Microsoft.AZ-500.v2026-08-05.q242

Exam Code:	AZ-500
Exam Name:	Microsoft Azure Security Technologies
Certification Provider:	Microsoft
Free Question Number:	242
Version:	v2026-08-05
# of views:	143
# of Questions views:	2420
https://www.freepdfdumps.com/Microsoft.AZ-500.v2026-08-05.q242.html	

NEW QUESTION: 1
You have an on-premises network and an Azure subscription.
You have the Microsoft SQL Server instances shown in the following table.

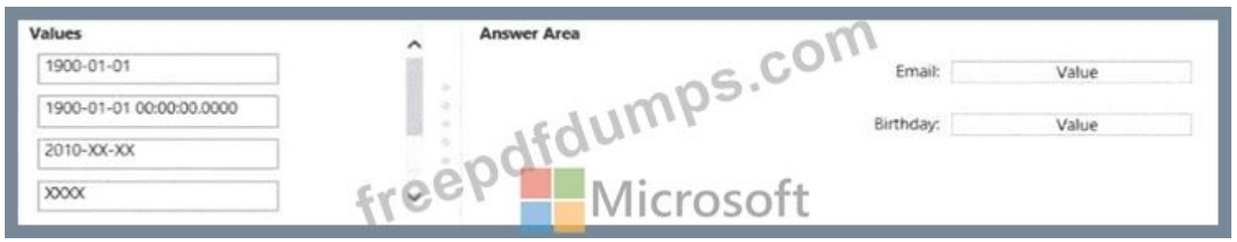
Name	Type
sql1	Azure SQL managed instance
sql2	SQL Server 2019 on an Azure virtual machine that runs Windows Server 2019
sql3	SQL Server 2019 on an Azure virtual machine that runs Red Hat Enterprise Linux (RHEL) 8.3
sql4	On-premises physical server that runs Windows Server 2016 and has SQL Server 2016 installed

You plan to implement Microsoft Defender for SQL.
Which SQL Server instances will be protected by Microsoft Defender for SQL?
A. sql1, sql2, sql3, and sql4
B. sql1 sql2 and so.14 only
C. sql1, sql2, andsql3 only
D. sql1 and sql2 only
Answer: A (LEAVE A REPLY)

NEW QUESTION: 2
You have an Azure subscription that contains an Azure SQL database named SQLDB1. SQLDB1 contains the columns shown in the following table.

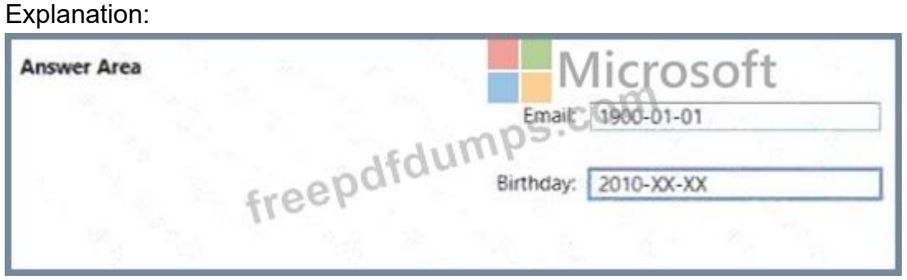
Name	Data type	Sample value
Email	Varchar	admin@contoso.com
Birthday	Date	2010-07-07

For the Email and Birthday columns, you implement dynamic data masking by using the default masking function.
Which value will the users see in each column? To answer, drag the appropriate values to the correct columns.
Each value 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:



NEW QUESTION: 3

You have an Azure subscription that contains a storage account and an Azure web app named App1.

App1 connects to an Azure Cosmos DB database named Cosmos1 that uses a private endpoint named Endpoint1. Endpoint1 has the default settings.

You need to validate the name resolution to Cosmos1.

Which DNS zone should you use?

A. Endpoint1. Privatelink,blob,core,windows,net

B. Endpoint1. Privatelink,documents,azure,com

C. Endpoint1. Privatelink,azurewebsites,net

D. Endpoint1. Privatelink,database,azure,com

Answer: B (LEAVE A REPLY)

NEW QUESTION: 4

You have an Azure subscription that contains the following resources:

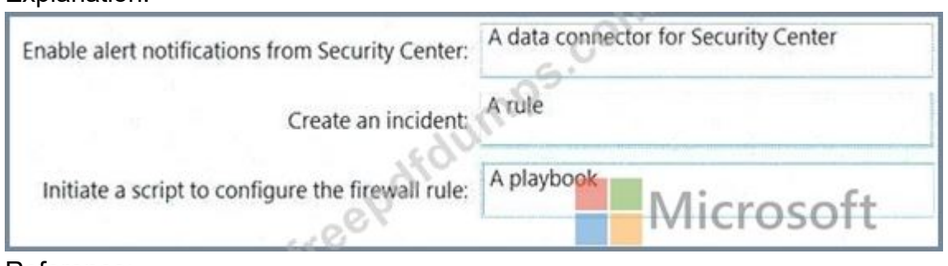
* A network virtual appliance (NVA) that runs non-Microsoft firewall software and routes all outbound traffic from the virtual machines to the internet
* An Azure function that contains a script to manage the firewall rules of the NVA
* Azure Security Center standard tier enabled for all virtual machines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

Explanation:



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: 5

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

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

In KeyVault1 the following events occur in sequence:

* item is deleted.

* Item2 and Policy1 are deleted.

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

NOTE: Each correct selection is worth one point.

ui

Answer Area

Statements	Yes	No
You can recover Policy1.	○	○
You can add a new key named Item1.	○	○
You can recover Item2.	○	○

Answer:

Explanation:

NEW QUESTION: 6
You have an Azure subscription that contains the resources shown in the following Table.

Name	Type
VM1	Virtual machine
VNET1	Virtual network
storage1	Storage account
Vault1	Key vault

You plan to enable Microsoft Defender for Cloud for the subscription. Which resources can be protected by using Microsoft Defender for Cloud?
A. VM1, VNET1, and storage1 only
B. VM1 and VNET only
C. VM1 and storage1 only
D. VM1.VNET1, storage1, and Vault1
E. VM1, storage1, and Vault1 only
Answer: (SHOW ANSWER)

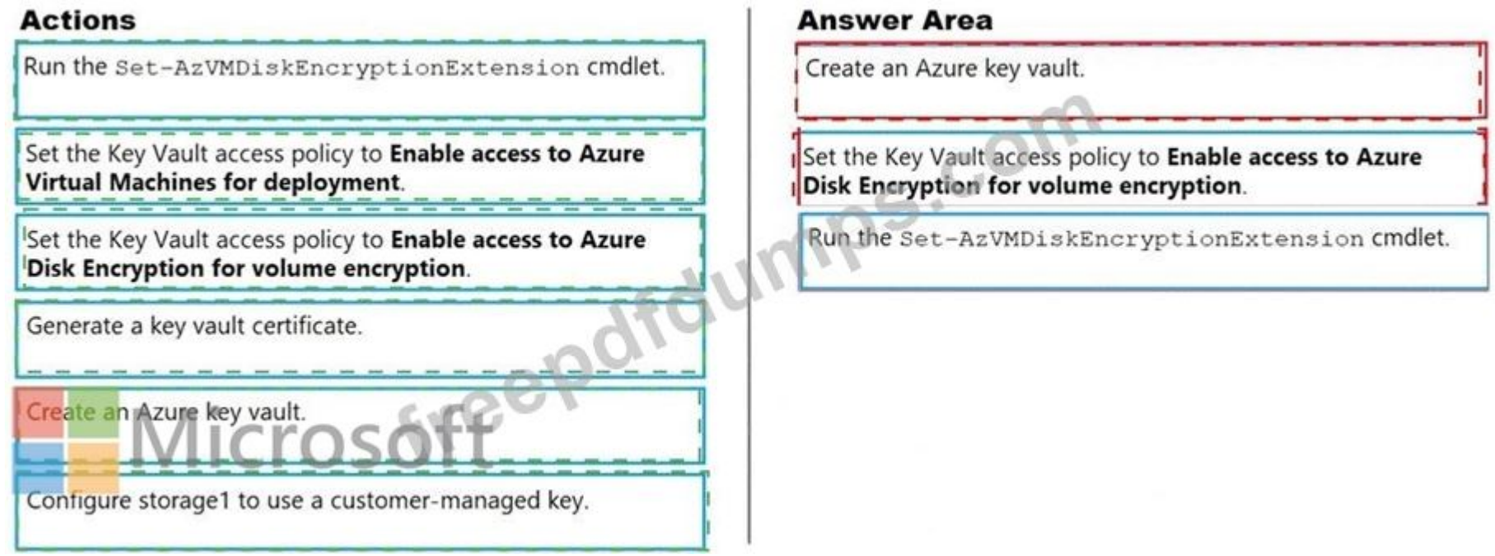
NEW QUESTION: 7
You have an Azure Storage account named storage1 and an Azure virtual machine named VM1. VM1 has a premium SSD managed disk.
You need to enable Azure Disk Encryption for VM1.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange then in the correct order.

Actions

- Run the `Set-AzVMDiskEncryptionExtension` cmdlet.
- Set the Key Vault access policy to **Enable access to Azure Virtual Machines for deployment**.
- Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption**.
- Generate a key vault certificate.
- Create an Azure key vault.
- Configure storage1 to use a customer-managed key.

Answer Area

Answer:



Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

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

NEW QUESTION: 8

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

Name	Type	Location
VM1	Virtual machine	East US
VNet1	Virtual network	East US
NSG1	Network security group (NSG)	East US
storage1	Storage account	West US

You need to configure network connectivity to meet the following requirements:

* Communication from VM1 to storage' must traverse an optimized Microsoft backbone network.
* All the outbound traffic from VM1 to the internet must be denied.
* The solution must minimize costs and administrative effort

What should you configure for VNetl and NSG1? To answer, drag the appropriate components to the correct resources. 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:

Explanation:

NEW QUESTION: 9

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have an Amazon Web Service (AWS) account named AWS1 that is connected to defender for Cloud.

You need to ensure that AWS foundational Security Best Practices. The solution must minimize administrate effort.

What should do you in Defender for Cloud?

A. Create a new custom standard.

B. Assign a built-in compliance standard.

C. Assign a built-in assessment.

D. Create a new customer assessment.

Answer: (SHOW ANSWER)

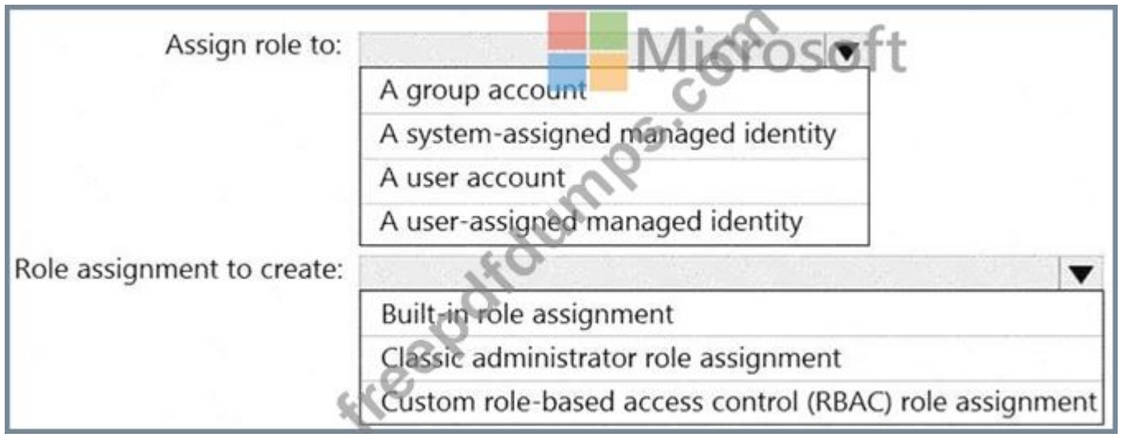
NEW QUESTION: 10

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

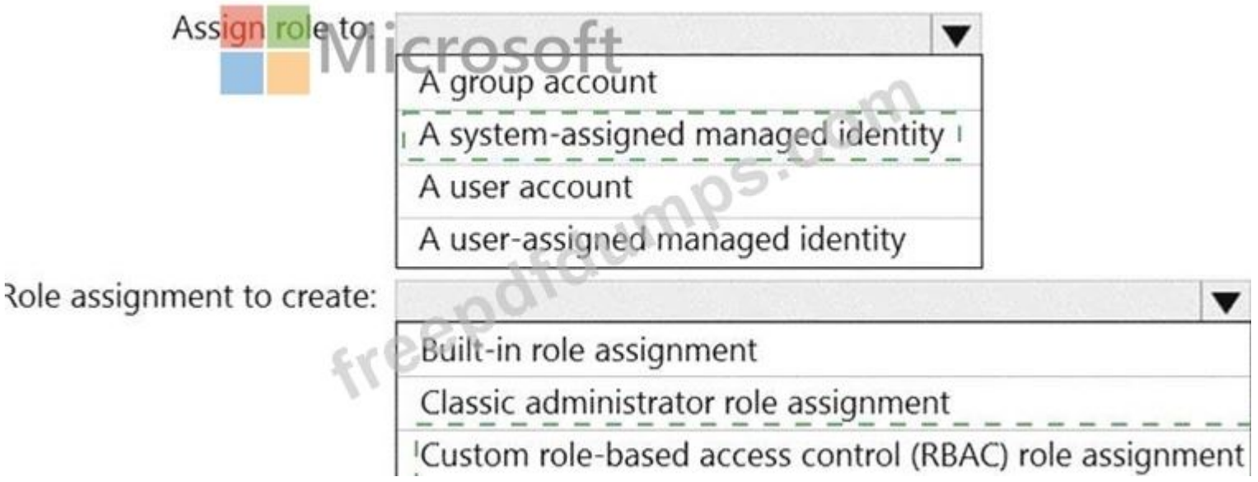
You need to grant Function1 the minimum required privileges to create the storage accounts. The solution must minimize administrative effort.

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

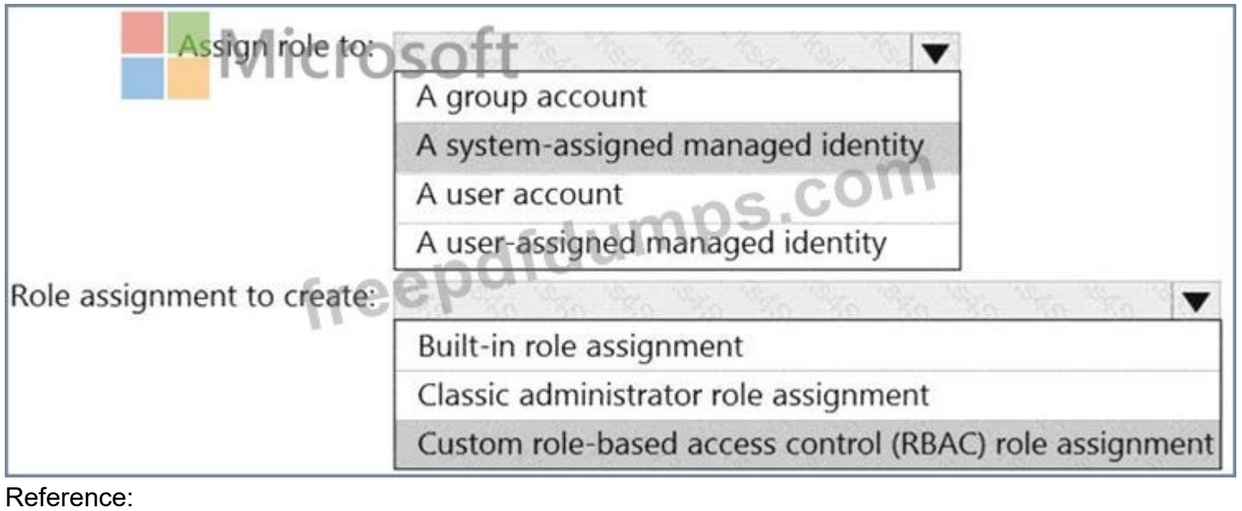
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

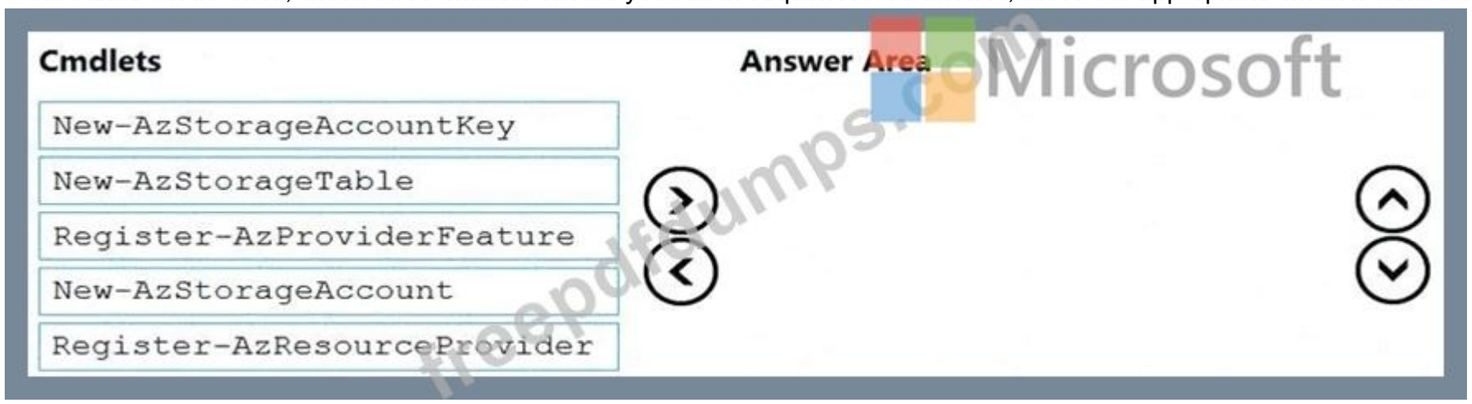


Reference:

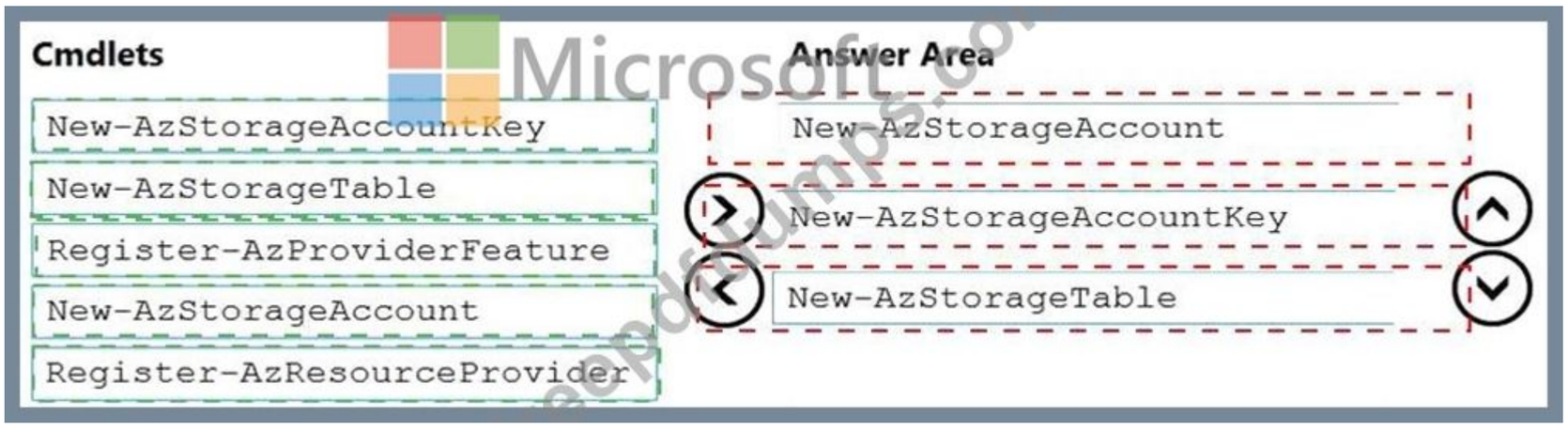
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

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

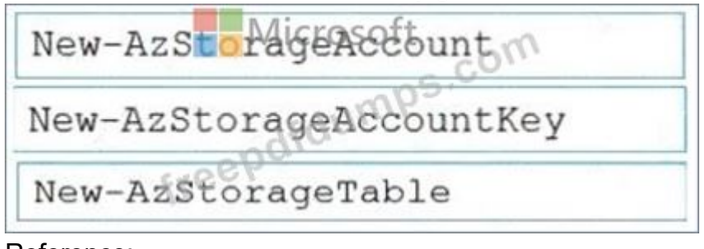
NEW QUESTION: 11
You have an Azure subscription.
You plan to create a storage account.
You need to use customer-managed keys to encrypt the tables in the storage account.
From Azure Cloud Shell, which three cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.



Answer:



Explanation:
Text, table Description automatically generated with medium confidence



Reference:
https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-key-vault?tabs=powershell

NEW QUESTION: 12
You have an Azure AD tenant.

You plan to implement an authentication solution to meet the following requirements:
* Require number matching.
* Display the geographical location when signing in.
Which authentication method should you include in the solution?
A. FID02 security key
B. SMS
C. Temporary Access Pass
D. Microsoft Authenticator
Answer: (SHOW ANSWER)

NEW QUESTION: 13
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)
References:
https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door

NEW QUESTION: 14
You have an Azure subscription. The subscription contains a virtual network named VNet1 that contains the subnets shown in the following table.

Name	Associated network security group (NSG)
Subnet1	NSG1
Subnet2	NSG1
Subnet3	NSG1
Subnet4	NSG1

The subscription contains the function apps shown in the following table.

Name	Description
App1	Uses the Azure Functions Premium plan and has virtual network integration with VNet1/Subnet1
App2	Uses an App Service plan in the Basic pricing tier and has virtual network integration with VNet1/Subnet2
App3	Uses an App Service plan in the Premium pricing tier and has virtual network integration with VNet1/Subnet3
App4	Uses an App Service plan in the Isolated pricing tier and is deployed to VNet1/Subnet4

The outbound traffic of which app is controlled by using NSG1?
A. App2, App3, and App4 only

B. App4 only
C. App3 and App4 only
D. App1, App2, App3, andApp4
Answer: D (LEAVE A REPLY)

NEW QUESTION: 15
You have an Azure subscription that uses Microsoft Defender for Cloud. The subscription contains an instance of Azure Database for PostgreSQL.
You need to ensure that an email alert is triggered when a suspected brute force attack on the database is detected. The solution must minimize administrative effort.
What should you configure?
A. an Azure Monitor alert rule
B. the Azure Monitor activity log
C. Microsoft Defender for open-source relational databases
D. the PostgreSQL Audit extension (pgAudit)
Answer: C (LEAVE A REPLY)

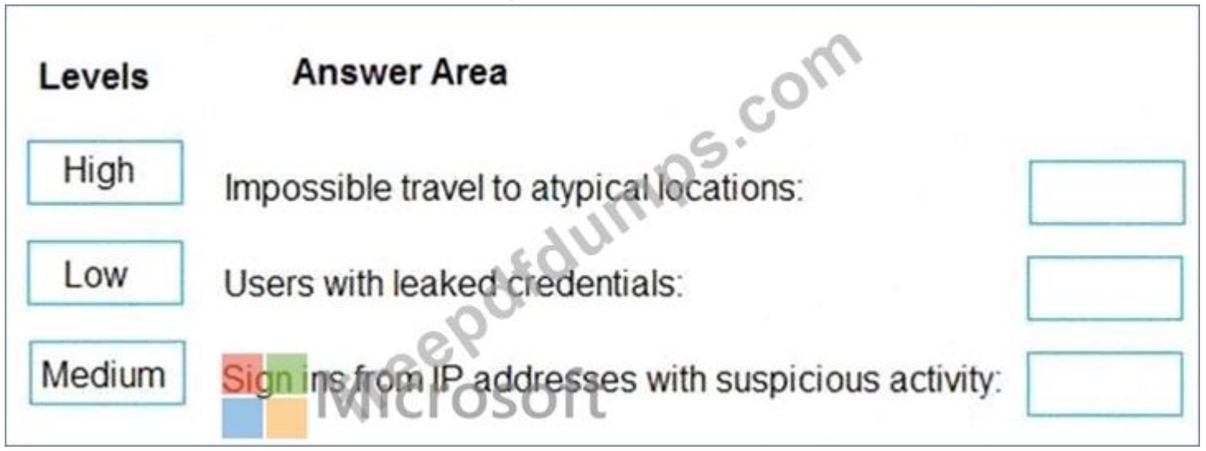
NEW QUESTION: 16
You have an Azure Active Din-dory (Azure AD) tenant named contoso.com that contains a user named User1.
You plan to publish several apps in the tenant.
You need to ensure that User1 can grant admin consent for the published apps.
Which two possible user roles can you assign to User! to achieve this goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. Application developer
B. Security administrator
C. Application administrator
D. User administrator
E. Cloud application administrator
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent

NEW QUESTION: 17
You are implementing conditional access policies.
You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.
You need to identify the risk level of the following risk events:
* Users with leaked credentials

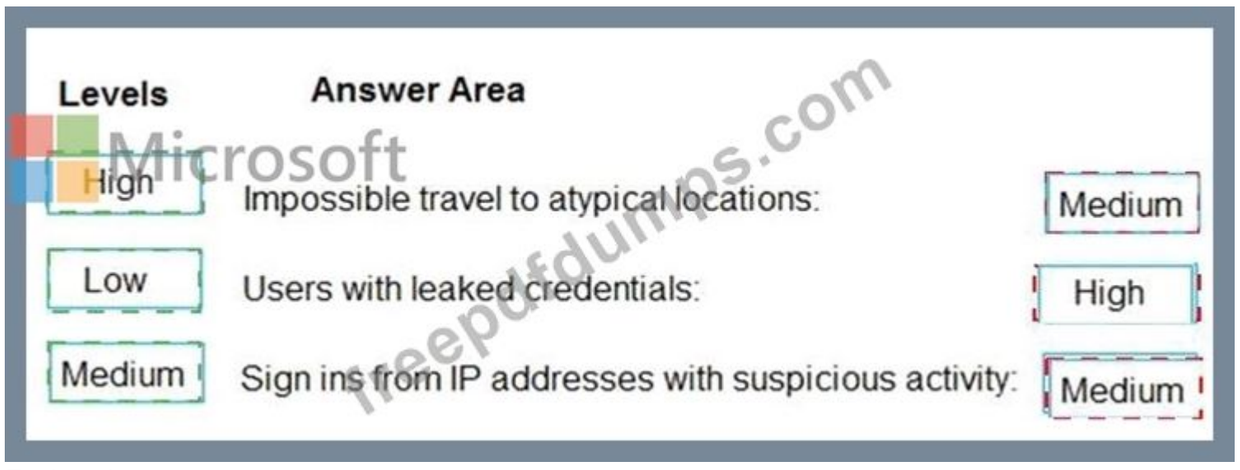
* Impossible travel to atypical locations
* Sign ins from IP addresses with suspicious activity

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

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Medium

High

Medium

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

NEW QUESTION: 18

You need to implement the planned change for VM1 to access storage1.

The solution must meet the technical requirements.

What should you do first?

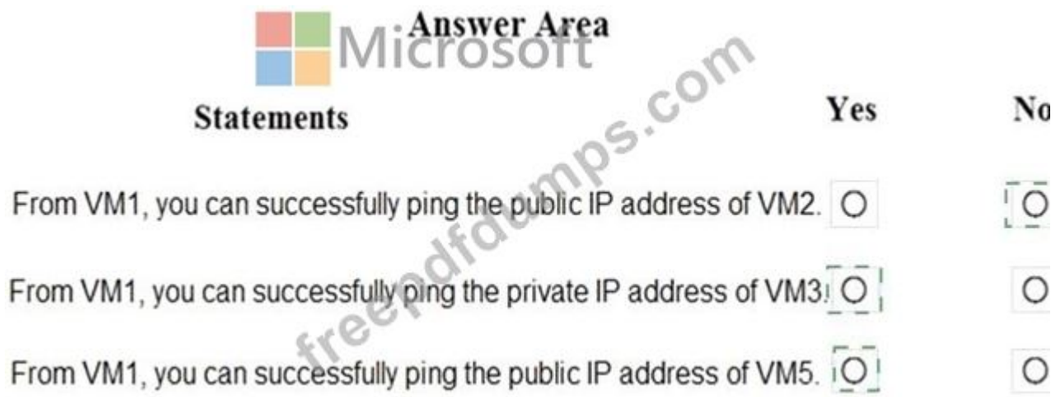
A. Assign ID1 to VM1.

B. Assign the Storage Blob Data Reader role to storage 1.

C. Configure a system-assigned managed identity on VM1.
D. Add a role assignment condition to storage1.
E. Configure federated identity credentials for ID1.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 19
You are evaluating the security of the network communication between the virtual machines in Sub2.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer:



Explanation:
Yes,
Yes
No

NEW QUESTION: 20
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 rout 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. Add an Azure Policy definition to the root management group.
B. Modify the role-based access control (RBAC) role assignments for the root management group.
C. Create a user-assigned identity.
D. Create a service principal.
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin

NEW QUESTION: 21
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.	○	○
You can add a new key named Item1.	○	○
You can add a new secret named Item2.	○	○

Answer:

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

Explanation:
NO. Policies cannot be recovered
YES, Item1 is permanently deleted
NO, You cannot use the same name cause Item2 is in Seoft-deleted status
https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview

NEW QUESTION: 22
You have an Azure subscription.
You plan to deploy a virtual machine named VM1.
You need to use confidential disk encryption on VM1.
Which virtual machine series should you use for VM1, and which type of disks can be encrypted by using confidential disk encryption? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION: 23

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

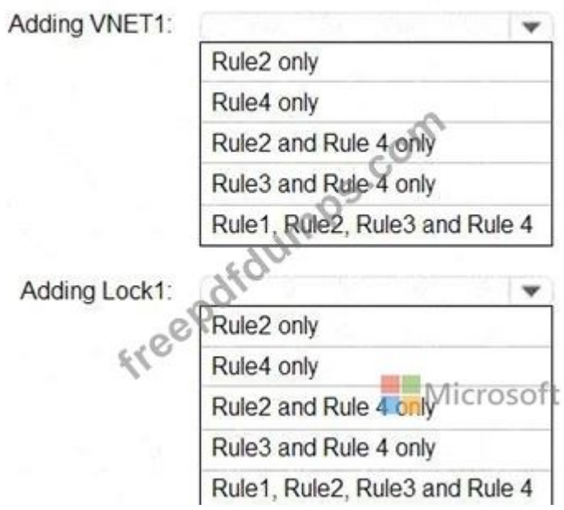
Admin1 performs the following actions on RG1:

* Adds a virtual network named VNET1

* Adds a Delete lock named Lock1

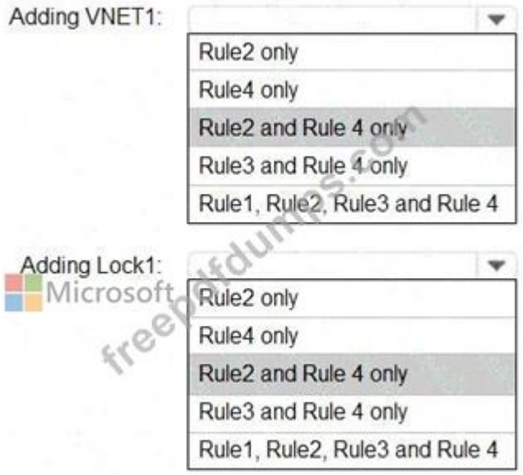
Which rules will trigger an alert as a result of the actions of Admin1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



NEW QUESTION: 24

You have an Azure subscription named Subscription1.

You need to view which security settings are assigned to Subscription1 by default.

Which Azure policy or initiative definition should you review?

A. the Audit diagnostic setting policy definition

B. the Enable Monitoring in Azure Security Center initiative definition

C. the Enable Azure Monitor for VMs initiative definition

D. the Azure Monitor solution 'Security and Audit' must be deployed policy definition

Answer: B (LEAVE A REPLY)

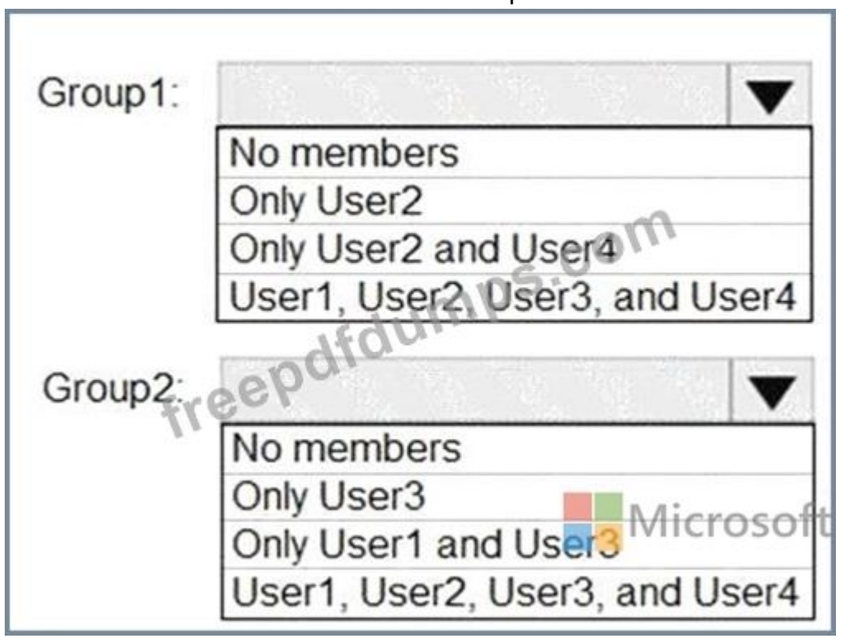
Reference:

https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy

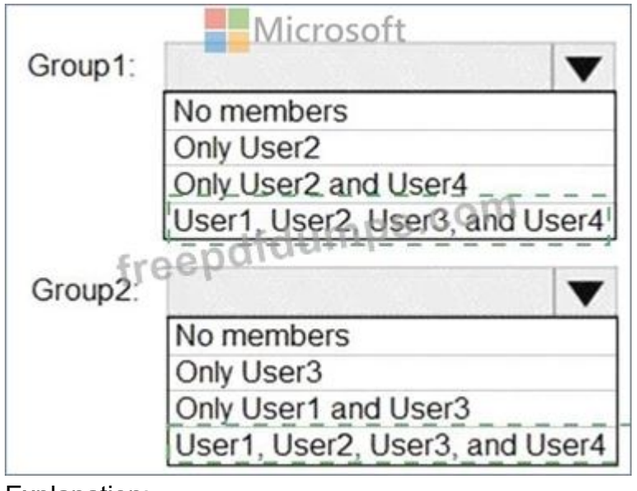
https://docs.microsoft.com/en-us/azure/security-center/policy-reference

NEW QUESTION: 25
You have an Azure subscription that contains an Azure web app named 1 and a virtual machine named VM1.
VM1 runs Microsoft SQL Server and is connected to a virtual network named VNet1. App1, VM1, and Vent are in the US Central Azure region.
You need to ensure that App1 can connect to VM1. The solution must minimize costs.
A. Azure Application Gateway integration
B. gateway-required virtual network integration
C. regional virtual network integration
D. NAT gateway integration
E. Azure Front Door
Answer: (SHOW ANSWER)

NEW QUESTION: 26
What is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Box 1: User1, User2, User3, User4

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

Box 2: User1, User2, User3, User4

References:

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

NEW QUESTION: 27

You have two Azure subscriptions named Sub1 and Sub2 that contain the virtual networks shown in the following table.

Name	Subscription	Location	Subnet
VNet1	Sub1	East US	Subnet1
VNet2	Sub2	East US	Subnet2
VNet3	Sub1	West US	Subnet3

You have an Azure Virtual Network Manager instance that has the following settings:

* Name: NetMgr1
* Region: East US
* Features: Connectivity
* Management scope: Sub1

For NetMgr1, you create the target network groups shown in the following table.

Name	Member type	Group member
Group1	Virtual network	VNet1
Group2	Virtual network	*None*
Group3	Subnet	*None*

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 add VNet1 to Group2.	○	○
You can add VNet2 to Group1.	○	○
You can add Subnet3 to Group3.	○	○

Answer:

Explanation:

NEW QUESTION: 28

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

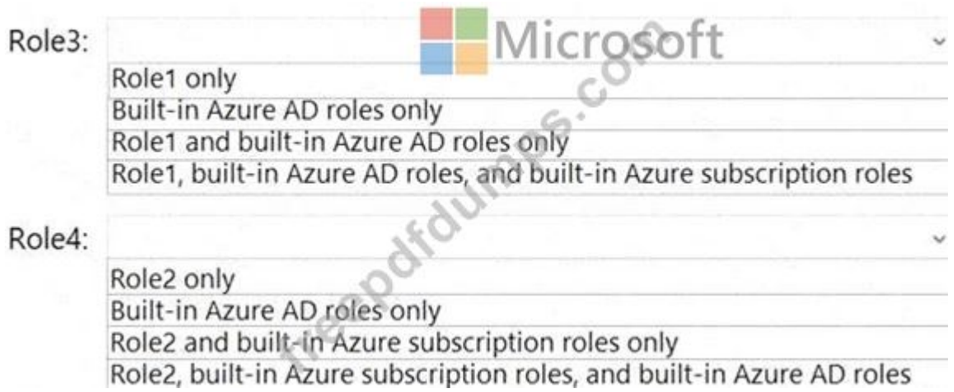
Name	Type
Role1	Azure Active Directory (Azure AD)
Role2	Azure subscription

In the Azure portal, you plan to create new custom roles by cloning existing roles. The new roles will be configured as shown in the following table.

Name	Type
Role3	Azure AD
Role4	Azure subscription

Which roles can you clone to create each new role? To answer, select the appropriate options in the answer area.

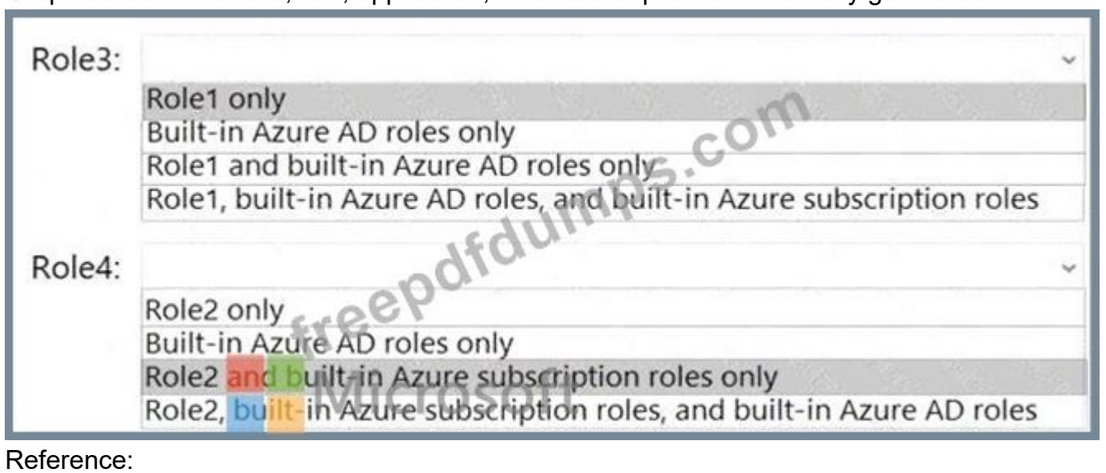
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Graphical user interface, text, application, email Description automatically generated



Reference:

https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-create

https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal

NEW QUESTION: 29

You need to implement the planned change for WAF1.

The solution must minimize administrative effort
What should you do?
A. Modify the Azure-managed DRS.
B. Create an Azure policy.
C. Add a custom rule.
D. Modify the Bot Manager 1.1 rule set.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 30
You have an Azure subscription that contains the storage accounts shown in the following, table.

Name	Performance	Account kind	Azure Data Lake Storage Gen2
storage1	Standard	BlobStorage	Enabled
storage2	Premium	BlockBlobStorage	Disabled
storage3	Standard	Storage	Disabled
storage4	Premium	FileStorage	Disabled
storage5	Standard	StorageV2	Enabled

You enable Microsoft Defender for Storage.
Which storage services of storages are monitored by Microsoft Defender for Storage, and which storage accounts are protected by Microsoft Defender for Storage? To answer, select the appropriate options in the answer area.

Answer:
see the answer below in explanation.
Explanation:
Answer as below.

NEW QUESTION: 31
You have an Azure subscription and the computers shown in the following table.

Name	Operating system	Description
VM1	Windows Server 2012 R2	Azure virtual machine
VM2	Red Hat Enterprise Linux (RHEL) 8.2	Azure virtual machine
Server1	Windows Server 2019	On-premises physical computer connected to Microsoft Defender for Cloud
VMSS1_0	Windows Server 2022	Azure virtual machine in a virtual machine scale set

You need to perform a vulnerability scan of the computers by using Microsoft Defender for Cloud. Which computers can you scan?

A. VM1 only
B. Server1 and VMSS1.0 only
C. VM1 and VM2 only
D. VM1, VM2, and Server1 only
E. VM1, VM2, Server1, and VMSS1.0
Answer: D (LEAVE A REPLY)

NEW QUESTION: 32
You have an Azure subscription that contains a virtual network named VNet1 VNet1 contains a single subnet.
The subscription contains a virtual machine named VM1 that is connected to VNet1.
You plan to deploy an Azure SQL managed instance named SQL1.
You need to ensure that VM1 can access SQL1.
Which three components should you create? Each correct answer presents pan of the solution.
NOTE: Each correct selection is worth one point.
A. a virtual network gateway
B. a network security group (NSG)
C. a network security perimeter
D. a route table
E. a subnet
Answer: B,D,E (LEAVE A REPLY)

NEW QUESTION: 33
You have an Azure subscription that contains an Azure App Services web app named WebApp1 and an Azure key vault named Vault1. Vault1 has the certificates shown in the following table.

Name	Content type	Key type	Key size
Cert1	PKCS #12	RSA	2048
Cert2	PKCS #12	RSA	4096
Cert3	PEM	RSA	2048
Cert4	PEM	RSA	4096

You plan to implement TLS for WebApp1.
You need to add a certificate to WebApp1.
Which certificates from Vault1 can you add to WebApp1?
A. Cert1 and Cert3 only
B. Cert1 and Cert2 only
C. Cert3 and Cert4 only
D. Cert1, Cert2, Cert3, and Cert4
Answer: B (LEAVE A REPLY)

NEW QUESTION: 34
You need to ensure that User2 can implement PIM.
What should you do first?
A. Assign User2 the Global administrator role.
B. Configure authentication methods for contoso.com.
C. Configure the identity secure score for contoso.com.
D. Enable multi-factor authentication (MFA) for User2.
Answer: (SHOW ANSWER)
To start using PIM in your directory, you must first enable PIM.
1. Sign in to the Azure portal as a Global Administrator of your directory.
You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.
Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com References:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting- started
Topic 3, Fabrikam inc
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
General Overview
Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.
Existing Environment

Network Environment

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

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

The Azure resources hierarchy is shown in the following exhibit.

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

Name	Type	Directory-synced	Role	Delegated to
User1	User	Yes	User	**None**
Admin1	User	No	User Access Administrator	Tenant Root Group
Admin2	User	No	Security administrator	MG1
Admin3	User	No	Contributor	Subscription1
Admin4	User	No	Owner	RG1
Group1	Group	No	**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 tor	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.

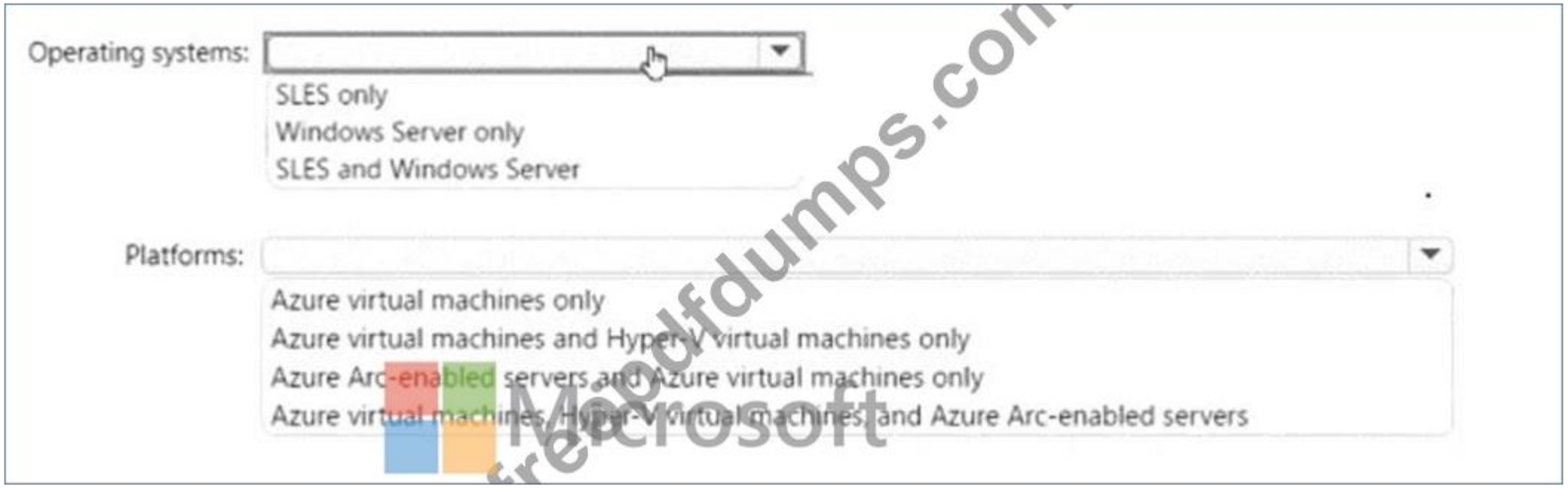
KeyVault1 traffic must NOT travel over the internet.

NEW QUESTION: 35

Your on-premises network contains the servers shown in the following table.

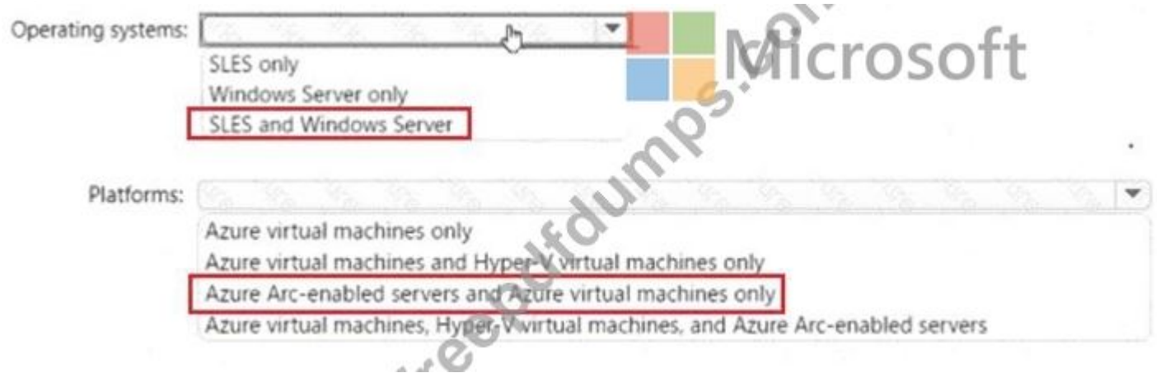
Name	Operating system	Description
Server1	Windows Server 2019	Hyper-V host hosting four virtual machines that run Windows Server 2022
Server2	Windows Server 2019	File server that has the Azure Arc agent installed
Server3	SUSE Linux Enterprise Server (SLES)	Database server that has the Azure Arc agent installed

You have an Azure subscription That contains multiple virtual machines that run either Windows Server 2019 Of SLES.



Answer:

Explanation:



NEW QUESTION: 36

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

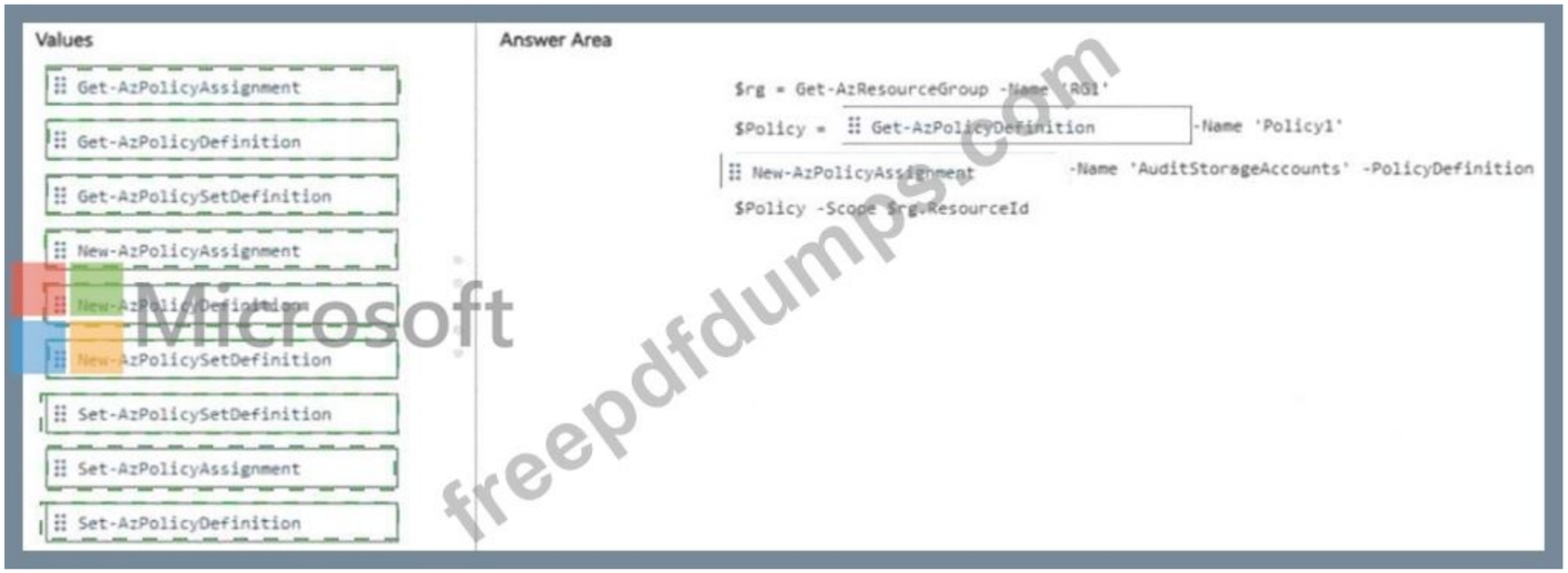
A. Azure Monitor

B. Azure Cosmos DB explorer

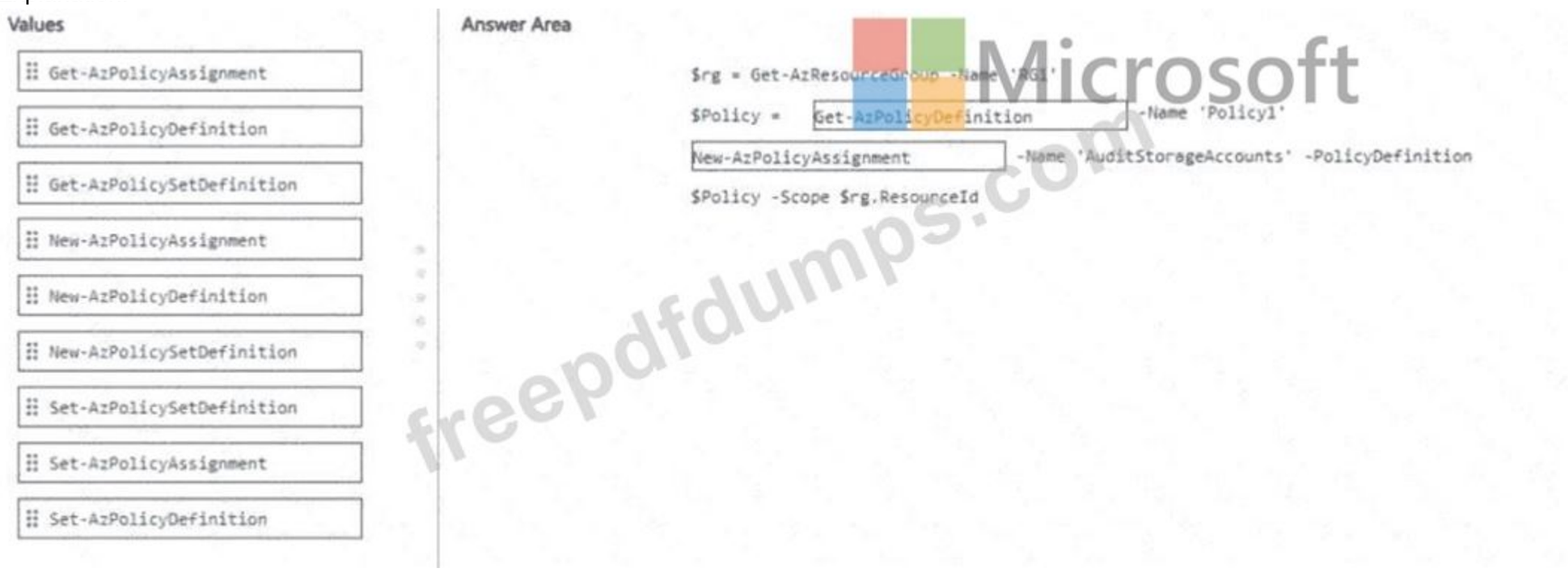
C. SQL query editor in Azure
D. Azure Storage Explorer
Answer: (SHOW ANSWER)

NEW QUESTION: 37
You have an Azure subscription that contains a resource group named RG1 and an Azure policy named Policy1.
You need to assign Policy1 to RG1.
How should you complete the script? To answer, drag the appropriate values to the correct targets. Each value 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:



NEW QUESTION: 38

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

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

You use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create an initiative and an assignment that is scoped to the Tenant Root Group management group.

Does this meet the goal?

A. Yes

B. No

Answer: A (LEAVE A REPLY)

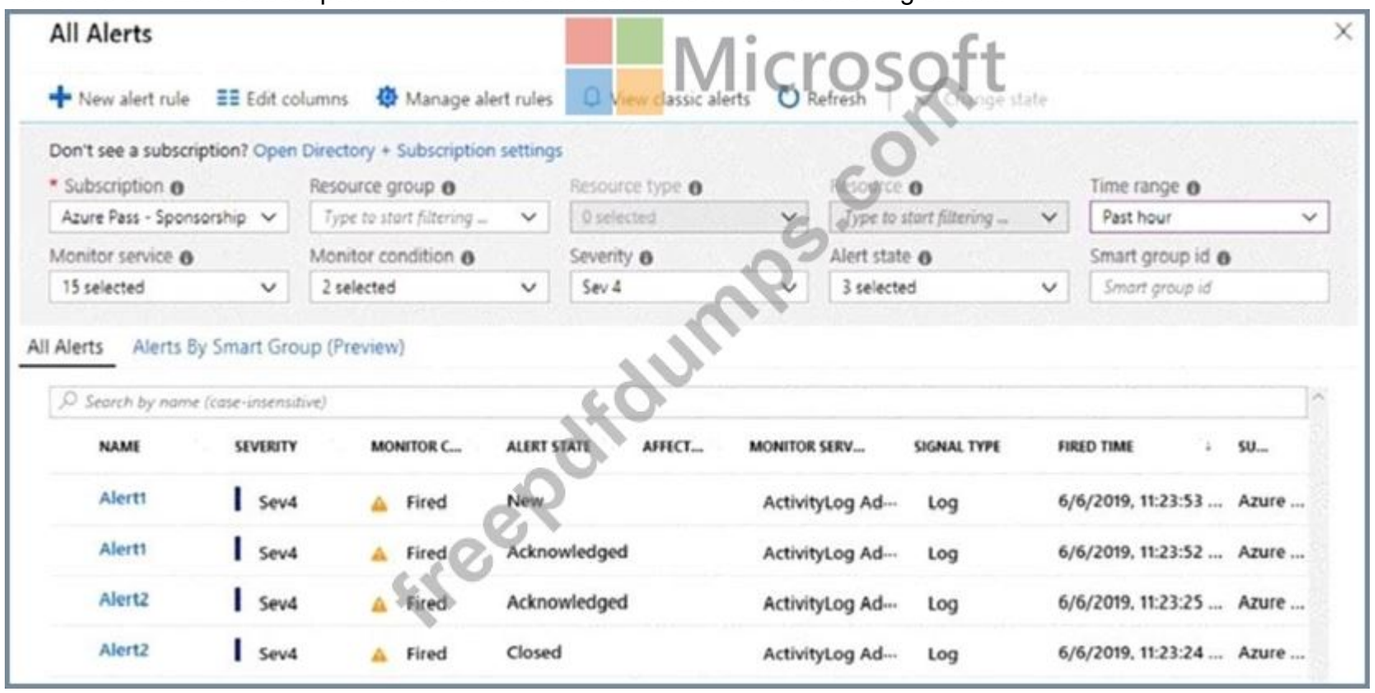
Reference:

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

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

NEW QUESTION: 39

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



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

NOTE: Each correct selection is worth one point.

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

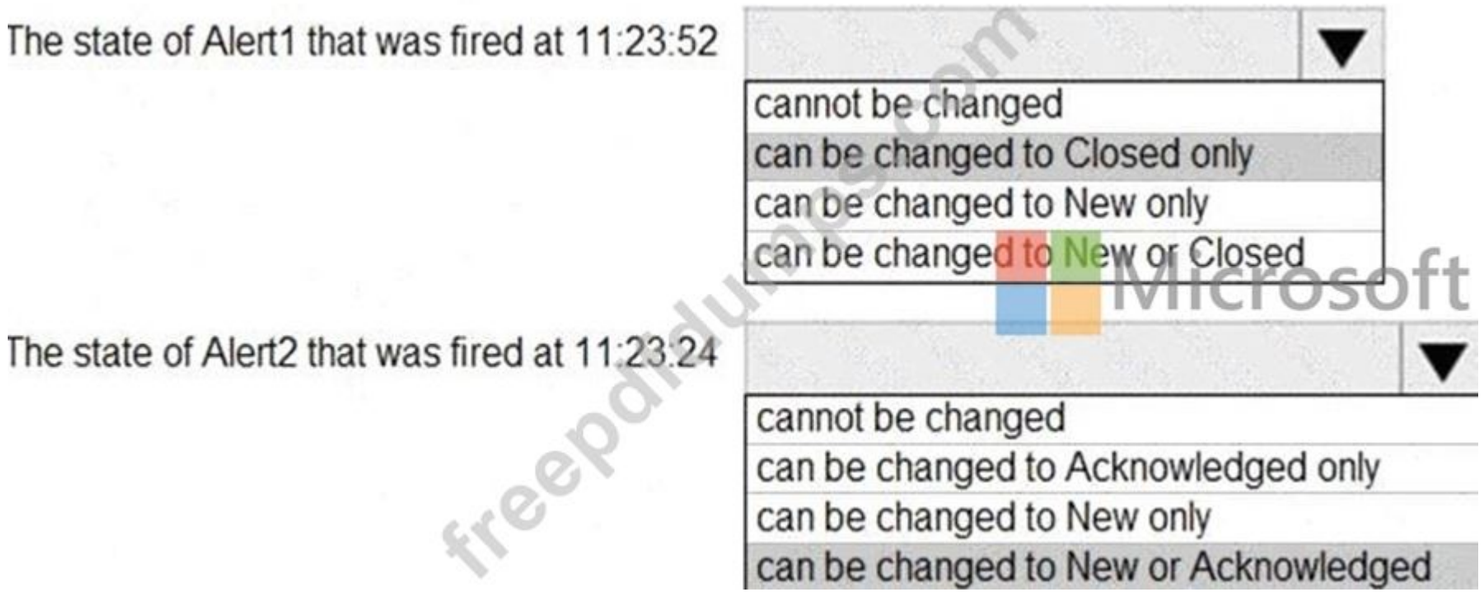
- cannot be changed
- can be changed to Closed only
- can be changed to New only
- can be changed to New or Closed

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

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

Answer:

Explanation:



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

NEW QUESTION: 40
You have an Azure subscription that contains the resources shown in the following table.

Name	Type
storage1	Storage account
Vault1	Azure Key vault
Vault2	Azure Key vault

You plan to deploy the virtual machines shown in the following table.

Name	Role
VM1	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1
VM2	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1
VM3	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1 • Key Vault Reader for Vault2
VM4	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1 • Key Vault Reader for Vault2

You need to assign managed identities to the virtual machines. The solution must meet the following requirements:

* Assign each virtual machine the required roles.

* Use the principle of least privilege.

What is the minimum number of managed identities required?

A. 1

B. 2

C. 3

D. 4

Answer: B (LEAVE A REPLY)

We have two different sets of required permissions. VM1 and VM2 have the same permission requirements.

VM3 and VM4 have the same permission requirements.

A user-assigned managed identity can be assigned to one or many resources. By using user-assigned managed identities, we can create just two managed identities: one with the permission requirements for VM1 and VM2 and the other with the permission requirements for VM3 and VM4.

Reference:

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

NEW QUESTION: 41

You have an Azure subscription named Subscription1 that contains a resource group named RG1 and the users shown in the following table.

Name	User principal name (UPN)	Type
User1	User1@outlook.com	Guest
User2	User2@outlook.com	Guest

You perform the following tasks:

* Assign User1 the Network Contributor role for Subscription1.

* Assign User2 the Contributor role for RG1.

To Subscription1 and RG1, you assign the following policy definition: External accounts with write permissions should be removed from your subscription.

What is the Compliance State of the policy assignments?

A. The Compliance State of both policy assignments is Non-compliant.

B. The Compliance State of the policy assignment to Subscription1 is Non-compliant, and the Compliance State of the policy assignment to RG1 is Compliant.

C. The Compliance State of both policy assignments is Compliant.

D. The Compliance State of the policy assignment to Subscription1 is Compliant, and the Compliance State of the policy assignment to RG1 is Non-compliant.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 42
You need to meet the technical requirements for VNetwork1.
What should you do first?
A. Create a new subnet on VNetwork1.
B. Remove the NSGs from Subnet11 and Subnet13.
C. Associate an NSG to Subnet12.
D. Configure DDoS protection for VNetwork1.
Answer: A (LEAVE A REPLY)
From scenario: Deploy Azure Firewall to VNetwork1 in Sub2.
Azure firewall needs a dedicated subnet named AzureFirewallSubnet.
References:
https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal

NEW QUESTION: 43
You have an Azure subscription named Sub1 that contains the resource groups shown in the following table.

Name	Location
RG1	West US
RG2	East US

You create the Azure Policy definition shown in the following exhibit.

You assign the policy to Sub1.
You plan to create the resources shown in the following table.

Name	Type	Location	Resource group
IPobject1	Public IP address	East US	RG2
obj1	Resource group	West US	*Not applicable*
OBJ3	Virtual network	West US	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.

Answer:

Explanation:

NEW QUESTION: 44

You have an Azure subscription that uses Microsoft Defender for Cloud.

You need to use Defender for Cloud to review regulatory compliance with the Azure CIS 1.4,0 standard. The solution must minimize administrative effort.

What should you do first?

A. Add a custom initiative.

B. Manually add the Azure CIS 1.4.0 standard.

C. Assign an Azure policy.

D. Disable one of the Out of the box standards.

Answer: (SHOW ANSWER)

NEW QUESTION: 45

You have an Azure subscription that contains a virtual machine named VM1.

You create an Azure key vault that has the following configurations:

* Name: Vault5

* Region: West US

* Resource group: RG1

You need to use Vault5 to enable Azure Disk Encryption on VM1. The solution must support backing up VM1 by using Azure Backup.

Which key vault settings should you configure?

A. Access policies

B. Secrets
C. Keys
D. Locks
Answer: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

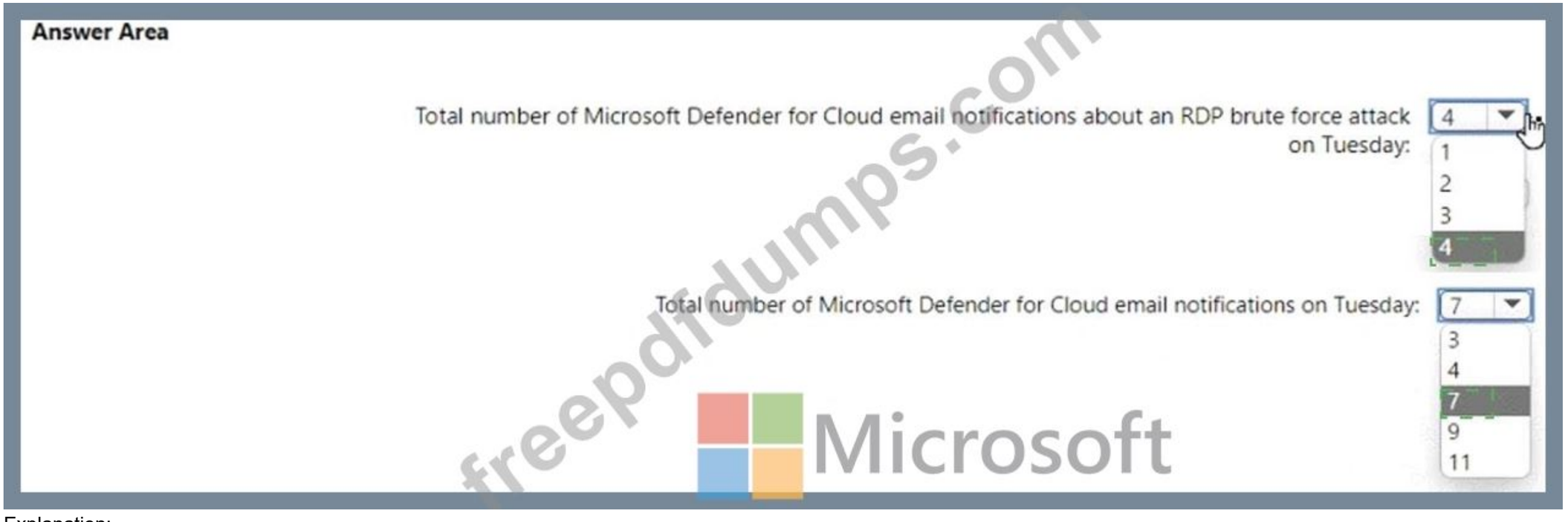
NEW QUESTION: 46
On Monday, you configure an email notification in Microsoft Defender for Cloud to notify user1 @contoso.
com about alerts that have a severity level of Low, Medium, or High. On Tuesday, Microsoft Defender for Cloud generates the security alerts shown in the following table.

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.

Answer Area

Answer:



Explanation:

NEW QUESTION: 47

You have an Azure subscription that contains a storage account named contoso2023. You need to perform the following tasks:

* Verify that identity-based authentication over SMB is enabled.
* Only grant users access to contoso2023 in the year 2023.

Which two settings should you use? To answer, select the appropriate settings in the answer area NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Answer Area

Explanation:

A screenshot of a computer Description automatically generated

Requirement: Verify that identity-based authentication over SMB is enabled Go there to configure Identity-based authentication (Active Directory) for Azure file shares.

Ref: https://learn.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview

2. Share access signature

Requirement: Only grant users access to contoso2023 in the year 2023

NEW QUESTION: 48

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	10.1.1.5	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

You have an Azure Cosmos DB account named cosmos1 configured as shown in the following exhibit.

Answer:

Explanation:

Yes, Yes, No

NEW QUESTION: 49

You have an Azure subscription that contains an Azure SQL database named DB1 in the East US Azure region. You create the storage accounts shown in the following table.

Name	Location	Performance	Premium account type
storage1	East US	Standard	*Not applicable*
storage2	East US	Premium	Block blobs
storage3	East US	Premium	File shares
storage4	East US 2	Standard	*Not applicable*

You plan to enable auditing for DB1.

Which storage accounts can you use as the auditing destination for DB1?

A. storage1 and storage4 only

B. Storage2 and storage3 only

C. storage1, storage2 and storage3 only

D. storage1 only

Answer: B (LEAVE A REPLY)

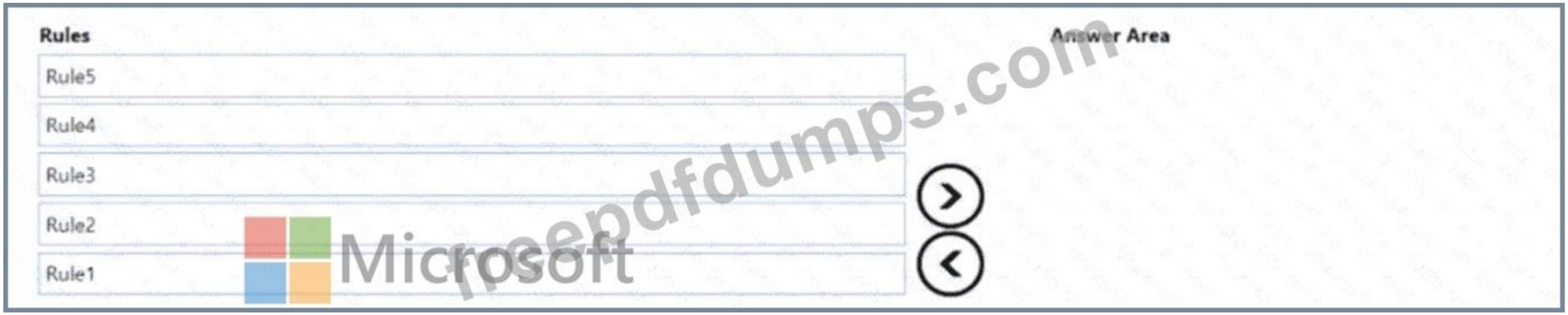
NEW QUESTION: 50

You have an Azure subscription.

You create an Azure Firewall policy that has the rules shown in the following table:

Name	Type	Priority
Rule1	Application rule collection	100
Rule2	NAT rule collection	200
Rule3	Network rule collection	300
Rule4	NAT rule collection	400
Rule5	Network rule collection	500

In which order should the rules be processed? To answer, move all rules from the list of rules to the answer area and arrange them in the correct order.



Answer:

Explanation:

The rules should be processed in the following order:

* Rule1: This is a network rule collection with the lowest priority (100). It allows any protocol and port from any source to any destination.
* Rule2: This is a NAT rule collection with the second lowest priority (200). It translates the source IP address of VM1 to a public IP address when it accesses the internet.
* Rule3: This is an application rule collection with the third lowest priority (300). It allows HTTP and HTTPS traffic from any source to any destination.
* Rule4: This is an application rule collection with the fourth lowest priority (400). It blocks HTTP and HTTPS traffic from any source to www.contoso.com.
* Rule5: This is a network rule collection with the highest priority (500). It blocks ICMP traffic from any source to any destination.

The rules are processed from the lowest priority to the highest priority. If a rule matches the traffic, it is applied and no further rules are evaluated. If no rule matches the traffic, it is denied by default.

NEW QUESTION: 51
You have an Azure subscription.
You plan to implement Azure DDoS Protection. The solution must meet the following requirement:
* Provide access to DDoS rapid response support during active attacks.
* Project Basic SKU public IP addresses.
You need to recommend which type of DDoS projection to use for each requirement.
What should you recommend? To answer, drag the appropriate DDoS projection types to the correct requirements. Each DDoS Projection type may be used once, or not at all. You may need to drag the split bar between panes or scroll to view connect.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION: 52
You have an Azure subscription that contains the virtual machines shown in the following table.

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

You create the Azure policies shown in the following table.

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

You create the resource locks shown in the following table.

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

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

NOTE: Each correct selection is worth one point.

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

Answer:

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

Explanation:

NO

NO

NO

1.) cannot perform write operation because following scope(s) are locked:

' subscriptions/xxxx/resourceGroups/xxx ' Please remove the lock and try again.

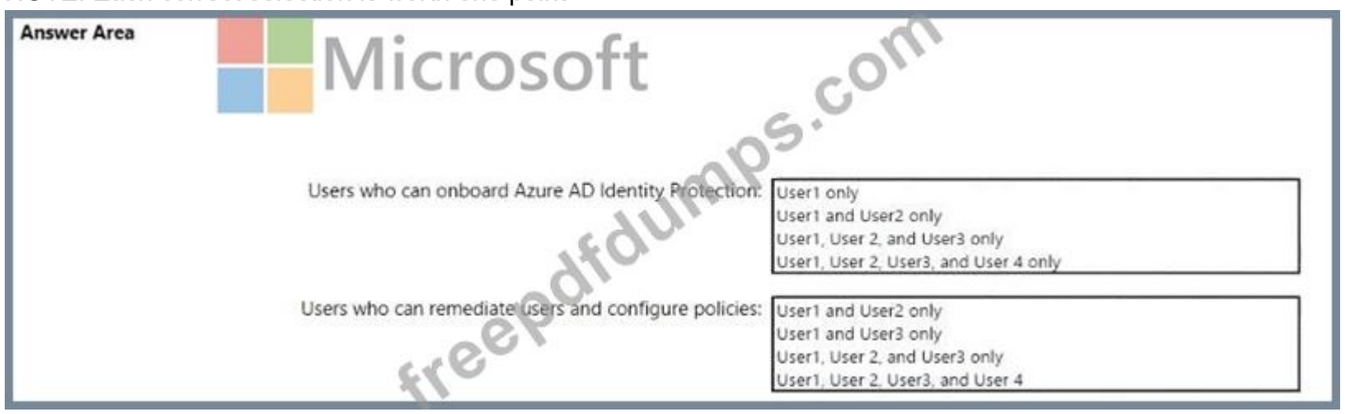
2.) When creating a VM in a resource group with a Read Only lock an error is shown:
" The selected resource group is read only "
3.) Because of the read only lock virtual machines cannot be started nor stopped when the lock is added after the machine started. (not part of this use case, but still good to know.
The article referenced in the answer states different because that is scoped to blueprints.
In the Lock Resources pages is states the following regarding starting VMs:
" A ReadOnly lock on a resource group that contains a virtual machine prevents all users from starting or restarting the virtual machine. These operations require a POST request. "
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

NEW QUESTION: 53
You have an Azure Active Directory (Azure AD) tenant.
You need to prevent nonprivileged Azure AD users from creating service principals in Azure AD.
What should you do in the Azure Active Directory admin center of the tenant?
A. From the User settings blade, set Users can register applications to No
B. From the User settings blade, set Restrict access to Azure AD administration portal to Yes.
C. From the Properties blade, set Access management fen Azure resources to No
D. From the Properties Wade, set Enable Security defaults to Yes.
Answer: A (LEAVE A REPLY)

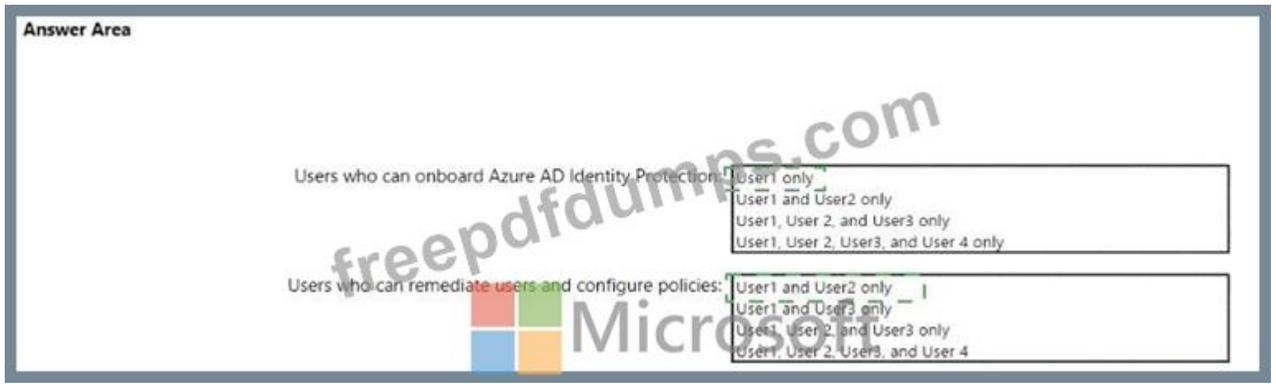
NEW QUESTION: 54
You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

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

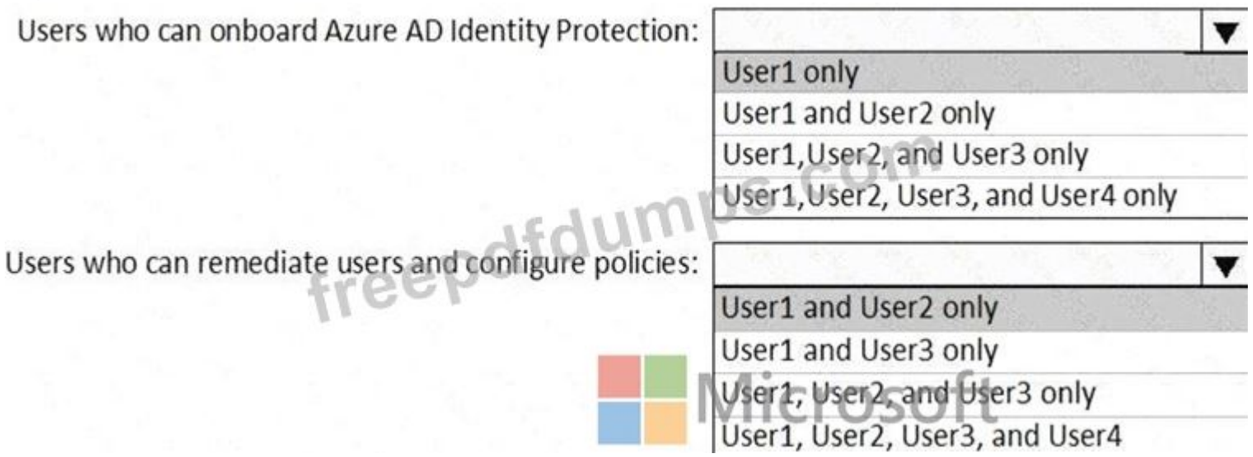
Each user is assigned an Azure AD Premium P2 license.
You plan lo onboard and configure Azure AD identity Protection.
Which users can onboard Azure AD Identity Protection, remediate users, and configure policies? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point



Answer:



Explanation:

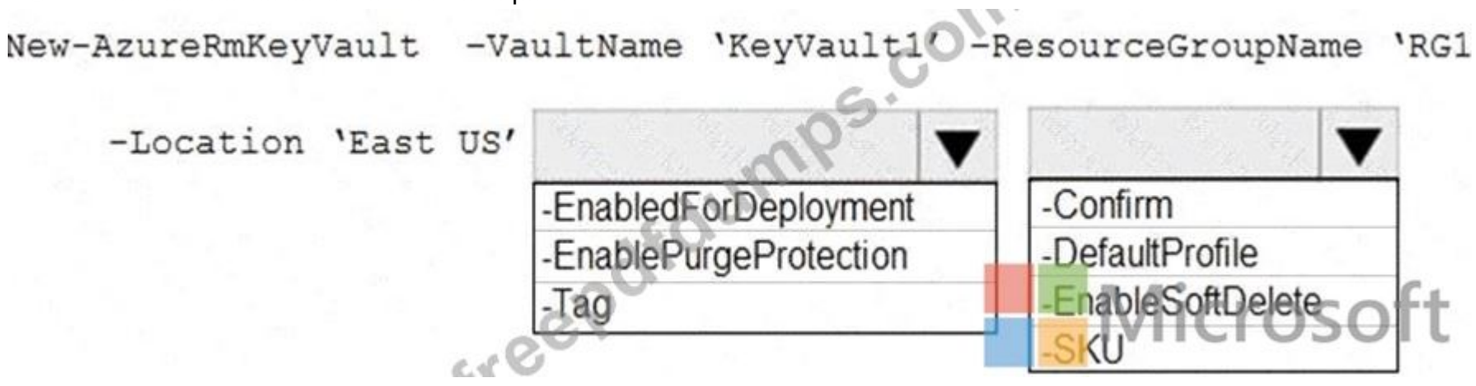


NEW QUESTION: 55

You need to create an Azure key vault. The solution must ensure that any object deleted from the key vault be retained for 90 days.

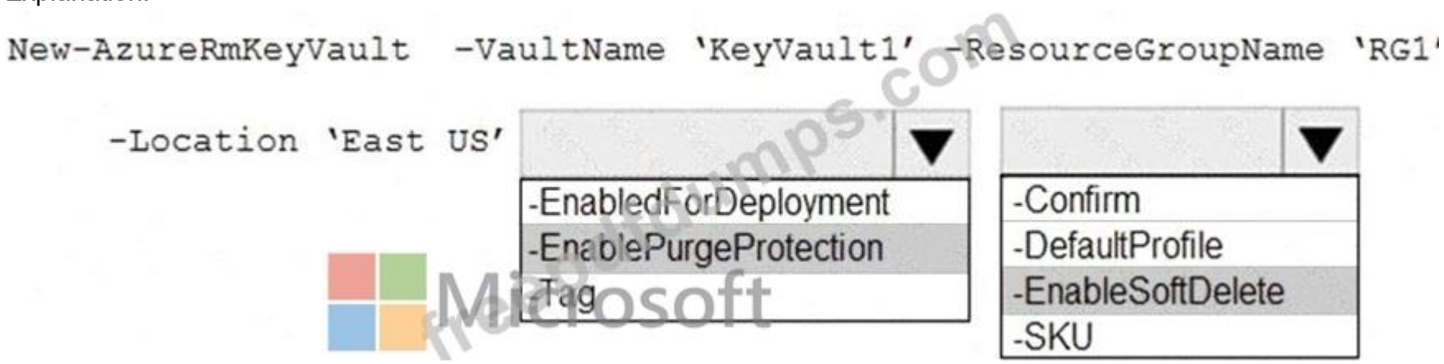
How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Box 1: -EnablePurgeProtection

If specified, protection against immediate deletion is enabled for this vault; requires soft delete to be enabled as well.

Box 2: -EnableSoftDelete

Specifies that the soft-delete functionality is enabled for this key vault. When soft-delete is enabled, for a grace period, you can recover this key vault and its contents after it is deleted.

References:

https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault

NEW QUESTION: 56

You have an Azure subscription that contains an Azure Key Vault Standard key vault named Vault1. Vault1 hosts a 2048-bit RSA key named key1.

You need to ensure that key1 is rotated every 90 days.

What should you do first?

A. Recreate key1 as an EC key.

B. Create a key rotation policy.

C. Upgrade Vault1 to Key Vault Premium.

D. Modify the Access policies settings of Vault1.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 57

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

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

You have a hybrid configuration of Azure Active Directory (AzureAD).

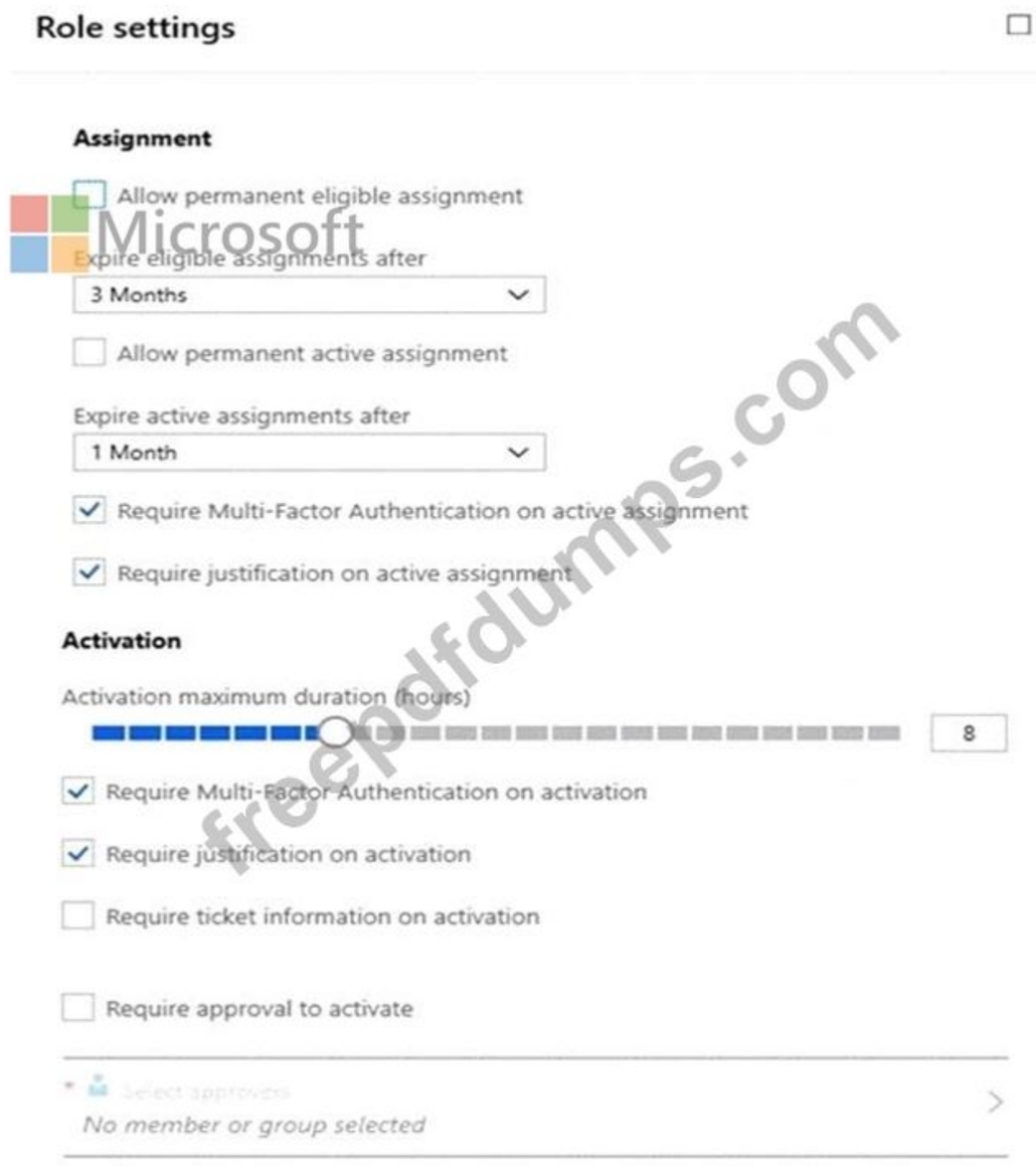
You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.
You need to configure the environment to support the planned authentication.
Solution: You deploy the On-premises data gateway to the on-premises network.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:
Create Azure Virtual Network.
Create a custom DNS server in the Azure Virtual Network.
Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
Configure forwarding between the custom DNS server and your on-premises DNS server.
References:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

NEW QUESTION: 58
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

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

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



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

Name	Assignment type
User1	Eligible
User2	Active
User3	Active

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
On May 15, 2019, User1 can activate the Contributor role.	○	○
On May 15, 2019, User2 can use the Contributor role.	○	○
On June 15, 2019, User3 can activate the Contributor role.	○	○

Answer:

Statements	Yes	No
On May 15, 2019, User1 can activate the Contributor role.	○	○
On May 15, 2019, User2 can use the Contributor role.	○	○
On June 15, 2019, User3 can activate the Contributor role.	○	○

Explanation:

Statements	Yes	No
On May 15, 2019, User1 can activate the Contributor role.	○	○
On May 15, 2019, User2 can use the Contributor role.	○	○
On June 15, 2019, User3 can activate the Contributor role.	○	○

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

NEW QUESTION: 59
You have an Azure subscription that contains the following Azure firewall:
* Name: Fw1

* Azure region: UK West
* Private IP address: 10.1.3.4
* Public IP address: 23.236.62.147

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

Name	Location	IP address space	Peered with
Vnet1	UK West	10.1.0.0/16	Vnet2
Vnet2	East US	10.2.0.0/16	Vnet1, Vnet3
Vnet3	West US	10.3.0.0/16	Vnet2,

The subscription contains the subnets shown in the following table.

Name	Virtual network	IP address range
Subnet1-1	Vnet1	10.1.1.0/24
Subnet1-2	Vnet1	10.1.2.0/24
AzureFirewallSubnet	Vnet1	10.1.3.0/24
Subnet2-1	Vnet2	10.2.1.0/24
Subnet3-1	Vnet3	10.3.1.0/24

The subscription contains the routes shown in the following table.

Name	Subnet	IP address prefix	Next hop type	Next hop IP address
Rt1	Subnet1-1	0.0.0.0/0	Virtual appliance	10.1.3.4
Rt2	Subnet1-2	10.1.1.0/24	Virtual appliance	10.1.3.4
Rt3	Subnet2-1	10.1.1.0/24	Virtual appliance	10.1.3.4
Rt4	Subnet3-1	10.2.1.0/24	Virtual appliance	10.1.3.4

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

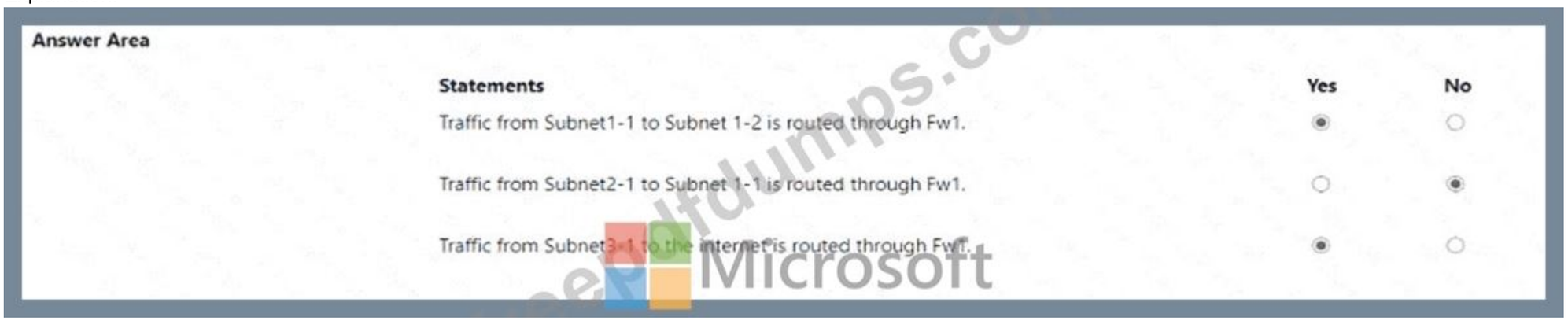
Statements	Yes	No
Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1.	○	○
Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1.	○	○
Traffic from Subnet3-1 to the internet is routed through Fw1.	○	○

Answer:

Answer Area

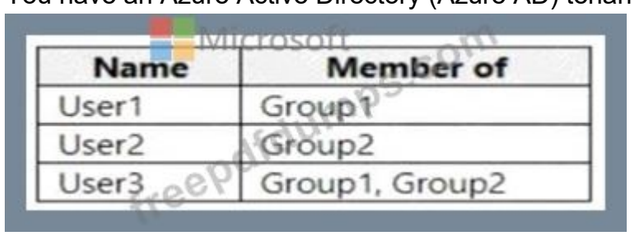
Statements	Yes	No
Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1.	○	○
Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1.	○	○
Traffic from Subnet3-1 to the internet is routed through Fw1.	○	○

Explanation:



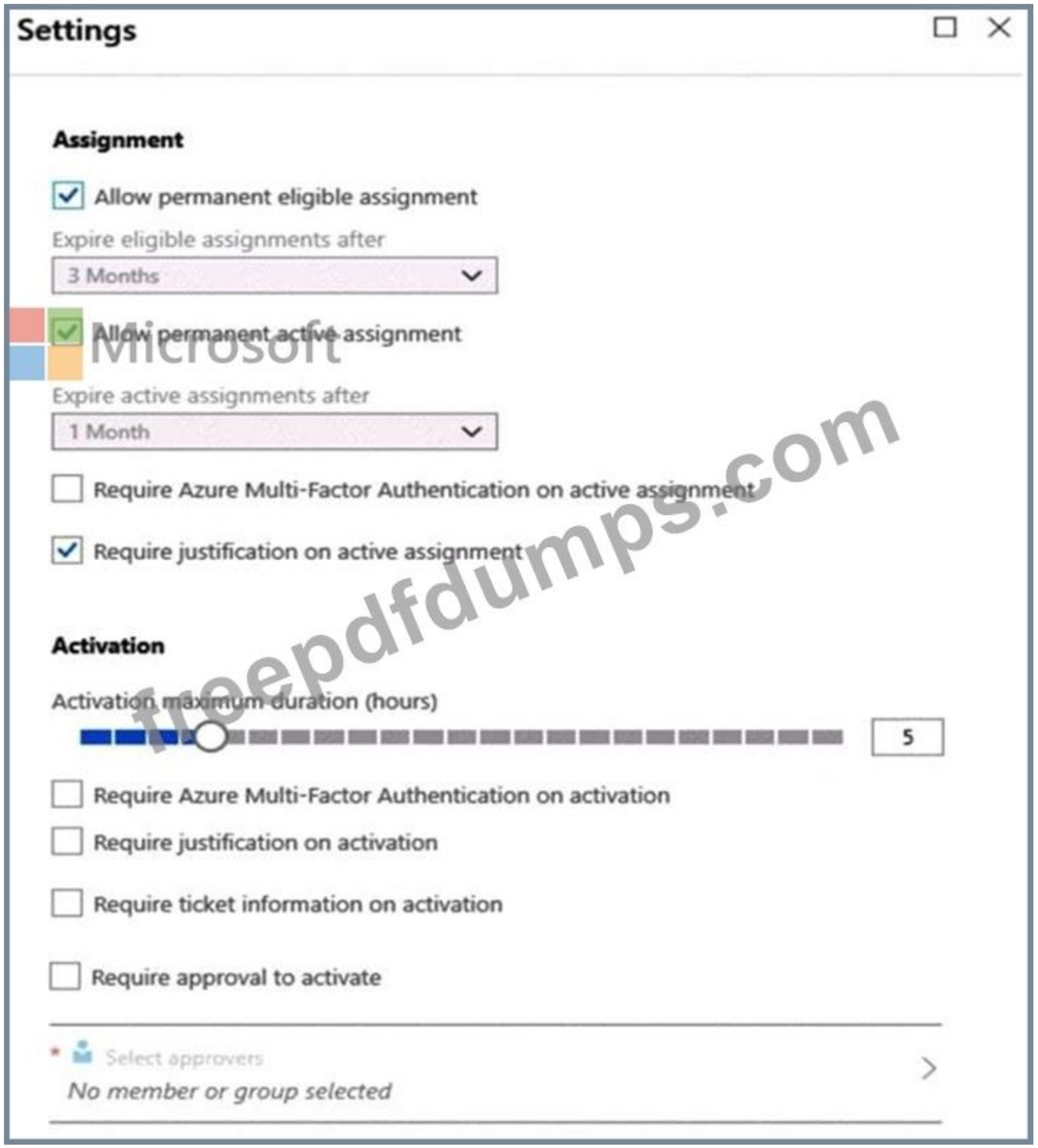
NEW QUESTION: 60

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



Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

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



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

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

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	○	○
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	○	○
User3 can activate the Security Administrator role.	○	○

Answer:

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	○	○
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	○	○
User3 can activate the Security Administrator role.	○	○

Explanation:

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	○	●
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	●	○
User3 can activate the Security Administrator role.	○	●

Box 1: Yes

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

You can choose from two assignment duration options for each assignment type (eligible and active) when you configure settings for a role. These options become the default maximum duration when a user is assigned to the role in Privileged Identity Management.
Use the Activation maximum duration slider to set the maximum time, in hours, that a role stays active before it expires. This value can be from one to 24 hours.
Box 2: Yes
Active Type: A role assignment that doesn't require a user to perform any action to use the role. Users assigned as active have the privileges assigned to the role Box 3: Yes User3 is member of Group2.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure
https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource- roles-configure-role-settings

NEW QUESTION: 61
You have an Azure subscription that contains an Azure key vault.
You create a storage account named storage1.
You plan to store data in the following storage1 services:
* Azure Files
* Azure Blob storage
* Azure Table storage
* Azure Queue storage
For which two services can you configure data encryption by using the keys stored in the key vault? Each correct answer presents a complete solution.
NOTE Each correct selection is worth one point.
A. Blob storage
B. Queue storage
C. Table storage
D. Azure Files
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 62
You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1. EASM1 contains the inventory assets shown in the following table.

Name	Type	State
VM1	Host	Approved inventory
VM2	Host	Dependency
VM3	Host	Monitor Only
VM4	Host	Candidate

Which assets are scanned daily, and which assets will display in the default dashboard charts? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

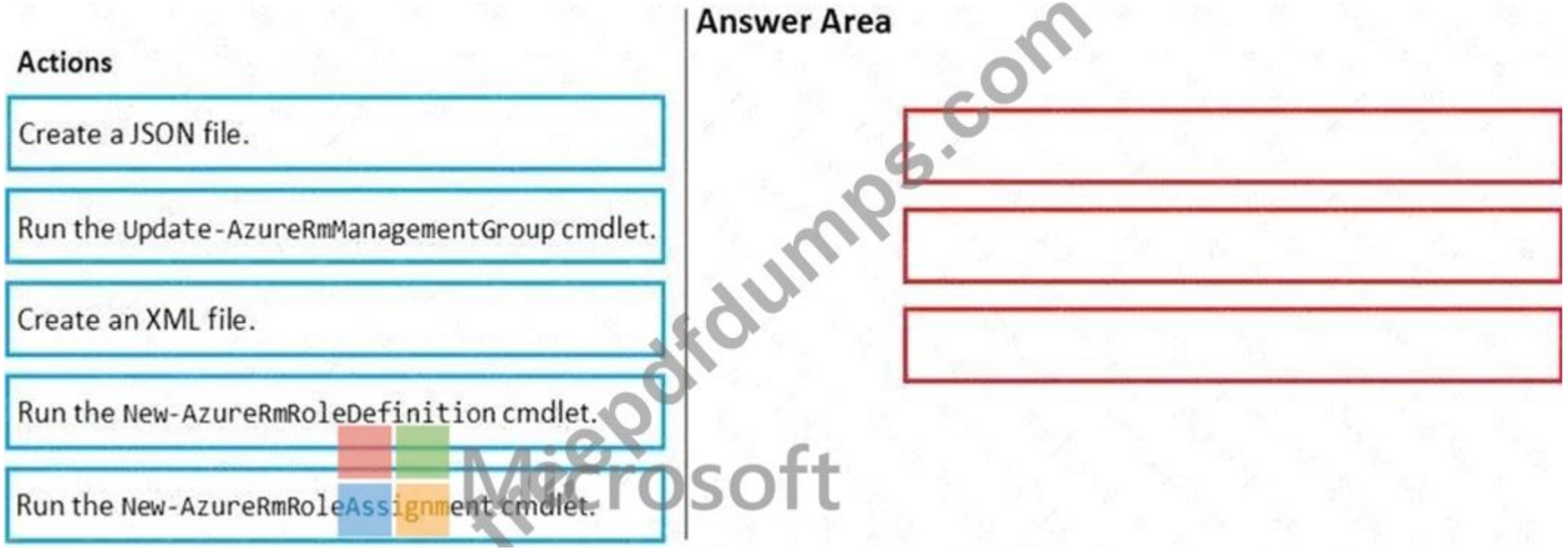
NEW QUESTION: 63

You have an Azure subscription named Sub1.

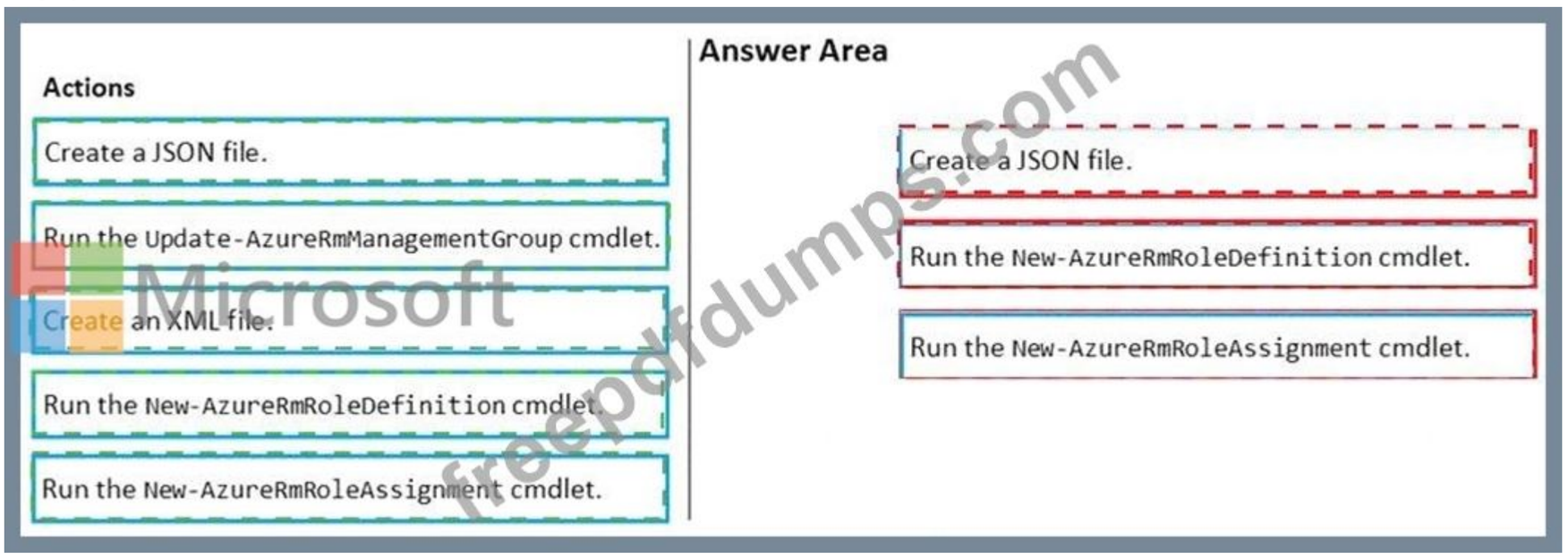
You have an Azure Active Directory (Azure AD) group named Group1 that contains all the members of your IT team.

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

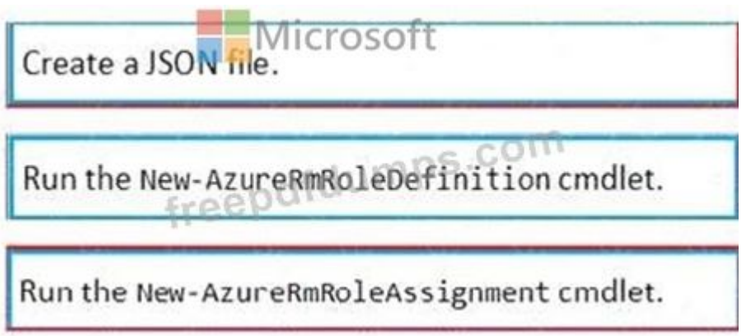
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:



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

NEW QUESTION: 64
You have 10 on-premises servers that run Windows Server.
You plan to implement Microsoft Defender for Cloud vulnerability scanning for the servers. What should you install on the servers first?
A. the Microsoft Configuration Manager client
B. the Azure Arc Connected Machine agent
C. the Security Events data connector in Microsoft Sentinel
D. the Microsoft Defender for Endpoint agent
Answer: B (LEAVE A REPLY)

NEW QUESTION: 65
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: 66

From Azure Security Center, you need to deploy SecPol1.
What should you do first?
A. Enable Azure Defender.
B. Create an Azure Management group.
C. Create an initiative.
D. Configure continuous export.
Answer: B (LEAVE A REPLY)
Reference:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/security-center/custom-security-policies.md
https://zimmergren.net/create-custom-security-center-recommendation-with-azure-policy/
Topic 4, Fabrikam, Inc.
Case Study
Overview
Existing Environment
Network Environment
Cloud Environment
Sub1 Resources
Fabrikam, Inc. is a consulting company. The company has a main office in New York City and branch offices in Amsterdam and Singapore.
The on-premises network contains a datacenter in each office.
Fabtikam has two Azure subscriptions named Sub1 and Sub2 and a Microsoft 365 subscription that includes Microsoft 365 E5 licenses.
All the subscriptions are linked to a Microsoft Entra tenant named fabrikam.com that contains the identities shown in the following table.

Name	Type	Microsoft Entra role	Azure role assignment for Sub1
Admin1	User	Privileged Authentication Administrator	Resource Policy Contributor
Admin2	User	Compliance Administrator	User Access Administrator
Admin3	User	Authentication Administrator	Contributor
Admin4	User	Global Administrator	*None*
User1	User	*None*	Reader
AKS1	System-assigned managed identity	*None*	*None*
ID1	User-assigned managed identity	*None*	*None*

The tenant contains the groups shown in the following table.

Name	Type	Role assignments allowed
Group1	Security	Yes
Group2	Security	No
Group3	Microsoft 365	Yes
Group4	Microsoft 365	No

All devices are enrolled in Microsoft Intune.
Sub2 Resources
Sub1 contains a resource group named RG1 that contains the resources shown in the following table.

Name	Description	Location
SQLServer1	Azure SQL Database logical server	East US
SQLdb1	Database on SQLServer1	East US
VM1	Virtual machine	East US
AKS1	Azure Kubernetes Service (AKS) cluster	East US
Registry1	Azure container registry	East US
storage1	Storage account	East US
AKV1	Azure key vault	East US

SQLServer1 uses Microsoft SQL Server authentication.

Sub1 has an Azure Web Application Firewall (WAF) named WAF1 that has the following types of rule sets:

* Bot Manager 1.1
* Azure-managed Default Rule Set (DRS)

Sub1 has the following compliance standards assigned in Microsoft Defender for Cloud:

* MIST SP 800-53 Rev. 4
* Microsoft cloud security benchmark (MCSB)
* System and Organization Controls (SOC) 2 Type 2

Planned Changes and Requirements

Planned Changes

Sub2 contains a resource group named RG2.

Fabtikam plans to implement the following changes:

* Deploy the following key vaults to RG1:
o AKV2 in the West Europe Azure region
o AKV3 in the Central US Azure region
o AKV4 in the East US Azure region
* Deploy the following key vaults to RG2:
o AKV5 in the East US region
* Configure VM1 to read data from storage1.
* Create function apps that have the following hosting plans:
o Fa1: Flex Consumption hosting plan
o Fa2: Consumption hosting plan
o Fa3: Dedicated hosting plan
* For WAF1, implement rate limiting rules based on the request location.
* Enable the NIST SP 800-53 Rev. 5 compliance standard in Defender for Cloud.
* Create a new storage account named storage2 that supports Azure Table storage.
* Enforce multifactor authentication (MFA) when database administrators access SQLdbl.
* Implement ExpressRoute circuits to the on-premises network as shown in the following table.

Name	Location	Deployment type
ER1	West Europe	ExpressRoute with a connectivity provider
ER2	West Europe	ExpressRoute Metro with a connectivity provider
ER3	East US	ExpressRoute Direct
ER4	Southeast Asia	ExpressRoute Metro Direct

* For RG1. create a new Privileged Identity Management (PIM) eligible role assignment that assigns the Contributor role to supported groups.
Technical Requirements
Fabrikam has the following technical requirements:
* If VM1 is deleted, the permissions for VM1 must be removed automatically.
* The AKS1 managed identity must only be able to pull images from Registry1.
* The ID1 managed identity must be able to push images to and pull images from Registry 1.
* All the data in the storage accounts must be encrypted by using Fabrikam-managed keys.
* All outbound traffic from the function apps to the on-premises network must use ExpressRoute circuits.
* ExpressRoute connectivity between the on-premises network and the Azure environment must be encrypted by using Layer 2 or Layer 3 encryption.

NEW QUESTION: 67
You have an Azure subscription named Sub1.
In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.
You need to modify Play1 to send email messages to a distribution group named Alerts.
What should you use to modify Play1?
A. Azure DevOps
B. Azure Application Insights
C. Azure Monitor
D. Azure Logic Apps Designer
Answer: D (LEAVE A REPLY)
You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up.
References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks

NEW QUESTION: 68
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: Userl -28681041@ExamUsers.com
Azure Password: GpOAe4@lDg
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 9
You need to ensure that the rg1lod28681041n1 Azure Storage account is encrypted by using a key stored in the KeyVault28681041 Azure key vault.
Answer:
Check below steps in explanation for Task
Explanation:
To ensure that the rg1lod28681041n1 Azure Storage account is encrypted by using a key stored in the KeyVault28681041 Azure key vault, you can follow these steps:

In the Azure portal, search for and select the storage account named rg1lod28681041n1.
In the left pane, select Encryption.
In the Encryption pane, select Customer-managed key.
In the Customer-managed key pane, select Select from Key Vault.
In the Select from Key Vault pane, enter the following information:
Key vault: Select the KeyVault28681041 Azure key vault.
Key: Select the key you want to use.
Select Save.

NEW QUESTION: 69
You have an Azure subscription that contains an Azure web app named Appl.
You plan to configure a Conditional Access policy for Appl. The solution must meet the following requirements:
* Only allow access to App1 from Windows devices.
* Only allow devices that are marked as compliant to access Appl.
Which Conditional Access policy settings should you configure? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all.
You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Answer:

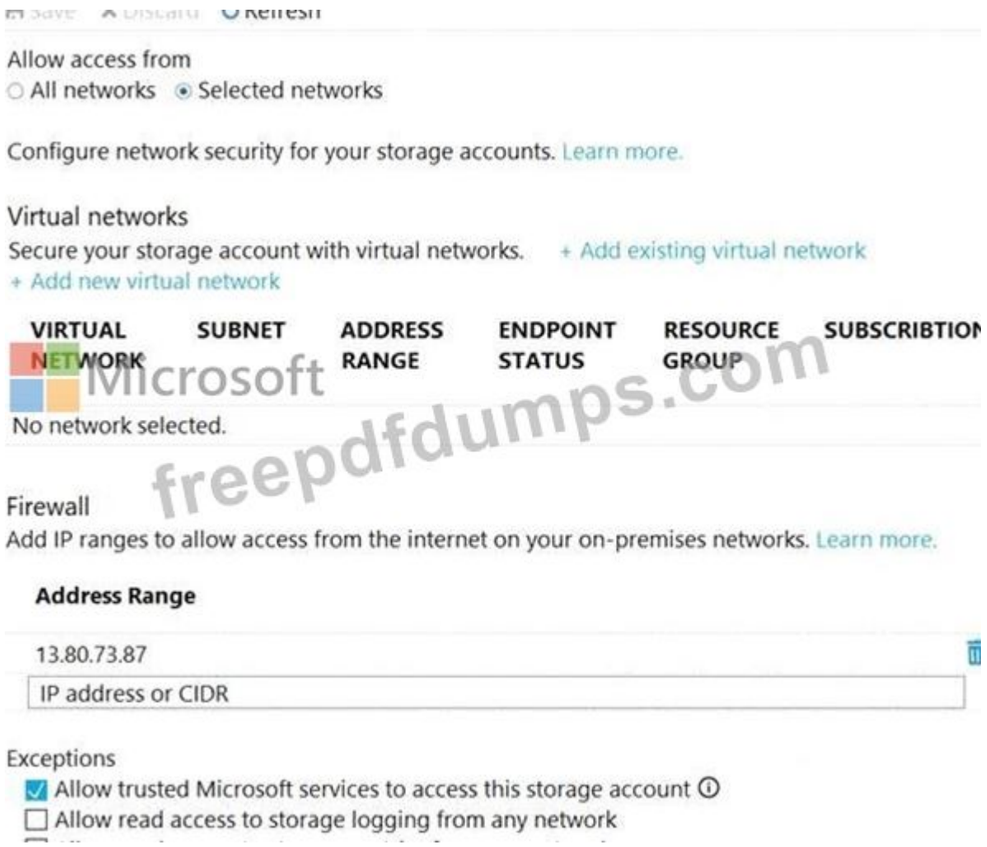
Explanation:

NEW QUESTION: 70
You onboard Azure Sentinel. You connect Azure Sentinel to Azure Security Center.
You need to automate the mitigation of incidents in Azure Sentinel. The solution must minimize administrative effort.
What should you create?
A. an alert rule
B. a runbook
C. a playbook
D. a function app
Answer: C (LEAVE A REPLY)

NEW QUESTION: 71
You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.4	13.80.73.87
VM2	VNET2/Subnet2	10.2.1.4	213.199.133.190
VM3	VNET2/Subnet2	10.2.1.5	*None*

Subnet1 and Subnet2 have a Microsoft.Storage service endpoint configured.
You have an Azure Storage account named storageacc1 that is configured as shown in the following exhibit.



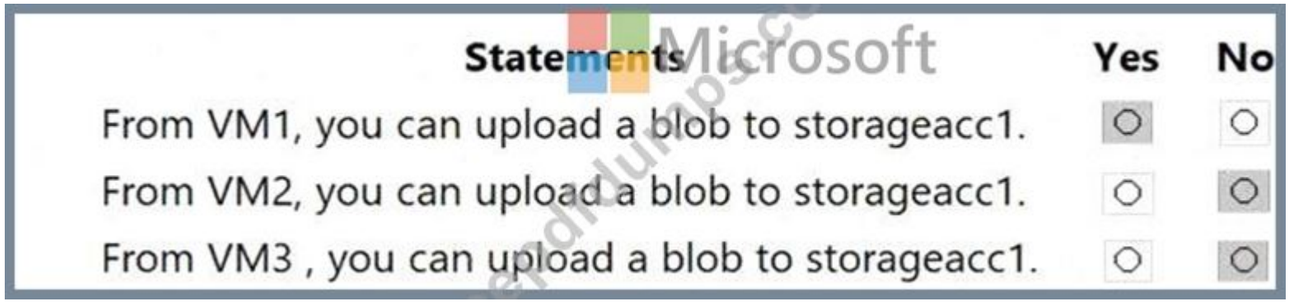
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	○	○
From VM2, you can upload a blob to storageacc1.	○	○
From VM3 , you can upload a blob to storageacc1.	○	○

Answer:

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	○	○
From VM2, you can upload a blob to storageacc1.	○	○
From VM3 , you can upload a blob to storageacc1.	○	○

Explanation:



Box 1: Yes

The public IP of VM1 is allowed through the firewall.

Box 2: No

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

Box 3: No

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

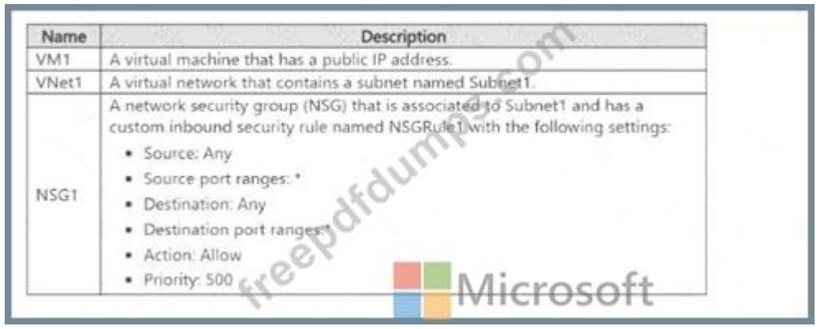
Reference:

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

NEW QUESTION: 72

You have a management group named MG1 that contains an Azure subscription named Sub1.

Sub1 contains the resources shown in the following table.



Name	Description
VM1	A virtual machine that has a public IP address.
VNet1	A virtual network that contains a subnet named Subnet1.
NSG1	A network security group (NSG) that is associated to Subnet1 and has a custom inbound security rule named NSGRule1 with the following settings: • Source: Any • Source port ranges: * • Destination: Any • Destination port ranges: * • Action: Allow • Priority: 500

You create an Azure Virtual Network Manager instance named AVNM1 that has the following configurations:

* Management scope: MG1

* Network groups:

o Name: Group1

Group members: VNet1

* Security admin configuration:

o Name: SAT

o Rule collections:

Name: SACollection1

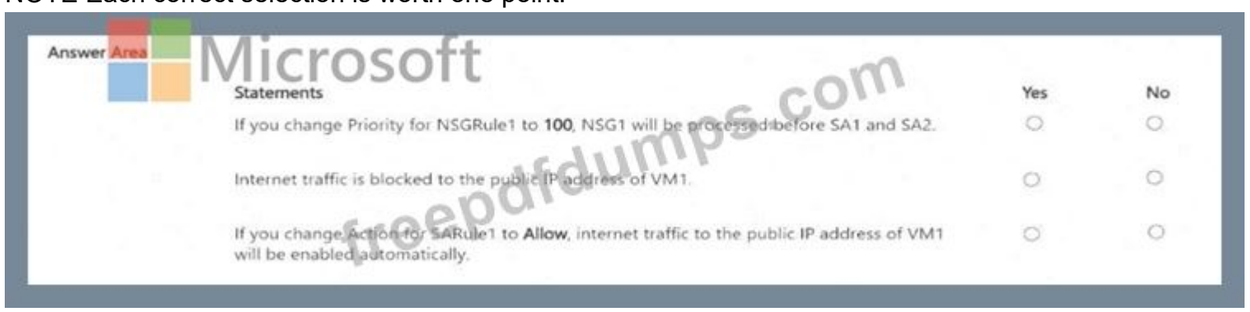
Target network groups: Group1

Security admin rules:

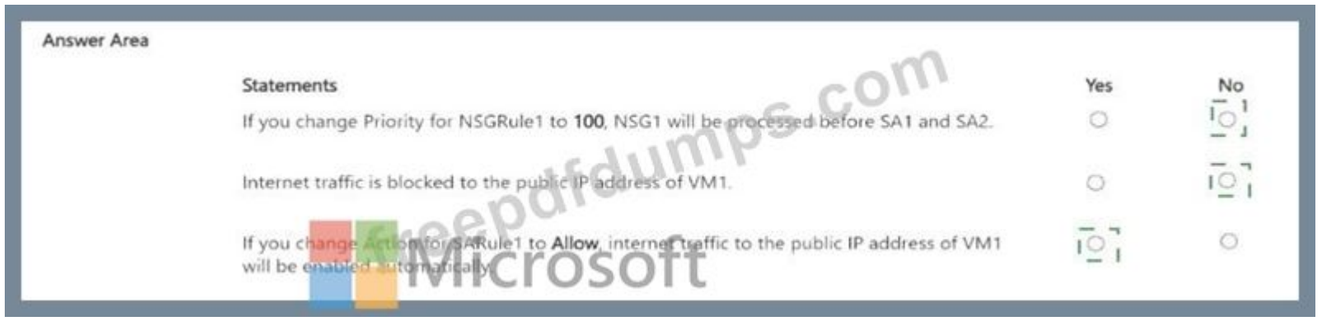
Name: SARule1

Priority: 500

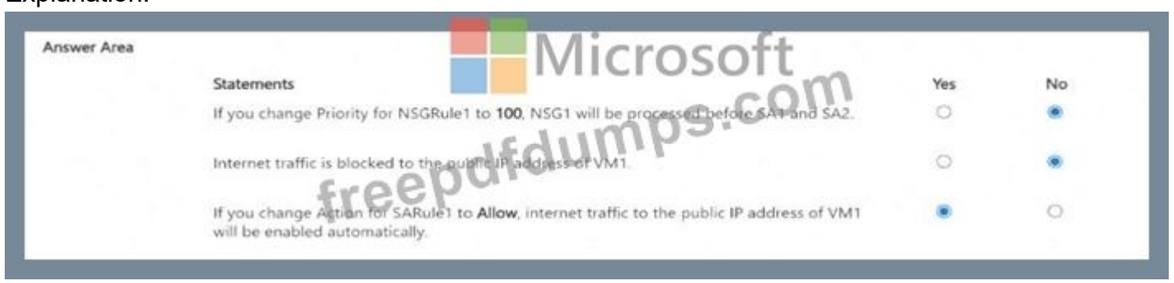
Action: Deny
Direction: Inbound
Source type: Any
Source port *
SA1 is deployed to all Azure regions.
You create a Virtual Network Manager instance named AVNM2 that has the following configurations:
* Management scope: Sub1
* Network groups:
o Name: Group2
Group members: VNet1
* Security admin configuration:
o Name: SA2
o Rule collections:
Name: SACollection2
Target network groups: Group2
Security admin rules:
Name: SARule2
Priority: 500
Action: Always allow
Direction: Inbound
Source type: Any
Source port: *
SA2 is deployed to all Azure regions.
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:



Explanation:



NEW QUESTION: 73

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

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

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

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

You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant.

What should you do?

A. From the Roles and administrators blade, assign the Security administrator role to Admin1.

B. From the Organizational relationships blade, add an identity provider.

C. From the Custom domain names blade, add a custom domain.

D. From the Users blade, modify the External collaboration settings.

Answer: D (LEAVE A REPLY)

You need to allow guest invitations in the External collaboration settings.

NEW QUESTION: 74

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.

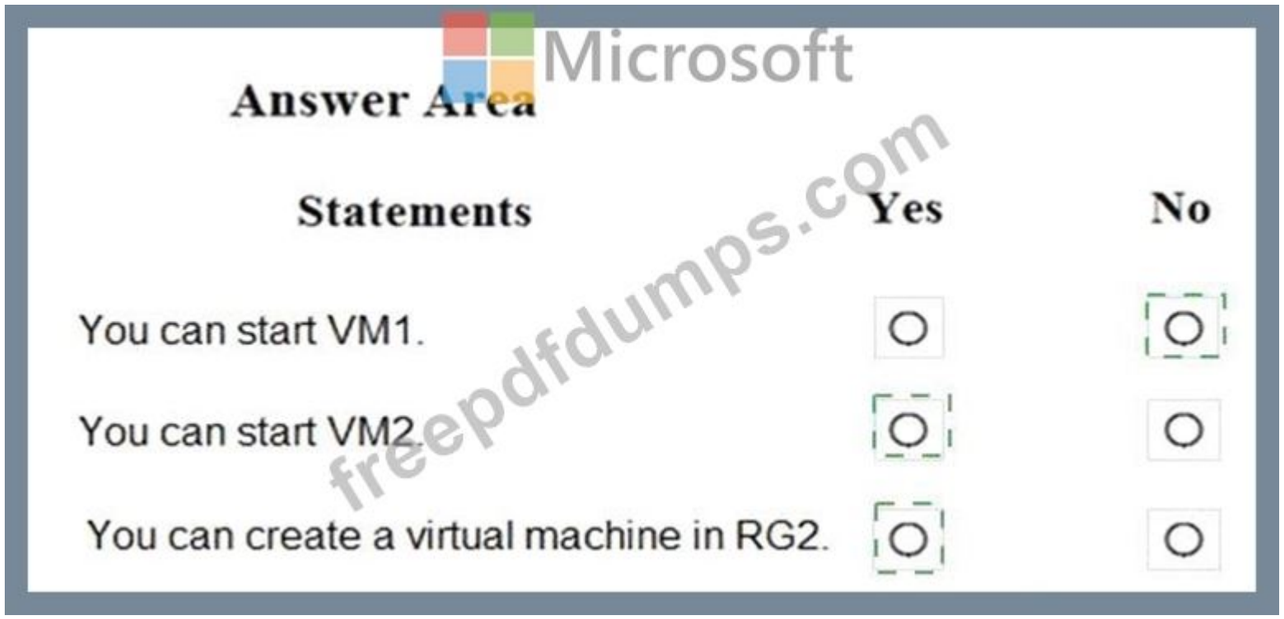
Name	Type	Created on
Lock1	Read-only	VM1
Lock2	Read-only	RG2

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

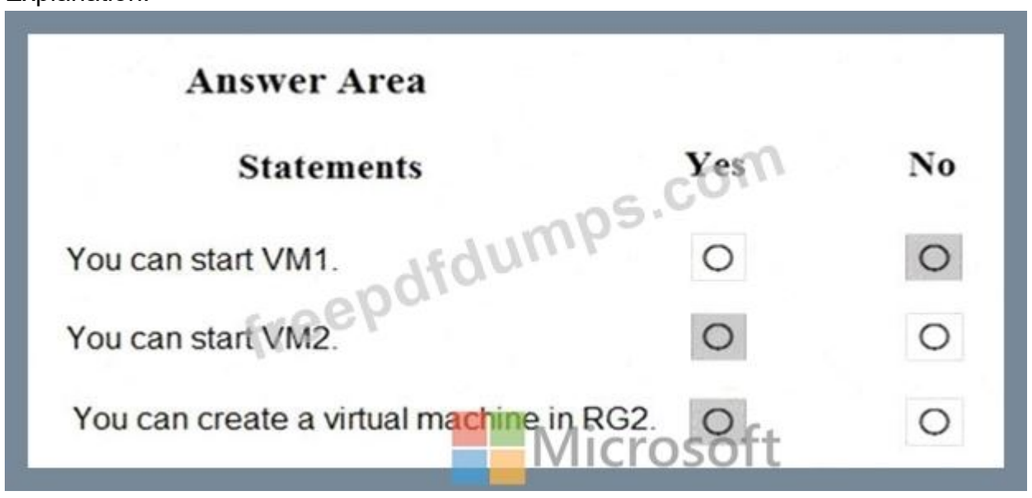
Answer Area

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

Answer:



Explanation:



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

NEW QUESTION: 75
You have an Azure subscription named Sub1 that contains the Azure key vaults shown in the following table.

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

In Sub1, you create a virtual machine that has the following configurations:
* Name:VM1
* Size: DS2v2
* Resource group: RG1
* Region: West Europe
* Operating system: Windows Server 2016
You plan to enable Azure Disk Encryption on VM1.
In which key vaults can you store the encryption key for VM1?
A. Vault1 or Vault3 only
B. Vault1, Vault2, Vault3, or Vault4
C. Vault1 only
D. Vault1 or Vault2 only
Answer: C (LEAVE A REPLY)
" Your key vault and VMs must be in the same subscription. Also, to ensure that encryption secrets don ' t cross regional boundaries, Azure Disk Encryption requires the Key Vault and the VMs to be co-located in the same region. " https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault

NEW QUESTION: 76
You have an Azure subscription that contains a SQL Server on Azure Virtual Machines instance named SQt1 and a Microsoft Sentinel workspace named Sentinel1.
You need to monitor security incidents on SQL1 by using Sentinel1.
What should you do first?
A. From the Azure portal, create a Log Analytics workspace.
B. On SQL1, enable SQL1 Server audit.
C. From Sentinel1, enable VM insights.
D. On SQL1. install the Connected Machine agent for Azure Arc-enabled servers.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 77
You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains the subnets shown in the following table.

Name	IP address space
Subnet1	10.10.0.0/24
Subnet2	172.16.0.0/24
Subnet3	192.168.10.0/24

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

Name	Connected to
VM1	Subnet1
VM2	Subnet2
VM3	Subnet3

VM3 contains a service that listens for connections on port 8080.

For VM1, you configure just-in-time (JIT) VM access as shown in the following exhibit.

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

NOTE; Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can establish a Remote Desktop connection from VM1 to VM3 for a maximum of three hours.	○	○
You can establish a Remote Desktop connection from VM2 to VM1 after requesting access.	○	○
You can establish a Remote Desktop connection from VM3 to VM1 without requesting access.	○	○

Answer:

Answer Area

Explanation:

Answer Area

NEW QUESTION: 78

You have an Azure AD turned that contains a user named User1.

You purchase an App named App1.

User1 needs to publish App1 by using Azure AD Application Proxy.

Which role should you assign to User1?

A. Cloud App Security Administrator

B. Application Administrator

C. Cloud Application Administrate

D. Hybrid identity Administrator

Answer: (SHOW ANSWER)

NEW QUESTION: 79

You have an Azure subscription that contains a web app named App1 and an Azure key vault named Vault1.

You need to configure App1 to store and access the secrets in Vault1.

How should you configure App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

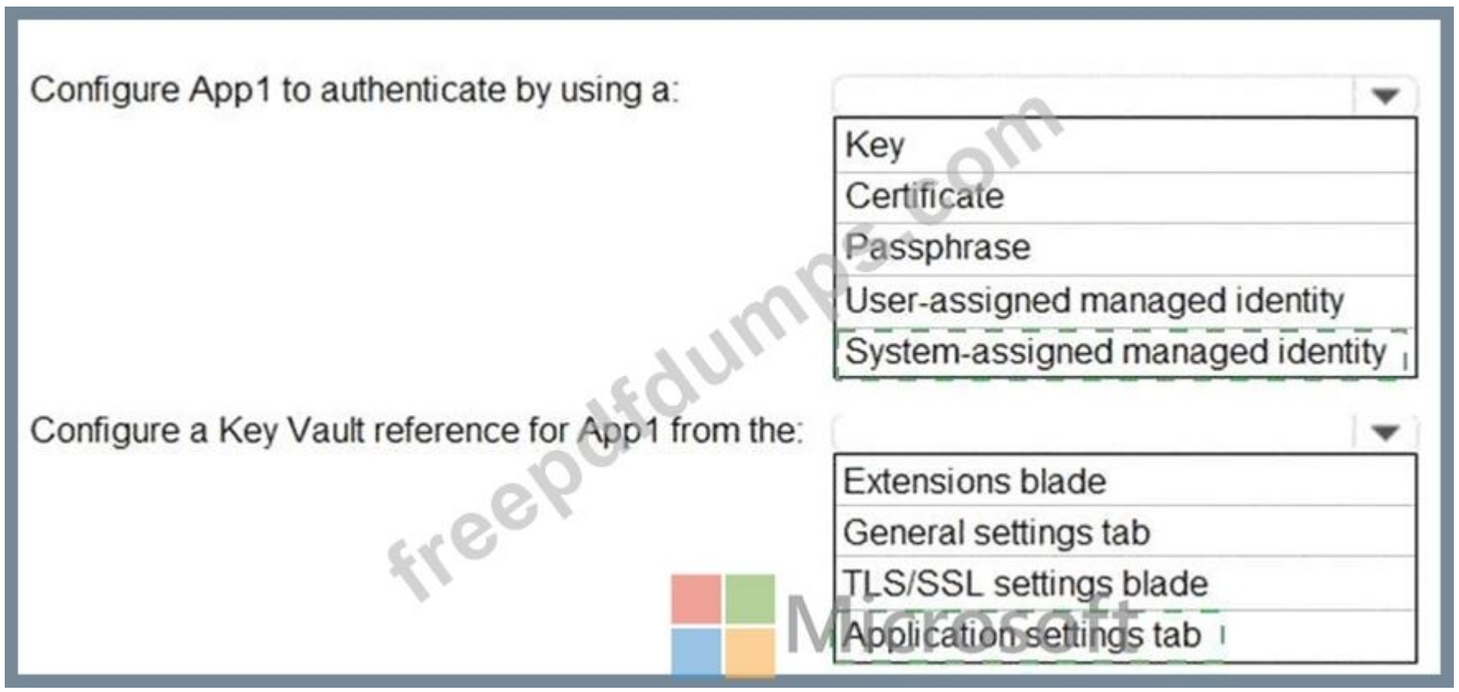
Configure App1 to authenticate by using a:

- Key
- Certificate
- Passphrase
- User-assigned managed identity
- System-assigned managed identity

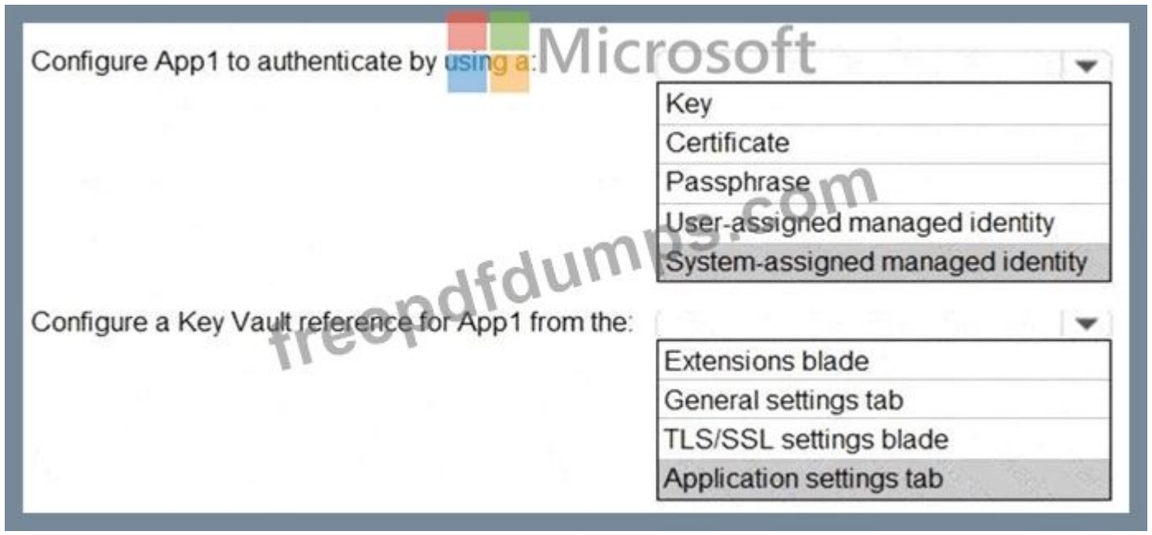
Configure a Key Vault reference for App1 from the:

- Extensions blade
- General settings tab
- TLS/SSL settings blade
- Application settings tab

Answer:

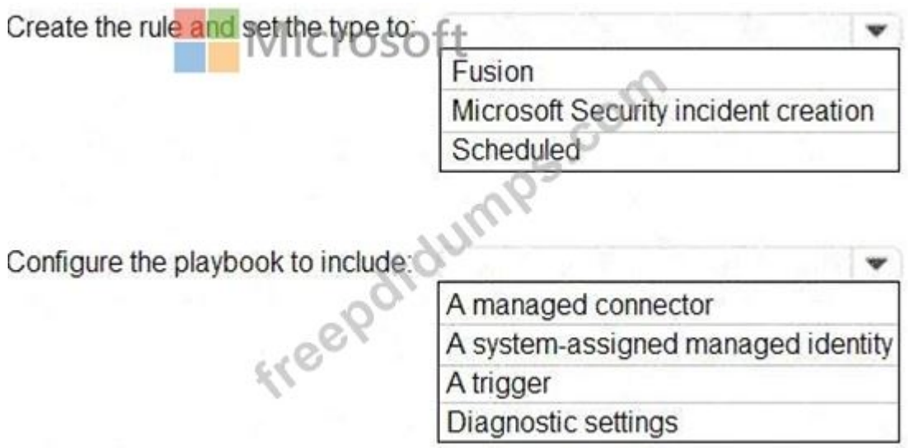


Explanation:

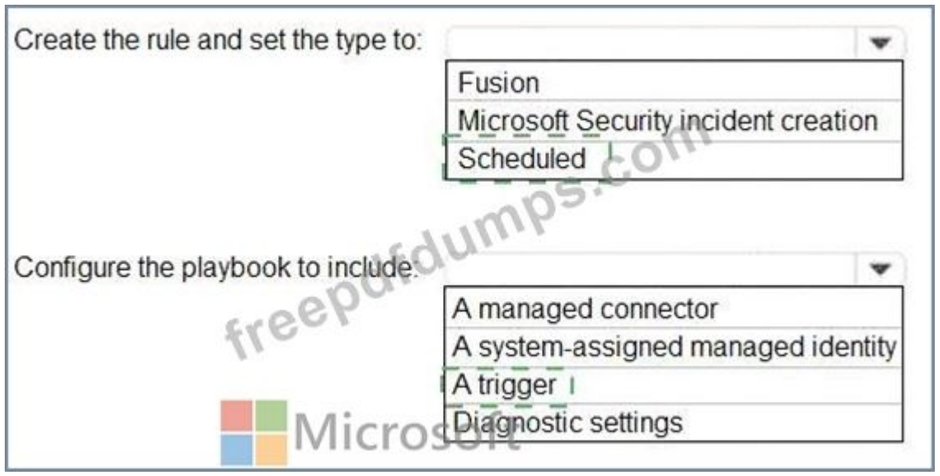


Reference:
https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet

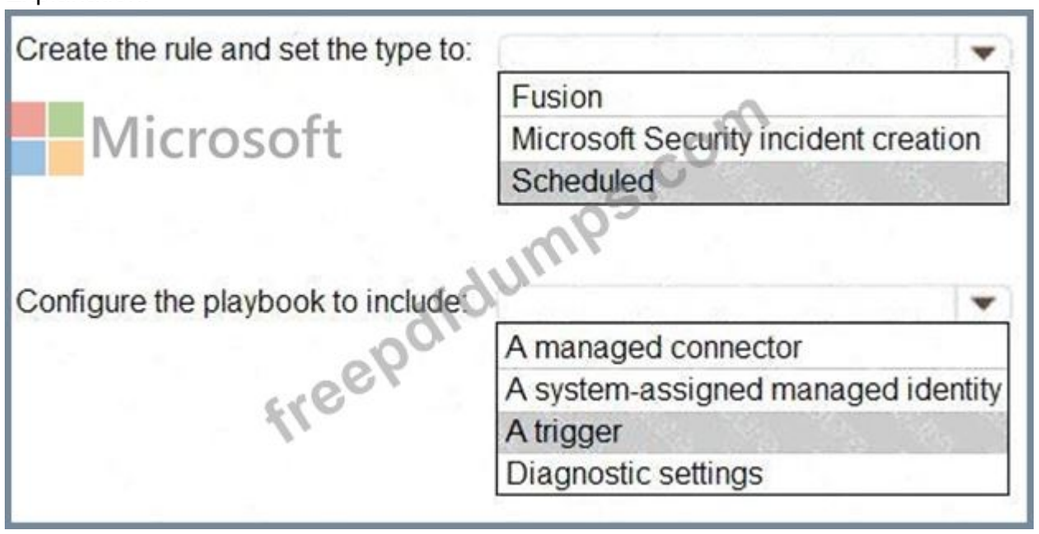
NEW QUESTION: 80
You have an Azure Sentinel workspace that contains an Azure Active Directory (Azure AD) connector, an Azure Log Analytics query named Query1 and a playbook named Playbook1.
Query1 returns a subset of security events generated by Azure AD.
You plan to create an Azure Sentinel analytic rule based on Query1 that will trigger Playbook1.
You need to ensure that you can add Playbook1 to the new rule.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



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

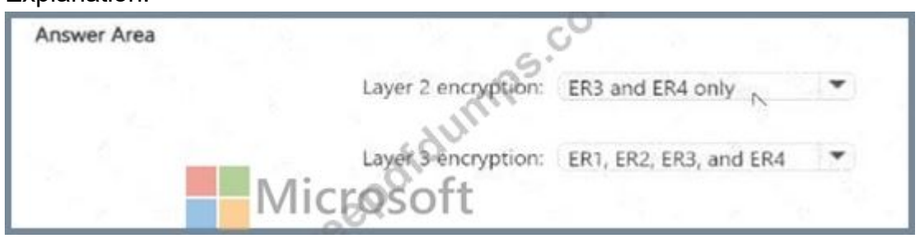
NEW QUESTION: 81
You need to ensure that you can meet the security operations requirements.
What should you do first?
A. Turn on Auto Provisioning in Security Center.
B. Integrate Security Center and Microsoft Cloud App Security.
C. Upgrade the pricing tier of Security Center to Standard.
D. Modify the Security Center workspace configuration.
Answer: C (LEAVE A REPLY)
The Standard tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The Standard tier also adds advanced threat detection capabilities, which uses built-in behavioral analytics and machine learning to identify attacks and zero-day exploits, access and application controls to reduce exposure to network attacks and malware, and more.

Scenario: Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center.
References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing

NEW QUESTION: 82
You need to recommend an encryption solution for the planned ExpressRoute implementation. The solution must meet the technical requirements.
Which ExpressRoute circuit should you recommend for each type of encryption? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:



NEW QUESTION: 83
You have an Azure subscription that contains an app named App1. App1 has the app registration shown in the following table.

API	Permission	Type	Admin consent required	Status
Microsoft.Graph	User.Read	Delegated	No	**None**
Microsoft.Graph	Calendars.Read	Delegated	No	**None**

You need to ensure that App1 can read all user calendars and create appointments. The solution must use the principle of least privilege.
What should you do?
A. Add a new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.
B. Add a new Application API permission for Microsoft.Graph Calendars.ReadWrite.
C. Select Grant admin consent.
D. Add a new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.Shared.
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/graph/permissions-reference#calendars-permissions

NEW QUESTION: 84
You create a new Azure subscription.
You need to ensure that you can create custom alert rules in Azure Security Center.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. Onboard Azure Active Directory (Azure AD) Identity Protection.
B. Create an Azure Storage account.
C. Implement Azure Advisor recommendations.
D. Create an Azure Log Analytics workspace.
E. Upgrade the pricing tier of Security Center to Standard.
Answer: (SHOW ANSWER)
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: 85
You plan to create an Azure Storage account named storage 1.
You need to ensure that all new objects created in storage1 are protected by using double encryption. The solution must minimize administrative effort.
What should you configure when creating storage1?
A. the access tier
B. the Encryption type option
C. the Infrastructure encryption option
D. the minimum TLS version
Answer: C (LEAVE A REPLY)

NEW QUESTION: 86
You have an Azure subscription that contains the resources shown in the following table.

Name	Type
LB1	Azure Standard Load Balancer
VM1	Virtual machine
SQL1	Azure SQL Database
VMSS1	Virtual machine scale set

You plan to deploy an Azure Private Link service named APL1.
Which resource must you reference during the creation of APL1?
A. SQL
B. LB1
C. VMSS1
D. VM1
Answer: B (LEAVE A REPLY)

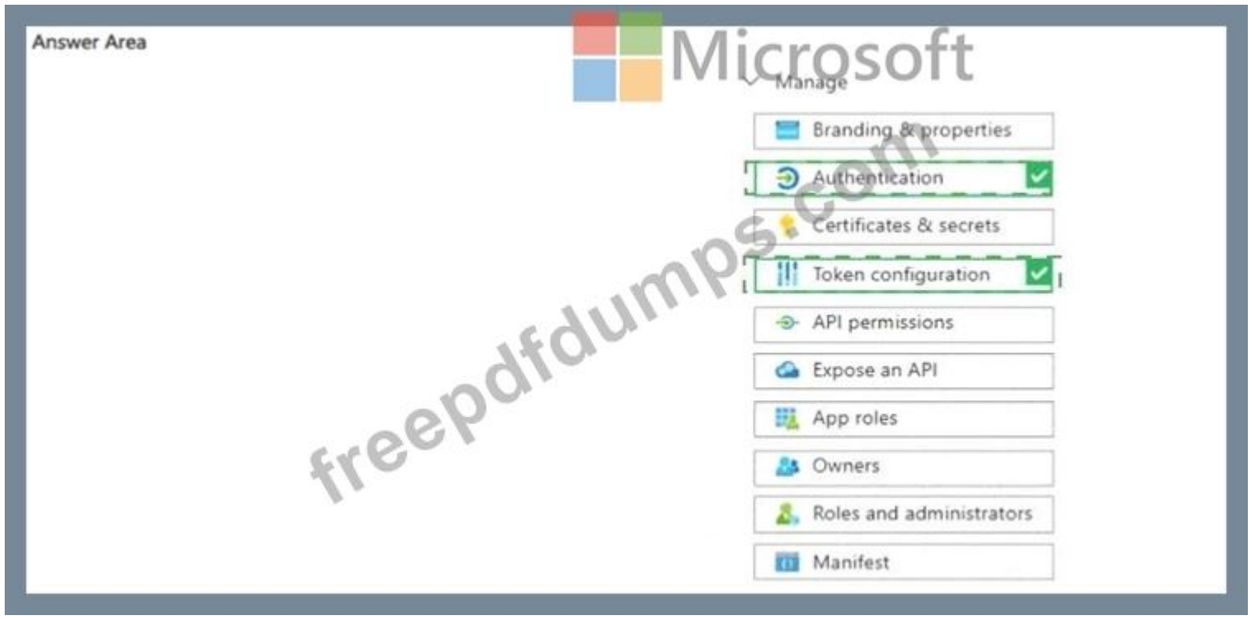
NEW QUESTION: 87
You have an Azure key vault named Vault1 that stores the resources shown in following table.

Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

Which resources support the creation of a rotation policy?
A. Key1 Only
B. Cert1 only
C. Secret1 and Cert1 only
D. Key1, Secret1, and Cert1
E. Key1 and Cert1 only
F. Key1 and Secret1 only
Answer: F (LEAVE A REPLY)

NEW QUESTION: 88
You have an Azure subscription that is linked to a Microsoft Entra tenant named contoso.com. In contoso.
com, you register an app named App1. You need to perform the following tasks for App1:
* Add and configure the Mobile and desktop applications platform.
* Add the ipaddr optional claim.
Which two settings should you select for App1? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

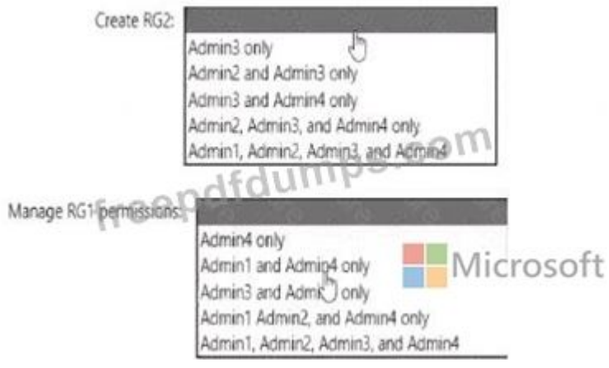
Answer:



Explanation:

NEW QUESTION: 89

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 area. NOTE: Each correct selection is worth one point



Answer:

Explanation:

Graphical user interface, text, application, chat or text message Description automatically generated

Box 1: Admin3 only

The Contributor role has the necessary write permissions to create the resource group.

Box 2: Admin4 only

You need Owner level access to be able to manage permissions. The Contributor role can do most things but cannot modify permissions on existing objects.

NEW QUESTION: 90

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.

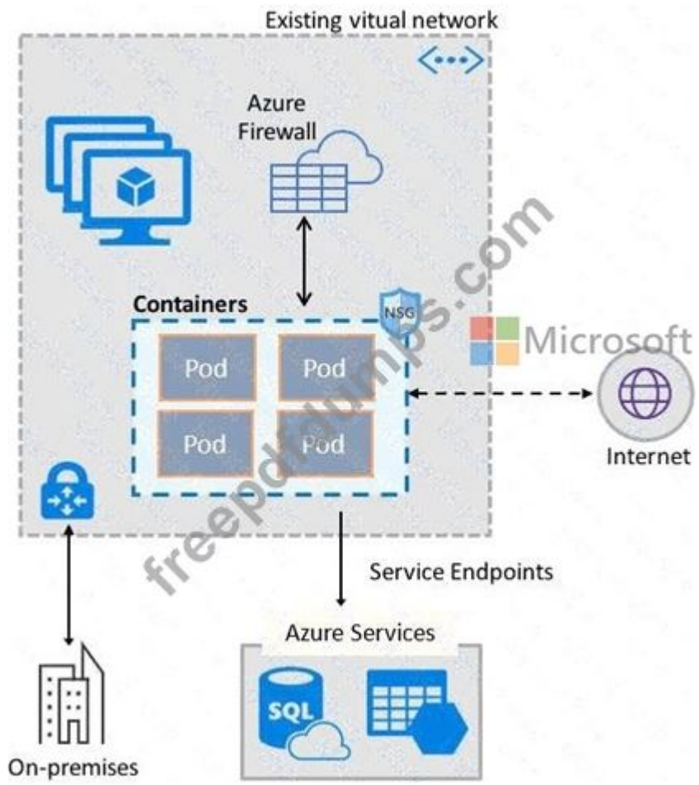
Answer: (SHOW ANSWER)

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: 91
You have an Azure subscription that contains a resource group named RG1 and a security group serverless RG1 contains 10 virtual machine, a virtual network VNET1, and a network security group (NSG) named NSG1. ServerAdmins can access the virtual machines by using RDP.
You need to ensure that NSG1 only RDP connections to the virtual for a maximum of 60 minutes when a member of ServerAdmins requests access.
What should you configure?
A. an Azure Active Directory (Azure AD) Privileged identity Management (PIM) role assignment.
B. a just in time (JIT) VM access policy in Azure Security Center
C. an azure policy assigned to RG1.
D. an Azure Bastion host on VNET1.
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/security-center/just-in-time-explained

NEW QUESTION: 92

You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

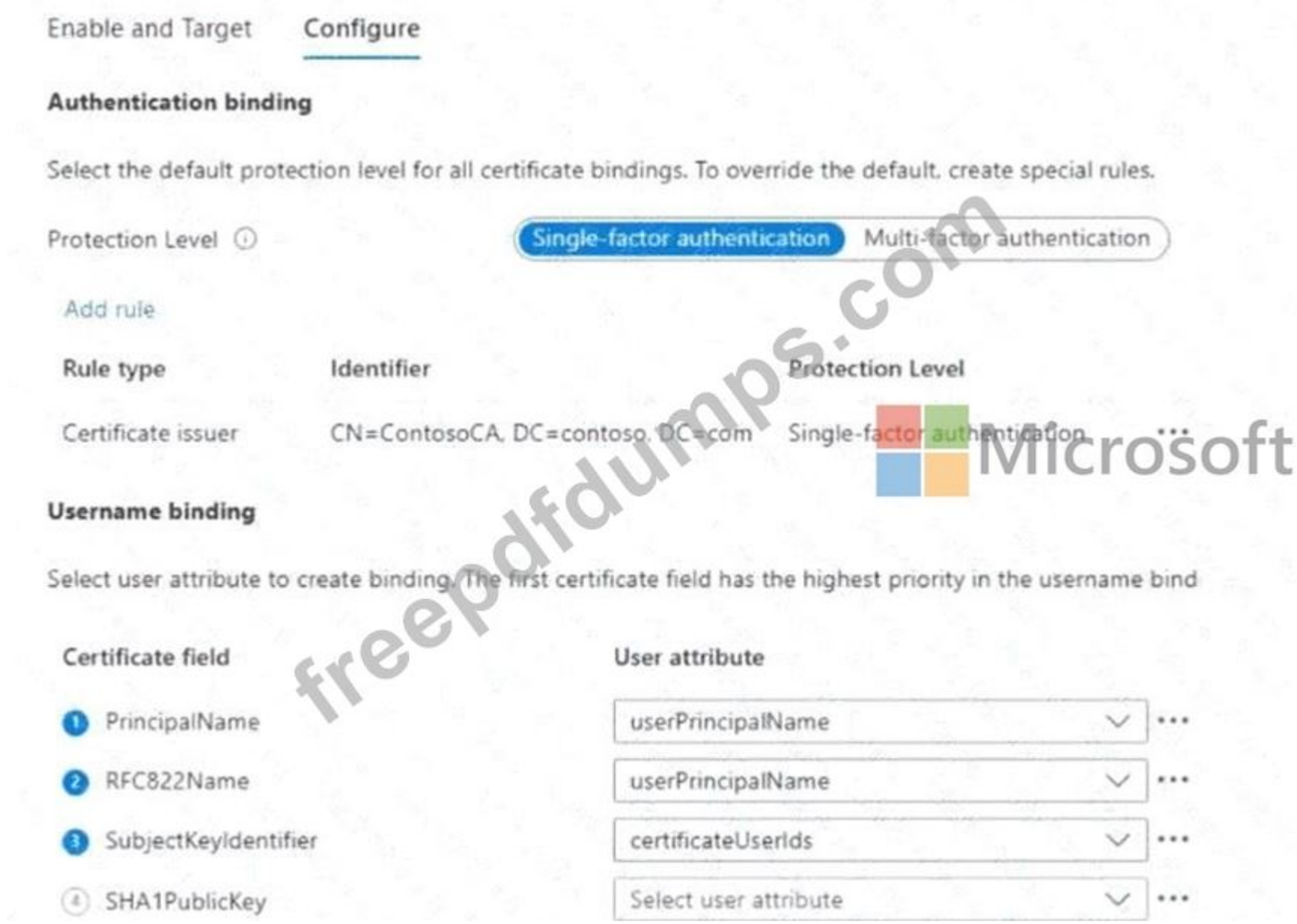
All the users have devices that contain certificates issued by a certification authority (CA) named ContosoCA.

You create a Conditional Access policy that has the following settings:

* Name: CAPoltcy1
* Assignments
o Users and groups: Group1
o Target resources
* Include: All cloud apps
o Access controls
* Grant access: Require multi-factor authentication
o Enable policy: On

You enable and target certificate-based authentication as shown in the Enable and Target exhibit. (Click the Enable and Target tab.)

You configure certificate-based authentication as shown in the Configure exhibit. (Click the Configure 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.

Answer Area

Statements	Yes	No
User1 can sign in without providing a password.	○	○
User2 can choose to use a certificate or a smart card to sign in.	○	○
User3 must use a certificate during sign-in.	○	○

Answer:

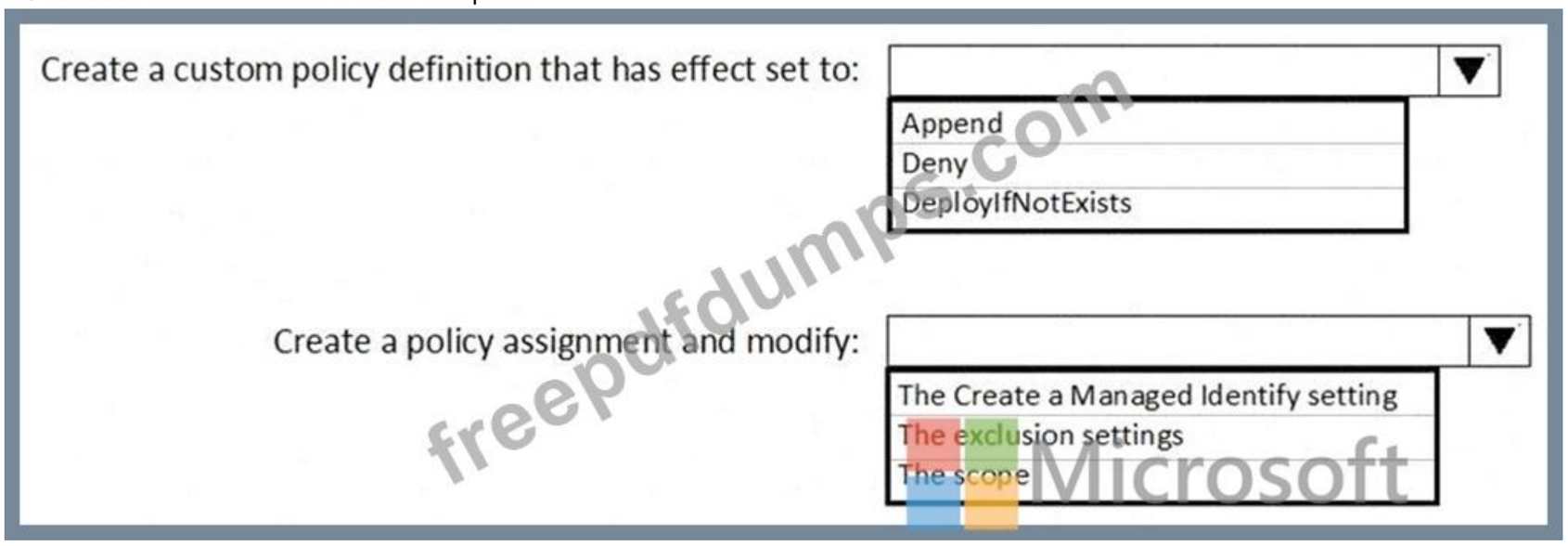
Explanation:

NEW QUESTION: 93

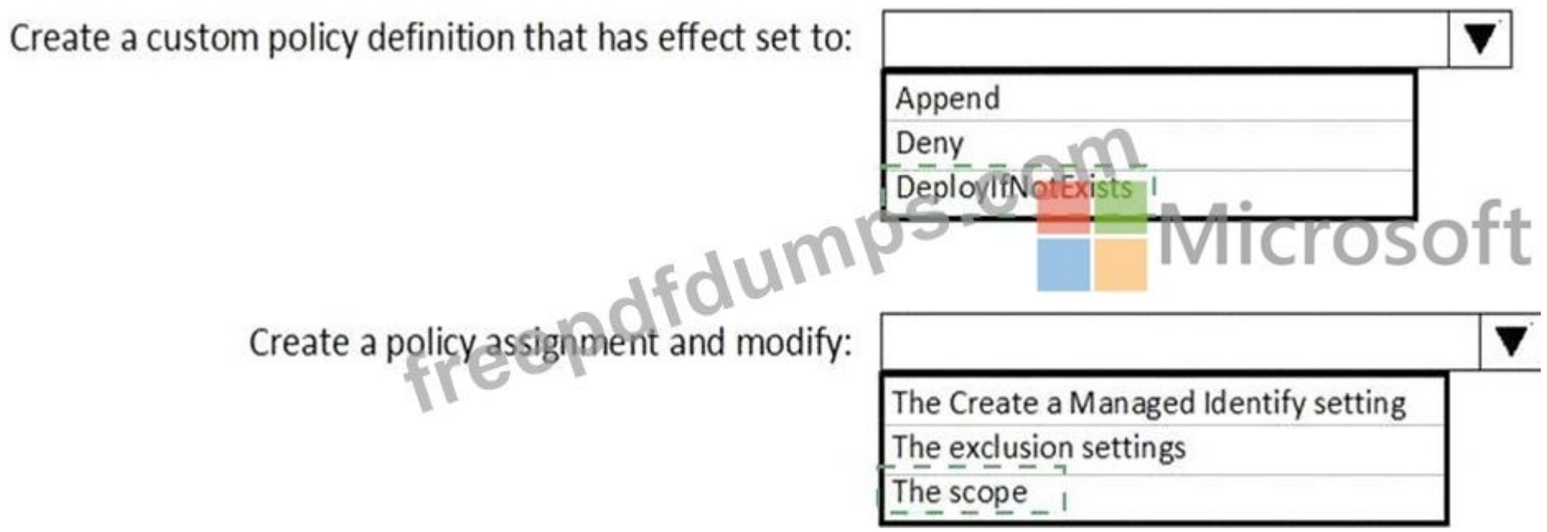
You need to deploy Microsoft Antimalware to meet the platform protection requirements.

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

NOTE: Each correct selection is worth one point.



Answer:



Explanation:
1. DeployifNotExists
2. Scope

NEW QUESTION: 94
You are troubleshooting a security issue for an Azure Storage account. You enable Azure Storage Analytics logs and archive it to a storage account. What should you use to retrieve the diagnostics logs?

A. File Explorer in Windows
B. the Microsoft Defender portal
C. AzCopy
D. Microsoft Defender for Cloud
Answer: C (LEAVE A REPLY)

NEW QUESTION: 95
You have an Azure subscription that contains a user named User1 and an Azure Container Registry named ConReg1.
You enable content trust for ContReg1.
You need to ensure that User1 can create trusted images in ContReg1. The solution must use the principle of least privilege.
Which two roles should you assign to User1? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. AcrQuarantineReader
B. Contributor
C. AcrPush
D. AcrImageSigner
E. AcrQuarantineWriter
Answer: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles

NEW QUESTION: 96
You have an Azure subscription name Sub1 that contains an Azure Policy definition named Policy1. Policy1 has the following settings:
Definition location: Tenant Root Group
Category: Monitoring
You need to ensure that resources that are noncompliant with Policy1 are listed in the Azure Security Center dashboard.
What should you do first?
A. Change the Category of Policy1 to Security Center.
B. Add Policy1 to a custom initiative.
C. Change the Definition location of Policy1 to Sub1.
D. Assign Policy1 to Sub1.
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/overview

NEW QUESTION: 97
You have an Azure subscription that is linked to an Azure AD tenant and contains the resources shown in the following table.

Name	Location	Description
Group1	*Not applicable*	Dynamic device security group in Azure AD
Managed1	East US	Managed identity
VM1	West US	Virtual machine that has a system-assigned managed identity
VM2	Central US	Virtual machine
App1	*Not applicable*	Enterprise application in Azure AD

Which resources can be assigned the Contributor role for VM1?
A. Group1. Managed1, and VM2only
B. Group1 and Managed1 only
C. Group1, Managed1, VM1. and App1 only
D. Managed1 and App1 only
Answer: D (LEAVE A REPLY)

NEW QUESTION: 98
You have an Azure subscription that contains an Azure Kubernetes Service (AKS) cluster named AKS1.
You have an Azure container registry that stores container images that were deployed by using Azure DevOps Microsoft-hosted agents.
You need to ensure that administrators can access AKS1 only from specific networks. The solution must minimize administrative effort.
What should you configure for AKS1?
A. a private endpoint
B. an Application Gateway Ingress Controller (AGIC)

C. a private cluster
D. authorized IP address ranges
Answer: (SHOW ANSWER)

NEW QUESTION: 99
Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
The company develops an application named App1. App1 is registered in Azure AD.
You need to ensure that App1 can access secrets in Azure Key Vault on behalf of the application users.
What should you configure?
A. an application permission without admin consent
B. a delegated permission without admin consent
C. a delegated permission that requires admin consent
D. an application permission that requires admin consent
Answer: B (LEAVE A REPLY)
Delegated permissions - Your client application needs to access the web API as the signed-in user, but with access limited by the selected permission. This type of permission can be granted by a user unless the permission requires administrator consent.
References:
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis

NEW QUESTION: 100
You have a Microsoft Entra tenant named contoso.com.
You collaborate with a partner organization that has a Microsoft Entra tenant named fabrikam.com. Fabrikam.
com has multi-factor authentication (MFA) enabled for all users.
Contoso.com has the Cross-tenant access settings configured as shown in the Cross-tenant access settings exhibit. (Click the Cross-tenant access settings:

Inbound access settings

Edit inbound defaults

Type	Applies to	Status
B2B collaboration	External users and groups	All allowed
B2B collaboration	Applications	All allowed
B2B direct connect	External users and groups	All blocked
B2B direct connect	Applications	All blocked
Trust settings	N/A	Disabled

Outbound access settings

Edit outbound defaults

Type	Applies to	Status
B2B collaboration	Users and groups	All allowed
B2B collaboration	External applications	All allowed
B2B direct connect	Users and groups	All blocked
B2B direct connect	External applications	All blocked

Contoso.com has the External collaboration settings configured as shown in the External collaboration settings exhibit. (Click the External collaboration settings tab.)

You create a Conditional Access policy that has the following settings:

* Name: CAPolicy1
* Assignments

o Guest or external users: B2B collaboration guest users

o Target resources

Include: All cloud apps o Access controls

Grant access

Require device to be marked as compliant

Require multi-factor authentication

Enable policy: On

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

NOTE: Each correct section is worth one point.

Answer Area

Statements	Yes	No
Users with devices that have a compliant device claim from fabrikam.com will be granted access to the cloud apps in contoso.com.	○	○
To minimize the number of MFA authentication prompts for the users in fabrikam.com, you must configure the Trust settings.	○	○
Users with devices that have a compliant device claim from fabrikam.com can review the user properties of the users in contoso.com.	○	○

Answer:

Answer Area

Statements	Yes	No
Users with devices that have a compliant device claim from fabrikam.com will be granted access to the cloud apps in contoso.com.	○	○
To minimize the number of MFA authentication prompts for the users in fabrikam.com, you must configure the Trust settings.	○	○
Users with devices that have a compliant device claim from fabrikam.com can review the user properties of the users in contoso.com.	○	○

Explanation:

Answer Area

Statements	Yes	No
Users with devices that have a compliant device claim from fabrikam.com will be granted access to the cloud apps in contoso.com.	◉	○
To minimize the number of MFA authentication prompts for the users in fabrikam.com, you must configure the Trust settings.	○	◉
Users with devices that have a compliant device claim from fabrikam.com can review the user properties of the users in contoso.com.	○	◉

NEW QUESTION: 101

You have an Azure subscription that contains three storage accounts, an Azure SQL managed instance named SQL1, and three Azure SQL databases.

The storage accounts are configured as shown in the following table.

Name	Type	Performance
storage1	StorageV2	Standard
storage2	StorageV2	Standard
storage3	BlockBlobStorage	Premium

SQL1 has the following settings:

* Auditing: On
* Audit log destination: storage!

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

Name	On server	Auditing	Audit log destination
DB1	SQL1	Off	*None*
DB2	SQL1	On	storage2
DB3	SQL1	Off	*None*

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
Audit events for DB1 are written to storage1.	○	○
Audit events for DB2 are written to storage1 and storage2.	○	○
Storage3 can be used as an audit log destination for DB3.	○	○

Answer:

Answer Area

Statements	Yes	No
Audit events for DB1 are written to storage1.	○	○
Audit events for DB2 are written to storage1 and storage2.	○	○
Storage3 can be used as an audit log destination for DB3.	○	○

Explanation:

NEW QUESTION: 102

You have an Azure Subscription that is connected to an on-premises datacenter and contains the resources shown in the following table.

Name	Description
storage1	A storage account
storage2	A storage account
KeyVault1	An Azure key vault
VNet1	A virtual network containing a single subnet that has five virtual machines connected
VNet2	A virtual network containing a single subnet that has three virtual machines connected

You need to configure virtual network service endpoints for VNet1 and VNet2. The solution must meet the following requirements:

* The virtual machines that connect to the subnet of VNet1 must access storage1, storage2, and Azure AD by using the Microsoft backbone network.
* The virtual machines that connect to the subnet of VNet2 must access storage1 and KeyVault1 by using the Microsoft backbone network.
* The virtual machines must use the Microsoft backbone network to communicate between VNet1 and VNet2.

How many service endpoints should you configure for each virtual network? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

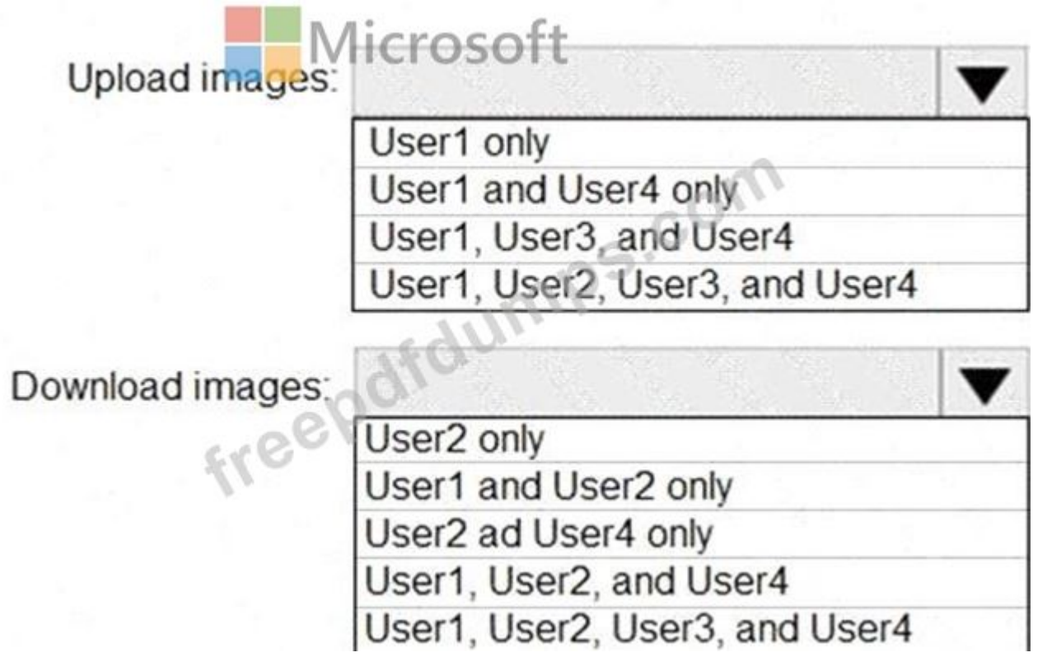
NEW QUESTION: 103
You have an Azure subscription that contains a web app named App1.
Users must be able to select between a Google identity or a Microsoft identity when authenticating to App1.
You need to add Google as an identity provider in Azure AD.
Which two pieces of information should you configure? Each correct answer presents part of the solution.
Each correct selection is worth one point
A. a tenant name
B. a tenant ID
C. the endpoint URL Of an application
D. a client ID
E. a client secret

Answer: D,E (LEAVE A REPLY)
https://learn.microsoft.com/en-us/azure/app-service/configure-authentication-provider-google

NEW QUESTION: 104
You have an Azure Container Registry named Registry1.
You add role assignment for Registry1 as shown in the following table.

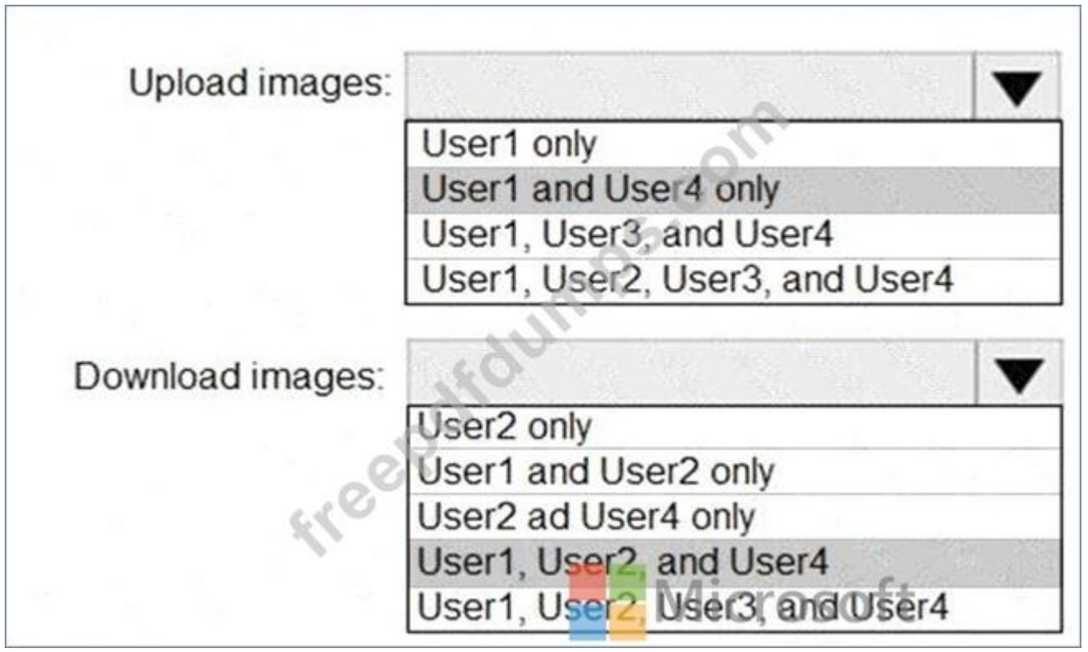
User	Role
User1	AcrPush
User2	AcrPull
User3	AcrImageSigner
User4	Contributor

Which users can upload images to Registry1 and download images from Registry1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Box 1: User1 and User4 only

Owner, Contributor and AcrPush can push images.

Box 2: User1, User2, and User4

All, except AcrImagineSigner, can download/pull images.

Role/Permission	Access Resource Manager	Create/delete registry	Push image	Pull image	Delete image data	Change policies	Sign images
Owner	X	X	X	X	X	X	
Contributor	X	X	X	X	X	X	
Reader	X			X			
AcrPush			X	X			
AcrPull				X			
AcrDelete					X		
AcrImageSigner							X

References:

https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles

NEW QUESTION: 105

You have an Azure subscription.

You plan to use Microsoft Defender for Cloud to provide AI security posture management capabilities.

You need to recommend a Defender for Cloud plan that supports the deployment requirements. The solution must minimize costs.

What should you recommend?

A. Defender Cloud Security Posture Management (CSPM)

B. Microsoft Defender for App Service

C. Microsoft Defender for APIs

D. Foundational Cloud Security Posture Management (CSPM)

Answer: D (LEAVE A REPLY)

NEW QUESTION: 106

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.

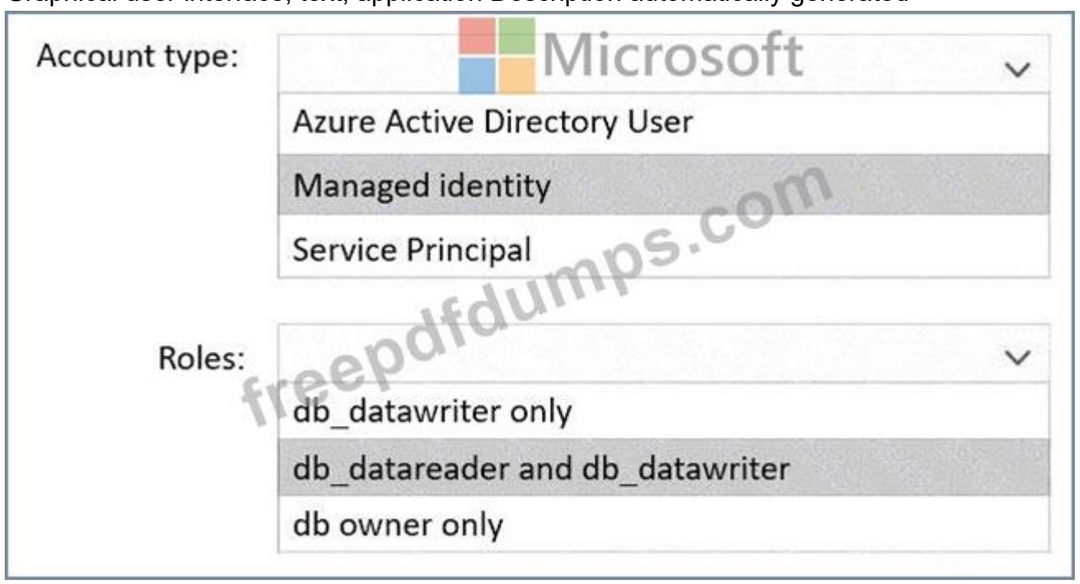
Which type of account should App1 use to access SQL1, and which database roles should you assign to App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Graphical user interface, text, application Description automatically generated



Reference:

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

NEW QUESTION: 107

Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.

After syncing all on-premises identities to Azure AD, you are informed that users with a givenName attribute starting with LAB should not be allowed to sync to Azure AD.

Which of the following actions should you take?

A. You should make use of the Synchronization Rules Editor to create an attribute-based filtering rule.

B. You should configure a DNAT rule on the Firewall.

C. B. You should configure a network traffic filtering rule on the Firewall.

D. You should make use of Active Directory Users and Computers to create an attribute-based filtering rule.

Answer: A (LEAVE A REPLY)

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

Reference:

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

NEW QUESTION: 108

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

Name	Member of	Mobile phone	Multi-factor authentication (MFA) status
User1	Group1	123 555 7890	Disabled
User2	Group1, Group2	None	Enabled
User3	Group1	123 555 7891	Required

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

* Assignment: Include Group1, Exclude Group2
* Conditions: Sign-in risk of Medium and above
* Access: Allow access, Require password change

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
f User1 signs in from an unfamiliar location, he must change his password.	○	○
If User2 signs in from an anonymous IP address, she must change her password.	○	○
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password	○	○

Answer:

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	○	○
If User2 signs in from an anonymous IP address, she must change her password.	○	○
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	○	○

Explanation:

Answer Area

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	○	○
If User2 signs in from an anonymous IP address, she must change her password.	○	○
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	○	○

Box 1: Yes

User1 is member of Group1. Sign in from unfamiliar location is risk level Medium.

Box 2: Yes

User2 is member of Group1. Sign in from anonymous IP address is risk level Medium.

Box 3: No

Sign-ins from IP addresses with suspicious activity is low.

Note:

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

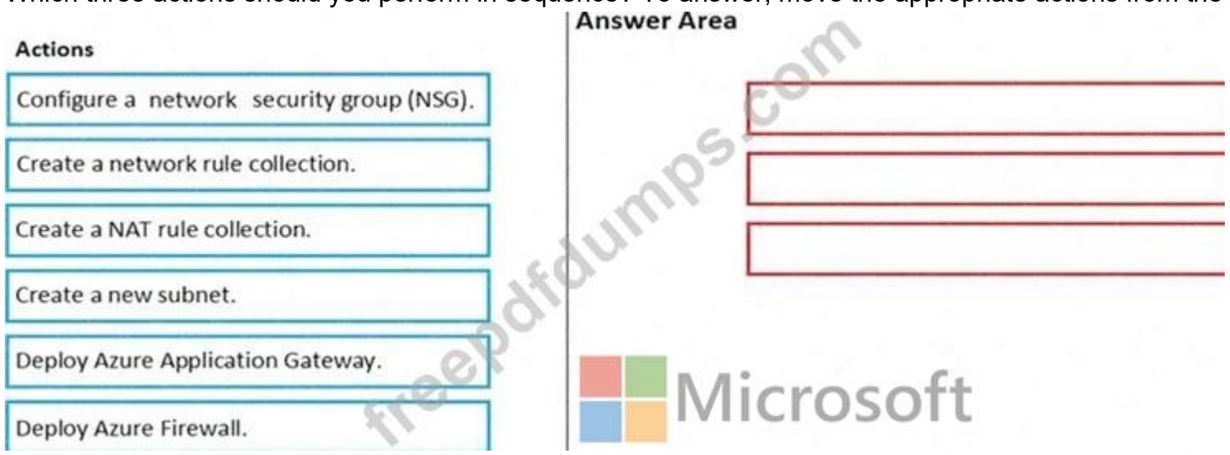
Azure AD Identity protection can detect six types of suspicious sign-in activities:

* Users with leaked credentials
* Sign-ins from anonymous IP addresses
* Impossible travel to atypical locations
* Sign-ins from infected devices
* Sign-ins from IP addresses with suspicious activity

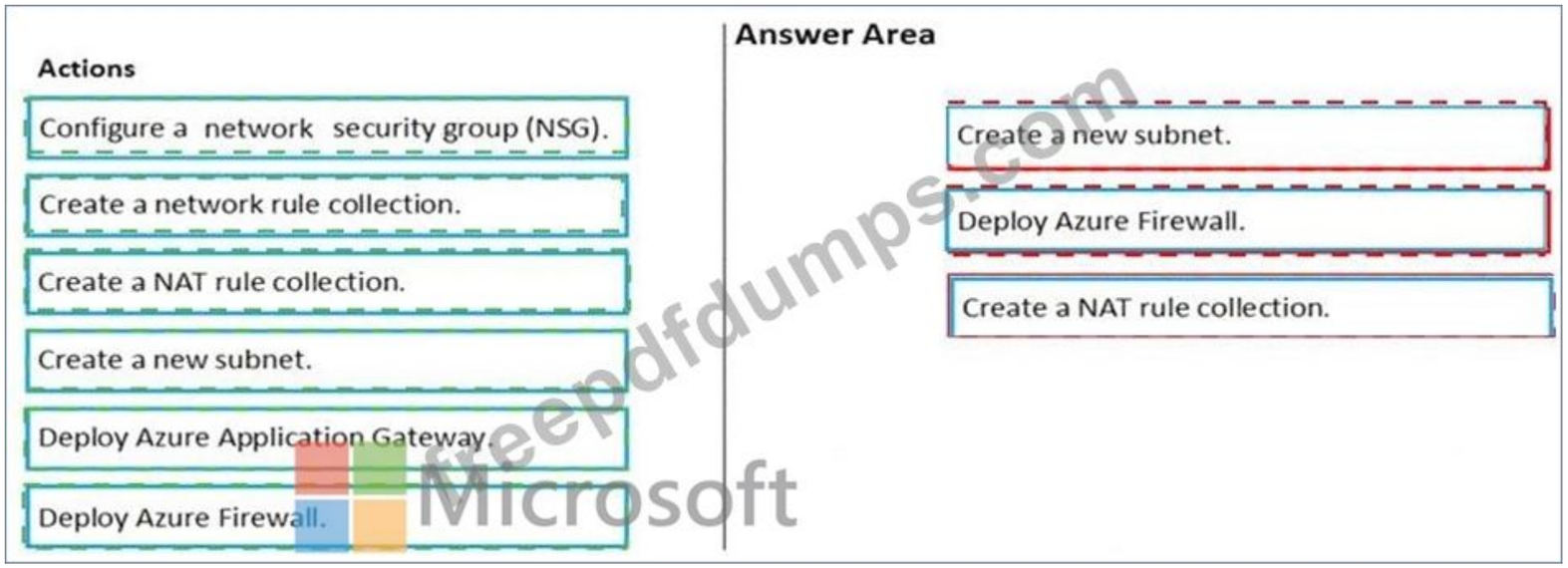
* Sign-ins from unfamiliar locations
These six types of events are categorized in to 3 levels of risks - High, Medium & Low:
References:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/

NEW QUESTION: 109
You have an Azure subscription that contains a web app named Appl. App1 provides users with product images and videos. Users access App1 by using a URL of HTTPS://appl.contoso.com. You deploy two server pools named Pool! and Pool2. Pool1 hosts product images. Pool2 hosts product videos. You need to optimize The performance of Appl. 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 Bastion
B. Azure Front Door
C. Azure Application Gateway
D. Azure Traffic Manager
Answer: C (LEAVE A REPLY)

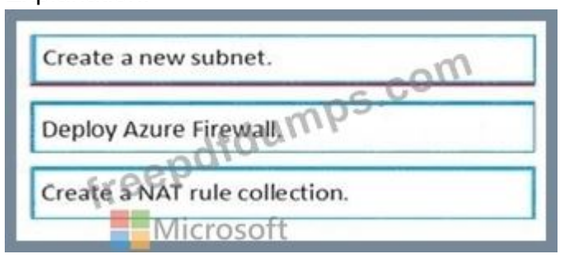
NEW QUESTION: 110
You have an Azure subscription that contains the following resources:
* A virtual network named VNET1 that contains two subnets named Subnet1 and Subnet2.
* A virtual machine named VM1 that has only a private IP address and connects to Subnet1.
You need to ensure that Remote Desktop connections can be established to VM1 from the internet.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange then in the correct order.



Answer:

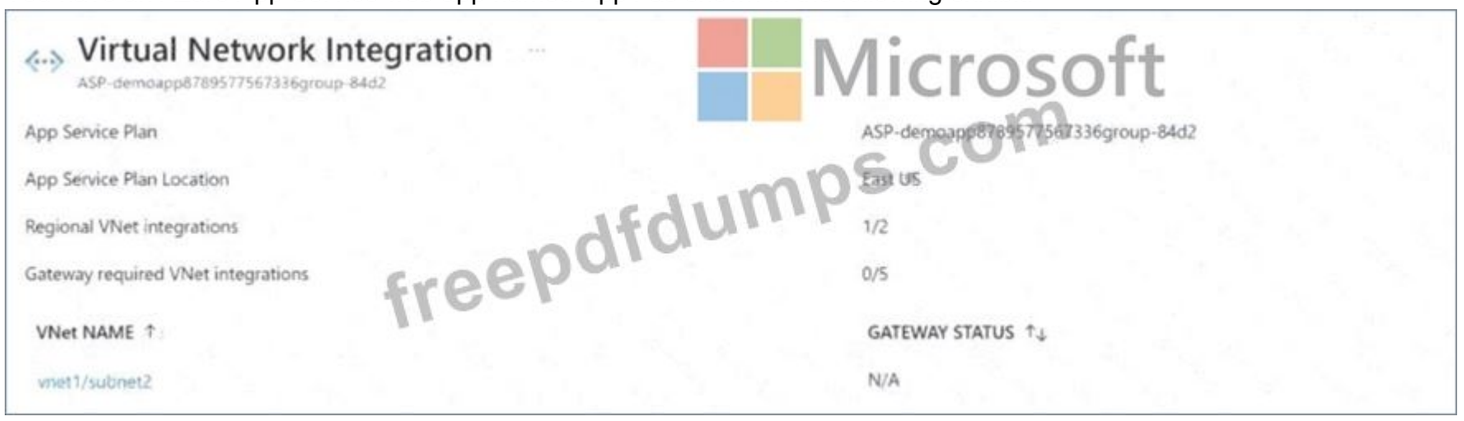


Explanation:



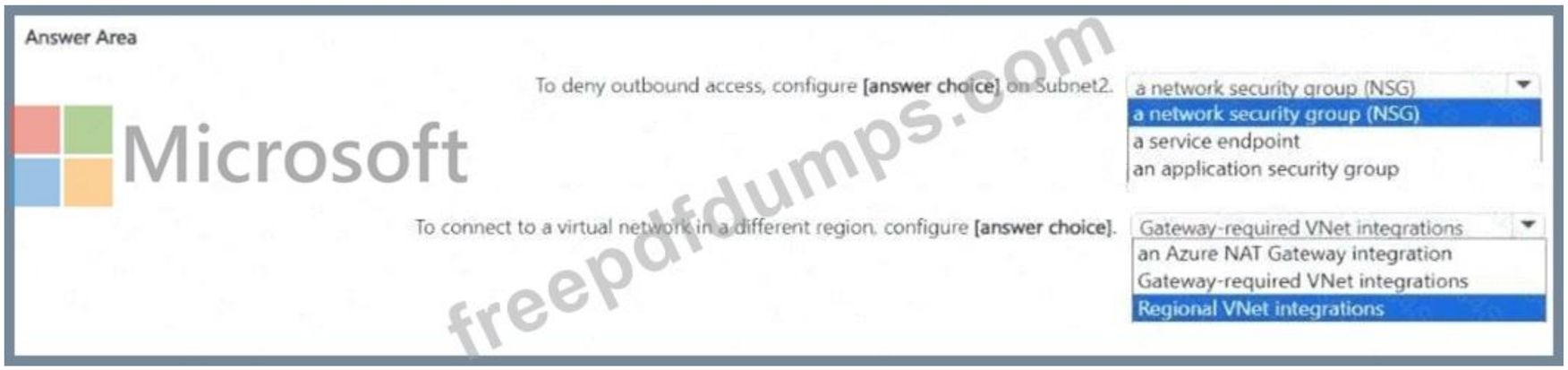
NEW QUESTION: 111

You have an Azure App Service web app named App1 as shown in the following exhibit.

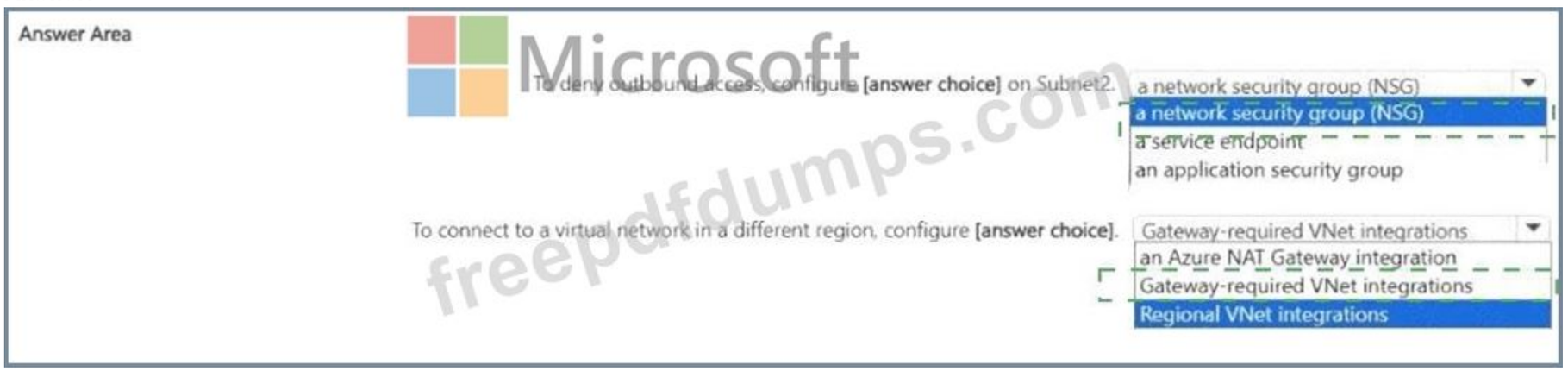


Subnet 2 contains a virtual machine named VM1.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic NOTE: Each correct selection is worth one point.



Answer:



Explanation:

NEW QUESTION: 112

You have a Microsoft Entra tenant that uses Microsoft Entra Permissions Management and contains the accounts shown in the following table:

Name	Role
Admin1	Global Administrator
Admin2	Privileged Role Administrator
Admin3	Privileged Authentication Administrator
Admin4	Exchange Administrator

Which accounts will be listed as assigned to highly privileged roles on the Azure AD insights tab in the Entra Permissions Management portal?

A. Admin1. Admin2, and Admin3 only

B. Admin2 and Admin3 only

C. Admin2. Admin3, and Admin4 only

D. Admin2 and Admin4 only
E. Admin1 only
F. Admin1. Admin2, Admin3. and Admin4
Answer: A (LEAVE A REPLY)

NEW QUESTION: 113
You need to recommend which virtual machines to use to host App1. The solution must meet the technical requirements for KeyVault1.
Which virtual machines should you use?
A. VM1, VM2, VM3. and VM4
B. VM1 and VM2 only
C. VM1 only
D. VM1, VM2, and VM4 only
Answer: (SHOW ANSWER)

NEW QUESTION: 114
You have multiple development teams that will create apps in Azure.
You plan to create a standard development environment that will be deployed for each team.
You need to recommend a solution that will enforce resource locks across the development environments and ensure that the locks are applied in a consistent manner.
What should you include in the recommendation?
A. an Azure policy
B. an Azure Resource Manager template
C. a management group
D. an Azure blueprint
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

NEW QUESTION: 115
You have a Microsoft Entra tenant that contains a user named User1.
You plan to enable passwordless authentication for the tenant.
You need to ensure that User1 can enable the combined registration experience. The solution must use the principle of least privilege.
Which role should you assign to User1?
A. Authentication Administrator
B. Security Administrator
C. Privileged Role Administrator
D. Global Administrator
Answer: A (LEAVE A REPLY)

NEW QUESTION: 116
Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals.

More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.
After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.
You have an Azure subscription that contains the resources shown in the following table.

Name	Type
Group1	Security group
Group2	Microsoft 365 group
App1	App registration
MI1	User-assigned managed identity

You have The users shown in the following table.

Name	Description
User1	• Member of Group1 and Group2 • Assigned Owner role for App1 and MI1
User2	• Member of Group1 and Group2 • Assigned Owner role for App1 and MI1

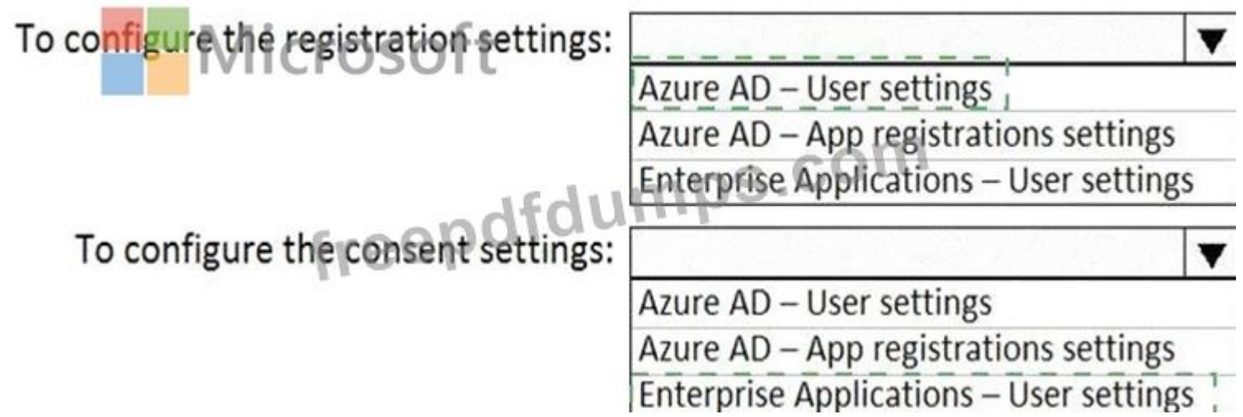
You create an Azure SQL managed instance named SQL1 and enable Microsoft Entra-only authentication.
You need to ensure that both User1 and User2 are set as the Microsoft Entra admin for SQL1.
Solution: You set MM as the Microsoft Entra admin for SQL1.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)

NEW QUESTION: 117
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.

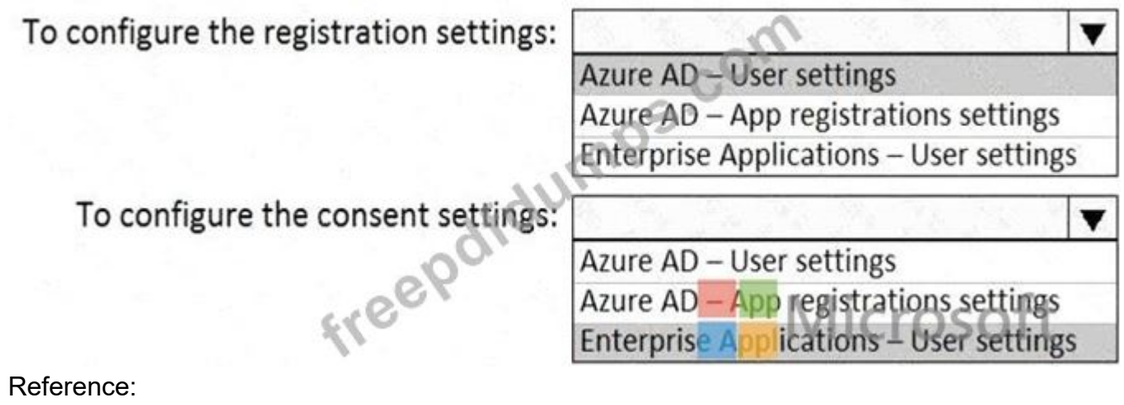
To configure the registration settings:
- Azure AD – User settings
- Azure AD – App registrations settings
- Enterprise Applications – User settings

To configure the consent settings:
- Azure AD – User settings
- Azure AD – App registrations settings
- Enterprise Applications – User settings

Answer:



Explanation:



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

Topic 2, Contoso

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

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

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

To start the case study

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

Overview

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

The company hosts its entire server infrastructure in Azure.

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

Technical requirements

Contoso identifies the following technical requirements:

* Deploy Azure Firewall to VNetWork1 in Sub2.

* Register an application named App2 in contoso.com.
* Whenever possible, use the principle of least privilege.
* Enable Azure AD Privileged Identity Management (PIM) for contoso.com

Existing Environment

Azure AD

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

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

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

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

Sub1

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

User2 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

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

Sub1 contains the Azure policies shown in the following table.

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

Sub2

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

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet1.1
VM2	NIC2	ASG2	Subnet1.1
VM3	NIC3	*None*	Subnet1.2
VM4	NIC4	ASG1	Subnet1.3
VM5	NIC5	*None*	Subnet2.1

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

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

Name	Associated to
NSG1	NIC2
NSG2	Subnet1.1
NSG3	Subnet1.3
NSG4	Subnet2.1

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

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

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

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

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

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

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

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

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

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

Contoso identifies the following technical requirements:

* Deploy Azure Firewall to VNetwork1 in Sub2.
* Register an application named App2 in contoso.com.
* Whenever possible, use the principle of least privilege.
* Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

NEW QUESTION: 118

You have an Azure subscription that contains a user named UseR1. You need to ensure that UseR1 can perform the following tasks:

* Create groups.
* Create access reviews for role-assignable groups.
* Assign Azure AD roles to groups.

The solution must use the principle of least privilege. Which role should you assign to User1?

A. Groups administrator
B. Identity Governance Administrator
C. Authentication administrator
D. Privileged role administrator
Answer: D (LEAVE A REPLY)

NEW QUESTION: 119

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

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

You use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

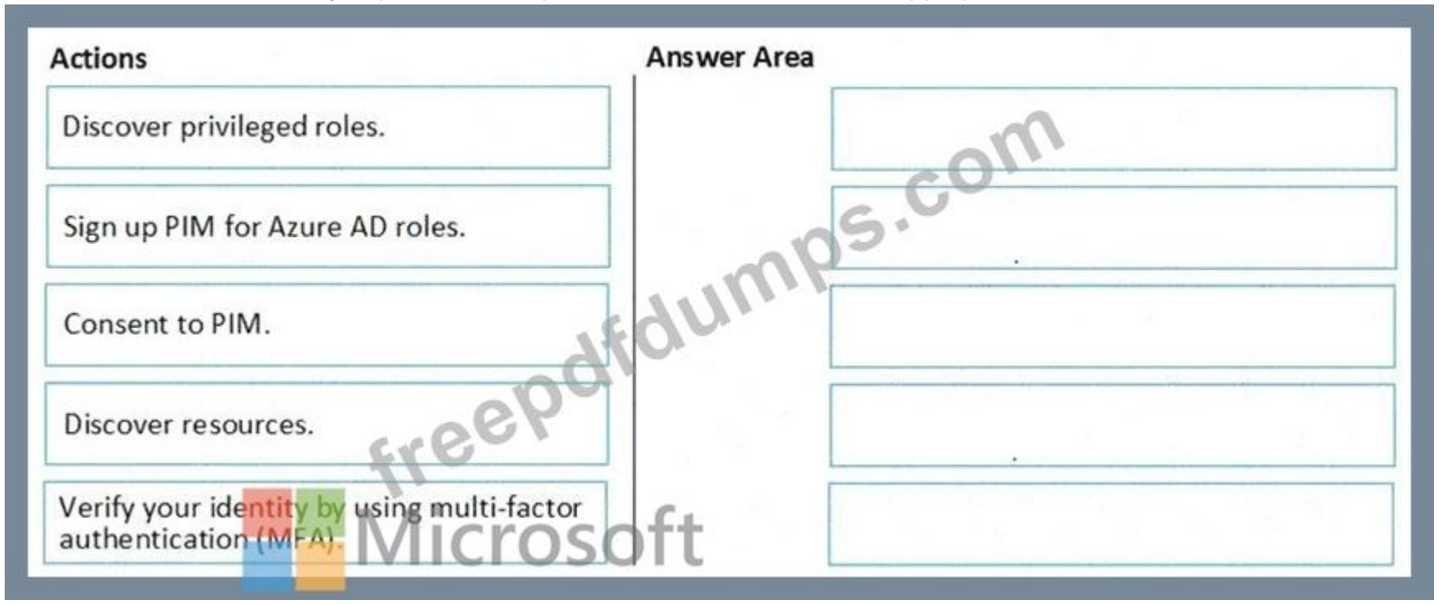
Solution: You create a policy definition and assignments that are scoped to resource groups.

Does this meet the goal?

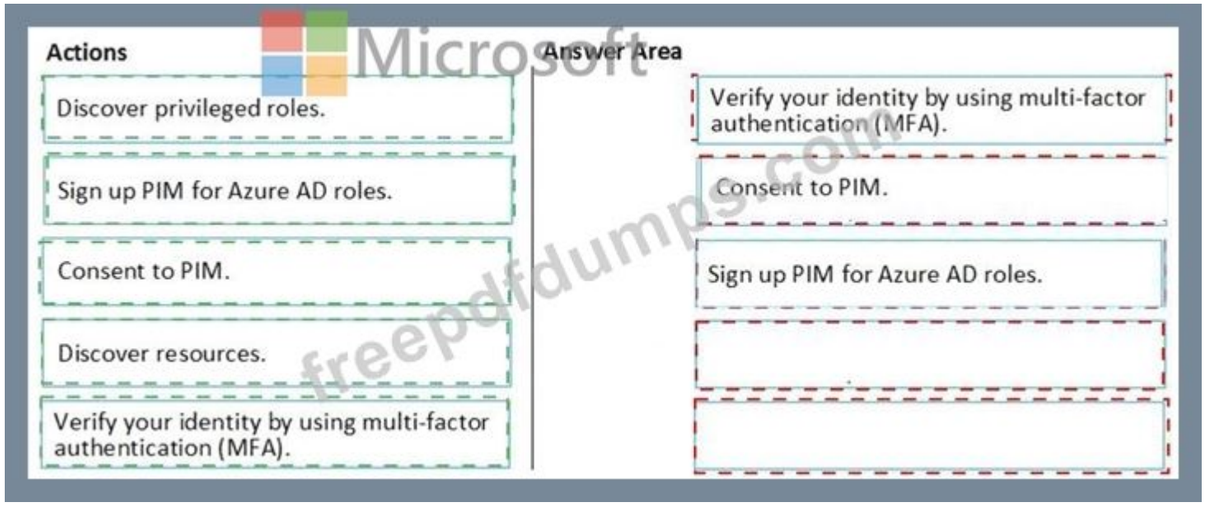
A. Yes
B. No
Answer: (SHOW ANSWER)

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

NEW QUESTION: 120
You create an Azure subscription with Azure AD Premium P2.
You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure roles.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



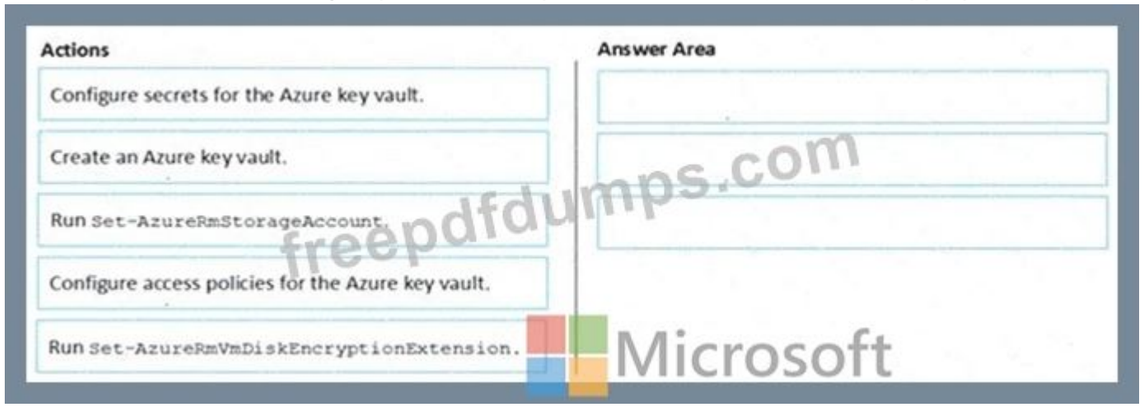
Answer:



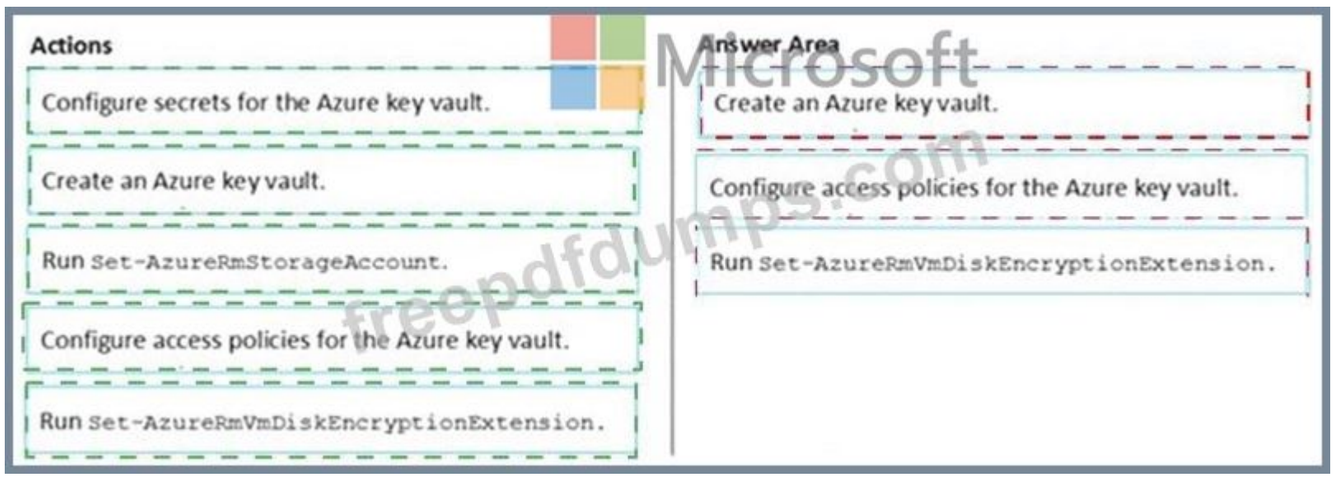
Explanation:
1. Verify your identity with MFA
2. Consent to PIM
3. Sign up PIM for AAD Roles

NEW QUESTION: 121
You have an Azure subscription that contains an Azure SQL server named SQL1. SQL1 contains. You need to use Microsoft Defender for Cloud to complete a vulnerability assessment for DB1. What should you do first?
A. Configure the Send scan report to setting.
B. Set Periodic recurring scans to ON.
C. Enable the Microsoft Defender for SQL plan.
D. From Advanced Threat Protection types, select SQL injection vulnerability.
Answer: D (LEAVE A REPLY)

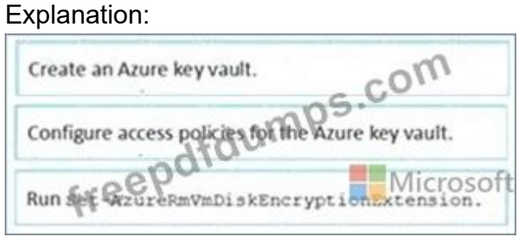
NEW QUESTION: 122
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Subscription named Sub1. Sub1 contains an Azure virtual machine named VM1 that runs Windows Server 2016.
You need to encrypt VM1 disks by using Azure Disk Encryption.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:



References:

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

NEW QUESTION: 123

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

A. KeyVault1 only

B. KeyVault2 and KeyVault3 only

C. KeyVault1 and KeyVault3 only

D. KeyVault1 KeyVault2 and KeyVault3

Answer: B (LEAVE A REPLY)

The storage account and the key vault must be in the same region and in the same Azure Active Directory (Azure AD) tenant, but they can be in different subscriptions.

Storage1 is in the West US region. KeyVault1 is the only key vault in the same region.

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview

NEW QUESTION: 124

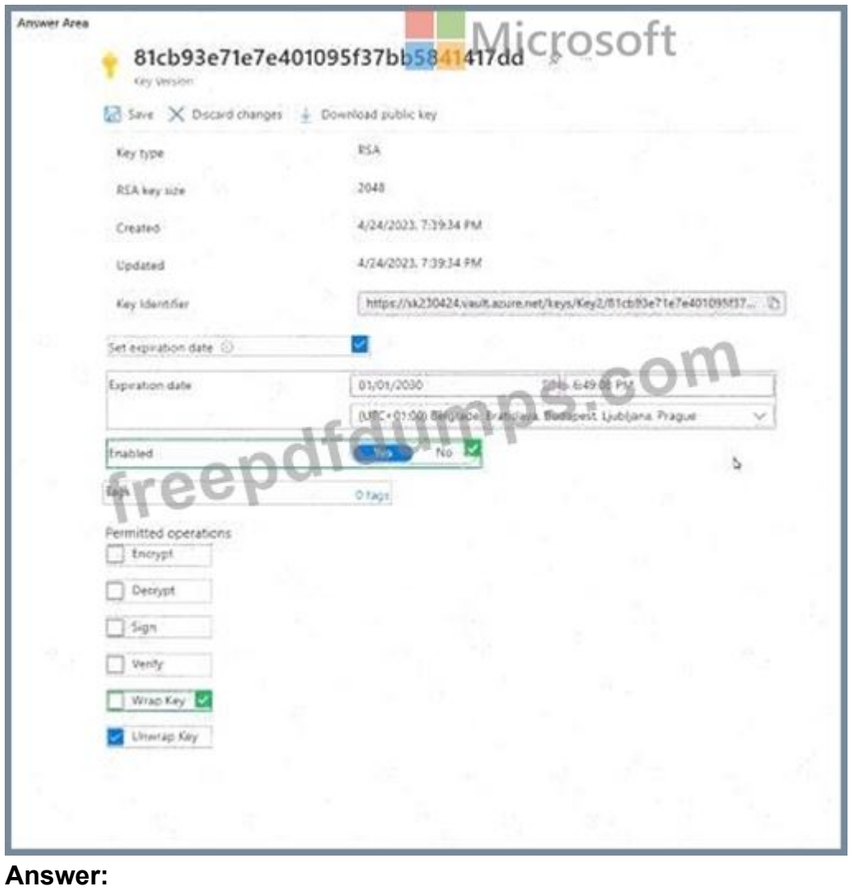
You have an Azure subscription that contains an Azure key vault and an Azure SQL database named SQL1.

You generate a key named Key1.

You need to enable Transparent Data Encryption (TDE) for SQL1 by using Key1.

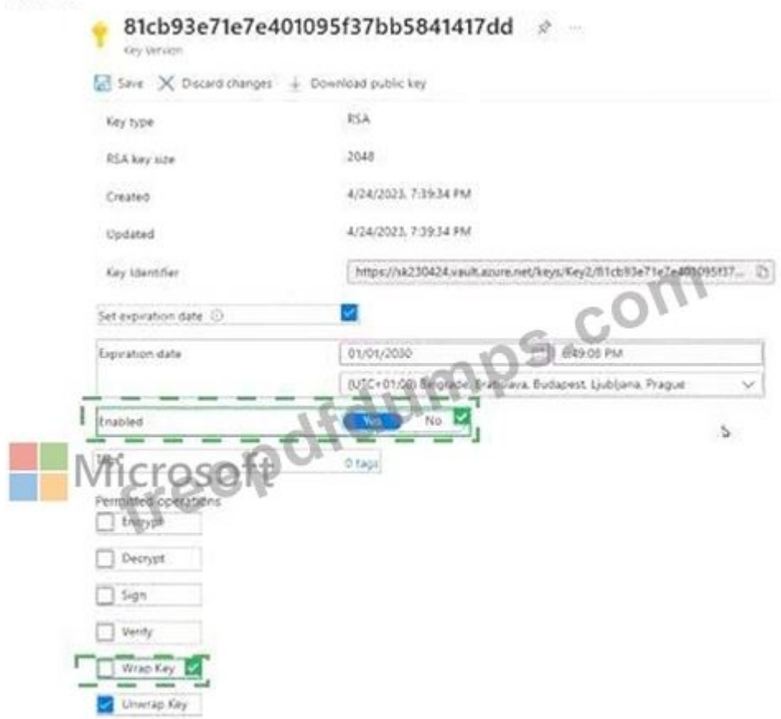
Which two settings should you modify for Key1? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Answer Area



Explanation:

NEW QUESTION: 125

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

Name	Type	Description
RG1	Resource group	Used to store virtual machines
RG2	Resource group	Used to store virtual networks
ServerAdmins	Security group	Used to manage virtual machines

You need to ensure that ServerAdmins can perform the following tasks:

Create virtual machine to the existing virtual network in RG2 only.

The solution must use the principle of least privilege.

Which two role-based access control (RBAC) roles should you assign to ServerAdmins? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. the Network Contributor role for RG1.

B. the Network Contributor role for RG2

C. the Virtual Machine Contributor role for RG1.

D. the Contributor role for the subscription

E. a custom RBAC role for RG2

F. A custom RBAC role for the subscription

Answer: (SHOW ANSWER)

NEW QUESTION: 126
You have an on-premises datacenter that contains multiple servers.
You have an Azure subscription.
You plan to onboard the on-premises servers to Microsoft Defender for Cloud by using a script.
You need to create an identity to enable the script to run without prompting for Microsoft Entra credentials.
Which type of identity should you create?
A. service principal
B. user account
C. system-assigned managed identity
D. user-assigned managed identity
E. group account
Answer: (SHOW ANSWER)

NEW QUESTION: 127
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.) References:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/sql-database/sql-database-aad- authentication-configure.md

NEW QUESTION: 128
You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Subnet	Subnet-associated network security group (NSG)	Peered with
VNet1	Subnet1	NSG1	VNet2
VNet2	Subnet2	NSG2	VNet1

NSG1 and NSG2 both have default rules only.
The subscription contains the virtual machines shown in the following table.

Name	Connected to
VM1	Subnet1
VM2	Subnet2

The subscription contains the web apps shown in the following table.

Name	Description
WebApp1	Uses an App Service plan in the Premium pricing tier and has virtual network integration with VNet1
WebApp2	Uses an App Service plan in the Isolated pricing tier and is deployed to Subnet2

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
WebApp1 can connect to VM2.	○	○
NSG1 controls inbound traffic to WebApp1.	○	○
WebApp2 can connect to VM1.	○	○

Answer:

Answer Area

Statements	Yes	No
WebApp1 can connect to VM2.	○	○
NSG1 controls inbound traffic to WebApp1.	○	○
WebApp2 can connect to VM1.	○	○

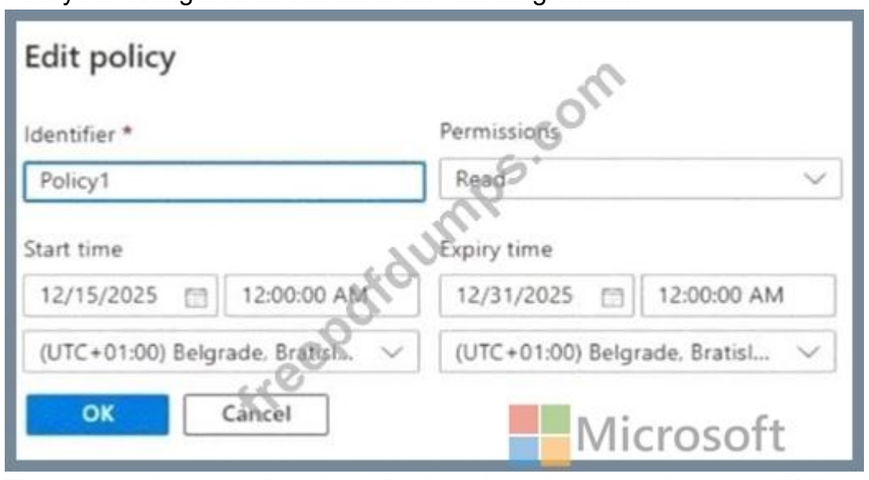
Explanation:

NEW QUESTION: 129

You have an Azure subscription that contains two users named User1 and User2 and the blob containers shown in the following table.

Name	Storage account	Access policy
container1	storage1	Policy1
container2	storage1	*None*

Policy1 is configured as shown in the following exhibit.



The storage1 account has the following shared access signature (SAS) named SAS1:

* Allowed services: Blob
* Allowed resource types: Container
* Allowed permissions: Read, Write. List, Add, Create
* Blob versioning permissions: Enables deletion of versions
* Allowed blob index permissions: Read/Write
* Start and expiry date/time:

o Start: 12/1/2025

o End: 12/31/2025

Dates are in MM/DD/YYYY format.

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

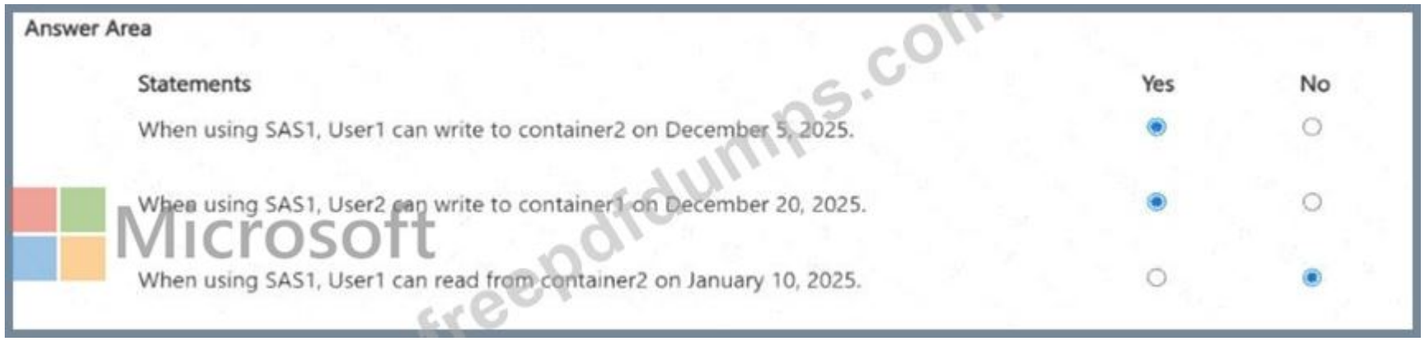
Statements	Yes	No
When using SAS1, User1 can write to container2 on December 5, 2025.	○	○
When using SAS1, User2 can write to container1 on December 20, 2025.	○	○
When using SAS1, User1 can read from container2 on January 10, 2025.	○	○

Answer:

Answer Area

Statements	Yes	No
When using SAS1, User1 can write to container2 on December 5, 2025.	○	○
When using SAS1, User2 can write to container1 on December 20, 2025.	○	○
When using SAS1, User1 can read from container2 on January 10, 2025.	○	○

Explanation:



NEW QUESTION: 130

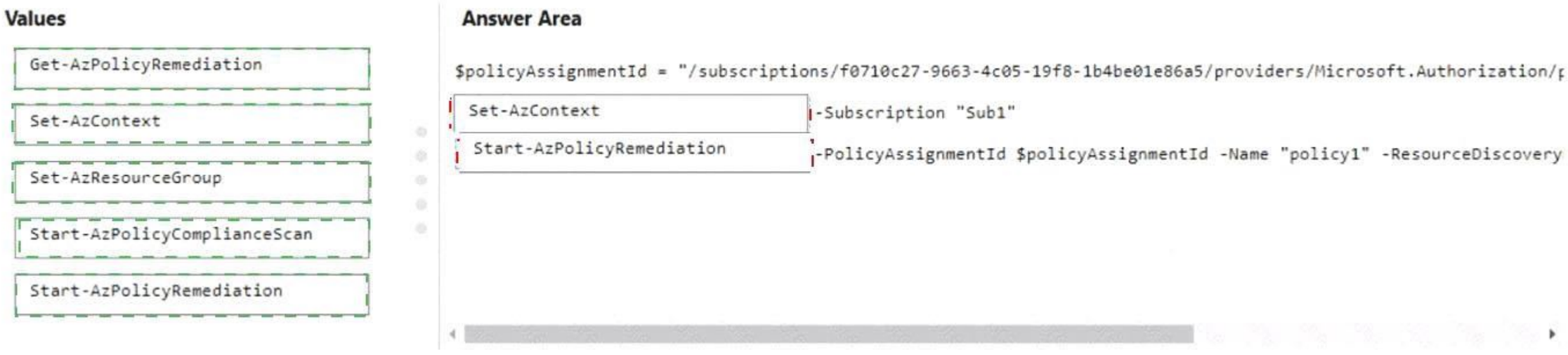
You have two Azure subscriptions named Sub1 and Sub2. Sub1 contains a resource group named RG1 and an Azure policy named Policy1.

You need to remediate the non-compliant resources in Sub1 based on Policy1.

How should you complete the PowerShell script? To answer, drag the appropriate values to the correct targets. Each value 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:

* For the first blank, use Set-AzContext to set the current subscription context.
* For the second blank, use Start-AzPolicyRemediation to create and start a policy remediation for a policy assignment.

The final script should look like this:

$policyAssignmentId = " /subscriptions/f0710c27-9663-4c05-1978-1bdbedle86as/providers/Microsoft.
Authorization/f Value Set-AzContext -Subscription "Sub1" Value Start-AzPolicyRemediation - PolicyAssignmentId $policyAssignmentId -Name " policy1" -ResourceDiscovery

NEW QUESTION: 131

You have an on-premises server named Server1.

You have an Azure subscription that contains a Microsoft Sentinel workspace named Sentinel 1.

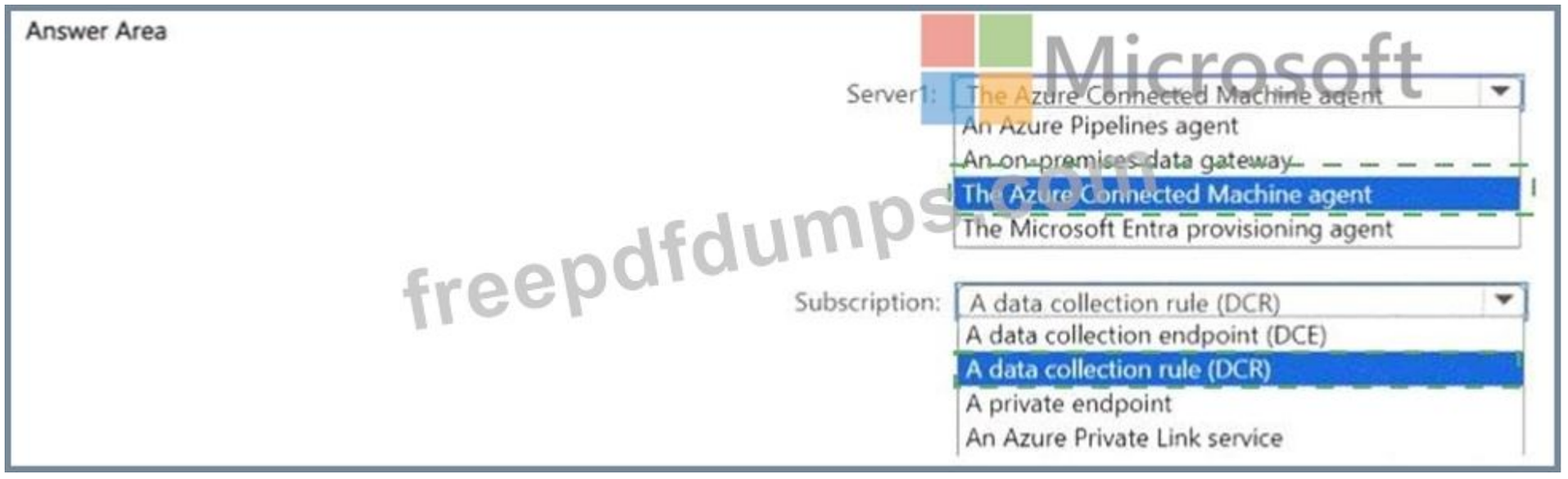
You install the Windows Firewall solution in Sentinel1.

You need to use Microsoft Sentinel to monitor Windows Defender Firewall on Server1.

What should you install on Server1, and what should you create in the Azure subscription? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:



Explanation:

NEW QUESTION: 132

You have been tasked with configuring an access review, which you plan to assigned to a new collection of reviews. You also have to make sure that the reviews can be reviewed by resource owners.

You start by creating an access review program and an access review control.

You now need to configure the Reviewers.

Which of the following should you set Reviewers to?

A. Selected users.

B. Members (Self).

C. Group Owners.

D. Anyone.

Answer: C (LEAVE A REPLY)

In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.
Graphical user interface, application Description automatically generated with medium confidence

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review
https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls

NEW QUESTION: 133
You have an Azure subscription. That contains the virtual machines shown in the following table.

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2022
Computer3	SUSE Linux Enterprise Server (SLES)

You need to enable file integrity monitoring in Microsoft Defender for Cloud. Which computers will support file integrity monitoring?
A. Computer1, Computer2, and Computer3
B. Computer 1 and Computer2 only
C. Computed and Computed only
D. Computed only
Answer: (SHOW ANSWER)

NEW QUESTION: 134
You have an Azure subscription that contains virtual machines.
You enable just in time (JIT) VM access to all the virtual machines.
You need to connect to a virtual machine by using Remote Desktop.
What should you do first?
A. From Azure Directory (Azure AD) Privileged Identity Management (PIM), activate the Security administrator user role.
B. From Azure Active Directory (Azure AD) Privileged Identity Management (PIM), activate the Owner role for the virtual machine.
C. From the Azure portal, select the virtual machine, select Connect, and then select Request access.
D. From the Azure portal, select the virtual machine and add the Network Watcher Agent virtual machine extension.
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/connect-logon

NEW QUESTION: 135
You have an Azure subscription that contains a route table named RT1. RT1 includes a route that has the following configurations:
* Name: RouteA
* IP address prefix: 192.168.0.0/24
* Next hop IP address: 172.16.10.10
You are evaluating whether to add the routes shown in the following table.

Name	IP address prefix	Next hop IP address
Route1	192.168.0.0/16	172.16.10.20
Route2	192.168.0.0/24	172.16.10.30
Route3	192.168.0.0/28	172.16.10.40

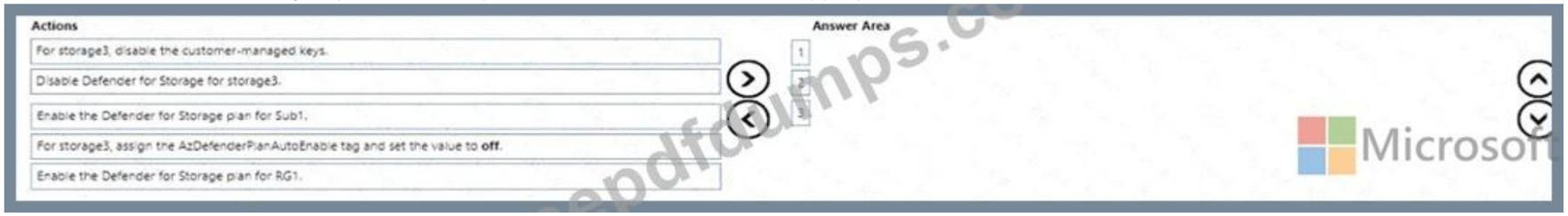
Which routes can you add to RT1?
A. Route1 and Route3 only
B. Route1 only
C. Route1 and Route2 only
D. Route2 and Route3 only
E. Route3 only
F. Route2 only
Answer: A (LEAVE A REPLY)

NEW QUESTION: 136
You have a Microsoft Entra tenant.
You need to prevent nonprivileged Microsoft Entra users from creating service principals in Microsoft Entra ID.
A. From the Properties blade, set Enable Security defaults to Yes.
B. From the Properties blade, set Access management for Azure resources to No.
C. From the User settings blade, set Restrict access to Microsoft Entra ID administration portal to Yes.
D. From the User settings blade, set Users can register applications to No.
Answer: D (LEAVE A REPLY)

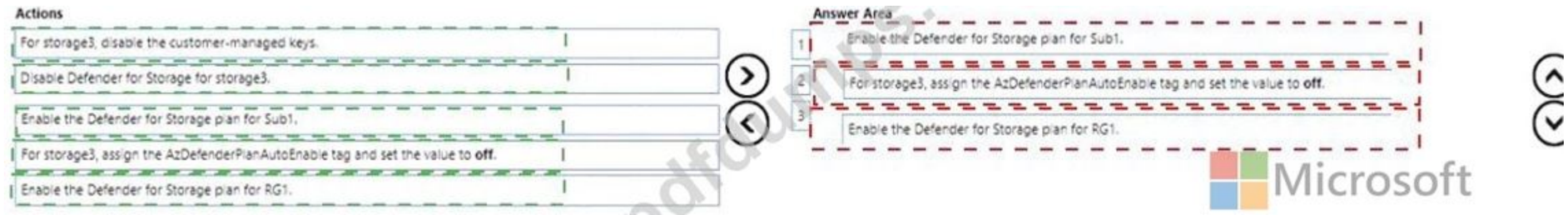
NEW QUESTION: 137
You have an Azure subscription named Sub1 that contains the storage accounts shown in the following table

Name	Resource group
storage1	RG1
storage2	RG1
storage3	RG2

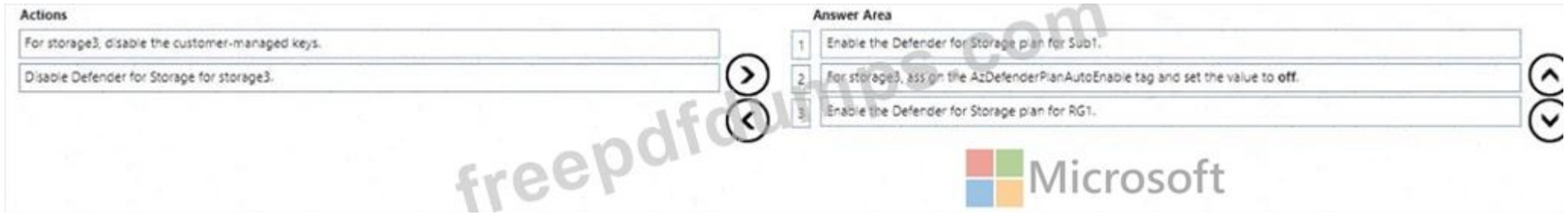
The storage3 storage account is encrypted by using customer-managed keys.
YOU need to enable Microsoft Defender for storage to meet the following requirements.
* The storage1 and storage2 account must be include in the defender for storage requirement.
* The storage3 account must be exclude from the Defender for Storage protections.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and them in the correct order.



Answer:



Explanation:



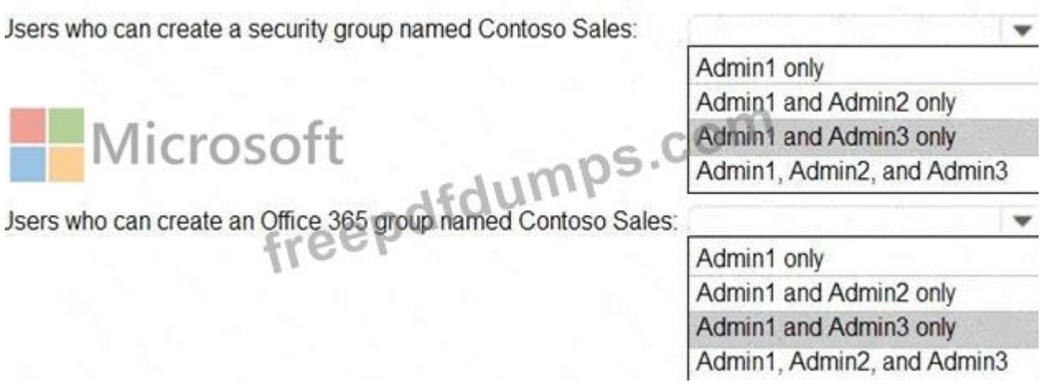
NEW QUESTION: 138
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

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.

Answer:

Explanation:



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

NEW QUESTION: 139
You have an Azure subscription that contains the virtual machines shown in the following table.

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

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

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

On which virtual machines is the Log Analytics agent installed?
A. VM3 only
B. VM1 and VM3 only
C. VM3 and VM4 only
D. VM1, VM2, VM3, and VM4
Answer: D (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: 140
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.
You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.
Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.
Solution: You recommend the use of federation with Active Directory Federation Services (AD FS).
Does the solution meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
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.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

NEW QUESTION: 141
You have an Azure subscription that contains an Azure SQL database named SQL1 and an Azure key vault named KeyVault1. KeyVault1 stores the keys shown in the following table.

Name	Type	RSA key size	Elliptic curve name
Key1	RSA	2048	*Not applicable*
Key2	RSA	3072	*Not applicable*
Key3	RSA	4096	*Not applicable*
Key4	EC	*Not applicable*	P-512

You reed to configure Transparent Data Encryption (TDE). TDE will use a customer-managed key for SQL1?

A. Key2 only

B. Key1 only

C. Key1 and key2 only

D. Key1. Key2 Key3. and Key4

E. Key2 and Key3 only

Answer: E (LEAVE A REPLY)

NEW QUESTION: 142

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

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

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

What should you do?

A. Enable a managed service identity on VM1.

B. Create a secret in KV1.

C. Configure a service endpoint on SQL1.

D. Create a key in KV1.

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 143

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

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

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

Name                                    :  StorageEA2Allow
ProvisionIngState                       :  Succeeded
Description                             :
Protocol                                :  *
SourcePortRange                         :  {*}
DestinationPortRange                    :  {443}
SourceAddressPrefix                     :  {*}
DestinationAddressPrefix                :  {Storage/EastUS2}
SourceApplicationSecurityGroups         :  []
DestinationApplicationSecurityGroups    :  []
Access                                  :  Allow
Priority                                :  104
Direction                               :  Outbound
                                        :
Name                                    :  Contoso_FTP
Description                             :
Protocol                                :  TCP
SourcePortRange                         :  {*}
DestinationPortRange                    :  {21}
SourceAddressPrefix                     :  {1.2.3.4/32}
DestinationAddressPrefix                :  {10.0.0.5/32}
SourceApplicationSecurityGroups         :  []
DestinationApplicationSecurityGroups    :  []
Access                                  :  Allow
Priority                                :  504
Direction                               :  Inbound
```

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

NOTE: Each correct selection is worth one point.

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

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

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

- allowed
- dropped
- forwarded

Answer:

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

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

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

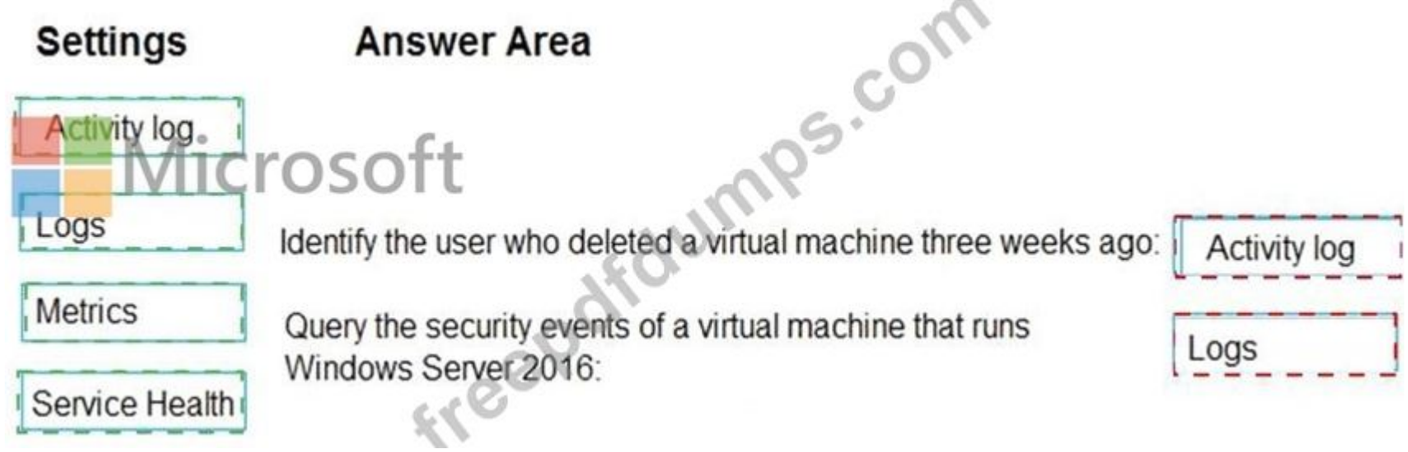
- allowed
- dropped
- forwarded

Explanation:
Box 1: able to connect to East US 2
The StorageEA2Allow has DestinationAddressPrefix {Storage/EastUS2}
Box 2: dropped
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group

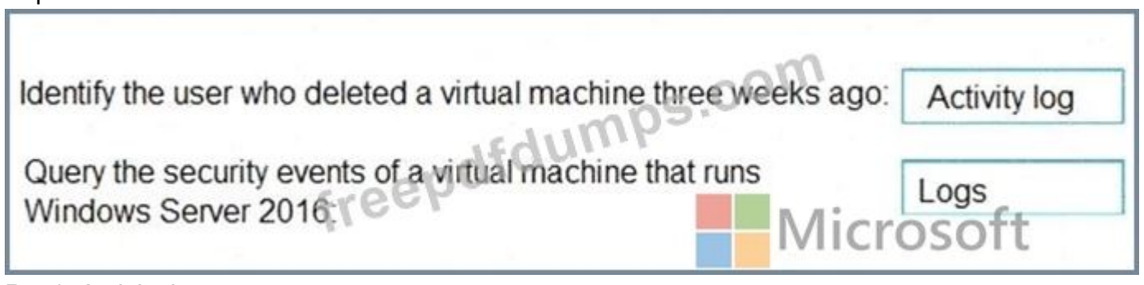
NEW QUESTION: 144
You have an Azure subscription that contains 100 virtual machines. Azure Diagnostics is enabled on all the virtual machines.
You are planning the monitoring of Azure services in the subscription.
You need to retrieve the following details:
* Identify the user who deleted a virtual machine three weeks ago.
* Query the security events of a virtual machine that runs Windows Server 2016.
What should you use in Azure Monitor? To answer, drag the appropriate configuration settings to the correct details. Each configuration setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Answer:



Explanation:



Box1: Activity log

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

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

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

Box 2: Logs

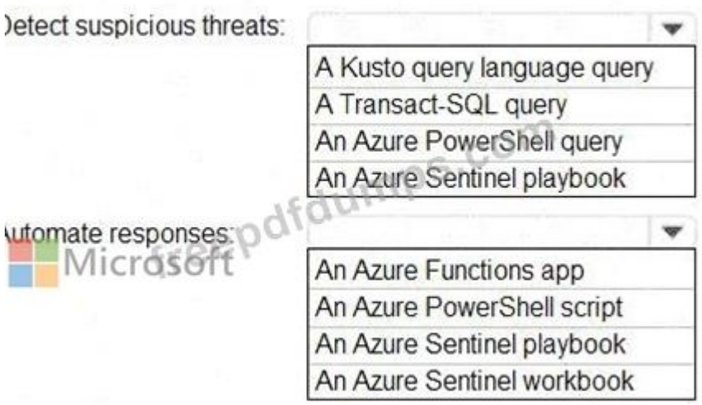
Log Integration collects Azure diagnostics from your Windows virtual machines, Azure activity logs, Azure Security Center alerts, and Azure resource provider logs. This integration provides a unified dashboard for all your assets, whether they're on-premises or in the cloud, so that you can aggregate,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

References:

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

NEW QUESTION: 145
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a hybrid configuration of Azure Active Directory (AzureAD).
You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.
You need to configure the environment to support the planned authentication.
Solution: You create a site-to-site VPN between the virtual network and the on-premises network.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)
You can connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:
Create Azure Virtual Network.
Create a custom DNS server in the Azure Virtual Network.
Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
Configure forwarding between the custom DNS server and your on-premises DNS server.
References:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

NEW QUESTION: 146
You plan to use Azure Sentinel to create an analytic rule that will detect suspicious threats and automate responses.
Which components are required for the rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

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: 147
You have an Azure subscription that contains the resources shown in the following table.

Name	Type
VM1	Virtual machine
VNet1	Virtual network
AFW1	Azure firewall

You need to configure AFW1 to only allow traffic from VM1 to storage accounts in the West US Azure region. The solution must minimize administrative effort.
What should you configure?
A. a DNAT rule
B. an SNAT private IP address range
C. a network rule
D. an application rule
Answer: C (LEAVE A REPLY)

NEW QUESTION: 148

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD). Azure AD Connect is installed on a domain member server named Server1.
You need to ensure that a domain administrator for the adatum.com domain can modify the synchronization options. The solution must use the principle of least privilege.
Which Azure AD role should you assign to the domain administrator?
A. Security administrator
B. Global administrator
C. User administrator
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

NEW QUESTION: 149
Lab Task
Task 1
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:
Explanation:
You need to configure the Network Security Group that is associated with subnet0.
1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET1. Alternatively, browse to Virtual Networks in the left navigation pane.
2. In the properties of VNET1, click on Subnets. This will display the subnets in VNET1 and the Network Security Group associated to each subnet. Note the name of the Network Security Group associated to Subnet0.
3. Type Network Security Groups into the search box and select the Network Security Group associated with Subnet0.
4. In the properties of the Network Security Group, click on Inbound Security Rules.
5. Click the Add button to add a new rule.
6. In the Source field, select Service Tag.
7. In the Source Service Tag field, select Internet.
8. Leave the Source port ranges and Destination field as the default values (* and All).
9. In the Destination port ranges field, enter 7777.
10.Change the Protocol to TCP.
11.Leave the Action option as Allow.
12.Change the Priority to 100.
13.Change the Name from the default Port_8080 to something more descriptive such as Allow_TCP_7777_from_Internet. The name cannot contain spaces.
14.Click the Add button to save the new rule.

NEW QUESTION: 150
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.

Answer:

Explanation:

Reference:

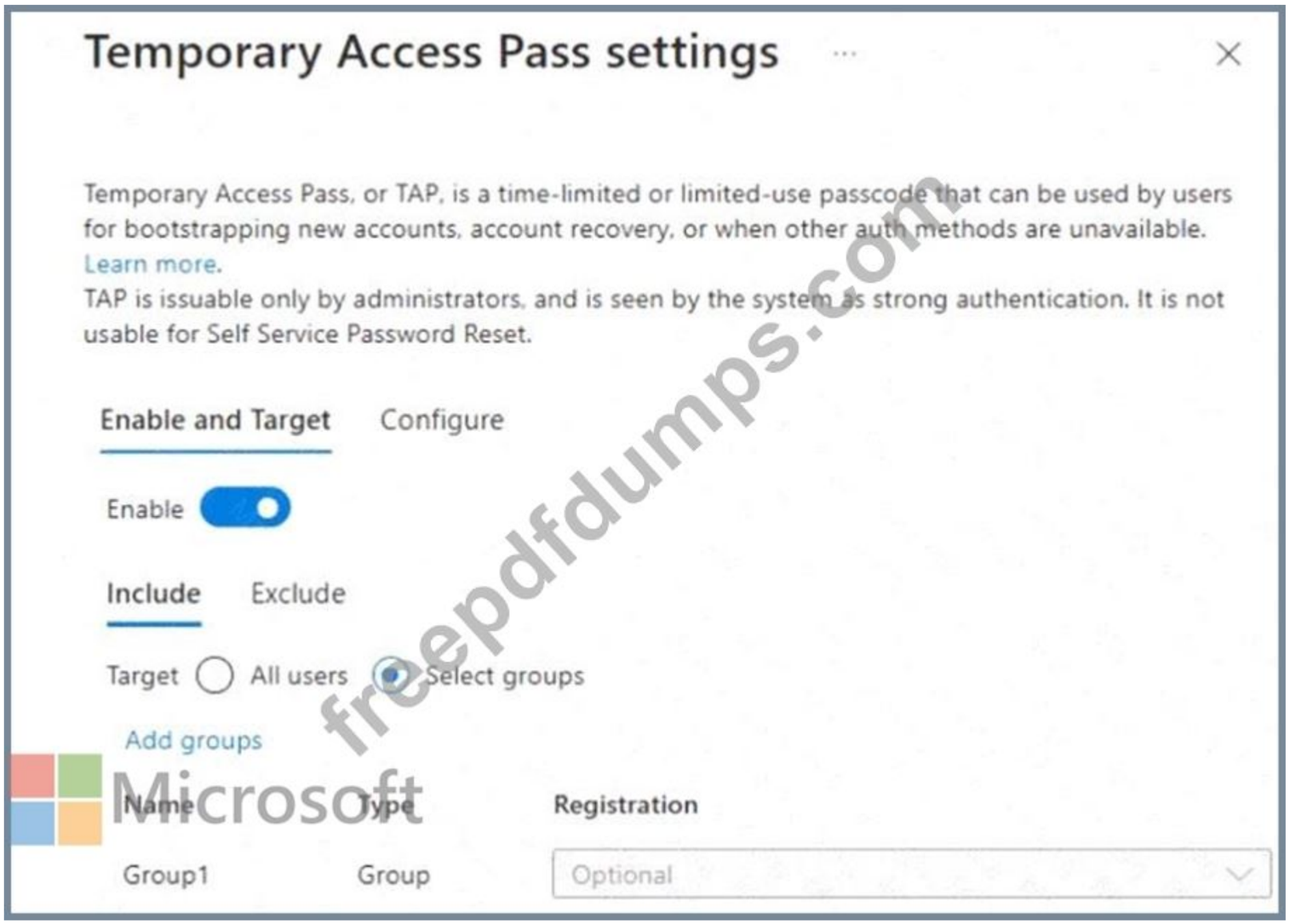
https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

NEW QUESTION: 151
You have an Azure SQL Database server named SQL1.
You plan to turn on Advanced Threat Protection for SQL1 to detect all threat detection types.
Which action will Advanced Threat Protection detect as a threat?
A. A user updates more than 50 percent of the records in a table.
B. A user attempts to sign as select * from table1.
C. A user is added to the db_owner database role.
D. A user deletes more than 100 records from the same table.
Answer: B (LEAVE A REPLY)
Advanced Threat Protection can detect potential SQL injections: This alert is triggered when an active exploit happens against an identified application vulnerability to SQL injection. This means the attacker is trying to inject malicious SQL statements using the vulnerable application code or stored procedures.
References:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview

NEW QUESTION: 152
You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Member of	Role
Admin1	Group1	Global Administrator
Admin2	Group1	Privileged Authentication Administrator
User1	*None*	*None*

You configure the Temporary Access Pass settings as shown in the following exhibit.



You add the Temporary Access Pass authentication method to Admin2.

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:

Explanation:

NEW QUESTION: 153

You have been tasked with applying conditional access policies for your company's current Azure Active Directory (Azure AD).

The process involves assessing the risk events and risk levels.

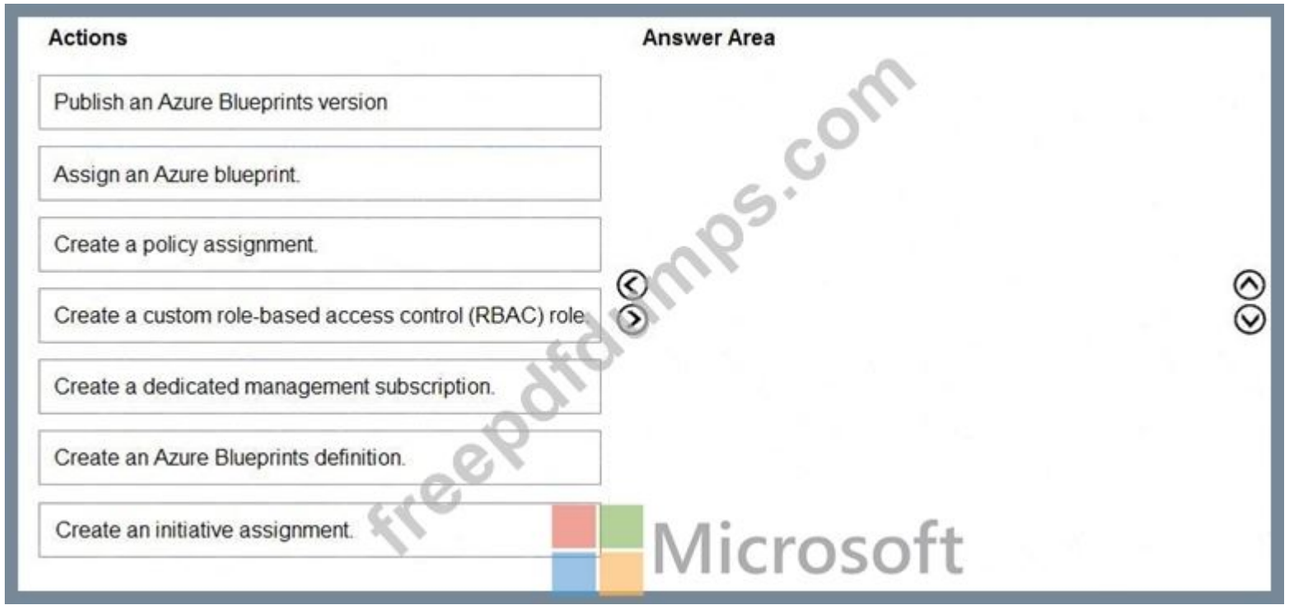
Which of the following is the risk level that should be configured for users that have leaked credentials?

A. None
B. Low
C. Medium
D. High
Answer: D (LEAVE A REPLY)
These six types of events are categorized in to 3 levels of risks - High, Medium & Low:
Table Description automatically generated

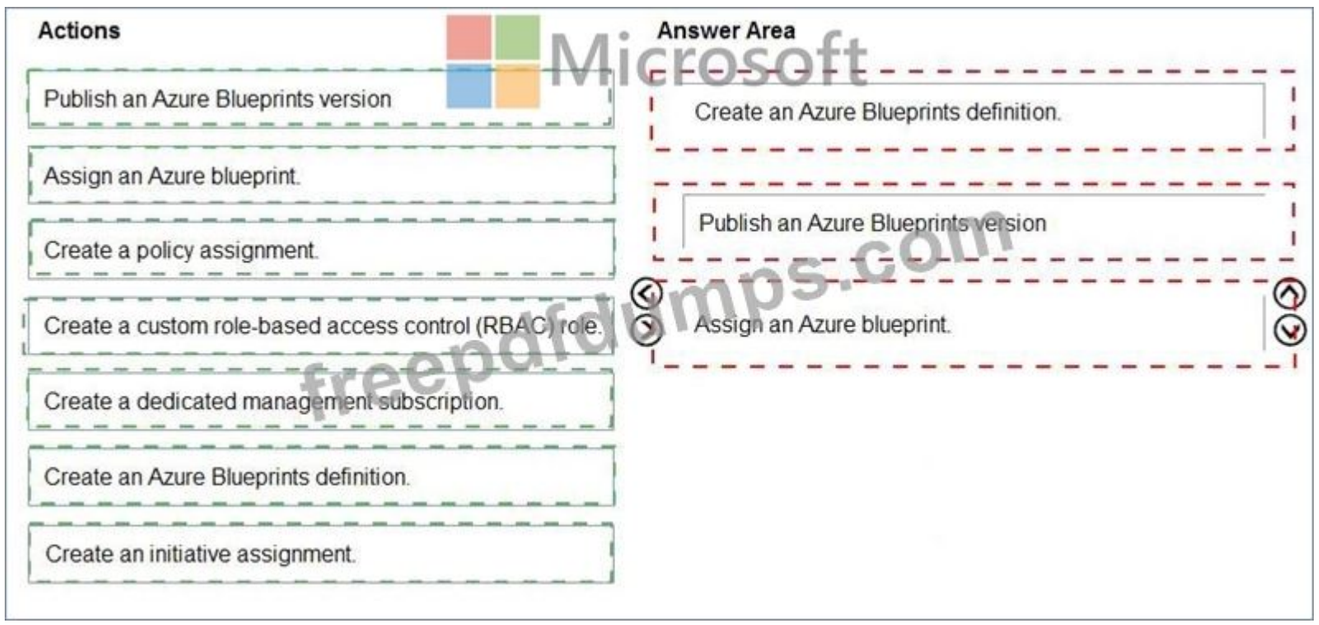
Sign-in Activity	Risk Level
Users with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from IP addresses with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium

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

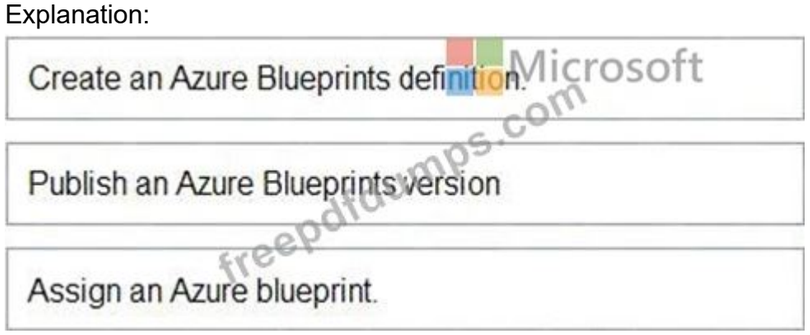
NEW QUESTION: 154
You have five Azure subscriptions linked to a single Azure Active Directory (Azure AD) tenant.
You create an Azure Policy initiative named SecurityPolicyInitiative1.
You identify which standard role assignments must be configured on all new resource groups.
You need to enforce SecurityPolicyInitiative1 and the role assignments when a new resource group is created.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



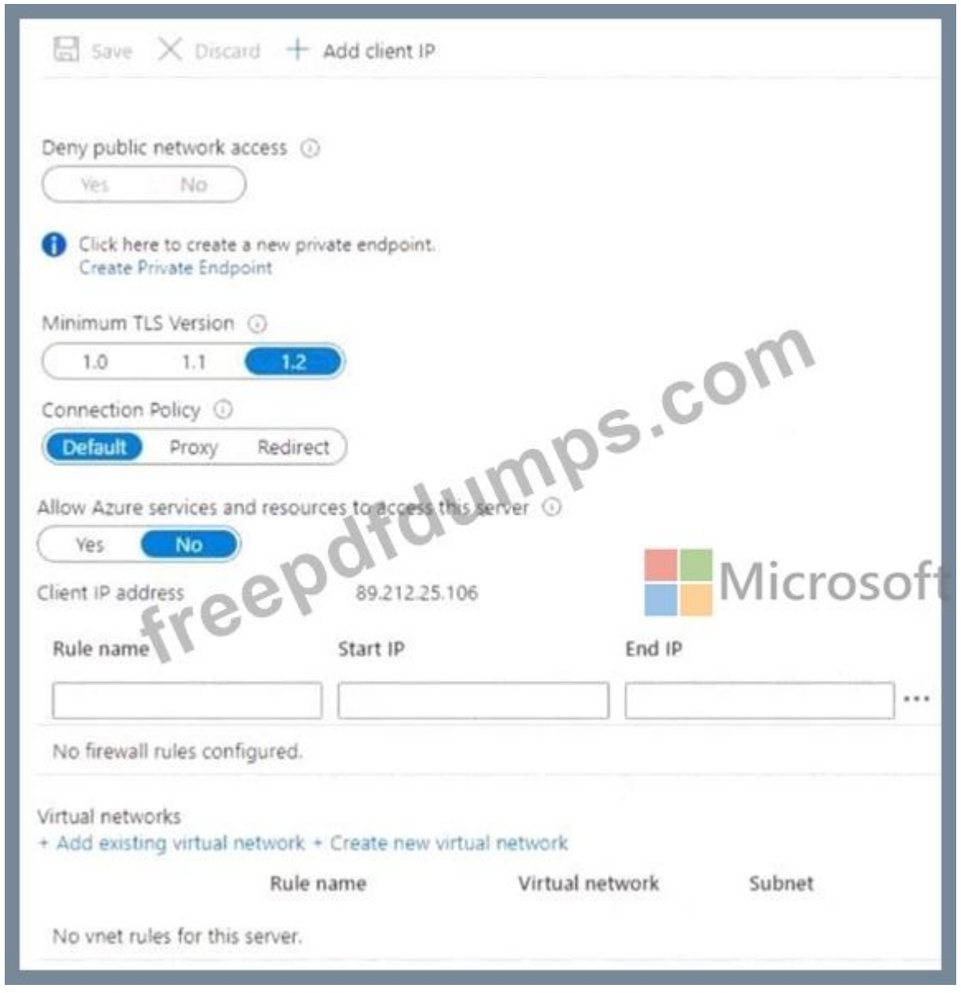
Explanation:



Reference:

https://docs.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-portal
https://docs.microsoft.com/en-us/azure/azure-australia/azure-policy

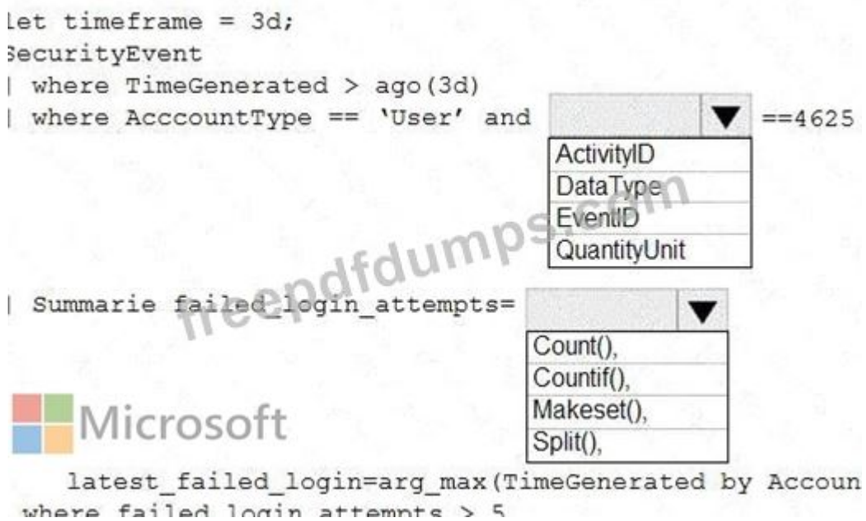
NEW QUESTION: 155
You have an Azure subscription that contains an Azure SQL Database logic server named SQL! and an Azure virtual machine named VM1. VM1 uses a private IP address only.
The Firewall and virtual networks settings for SQL1 are shown in the following exhibit.



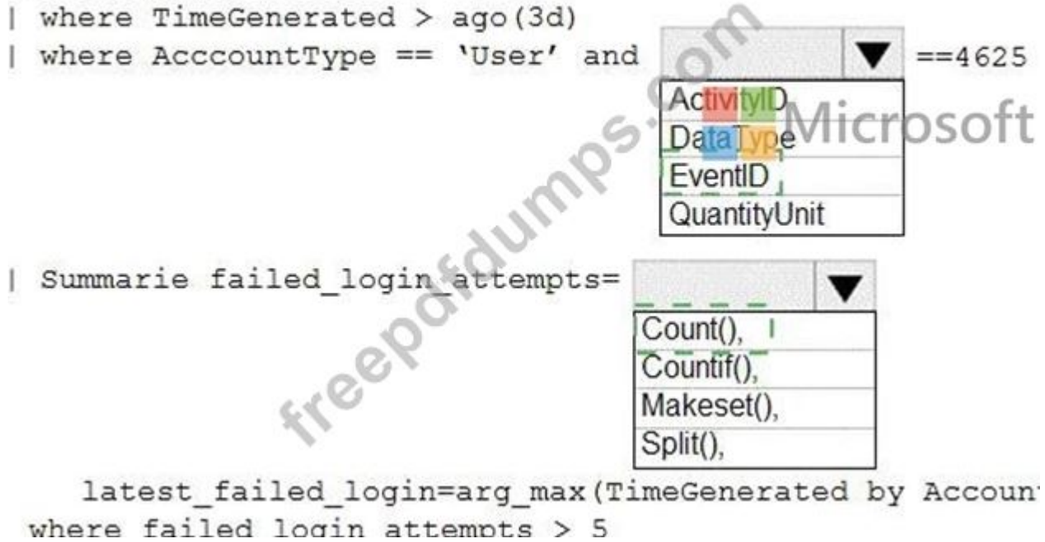
You need to ensure that VM1 can connect to SQL1. The solution must use the principle of least privilege.
What should you do?
A. Set Allow Azure services and resources to access this server to Yes.
B. Set Connection Policy to Proxy.
C. Create a new firewall rule.
D. Add an existing virtual network.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 156
You suspect that users are attempting to sign in to resources to which they have no access.

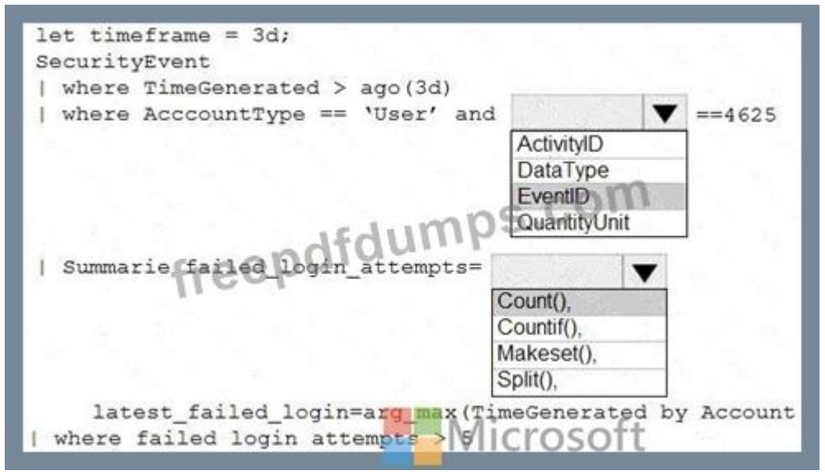
You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than five failed sign-in attempts.
How should you configure the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



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: 157

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)

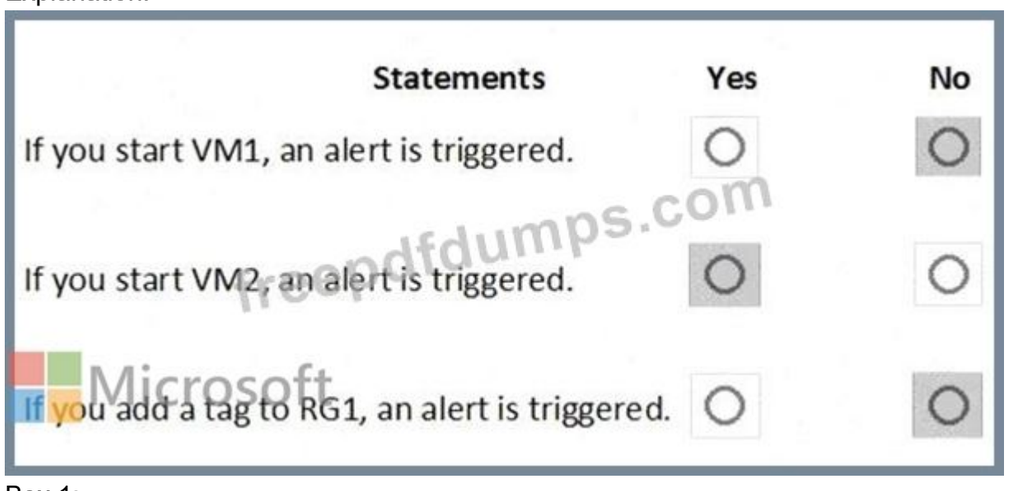
* Name: ActionRule1

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

Note: Each correct selection is worth one point.

Answer:

Explanation:



Box 1:

The scope for the action rule is set to VM1 and is set to suppress alerts indefinitely.

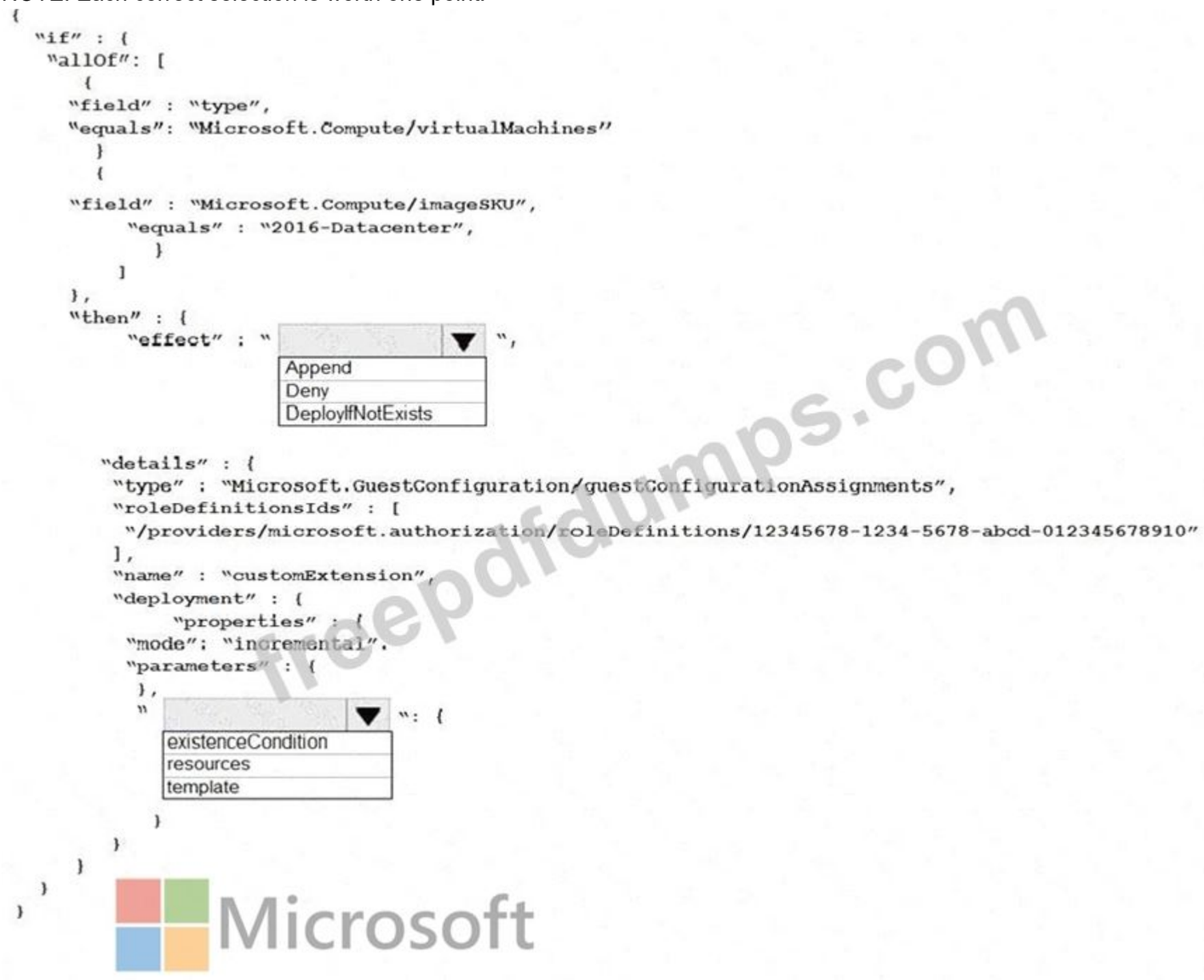
Box 2:

The scope for the action rule is not set to VM2.

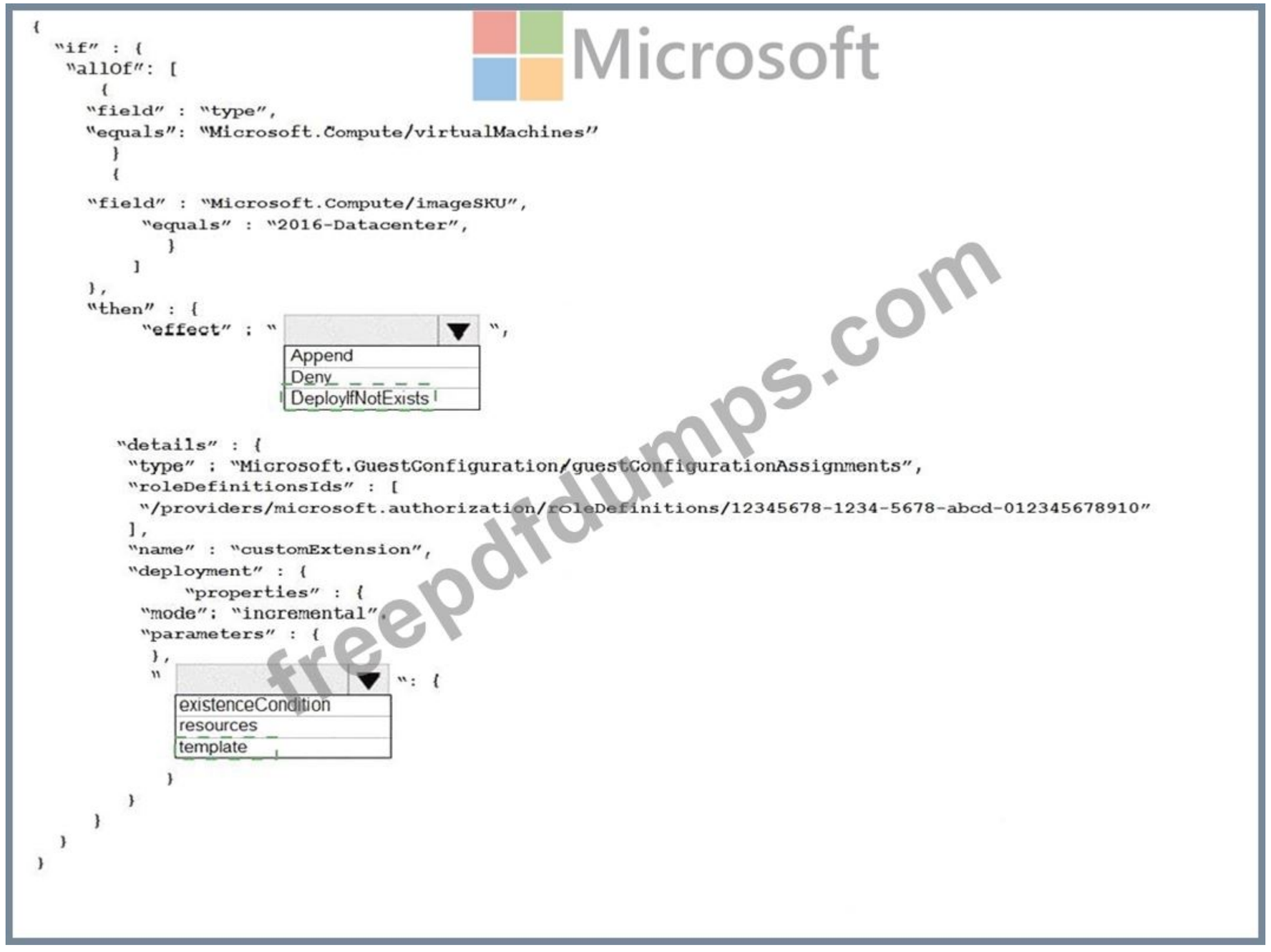
Box 3:

Adding a tag is not an administrative operation.
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-action-rules

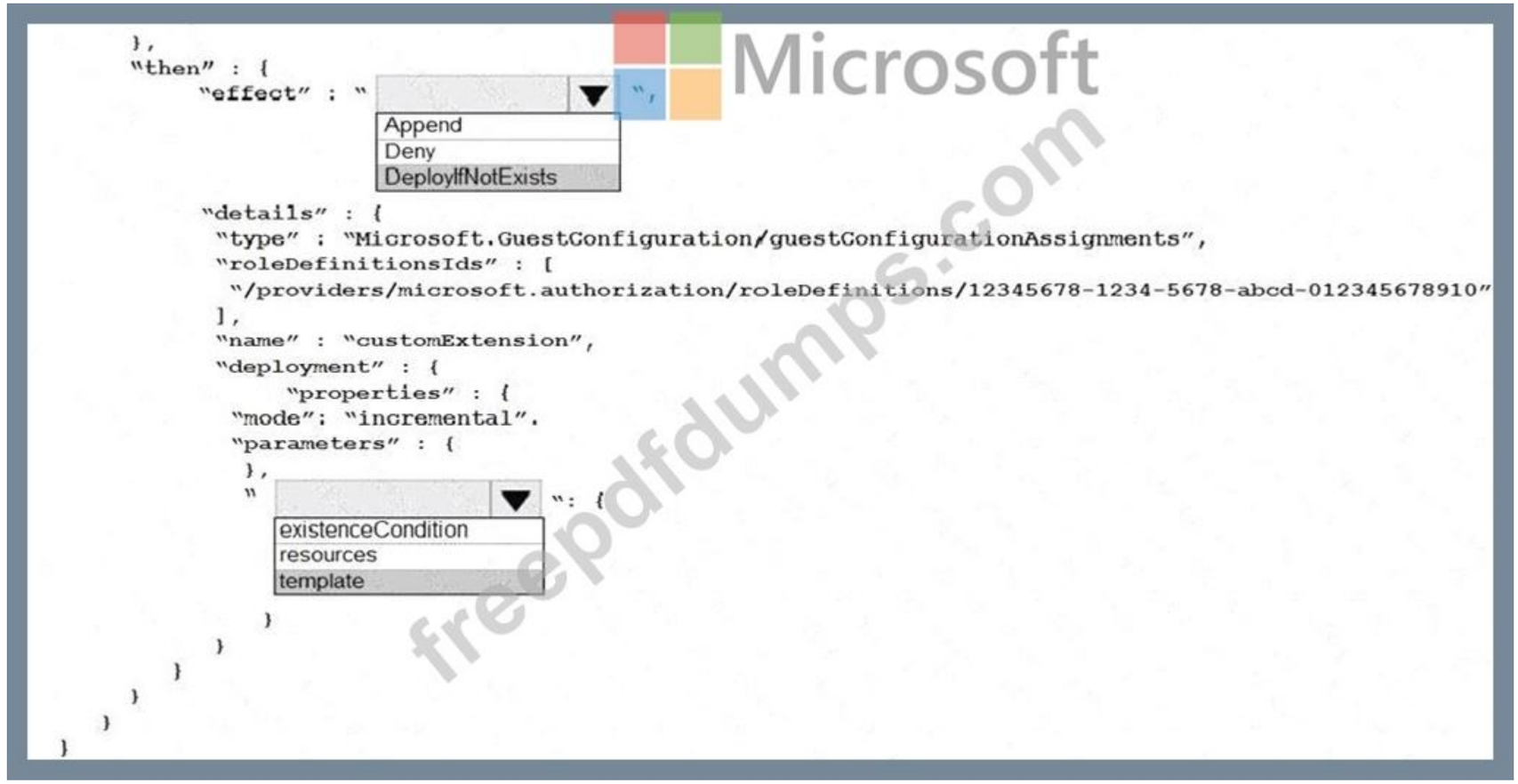
NEW QUESTION: 158
You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.
You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.
How should you complete the policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



Box 1: DeployIfNotExists
DeployIfNotExists executes a template deployment when the condition is met.
Box 2: Template
The details property of the DeployIfNotExists effects has all the subproperties that define the related resources to match and the template deployment to execute.
Deployment [required]
This property should include the full template deployment as it would be passed to the Microsoft.Resources
/deployment
References:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

NEW QUESTION: 159
You have a Microsoft Entra tenant that contains a user named User1.
You have an app registration named App1.
For App1, you create an app role named Role1.
You need to assign User1 to Role1.
What should you use in the Azure portal?
A. Roles and administrators from the Microsoft Entra admin center
B. API permissions for App1 from App registrations
C. Users and groups for App1 from Enterprise applications

D. App roles for App1 from App registrations
E. Roles and administrators for App1 from Enterprise applications
Answer: C (LEAVE A REPLY)

NEW QUESTION: 160
You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Location	Peered with
VNet1	East US	VNet2
VNet2	West US	VNet1

The virtual networks contain the subnets shown in the following table.

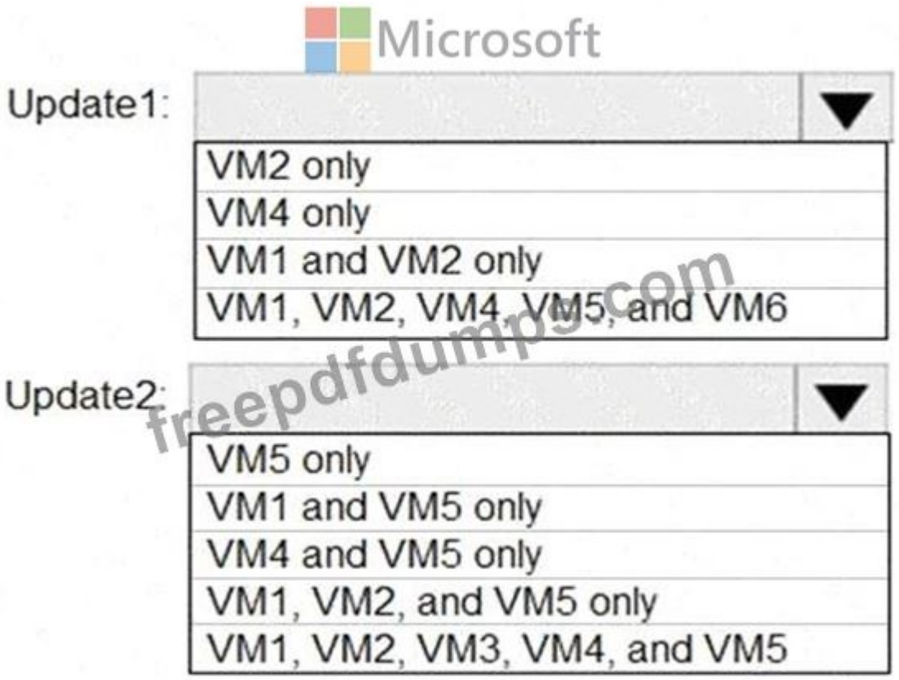
Answer:

Explanation:

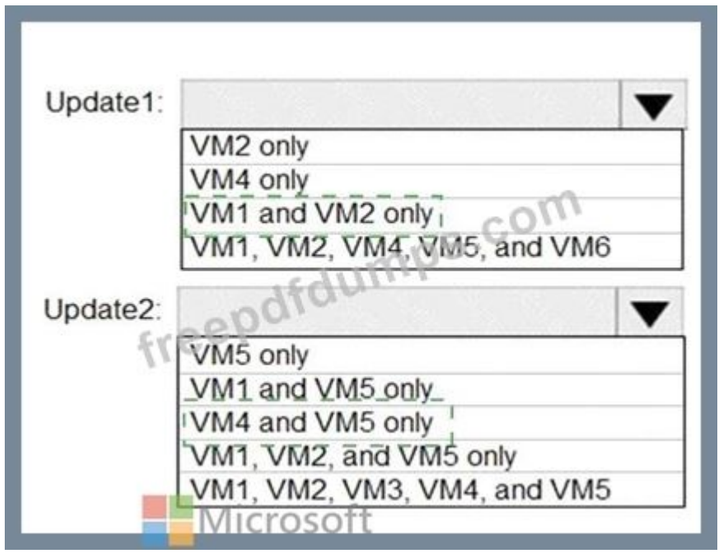
NEW QUESTION: 161
You have Azure virtual machines that have Update Management enabled. The virtual machines are configured as shown in the following table.

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

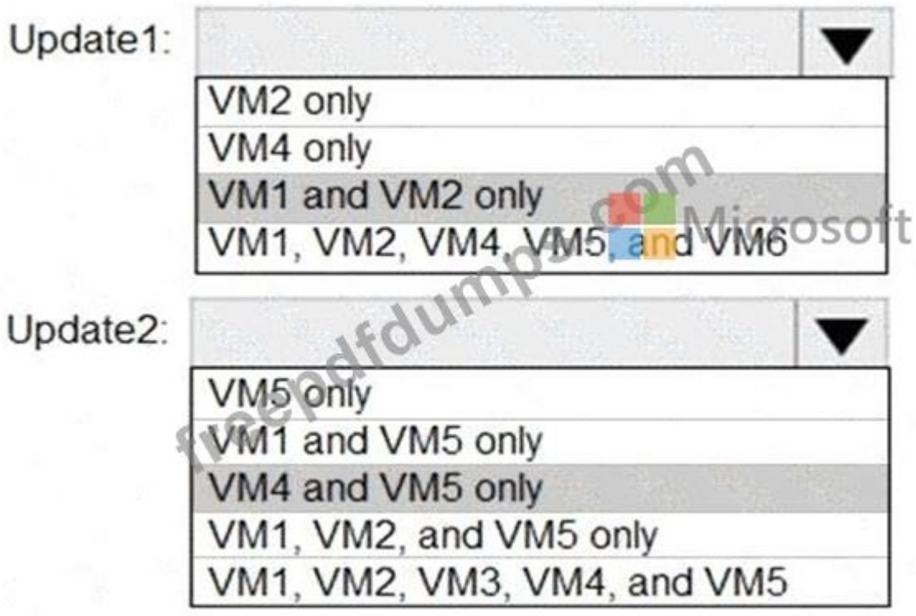
You schedule two update deployments named Update1 and Update2. Update1 updates VM3. Update2 updates VM6.
Which additional virtual machines can be updated by using Update1 and Update2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



Update1: VM1 and VM2 only
VM3: Windows Server 2016 West US RG2
Update2: VM4 and VM5 only
VM6: CentOS 7.5 East US RG1
For Linux, the machine must have access to an update repository. The update repository can be private or public.
References:
https://docs.microsoft.com/en-us/azure/automation/automation-update-management

NEW QUESTION: 162
You need to configure WebApp1 to meet the data and application requirements.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. Upload a public certificate.
B. Turn on the HTTPS Only protocol setting.
C. Set the Minimum TLS Version protocol setting to 1.2.
D. Change the pricing tier of the App Service plan.
E. Turn on the Incoming client certificates protocol setting.
Answer: (SHOW ANSWER)
Refer https://docs.microsoft.com/en-us/azure/app-service/app-service-web-configure-tls-mutual-auth
Topic 1, Litware, inc
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

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

To start the case study

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

Overview

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

Existing Environment

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

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

The tenant contains the groups shown in the following table.

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

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

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subent0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://litwareinc.com and http://www.litwareinc.com.
Resource Group1	Resource group	Resource Group1 is a resource group that contains VNet1, VM0, and VM1.
Resource Group2	Resource group	Resource Group2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Free tier.

Planned changes

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

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

Litware identifies the following identity and access requirements:

* All San Francisco users and their devices must be members of Group1.
* The members of Group2 must be assigned the Contributor role to Resource Group2 by using a permanent eligible assignment.
* Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

Platform Protection Requirements

Litware identifies the following platform protection requirements:

* Microsoft Antimalware must be installed on the virtual machines in Resource Group1.
* The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
* Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.
* Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.
* A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

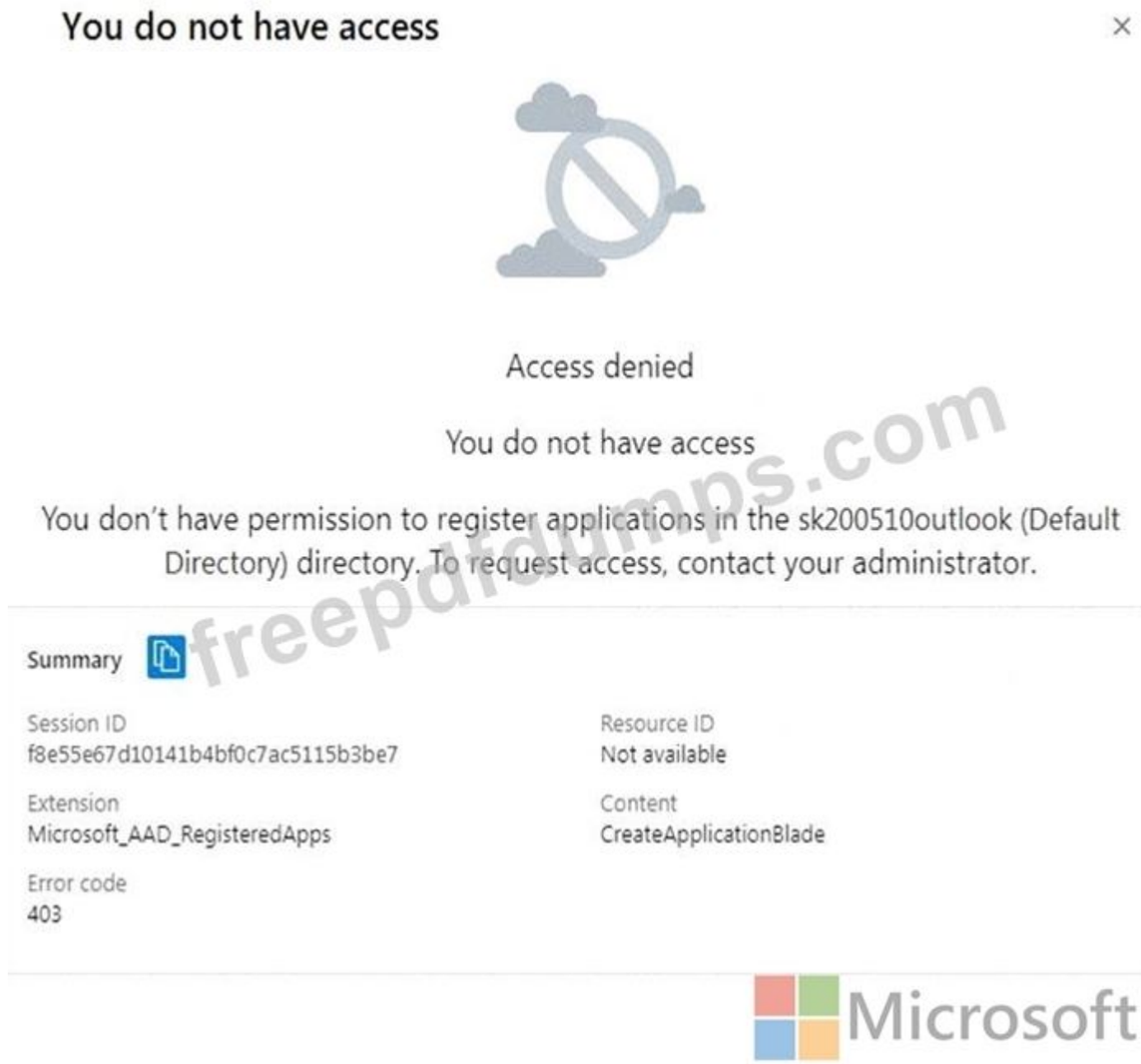
Security Operations Requirements

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

NEW QUESTION: 163

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant.

When a developer attempts to register an app named App1 in the tenant, the developer receives the error message shown in the following exhibit.

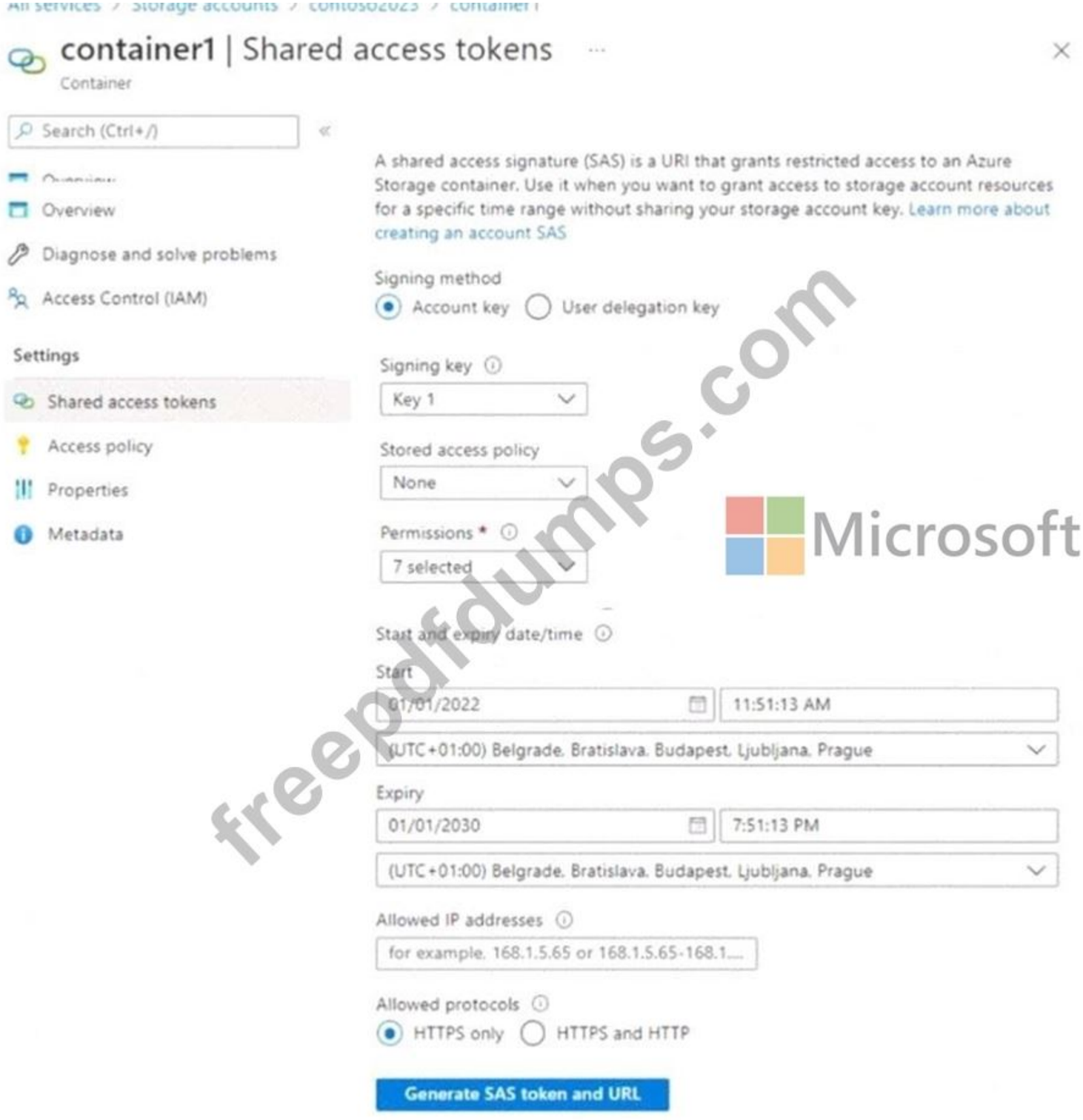


You need to ensure that the developer can register App1 in the tenant.
What should you do for the tenant?
A. Modify the User settings
B. Set Enable Security default to Yes.
C. Modify the Directory properties.
D. Configure the Consent and permissions settings for enterprise applications.
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

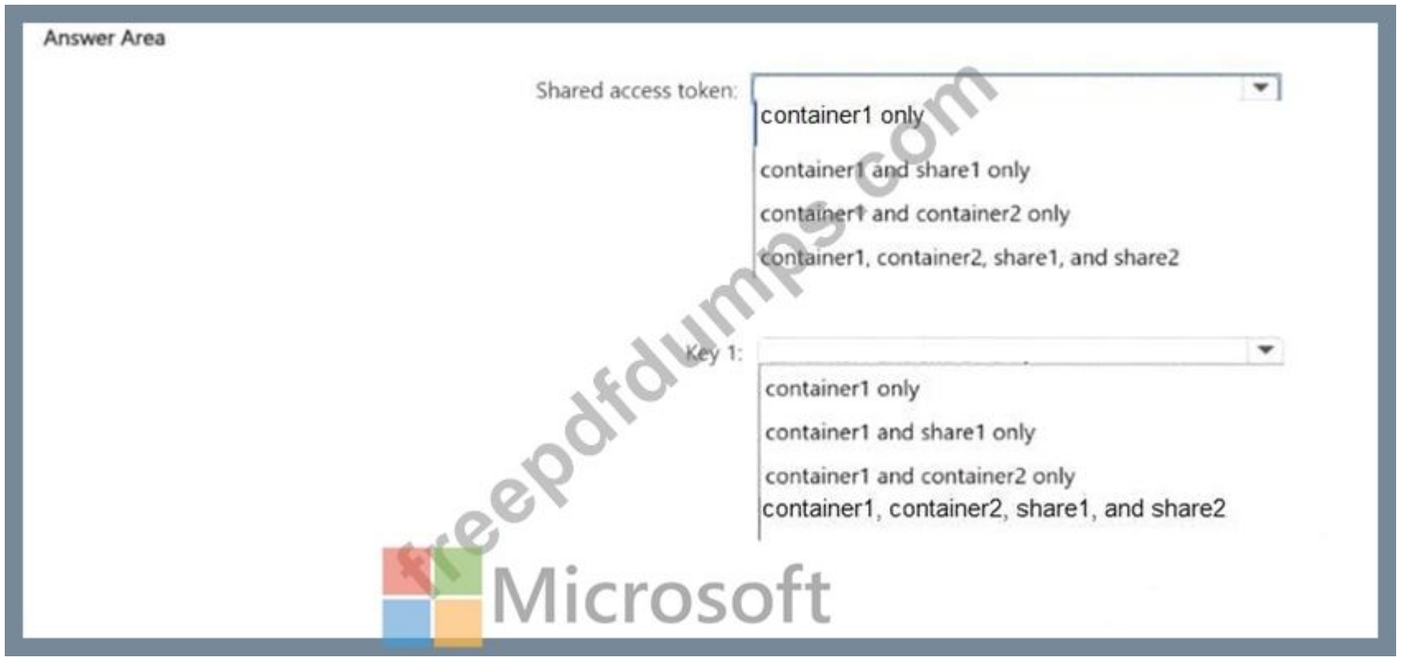
NEW QUESTION: 164
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
container1	Blob container	In a storage account named contoso2023
container2	Blob container	In a storage account named contoso2024
share1	File share	In a storage account named contoso2023
share2	File share	In a storage account named contoso2024

You create a shared access token as shown in the following exhibit.



Which resources can you access by using the shared access token and Key 1? To answer, select the appropriate options in the answer area.
NOTE: Each correct answer is worth one point.



Answer:

Explanation:

NEW QUESTION: 165

You have an Azure virtual machine named VM1.

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

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

What should you do?

A. Add the Microsoft Antimalware extension to VM1.

B. Install Microsoft System Center Security Management Pack for Endpoint Protection on VM1.

C. Add the Network Watcher Agent for Windows extension to VM1.

D. Onboard VM1 to Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 166

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

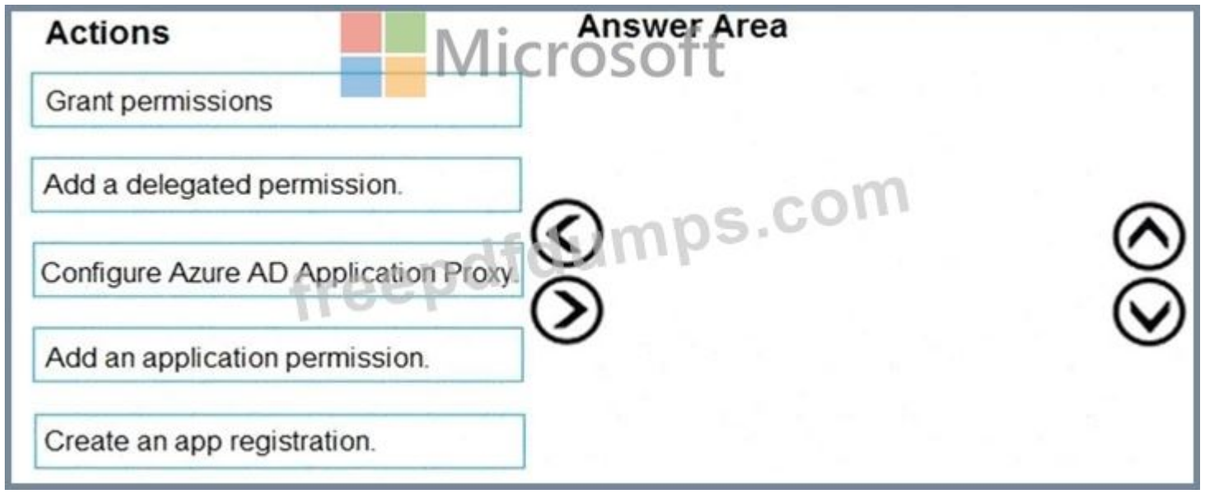
NEW QUESTION: 167

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

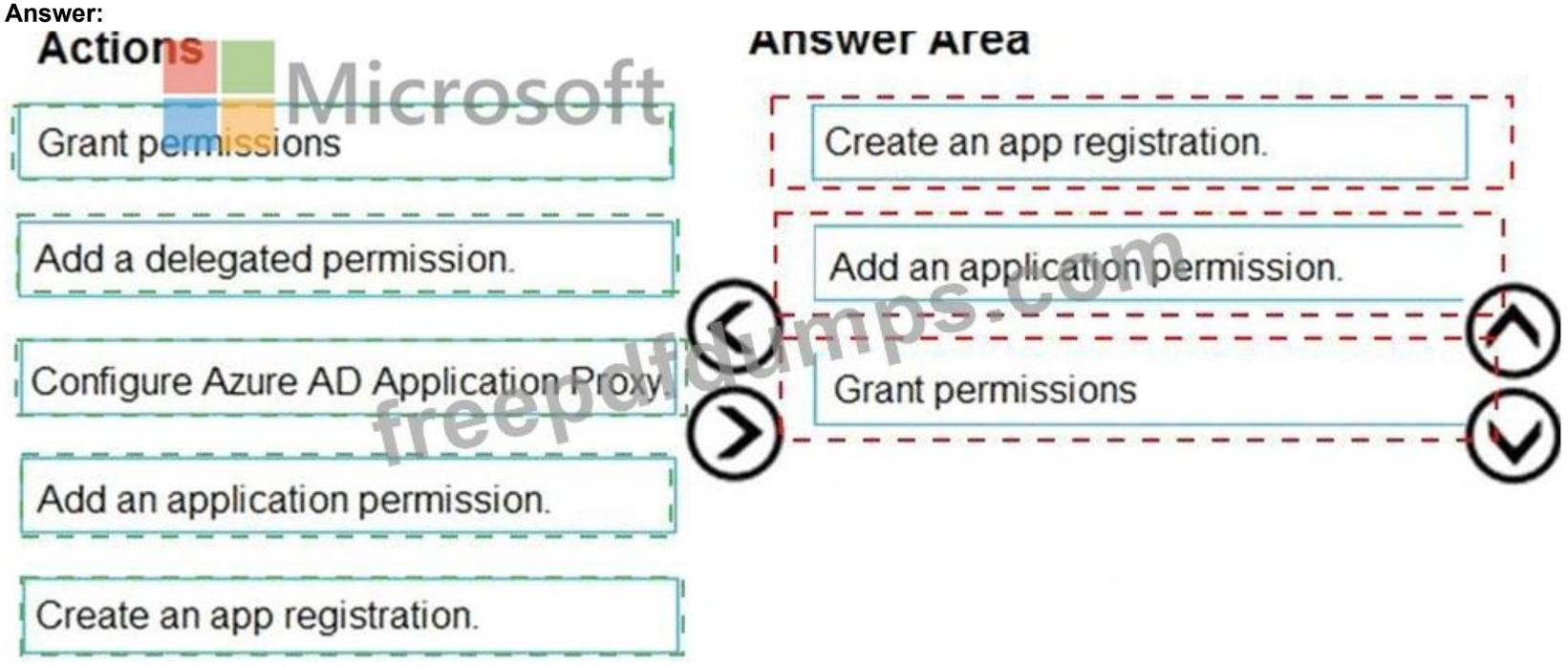
The company is developing an application named App1. App1 will run as a service on server that runs Windows Server 2016. App1 will authenticate to contoso.com and access Microsoft Graph to read directory data.

You need to delegate the minimum required permissions to App1.

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



Answer:



Explanation:

Step 1: Create an app registration

First the application must be created/registered.

Step 2: Add an application permission

Application permissions are used by apps that run without a signed-in user present.
Step 3: Grant permissions
References:
https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-permissions-and-consent

NEW QUESTION: 168
You have an Azure Sentinel deployment.
You need to create a scheduled query rule named Rule1.
What should you use to define the query rule logic for Rule1?
A. a Transact-SQL statement
B. a JSON definition
C. GraphQL
D. a Kusto query
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

NEW QUESTION: 169
You have an Azure subscription that is linked to a Microsoft Entra tenant named contoso.com. You register an application named App1 in contoso.com You need to add a platform configuration for Android applications to the App1 registration. What should you configure in the Azure portal?
A. Branding & properties
B. Token configuration
C. Manifest
D. Authentication
Answer: D (LEAVE A REPLY)

NEW QUESTION: 170
You have an Azure subscription that contains 100 virtual machines and has Azure Security Cent,-. Standard tier enabled.
You plan to perform a vulnerability scan of each virtual machine.
You need to deploy the vulnerability scanner extension to the virtual machines by using an Azure Resource Manager template.
Which two values should you specify in the code to automate the deployment of the extension to the virtual machines? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. the user assigned managed identity
B. the Key Vault managed storage account Key
C. the Azure Active Directory (Azure AD) ID
D. the system-assigned managed identity
E. the primary shared key
F. the workspace ID
Answer: A,C (LEAVE A REPLY)
https://docs.microsoft.com/en-us/azure/azure-arc/servers/onboard-service-principal

NEW QUESTION: 171
You have an Azure subscription that contains the Azure App Service apps shown in the following table.

Name	App Service plan
App1	Free
App2	Shared
App3	Basic
App4	Standard

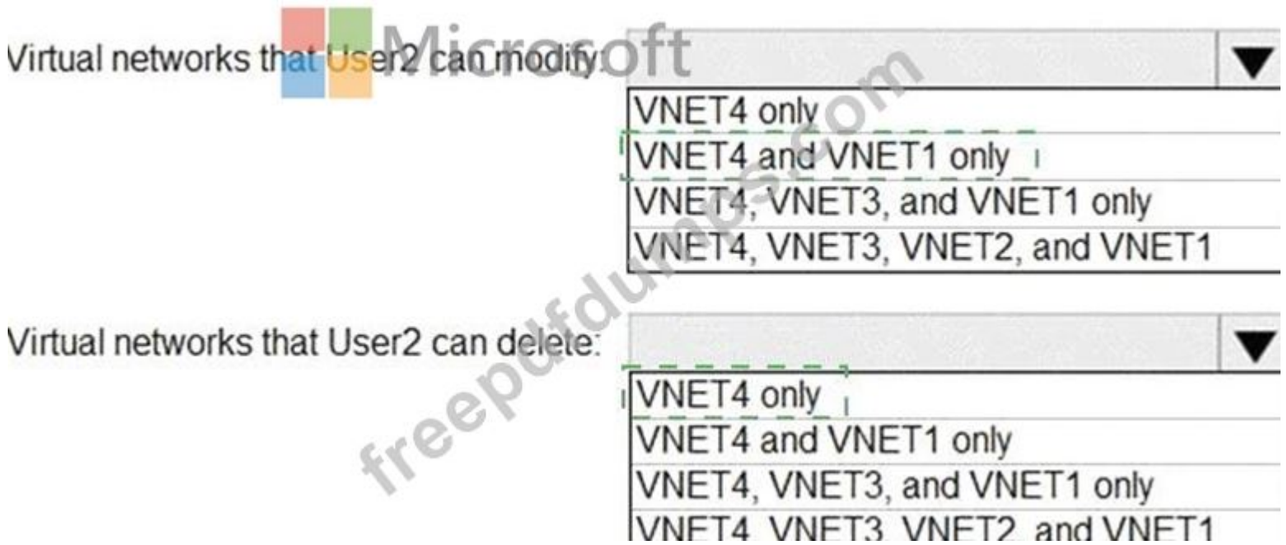
You purchase custom SSL certificates from a trusted third-party authority.
To which apps can you assign the custom SSL certificates?
A. App2. App3. and App4 only
B. App1. App2, App3. and App4
C. App4 only
D. App3 and App4 only
Answer: (SHOW ANSWER)

NEW QUESTION: 172
Which virtual networks in Sub1 can User2 modify and delete in their current state? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

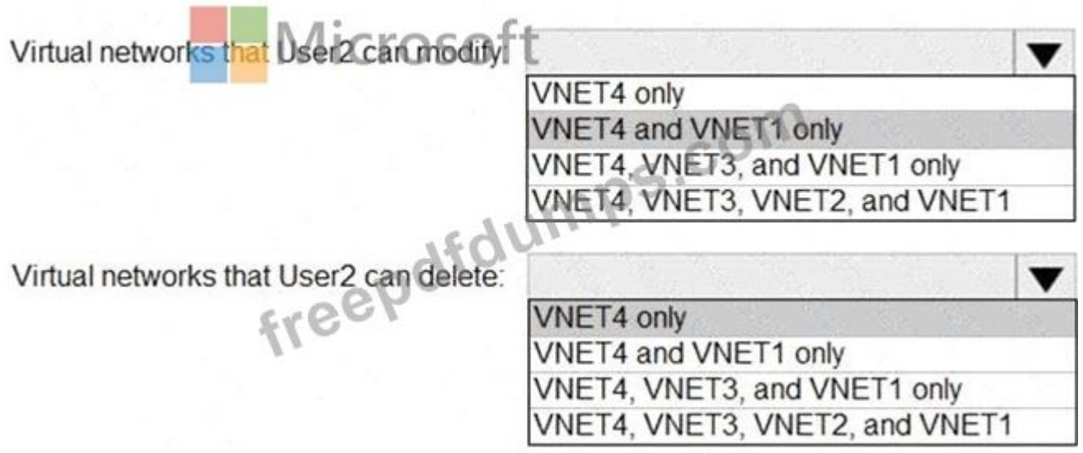
Virtual networks that User2 can modify:
- VNET4 only
- VNET4 and VNET1 only
- VNET4, VNET3, and VNET1 only
- VNET4, VNET3, VNET2, and VNET1

Virtual networks that User2 can delete:
- VNET4 only
- VNET4 and VNET1 only
- VNET4, VNET3, and VNET1 only
- VNET4, VNET3, VNET2, and VNET1

Answer:



Explanation:



Box 1: VNET4 and VNET1 only

RG1 has only Delete lock, while there are no locks on RG4.

RG2 and RG3 both have Read-only locks.

Box 2: VNET4 only

There are no locks on RG4, while the other resource groups have either Delete or Read-only locks.

Note: As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.

* CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource.
* ReadOnly means authorized users can read a resource, but they can't delete or update the resource.

Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Scenario:

User2 is a Security administrator.

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

User2 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

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

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

NEW QUESTION: 173
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
An administrator named Admin1 has access to the following identities:
* An OpenID-enabled user account
* A Hotmail account
* An account in contoso.com
* An account in an Azure AD tenant named fabrikam.com
You plan to use Azure Account Center to transfer the ownership of Sub1 to Admin1.
To which accounts can you transfer the ownership of Sub1?
A. contoso.com only
B. contoso.com, fabrikam.com, and Hotmail only
C. contoso.com and fabrikam.com only
D. contoso.com, fabrikam.com, Hotmail, and OpenID-enabled user account
Answer: C (LEAVE A REPLY)
When you transfer billing ownership of your subscription to an account in another Azure AD tenant, you can move the subscription to the new account's tenant. If you do so, all users, groups, or service principals who had role based access (RBAC) to manage subscriptions and its resources lose their access. Only the user in the new account who accepts your transfer request will have access to manage the resources.
Reference:
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transferring-subscription-to-anaccount-in-another-azure-ad-tenant

NEW QUESTION: 174

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

Name	Type	Resource group
RG1	Resource group	Not applicable
RG2	Resource group	Not applicable
RG3	Resource group	Not applicable
SQL1	Azure SQL Database	RG3

Transparent Data Encryption (TDE) is disabled on SQL1.

You assign policies to the resource groups as shown in the following table.

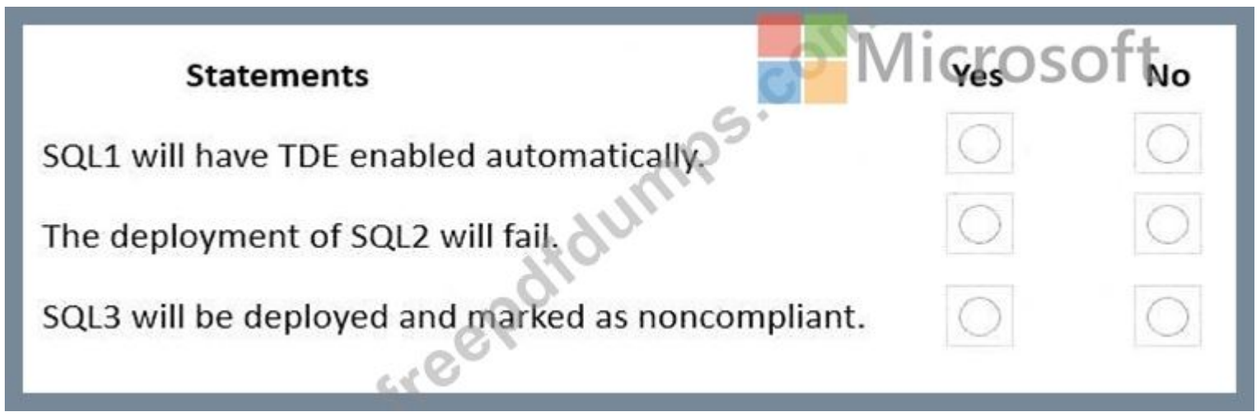
Name	Condition	Effect if condition is false	Assignment
Policy1	TDE enabled	Deny	RG1, RG2
Policy2	TDE enabled	DeployIfNotExists	RG2, RG3
Policy3	TDE enabled	Audit	RG1

You plan to deploy Azure SQL databases by using an Azure Resource Manager (ARM) template. The databases will be configured as shown in the following table.

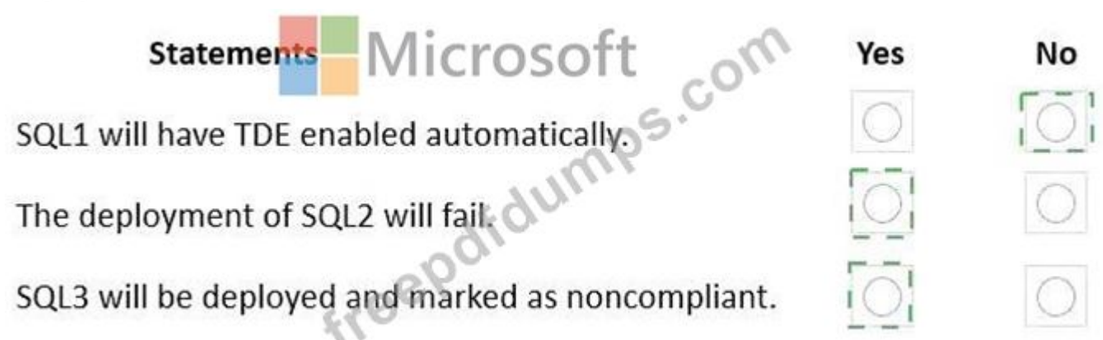
Name	Resource group	TDE
SQL2	RG2	Disabled
SQL3	RG1	Disabled

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

NOTE: Each correct selection is worth one point.

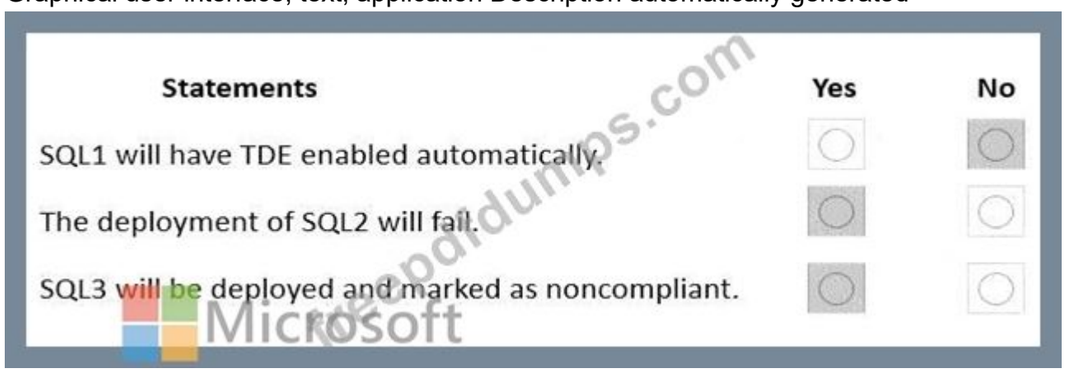


Answer:



Explanation:

Graphical user interface, text, application Description automatically generated



Reference:

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

NEW QUESTION: 175

Your company uses Azure DevOps.

You need to recommend a method to validate whether the code meets the company's quality standards and code review standards.

What should you recommend implementing in Azure DevOps?

A. branch folders

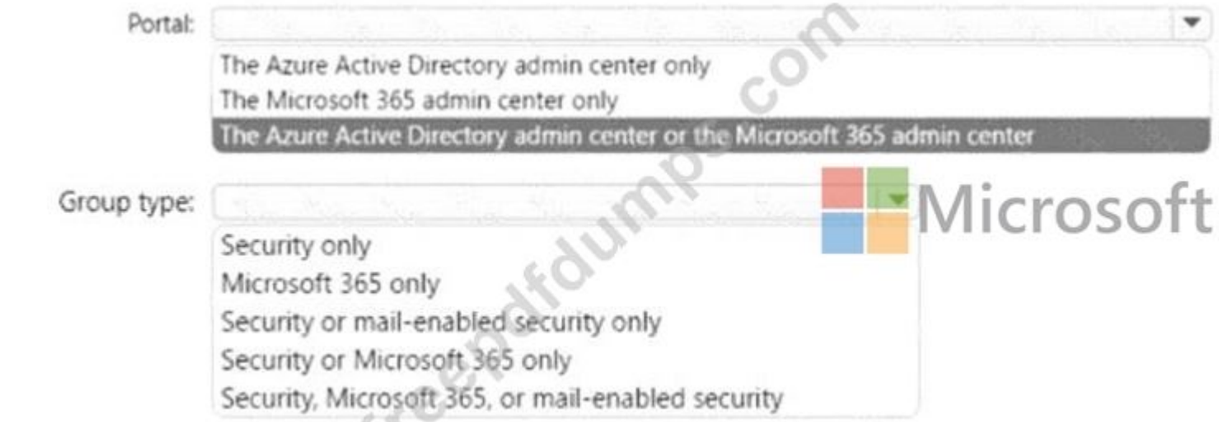
B. branch permissions

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

NEW QUESTION: 176
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.
You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.
Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.
Solution: You recommend the use of password hash synchronization and seamless SSO.
Does the solution meet the goal?
A. No
B. Yes
Answer: A (LEAVE A REPLY)

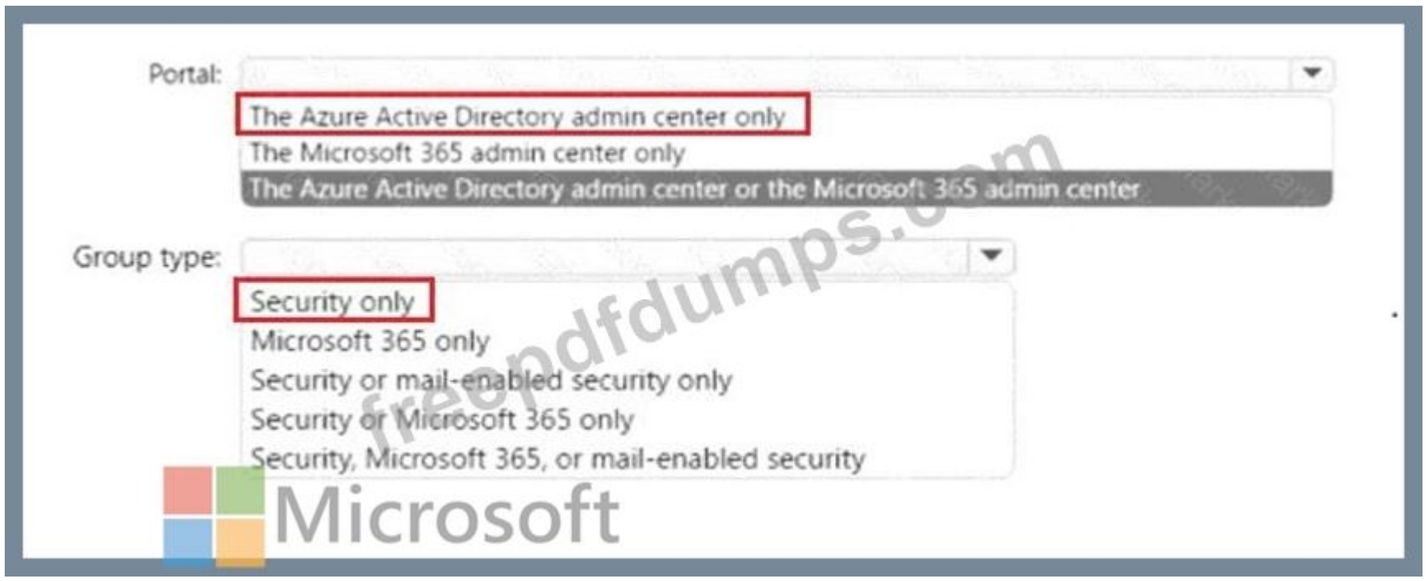
NEW QUESTION: 177
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center for the centralized policy management of three Azure subscriptions.
You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a resource graph and an assignment that is scoped to a management group.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/azure/governance/management-groups/create

NEW QUESTION: 178
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



Answer:

Explanation:



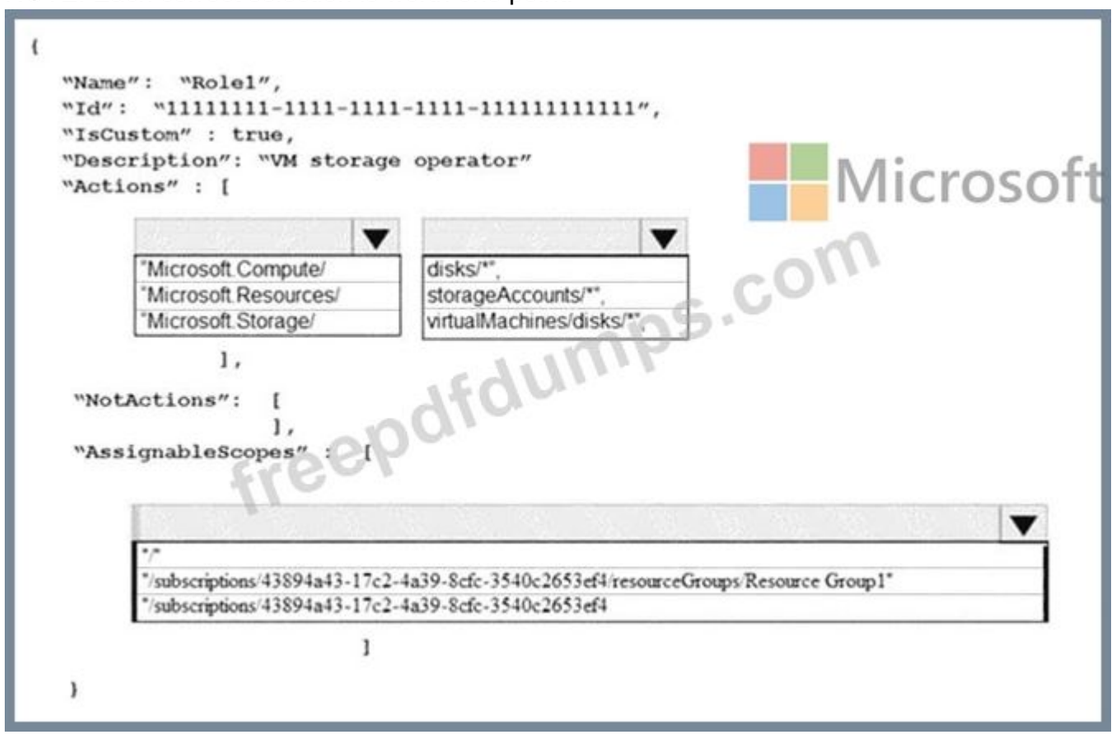
https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-create-eligible

NEW QUESTION: 179
You have an Azure subscription that contains several Azure SQL databases and an Azure Sentinel workspace.
You need to create a saved query in the workspace to find events reported by Advanced Threat Protection for Azure SQL Database.
What should you do?
A. From the Azure SQL Database query editor, create a Transact-SQL query.
B. From Azure CLI run the Get-AzOperationalInsightsworkspace cmdlet.
C. From Microsoft SQL Server Management Studio (SSMS), create a Transact-SQL query.
D. From the Azure Sentinel workspace, create a Kusto Query Language query.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 180
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: 181
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.



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

```
            ]
}
```


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

NEW QUESTION: 182
You have an Azure subscription that contains an Azure SQL database named sql1.
You plan to audit sql1.
You need to configure the audit log destination. The solution must meet the following requirements:
Support querying events by using the Kusto query language.
Minimize administrative effort.

What should you configure?
A. an event hub
B. a storage account
C. a Log Analytics workspace
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-log-analytics-wizard

NEW QUESTION: 183
You need to implement the function apps to meet the technical requirements.
Which apps should you include in the implementation?
A. Fa2 and Fa3 only
B. Fa1 and Fa2 only
C. Fa1 and Fa3 only
D. Fa1, Fa2, and Fa3
Answer: D (LEAVE A REPLY)

NEW QUESTION: 184
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.

Answer:

Explanation:

YES (Already active)

YES (The user will be prompted for MFA regardless the MFA Status of the user) NO (Even the user is included in the group, a user can ' t approve itself)

https://docs.microsoft.com/es-es/azure/active-directory/privileged-identity-management/pim-deployment-plan (Require approval section)

NEW QUESTION: 185

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

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

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

Which two services data encryption by using the keys stored in the key vault? Each correct answer present a complete solution.

NOTE: Each correct selection is worth one point.

A. Queue storage

B. Table storage

C. Azure Files

D. Blob storage

Answer: C,D (LEAVE A REPLY)

https://docs.microsoft.com/en-us/azure/storage/common/account-encryption-key-create?tabs=portal

NEW QUESTION: 186

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
You are assigned the Global administrator role for the tenant. You are responsible for managing Azure Security Center settings.
You need to create a custom sensitivity label.
What should you do first?
A. Create a custom sensitive information type.
B. Elevate access for global administrators in Azure AD.
C. Upgrade the pricing tier of the Security Center to Standard.
D. Enable integration with Microsoft Cloud App Security.
Answer: A (LEAVE A REPLY)
First, you need to create a new sensitive information type because you can't directly modify the default rules.
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-type

NEW QUESTION: 187
You have an Azure subscription that contains the resources shown in the following table.

Name	Type
storage1	Storage account
KeyVault1	Azure key vault

You need to configure storage1 to regenerate keys automatically every 90 days. Which cmdlet should you run?
A. set -A=StorageAccount
B. Add-A:StorogcAccountmanagementPolicyAction
C. Set-A;StorageAccountimanagementPolicy
D. Add-AsKeyVaultmanageStorageAccount
Answer: D (LEAVE A REPLY)

NEW QUESTION: 188
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 display name of each user
B. only the user principal name (UPN) and object identifier of each user
C. Only the user principal name (UPN) and display name of each user
D. only the user principal name (UPN) of each user
E. only the object identifier of each user
Answer: C (LEAVE A REPLY)

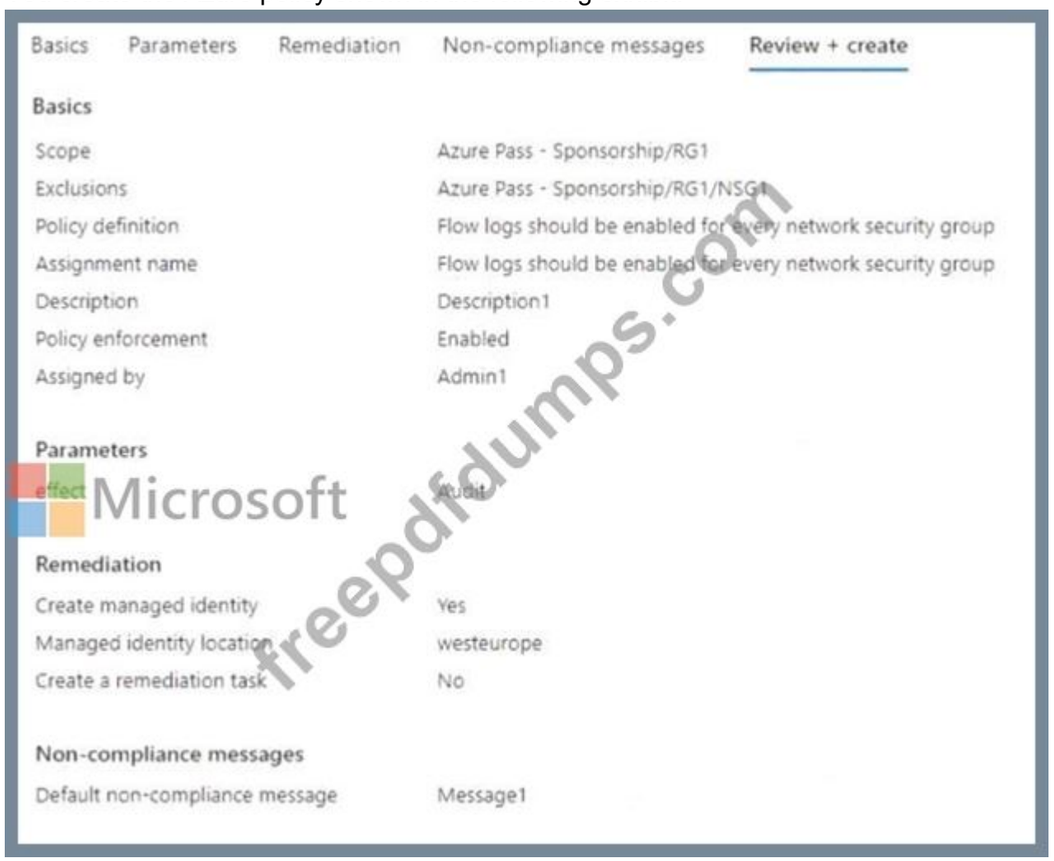
NEW QUESTION: 189
You company has an Azure subscription named Sub1. Sub1 contains an Azure web app named WebApp1 that uses Azure Application Insights. WebApp1 requires users to authenticate by using OAuth 2.0 client secrets.

Developers at the company plan to create a multi-step web test app that preforms synthetic transactions emulating user traffic to Web App1.
You need to ensure that web tests can run unattended.
What should you do first?
A. In Microsoft Visual Studio, modify the .webtest file.
B. Upload the .webtest file to Application Insights.
C. Register the web test app in Azure AD.
D. Add a plug-in to the web test app.
Answer: B (LEAVE A REPLY)
https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep

NEW QUESTION: 190
You have an Azure subscription that contains a resource group named RG1 and the network security groups (NSGs) shown in the following table.

Name	Location	Flow logs status
NSG1	West Europe	Off
NSG2	West Europe	Off

You create the Azure policy shown in the following exhibit.



You assign the policy to RG1.
What will occur if you assign the policy to NSG1 and NSG2?
A. Flow logs will be enabled for NSG2 only.

B. Flow logs will be enabled for NSG1 and NSG2.
C. Flow logs will be disabled for NSG1 and NSG2.
D. Flow logs will be enabled for NSG1 only.
Answer: (SHOW ANSWER)

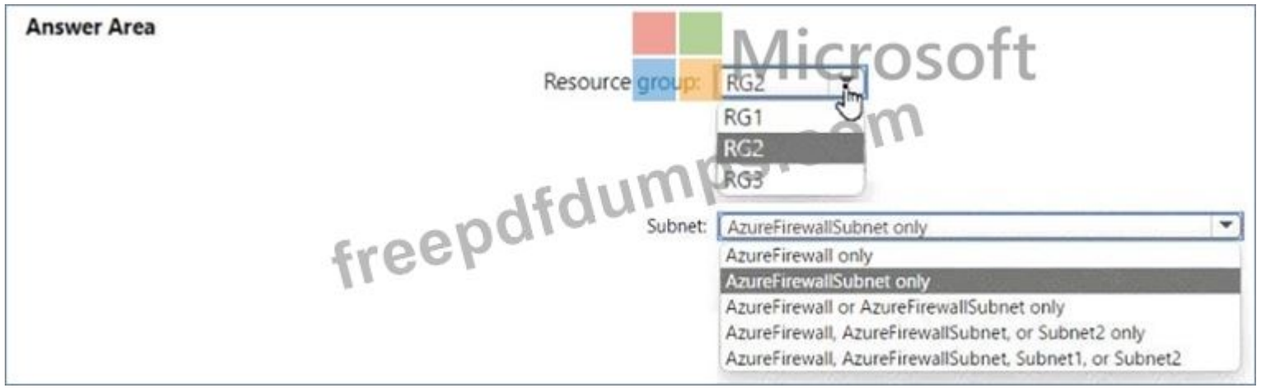
NEW QUESTION: 191
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Location	In resource group
RG1	Resource group	East US	*Not applicable*
RG2	Resource group	West US	*Not applicable*
RG3	Resource group	Central US	*Not applicable*
VNet1	Virtual network	Central US	RG2

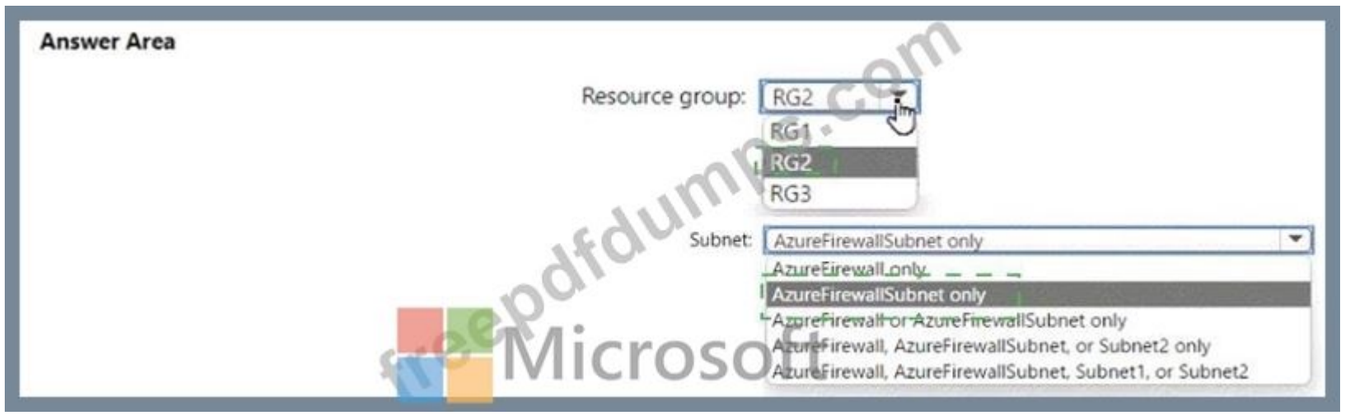
VNet1 contains the subnets shown in the following table.

Name	Description
AzureFirewall	Contains no resources
AzureFirewallSubnet	Contains no resources
Subnet1	Contains a virtual machine
Subnet2	Contains no resources

You plan to use the Azure portal to deploy an Azure firewall named AzFW1 to VNet1.
Which resource group and subnet can you use to deploy AzFW1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

NEW QUESTION: 192

From Azure Security Center, you enable Azure Container Registry vulnerability scanning of the images in Registry1.

You perform the following actions:

Push a Windows image named Image1 to Registry1.

Push a Linux image named Image2 to Registry1.

Push a Windows image named Image3 to Registry1.

Modify Image1 and push the new image as Image4 to Registry1.

Modify Image2 and push the new image as Image5 to Registry1.

Which two images will be scanned for vulnerabilities? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Image2

B. Image3

C. Image5

D. Image4

E. Image1

Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 193

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

You need to use the auto-generated service principal to authenticate to the Azure Container Registry.

What should you create?

A. an Azure Active Directory (Azure AD) group

B. an Azure Active Directory (Azure AD) role assignment

C. an Azure Active Directory (Azure AD) user

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

NEW QUESTION: 194
You have an Azure environment.
You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001:2013 standards.
What should you use?
A. Microsoft Defender for Cloud
B. Microsoft Defender for Identity
C. Microsoft Sentinel
D. Azure Active Directory (Azure AD) Identity Protection
Answer: A (LEAVE A REPLY)

NEW QUESTION: 195
You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Answer:

Explanation:

Step 1: Create an access review program

Step 2: Create an access review control

Step 3: Set Reviewers to Group owners

In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.

References:

https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls

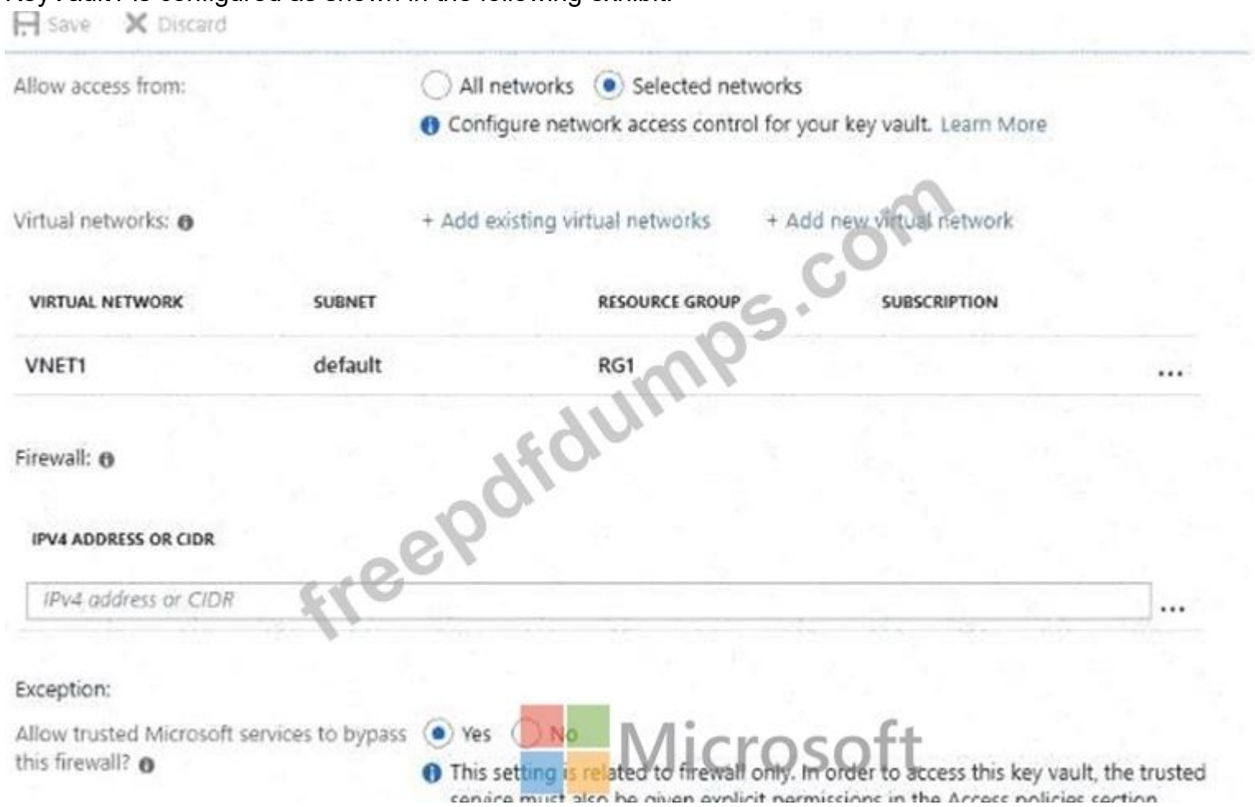
NEW QUESTION: 196

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 enable the Azure Disk Encryption for volume encryption KeyVault1 setting.

KeyVault1 is configured as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Answer Area

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

Answer:

Explanation:

NEW QUESTION: 197

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: Userl -28681041@ExamUsers.com

Azure Password: GpOAe4@lDg

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 7

You need to collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account. To complete this task, sign in to the Azure portal.

Answer:

Check below steps in explanation for Task

Explanation:

To collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account, you can follow these steps:

In the Azure portal, search for and select the virtual machine named VM1.

In the left pane, select Diagnostic settings.

Select Add diagnostic setting.

In the Add diagnostic setting pane, enter the following information:
Name: Enter a name for the diagnostic setting.
Destination: Select Storage account.
Storage account: Select the storage account you want to use.
Logs: Select Windows Event Logs.
Categories: Select Security.
Event types: Select Audit Failure.
Select Save.

NEW QUESTION: 198
You have an Azure subscription that contains an Azure SQL database named SQL1. SQL1 contains the columns shown in the following table.

Name	Contains
Column1	Comments from a confidential investigation
Column2	Government ID numbers
Column3	Images
Column4	Videos

You configure SQL! to use Always Encrypted.
You need to configure deterministic encryption.
Which column supports deterministic encryption?
A. Column2
B. Column4
C. Column3
D. Column1
Answer: A (LEAVE A REPLY)

NEW QUESTION: 199
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Resource provider
VM1	Virtual machine	Microsoft.Compute
storage1	Storage account	Microsoft.Storage
WebApp1	Azure App Service web app	Microsoft.Web

You plan to use service endpoints and service endpoint policies.
Which resources can be accessed by using a service endpoint, and which resources support service endpoint policies? To answer, select the appropriate options in the answer area.
NOTE; Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION: 200

You have an Azure subscription that contains a virtual network named VNet1. The subscription contains an Azure App Service web app named App1.

You have an Azure Front Door profile named AFD1 that has an Azure Web Application Firewall (WAF) policy.

You need to ensure that all inbound traffic to App1 is filtered through AFD1.

What should you do?

A. Configure Microsoft Entra application proxy.

B. For VNet1, configure network security group (NSG) rules.

C. For App1, configure the HTTP headers filter settings.

D. For App1, enable virtual network integration.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 201

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

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

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

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

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

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

NOTE: Each correct selection is worth one point.

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

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

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

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

Answer:

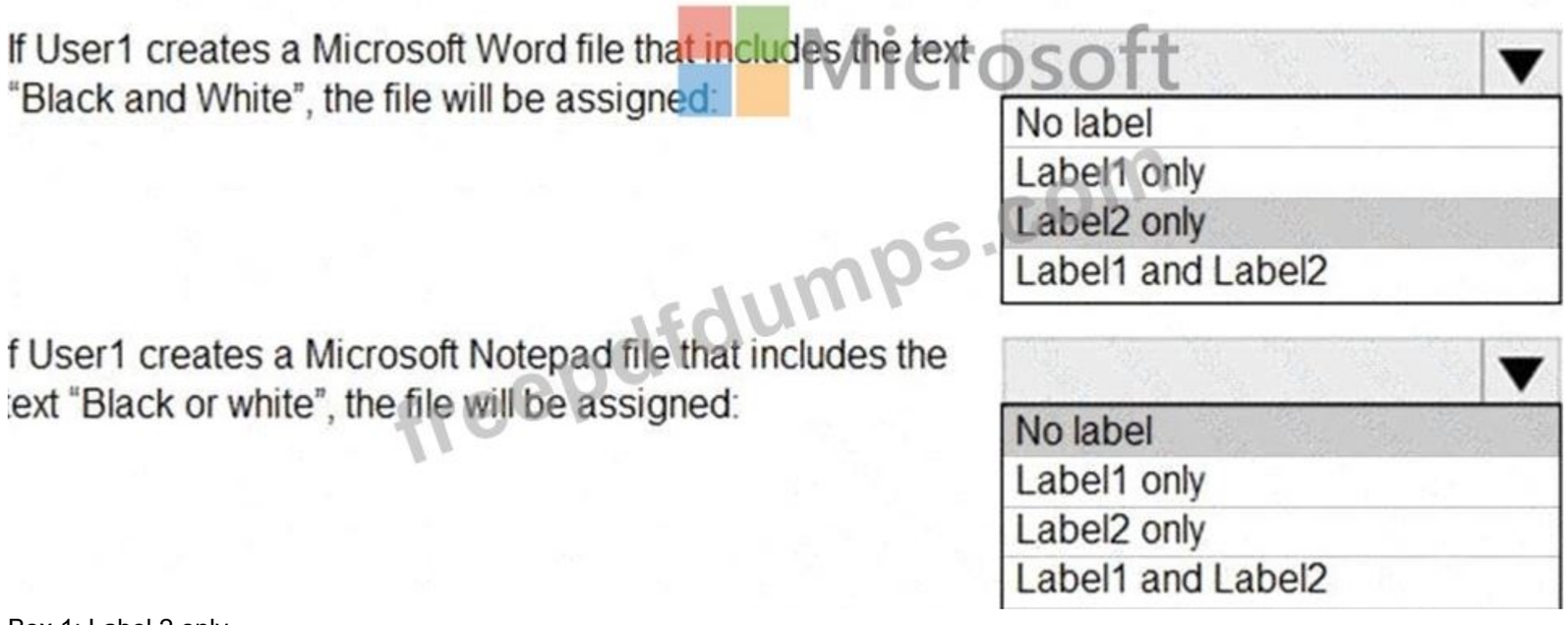
If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

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

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

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

Explanation:



Box 1: Label 2 only

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

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

* The most sensitive label is applied.

* The last sublabel is applied.

Box 2: No Label

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

References:

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

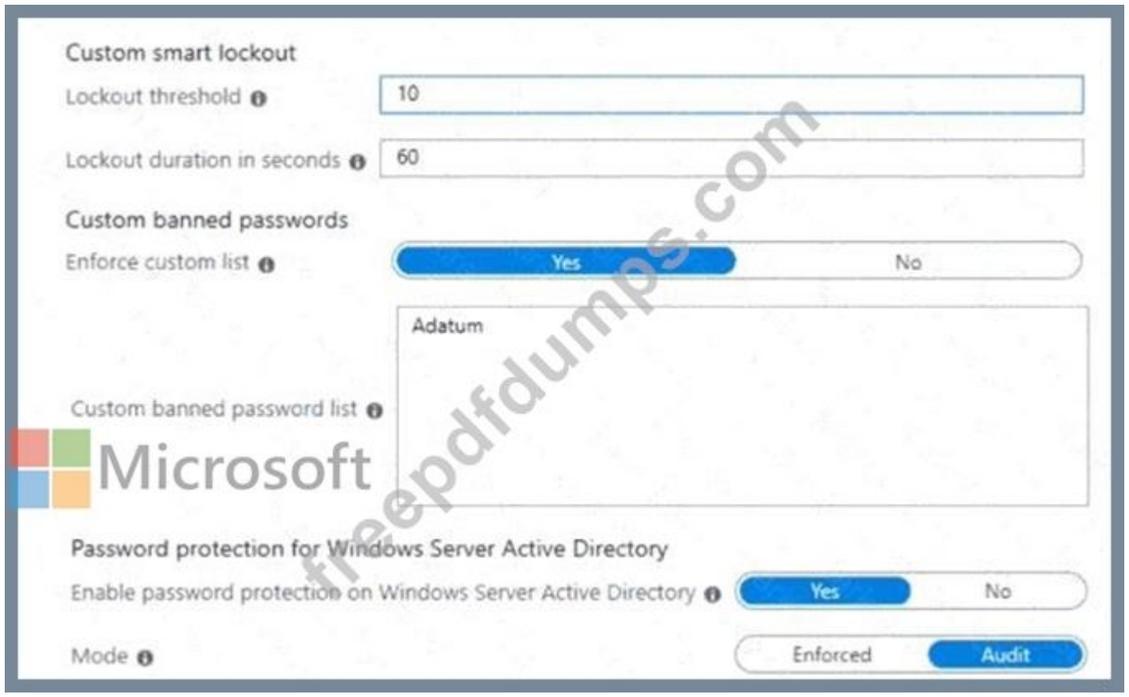
NEW QUESTION: 202

Your network contains an on-premises Active Directory domain named adatum.com that syncs to a Microsoft Entra tenant.

The Microsoft Entra tenant contains the users shown in the following table.

Name	On-premises sync enabled	Password
User1	No	Adatum123
User2	No	N3w3rT0Gue33
User3	Yes	ComplexPassword33

You configure the Microsoft Entra Password Protection settings for adatum.com as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Answer:

Answer Area

Statements	Yes	No
User1 will be prompted to change the password on the next sign-in.	○	○
User2 can change the password to @d@tum_C0mpleX123.	○	○
User3 can change the password to Adatum123!.	○	○

Explanation:

NEW QUESTION: 203
You have an Azure subscription that contains a storage account named storage1 and a virtual machine named VM1.
VM1 is connected to a virtual network named VNet1 that contains one subnet and uses Azure DNS.
You need to ensure that VM1 connects to storage1 by using a private IP address. The solution must minimize administrative effort.
What should you do?
A. On VNet1. create a new subnet.
B. For storage1, create a new private endpoint.
C. Create an Azure Private DNS zone.
D. For storage1, disable public network access.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 204
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 that contains an Azure Kubernetes Service (AKS) cluster named AKS1 and an Azure container registry named AZCR1.
You need to ensure that AKS1 can deploy container images stored in AZCR1.
Solution: You assign the AcrPush role-based access control (RBAC) role to the system-assigned managed identity of AKS1.
Does this meet the requirement?
A. No
B. Yes
Answer: A (LEAVE A REPLY)

NEW QUESTION: 205
You have an Azure subscription that contains the resources show in the following table.

Name	Type
DB1	Azure Cosmos DB account
VM1	Virtual machine
VM2	Virtual machine
VNET1	Virtual network
NSG1	Network security group (NSG)

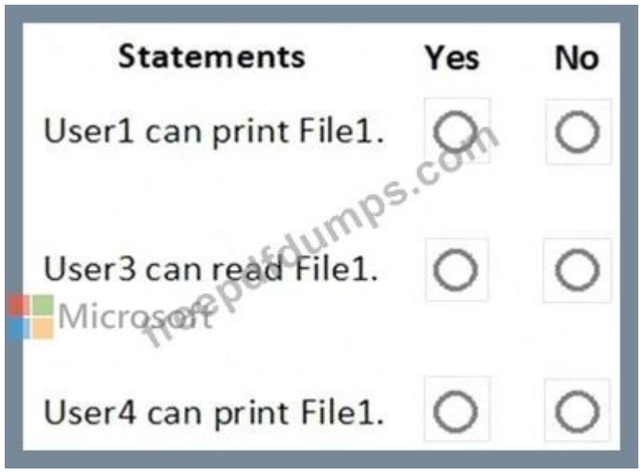
Both VM1 and VM2 connect to VNET1 and are configured to use NSG1.
You need to ensure that only VM1 and VM2 can access DB1.
What should you do?
A. Configure DB1 to allow access from only VNET1.
B. Create an application security group.
C. For NSG1, configure a rule that has a service tag.
D. Add the IP address range of VNET1 to the Firewall setting of DB1.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 206
You have an Azure Active Directory (Azure AD) tenant named contoso1812.onmicrosoft.com that contains the users shown in the following table.

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

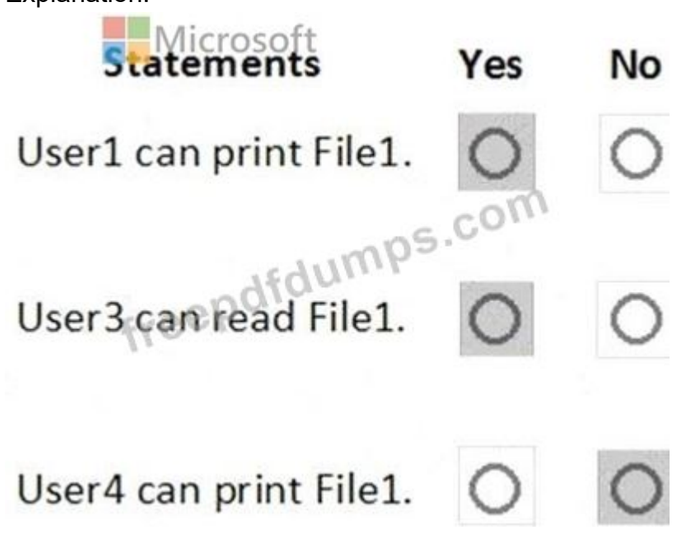
You create an Azure Information Protection label named Label1. The Protection settings for Label1 are configured as shown in the exhibit. (Click the Exhibit tab.)

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



Answer:

Explanation:



NEW QUESTION: 207

You have an Azure environment.
You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001 standards. What should you use?
A. Azure Sentinel
B. Azure Active Directory (Azure AD) Identity Protection
C. Azure Security Center
D. Azure Advanced Threat Protection (ATP)
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard

NEW QUESTION: 208
You have a Microsoft Entra tenant named contoso.com that contains a user named User1.
You register an app named App1 in contoso.com and create an app role named Role1.
You need to assign Role1 to User1.
What should you configure on the Enterprise applications blade of App1 in the Microsoft Entra admin center?
A. Users and groups
B. Roles and administrators
C. API permissions
D. App roles
Answer: (SHOW ANSWER)

NEW QUESTION: 209
You are securing access to the resources in an Azure subscription.
A new company policy states that all the Azure virtual machines in the subscription must use managed disks.
You need to prevent users from creating virtual machines that use unmanaged disks.
What should you use?
A. Azure Service Health
B. Azure Policy
C. Azure Monitor
D. Azure Security Center
Answer: B (LEAVE A REPLY)

NEW QUESTION: 210
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.

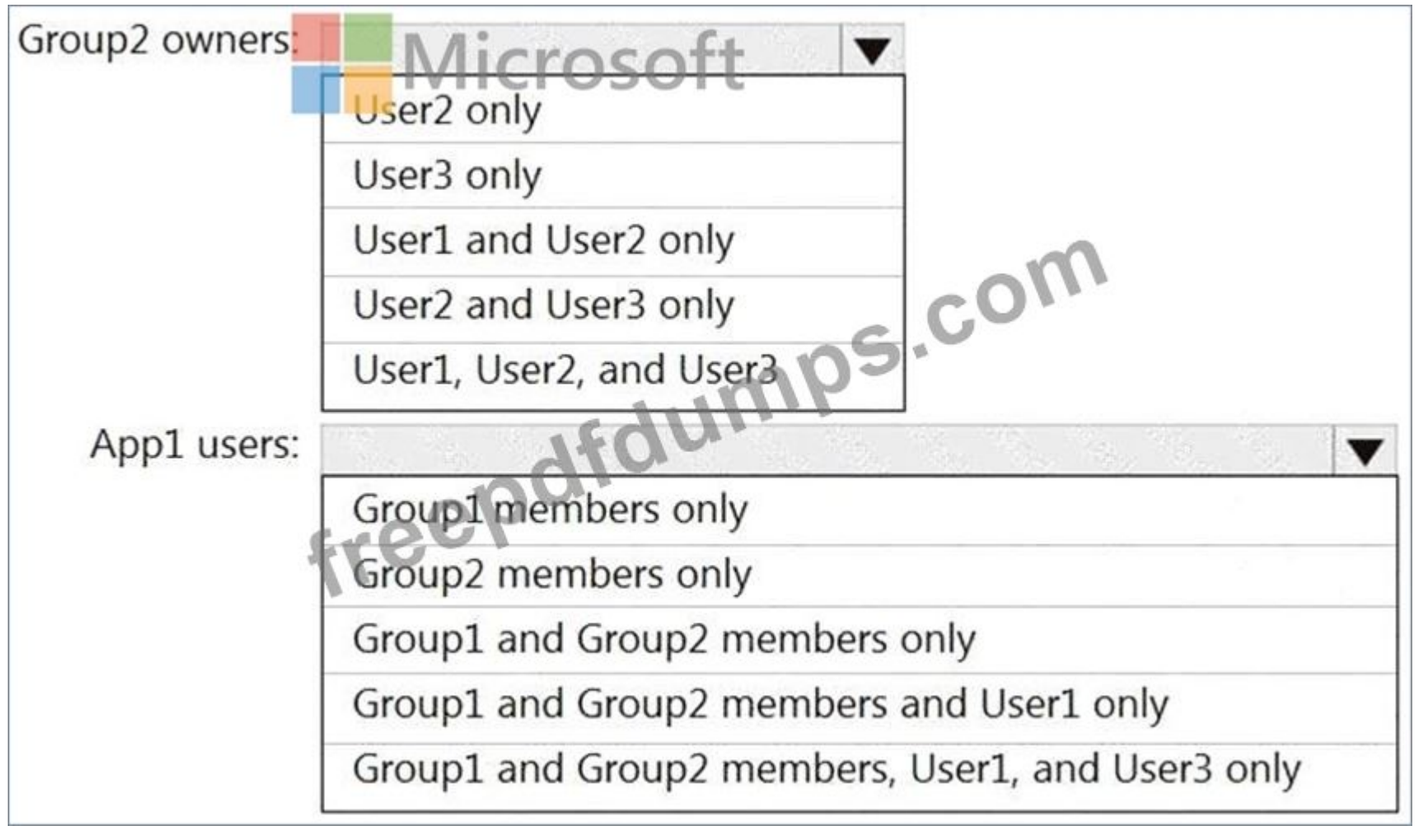
You enable self-service application access for App1 as shown in the following exhibit.

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.



Answer:

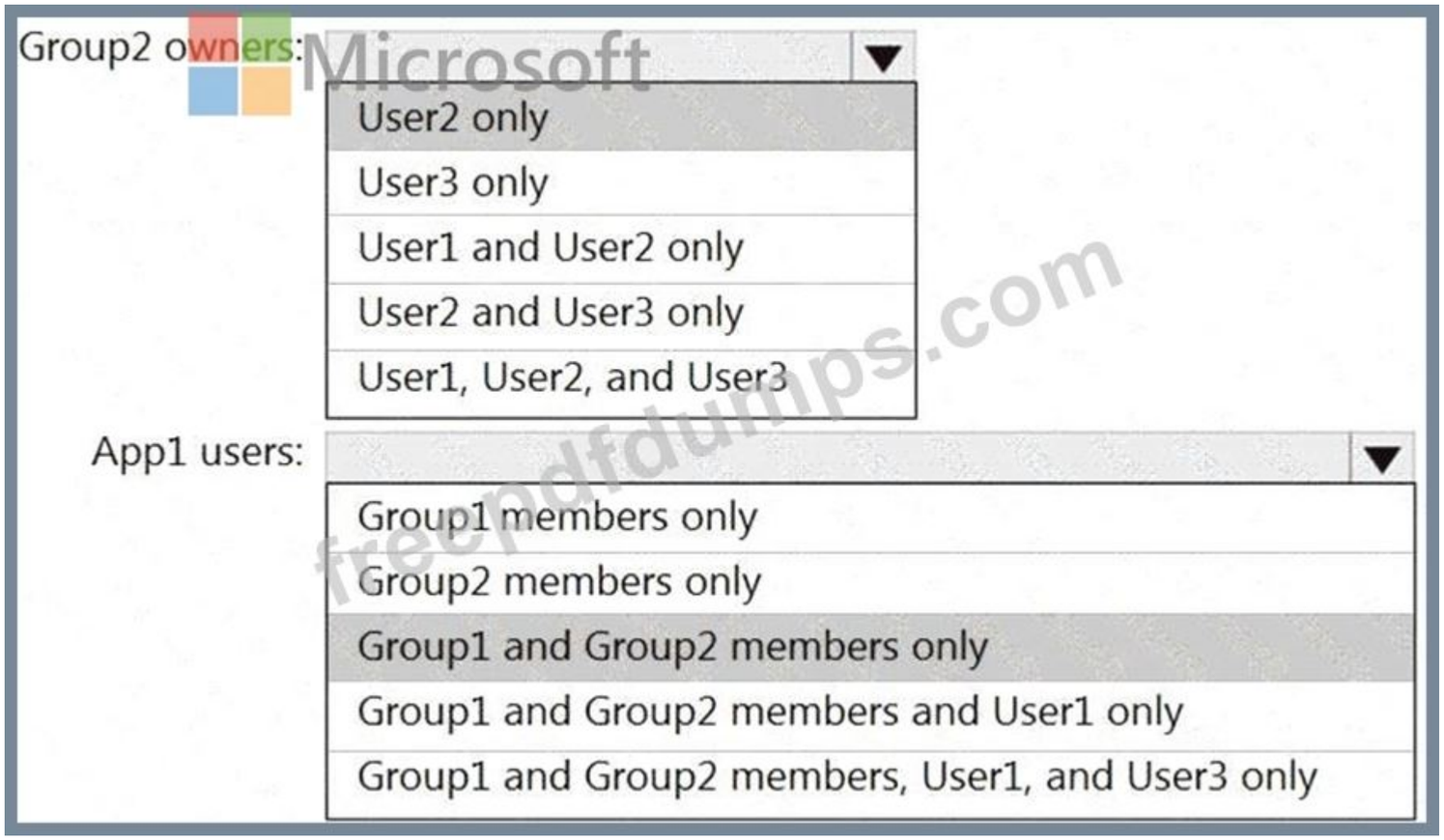
Group2 owners:

- 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:

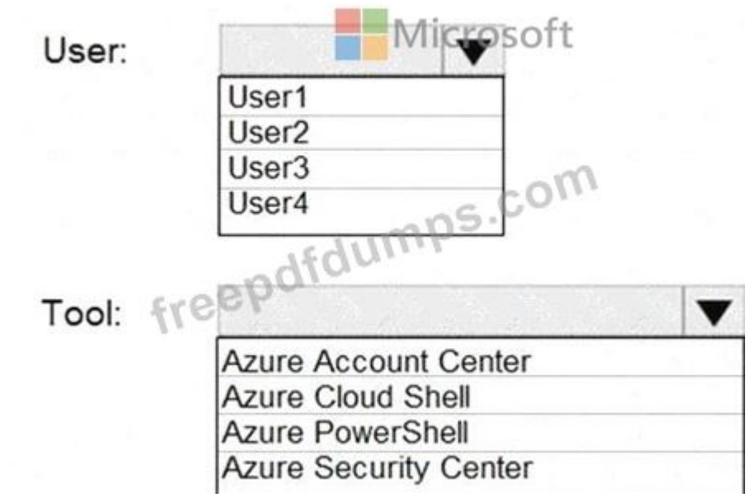


Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access

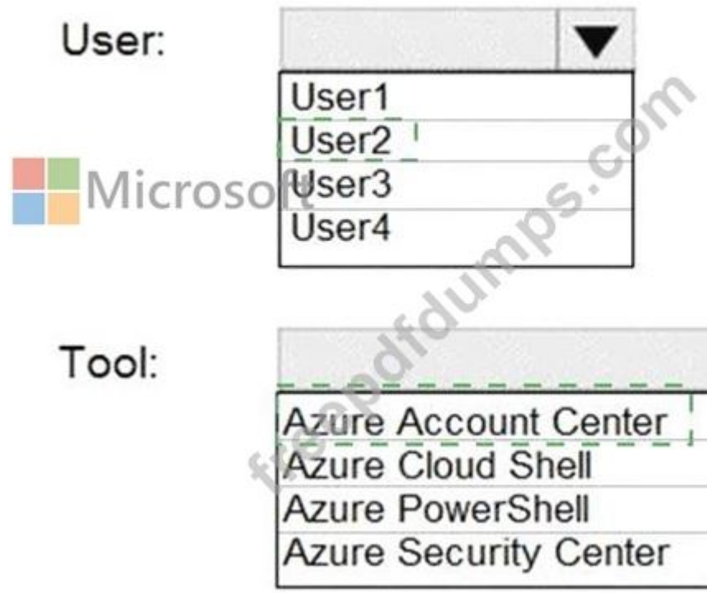
NEW QUESTION: 211
Your company has an Azure subscription named Subscription1 that contains the users shown in the following table.

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

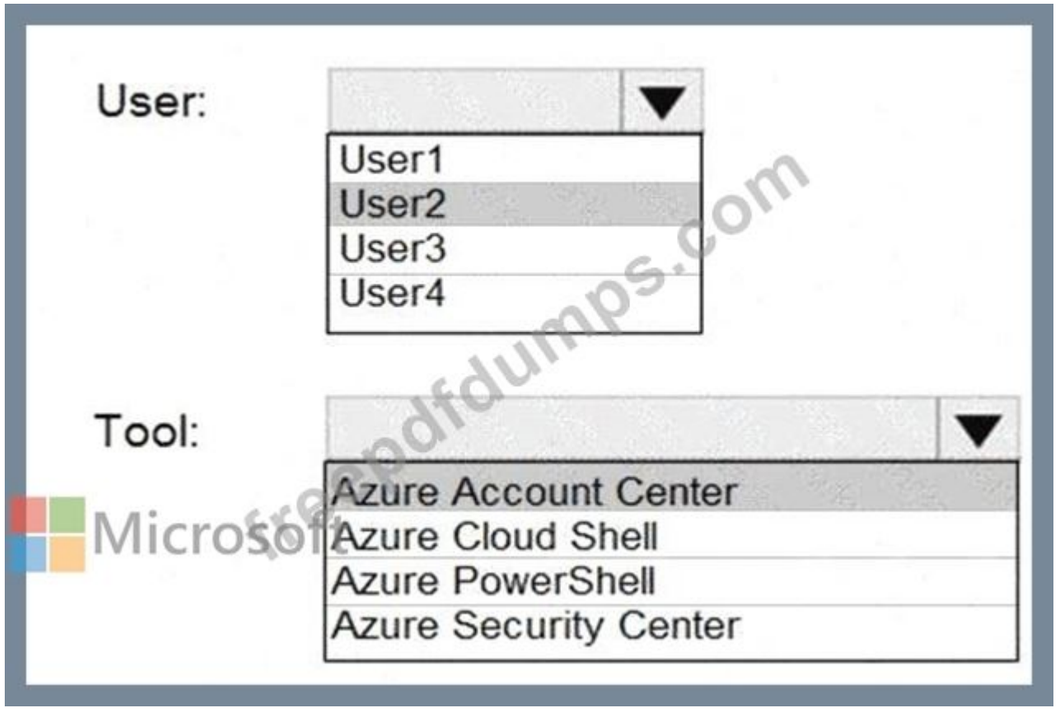
The company is sold to a new owner.
The company needs to transfer ownership of Subscription1.
Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



Box 1; User2

Billing Administrator

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

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

Box 2: Azure Account Center

Azure Account Center can be used.

Reference:

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

NEW QUESTION: 212

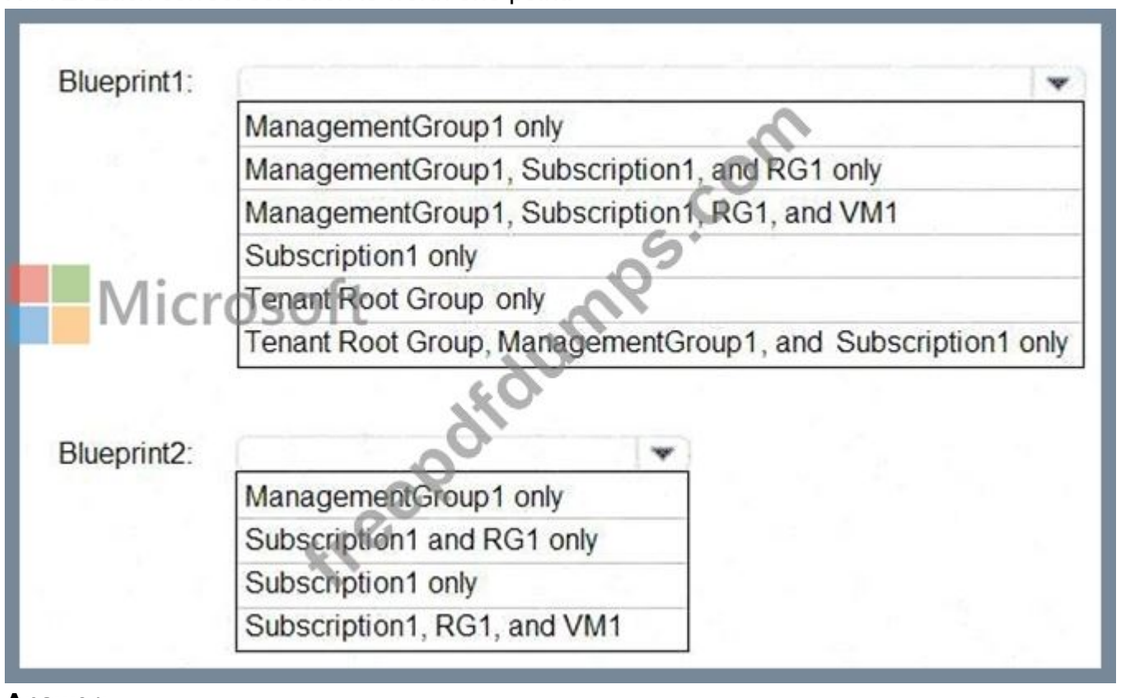
You have the hierarchy of Azure resources shown in the following exhibit.

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

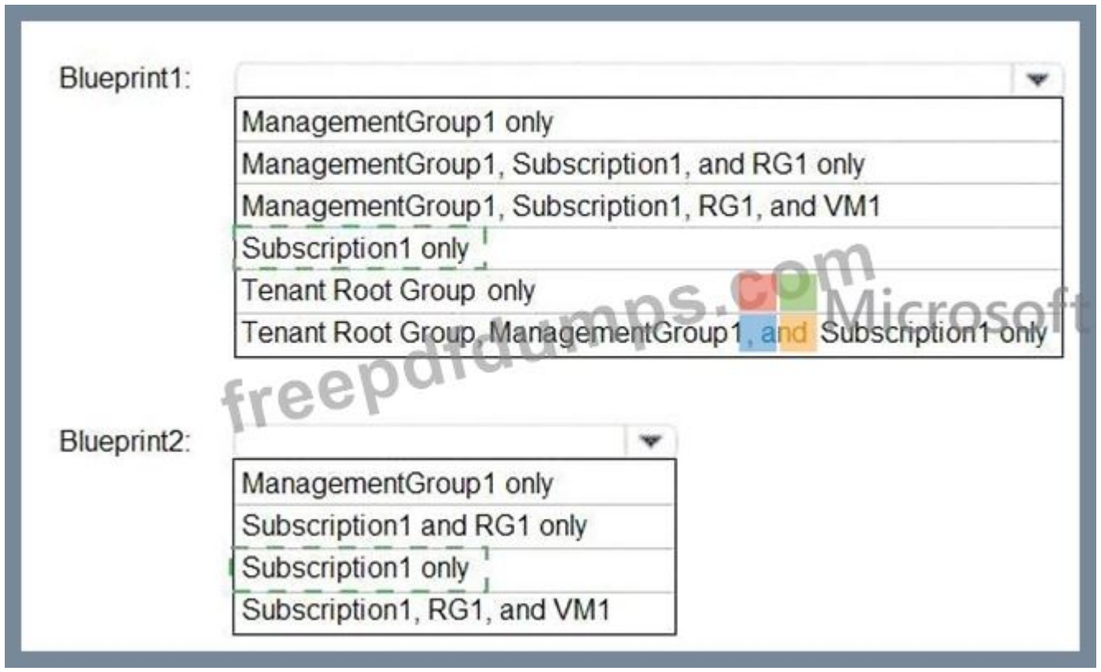
Name	Published at
Blueprint1	Tenant Root Group
Blueprint2	Subscription1

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

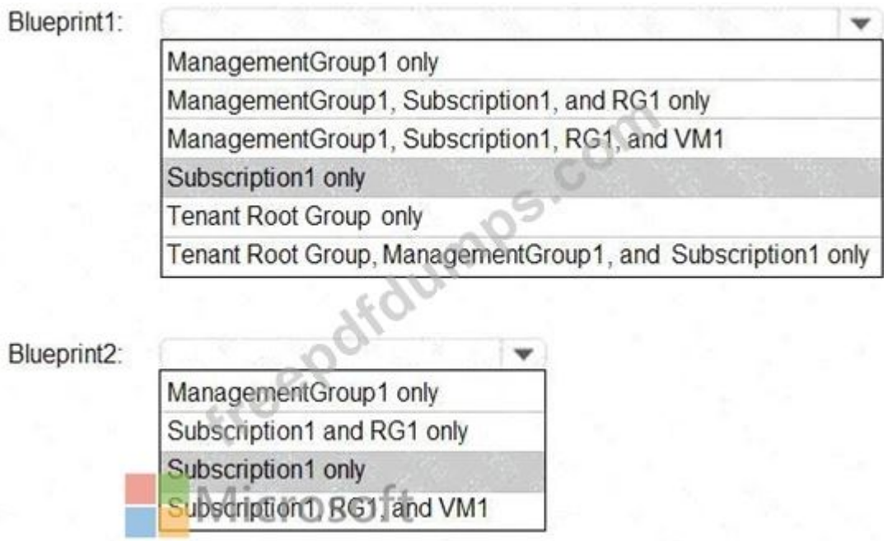
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



Blueprints can only be assigned to subscriptions.

NEW QUESTION: 213

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

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

What should you use?

A. Azure Advisor

B. an Azure Desired State Configuration (DSC) virtual machine extension

C. security policies in Azure Security Center

D. Azure Logic Apps

Answer: B (LEAVE A REPLY)

NEW QUESTION: 214

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.	○	○
Admin2 can purge secret1 on June 12.	○	○
Admin3 can recover key1 on June 17.	○	○

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.	○	○

Explanation:

Yes

Yes

No

NEW QUESTION: 215

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",
                "Microsoft.Storage/storageAccounts/ListAccountSas/action",
                "Microsoft.Storage/storageAccounts/read"
            ],
            "notActions": [],
            "dataActions": [],
            "notDataActions": []
        }
]
```

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

Name	Role
User1	Role1
User2	Role2
User3	Role1, Role2

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

Answer:

Answer Area

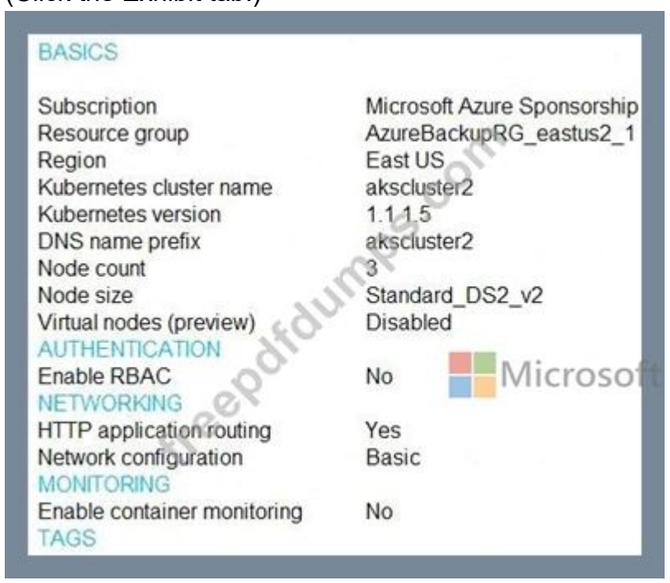
Statements	Yes	No
User1 can read data in storage1.	○	○
User2 can read data in storage1.	○	○
User3 can restore storage1 from a backup in Azure Backup.	○	○

Explanation:

NEW QUESTION: 216

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

(Click the Exhibit tab.)



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: 217

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

Name	Connected 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	Yes	No
Connections from VM1 to storage1 always use IP address 10.1.1.5.	○	○
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	○	○
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	○	○

Answer:

Answer Area

Statements	Yes	No
Connections from VM1 to storage1 always use IP address 10.1.1.5.	○	○
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	○	○
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	○	○

Explanation:

Answer Area

Statements	Yes	No
Connections from VM1 to storage1 always use IP address 10.1.1.5.	○	●
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	○	●
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	●	○

NEW QUESTION: 218

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": "3336fcbf-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": "i
    `   "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:

See the answer below at Explanation.

Explanation:

Answer is as image below.

NEW QUESTION: 219
You have an Azure subscription that contains a virtual machine named VM1.
You are creating a data collection rule (DCR) named DCR1 that will collect events from VM1.
You need to ensure that only events that have an ID of 4798 are collected.
What should you use in DCR1?
A. a KQL query
B. an XPath query
C. a PowerShell script
D. aT-SQLquery
Answer: B (LEAVE A REPLY)

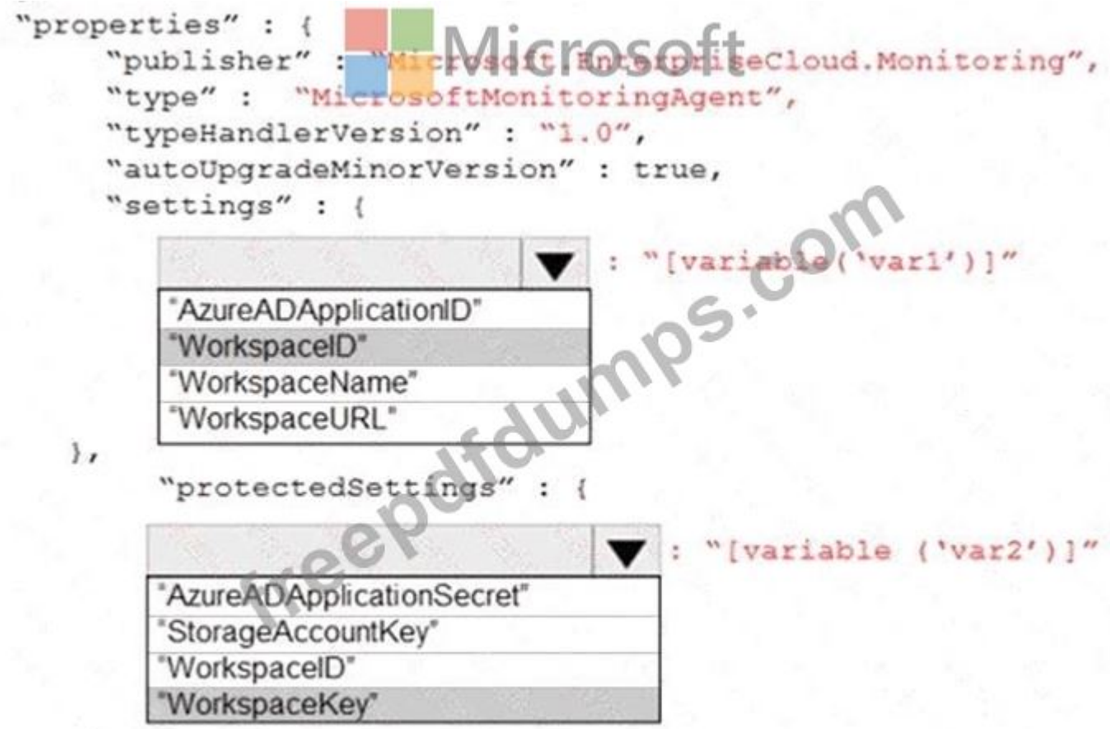
NEW QUESTION: 220
You plan to use Azure Log Analytics to collect logs from 200 servers that run Windows Server 2016.
You need to automate the deployment of the Microsoft Monitoring Agent to all the servers by using an Azure Resource Manager template.
How should you complete the template? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

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


Answer:

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


Explanation:



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

NEW QUESTION: 221
You have 15 Azure virtual machines in a resource group named RG1.
All virtual machines run identical applications.
You need to prevent unauthorized applications and malware from running on the virtual machines.
What should you do?
A. Configure Azure Active Directory (Azure AD) Identity Protection.
B. From Microsoft Defender for Cloud, configure adaptive application controls.
C. Apply an Azure policy to RGI.
D. Apply a resource lock to RGI.
Answer: (SHOW ANSWER)
Microsoft Defender for Cloud helps you prevent, detect, and respond to threats. Defender for Cloud gives you increased visibility into, and control over, the security of your Azure resources. It provides integrated security monitoring and policy management across your Azure subscriptions. It helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions.
Defender for Cloud helps you optimize and monitor the security of your virtual machines by:
* Providing security recommendations for the virtual machines. Example recommendations include:
apply system updates, configure ACLs endpoints, enable antimalware, enable network security groups, and apply disk encryption.
* Monitoring the state of your virtual machines.

https://learn.microsoft.com/en-us/azure/security/fundamentals/virtual-machines-overview

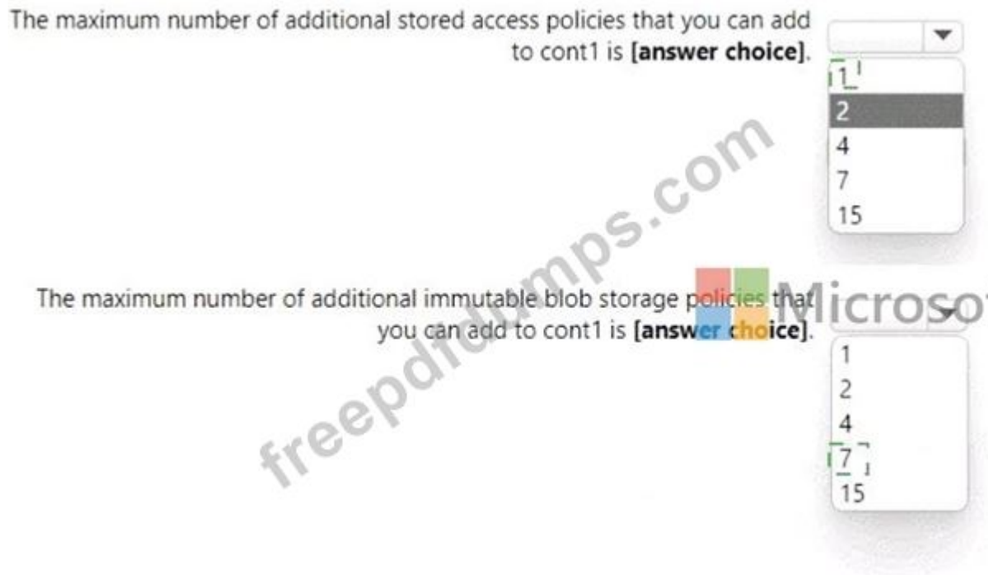
NEW QUESTION: 222
Lab Task
Task 2
You need to ensure that the events in the NetworkSecurityGroupRuleCounter log of the VNETOI-Subnet0-NSG network security group (NSG) are stored in the logs31330471 Azure Storage account for 30 days.
Answer:
see the task answer with step by step below:
Enable diagnostic resource logging for the NSG. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select the Rule counter category under Logs and choose the logs31330471 storage account as the destination.
Configure the retention policy for the storage account to keep the logs for 30 days. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to specify the days parameter as
30 for the Set-AzStorageServiceProperty cmdlet or the az storage logging update command.
View and analyze the logs in the storage account. You can use any tool that can read JSON files, such as Azure Storage Explorer or Visual Studio Code. You can also export the logs to any visualization tool, SIEM solution, or IDS of your choice

NEW QUESTION: 223
You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure SQL Database instance that is configured to support Azure AD authentication.
Database developers must connect to the database instance and authenticate by using their on-premises Active Directory account.
You need to ensure that developers can connect to the instance by using Microsoft SQL Server Management Studio. The solution must minimize authentication prompts.
Which authentication method should you recommend?
A. Active Directory - Password
B. Active Directory - Universal with MFA support
C. SQL Server Authentication
D. Active Directory - Integrated
Answer: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

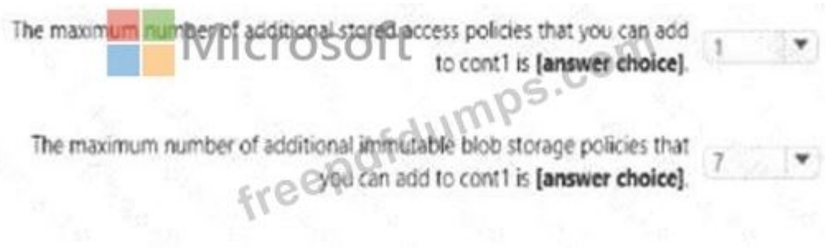
NEW QUESTION: 224
You have an Azure subscription that contains a blob container named cont1. Cont1 has the access policies shown in the following exhibit.

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

Answer:



Explanation:



NEW QUESTION: 225

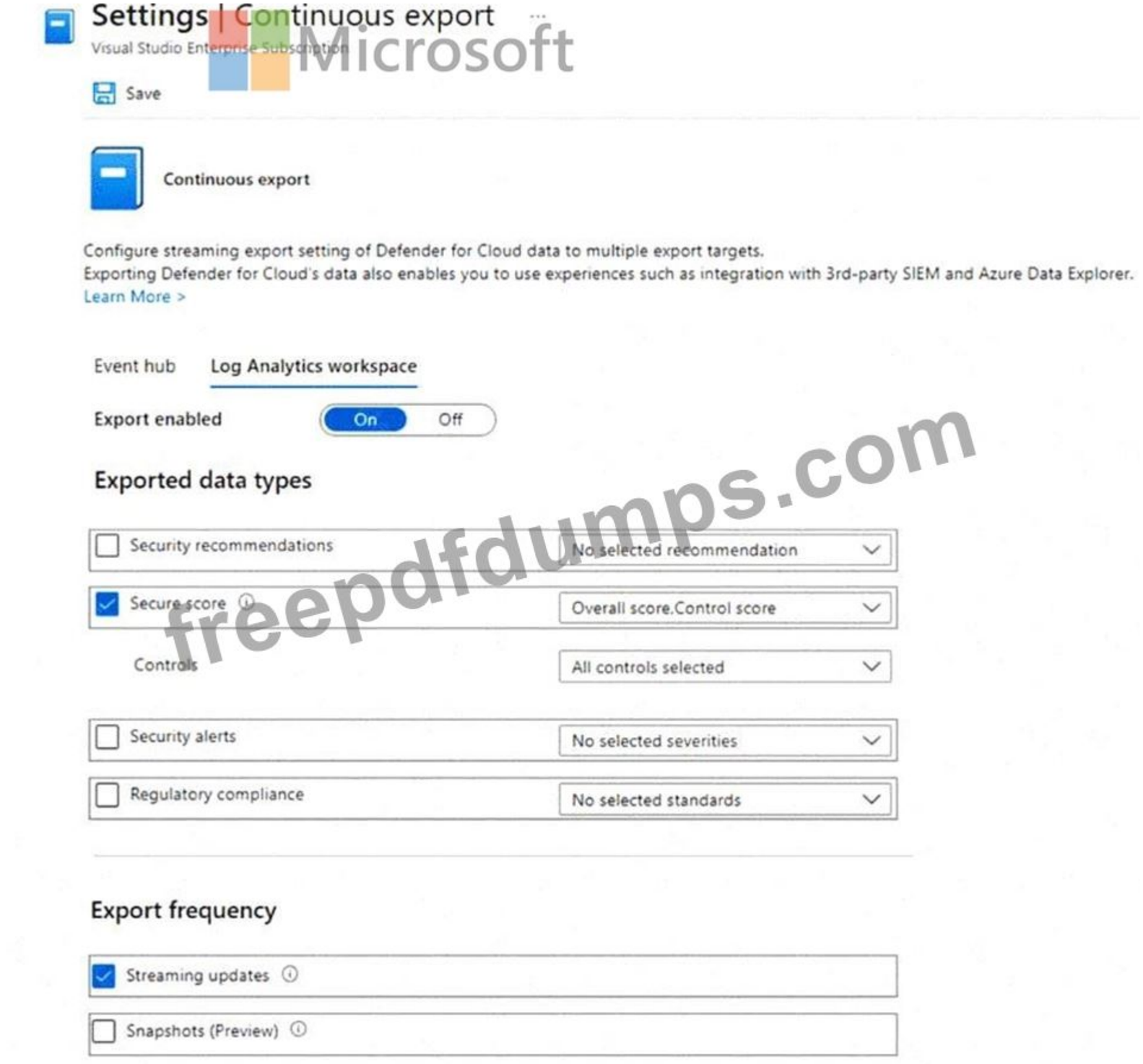
You have an Azure subscription that uses Microsoft Defender for Cloud.

You plan to use the Secure Score Over Time workbook.

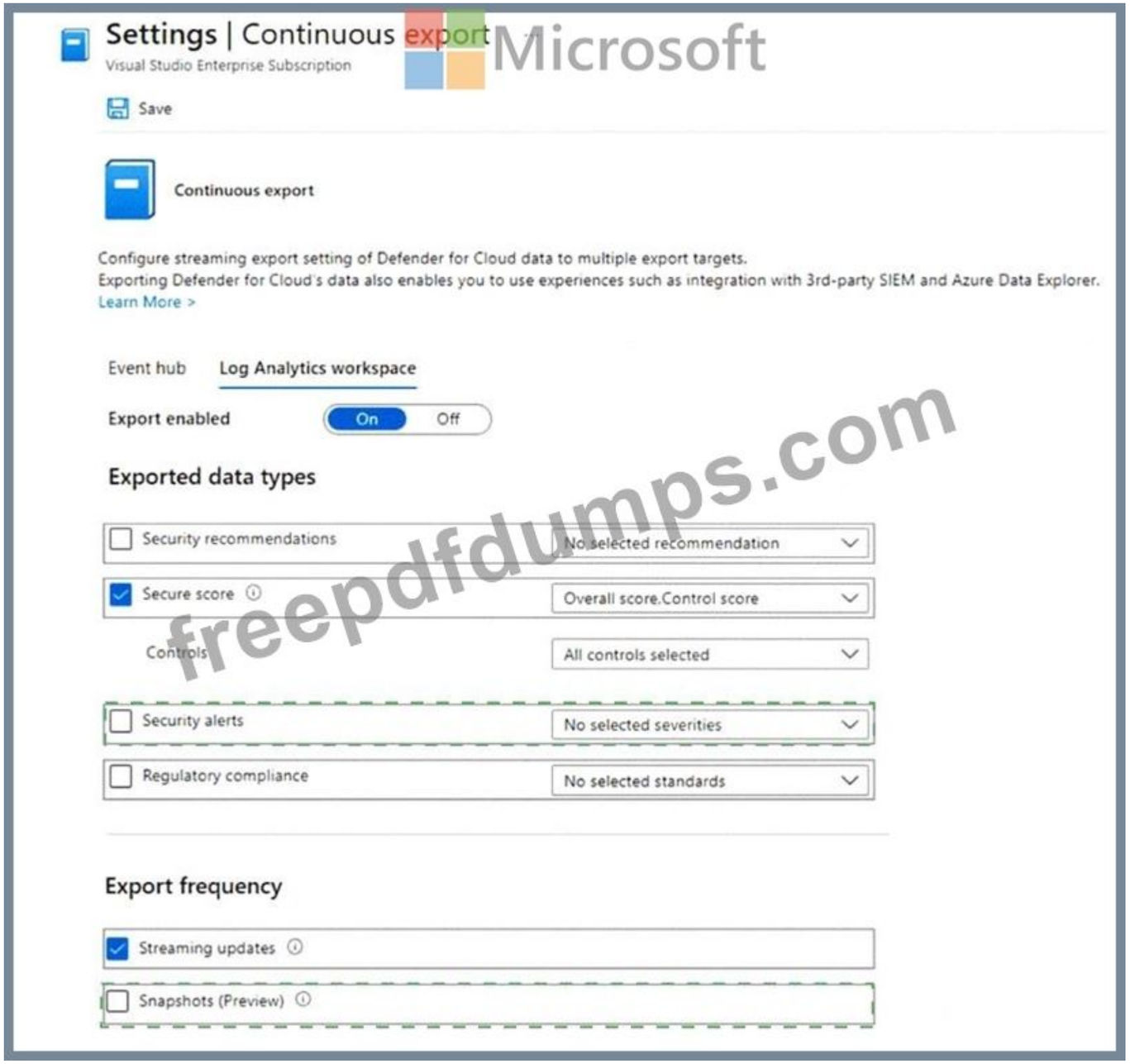
You need to configure the Continuous export settings for the Defender for Cloud data.

Which two settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

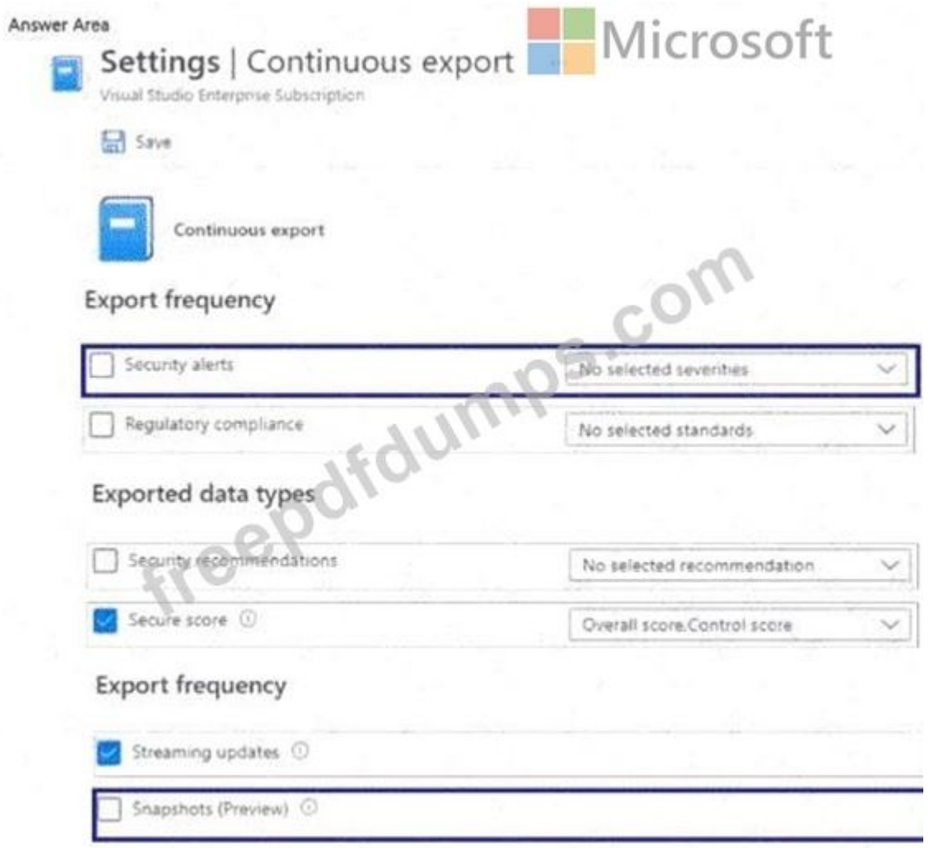


Answer:



Explanation:

Answer Area



NEW QUESTION: 226
You need to implement the planned change for SQLdb1.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. Create a compliance policy.
B. Configure Federated client identity for SQLdb1.
C. Configure a user-assigned managed identity for SQLdb1.
D. Create a Conditional Access policy.
E. Configure Microsoft Entra authentication for SQLServer1.
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 227

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.
You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to Sa1.
Solution: You create a lock on Sa1.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier.
Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.
References:
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

NEW QUESTION: 228
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:

Answer Area

Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	○	○
User2 can configure firewalls and virtual networks for Vault1.	○	○
User3 can add access policies to Vault1.	○	○

Explanation:

Answer Area

Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	●	○
User2 can configure firewalls and virtual networks for Vault1.	○	●
User3 can add access policies to Vault1.	○	●

NEW QUESTION: 229

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

Name	Subnet	Subnet-associated network security group (NSG)	Peered with
VNet1	Subnet1	NSG1	VNet2
VNet2	Subnet2	NSG2	VNet1

NSG1 and NSG2 both have default rules only.

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

Name	Connected to
VM1	Subnet1
VM2	Subnet2

The subscription contains t he app service web apps shown in the following table.

Name	Description
WebApp1	Uses an App Service plan in the Premium pricing tier and has virtual network integration with VNet1
WebApp2	Uses an App Service plan in the Isolated pricing tier and is deployed to Subnet2

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
WebApp1 can connect to VM2.	○	○
NSG1 controls inbound traffic to WebApp1.	○	○
WebApp2 can connect to VM1.	○	○

Answer:

Answer Area

Statements	Yes	No
WebApp1 can connect to VM2.	◉	○
NSG1 controls inbound traffic to WebApp1.	◉	○
WebApp2 can connect to VM1.	○	◉

Explanation:

Answer Area

Statements	Yes	No
WebApp1 can connect to VM2.	◉	○
NSG1 controls inbound traffic to WebApp1.	◉	○
WebApp2 can connect to VM1.	○	◉

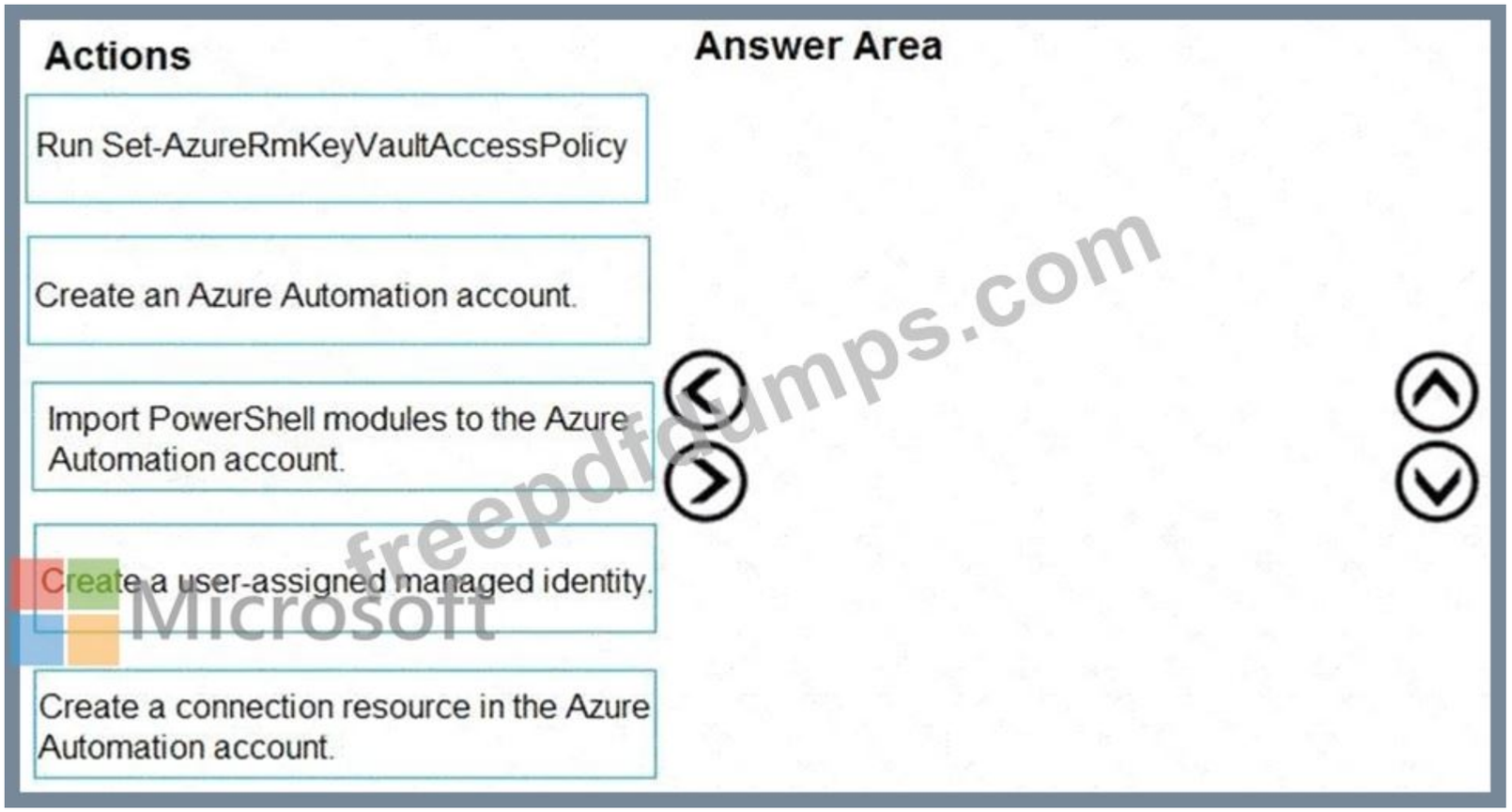
NEW QUESTION: 230

You have an Azure subscription named Sub1 that contains an Azure Storage account named Contosostorage1 and an Azure key vault named Contosokeyvault1.

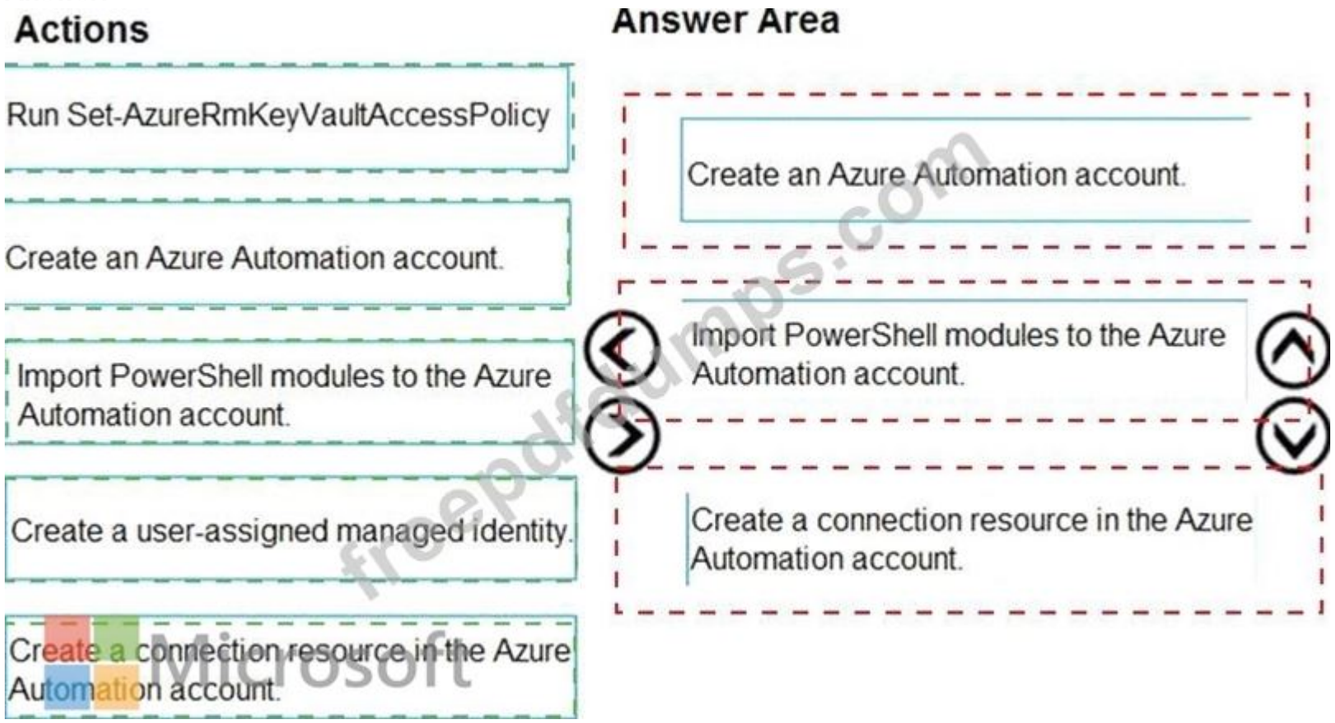
You plan to create an Azure Automation runbook that will rotate the keys of Contosostorage1 and store them in Contosokeyvault1.

You need to implement prerequisites to ensure that you can implement the runbook.

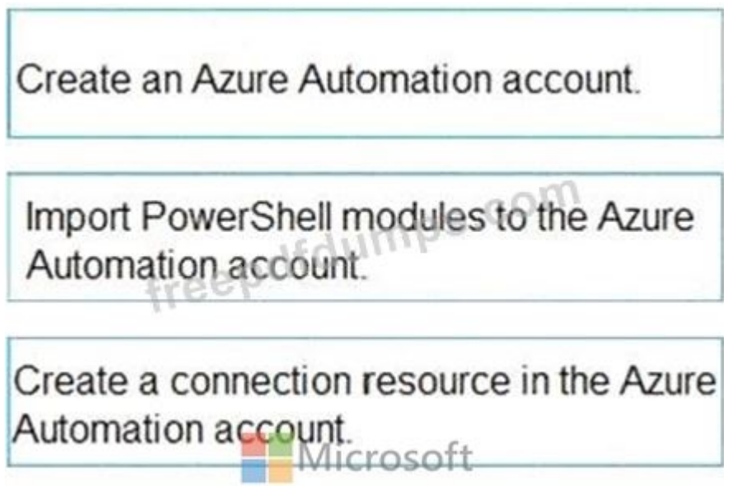
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.


Actions
Answer Area
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.
freepdfdumps.com
Microsoft

Answer:


Actions
Answer Area
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.
Create an Azure Automation account.
Import PowerShell modules to the Azure Automation account.
Create a connection resource in the Azure Automation account.
freepdfdumps.com
Microsoft

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: 231
You have an Azure subscription that uses Azure AD Privileged Identity Management (PIM).
A user named User1 is eligible for the Billing administrator role.

You need to ensure that the role can only be used for a maximum of two hours.
What should you do?
A. Create a new access review.
B. Update the end date of the user assignment
C. Edit the role assignment settings.
D. Edit the role activation settings.
Answer: (SHOW ANSWER)

NEW QUESTION: 232
You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

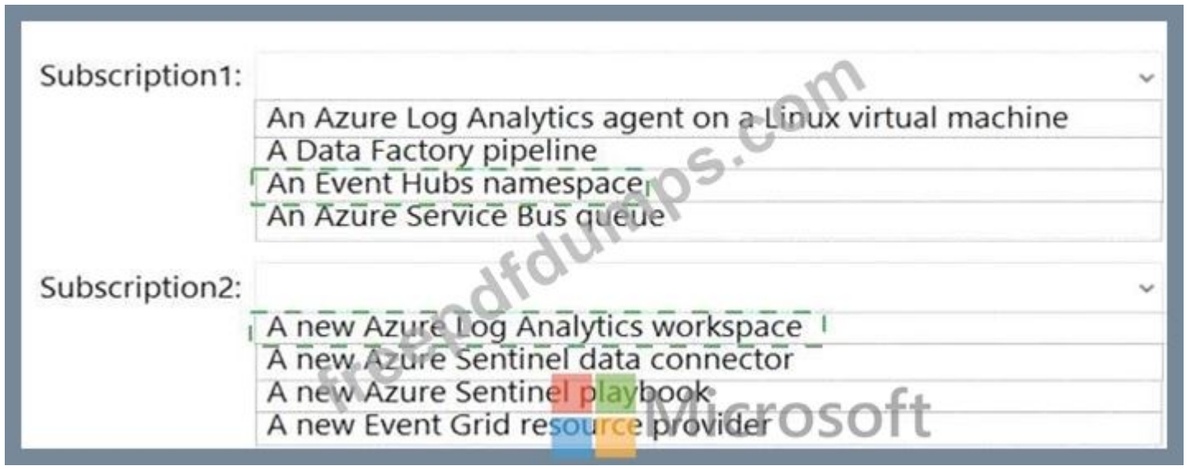
Name	Type	Description
EventHub1	Azure Event Hubs	**Not applicable**
Adf1	Azure Data Factory	**Not applicable**
NVA1	Network virtual appliance (NVA)	The NVA sends security event messages in the Common Event Format (CEF).

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:



Explanation:

Graphical user interface, text, application, email Description automatically generated

NEW QUESTION: 233

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

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

You use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a policy initiative and assignments that are scoped to resource groups.

Does this meet the goal?

A. Yes

B. No

Answer: B (LEAVE A REPLY)

Instead use a management group.

Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously.

Reference:

https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-managementgroups/

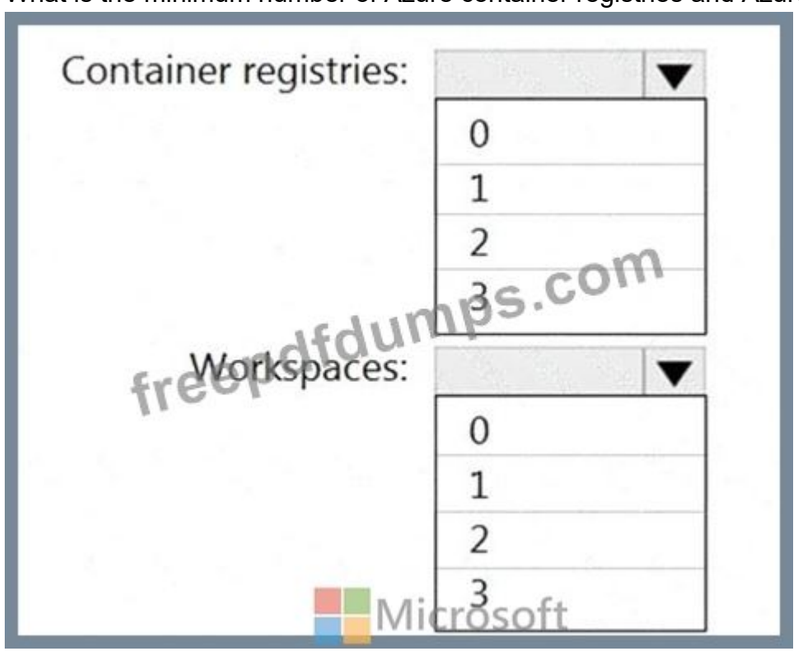
NEW QUESTION: 234
Lab Task
use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password. place your cursor in the Enter password box and click on the password below.
Azure Username: Userl -28681041@ExamUsers.com
Azure Password: GpOAe4@lDg
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: 235
Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.
You need to configure each subscription to have the same role assignments.
What should you use?
A. Azure Security Center
B. Azure Policy
C. Azure AD Privileged Identity Management (PIM)
D. Azure Blueprints
Answer: D (LEAVE A REPLY)
Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements.
Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:
Role Assignments
Policy Assignments
Azure Resource Manager templates
Resource Groups
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

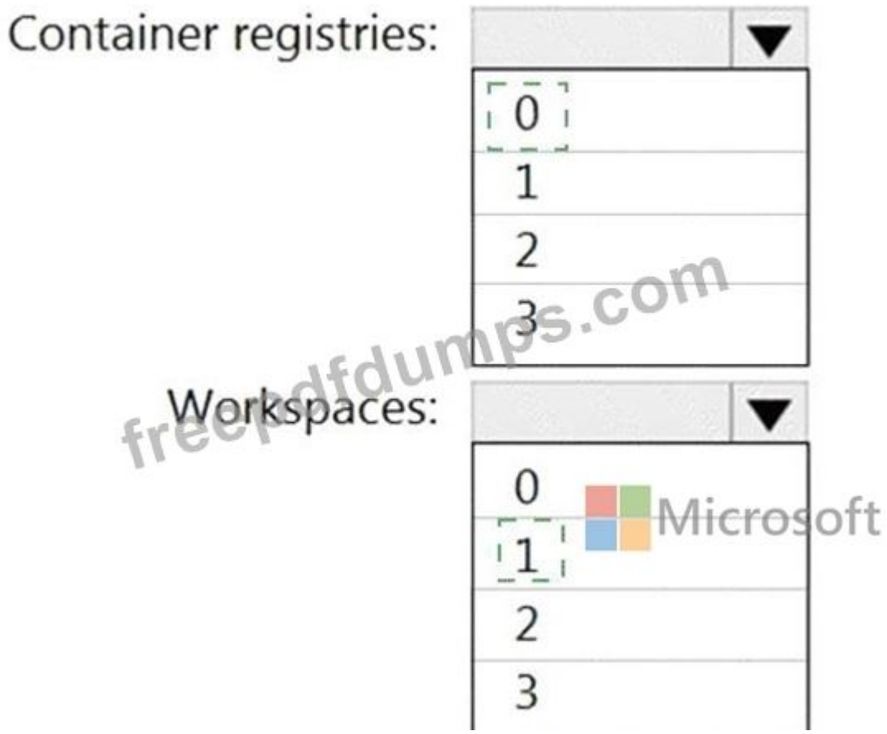
NEW QUESTION: 236

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

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

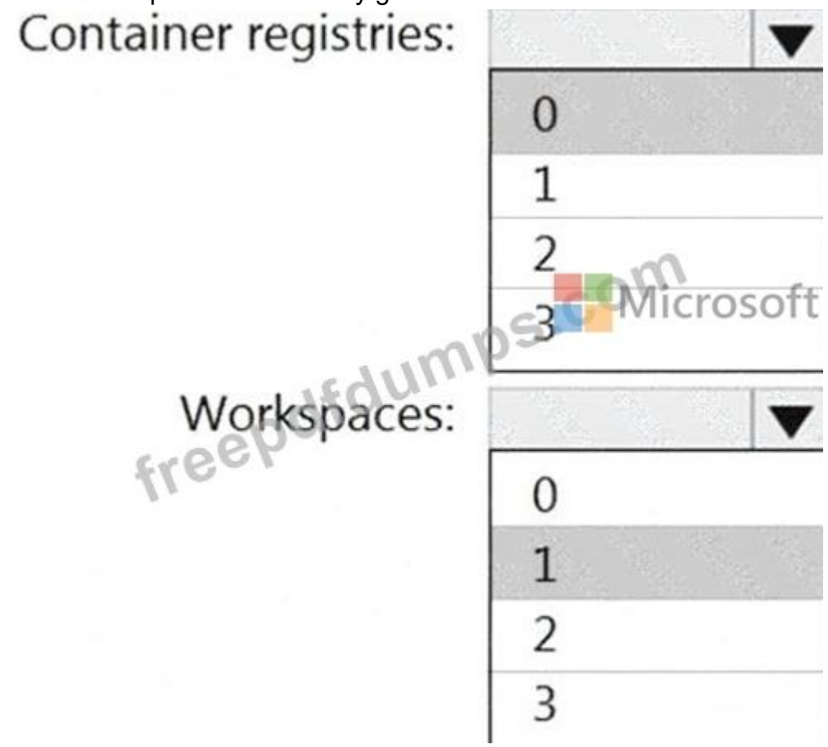


Answer:



Explanation:

Table Description automatically generated with medium confidence

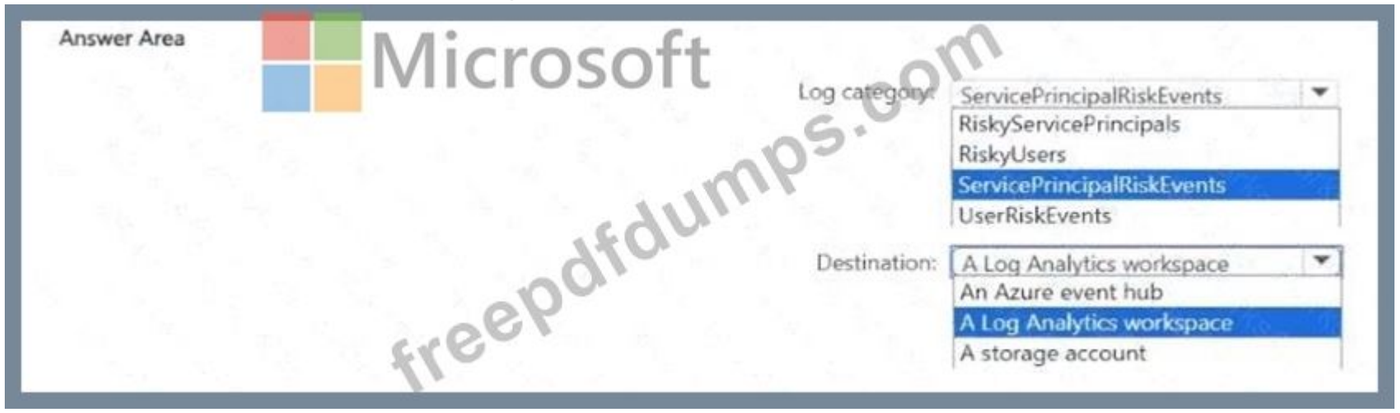


Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

NEW QUESTION: 237
You have 10 on-premises servers that run Windows Server 2019.
You plan to implement Azure Security Center vulnerability scanning for the servers.
What should you install on the servers first?
A. the Security Events data connector in Azure Sentinel
B. the Microsoft Endpoint Configuration Manager client
C. the Azure Arc enabled servers Connected Machine agent
D. the Microsoft Defender for Endpoint agent
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/azure-arc/servers/agent-overview
https://docs.microsoft.com/en-us/azure/security-center/deploy-vulnerability-assessment-vm

NEW QUESTION: 238
You have an Azure subscription that is linked to a Microsoft Entra tenant. The tenant uses Microsoft Entra ID Protection.
You have 2,000 users that are each assigned a Microsoft Entra ID P2 license.
You plan to use Azure Monitor to generate an alert when a workload identity that is using leaked credentials is detected.
You need to configure the Diagnostic setting to support the planned alert. The solution must minimize administrative effort.

Which log category should you collect, and to
which destination should you send the logs? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

NEW QUESTION: 239
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)

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership Scenario:
Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1.
The tenant currently contain this group:

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

References:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure- portal

NEW QUESTION: 240
You have an Azure subscription.
You plan to create a workflow automation in Microsoft Defender for Cloud that will automatically remediate a security vulnerability.
What should you create first?
A. an automation account
B. a managed identity
C. an Azure logic app
D. an alert rule
E. an Azure function app
Answer: (SHOW ANSWER)

NEW QUESTION: 241
You have an Azure subscription that contains an Azure SQL database named SQL1. You need to configure SQL1 to use Always Encrypted. What should you use?
A. the Azure portal
B. MySQL Workbench
C. Microsoft SQL Server Management Studio (SSMS)
D. pgAdmin
Answer: C (LEAVE A REPLY)

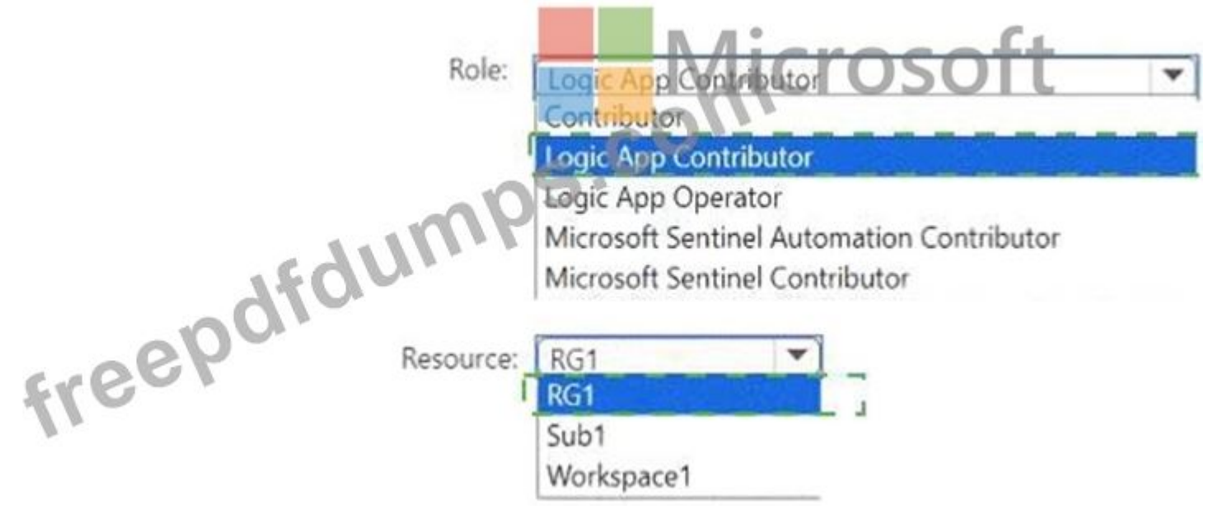
NEW QUESTION: 242
You have an Azure subscription named Sub1 and use Microsoft Defender for Cloud. Sub1 contains a user named User1 and a resource group named RG1. RG1 contains a Log Analytics workspace named Workspace1.
You need to ensure that User1 can modify Azure Logic Apps workflows triggered in response to security incidents. The solution must follow the principle of least privilege.
Which role should you assign to User1. and to which resource should you assign the role? To answer, select the appropriate options in the answer area.

NOTE; Each correct selection is worth one point.

Answer Area

Answer:

Answer Area



Explanation:

Answer Area