privilege.

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.



Answer:



Reference:

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

NEW QUESTION: 110

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

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

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

Name	Applies to	Use label	Set the default label
Global	<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.

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

Microsoft

- 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:

Microsoft

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

Answer:

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

Microsoft

- 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].

Microsoft

- allowed
- dropped
- forwarded

Explanation

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

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

No label
Label1 only
Label2 only
Label1 and Label2

Box 1: Label 2 only

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

- * The labels are ordered for evaluation, according to their position that you specify in the policy: The label positioned first has the lowest position (least sensitive) and the label positioned last has the highest position (most sensitive).
- * The most sensitive label is applied.
- * The last sublabel is applied.

Box 2: No Label

Automatic classification applies to Word, Excel, and PowerPoint when documents are saved, and apply to Outlook when emails are sent. Automatic classification does not apply to Microsoft Notepad.

References:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

NEW QUESTION: 111

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.

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:

Create a custom policy definition that has effect set to:

▼
Append
Deny
DeployIfNotExists

Create a policy assignment and modify:

▼
The Create a Managed Identity setting
The exclusion settings
The scope

NEW QUESTION: 112

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

NOTE: Each correct selection is worth one point.

```
set timeframe = 3d;  
securityEvent
```



```
where TimeGenerated > ago(3d)  
where AccountType == 'User' and
```

▼	==4625
ActivityID	
DataType	
EventID	
QuantityUnit	

```
Summarize failed_login_attempts=
```

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

```
latest_failed_login=arg_max(TimeGenerated by AccountType)
```

Answer:

```
let timeframe = 3d;
SecurityEvent
```



```
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and
```

Dropdown menu with value '4625' and options: ActivityID, DataType, EventID (highlighted), QuantityUnit

```
| Summarize failed_login_attempts=
```

Dropdown menu with options: Count(), Countif(), Makeset(), Split() (highlighted)

```
latest_failed_login=arg_max(TimeGenerated by Account
| where failed_login_attempts > 5
```

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples>

NEW QUESTION: 113

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

Name	Type	Resource group	Location
RG1	Resource group	Not applicable	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.

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 [i](#)

Rule syntax Edit

```
(user.accountEnabled - eq true) or (user.usageLocation - eq "US")
```

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

Statements	Yes	No
User1 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:



Statements

Yes No

User1 is a member of Group1 and Group2.

User2 is a member of Group2 only.

Managed1 is a member of Group1 and Group2.

Reference:

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

NEW QUESTION: 114

You have an Azure subscription that contains a user named Admin1 and a resource group named RG1.

In Azure Monitor, you create the alert rules shown in the following table.

Name	Resource	Condition
Rule1	RG1	All security operations
Rule2	RG1	All administrative operations
Rule3	Azure subscription	All security operations by Admin1
Rule4	Azure subscription	All administrative operations by Admin1

Admin1 performs the following actions on RG1:

Adds a virtual network named VNET1

Adds a Delete lock named Lock1

Which rules will trigger an alert as a result of the actions of Admin1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

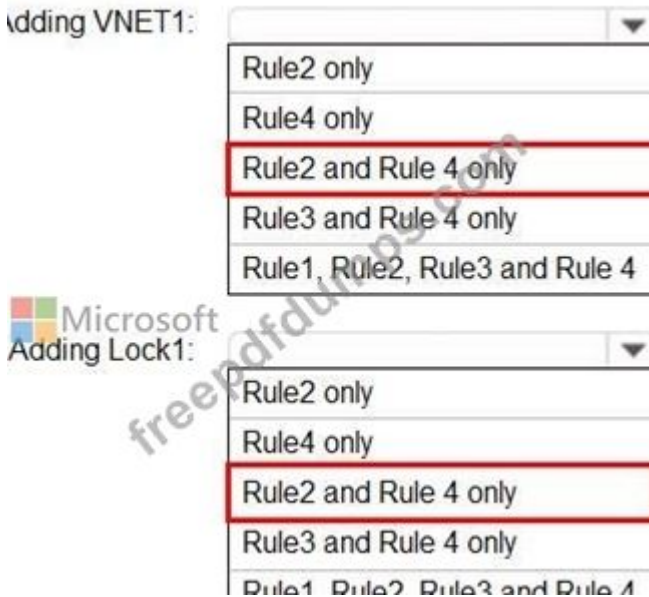
Adding VNET1:

- Rule2 only
- Rule4 only
- Rule2 and Rule 4 only
- Rule3 and Rule 4 only
- Rule1, Rule2, Rule3 and Rule 4

Adding Lock1:

- Rule2 only
- Rule4 only
- Rule2 and Rule 4 only
- Rule3 and Rule 4 only
- Rule1, Rule2, Rule3 and Rule 4

Answer:



NEW QUESTION: 115

You have an Azure subscription.

You create an Azure web app named Contoso1812 that uses an S1 App service plan.

You create a DNS record for www.contoso.com that points to the IP address of Contoso1812.

You need to ensure that users can access Contoso1812 by using the https://www.contoso.com URL.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Turn on the system-assigned managed identity for Contoso1812.
- B. Add a hostname to Contoso1812.
- C. Scale out the App Service plan of Contoso1812.
- D. Add a deployment slot to Contoso1812.
- E. Scale up the App Service plan of Contoso1812.

Answer: B,E (LEAVE A REPLY)

B: You can configure Azure DNS to host a custom domain for your web apps. For example, you can create an Azure web app and have your users access it using either www.contoso.com or contoso.com as a fully qualified domain name (FQDN).

To do this, you have to create three records:

A root "A" record pointing to contoso.com

A root "TXT" record for verification

A "CNAME" record for the www name that points to the A record

E: To map a custom DNS name to a web app, the web app's App Service plan must be a paid tier (Shared, Basic, Standard, Premium or Consumption for Azure Functions). I Scale up the App

Service plan: Select any of the non-free tiers (D1, B1, B2, B3, or any tier in the Production category).

References:

<https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain>


NEW QUESTION: 116

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.

Statements	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:

Statements	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"/>



NEW QUESTION: 117

You are implementing conditional access policies.

You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.

You need to identify the risk level of the following risk events:

Users with leaked credentials

Impossible travel to atypical locations

Sign ins from IP addresses with suspicious activity

Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Levels	Answer Area	
High	Impossible travel to atypical locations:	<input type="text"/>
Low	Users with leaked credentials:	<input type="text"/>
Medium	Sign ins from IP addresses with suspicious activity:	<input type="text"/>

Answer:

Levels	Answer Area	
High	Impossible travel to atypical locations:	Medium
Low	Users with leaked credentials:	High
Medium	Sign ins from IP addresses with suspicious activity:	Medium

NEW QUESTION: 118

You have an Azure subscription named Subscription1 that contains a resource group named RG1 and a user named User1. User1 is assigned the Owner role for RG1.

You create an Azure Blueprints definition named Blueprint1 that includes a resource group named RG2 as shown in the following exhibit.

Edit blueprint		
Basics Artifacts		
Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.		
NAME	ARTIFACT TYPE	PARAMETERS
Subscription		
+ Add artifact...		
RG2	Resource group	2 out of 2 parameters populated
User1 (User1@sk200628outlook.onmicrosoft.com) : Tag Contributor	Role assignment	1 out of 1 parameters populated
+ Add artifact...		

You assign Blueprint1 to Subscription1 by using the following settings:

Lock assignment: Read Only

Managed Identity: System assigned

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

Statements		Yes	No
A locking mode of Read Only will be assigned to RG1.		<input type="radio"/>	<input type="radio"/>
User1 can add tags to RG2.		<input type="radio"/>	<input type="radio"/>
You can remove User1 from the Tag Contributor role for RG2.		<input type="radio"/>	<input type="radio"/>

Answer:

Statements		Yes	No
A locking mode of Read Only will be assigned to RG1.		<input checked="" type="radio"/>	<input type="radio"/>
User1 can add tags to RG2.		<input checked="" type="radio"/>	<input type="radio"/>
You can remove User1 from the Tag Contributor role for RG2.		<input type="radio"/>	<input checked="" type="radio"/>

Reference:

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

NEW QUESTION: 119

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

Name	Location	Connected to
VM1	West US 2	VNET1/Subnet1
VM2	West US 2	VNET1/Subnet1
VM3	West US 2	VNET1/Subnet2
VM4	East US	VNET2/Subnet3
VM5	West US 2	VNET5/Subnet5

Each virtual machine has a single network interface.

You add the network interface of VM1 to an application security group named ASG1.

You need to identify the network interfaces of which virtual machines you can add to ASG1.

What should you identify?

- A. VM2 only
- B. VM2, VM3, VM4, and VM5
- C. VM2, VM3, and VM5 only
- D. Vm2 and Vm3 only

Answer: D ([LEAVE A REPLY](#))

Reference:

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

NEW QUESTION: 120



You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.

You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.

How should you complete the policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

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



```

{
  "if" : {
    "allof" : [
      {
        "field" : "type",
        "equals" : "Microsoft.Compute/virtualMachines"
      }
      {
        "field" : "Microsoft.Compute/imagesSKU",
        "equals" : "2016-Datacenter",
      }
    ]
  },
  "then" : {
    "effect" : "
  },
  "details" : {
    "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
    "roleDefinitionsIds" : [
      "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
    ],
    "name" : "customExtension",
    "deployment" : {
      "properties" : {
        "mode": "incremental",
        "parameters" : {
          "
        },
        "
      }
    }
  }
}

```

Explanation

```

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

```



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>

NEW QUESTION: 121

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains three security groups named Group1, Group2, and Group3 and the users shown in the following table.

Name	Role	Member of
User1	Application administrator	Group1
User2	Application developer	Group2
User3	Cloud application administrator	Group3

Group3 is a member of Group2.

In contoso.com, you register an enterprise application named App1 that has the following settings:

Owners: User1


Users and groups: Group2

You configure the properties of App1 as shown in the following exhibit.

Enabled for users to sign-in? Yes No

Name *

Homepage URL

Logo 

Application ID

Object ID

User assignment required? Yes No

Visible to users Yes No

Notes

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

Statements	Yes	No
User1 has App1 listed on his My Apps portal.	<input type="radio"/>	<input type="radio"/>
User2 has App1 listed on her My Apps portal.	<input type="radio"/>	<input type="radio"/>
User3 has App1 listed on her My Apps portal.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 has App1 listed on his My Apps portal.	<input type="radio"/>	<input type="radio"/>
User2 has App1 listed on her My Apps portal.	<input type="radio"/>	<input type="radio"/>
User3 has App1 listed on her My Apps portal.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam! Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (460 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 122

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.

Microsoft

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:

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

Microsoft

NEW QUESTION: 123

You need to perform the planned changes for OU2 and User1.

Which tools should you use? To answer, drag the appropriate tools to the correct resources. Each tool 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.

Tools

- The Azure portal
- Azure AD Connect
- The Active Directory admin center
- Active Directory Sites and Services
- Active Directory Users and Computers

Answer Area

- OU2: Tool
- User1: Tool

**Answer:**

Tools

- The Azure portal
- Azure AD Connect
- The Active Directory admin center
- Active Directory Sites and Services
- Active Directory Users and Computers

Answer Area

- OU2: Azure AD Connect
- User1: The Azure portal

NEW QUESTION: 124

You are troubleshooting a security issue for an Azure Storage account.

You enable the diagnostic logs for the storage account.

What should you use to retrieve the diagnostics logs?

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

Answer: D (LEAVE A REPLY)

Explanation/Reference:

References:

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

NEW QUESTION: 125

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

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

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

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

You need to identify how Azure Information Protection will label files.

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

NOTE: Each correct selection is worth one point.

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



No label

Label1 only

Label2 only

Label1 and Label2

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

No label

Label1 only

Label2 only

Label1 and Label2

Answer:

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

No label

Label1 only

Label2 only

Label1 and Label2

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

No label

Label1 only

Label2 only

Label1 and Label2

Reference:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

NEW QUESTION: 126

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.

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:

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.

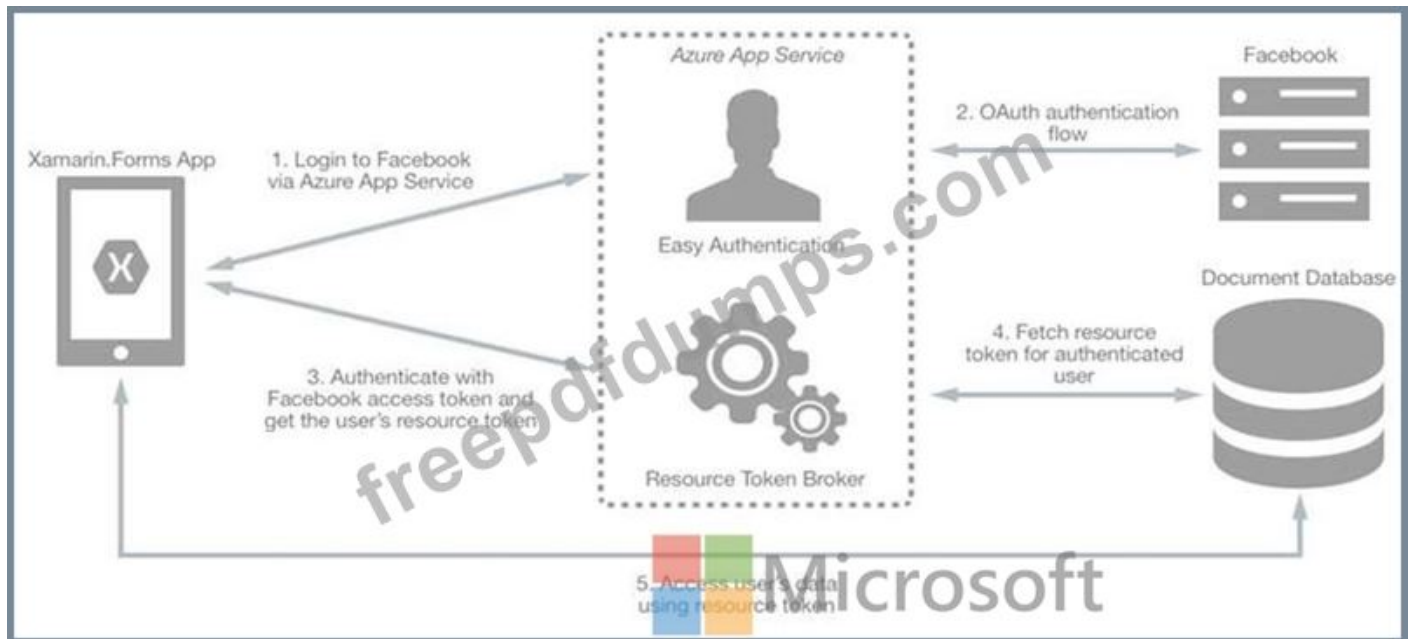
Explanation:

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>

NEW QUESTION: 127

You have an Azure subscription named Subscription1 that contains a resource group named RG1 and a user named User1. User1 is assigned the Owner role for RG1.

You create an Azure Blueprints definition named Blueprint1 that includes a resource group named RG2 as shown in the following exhibit.



You assign Blueprint1 to Subscription1 by using the following settings:

Lock assignment: Read Only

Managed Identity: System assigned

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
A locking mode of Read Only will be assigned to RG1.	<input type="radio"/>	<input type="radio"/>
User1 can add tags to RG2.	<input type="radio"/>	<input type="radio"/>
You can remove User1 from the Tag Contributor role for RG2.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
A locking mode of Read Only will be assigned to RG1.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can add tags to RG2.	<input checked="" type="radio"/>	<input type="radio"/>
You can remove User1 from the Tag Contributor role for RG2.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

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

NEW QUESTION: 128

On Monday, you configure an email notification in Azure Security Center to notify user user1@contoso.com.

On Tuesday, Security Center generates the security alerts shown in the following table.

Time	Description	Severity
01:00	Failed RDP brute force attack	Medium
01:01	Successful RDP brute force attack	High
06:10	Suspicious process executed	High
09:00	Malicious SQL activity	High
11:15	Network communication with a malicious machine detected	Low
13:30	Suspicious process executed	High
14:00	Failed RDP brute force attack	Medium
16:01	Successful RDP brute force attack	High
23:20	Possible outgoing spam activity detected	Low
23:25	Modified system binary discovered in dump file	High
23:30	Malicious SQL activity	High

How many email notifications will user1@contoso.com receive on Tuesday? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Total number of Security Center email notifications about an RDP brute force attack on Tuesday:

▼

1

2

3

4

Total number of Security Center email notifications on Tuesday:

▼

3

4

6

9

11

Answer:

Total number of Security Center email notifications about an RDP brute force attack on Tuesday:

1
2
3
4

Total number of Security Center email notifications on Tuesday:

3
4
6
9
11

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>

NEW QUESTION: 129

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

NOTE: Each correct selection is worth one point.

Microsoft
let timeframe = 3d;
SecurityEvent

| where TimeGenerated > ago(3d)
| where AccountType == 'User' and

	▼	==4625
ActivityID		
DataType		
EventID		
QuantityUnit		

| Summarize failed_login_attempts=

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

latest_failed_login=arg_max(TimeGenerated by Account
| where failed_login_attempts > 5

Answer:

let timeframe = 3d;
SecurityEvent

| where TimeGenerated > ago(3d)
| where AccountType == 'User' and

	▼	==4625
ActivityID		
DataType		
EventID		
QuantityUnit		

| Summarize failed_login_attempts=

	▼
Count(),	!
Countif(),	
Makeset(),	
Split(),	

Microsoft
latest_failed_login=arg_max(TimeGenerated by Account
| where failed_login_attempts > 5

Explanation

```

let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and EventID == 4625

| Summarize failed_login_attempts=
    latest_failed_login=arg_max(TimeGenerated by Account
| where failed_login_attempts > 5

```

The following example identifies user accounts that failed to log in more than five times in the last day, and when they last attempted to log in.

```

let timeframe = 1d;
SecurityEvent
| where TimeGenerated > ago(1d)
| where AccountType == 'User' and EventID == 4625 // 4625 - failed log in
| summarize failed_login_attempts=count(), latest_failed_login=arg_max(TimeGenerated,
Account) by Account
| where failed_login_attempts > 5
| project-away Account1

```

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples>

NEW QUESTION: 130

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

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

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

- * When Azure Sentinel identifies a threat, an incident must be created.
- * A ticket must be logged in the service management platform when an incident is created in Azure Sentinel.

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

NOTE: Each correct selection is worth one point.

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



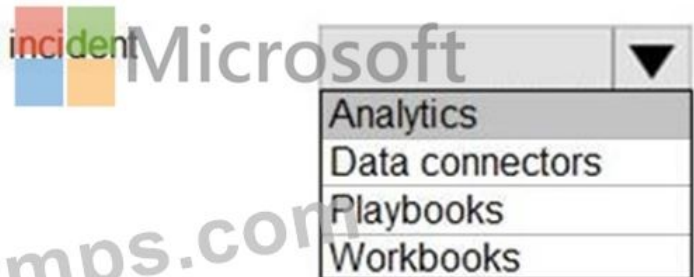
A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:



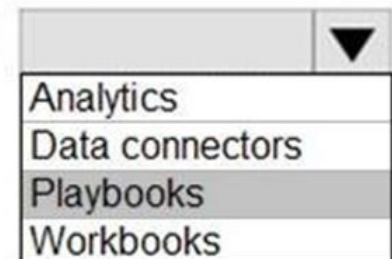
Answer:

Explanation

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



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



Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

NEW QUESTION: 131

You create a new Azure subscription.

You need to ensure that you can create custom alert rules in Azure Security Center.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

<https://www.fast2test.com/AZ-500-practice-test.html> 71

Valid Fast2test AZ-500 Exam PDF Dumps - New AZ-500 Real Exam Questions

A. Onboard Azure Active Directory (Azure AD) Identity Protection.

B. Create an Azure Storage account.

C. Implement Azure Advisor recommendations.

D. Create an Azure Log Analytics workspace.

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

Answer: B,D (LEAVE A REPLY)

D: You need write permission in the workspace that you select to store your custom alert.

References:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-custom-alert>

NEW QUESTION: 132

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

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

An IP address of 10.1.0.4 is assigned to VM5. VM5 does not have a public IP address.

VM5 has just in time (JIT) VM access configured as shown in the following exhibit.

JIT VM access configuration

VM5

+ Add Save X Discard

Configure the ports for which the just-in-time VM access will be applicable

Port	Protocol	Allowed source IPs	IP range	Time range (hours)
3389	Any	Per request	N/A	3 hours

You enable JIT VM access for VM5.

NSG1 has the inbound rules shown in the following exhibit.

Priority	Name	Port	Protocol	Source	Destination	Action
00	SecurityCenter-JITRule_...	3389	Any	Any	10.1.0.4	Allow
000	SecurityCenter-JITRule_341...	3389	Any	Any	10.1.0.4	Deny
001	RDP	3389	TCP	Any	Any	Allow
5000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
5001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
5500	DenyAllInBound	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.

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	<input type="radio"/>	<input type="radio"/>
Remote Desktop access to VM5 is blocked.	<input type="radio"/>	<input type="radio"/>
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	<input type="checkbox"/>	<input type="checkbox"/>
Remote Desktop access to VM5 is blocked.	<input type="checkbox"/>	<input type="checkbox"/>
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	<input type="checkbox"/>	<input type="checkbox"/>

Explanation

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Remote Desktop access to VM5 is blocked.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

NEW QUESTION: 133

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

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

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

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

NOTE: Each correct selection is worth one point.

Update1: ▼

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

Update2: ▼

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

Answer:

Update1: ▼

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

Update2: ▼

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

References:

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

NEW QUESTION: 134

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.

Microsoft
Statements **Yes** **No**

User1 can print File1.

User3 can read File1.

User4 can print File1.

Answer:


Statements **Yes** **No**

User1 can print File1.

User3 can read File1.

User4 can print File1.

Explanation

 Microsoft

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"/>

NEW QUESTION: 135

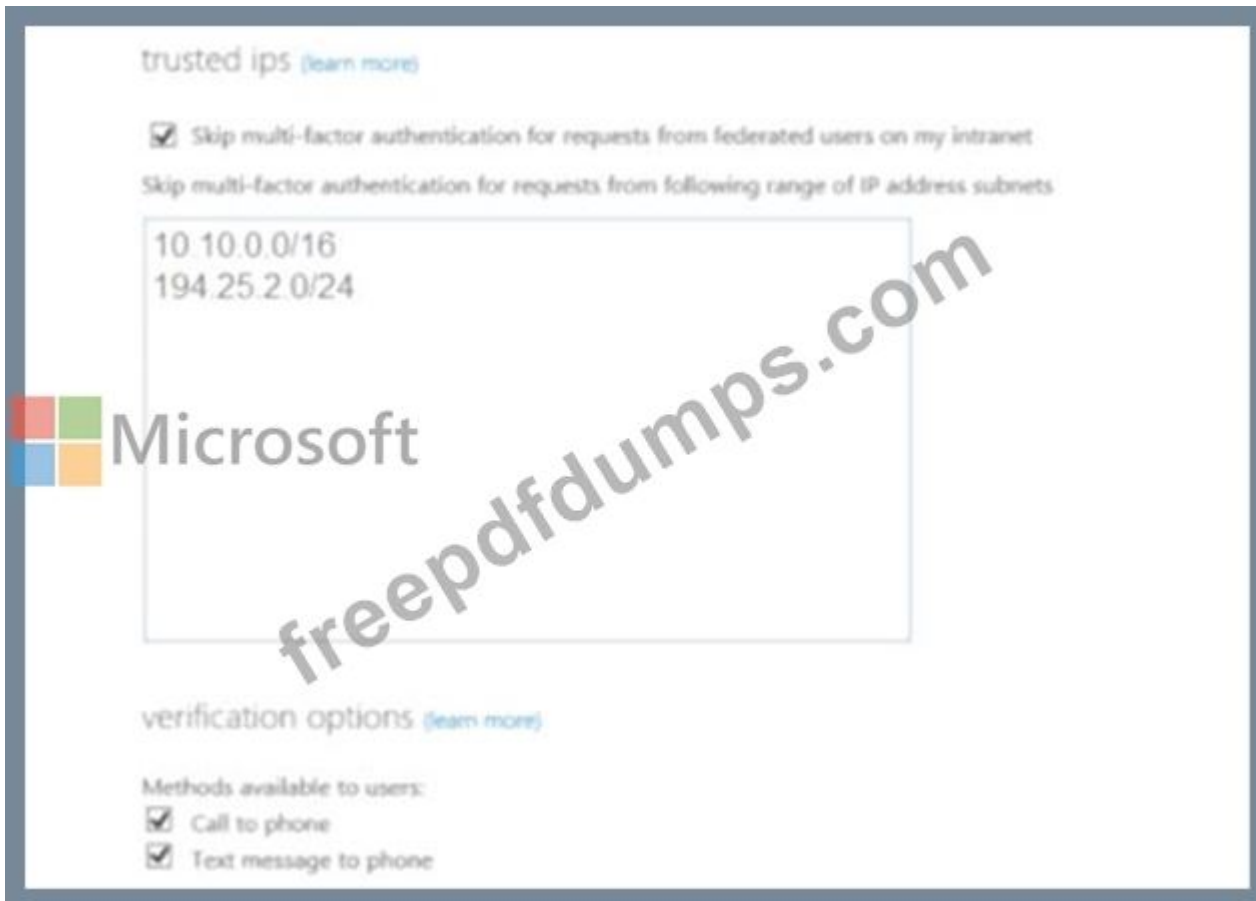
Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.

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

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

Name	Multi-factor authentication (MFA) status
User1	Enabled
User2	Enforced

The MFA service settings are configured as shown in the exhibit. (Click the Exhibit tab.)



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

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	<input type="radio"/>	<input type="radio"/>

Answer:

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

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

NEW QUESTION: 136

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.

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

Answer:

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

Reference:

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

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam! Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (460 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 137

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

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

You create the Azure policies shown in the following table.

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

You create the resource locks shown in the following table.

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

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

NOTE: Each correct selection is worth one point.

Answer Area



Statements

Yes

No

You can start VM1.

You can start VM2.

You can create a virtual machine in RG2.

Answer:

Answer Area

Statements

Yes

No

You can start VM1.

You can start VM2.

You can create a virtual machine in RG2.

Reference:

NEW QUESTION: 138

You plan to use Azure Resource Manager templates to perform multiple deployments of identically configured Azure virtual machines. The password for the administrator account of each deployment is stored as a secret in different Azure key vaults.

You need to identify a method to dynamically construct a resource ID that will designate the key vault containing the appropriate secret during each deployment. The name of the key vault and the name of the secret will be provided as inline parameters.

What should you use to construct the resource ID?

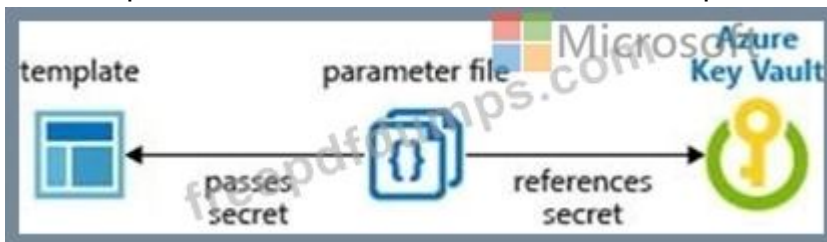
- A. a key vault access policy
- B. a linked template
- C. a parameters file
- D. an automation account

Answer: (SHOW ANSWER)

Section: [none]

Explanation:

You reference the key vault in the parameter file, not the template. The following image shows how the parameter file references the secret and passes that value to the template.



Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-keyvault-parameter> Testlet 1 This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

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

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

To start the case study

To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem

statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

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

Existing Environment

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

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

The tenant contains the groups shown in the following table.

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

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

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to 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://litwareinc.com and http://www.litwareinc.com .
Resource Group1	Resource group	Resource Group1 is a resource group that contains VNet1, VM0, and VM1.
Resource Group2	Resource group	Resource Group2 is a resource group that contains shared IT resources.

Identity and Access Requirements

Azure Security Center is set to the Free tier.

Planned changes

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

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

Litware identifies the following identity and access requirements:

- * All San Francisco users and their devices must be members of Group1.
- * The members of Group2 must be assigned the Contributor role to Resource Group2 by using a permanent eligible assignment.
- * Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

Platform Protection Requirements

Litware identifies the following platform protection requirements:

- * Microsoft Antimalware must be installed on the virtual machines in Resource Group1.
- * The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
- * Azure AD users must be 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 Resource Group1. Role1 must be available only for Resource Group1.

Security Operations Requirements

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

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 minimized.

NEW QUESTION: 139

Use the following login credentials as needed:

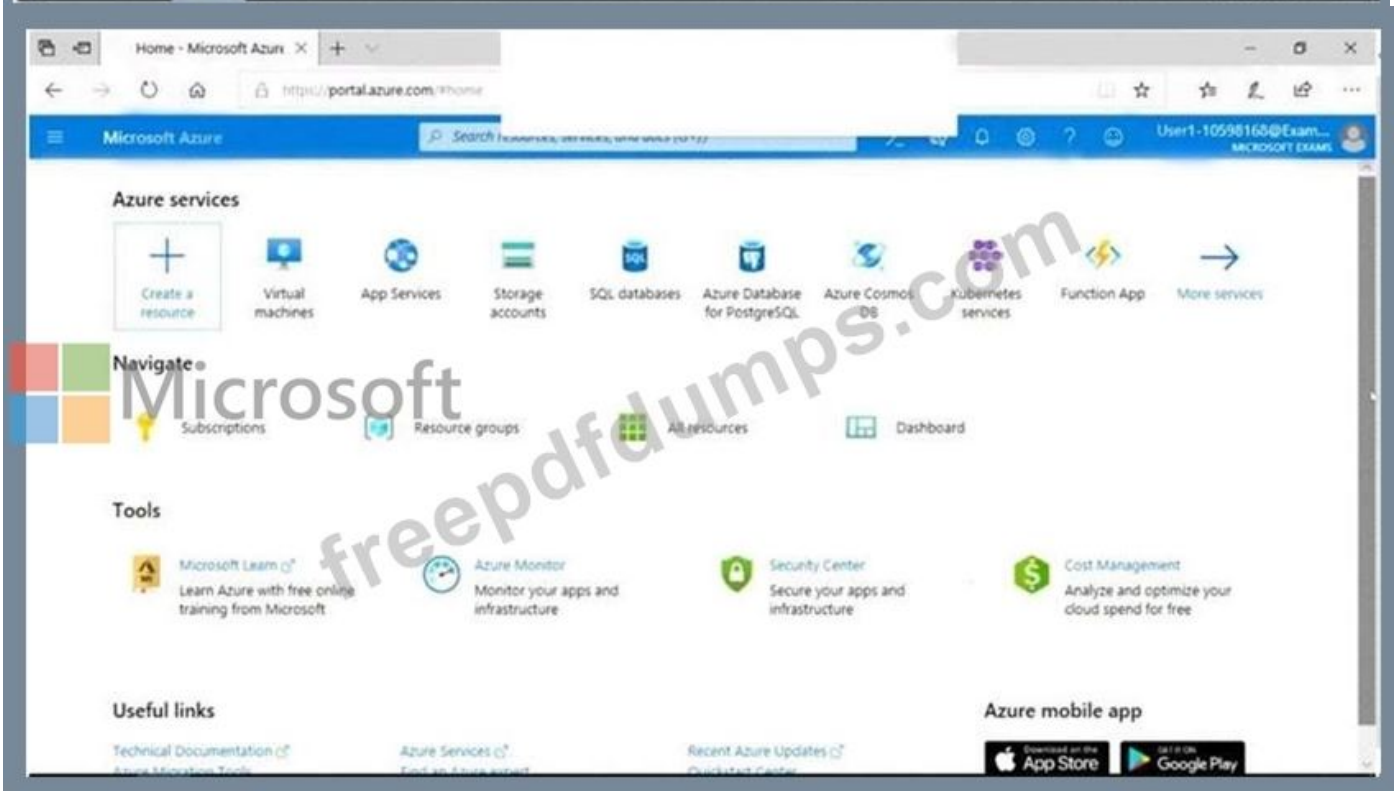
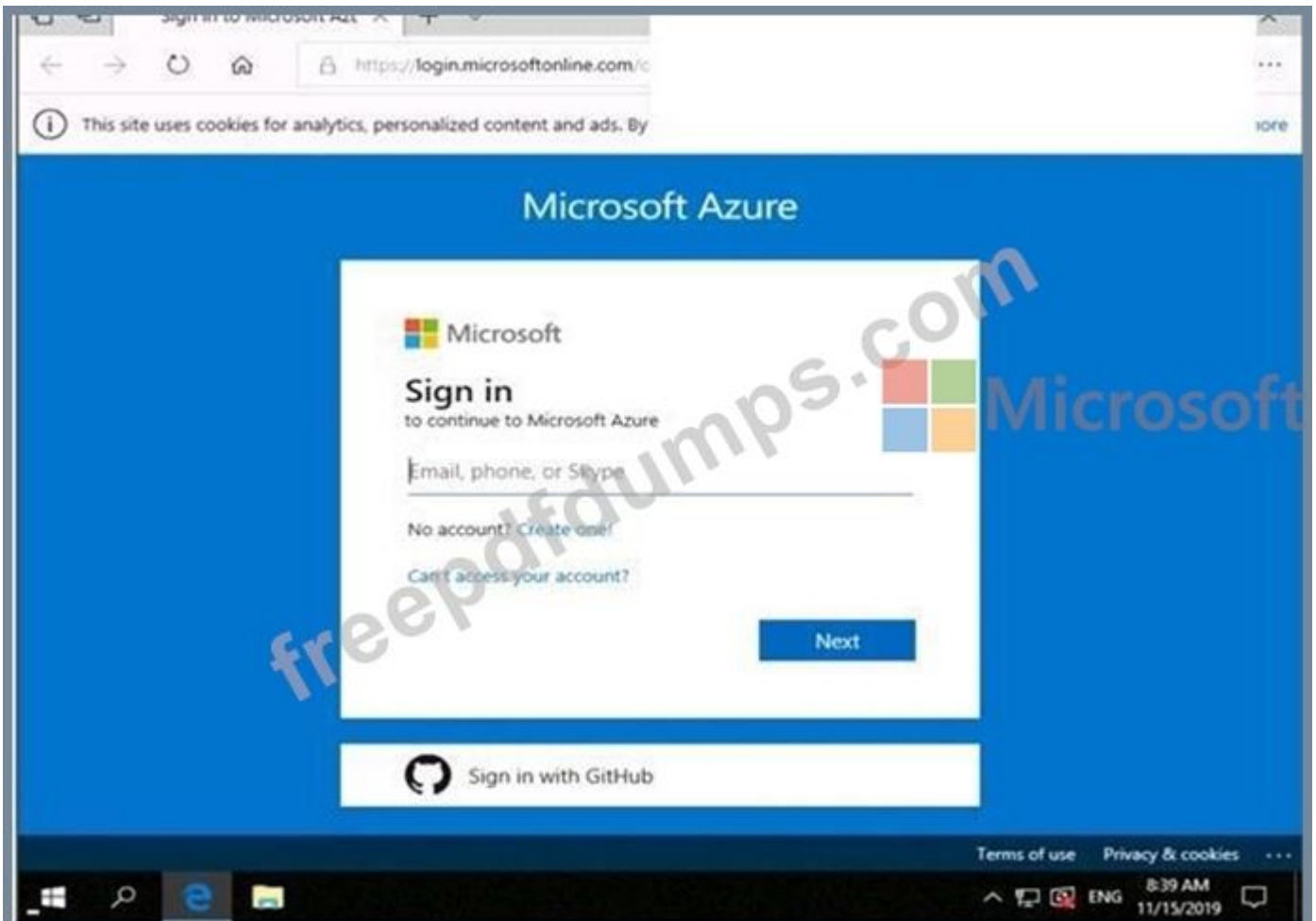
To enter your username, place your cursor in the Sign in box and click on the username below. To enter your password, place your cursor in the Enter password box and click on the password below.

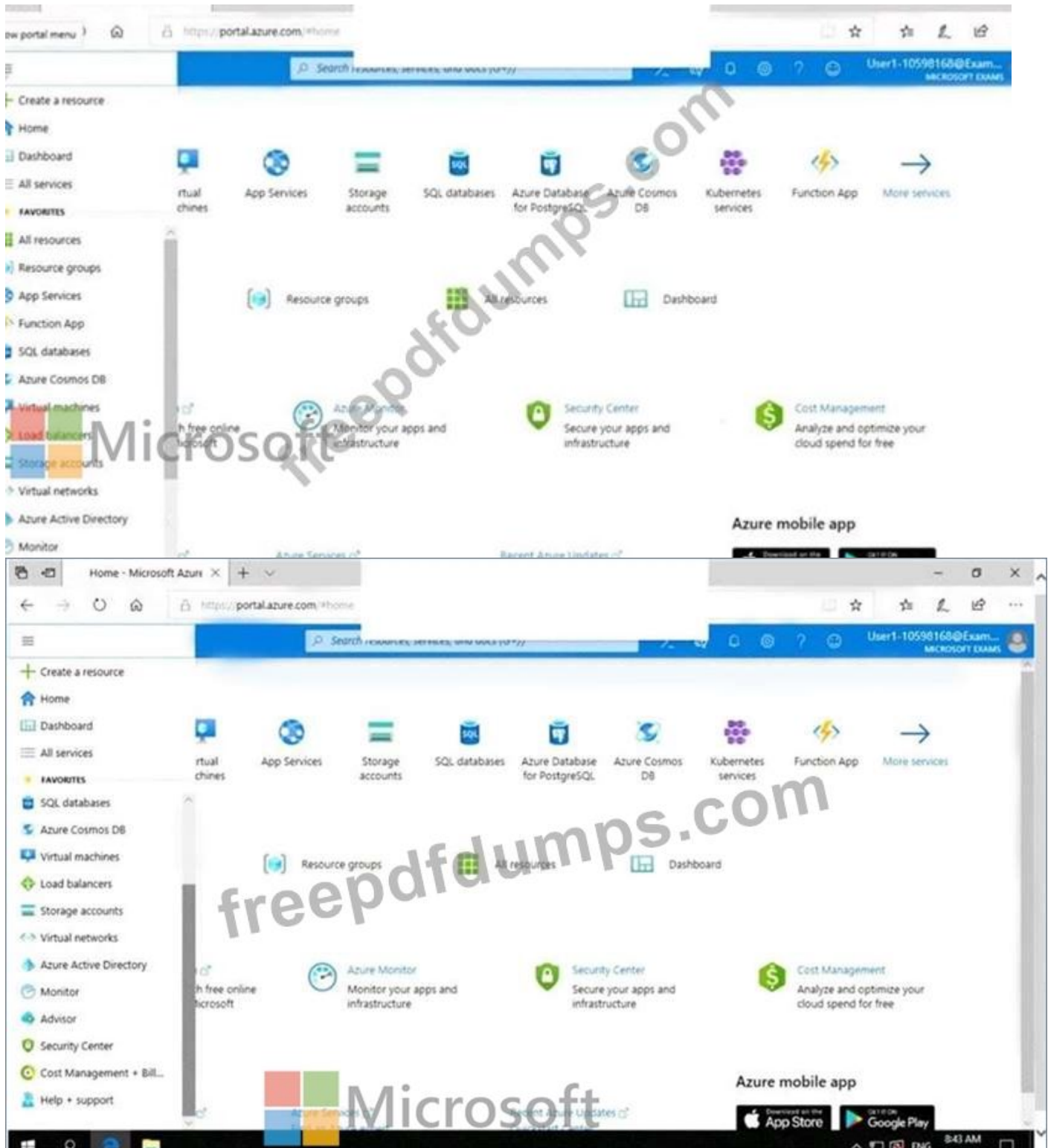
Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168





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

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

Answer:

See the explanation below.

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>

NEW QUESTION: 140

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.

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

Answer:

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



Create a JSON file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

Reference:

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

NEW QUESTION: 141

Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.

You need to configure each subscription to have the same role assignments.

What should you use?

- A. Azure Security Center
- B. Azure Blueprints
- C. Azure AD Privileged Identity Management (PIM)
- D. Azure Policy

Answer: B (LEAVE A REPLY)

Explanation

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

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>

NEW QUESTION: 142

You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role
User1	Global administrator
User2	Security administrator
User3	Security reader
User4	License administrator


Each user is assigned an Azure AD Premium P2 license.

You plan to onboard and configure Azure AD Identity Protection.

Which users can onboard Azure AD Identity Protection, remediate users, and configure policies?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Answer Area  Microsoft

Users who can onboard Azure AD Identity Protection:

Users who can remediate users and configure policies:

Options for onboarding: User1 only, User1 and User2 only, User1, User 2, and User3 only, User1, User 2, User3, and User 4 only

Options for remediation: User1 and User2 only, User1 and User3 only, User1, User 2, and User3 only, User1, User 2, User3, and User 4

Answer:

Answer Area  Microsoft

Users who can onboard Azure AD Identity Protection:

Users who can remediate users and configure policies:

Options for onboarding: User1 only, User1 and User2 only, User1, User 2, and User3 only, User1, User 2, User3, and User 4 only

Options for remediation: User1 and User2 only, User1 and User3 only, User1, User 2, and User3 only, User1, User 2, User3, and User 4

NEW QUESTION: 143

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

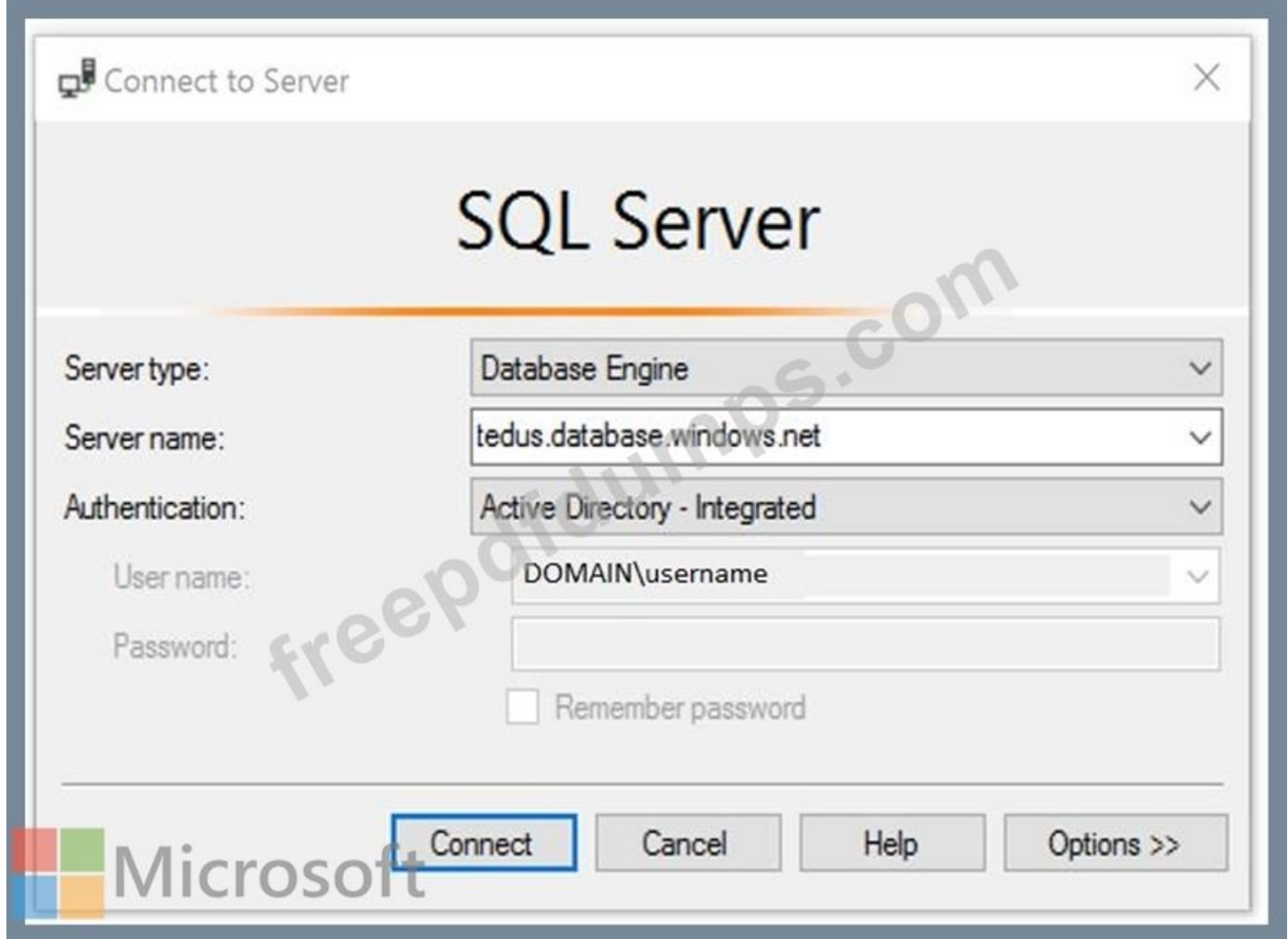
- A. SQL Login
- B. Active Directory - Universal with MFA support
- C. Active Directory - Integrated
- D. Active Directory - Password

Answer: (SHOW ANSWER)

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.) Reference:

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/sql-database/sql-database-aad-authentication-configure.md>

NEW QUESTION: 144

You have a Azure subscription.

You enable Azure Active Directory (Azure AD) Privileged identify (PIM).

Your company's security policy for administrator accounts has the following conditions:

- * The accounts must use multi-factor authentication (MFA).
- * The account must use 20-character complex passwords.
- * The passwords must be changed every 180 days.
- * The account must be managed by using PIM.

You receive alerts about administrator who have not changed their password during the last 90 days.

You need to minimize the number of generated alerts.

Which PIM alert should you modify?

- A. Roles don't require multi-factor authentication for activation.
- B. Administrator aren't using their privileged roles
- C. Roles are being assigned outside of Privileged identity Management
- D. Potential stale accounts in a privileged role.

Answer: ([SHOW ANSWER](#))

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new>

NEW QUESTION: 145

Lab Task

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 3

The developers at your company plan to create a web app named App28681041 and to publish the app to

<https://www.contoso.com>. You need to perform the following tasks:

- * Ensure that App28681041 is registered to Azure AD.
- * Generate a password for App28681041.

Answer:

Check below steps in explanation for Task.

Explanation

To register App28681041 to Azure AD and generate a password for it, you can follow these steps:

In the Azure portal, search for and select Azure Active Directory.

In the left pane, select App registrations.

Select New registration.

In the Register an application pane, enter the following information:

Name: App28681041

Supported account types: Select the appropriate account types for your scenario.

Redirect URI: Leave this field blank.

Select Register.

In the App registrations pane, select the newly created App28681041 application.
In the left pane, select Certificates & secrets.

Select New client secret.

In the Add a client secret pane, enter the following information:

Description: Enter a description for the client secret.

Expires: Select an appropriate expiration date for the client secret.

Select Add.

In the Certificates & secrets pane, copy the value of the newly created client secret.

You can find more information on this topic in the following Microsoft documentation: Quickstart:

Register an application with the Microsoft identity platform.

NEW QUESTION: 146

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

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

```

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

```

```

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

```

```

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

```

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

NOTE: Each correct selection is worth one point.

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


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

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

	▼
allowed	
dropped	
forwarded	

Answer:

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



FTP connections from 1.2.3.4 to 10.0.0.10/32 are [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	

	▼
allowed	
dropped	
forwarded	

Explanation

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	

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:

NEW QUESTION: 147

You have an Azure Container Registry named Registry1.

You add role assignment for Registry1 as shown in the following table.

User	Role
User1	AcrPush
User2	AcrPull
User3	AcrImageSigner
User4	Contributor

Which users can upload images to Registry1 and download images from Registry1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Upload images: ▼

- User1 only
- User1 and User4 only
- User1, User3, and User4
- User1, User2, User3, and User4

Download images: ▼

- User2 only
- User1 and User2 only
- User2 and User4 only
- User1, User2, and User4
- User1, User2, User3, and User4

Answer:



Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles>

NEW QUESTION: 148

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

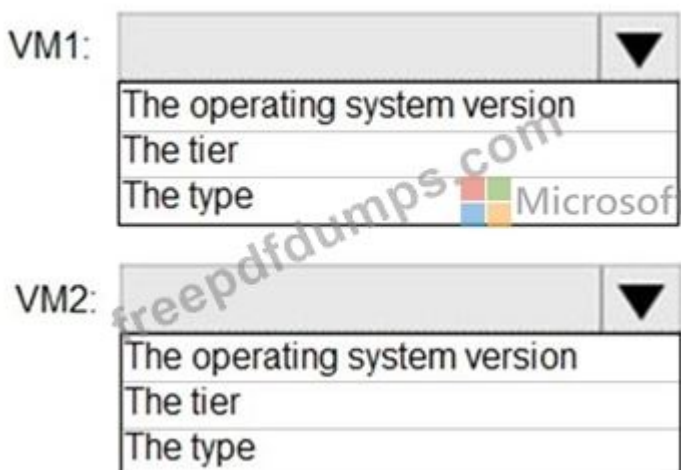
Name	Operating system	Type	Tier
VM1	Windows Server 2008 R2	A3	Basic
VM2	Ubuntu 16.04-DAILY-LTS	L4s	Standard

You deploy and configure an Azure Key vault.

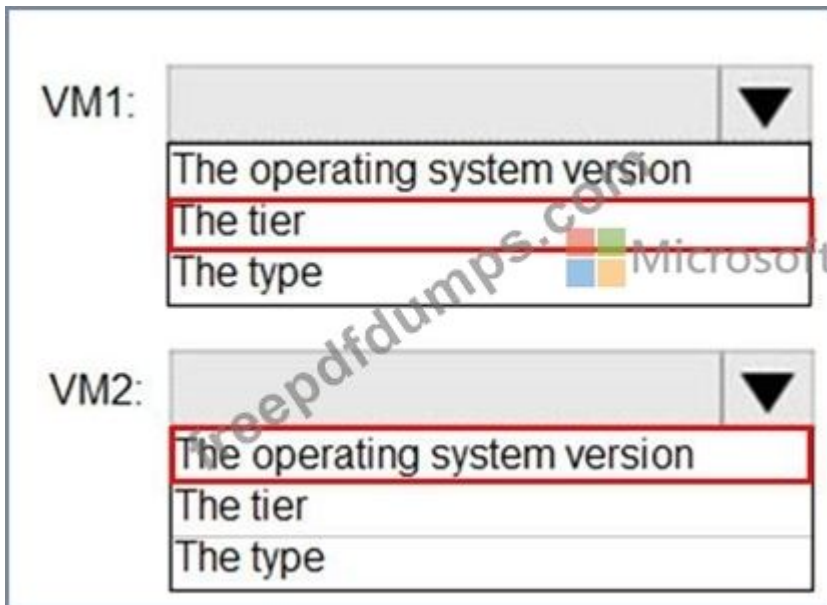
You need to ensure that you can enable Azure Disk Encryption on VM1 and VM2.

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

NOTE: Each correct selection is worth one point.



Answer:



Reference:

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

NEW QUESTION: 149

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

Contoso.com contains a group naming policy. The policy has a custom blocked word list rule that includes the word Contoso.

Which users can create a group named Contoso Sales in contoso.com? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Users who can create a security group named Contoso Sales:

<input type="checkbox"/>	Admin1 only
<input type="checkbox"/>	Admin1 and Admin2 only
<input type="checkbox"/>	Admin1 and Admin3 only
<input type="checkbox"/>	Admin1, Admin2, and Admin3

Users who can create an Office 365 group named Contoso Sales:

<input type="checkbox"/>	Admin1 only
<input type="checkbox"/>	Admin1 and Admin2 only
<input type="checkbox"/>	Admin1 and Admin3 only
<input type="checkbox"/>	Admin1, Admin2, and Admin3

Answer:

Users who can create a security group named Contoso Sales:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3

Users who can create an Office 365 group named Contoso Sales:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3



Explanation



Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy>

NEW QUESTION: 150

You have an Azure Subscription that is linked to an Azure Active Directory (Azure AD). The tenant contains the users shown in the following table.

Name	Role	Member of
User1	Security administrator	Group1
User2	Network Contributor	Group2
User3	Key Vault Contributor	Group1, Group2

You have an Azure key vault named Vault1 that has Purge protection set to Disabled. Vault1 contains the access policies shown in the following table.

Name	Key permission	Secret permission	Certificate permission
Group1	Purge	Purge	Purge
Group2	Select all	Select all	Select all

You create role assignments for Vault1 as shown in the following table.

Name	Role
User1	None
User2	Key Vault Reader
User3	User Access Administrator

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	<input type="radio"/>	<input type="radio"/>
User2 can configure firewalls and virtual networks for Vault1.	<input type="radio"/>	<input type="radio"/>
User3 can add access policies to Vault1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can configure firewalls and virtual networks for Vault1.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can add access policies to Vault1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 151

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.

Actions	Answer Area
From the Azure portal, create an Azure AD administrator for LitwareSQLServer1.	
In SQLDB1, create contained database users.	
Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS).	<input type="button" value="←"/> <input type="button" value="→"/>
In Azure AD, create a system-assigned managed identity.	<input type="button" value="↑"/> <input type="button" value="↓"/>
In Azure AD, create a user-assigned managed identity.	

Answer:

Statements	Yes	No
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	<input type="radio"/>	<input type="radio"/>
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	<input type="radio"/>	<input type="radio"/>
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	<input type="radio"/>	<input type="radio"/>

Explanation

From the Azure portal, create an Azure AD administrator for LitwareSQLServer1 Connect to SQLDB1 by using SSMS In SQLDB1, create contained database users

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

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam! Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (460 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 152

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

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

KV1 stores a secret named Secret1 and a key for a managed storage account named Key1.

You back up Secret1 and Key1.

To which key vaults can you restore each backup? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

You can restore the Secret1 backup to:

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

You can restore the Key1 backup to:

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

Answer:

You can restore the Secret1 backup to:

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

You can restore the Key1 backup to:

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

NEW QUESTION: 153

On Monday, you configure an email notification in Azure Security Center to email notifications to user1@contoso.com.

On Tuesday, Security Center generates the security alerts shown in the following table.

Time	Description	Severity
01:00	Failed RDP brute force attack	Medium
01:01	Successful RDP brute force attack	High
06:10	Suspicious process executed	High
09:00	Malicious SQL activity	High
11:15	Network communication with a malicious machine detected	Low
13:30	Suspicious process executed	High
14:00	Failed RDP brute force attack	Medium
16:01	Successful RDP brute force attack	High
23:20	Possible outgoing spam activity detected	Low
23:25	Modified system binary discovered in dump file	High
23:30	Malicious SQL activity	High

How many email notifications will user1@contoso.com receive on Tuesday? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Total number of Security Center email notifications about an RDP brute force attack on Tuesday:

	▼
1	
2	
3	
4	

Total number of Security Center email notifications on Tuesday:

	▼
3	
4	
6	
9	
11	

Answer:

Total number of Security Center email notifications about an RDP brute force attack on Tuesday:

Microsoft

Total number of Security Center email notifications on Tuesday:

1
2
3
4

3
4
6
9
11

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>

NEW QUESTION: 154

You create an Azure subscription.

You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure AD roles.

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

Actions

Answer Area

Verify your identity by using multi-factor authentication (MFA).

Consent to PIM.

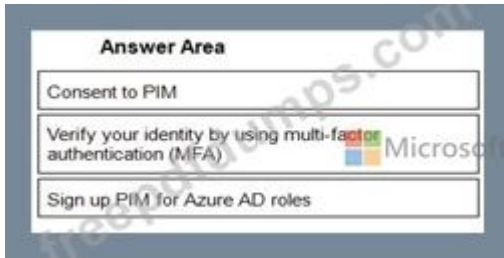
Sign up PIM for Azure AD roles.

Discover privileged roles.

Discover resources.



Answer:



1 - Consent to PIM

2 - Verify your identity by using multi-factor authentication (MFA)

3 - Sign up PIM for Azure AD roles

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started>

NEW QUESTION: 155

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

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

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

Which two services data encryption by using the keys stored in the key vault? Each correct answer present a complete solution.

NOTE: Each correct selection is worth one point.

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

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 156

You create an alert rule that has the following settings:

- * Resource: RG1
- * Condition: All Administrative operations
- * Actions: Action groups configured for this alert rule: ActionGroup1
- * Alert rule name: Alert1

You create an action rule that has the following settings:

- * Scope: VM1
- * Filter criteria: Resource Type = "Virtual Machines"
- * Define on this scope: Suppression

* Suppression config: From now (always)

* Name: ActionRule1

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

Note: Each correct selection is worth one point.

Statements	Yes	No
If you start VM1, an alert is triggered.	<input type="radio"/>	<input type="radio"/>
If you start VM2, an alert is triggered.	<input type="radio"/>	<input type="radio"/>
If you add a tag to RG1, an alert is triggered.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Tools for Container1:

Robocopy.exe
Azure Storage Explorer
File Explorer

Tools for Share1:

Robocopy.exe
Azure Storage Explorer
File Explorer

Explanation

Statements	Yes	No
If you start VM1, an alert is triggered.	<input type="radio"/>	<input checked="" type="radio"/>
If you start VM2, an alert is triggered.	<input checked="" type="radio"/>	<input type="radio"/>
If you add a tag to RG1, an alert is triggered.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1:

The scope for the action rule is set to VM1 and is set to suppress alerts indefinitely.

Box 2:

The scope for the action rule is not set to VM2.

Box 3:

Adding a tag is not an administrative operation.

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log>

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

NEW QUESTION: 157

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

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

From Azure AD Privileged Identity Management (PIM), you configure the settings for the Security Administrator role as shown in the following exhibit.

Assignment

- Allow permanent eligible assignment
- Expire eligible assignments after: 3 Months
- Allow permanent active assignment
- Expire active assignments after: 1 Month
- Require Azure Multi-Factor Authentication on active assignment
- Require justification on active assignment

Activation

Activation maximum duration (hours): 5

- Require Azure Multi-Factor Authentication on activation
- Require justification on activation
- Require ticket information on activation
- Require approval to activate

Select approvers: No member or group selected

From PIM, you assign the Security Administrator role to the following groups:

Group1: Active assignment type, permanently assigned

Group2: Eligible assignment type, permanently eligible

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	<input type="radio"/>	<input type="radio"/>
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	<input type="radio"/>	<input type="radio"/>
User3 can activate the Security Administrator role.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can activate the Security Administrator role.	<input checked="" type="radio"/>	<input type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

<https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings>

NEW QUESTION: 158

You have an Azure subscription that has a managed identity named identity and is linked to an Azure Active Directory (Azure AD) tenant. The tenant contains the resources shown in the following table.

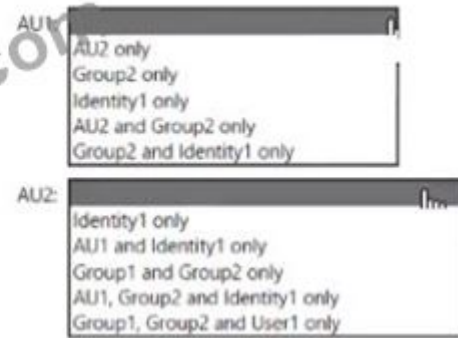
Which resources can be added to AU1 and AU2? To answer, select the appropriate options in the answer area.

Name	Type	Assigned object
AU1	Administrative unit	User1, Group1
AU2	Administrative unit	None
User1	User	Not applicable
Group1	Security group	Not applicable
Group2	Microsoft 365 group	Not applicable

Which resources can be added to AU1 and AU2? To answer, select the appropriate options in the

answer area.

NOTE: Each correct selection is worth one point.



Answer:

Answer Area



NEW QUESTION: 159

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

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

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

Which virtual machines can be enrolled in Analytics1?

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

Answer: A (LEAVE A REPLY)

Note: Create a workspace

* In the Azure portal, click All services. In the list of resources, type Log Analytics. As you begin typing, the list

filters based on your input. Select Log Analytics.

* Click Create, and then select choices for the following items:

Provide a name for the new Log Analytics workspace, such as DefaultLAWorkspace. OMS workspaces are now referred to as Log Analytics workspaces.

Select a Subscription to link to by selecting from the drop-down list if the default selected is not appropriate.

For Resource Group, select an existing resource group that contains one or more Azure virtual machines.

Select the Location your VMs are deployed to. For additional information, see which regions Log Analytics is available in.

Incorrect Answers:

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

D: VM4 is a different resource group.

References:

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

NEW QUESTION: 160

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

What should you do?

A. Add a membership rule to Group1.

B. Delete Group1. Create a new group named Group1 that has a membership type of Office 365. Add users and devices to the group.

C. Modify the membership rule of Group1.

D. Change the membership type of Group1 to Assigned. Create two groups that have dynamic memberships. Add the new groups to Group1.

Answer: (SHOW ANSWER)

Explanation

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

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

The tenant currently contain this group:

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

References:

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

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

NEW QUESTION: 161

You have an Azure AD tenant that contains 500 users and an administrative unit named AU1. From the Azure Active Directory admin center, you plan to add the users to AU1 by using Bulk add members.

You need to create and upload a file for the bulk add.

What should you include in the file?

- A. Only the user principal name (UPN) and display name of each user
- B. only the display name of each user
- C. only the object identifier of each user
- D. only the user principal name (UPN) and object identifier of each user
- E. only the user principal name (UPN) of each user

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 162

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

NOTE: Each correct selection is worth one point.

```
set timeframe = 3d;
securityEvent
  where TimeGenerated > ago(3d)
  where AccountType == 'User' and
```

Microsoft

ActivityID
DataType
EventID
QuantityUnit

Summary failed_login_attempts=

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

```
latest_failed_login=arg_max(TimeGenerated by AccountType)
where failed_login_attempts > 5
```

Answer:

```

let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and EventID == 4625

| Summarize failed_login_attempts=
    Count(),
    latest_failed_login=arg_max(TimeGenerated by Account)
| where failed_login_attempts > 5

project-away Account1

```

Explanation:

The following example identifies user accounts that failed to log in more than five times in the last day, and when they last attempted to log in.

```
let timeframe = 1d;
```

```
SecurityEvent
```

```
| where TimeGenerated > ago(1d)
```

```
| where AccountType == 'User' and EventID == 4625 // 4625 - failed log in
```

```
| summarize failed_login_attempts=count(), latest_failed_login=arg_max(TimeGenerated,
Account) by Account
```

```
| where failed_login_attempts > 5
```

```
| project-away Account1
```

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples>

NEW QUESTION: 163

You have an Azure subscription.

You need to create and deploy an Azure policy that meets the following requirements:

When a new virtual machine is deployed, automatically install a custom security extension.

Trigger an autogenerated remediation task for non-compliant virtual machines to install the extension.

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

NOTE: Each correct selection is worth one point.

Definition effect:

Append
DeployIfNotExists
EnforceOPAConstraint
EnforceRegoPolicy
Modify

Assignment remediation task:

A managed identity that has the Contributor role
A managed identity that has the User Access Administrator role
A service principal that has the Contributor role
A service principal that has the User Access Administrator role

Answer:

Definition effect:

Append
DeployIfNotExists
EnforceOPAConstraint
EnforceRegoPolicy
Modify

Assignment remediation task:

A managed identity that has the Contributor role
A managed identity that has the User Access Administrator role
A service principal that has the Contributor role
A service principal that has the User Access Administrator role

Explanation

Definition effect:

Append
DeployIfNotExists
EnforceOPAConstraint
EnforceRegoPolicy
Modify

Assignment remediation task:

A managed identity that has the Contributor role
A managed identity that has the User Access Administrator role
A service principal that has the Contributor role
A service principal that has the User Access Administrator role

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources>

NEW QUESTION: 164

You network contains an on-premises Active Directory domain that syncs to an Azure Active

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

Name	Source
User1	Azure AD
User2	Azure AD
User3	On-premises Active Directory

The tenant contains the groups shown in the following table.

Name	Members
Group1	User1, User2, User3
Group2	User2

You configure a multi-factor authentication (MFA) registration policy that and the following settings:

* Assignments:

* Include: Group1

* Exclude Group2

Controls: Require Azure MFA registration

Enforce Policy: On

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

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>

Answer:

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

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

Explanation

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user's next Azure AD authentication.	<input type="radio"/>	<input checked="" type="radio"/>
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION: 165

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.

Answer:

see the task answer with step by step below:

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.

NEW QUESTION: 166


You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.

You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.

How should you complete the policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

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



The screenshot shows a policy configuration interface. The 'effect' dropdown menu is open, showing options: Append, Deny, and DeployIfNotExists. The 'existenceCondition' dropdown menu is also open, showing options: existenceCondition, resources, and template. The background features a Microsoft logo and a watermark 'freepdfdumps.com'.

Answer:

```

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

```



Reference:

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

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam! Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (460 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 167

You need to meet the technical requirements for the finance department users.

Which CAPolicy1 settings should you modify?

- A. Cloud apps or actions
- B. Conditions
- C. Grant
- D. Session

Answer: D (LEAVE A REPLY)

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional->

access-session-lifetime

NEW QUESTION: 168

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.

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

Answer:

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

Explanation

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

NEW QUESTION: 169

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

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

What should you create?

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

Answer: B ([LEAVE A REPLY](#))

Reference:

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

NEW QUESTION: 170

You are implementing conditional access policies.

You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.

You need to identify the risk level of the following risk events:

Users with leaked credentials

Impossible travel to atypical locations

Sign ins from IP addresses with suspicious activity

Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Levels	Answer Area
High	Impossible travel to atypical locations: <input type="text"/>
Low	Users with leaked credentials: <input type="text"/>
Medium	Sign ins from IP addresses with suspicious activity: <input type="text"/>

Answer:

Levels	Answer Area
High	Impossible travel to atypical locations: Medium
Low	Users with leaked credentials: High
Medium	Sign ins from IP addresses with suspicious activity: Medium

Explanation

Medium

High

Medium

Refer

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events#sign-ins-from-ip>

NEW QUESTION: 171

You have an Azure subscription that contains an Azure key vault. The role assignments for the key vault are shown in the following exhibit.

```
[
  {
    "RoleAssignmentId": "3336fcfb-33d8-4c8a-85b6-d8edd964762b",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa",
    "DisplayName": "User1",
    "SignInName": "User1@contoso.com",
    "RoleDefinitionName": "Owner",
    ...
  },
  {
    "RoleAssignmentId": "9d080a14-246e-4580-8b8b-077bfec22f7c",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
    "DisplayName": "User2",
    "SignInName": "User2@contoso.com",
    "RoleDefinitionName": "Key Vault Crypto Officer",
    "RoleAssignmentId": "4",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
    "DisplayName": "User3",
    "SignInName": "User3@contoso.com",
    "RoleDefinitionName": "Key Vault Secrets Officer",
    ...
  },
  {
    "RoleAssignmentId": "f1e46302-c5d0-4519-9ee7-128594eea97c",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG3/providers/Microsoft.KeyVault/vaults/KeyVault1/keys/Key1",
    "DisplayName": "User4",
    "SignInName": "User4@contoso.com",
    "RoleDefinitionName": "Key Vault Administrator",
    ...
  }
]
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Answer Area

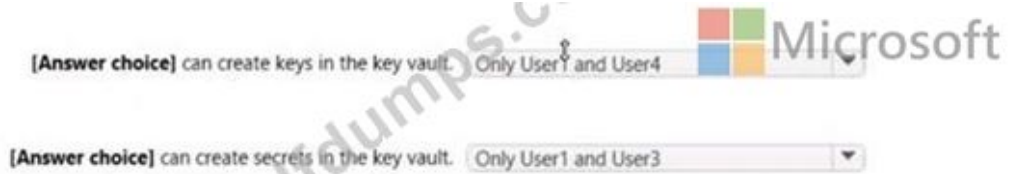
[Answer choice] can create keys in the key vault.

[Answer choice] can create secrets in the key vault.

Answer:

Answer is as image below.

Answer Area



NEW QUESTION: 172

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

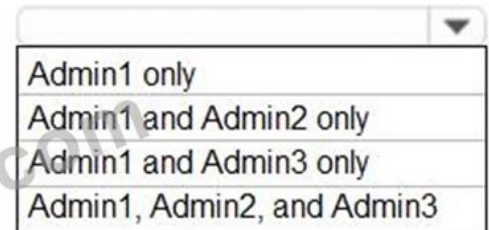
Name	Role
Admin1	Global administrator
Admin2	Group administrator
Admin3	User administrator

Contoso.com contains a group naming policy. The policy has a custom blocked word list rule that includes the word Contoso.

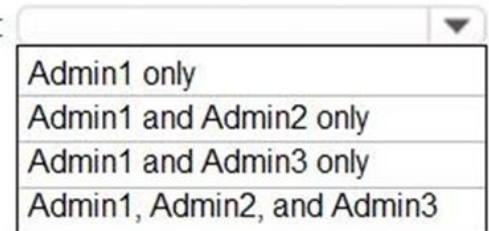
Which users can create a group named Contoso Sales in contoso.com? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Users who can create a security group named Contoso Sales:



Users who can create an Office 365 group named Contoso Sales:



Answer:



Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy>

NEW QUESTION: 173

You create an alert rule that has the following settings:

Resource: RG1

Condition: All Administrative operations

Actions: Action groups configured for this alert rule: ActionGroup1

Alert rule name: Alert1

You create an action rule that has the following settings:

Scope: VM1

Filter criteria: Resource Type = "Virtual Machines"

Define on this scope: Suppression

Suppression config: From now (always)

Name: ActionRule1

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

Note: Each correct selection is worth one point.

Statements	Yes	No
If you start VM1, an alert is triggered.	<input type="radio"/>	<input type="radio"/>
If you start VM2, an alert is triggered.	<input type="radio"/>	<input type="radio"/>
If you add a tag to RG1, an alert is triggered.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
If you start VM1, an alert is triggered.	<input type="radio"/>	<input checked="" type="radio"/>
If you start VM2, an alert is triggered.	<input checked="" type="radio"/>	<input type="radio"/>
If you add a tag to RG1, an alert is triggered.	<input type="radio"/>	<input checked="" type="radio"/>

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log>

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-action-rules

NEW QUESTION: 174

Use the following login credentials as needed:

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

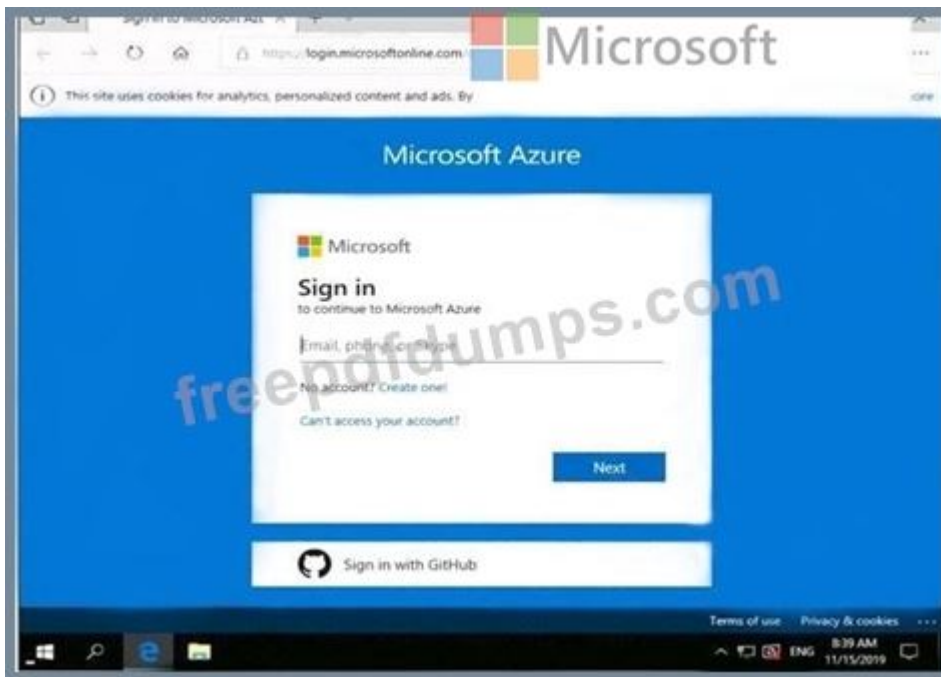
To enter your password, place your cursor in the Enter password box and click on the password below.

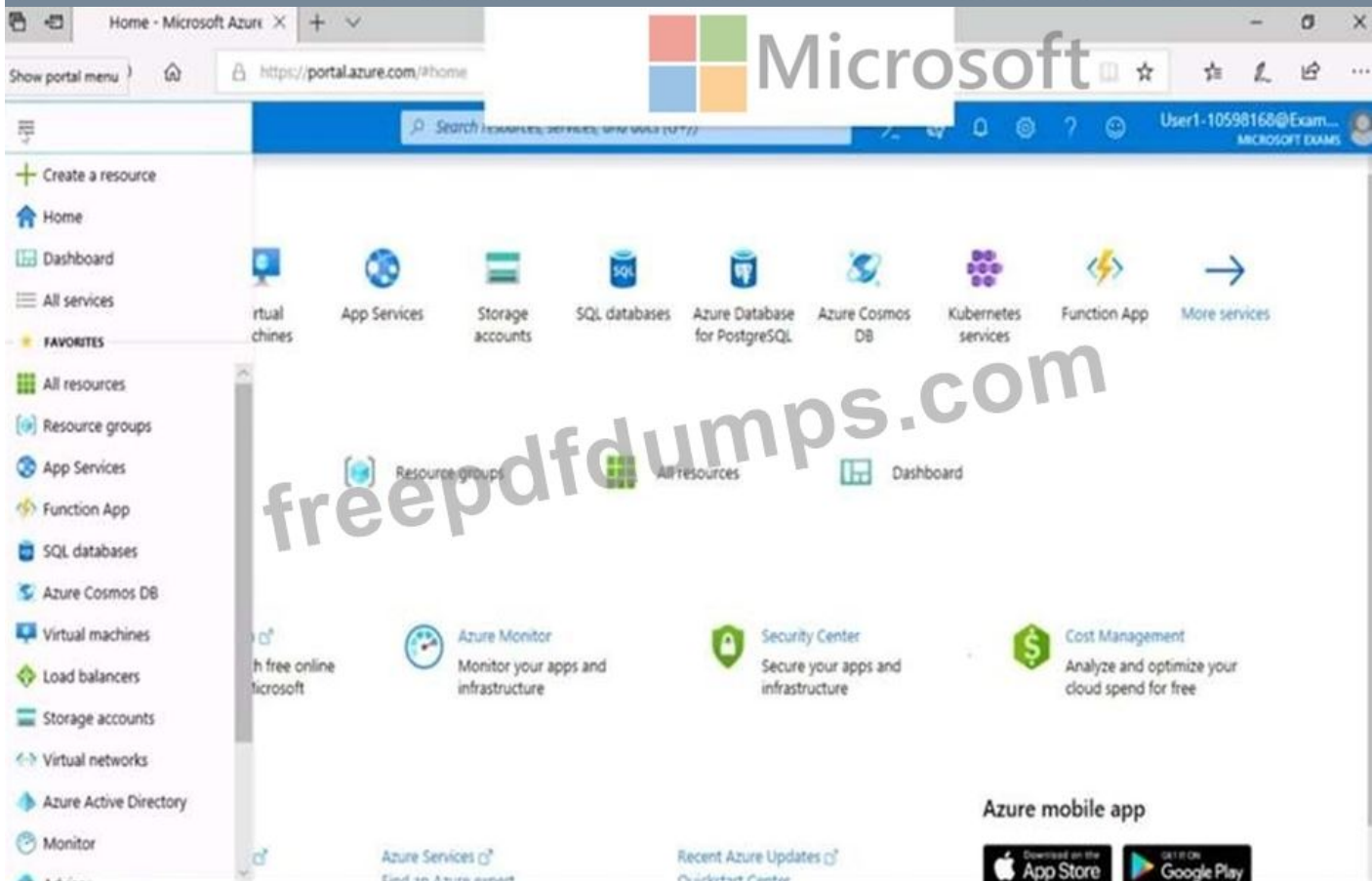
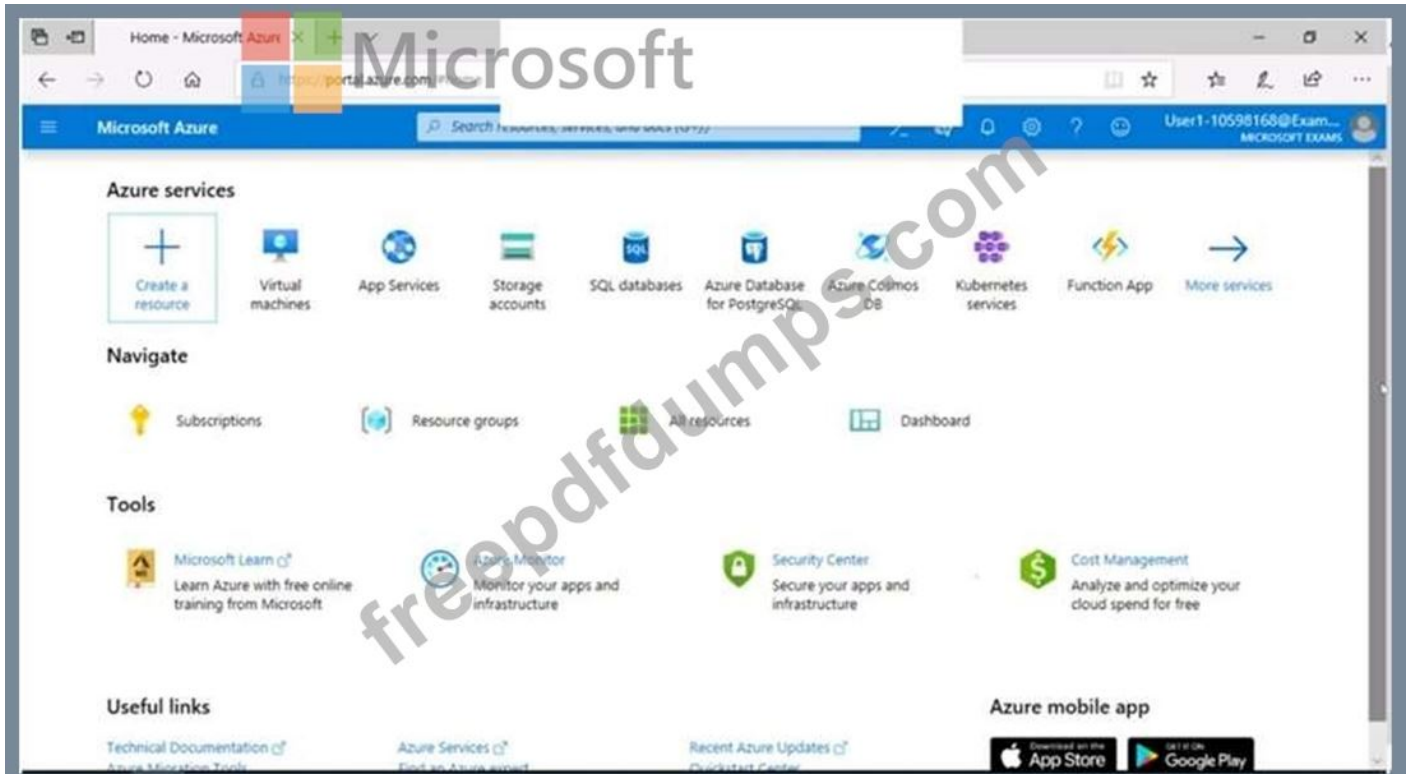
Azure Username: User1-10598168@ExamUsers.com

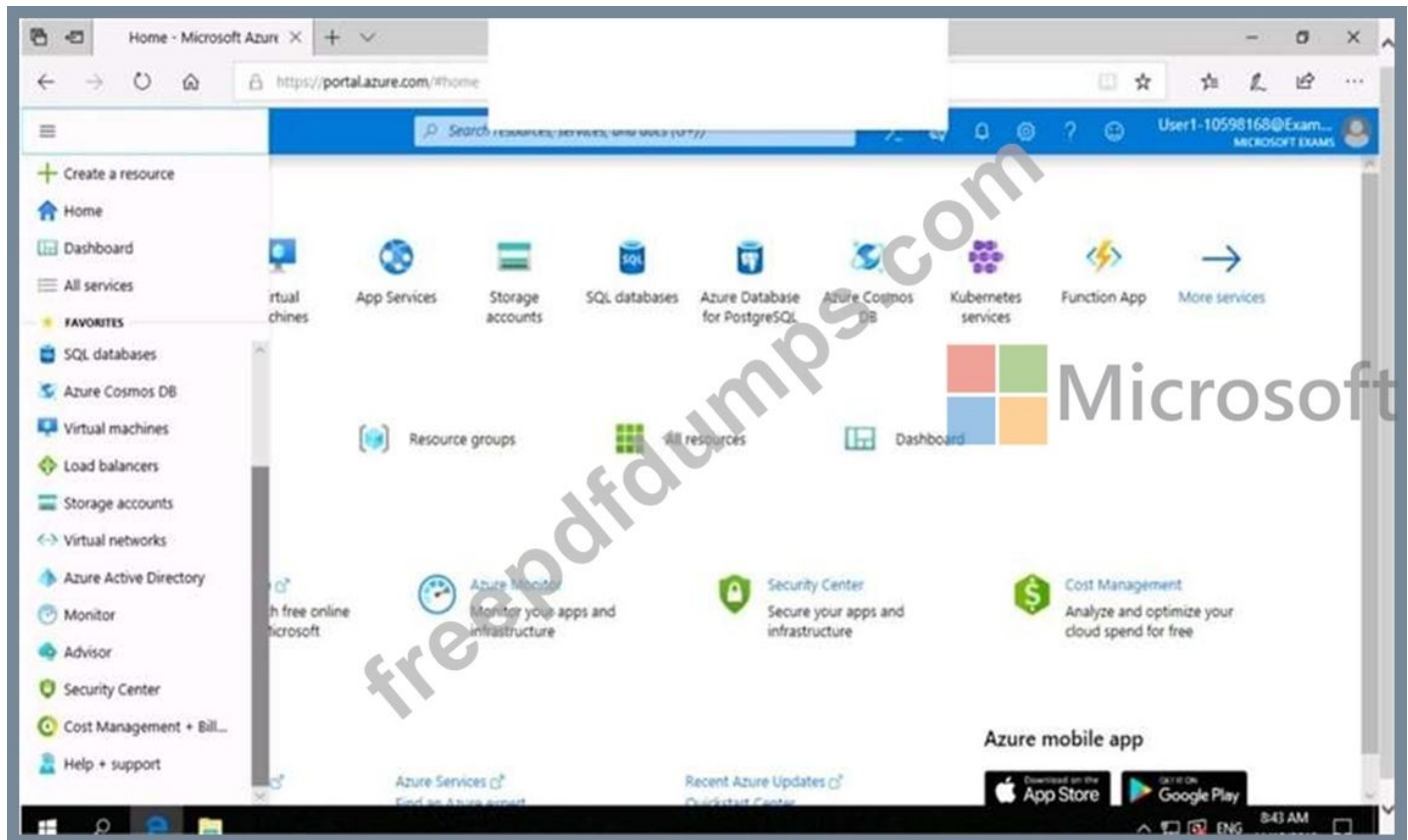
Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168







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

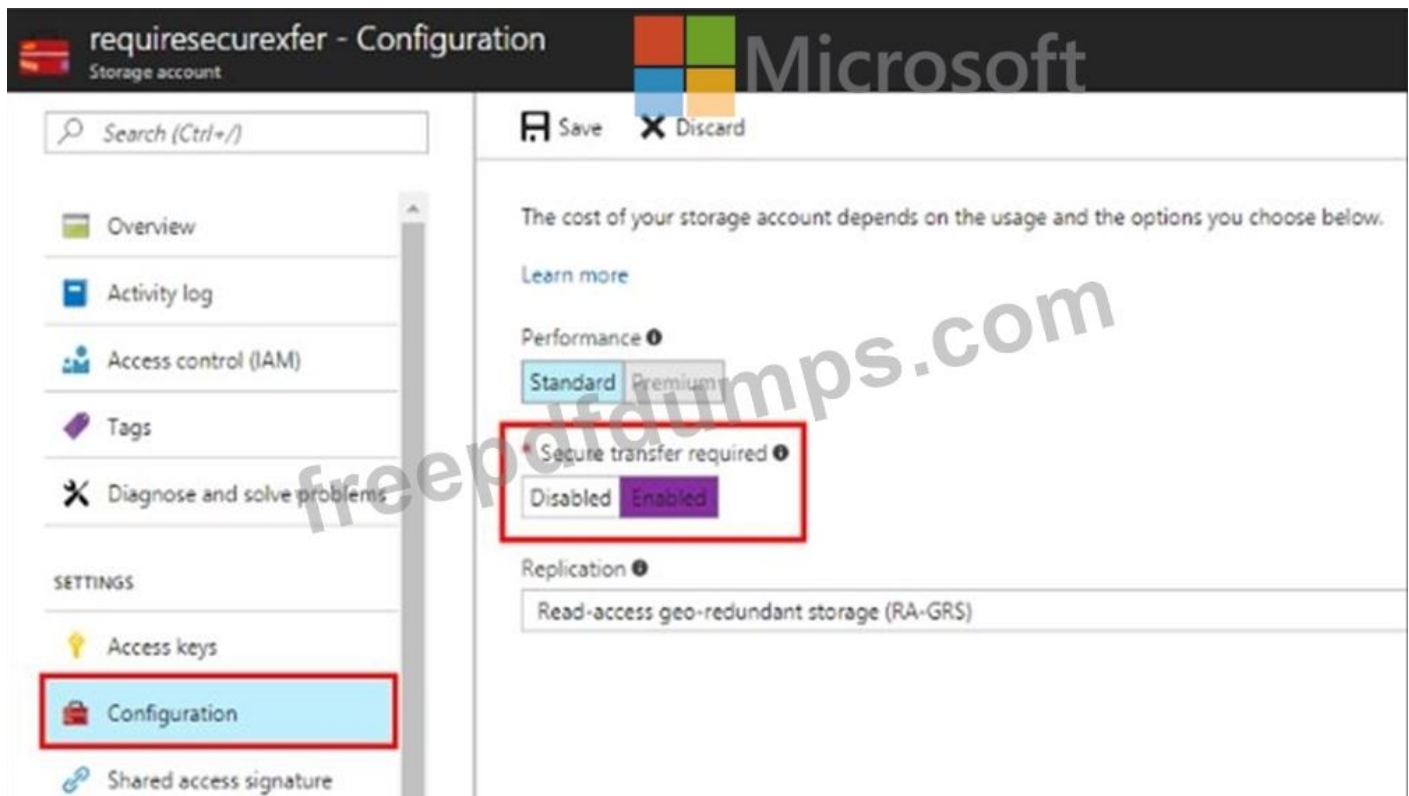
Answer:

See the explanation below.

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>

NEW QUESTION: 175

Your company has an Azure subscription named Subscription1. Subscription1 is associated with the Azure Active Directory tenant that includes the users shown in the following table.

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

The company is sold to a new owner.

The company needs to transfer ownership of Subscription1.

Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User:

 Microsoft	▼
User1	
User2	
User3	
User4	

Tool:

	▼
Azure Account Center	
Azure Cloud Shell	
Azure PowerShell	
Azure Security Center	

Answer:

Microsoft


User:

- User1
- User2
- User3
- User4

Tool:

- Azure Account Center
- Azure Cloud Shell
- Azure PowerShell
- Azure Security Center

Explanation

User:  Microsoft ▼

User1

User2

User3

User4

Tool: ▼

Azure Account Center

Azure Cloud Shell

Azure PowerShell

Azure Security Center

Table Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer>

NEW QUESTION: 176

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

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

KV1 stores a secret named Secret1 and a key for a managed storage account named Key1. You back up Secret1 and Key1.

To which key vaults can you restore each backup? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

You can restore the Secret1 backup to:

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

You can restore the Key1 backup to:

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

Answer:

You can restore the Secret1 backup to:

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

You can restore the Key1 backup to:

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

Explanation:

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

NEW QUESTION: 177

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.

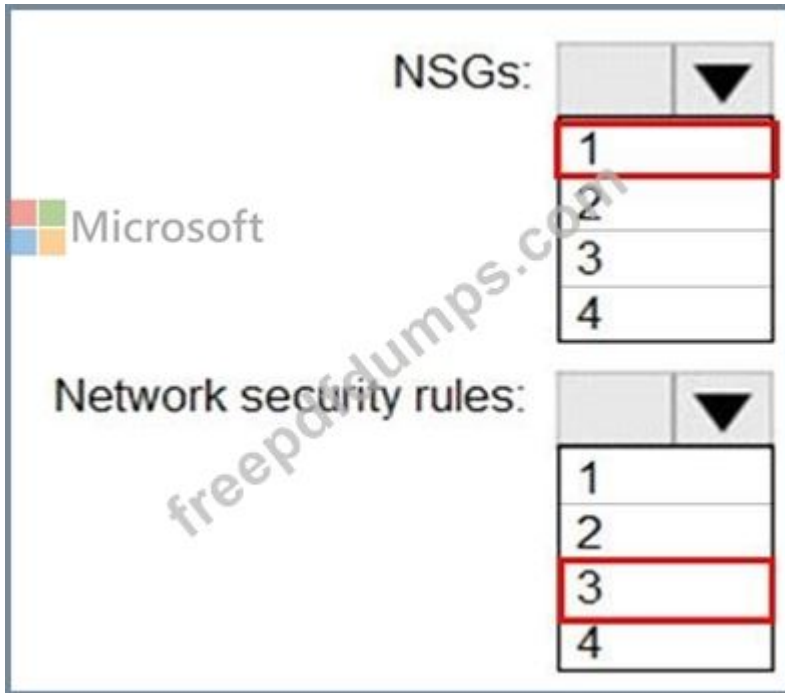
NOTE: Each correct selection is worth one point.

NSGs: ▼

1
2
3
4

Network security rules: ▼

1
2
3
4



Explanation:

NSGs: 1

Network security rules: 3

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

References:

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

NEW QUESTION: 178

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

Name	Type	Resource group	Location
RG1	Resource group	Not applicable	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.

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")
```

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

Statements	Yes	No
User1 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:

Statements Microsoft

Yes No

User1 is a member of Group1 and Group2.

User2 is a member of Group2 only.

Managed1 is a member of Group1 and Group2.

Reference:

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

NEW QUESTION: 179

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.

Name	Source
User1	Azure AD
User2	Azure AD
User3	On-premises Active Directory

The tenant contains the groups shown in the following table.

Name	Members
Group1	User1, User2, User3
Group2	User2

You configure a multi-factor authentication (MFA) registration policy that and the following settings:

Assignments:

Include: Group1

Exclude Group2

Controls: Require Azure MFA registration

Enforce Policy: On

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

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input checked="" type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user's next Azure AD authentication.	<input type="radio"/>	<input checked="" type="radio"/>
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION: 180

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		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	<input type="text"/>
IP address or CIDR	<input type="text"/>

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.

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:

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

Reference:

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

NEW QUESTION: 181

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

Microsoft

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	
<input type="text" value="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.

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:

Statements



Yes

No

From VM1, you can upload a blob to storageacc1.

From VM2, you can upload a blob to storageacc1.

From VM3, you can upload a blob to storageacc1.

Reference:

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

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!

Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (460 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 182

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.

Name	Source
User1	Azure AD
User2	Azure AD
User3	On-premises Active Directory

The tenant contains the groups shown in the following table.

Name	Members
Group1	User1, User2, User3
Group2	User2

You configure a multi-factor authentication (MFA) registration policy that and the following settings:

Assignments:

Include: Group1

Exclude Group2

Controls: Require Azure MFA registration

Enforce Policy: On

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

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input checked="" type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user's next Azure AD authentication.	<input type="radio"/>	<input checked="" type="radio"/>
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION: 183

You have a Azure subscription.

You enable Azure Active Directory (Azure AD) Privileged identify (PIM).

Your company's security policy for administrator accounts has the following conditions:

- * The accounts must use multi-factor authentication (MFA).
- * The account must use 20-character complex passwords.
- * The passwords must be changed every 180 days.
- * The account must be managed by using PIM.

You receive alerts about administrator who have not changed their password during the last 90 days.

You need to minimize the number of generated alerts.

Which PIM alert should you modify?

- A. Roles don't require multi-factor authentication for activation.
- B. Administrator aren't using their privileged roles
- C. Roles are being assigned outside of Privileged identity Management
- D. Potential state accounts in a privileged role.

Answer: D ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how->

to-configure-security-alerts?tabs=new

NEW QUESTION: 184

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

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

You have an Azure Subscription named Sub1.

You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service.

You need to revoke all access to Sa1.

Solution: You generate new SASs.

Does this meet the goal?

A. Yes

B. No

Answer: (SHOW ANSWER)

Instead you should create a new stored access policy.

To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier.

Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.

Reference:

<https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy>

NEW QUESTION: 185

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains three security groups named Group1, Group2, and Group3 and the users shown in the following table.

Name	Role	Member of
User1	Application administrator	Group1
User2	Application developer	Group2
User3	Cloud application administrator	Group3

Group3 is a member of Group2.

In contoso.com, you register an enterprise application named App1 that has the following settings:

Owners: User1

Users and groups: Group2


You configure the properties of App1 as shown in the following exhibit.

Save Discard Delete Got feedback

Enabled for users to sign-in? Yes No

Name *

Homepage URL

Logo 

Application ID

Object ID

User assignment required? Yes No

Visible to users Yes No

Notes

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

Statements	Yes	No
User1 has App1 listed on his My Apps portal.	<input type="radio"/>	<input type="radio"/>
User2 has App1 listed on her My Apps portal.	<input type="radio"/>	<input type="radio"/>
User3 has App1 listed on her My Apps portal.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 has App1 listed on his My Apps portal.	<input type="radio"/>	<input type="radio"/>
User2 has App1 listed on her My Apps portal.	<input type="radio"/>	<input type="radio"/>
User3 has App1 listed on her My Apps portal.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>

NEW QUESTION: 186

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

Name	Location	Connected to
VM1	West US 2	VNET1/Subnet1
VM2	West US 2	VNET1/Subnet1
VM3	West US 2	VNET1/Subnet2
VM4	East US	VNET2/Subnet3
VM5	West US 2	VNET5/Subnet5

Each virtual machine has a single network interface.

You add the network interface of VM1 to an application security group named ASG1.

You need to identify the network interfaces of which virtual machines you can add to ASG1.

What should you identify?

- A. VM2 only
- B. VM2 and VM3 only

<https://www.fast2test.com/AZ-500-practice-test.html> 24

Valid Fast2test AZ-500 Exam PDF Dumps - New AZ-500 Real Exam Questions

- C. VM2, VM3, VM4, and VM5
- D. VM2, VM3, and VM5 only

Answer: B (LEAVE A REPLY)

Explanation/Reference:

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

NEW QUESTION: 187

You have an Azure subscription that contains the following resources:

- A network virtual appliance (NVA) that runs non-Microsoft firewall software and routes all outbound traffic from the virtual machines to the internet
- An Azure function that contains a script to manage the firewall rules of the NVA
- Azure Security Center standard tier enabled for all virtual machines
- An Azure Sentinel workspace
- 30 virtual machines

You need to ensure that when a high-priority alert is generated in Security Center for a virtual machine, an incident is created in Azure Sentinel and then a script is initiated to configure a firewall rule for the NVA.

How should you configure Azure Sentinel to meet the requirements? To answer, drag the appropriate components to the correct requirements. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Answer:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts>

<https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center>

NEW QUESTION: 188

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

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

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

You plan to deploy an Azure firewall to HubVNet.

You create the following two routing tables:

RT1: Includes a user-defined route that points to the private IP address of the Azure firewall as a

next hop address RT2: Disables BGP route propagation and defines the private IP address of the Azure firewall as the default gateway You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.

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

NOTE: Each correct selection is worth one point.

Subnets

- Azure FirewallSubnet
- GatewaySubnet
- HubVNetSubnet0

Answer Area

RT1:

RT2:

Answer:

Subnets

- Azure FirewallSubnet
- GatewaySubnet
- HubVNetSubnet0

Answer Area

RT1:

RT2:

NEW QUESTION: 189

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

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

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

Create an access review

Access reviews enable reviewers to attest to users access.

Review name:

Description:

Start date: 2019-03-01

Frequency:

Review role membership:

Reviewers:

Scope: Everyone

Start date: 2019-03-20

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.

User3 can perform Review1 for

- User3 only
- User1 and User2 only
- User1, User2, and User3

If User2 fails to complete Review1 by March 20, 2019

- The Password administrator role will be revoked from User2
- User2 will retain the Password administrator role
- User3 will receive a confirmation request

Answer:

User3 can perform Review1 for

- User3 only
- User1 and User2 only
- User1, User2, and User3

If User2 fails to complete Review1 by March 20, 2019



- The Password administrator role will be revoked from User2
- User2 will retain the Password administrator role
- User3 will receive a confirmation request

References:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review>

NEW QUESTION: 190

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.

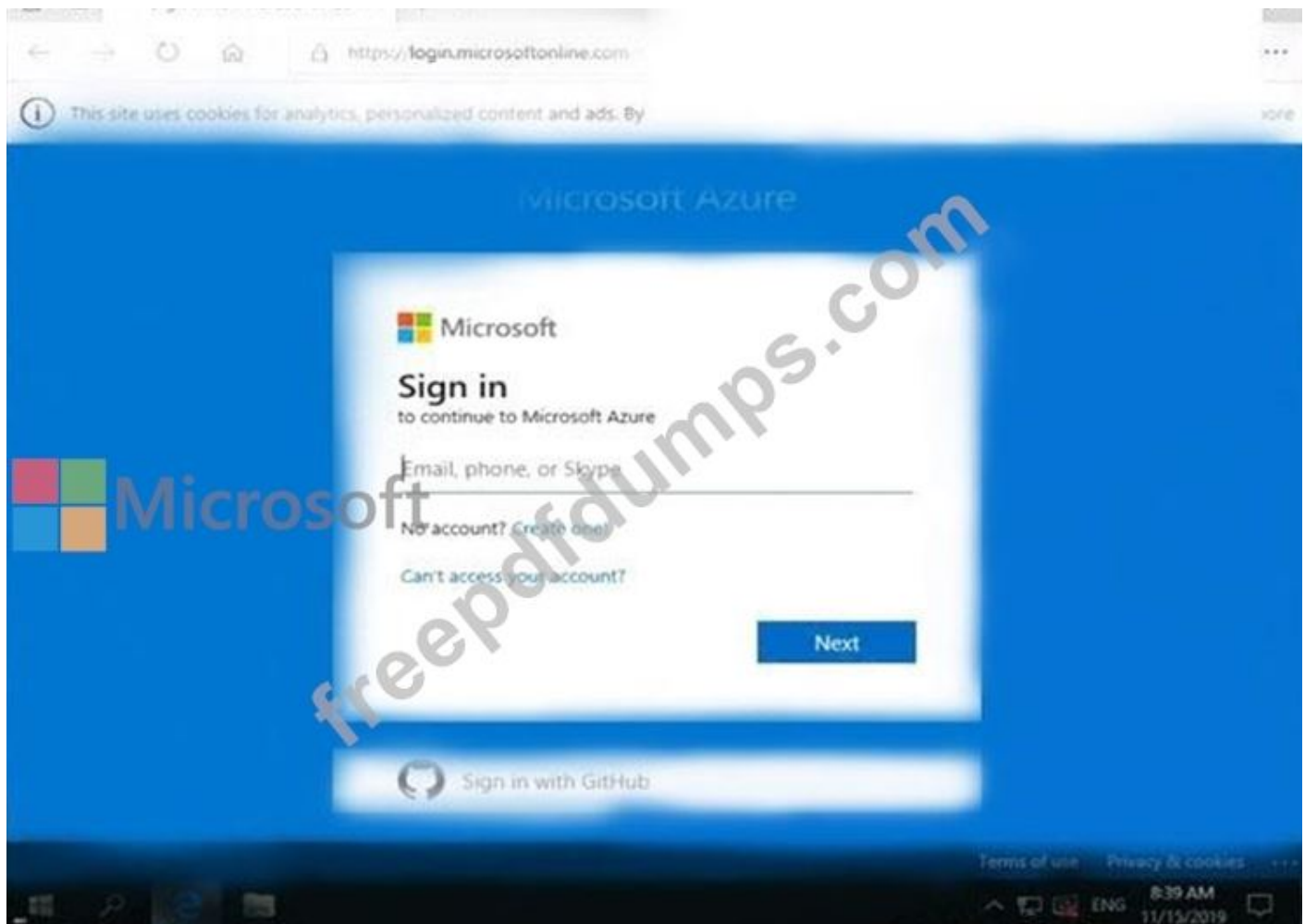
To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168



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 | Azure Monitor | Security Center | Cost Management

Useful links

Azure mobile app

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor

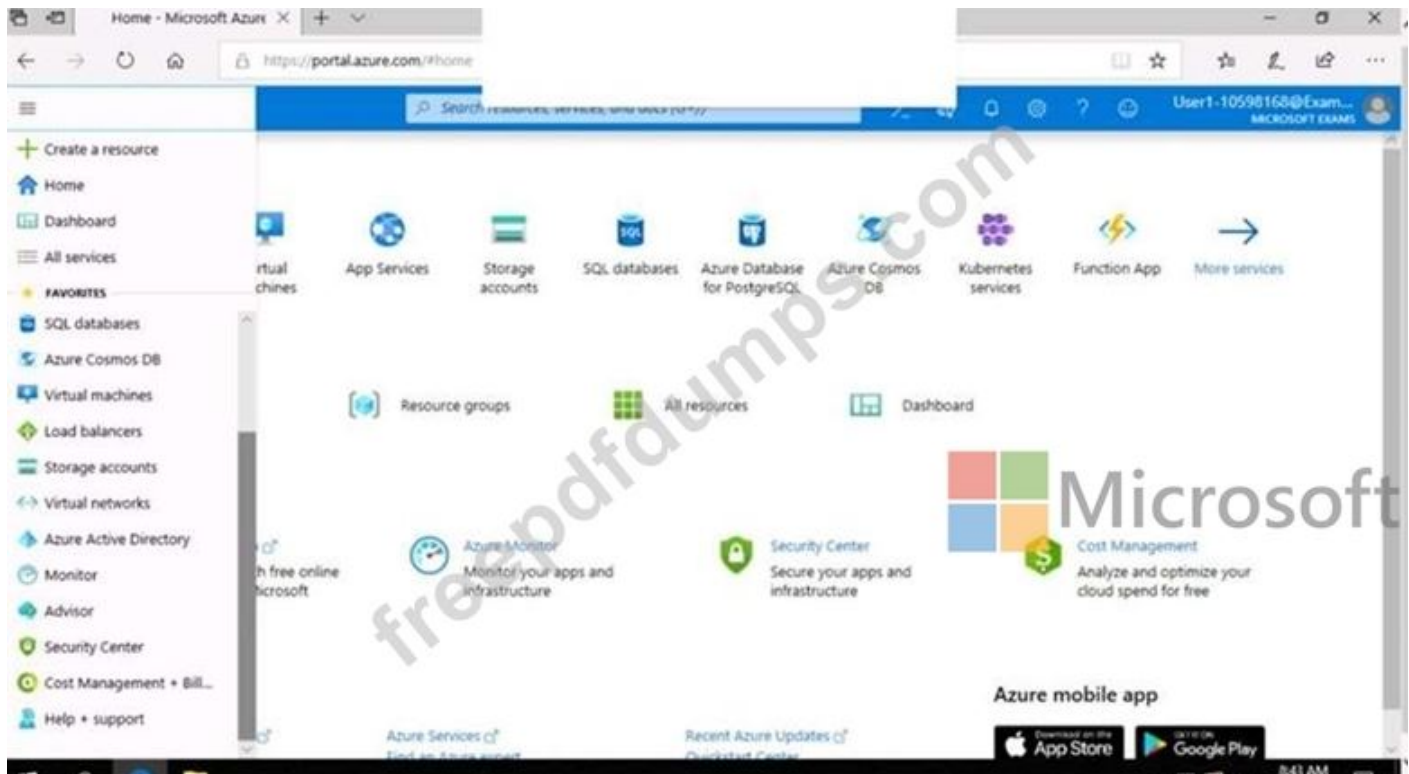
Virtual machines | App Services | Storage accounts | SQL databases | Azure Database for PostgreSQL | Azure Cosmos DB | Kubernetes services | Function App | More services

Resource groups | All resources | Dashboard

Azure Monitor | Security Center | Cost Management

Azure mobile app

freepdfdumps.com Microsoft



You need to add the network interface of a virtual machine named VM1 to an application security group named ASG1.

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

Answer:

See the explanation below.

* In the Search resources, services, and docs box at the top of the portal, begin typing the name of a virtual machine, VM1 that has a network interface that you want to add to, or remove from, an application security group.

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

* Under SETTINGS, select Networking. Select Configure the application security groups, select the application security groups that you want to add the network interface to, or unselect the application security groups that you want to remove the network interface from, and then select Save.

Reference:

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

NEW QUESTION: 191

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

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

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

Create an access review

Access reviews enable reviewers to attest to users access.

* Review name:

Description:

* Start date:

Frequency:

End date:

Scope: Everyone

* Review role membership:

Reviewers:

Upon completion settings:

Auto apply results to resources:

Should reviewer be required:

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.

User3 can perform Review1 for

- User3 only
- User1 and User2 only
- User1, User2, and User3

If User2 fails to complete Review1 by March 20, 2019

- The Password administrator role will be revoked from User2
- User2 will retain the Password administrator role
- User3 will receive a confirmation request

Answer:

User3 can perform Review1 for

- User3 only
- User1 and User2 only
- User1, User2, and User3

If User2 fails to complete Review1 by March 20, 2019

- The Password administrator role will be revoked from User2
- User2 will retain the Password administrator role
- User3 will receive a confirmation request

Explanation

User3 can perform Review1 for

- User3 only
- User1 and User2 only
- User1, User2, and User3

If User2 fails to complete Review1 by March 20, 2019

- The Password administrator role will be revoked from User2
- User2 will retain the Password administrator role
- User3 will receive a confirmation request

Box 1: User3 only

Use the Members (self) option to have the users review their own role assignments.

Box 2: User3 will receive a confirmation request

Use the Should reviewer not respond list to specify what happens for users that are not reviewed by the reviewer within the review period. This setting does not impact users who have been reviewed by the reviewers manually. If the final reviewer's decision is Deny, then the user's access will be removed.

No change - Leave user's access unchanged

Remove access - Remove user's access

Approve access - Approve user's access

Take recommendations - Take the system's recommendation on denying or approving the user's continued access

References:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-start-se>

NEW QUESTION: 192

You have an Azure subscription. The subscription contains Azure virtual machines that run

Windows Server

2016.

You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.

How should you complete the policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

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

Append
Deny
DeployIfNotExists

Microsoft

Answer:

Explanation

```

    },
    "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
            ": {
          }
        }
      }
    }
  }
}

```



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>

NEW QUESTION: 193

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.

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:

Actions	Answer Area
Run Set-AzureRmKeyVaultAccessPolicy	
Create an Azure Automation account.	Create an Azure Automation account.
Import PowerShell modules to the 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.	Create a connection resource in the Azure Automation account.

Explanation

Create an Azure Automation account.
Import PowerShell modules to the Azure Automation account.
Create a connection resource in the Azure Automation account.

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/>

NEW QUESTION: 194

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

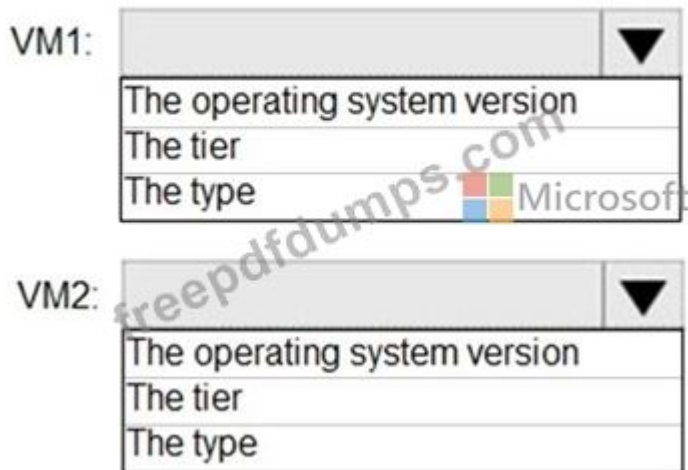
Name	Operating system	Type	Tier
VM1	Windows Server 2008 R2	A3	Basic
VM2	Ubuntu 16.04-DAILY-LTS	L4s	Standard

You deploy and configure an Azure Key vault.

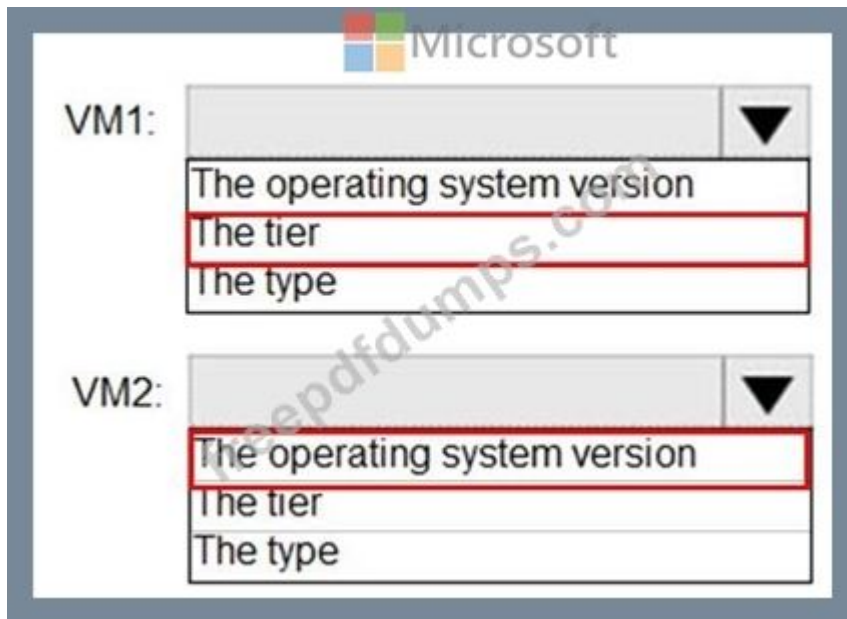
You need to ensure that you can enable Azure Disk Encryption on VM1 and VM2.

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

NOTE: Each correct selection is worth one point.



Answer:



References:

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

NEW QUESTION: 195

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

Answer: (SHOW ANSWER)

Section: [none]

Explanation/Reference:

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

NEW QUESTION: 196

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

Answer: (SHOW ANSWER)

Section: [none]

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>

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!

Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (460 Q&As Dumps, **30%OFF**)

Special Discount: Freepdfdumps)

NEW QUESTION: 197

You have an Azure Sentinel workspace that has the following data connectors:

Azure Active Directory Identity Protection

Common Event Format (CEF)

Azure Firewall

You need to ensure that data is being ingested from each connector.

From the Logs query window, which table should you query for each connector? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Azure Active Directory Identity Protection:

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog



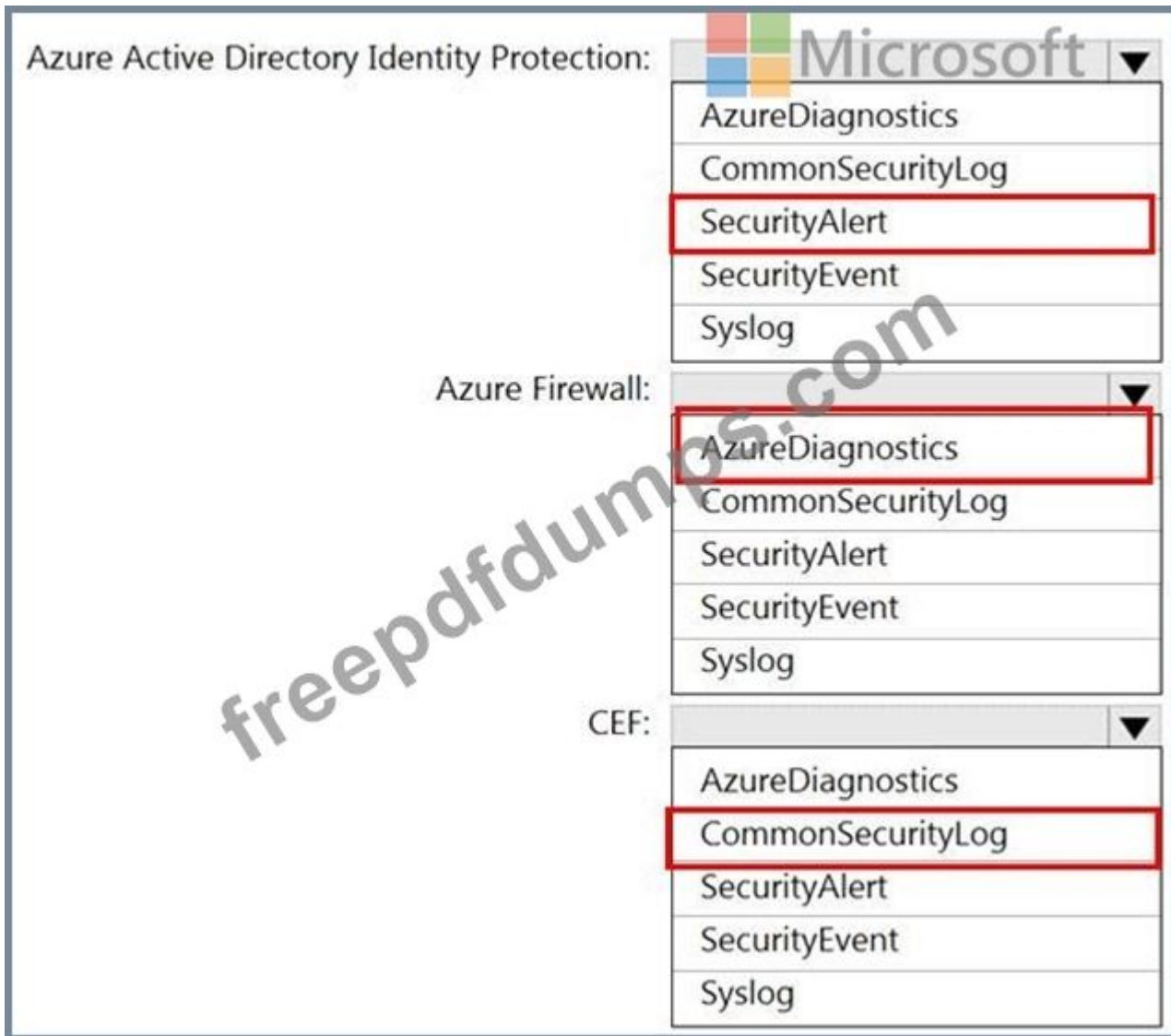
Azure Firewall:

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

CEF:

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

Answer:



NEW QUESTION: 198

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.

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:

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

NEW QUESTION: 199

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

Name	Type	Resource group	Location
RG1	Resource group	Not applicable	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.

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")
```

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 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:

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"/>

Reference:

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

NEW QUESTION: 200

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

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
From VM1, you can successfully ping the private IP address of VM4.	<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:

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"/>

Topic 1, Contoso

Technical Requirements

Contoso identifies the following technical requirements:

Deploy Azure Firewall to VNetWork1 in Sub2.

Register an application named App2 in contoso.com.

Whenever possible, use the principle of least privilege.

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

Existing Environment

Azure AD

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

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

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

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

Sub1

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

User2 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

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

Sub1 contains the Azure policies shown in the following table.

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

Sub2

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

Sub2 contains the virtual machines shown in the following table.

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

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

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

Name	Associated to
NSG1	NIC2
NSG2	Subnet1.1
NSG3	Subnet1.3
NSG4	Subnet2.1

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

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

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

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

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

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

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

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

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

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

Contoso identifies the following technical requirements:

Deploy Azure Firewall to VNetwork1 in Sub2.

Register an application named App2 in contoso.com.

Whenever possible, use the principle of least privilege.

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

NEW QUESTION: 201

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

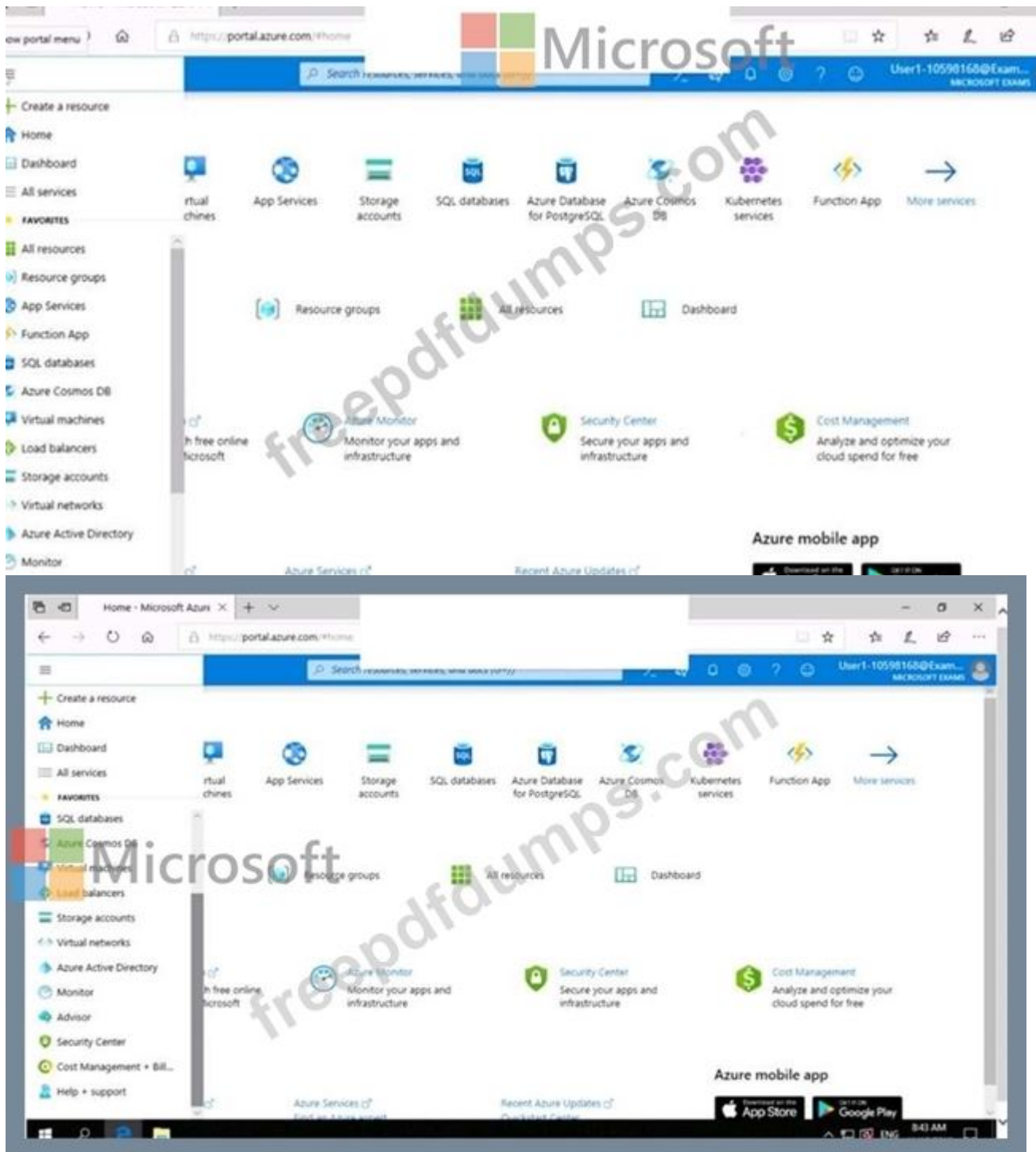
The following information is for technical support purposes only:

Lab Instance: 10598168

The image shows a browser window displaying the Microsoft Azure sign-in page. The address bar shows the URL <https://login.microsoftonline.com/>. The page features the Microsoft logo and the text "Sign in to continue to Microsoft Azure". Below this is a text input field for "Email, phone, or Skype", followed by links for "No account? Create one!" and "Can't access your account?". A blue "Next" button is positioned at the bottom right of the sign-in form. Below the form is a "Sign in with GitHub" option. The browser's taskbar at the bottom shows the Windows Start button, search icon, and several open applications. The system tray displays the date and time as "ENG 8:39 AM 11/15/2019".

Below the sign-in page, the Microsoft Azure portal dashboard is visible. The page title is "Microsoft Azure" and the user is identified as "User1-10598168@Exam... MICROSOFT EXAM". The dashboard is organized into several sections:

- Azure services:** Includes "Create a resource" and icons for Virtual machines, App Services, Storage accounts, SQL databases, Azure Database for PostgreSQL, Azure Cosmos DB, Kubernetes services, and Function App.
- Navigate:** Includes icons for Subscriptions, Resource groups, All resources, and Dashboard.
- Tools:** Includes "Microsoft Learn" (Learn Azure with free online training from Microsoft), "Azure Monitor" (Monitor your apps and infrastructure), "Security Center" (Secure your apps and infrastructure), and "Cost Management" (Analyze and optimize your cloud spend for free).
- Useful links:** Includes "Technical Documentation", "Azure Services", and "Recent Azure Updates".
- Azure mobile app:** Includes links to download the app on the App Store and 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.

Answer:

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



5. In the Role drop-down list, select the role Virtual Machine Contributor.

Virtual Machine Contributor lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.

6. In the Select list, select user user21059868

7. Click Save to assign the role.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal>

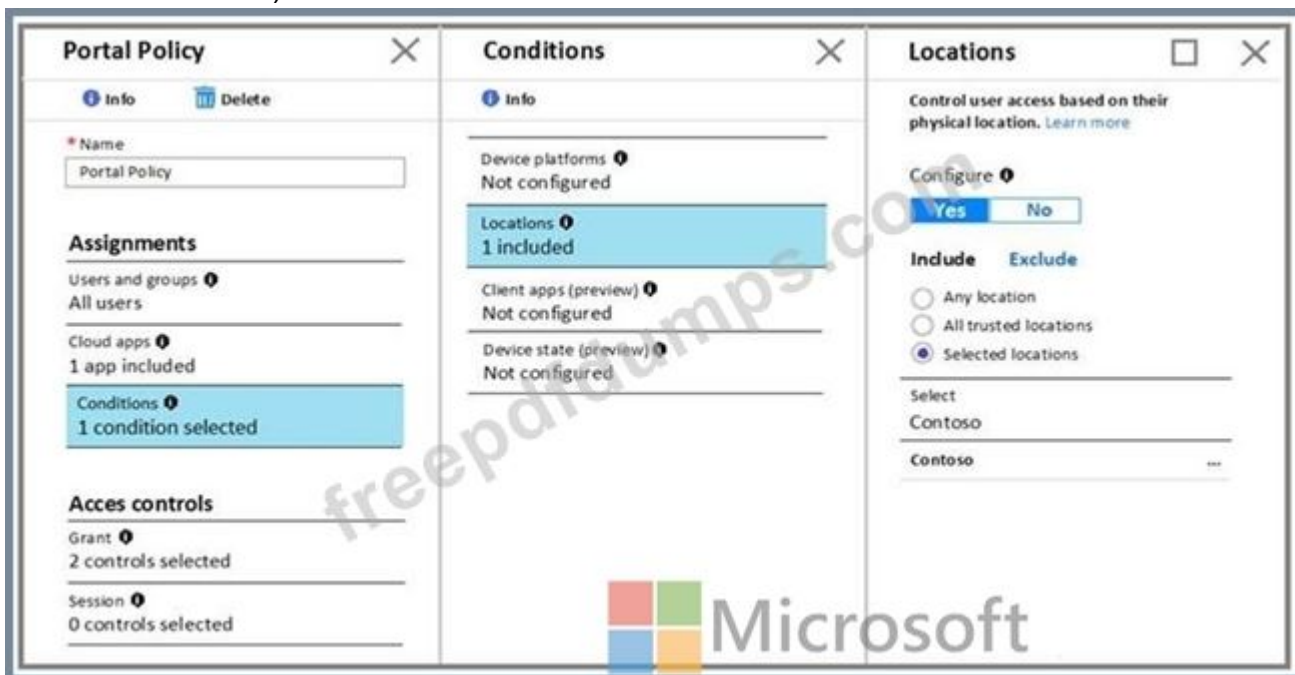
<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor>

NEW QUESTION: 202

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

You create one active conditional access policy named Portal Policy. Portal Policy is used to provide access to the Microsoft Azure Management cloud app.

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



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

Portal Policy

[Info](#) [Delete](#)

Name
Portal Policy

Assignments

Users and groups ⓘ
All users

Cloud apps ⓘ
1 app included

Conditions ⓘ
1 condition selected

Access controls

Grant ⓘ
2 controls selected

Session ⓘ
0 controls selected

Grant

Select the controls to be enforced.

Block access

Grant access

Require multi-factor authentication ⓘ

Require device to be marked as compliant ⓘ

Require Hybrid Azure AD jointed device ⓘ

Require approved client app ⓘ
[See list of approved client apps](#)

For multiple controls

Require all the selected controls

Require one of the selected controls

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

Statements	Yes	No
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	<input type="radio"/>	<input type="radio"/>
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	<input type="radio"/>	<input type="radio"/>
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	<input type="radio"/>	<input checked="" type="radio"/>
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	<input checked="" type="radio"/>	<input type="radio"/>
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: No

The Contoso location is excluded

Box 2: Yes

Box 3: Yes

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

NEW QUESTION: 203

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.

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	<input type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the private IP address of VM3.	<input type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the private IP address of VM5.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	<input type="radio"/>	<input checked="" type="radio"/>
From VM1, you can successfully ping the private IP address of VM3.	<input checked="" type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the private IP address of VM5.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION: 204

You need to create Role1 to meet the platform protection requirements.

How should you complete the role definition of Role1? To answer, select the appropriate options

in the answer area.

NOTE: Each correct selection is worth one point.

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

Answer:

```
{  
  "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"  
  ]  
}
```

NEW QUESTION: 205

You have an Azure Active Directory (Azure AD) tenant and a root management group. You create 10 Azure subscriptions and add the subscriptions to the root management group. You need to create an Azure Blueprints definition that will be stored in the root management group.

What should you do first?

- A. Modify the role-based access control (RBAC) role assignments for the root management group.
- B. Add an Azure Policy definition to the root management group.
- C. Create a user-assigned identity.
- D. Create a service principal.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin>

NEW QUESTION: 206

You create an alert rule that has the following settings:

Resource: RG1

Condition: All Administrative operations

Actions: Action groups configured for this alert rule: ActionGroup1

Alert rule name: Alert1

You create an action rule that has the following settings:

Scope: VM1

Filter criteria: Resource Type = "Virtual Machines"

Define on this scope: Suppression

Suppression config: From now (always)

Name: ActionRule1

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

Note: Each correct selection is worth one point.

Statements	Yes	No
If you start VM1, an alert is triggered.	<input type="radio"/>	<input type="radio"/>
If you start VM2, an alert is triggered.	<input type="radio"/>	<input type="radio"/>
If you add a tag to RG1, an alert is triggered.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
If you start VM1, an alert is triggered.	<input type="radio"/>	<input checked="" type="radio"/>
If you start VM2, an alert is triggered.	<input checked="" type="radio"/>	<input type="radio"/>
If you add a tag to RG1, an alert is triggered.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log>

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

NEW QUESTION: 207

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

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

In KeyVault, the following events occur in sequence:

Item1 is deleted

Administrator enables soft delete

Item2 and Policy1 are deleted.

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

NOTE: Each correct selection is worth one point.

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 add a new secret named Item2.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
You can recover Policy1.	<input type="radio"/>	<input checked="" type="radio"/>
You can add a new key named Item1.	<input checked="" type="radio"/>	<input type="radio"/>
You can add a new secret named Item2.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 208

You have an Azure subscription that contains a resource group named RG1. RG1 contains a storage account named storage1.

You have two custom Azure roles named Role1 and Role2 that are scoped to RG1.

The permissions for Role1 are shown in the following JSON code.

```

"permissions": [
  {
    "actions": [
      "Microsoft.Storage/storageAccounts/listKeys/action"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
]

```

The permissions for Role2 are shown in the following JSON code.

```

"permissions": [
  {
    "actions": [
      "Microsoft.Storage/storageAccounts/listKeys/action",
      "Microsoft.Storage/storageAccounts/ListAccountSas/action",
      "Microsoft.Storage/storageAccounts/read"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
]

```

Statements	Yes	No
User1 can read data in storage1.	<input type="radio"/>	<input type="radio"/>
User2 can read data in storage1.	<input type="radio"/>	<input type="radio"/>
User3 can restore storage1 from a backup in Azure Backup.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements

User1 can read data in storage1.

User2 can read data in storage1.

User3 can restore storage1 from a backup in Azure Backup.



Yes

No

NEW QUESTION: 209

You create an Azure subscription.

You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure AD roles.

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

Actions

- Verify your identity by using multi-factor authentication (MFA).
- Consent to PIM.
- Sign up PIM for Azure AD roles.
- Discover privileged roles.
- Discover resources.

Answer Area

Answer:

Actions

Verify your identity by using multi-factor authentication (MFA).

Consent to PIM.

Sign up PIM for Azure AD roles.

Discover privileged roles.

Discover resources.

ANSWER AREA

Consent to PIM.

Verify your identity by using multi-factor authentication (MFA).

Sign up PIM for Azure AD roles.

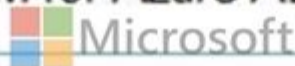


Explanation

Consent to PIM.

Verify your identity by using multi-factor authentication (MFA).

Sign up PIM for Azure AD roles.



Step 1: Consent to PIM

The screenshot shows the Azure portal interface. In the left-hand navigation pane, the 'Consent to PIM' link is highlighted with a red rectangular box. The main content area displays the 'Privileged Identity Management - Consent to PIM' page. At the top, there is a 'Verify my identity' button with a red exclamation mark icon. Below this, the 'Azure AD Privileged Identity Management' section is visible, featuring a green diamond icon and the text 'Azure AD PIM is a Premium feature that enables you to limit standing admin access to priv...'. There are also two cards: 'Limit standing access' and 'Discover who has access'.

Step: 2 Verify your identity by using multi-factor authentication (MFA) Click Verify my identity to verify your identity with Azure MFA. You'll be asked to pick an account.

Step 3: Sign up PIM for Azure AD roles

Once you have enabled PIM for your directory, you'll need to sign up PIM to manage Azure AD roles.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim->

getting-started

NEW QUESTION: 210

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

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

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

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

You need to configure auditing for SQL1.

Which storage accounts and Log Analytics workspaces can you use as the audit log destination?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Storage accounts that can be used as the audit log destination:

- Storage1 only
- Storage2 only
- Storage1 and Storage2 only
- Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

- Analytics1 only
- Analytics1 and Analytics2 only
- Analytics1 and Analytics3 only
- Analytics1, Analytics2, and Analytics3

Answer:

Answer Area

Storage accounts that can be used as the audit log destination:

- Storage1 only
- Storage2 only
- Storage1 and Storage2 only
- Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

- Analytics1 only
- Analytics1 and Analytics2 only
- Analytics1 and Analytics3 only
- Analytics1, Analytics2, and Analytics3

NEW QUESTION: 211

You have an Azure AD tenant that contains the users shown in the following table.

Name	User device
User1	Android mobile device with facial recognition
User2	Windows device with a camera for Business-compatible hardware

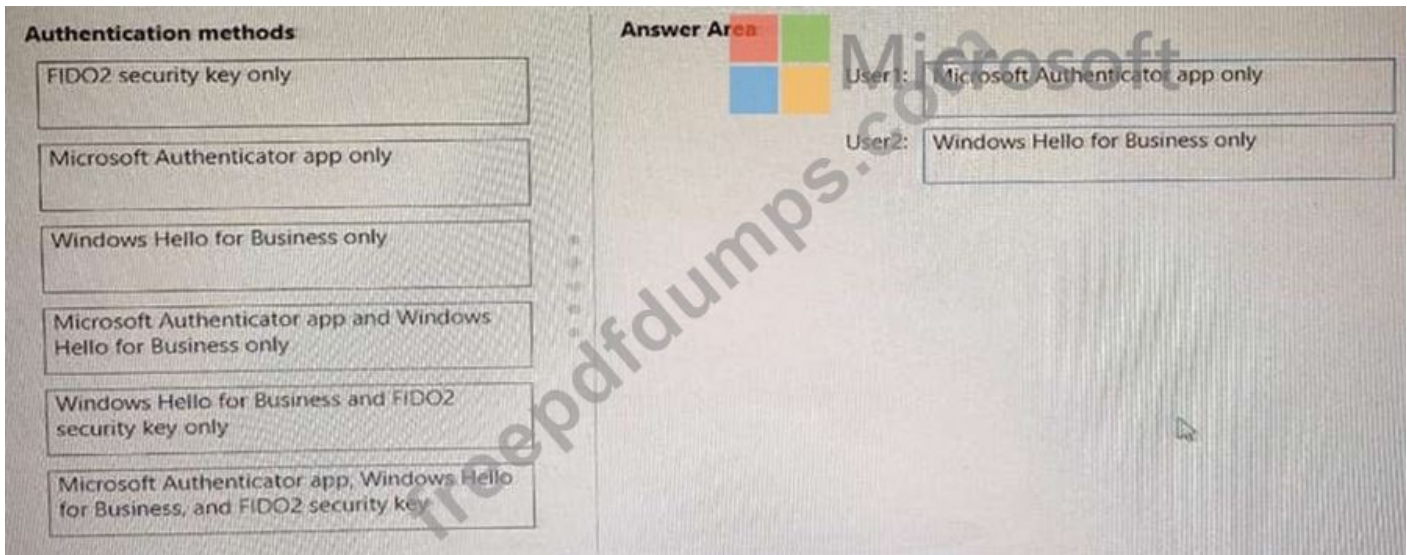
You enable passwordless authentication for the tenant.

Which authentication method can each user use for passwordless authentication? To answer, drag the appropriate authentication methods to the correct users. Each authentication method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Answer:

Explanation



Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam! Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (460 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

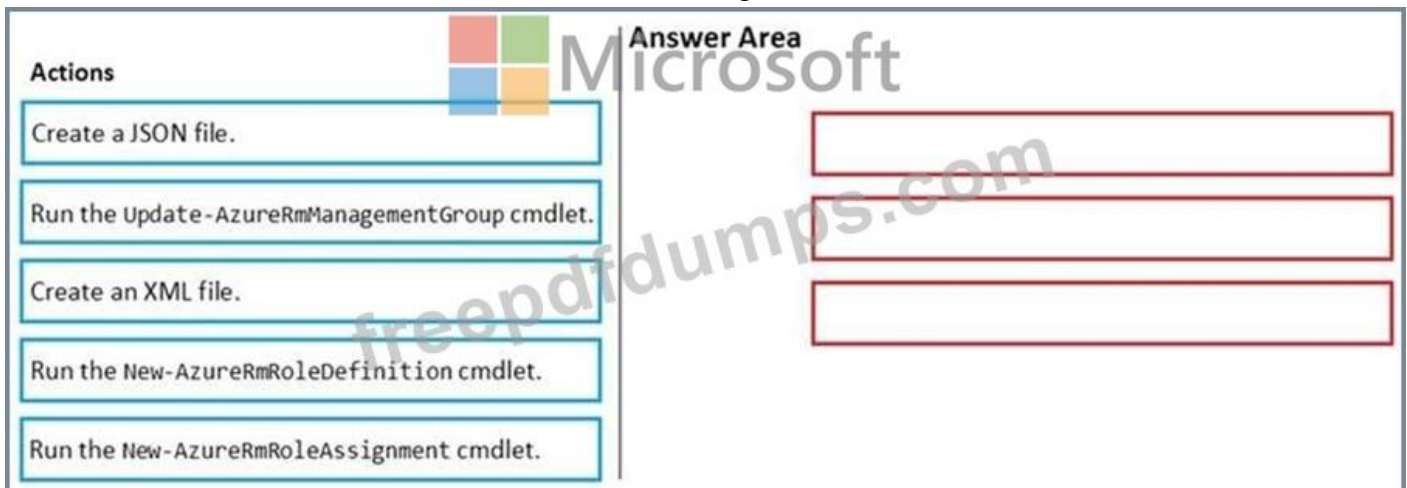
NEW QUESTION: 212

You have an Azure subscription named Sub1.

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


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

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



Answer:

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



Reference:

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

NEW QUESTION: 213

You have an Azure subscription that contains a user named Admin1 and a resource group named RG1.

In Azure Monitor, you create the alert rules shown in the following table.

Name	Resource	Condition
Rule1	RG1	All security operations
Rule2	RG1	All administrative operations
Rule3	Azure subscription	All security operations by Admin1
Rule4	Azure subscription	All administrative operations by Admin1

Admin1 performs the following actions on RG1:

Adds a virtual network named VNET1

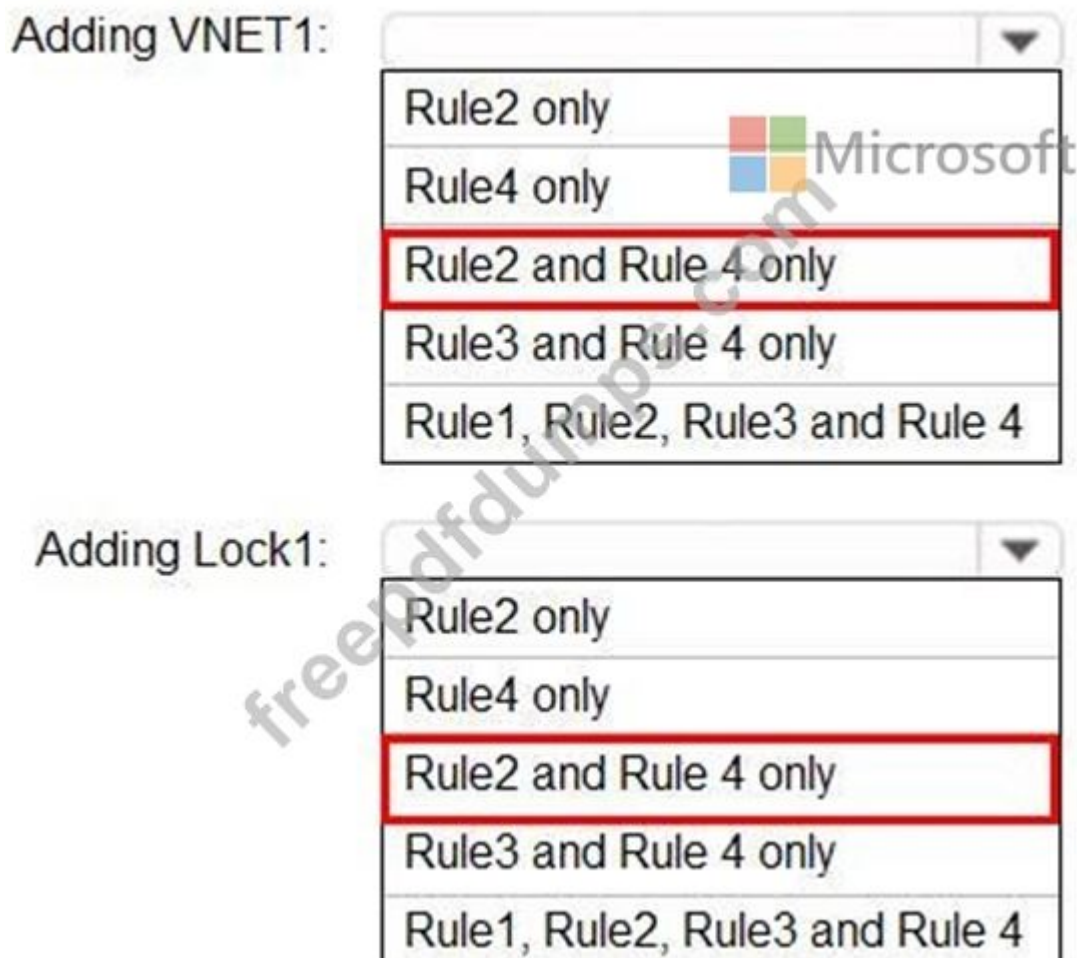
Adds a Delete lock named Lock1

Which rules will trigger an alert as a result of the actions of Admin1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 214

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

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

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

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

You need to identify how Azure Information Protection will label files.

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

NOTE: Each correct selection is worth one point.

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

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

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

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

Answer:

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

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

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

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

Reference:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

NEW QUESTION: 215

You have three Azure subscriptions and a user named User1. You need to provide User1 with the ability to manage and view costs for the resources across all three subscriptions. 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.

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

Actions

- Create a management group.
- Add the three subscriptions to the management group.
- Assign User1 the Global administrator role.
- Assign User1 the Owner role for the management group.
- Assign User1 the Cost Management Contributor role for the management group.

Answer:

Answer Area

- Assign User1 the Cost Management Reader,,,,
- Assign User1 the Global administrator role.
- Add the three subscriptions to the management group.

- 1 - Assign User1 the Cost Management Reader,,,,
- 2 - Assign User1 the Global administrator role.
- 3 - Add the three subscriptions to the management group.

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!

Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (460 Q&As Dumps, **30%OFF**)

Special Discount: Freepdfdumps)