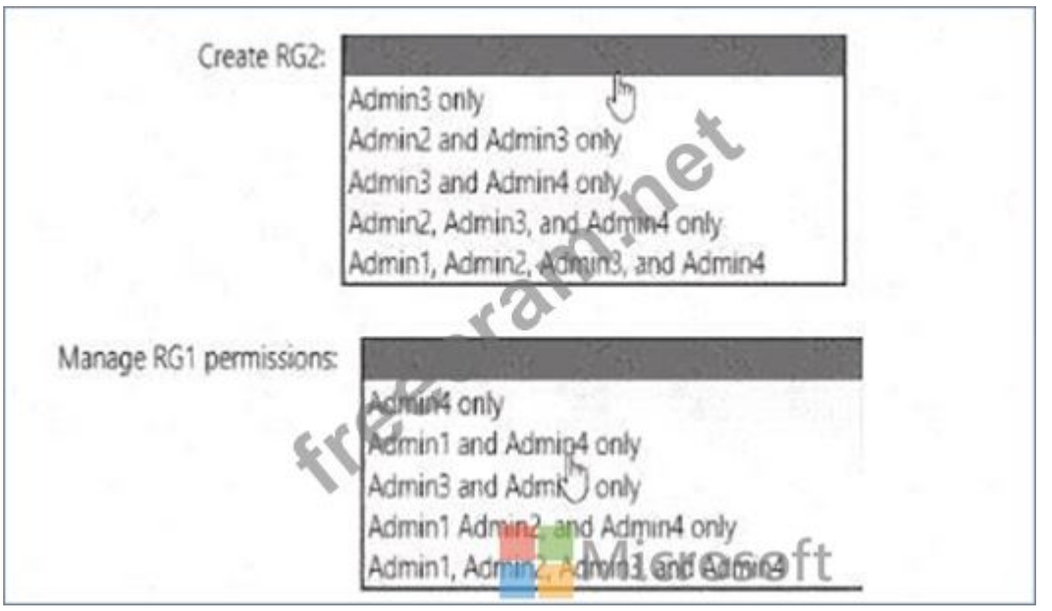
Microsoft.AZ-500.v2026-02-11.q215

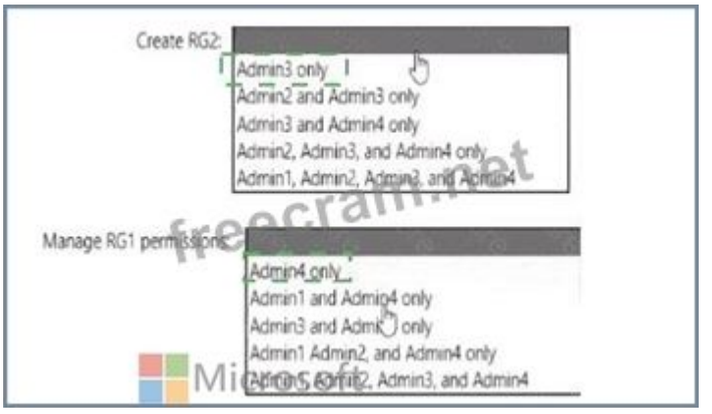
Exam Code:	AZ-500
Exam Name:	Microsoft Azure Security Technologies
Certification Provider:	Microsoft
Free Question Number:	215
Version:	v2026-02-11
# of views:	118
# of Questions views:	2848
https://www.freecram.net/torrent/Microsoft.AZ-500.v2026-02-11.q215.html	

NEW QUESTION: 1
You have an Azure subscription that uses Microsoft Defender for Cloud.
You have an Amazon Web Services (AWS) account.
You need to add the AWS account to Defender for Cloud.
What should you do first?
A. From the Azure portal, add the AWS enterprise application.
B. From Defender for Cloud, configure the Environment settings.
C. From Defender for Cloud, configure the Security solutions settings.
D. From the AWS account, enable a security hub.
Answer: (SHOW ANSWER)

NEW QUESTION: 2
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

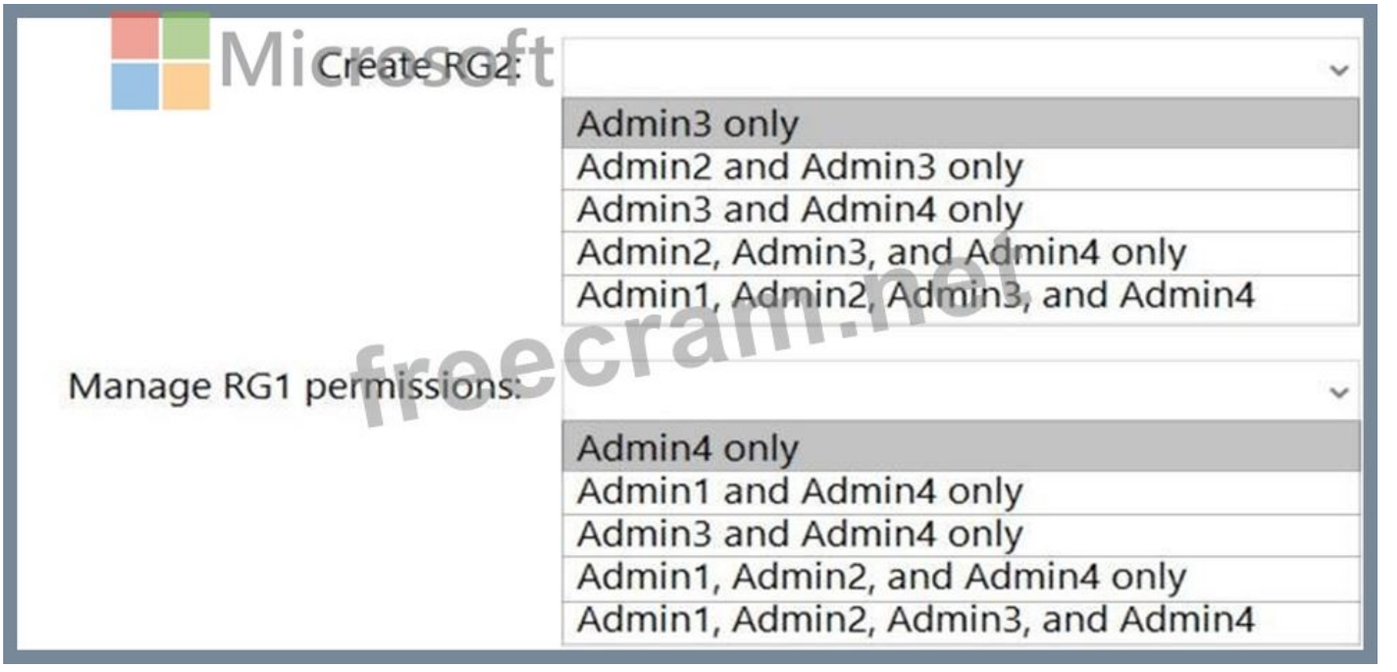


Answer:



Explanation:

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



Box 1: Admin3 only

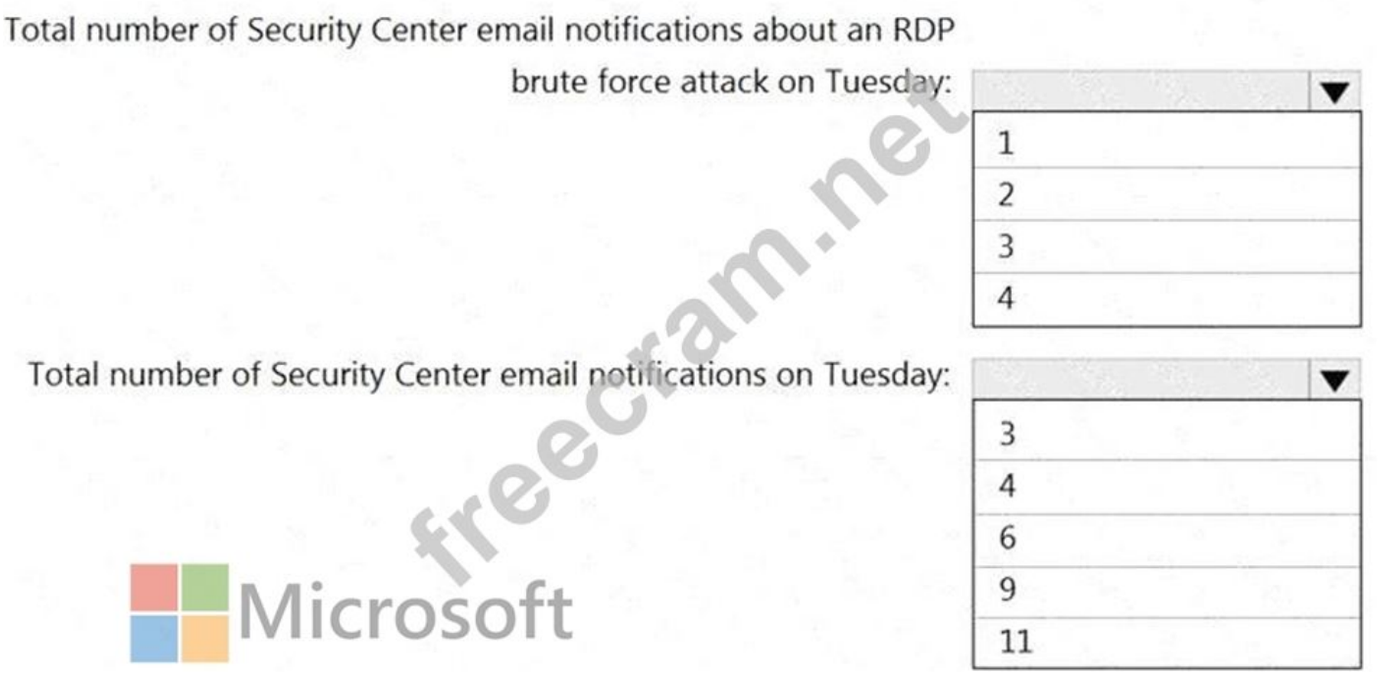
The Contributor role has the necessary write permissions to create the resource group.
Box 2: Admin4 only
You need Owner level access to be able to manage permissions. The Contributor role can do most things but cannot modify permissions on existing objects.

NEW QUESTION: 3
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. NAT gateway integration
D. regional virtual network integration
E. Azure Front Door
Answer: (SHOW ANSWER)

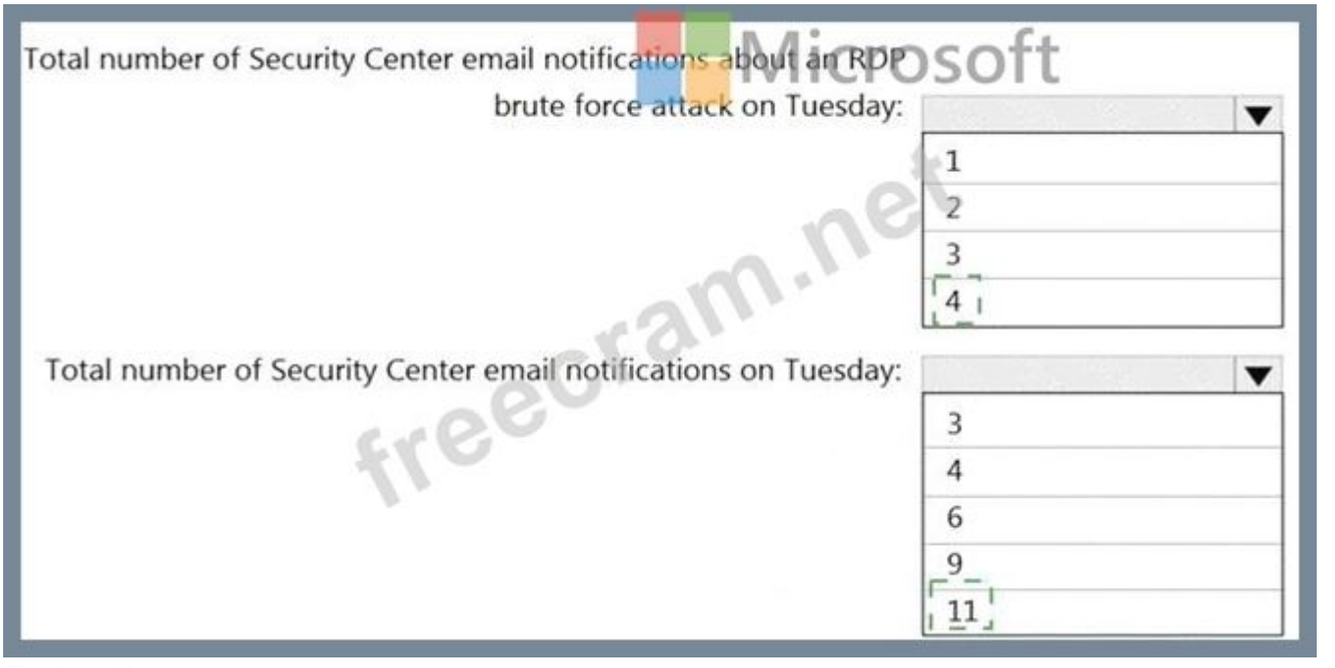
NEW QUESTION: 4
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
You are assigned the Global administrator role for the tenant. You are responsible for managing Azure Security Center settings.
You need to create a custom sensitivity 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: (SHOW ANSWER)
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: 5
On Monday, you configure an email notification in Azure Security Center to notify user user1@contoso.com.
On Tuesday, Security Center generates the security alerts shown in the following table.

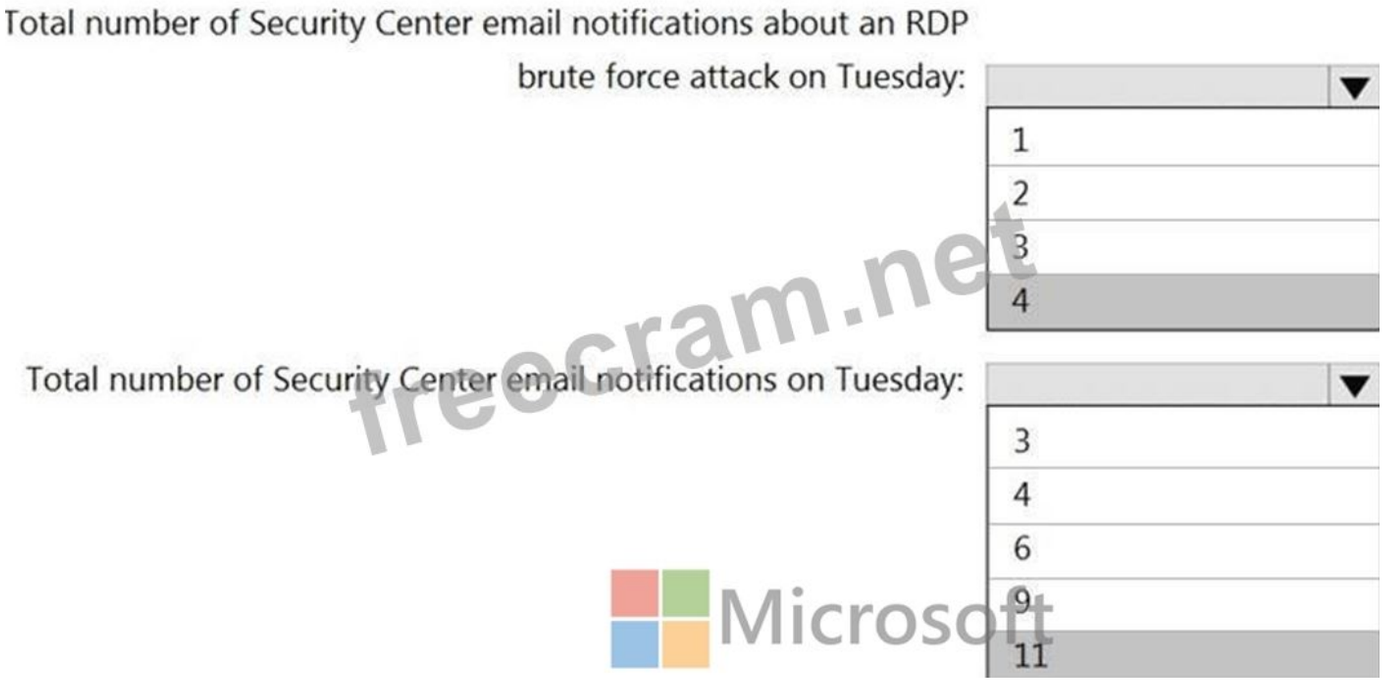
How many email notifications will user1@contoso.com receive on Tuesday? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



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

NEW QUESTION: 6
You are troubleshooting a security issue for an Azure Storage account.
You enable the diagnostic logs for the storage account.
What should you use to retrieve the diagnostics logs?
A. Azure Storage Explorer
B. SQL query editor in Azure
C. File Explorer in Windows
D. Azure Security Center
Answer: (SHOW ANSWER)
If you want to download the metrics for long-term storage or to analyze them locally, you must use a tool or write some code to read the tables. You must download the minute metrics for analysis. The tables do not appear if you list all the tables in your storage account, but you can access them directly by name. Many storage-browsing tools are aware of these tables and enable you to view them directly (see Azure Storage Client Tools for a list of available tools).
Microsoft provides several graphical user interface (GUI) tools for working with the data in your Azure Storage account. All of the tools outlined in the following table are free.

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

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

NEW QUESTION: 7
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: (SHOW ANSWER)
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: 8
You have an Azure subscription that contains a managed identity named Identity1 and the Azure key vaults shown in the following table.

Name	Permission model
KeyVault1	Vault access policy
KeyVault2	Azure role-based access control (Azure RBAC)

Key Vault1 contains an access policy that grants Identity1 the following key permissions:
* Get
* List
* Wrap
* Unwrap
You need to provide Identity1 with the same permissions for KeyVault2. The solution must use the principle of least privilege.
Which role should you assign to Identity1?
A. Key Vault Crypto Officer
B. Key Vault Crypto Service Encryption User
C. Key Vault Reader
D. Key Vault Crypto User
Answer: (SHOW ANSWER)

NEW QUESTION: 9
You have an Azure subscription.
You configure Microsoft Sentinel to use multiple data sources.
You need to create analytic rules that meet the following requirements:
* Rule 1: Automatically match Common Event Format (CEF) logs and syslog data with domain, IP address, and URL indicators.
* Rule 2: Use Microsoft proprietary algorithms.
Which type of detection should you use for each rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION: 10

You have an Azure Active Directory (Azure AD) tenant.
You have the deleted objects shown in the following table.
On May 4, 2020, you attempt to restore the deleted objects by using the Azure Active Directory admin center.
Which two objects can you restore? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Group1

B. Group2

C. User2

D. User1

Answer: (SHOW ANSWER)

Deleted users and deleted Office 365 groups are available for restore for 30 days.
You cannot restore a deleted security group.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-restore-deleted

NEW QUESTION: 11

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

Name	Type
Policy1	Standard
Policy2	Premium

The subscription contains the firewalls shown in the following table.

Name	Tier	Policy
FW1	Premium	Policy2
FW2	Premium	Policy1

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

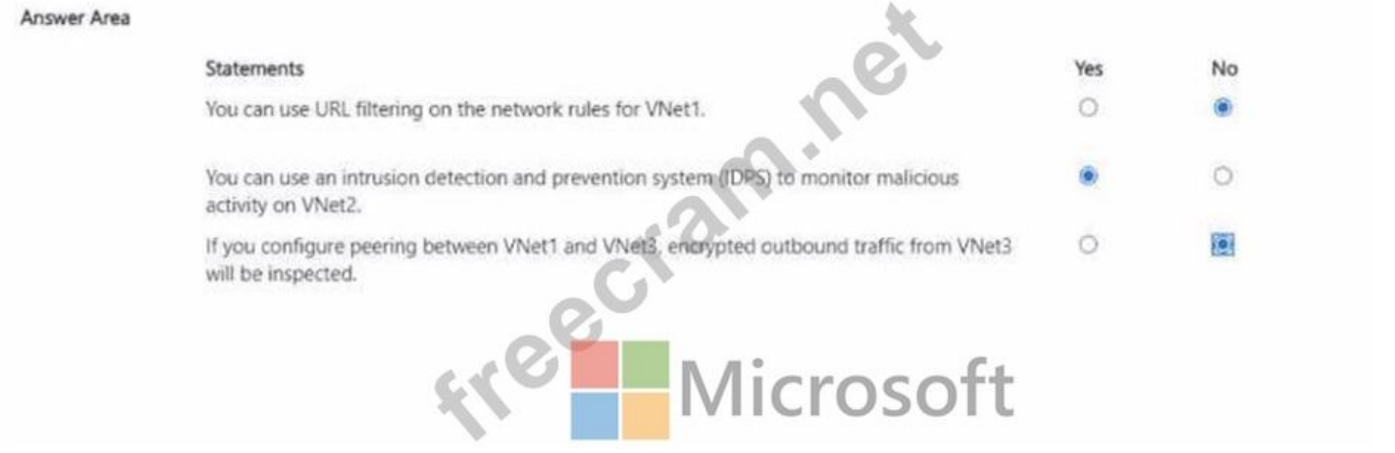
Name	Firewall
VNet1	FW1
VNet2	FW2
VNet3	None

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:

Explanation:



NEW QUESTION: 12

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:

* 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: 13

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

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

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

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

You assign Role1 to User1 on RG1.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can add VM1 to VNET1.	○	○
User1 can start and stop App1.	○	○
User1 can start and stop cont1.	○	○

Answer:

Statements	Yes	No
User1 can add VM1 to VNET1.	○	○
User1 can start and stop App1.	○	○
User1 can start and stop cont1.	○	○

Explanation:

Text Description automatically generated

Statements	Yes	No
User1 can add VM1 to VNET1.	○	○
User1 can start and stop App1.	○	○
User1 can start and stop cont1.	○	○

Reference:

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

NEW QUESTION: 14

You have an Azure Container Registry named Registry1.

You add role assignment for Registry1 as shown in the following table.

User	Role
User1	AcrPush
User2	AcrPull
User3	AcrImageSigner
User4	Contributor

Which users can upload images to Registry1 and download images from Registry1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Upload images:

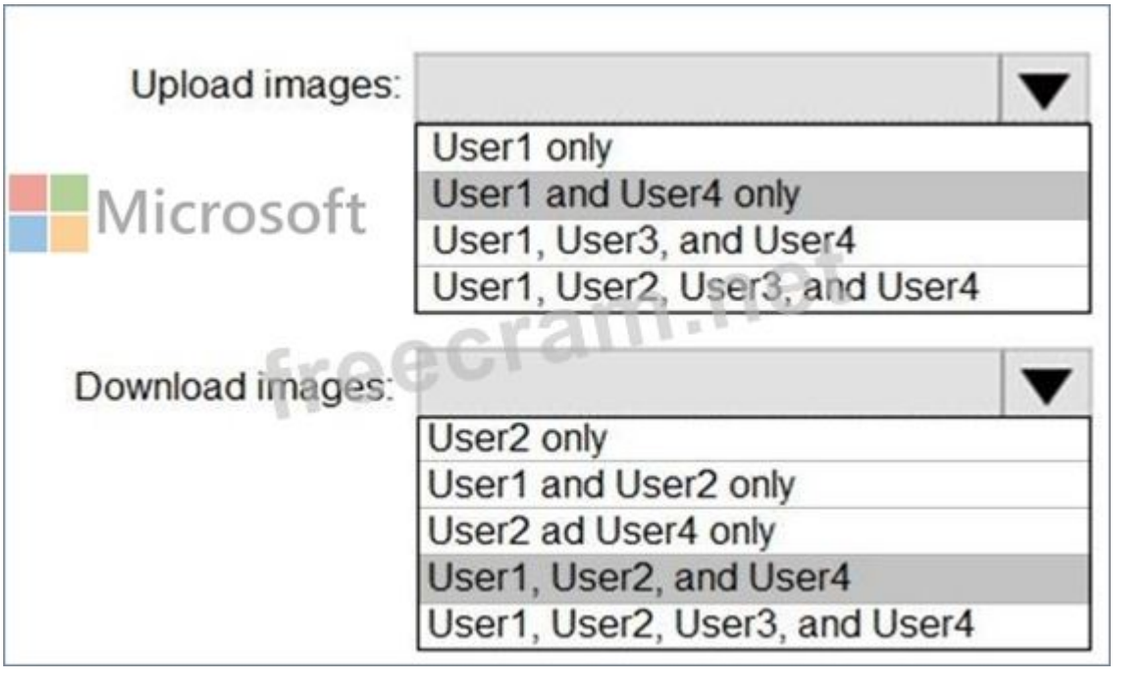
- User1 only
- User1 and User4 only
- User1, User3, and User4
- User1, User2, User3, and User4

Download images:

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

Answer:

Explanation:



Box 1: User1 and User4 only

Owner, Contributor and AcrPush can push images.

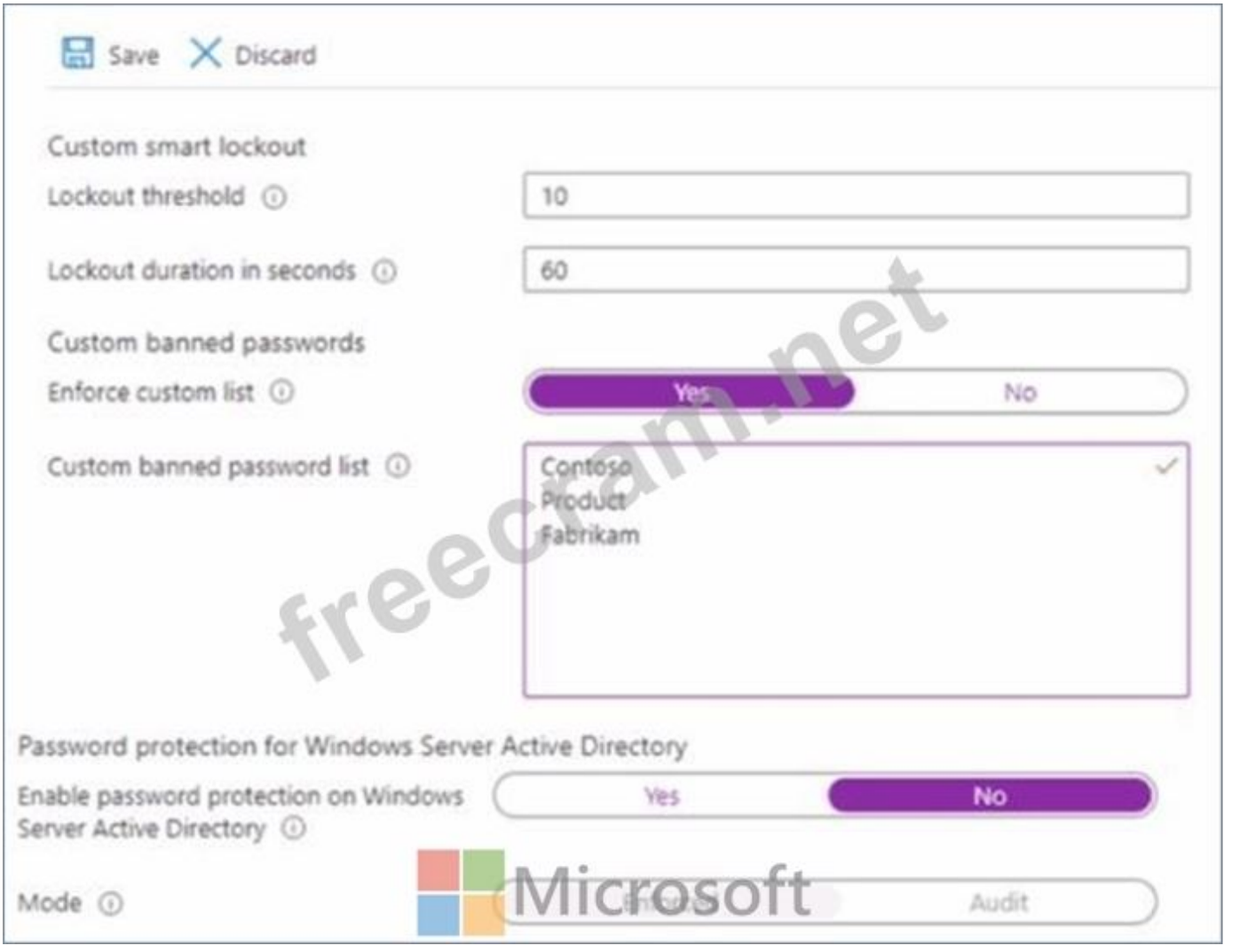
Box 2: User1, User2, and User4

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: 15
You have a Microsoft Entra tenant that contains three users named User1, User2, and User3.
You configure Microsoft Entra Password Protection as shown in the following exhibit.



The users perform the following tasks:
* User1 attempts to reset her password to COntOsO

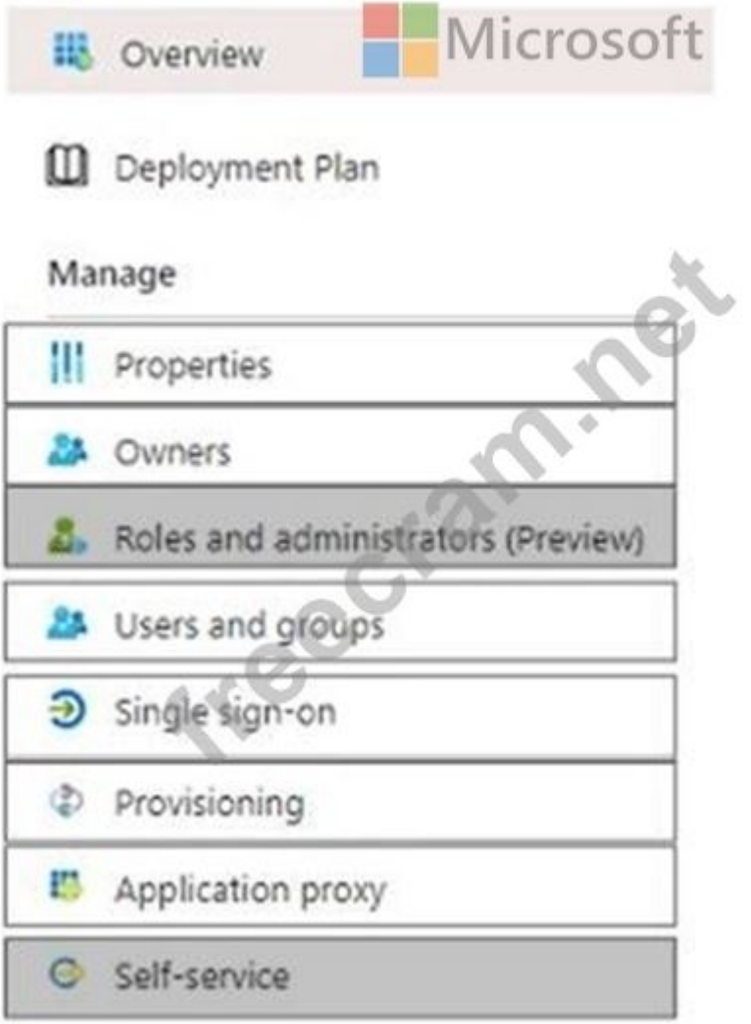
* User2 attempts to reset her password to F@brikamHQ
* User3 attempts to reset her password to PrOduct123.
Which password reset attempts fail?
A. User1, User2, and User3
B. User1 and User3 only
C. User3 only
D. User1 only
E. User2only
Answer: A (LEAVE A REPLY)

NEW QUESTION: 16
You have an Azure Active Directory (Azure AD) tenant that contains two users named User1 and User2 and a registered app named App1.
You create an app-specific role named Role1.
You need to assign Role1 to User1 and enable User2 to request access to App1.
Which two settings should you modify? To answer select the appropriate settings in the answer area NOTE: Each correct selection is worth one pant.

Answer:

Explanation:

Graphical user interface, application Description automatically generated



NEW QUESTION: 17

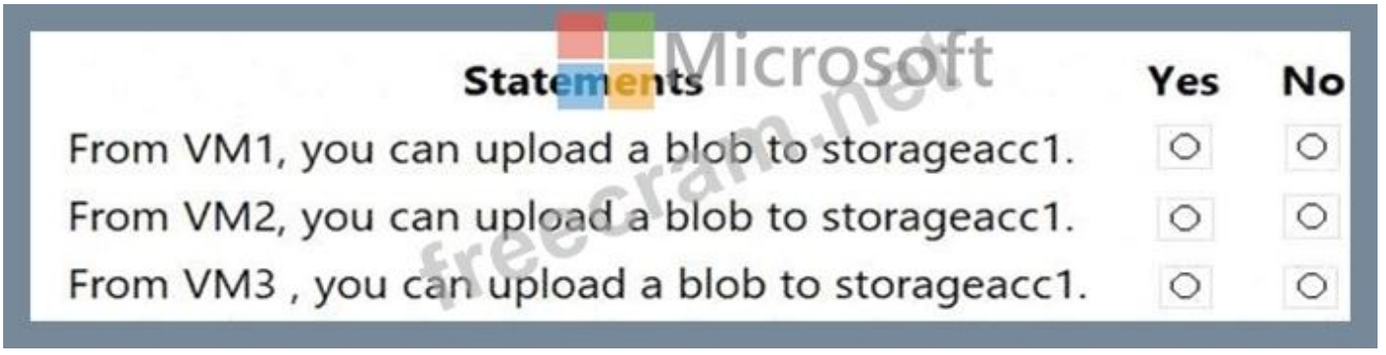
You have an Azure subscription that contains the virtual machines shown in the following table.

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.

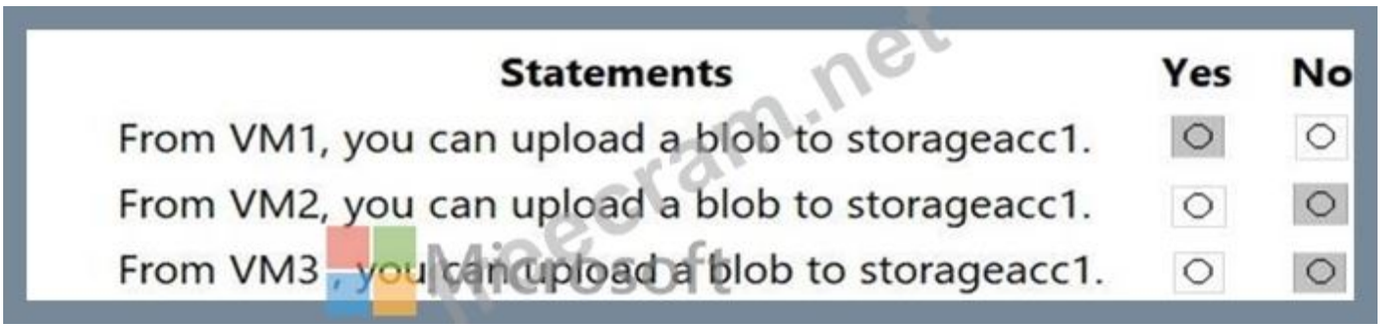
You have an Azure Storage account named storageacc1 that is configured as shown in the following exhibit.

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



Answer:

Explanation:

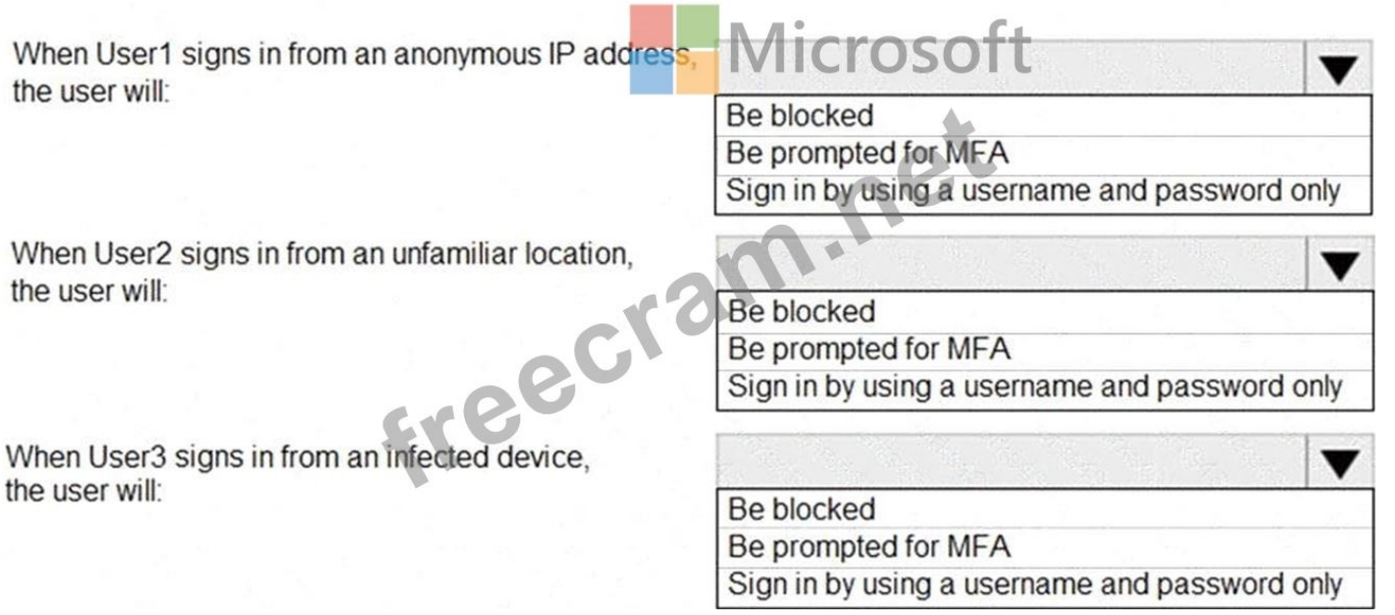


Box 1: Yes
The public IP of VM1 is allowed through the firewall.
Box 2: No
The allowed virtual network list is empty so VM2 cannot access storageacc1 directly. The public IP address of VM2 is not in the allowed IP list so VM2 cannot access storageacc1 over the Internet.
Box 3: No
The allowed virtual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

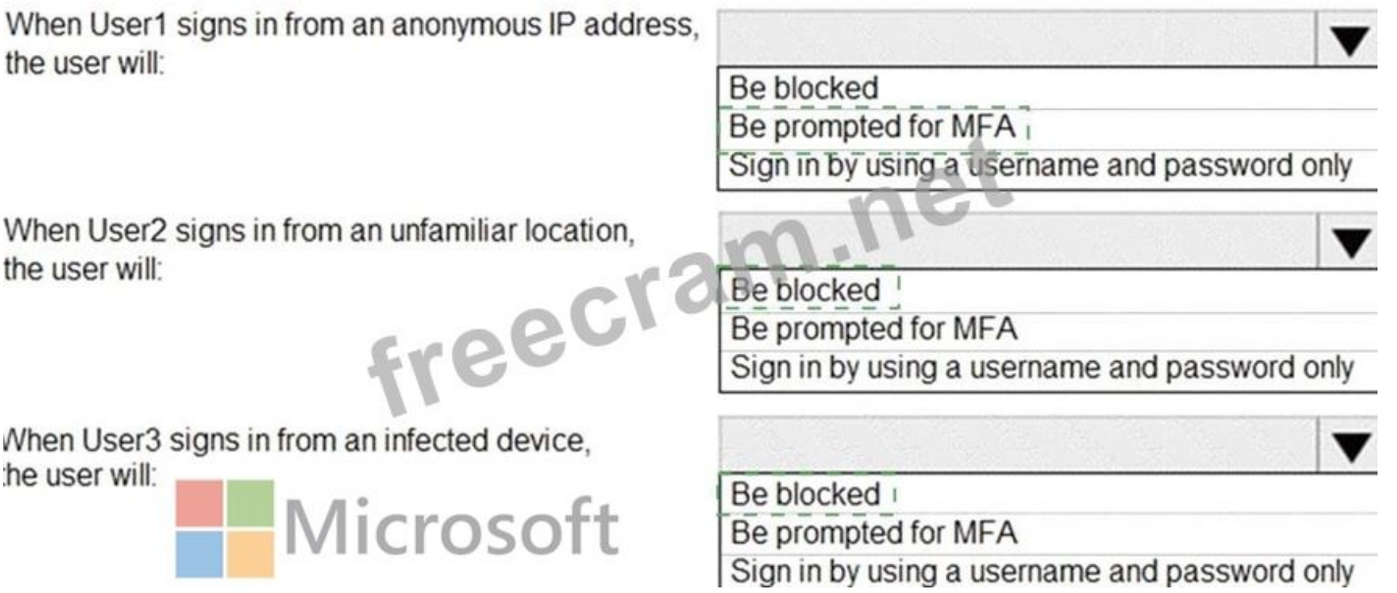
NEW QUESTION: 18
You have an on-premises network and an Azure subscription.
You have the Microsoft SQL Server instances shown in the following table.
You plan to implement Microsoft Defender for SQL.
Which SQL Server instances will be protected by Microsoft Defender for SQL?
A. sql1, sql2, andsql3 only
B. sql1 and sql2 only
C. sql1, sql2, sql3, and sql4
D. sql1 sql2 and so.14 only
Answer: (SHOW ANSWER)

NEW QUESTION: 19
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.
You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:
* Assignments: Include Group1, exclude Group2
* Conditions: Sign-in risk level: Medium and above
* Access Allow access, Require multi-factor authentication
You need to identify what occurs when the users sign in to Azure AD.
What should you identify for each user? To answer, select the appropriate options in the answer area.

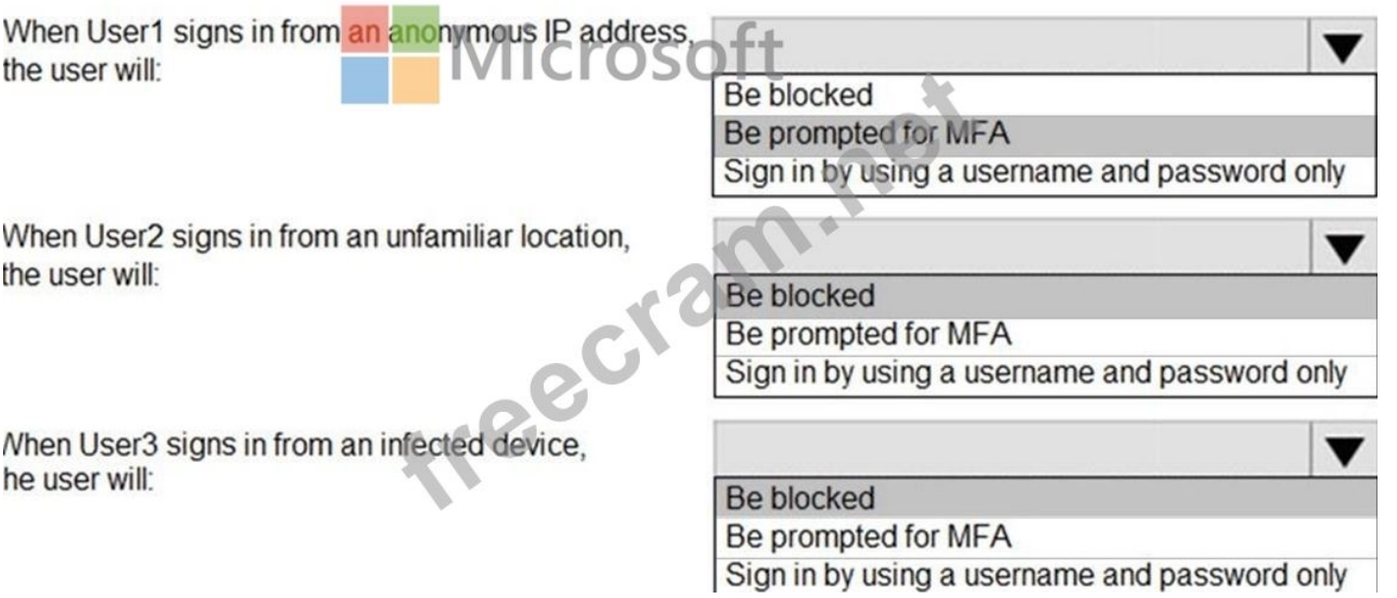
NOTE: Each correct selection is worth one point.



Answer:

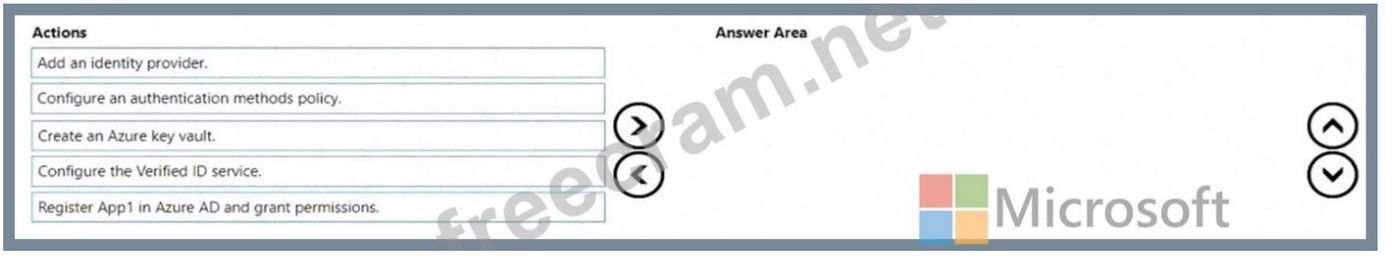


Explanation:

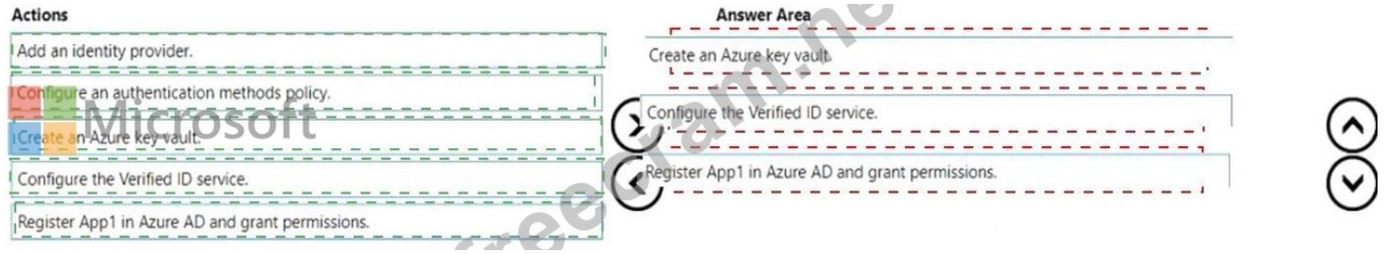


References:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection- policies
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

NEW QUESTION: 20
You have an Azure AD Tenant and an application named App1.
You need to ensure that App1 can use Microsoft Entra Verified ID to verify credentials.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:
https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/verifiable-credentials-configure- tenant

NEW QUESTION: 21
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: 22
You have an Azure subscription that contains the virtual machines shown in the following table.

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

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

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

On which virtual machines is the Microsoft Monitoring agent installed?
A. VM3 only
B. VM1 and VM3 only
C. VM3 and VM4 only
D. VM1, VM2, VM3, and VM4
Answer: (SHOW ANSWER)
When automatic provisioning is enabled, Security Center provisions the Microsoft Monitoring Agent on all supported Azure VMs and any new ones that are created.
Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803.
References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-faq

NEW QUESTION: 23

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:

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

Explanation:

Answer Area

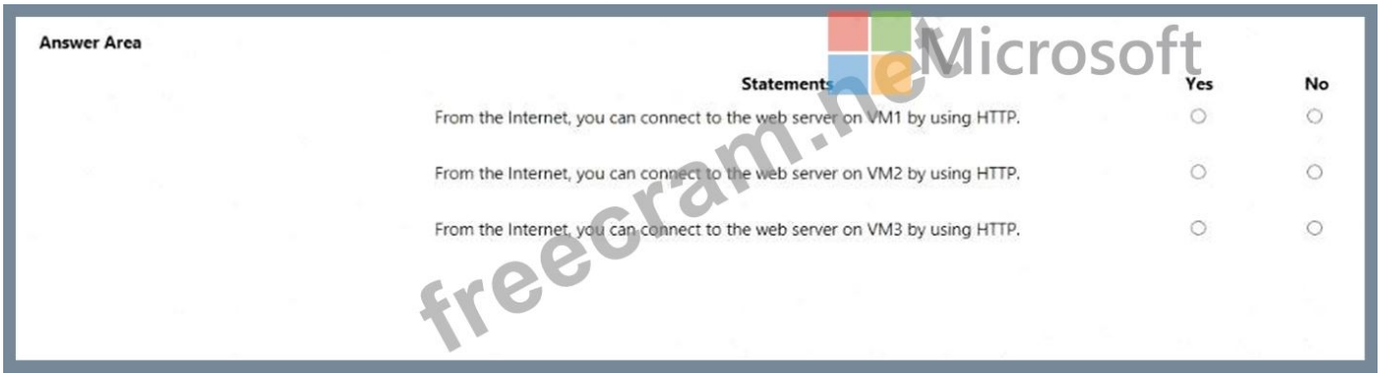
Statements	Yes	No
WebApp1 can connect to VM2.	◉	○
NSG1 controls inbound traffic to WebApp1.	○	◉
WebApp2 can connect to VM1.	○	◉

NEW QUESTION: 24
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:
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: 25
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 Microsoft SQL Server Management Studio (SSMS), create a Transact-SQL query.
B. From Azure CLI run the Get-AzOperationalInsightsworkspace cmdlet.
C. From the Azure Sentinel workspace, create a Kusto Query Language query.
D. From the Azure SQL Database query editor, create a Transact-SQL query.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 26
You are evaluating the security of VM1, VM2, and VM3 in Sub2.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

NEW QUESTION: 27

You have an Azure subscription.

You plan to deploy an Azure SQL managed instance named AzSQL1.

You need to recommend an encryption solution for AzSQL1.

The solution must meet the following requirements:

* The database engine must be prevented from performing key provisioning, data encryption, and decryption operations.

* Database administrators must be prevented from viewing the encrypted data in plain text.

What should you include in the recommendation?

A. Always Encrypted

B. Transparent Data Encryption (TDE) with Microsoft-managed keys

C. TLS

D. Azure Disk Encryption

E. Transparent Data Encryption (TDE) with customer-managed keys

Answer: (SHOW ANSWER)

NEW QUESTION: 28

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. Modify the Access policies settings of Vault1.

B. Create a key rotation policy.

C. Upgrade Vault1 to Key Vault Premium.

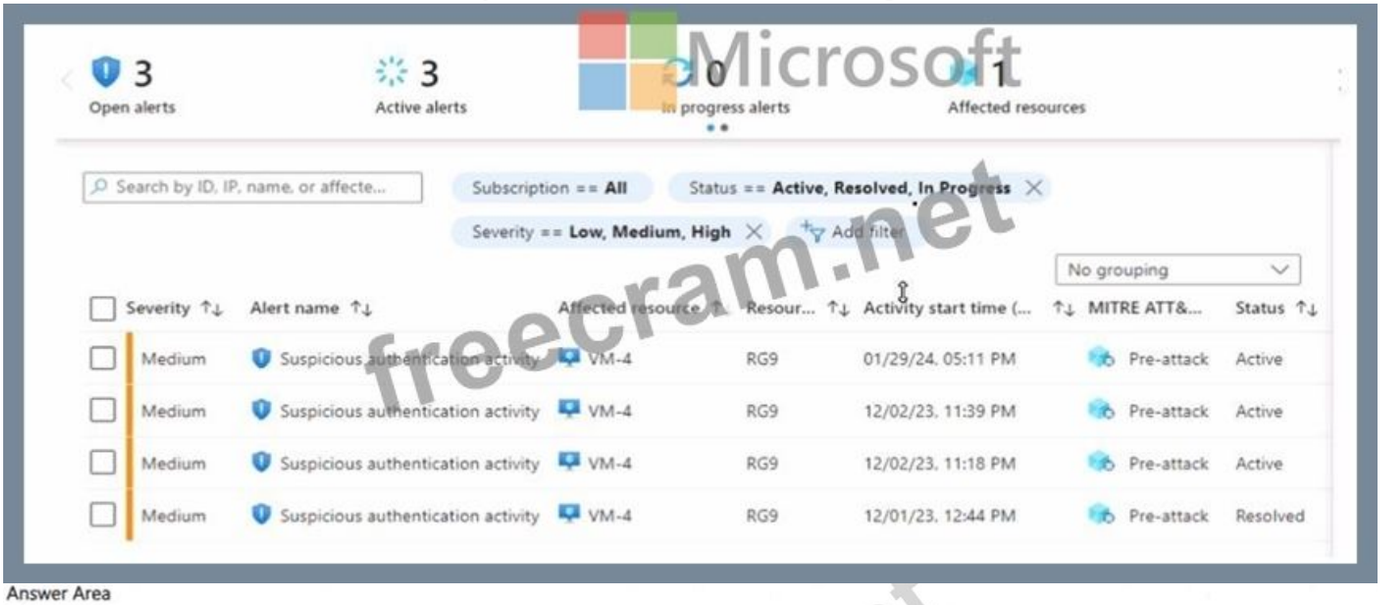
D. Recreate key1 as an EC key.

Answer: (SHOW ANSWER)

NEW QUESTION: 29

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

Defender for Cloud has the security alerts shown in the following exhibit.



Answer Area

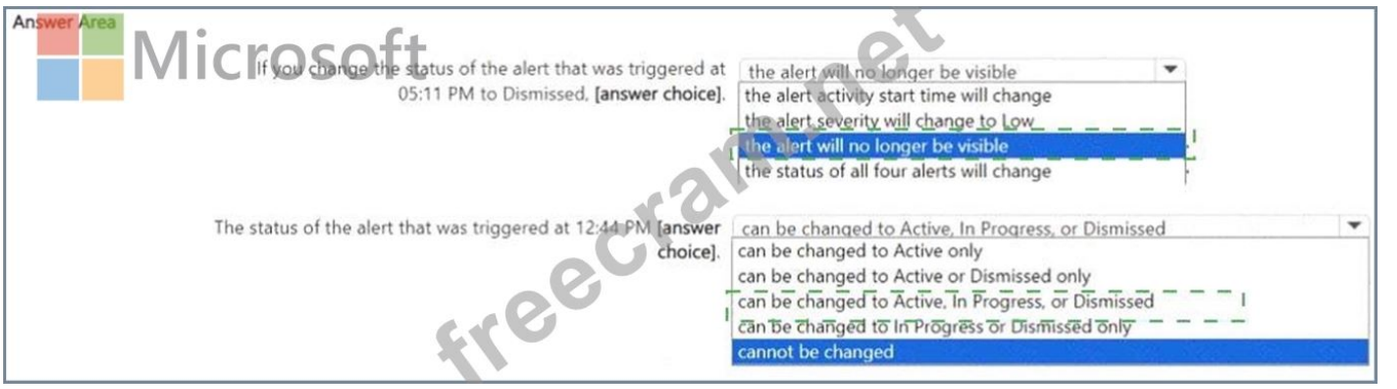
If you change the status of the alert that was triggered at 05:11 PM to Dismissed, [answer choice].

- the alert will no longer be visible
- the alert activity start time will change
- the alert severity will change to Low
- the alert will no longer be visible
- the status of all four alerts will change

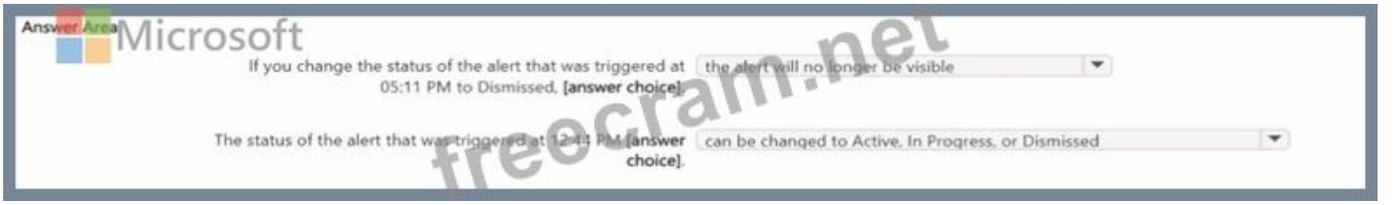
The status of the alert that was triggered at 12:44 PM [answer choice].

- can be changed to Active, In Progress, or Dismissed
- can be changed to Active only
- can be changed to Active or Dismissed only
- can be changed to Active, In Progress, or Dismissed
- can be changed to In Progress or Dismissed only
- cannot be changed

Answer:

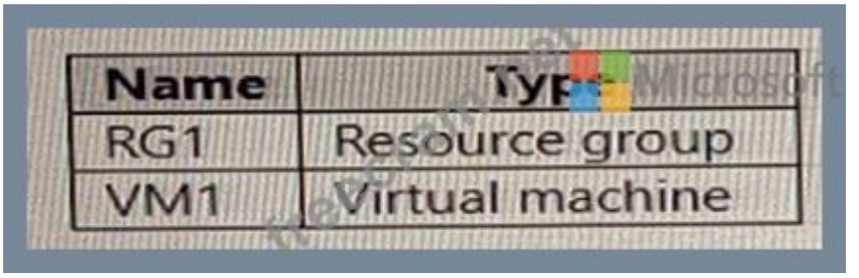


Explanation:



NEW QUESTION: 30

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



Name	Type
RG1	Resource group
VM1	Virtual machine

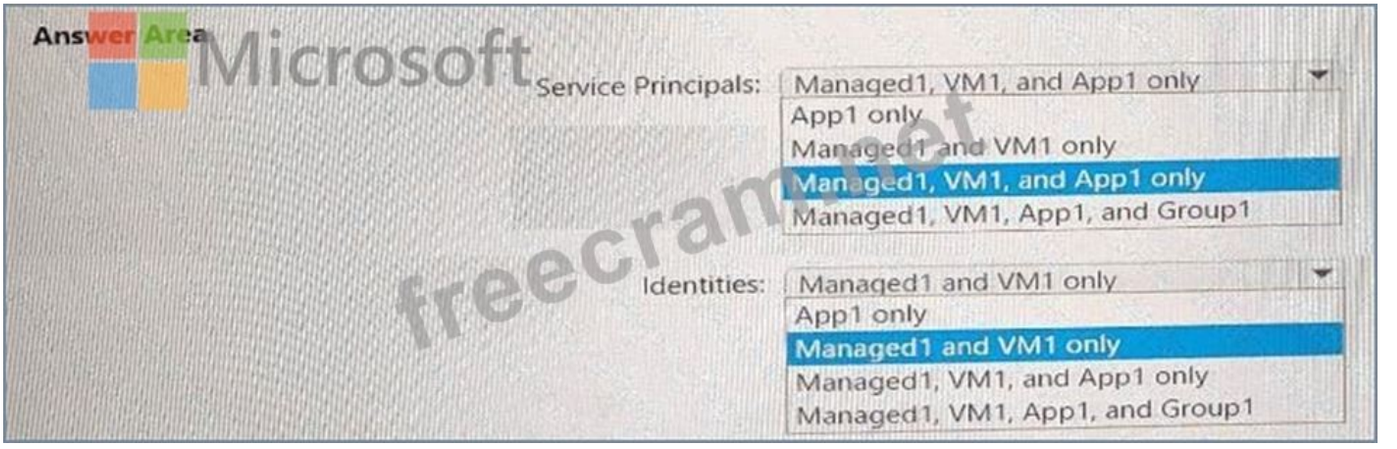
You perform the following tasks:

Create a managed identity named Managed1.

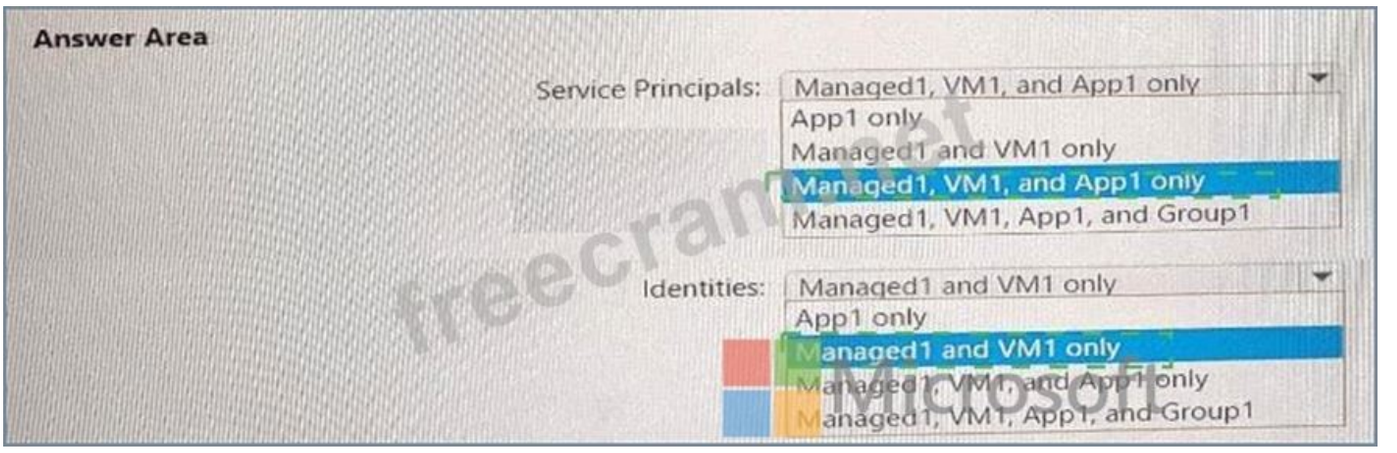
Create a Microsoft 365 group named Group1.

You need to identify which service principals were created and which identities can be assigned the Reader role for RG1.

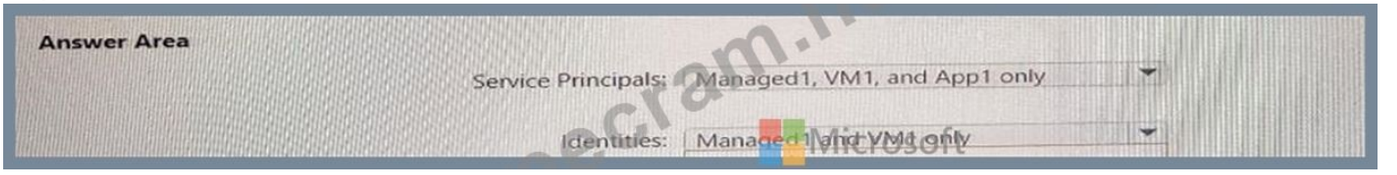
What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 31

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

User1	User	*Not applicable*
Group1	Microsoft 365 group	Yes
Group2	Security group	No
Group3	Security group	Yes
Group4	Security group	Yes

You assign Group4 the Contributor role for RG1.

Which identities can you add to Group4 as members?

A. User1, Group1, Group2, and Group3

B. User1, Group2, and Group3 only

C. User1, Group1, and Group3 only

D. User1 and Group3 only

E. User1 only

Answer: (SHOW ANSWER)

NEW QUESTION: 32
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: (SHOW ANSWER)
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: 33
You have an Azure subscription. That contains the virtual machines shown in the following table.
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. Computed and Computed only
C. Computer 1 and Computer2 only
D. Computed only
Answer: (SHOW ANSWER)

NEW QUESTION: 34
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: 35

You have an app that uses an Azure SQL database.
You need to be notified if a SQL injection attack is launched against the database.
What should you do?

A. Modify the Diagnostics settings for the database.

B. Deploy the SQL Health Check solution in Azure Monitor.

C. Enable server-level auditing for the database.

D. Enable Azure Defender for SQL for the database.

Answer: (SHOW ANSWER)

NEW QUESTION: 36

You have an Azure subscription.
You plan to create two custom roles named Role1 and Role2.
The custom roles will be used to perform the following tasks:
* Members of Role1 will manage application security groups.
* Members of Role2 will manage Azure Bastion.
You need to add permissions to the custom roles.
Which resource provider should you use for each role? To answer, drag the appropriate resource providers to the correct roles. Each resource provider 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

Answer:

Explanation:

NEW QUESTION: 37
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. For App1, enable virtual network integration.
B. For VNet1, configure network security group (NSG) rules.
C. Configure Microsoft Entra application proxy.
D. For App1, configure the HTTP headers filter settings.
Answer: (SHOW ANSWER)

NEW QUESTION: 38
You have a Azure subscription that contains an Azure Container Registry named Registry1. The subscription uses the Standard use tier of Azure Security Center.
You upload several container images to Register1.
You discover that vulnerability security scans were not performed
You need to ensured that the images are scanned for vulnerabilities when they are uploaded to Registry1.
What should you do?
A. From the Azure portal modify the Pricing tier settings.
B. From Azure CLI, lock the container images.
C. Upload the container images by using AzCopy
D. Push the container images to Registry1 by using Docker
Answer: (SHOW ANSWER)
Reference:
https://charbelnemnom.com/scan-container-images-in-azure-container-registry-with-azure-security-center/

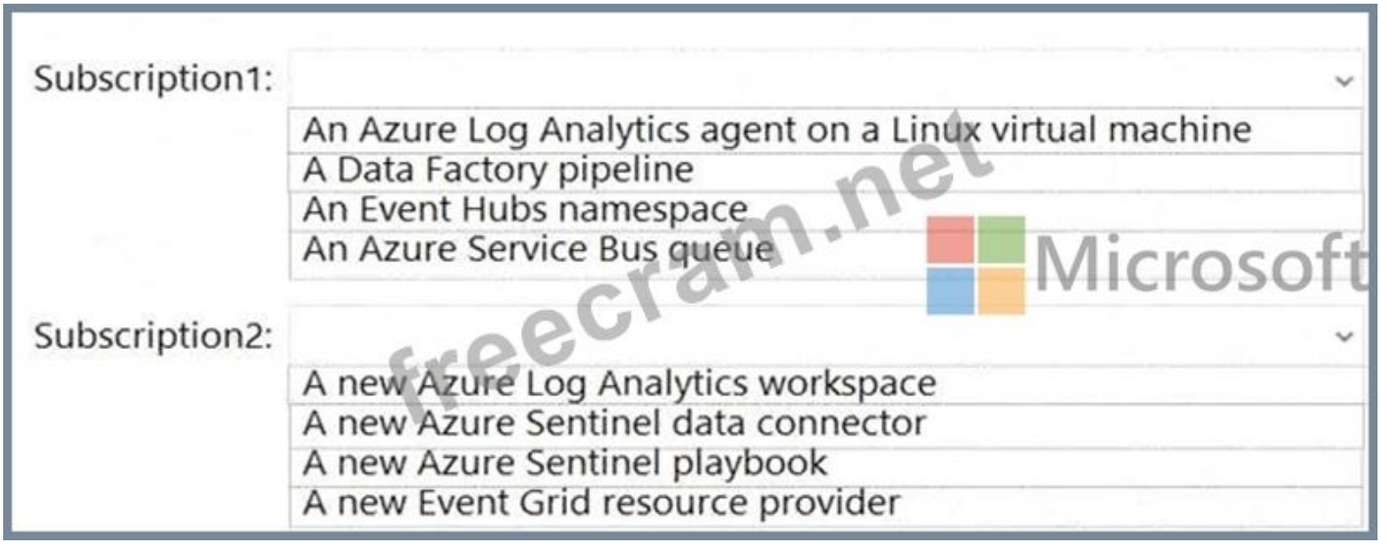
NEW QUESTION: 39
You have an Azure subscription that uses Microsoft Defender.
You enable the CIS Microsoft Azure Foundations Benchmark v2.0.0 built-in to the subscription.

You need to ensure that when users attempt to assign custom role-based access control (RBAC) roles, they receive a custom error message that includes a link to an internal website. The solution must minimize the impact on other policies.
What should you configure?
A. the effect of the policy
B. the default non-compliance message of the built-in
C. the remediation task of the policy
D. a policy-specific non-compliance message
Answer: (SHOW ANSWER)

NEW QUESTION: 40
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).

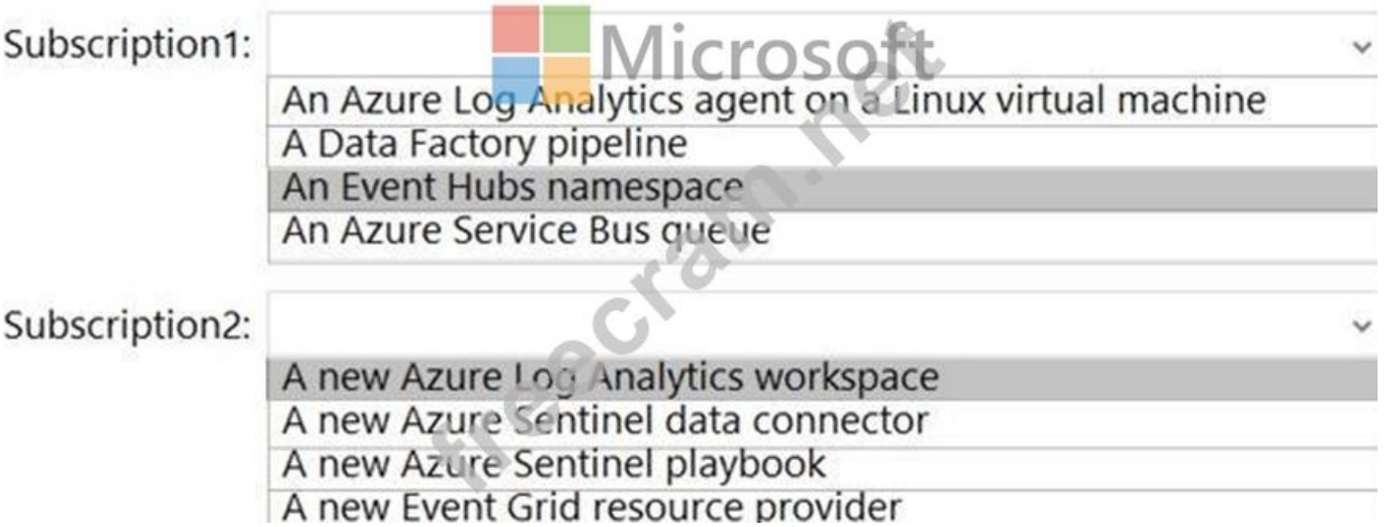
You have an Azure subscription named Subscription2 that contains the following resources:
* An Azure Sentinel workspace
* An Azure Event Grid instance
You need to ingest the CEF messages from the NVAs to Azure Sentinel.
What should you configure for each subscription? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

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



NEW QUESTION: 41

You have an Azure SQL database named DB1 that contains a table named Table.

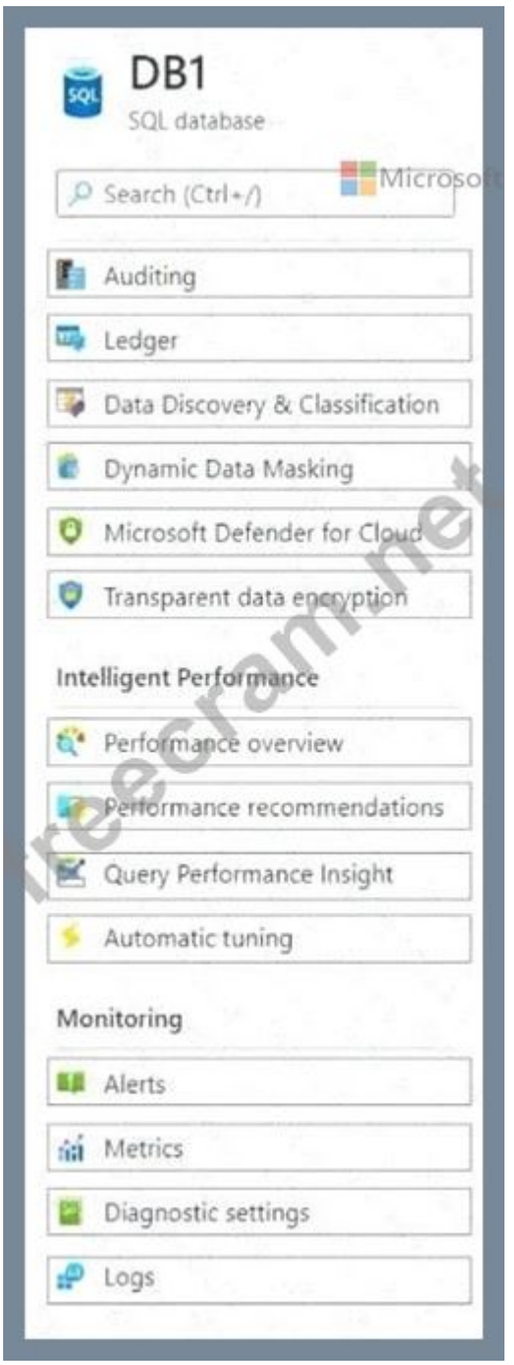
You need to configure DB1 to meet the following requirements;

* Sensitive data in Table1 must be identified automatically.

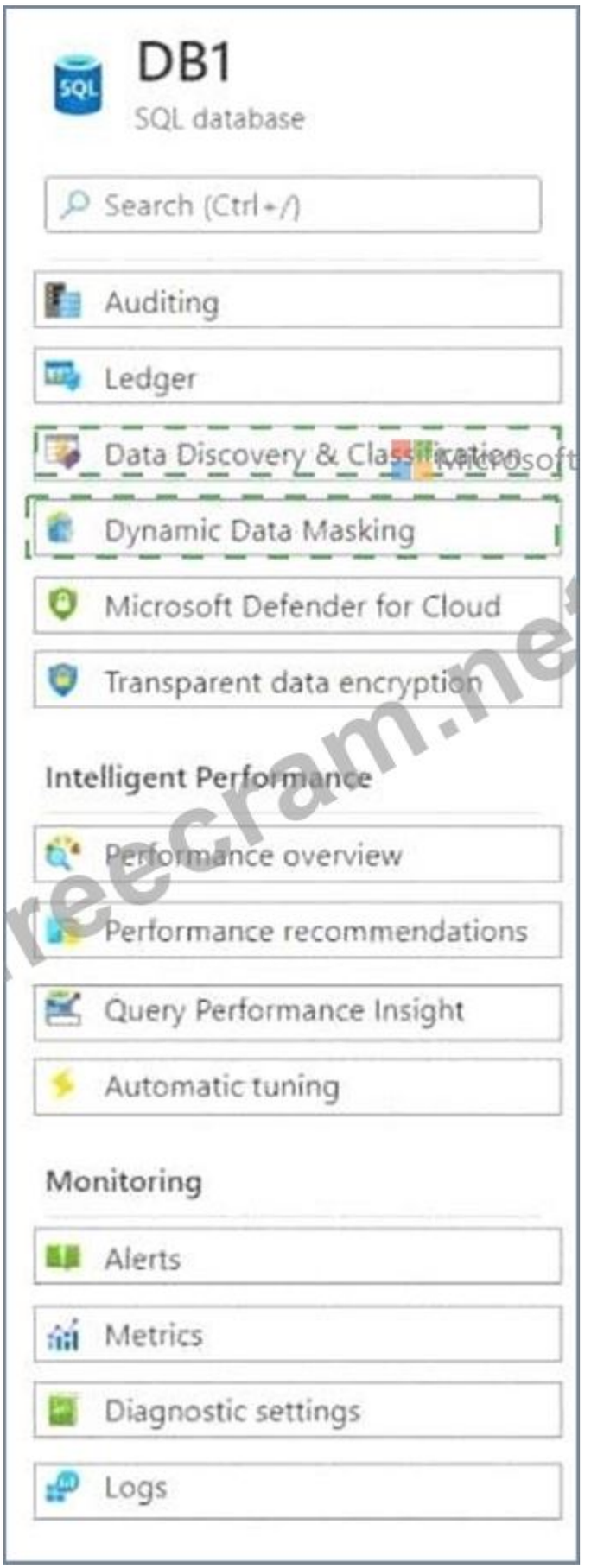
* Only the first character and last character of the sensitive data must be displayed in query results.

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

NOTE: Each correct selection is worth one point.


DB1
SQL database
Search (Ctrl+/)
Auditing
Ledger
Data Discovery & Classification
Dynamic Data Masking
Microsoft Defender for Cloud
Transparent data encryption
Intelligent Performance
Performance overview
Performance recommendations
Query Performance Insight
Automatic tuning
Monitoring
Alerts
Metrics
Diagnostic settings
Logs

Answer:



Explanation:

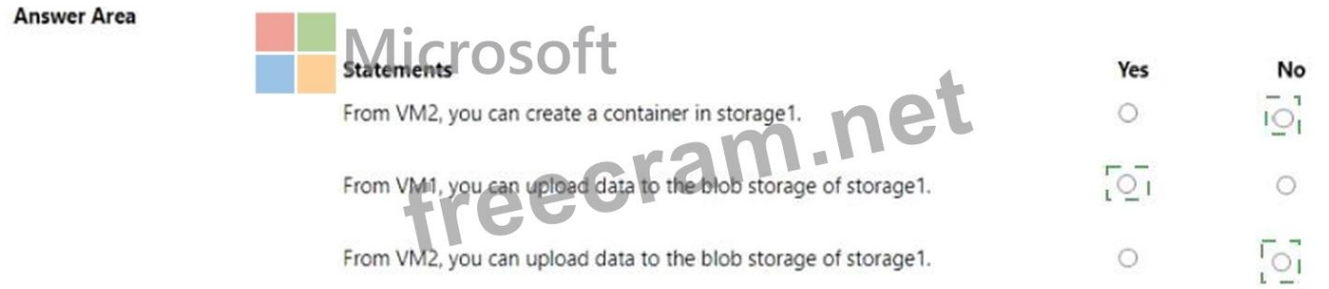
1. Data Discovery & Classification

2. Dynamic Data Masking
https://learn.microsoft.com/en-us/azure/azure-sql/database/data-discovery-and-classification-overview?
view=azuresql
Data Discovery & Classification is built into Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics. It provides basic capabilities for discovering, classifying, labeling, and reporting the sensitive data in your databases.

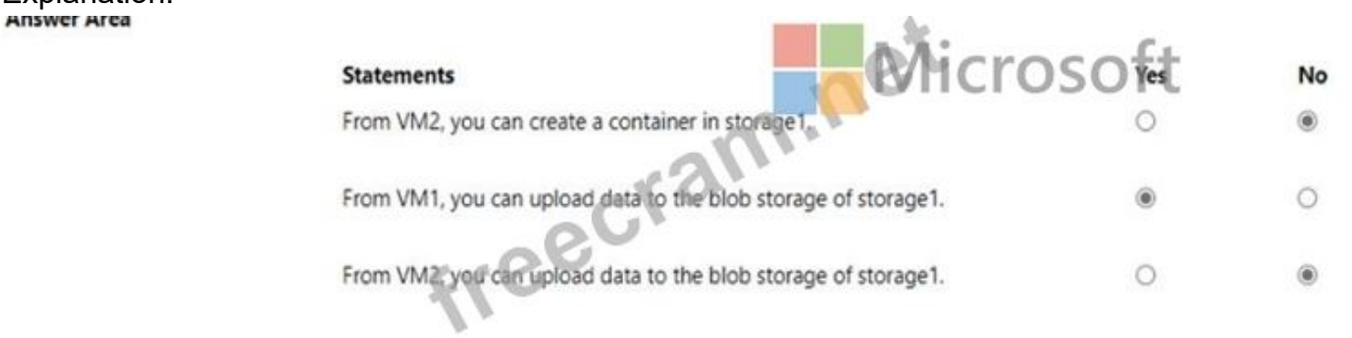
NEW QUESTION: 42
You have an Azure subscription that contains four Azure SQL managed instances.
You need to evaluate the vulnerability of the managed instances to SQL injection attacks.
What should you do first?
A. Create an Azure Sentinel workspace.
B. Add the SQL Health Check solution to Azure Monitor.
C. Create an Azure Advanced Threat Protection (ATP) instance.
D. Enable Advanced Data Security.
Answer: (SHOW ANSWER)

NEW QUESTION: 43
You have an Azure subscription that contains the virtual machines shown in the following table.
Subnet1 and Subnet2 have a network security group {NSG). The NSG has an outbound rule that has the following configurations:
* Port; Any
* Source: Any
* Priority: 100
* Action: Deny
* Protocol: Any
* Destination: Storage
The subscription contains a storage account named storage1.
You create a private endpoint named Private1 that has the following settings:
* Resource type: Microsoft.Storage/storageAccounts
* Resource: storage1
* Target sub-resource: blob
* Virtual network: VNet1
* Subnet: Subnet1
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 contains an Azure SQL database named SQL1.

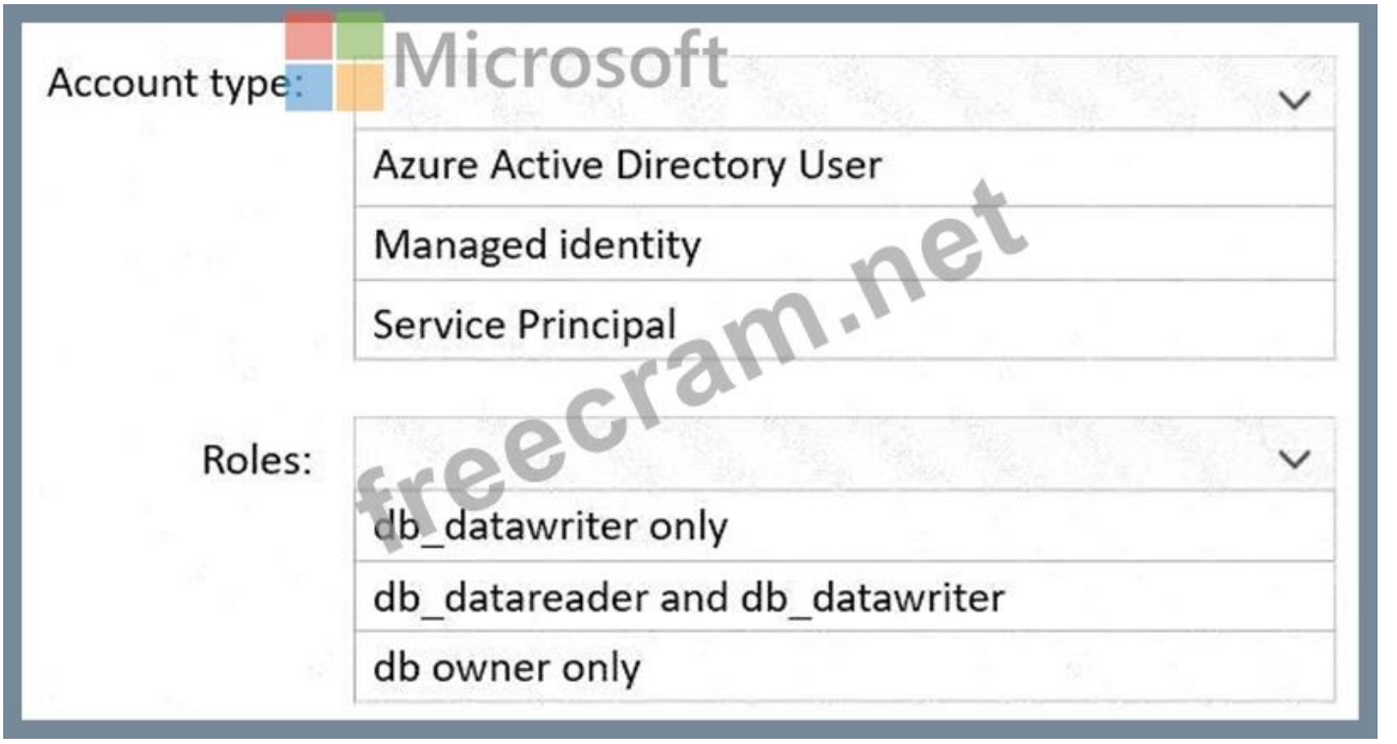
You plan to deploy a web app named App1.

You need to provide App1 with read and write access to SQL1. The solution must meet the following requirements:

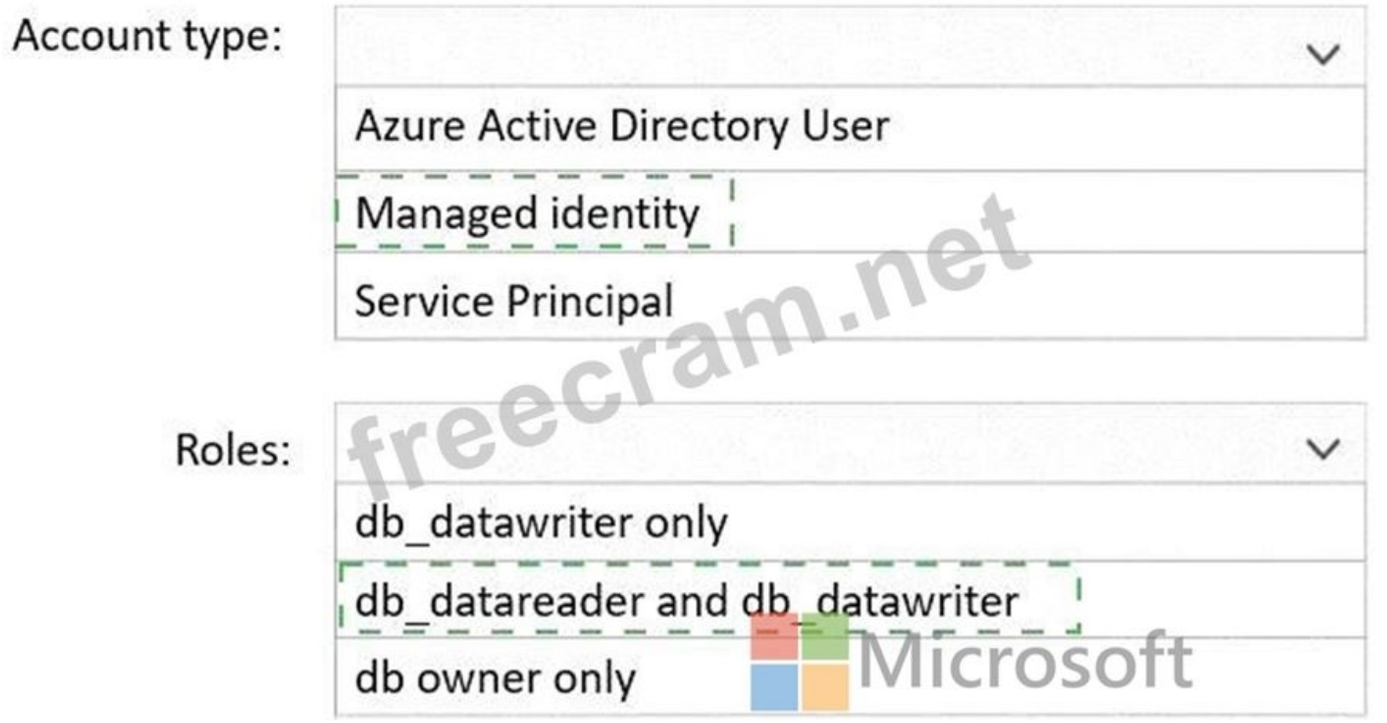
* Provide App1 with access to SQL1 without storing a password.
* Use the principle of least privilege.
* Minimize administrative effort.

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.

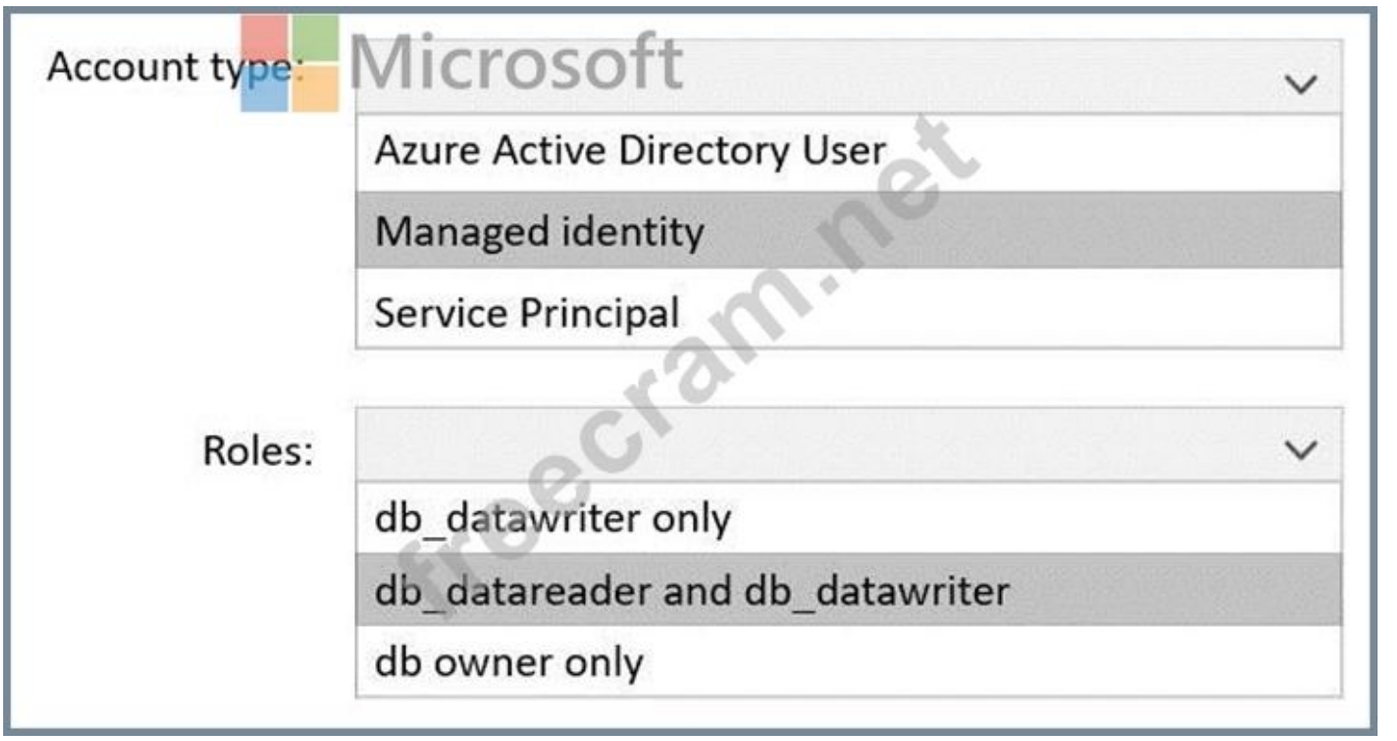


Answer:



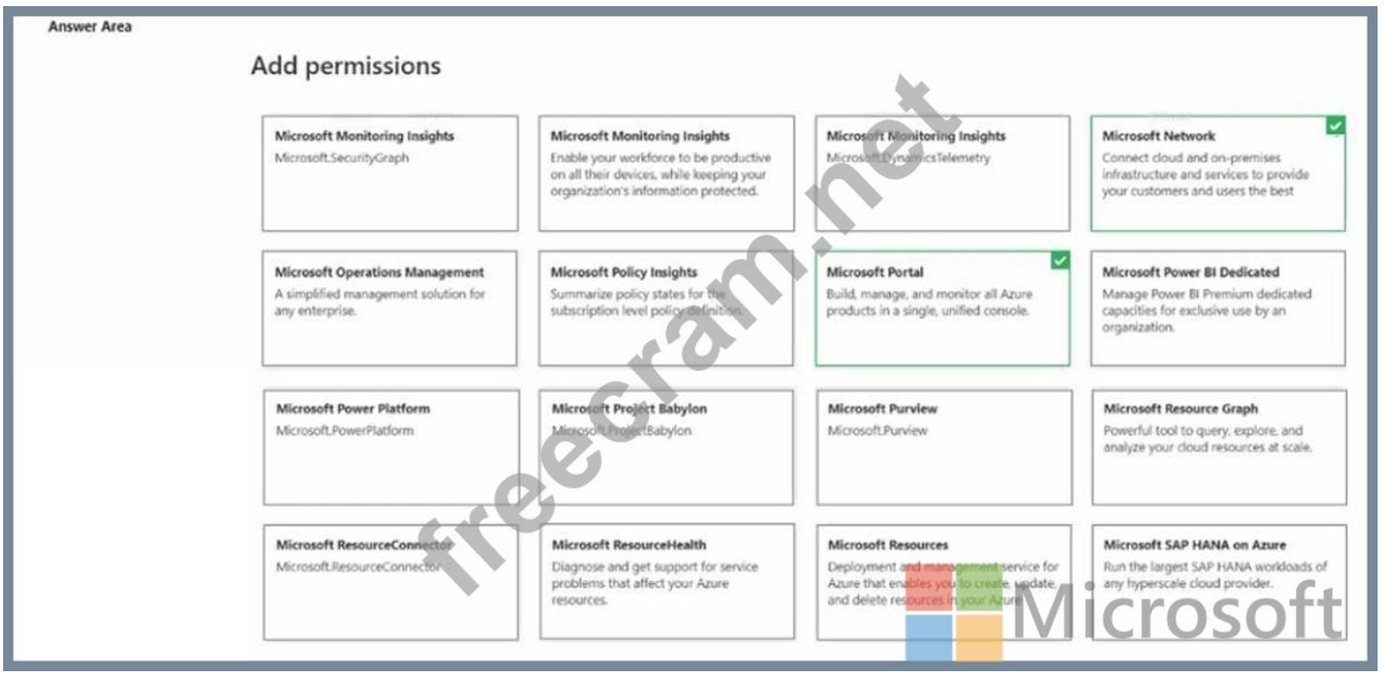
Explanation:

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: 45
You have an Azure subscription that contains a user named User1. User1 is assigned the Reader role for the subscription.
You plan to create a custom role named Role1 and assign Role1 to User1.
You need to ensure that User1 can create and manage application security groups by using the Azure portal.
Which two permissions should you add to Role1? To answer, select the appropriate permission in the answer area.
NOTE: Each correct selection is worth one point.
Answer:



1. Microsoft Portal 2. Microsoft Network https://learn.microsoft.com/en-us/azure/azure-resource-manager
/management/azure-services-resource-providers

NEW QUESTION: 46

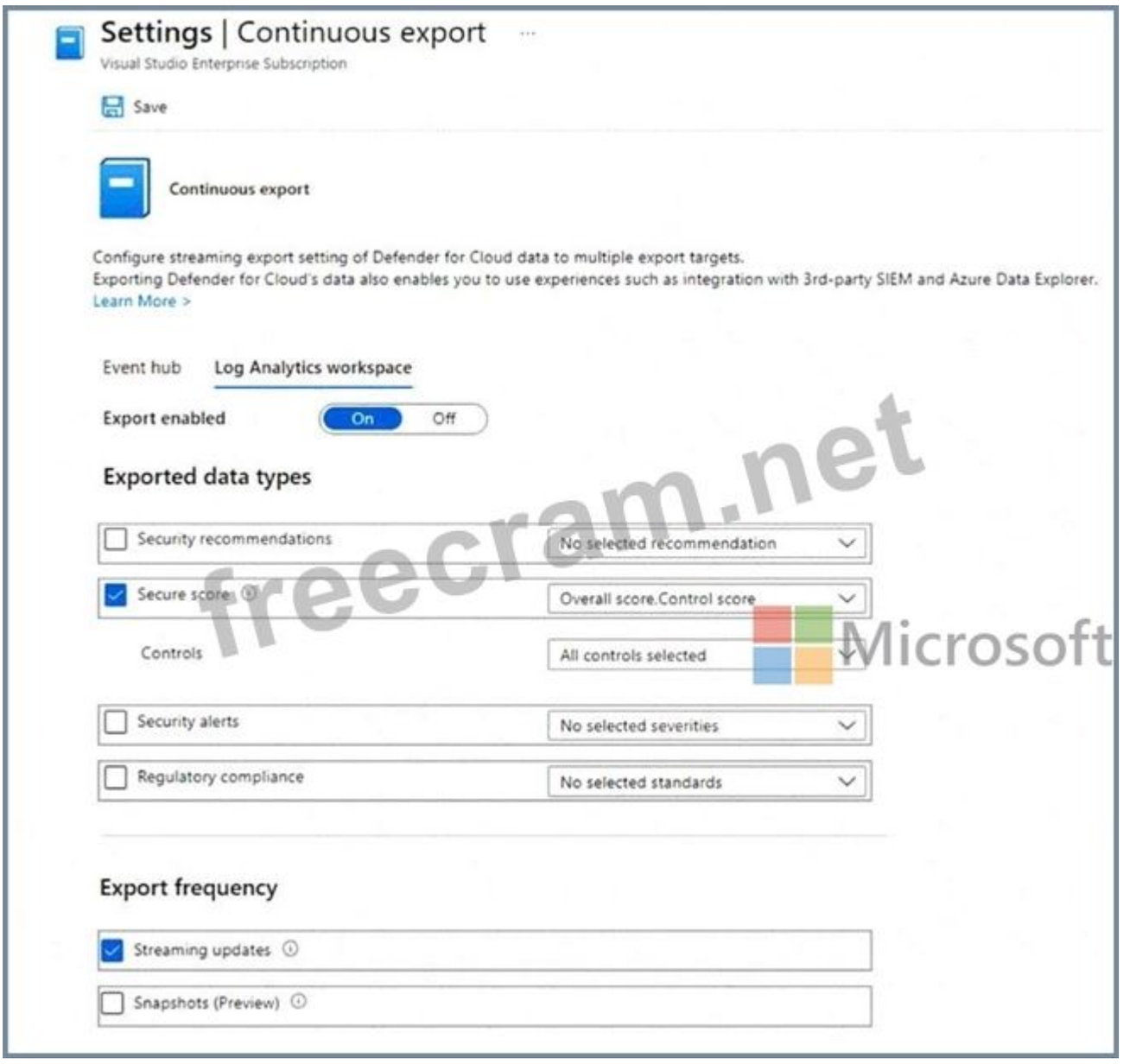
You have an Azure subscription that uses Microsoft Defender for Cloud.

You plan to use the Secure Score Over Time workbook.

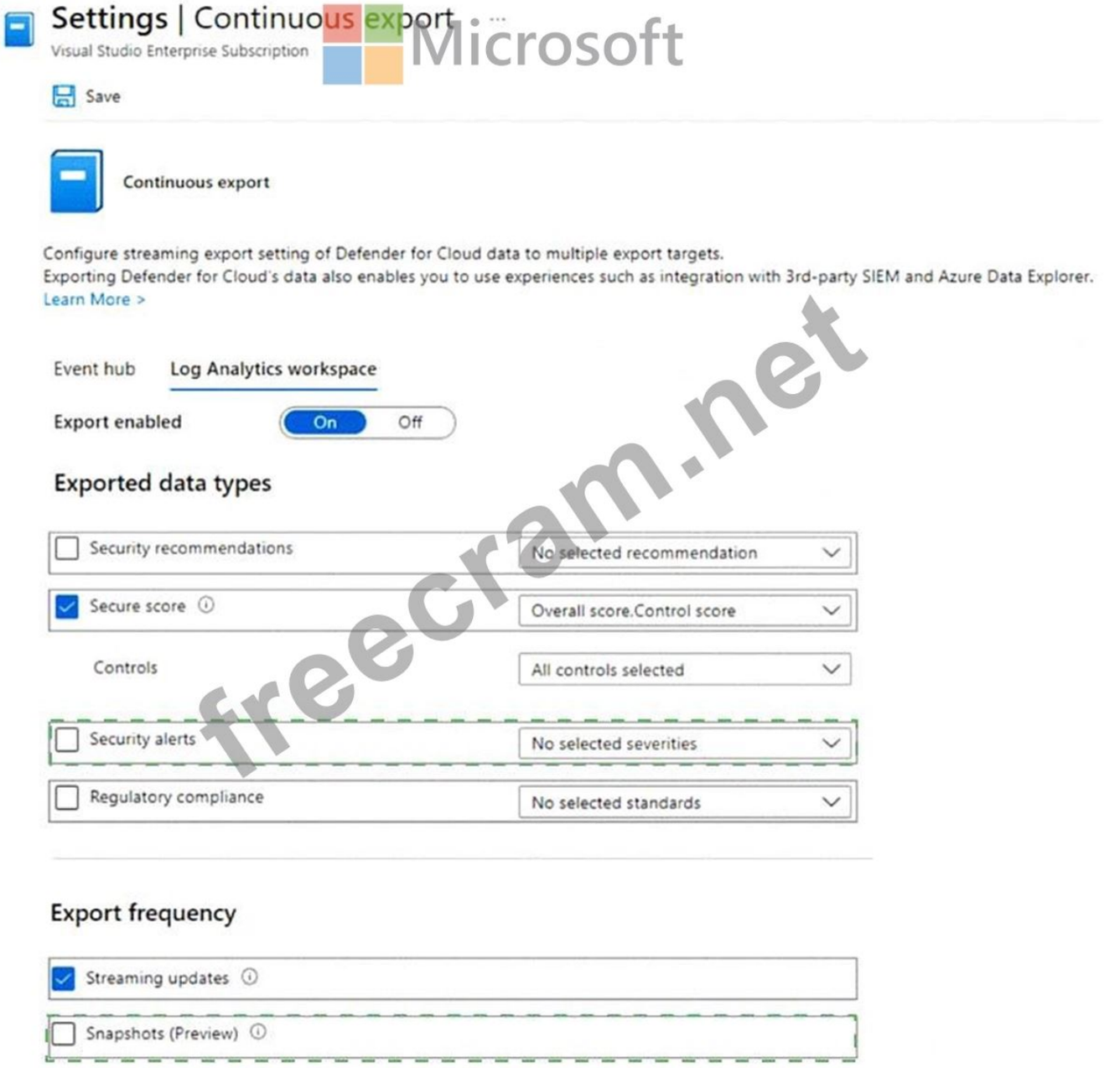
You need to configure the Continuous export settings for the Defender for Cloud data.

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

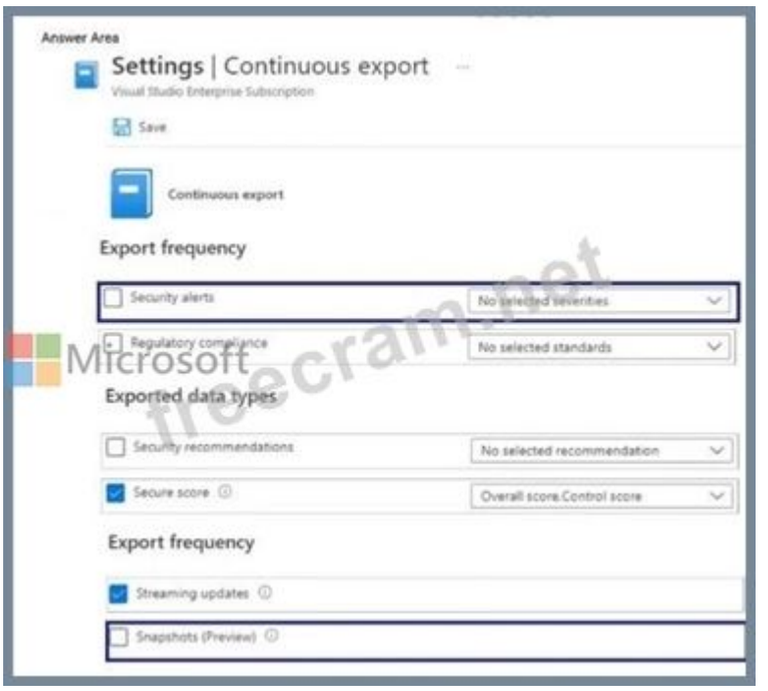
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

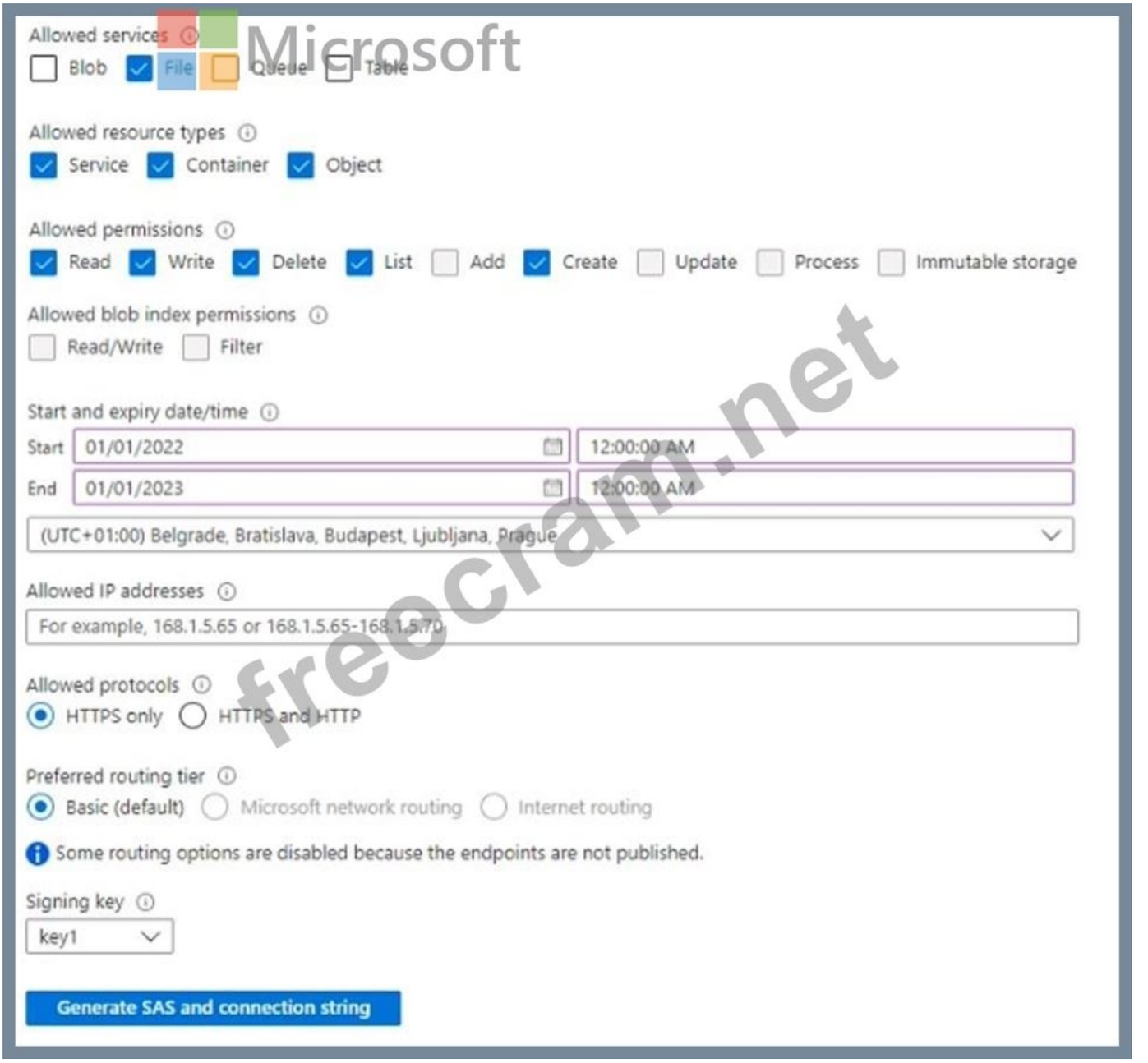


NEW QUESTION: 47

You have an Azure subscription that contains a user named User1 and a storage account named storage1. The storage1 account contains the resources shown in the following table.

Name	Type
container1	Container
folder1	File Share
table1	Table

In storage1, you create a shared access signature (SAS) named SAS1 as shown in the following exhibit.



To which resources can User! write on July 1, 2022 by using SAS1 and key 1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Answer Area

NEW QUESTION: 48

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

You need to ensure that User1 can create and manage administrative units. The solution must use the principle of least privilege.

Which role should you assign to User1?

A. Helpdesk administrator

B. Global administrator

C. Privileged role administrator

D. Security administrator

Answer: (SHOW ANSWER)

NEW QUESTION: 49

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

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.

Answer:

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: 50

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. Set Periodic recurring scans to ON.

B. Enable the Microsoft Defender for SQL plan.

C. Configure the Send scan report to setting.

D. From Advanced Threat Protection types, select SQL injection vulnerability.

Answer: (SHOW ANSWER)

NEW QUESTION: 51

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

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

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

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

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

Which virtual machines should you identify?

A. VM4 only

B. VM1 and VM3 only

C. VM1, VM3 and VM4 only

D. VM1, VM2, VM3, and VM4

Answer: (SHOW ANSWER)

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

Reference:

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

NEW QUESTION: 52

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

Name	Role
Admin1	Global administrator
Admin2	Group administrator
Admin3	User administrator

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

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

NOTE: Each correct selection is worth one point.

Users who can create a security group named Contoso Sales:

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

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

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

Answer:

Users who can create a security group named Contoso Sales:

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

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

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

Explanation:

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

NEW QUESTION: 53
You have the Azure virtual machines shown in the following table.

Name	Location	Connected to
VM1	West US 2	VNET1/Subnet1
VM2	West US 2	VNET1/Subnet1
VM3	West US 2	VNET1/Subnet2
VM4	East US	VNET2/Subnet3
VM5	West US 2	VNET5/Subnet5

Each virtual machine has a single network interface.
You add the network interface of VM1 to an application security group named ASG1.
You need to identify the network interfaces of which virtual machines you can add to ASG1.
What should you identify?
A. VM2 only
B. VM2, VM3, VM4, and VM5
C. VM2, VM3, and VM5 only
D. Vm2 and Vm3 only
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups

NEW QUESTION: 54
Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.

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

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

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

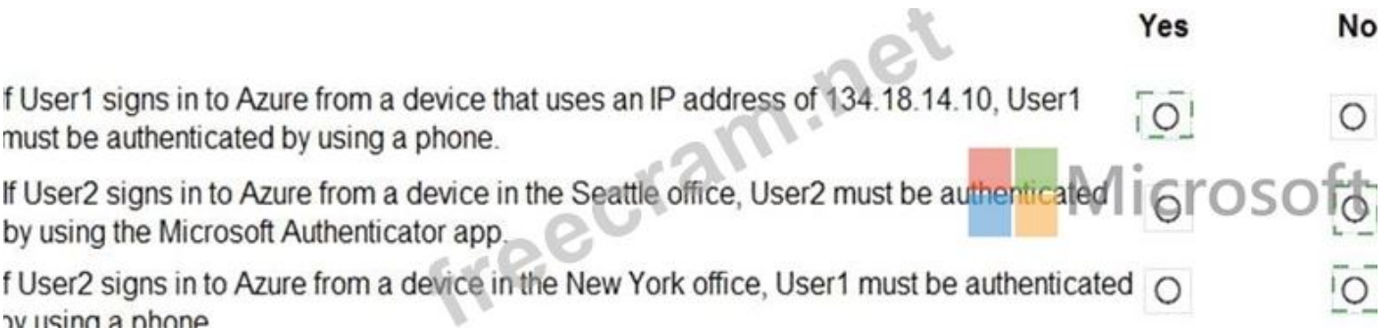
The MFA service settings are configured as shown in the exhibit. (Click the Exhibit tab.)

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

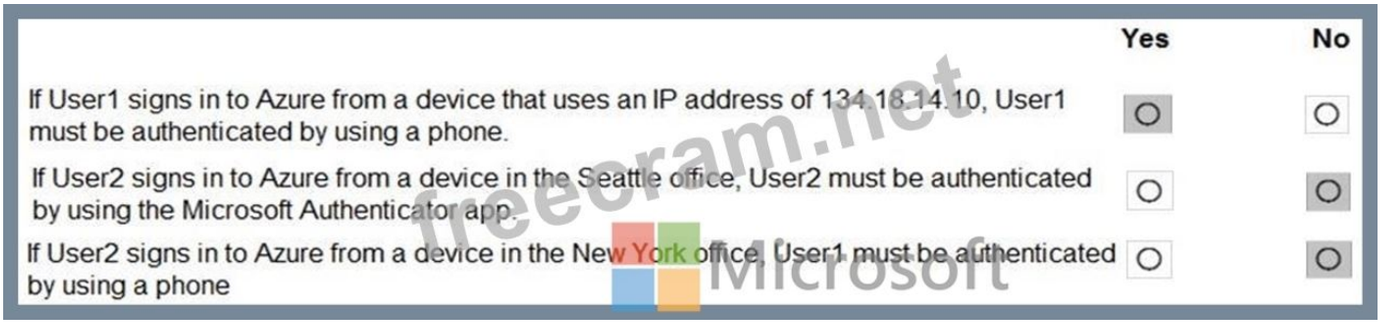
NOTE: Each correct selection is worth one point.

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	○	○
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	○	○
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	○	○

Answer:



Explanation:



Box 2: No

Use of Microsoft Authenticator is not required.

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

Box 3: No

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

References:

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

NEW QUESTION: 55

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

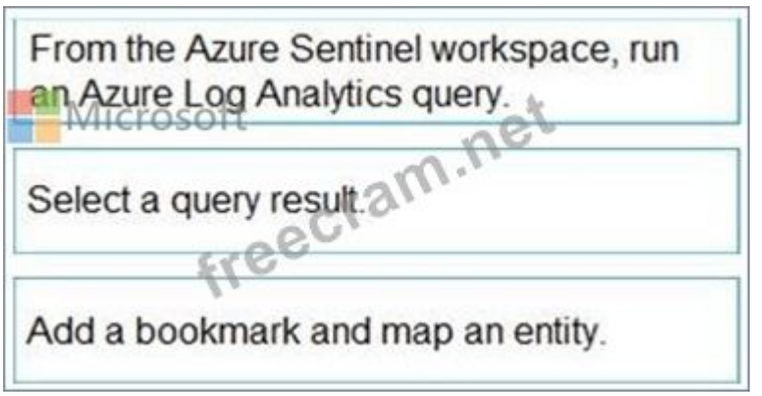
C. Azure Files

D. Blob storage

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

NEW QUESTION: 56
You need to deploy AKS1 to meet the platform protection requirements.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.
Answer:
Scenario: Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.
Litewire plans to deploy AKS1, which is a managed AKS (Azure Kubernetes Services) cluster.
Step 1: Create a server application
To provide Azure AD authentication for an AKS cluster, two Azure AD applications are created.
The first application is a server component that provides user authentication.
Step 2: Create a client application
The second application is a client component that's used when you're prompted by the CLI for authentication.
This client application uses the server application for the actual authentication of the credentials provided by the client.
Step 3: Deploy an AKS cluster.
Use the az group create command to create a resource group for the AKS cluster.
Use the az aks create command to deploy the AKS cluster.
Step 4: Create an RBAC binding.
Before you use an Azure Active Directory account with an AKS cluster, you must create role-binding or cluster role-binding. Roles define the permissions to grant, and bindings apply them to desired users. These assignments can be applied to a given namespace, or across the entire cluster.
Reference:
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration

NEW QUESTION: 57
You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) data connector.
You are threat hunting suspicious traffic from a specific IP address.
You need to annotate an intermediate event stored in the workspace and be able to reference the IP address when navigating through the investigation graph.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Answer:



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

NEW QUESTION: 58
You have an Azure Active Directory (Azure AD) tenant named contoso.com
You need to configure diagnostic settings for contoso.com. The solution must meet the following requirements:
* Retain loqs for two years.
* Query logs by using the Kusto query language
* Minimize administrative effort.
Where should you store the logs?
A. an Azure Log Analytics workspace
B. an Azure event hub
C. an Azure Storage account
Answer: (SHOW ANSWER)
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-queries

NEW QUESTION: 59
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 3
The developers at your company plan to create a web app named App28681041 and to publish the app to
https://www.contoso.com. You need to perform the following tasks:

* Ensure that App28681041 is registered to Azure AD.
* Generate a password for App28681041.

Answer:

Check below steps in explanation for Task.

Explanation

To register App28681041 to Azure AD and generate a password for it, you can follow these steps:

In the Azure portal, search for and select Azure Active Directory.

In the left pane, select App registrations.

Select New registration.

In the Register an application pane, enter the following information:

Name: App28681041

Supported account types: Select the appropriate account types for your scenario.

Redirect URI: Leave this field blank.

Select Register.

In the App registrations pane, select the newly created App28681041 application.

In the left pane, select Certificates & secrets.

Select New client secret.

In the Add a client secret pane, enter the following information:

Description: Enter a description for the client secret.

Expires: Select an appropriate expiration date for the client secret.

Select Add.

In the Certificates & secrets pane, copy the value of the newly created client secret.

You can find more information on this topic in the following Microsoft documentation: Quickstart: Register an application with the Microsoft identity platform.

NEW QUESTION: 60

You need to ensure that users can access VM0. The solution must meet the platform protection requirements.

What should you do?

A. Move VM0 to Subnet1.

B. On Firewall, configure a network traffic filtering rule.

C. Assign RT1 to AzureFirewallSubnet.

D. On Firewall, configure a DNAT rule.

Answer: (SHOW ANSWER)

https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat

NEW QUESTION: 61

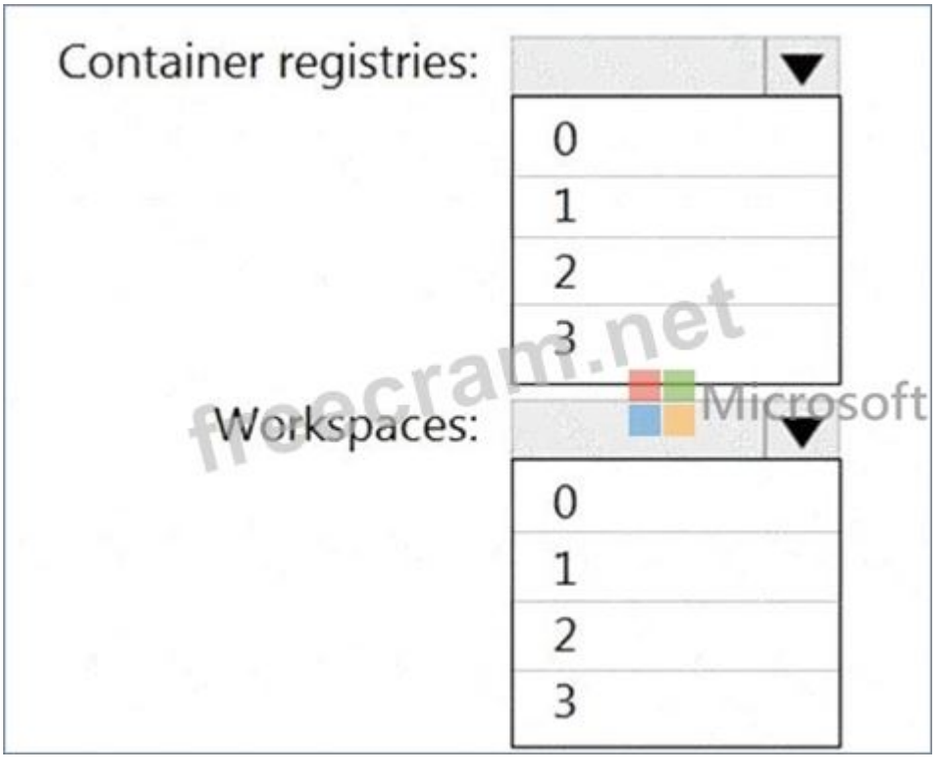
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Subscription. The subscription contains 50 virtual machines that run Windows Server
2012 R2 or Windows Server 2016.
You need to deploy Microsoft Antimalware to the virtual machines.
Solution: You connect to each virtual machine and add a Windows feature.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)
Microsoft Antimalware is deployed as an extension and not a feature.
References:
https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

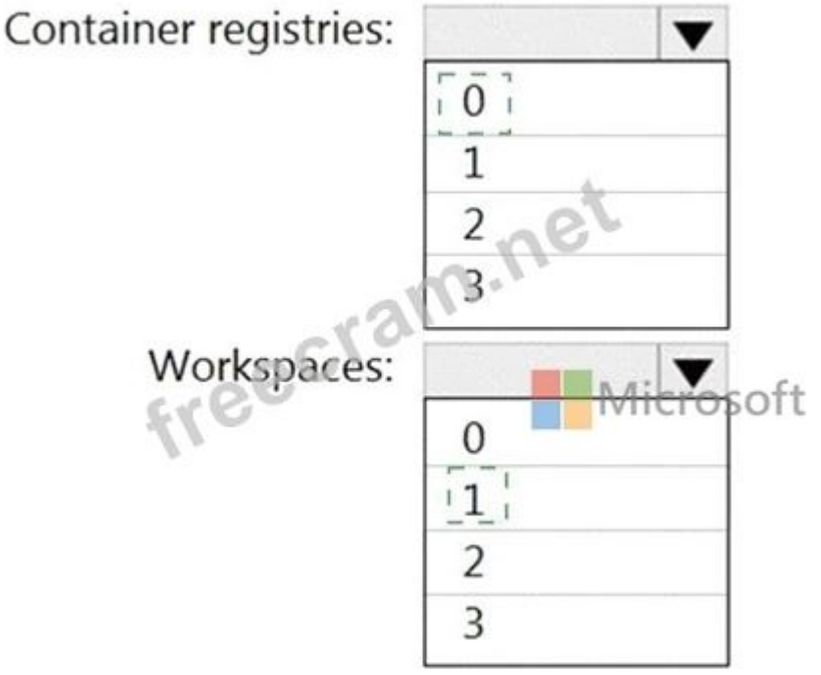
NEW QUESTION: 62
You are configuring and securing a network environment.
You deploy an Azure virtual machine named VM1 that is configured to analyze network traffic.
You need to ensure that all network traffic is routed through VM1.
What should you configure?
A. a system route
B. a network security group (NSG)
C. a user-defined route
Answer: (SHOW ANSWER)
Although the use of system routes facilitates traffic automatically for your deployment, there are cases in which you want to control the routing of packets through a virtual appliance. You can do so by creating user defined routes that specify the next hop for packets flowing to a specific subnet to go to your virtual appliance instead, and enabling IP forwarding for the VM running as the virtual appliance.
Note: User Defined Routes
For most environments you will only need the system routes already defined by Azure. However, you may need to create a route table and add one or more routes in specific cases, such as:

* Force tunneling to the Internet via your on-premises network.
* Use of virtual appliances in your Azure environment.
* In the scenarios above, you will have to create a route table and add user defined routes to it.
Reference:
https://github.com/uglide/azure-content/blob/master/articles/virtual-network/virtual-networks-udr-overview.
md

NEW QUESTION: 63
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?

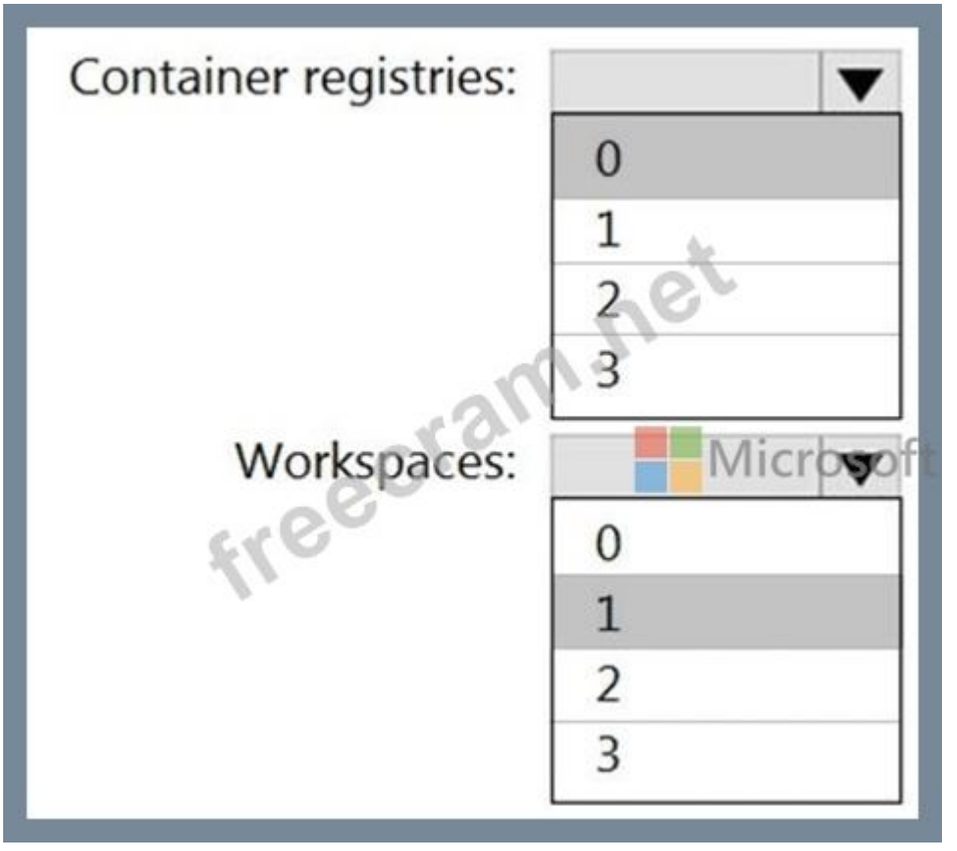


Answer:



Explanation:

Table Description automatically generated with medium confidence



Reference:

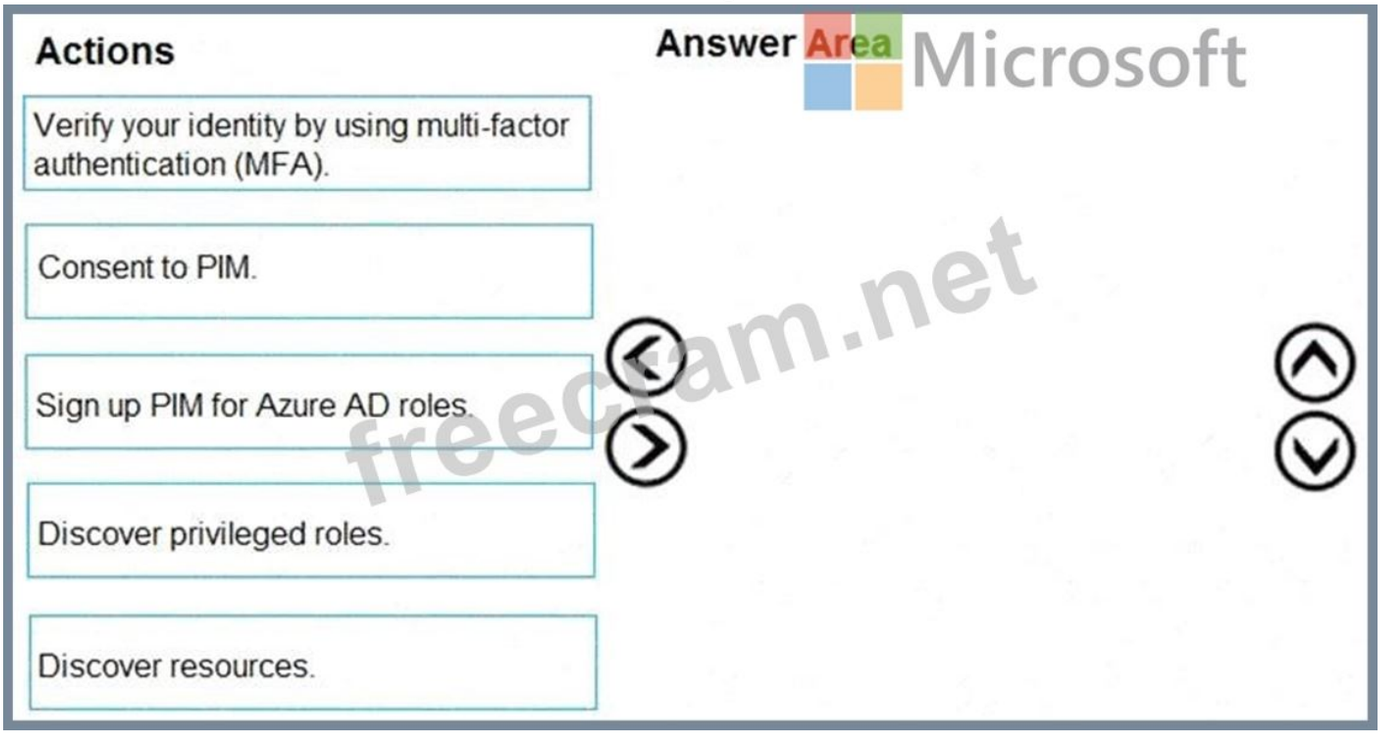
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

NEW QUESTION: 64

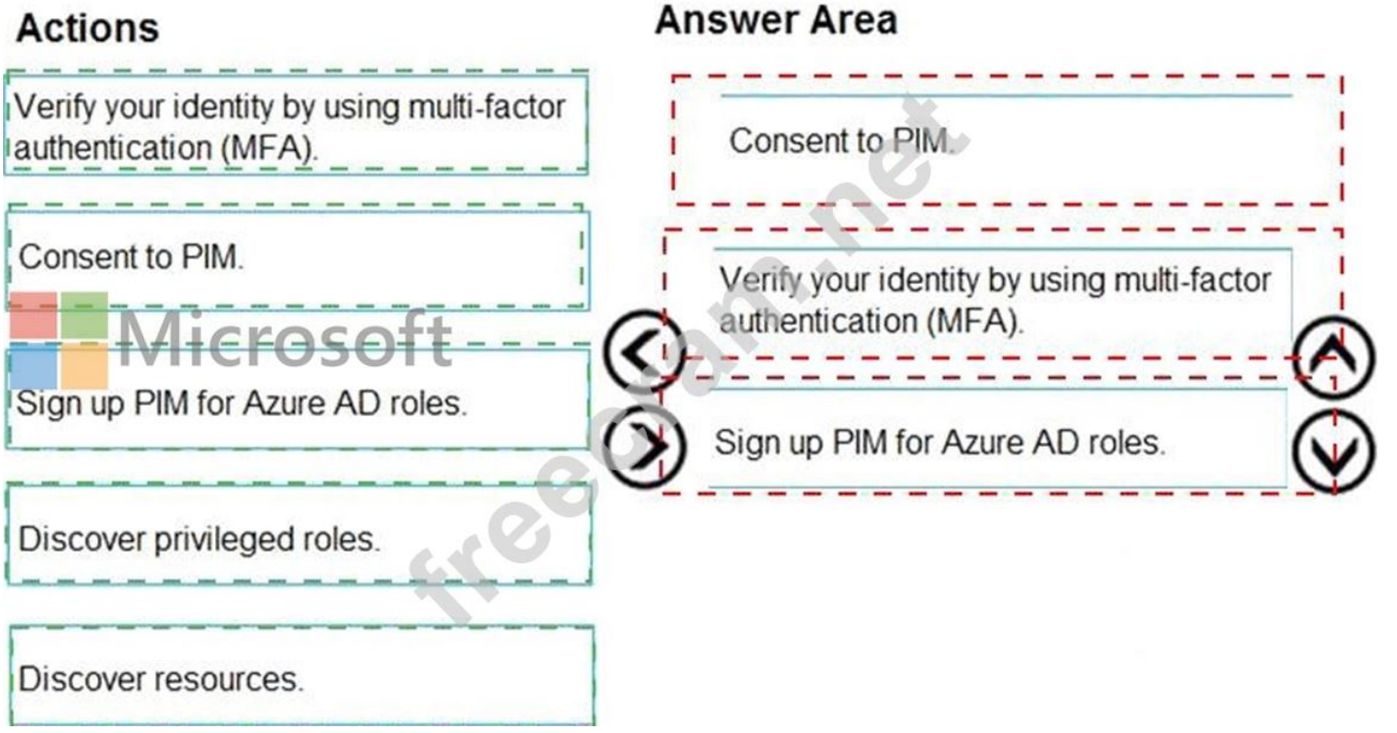
You create an Azure subscription.

You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure AD roles.

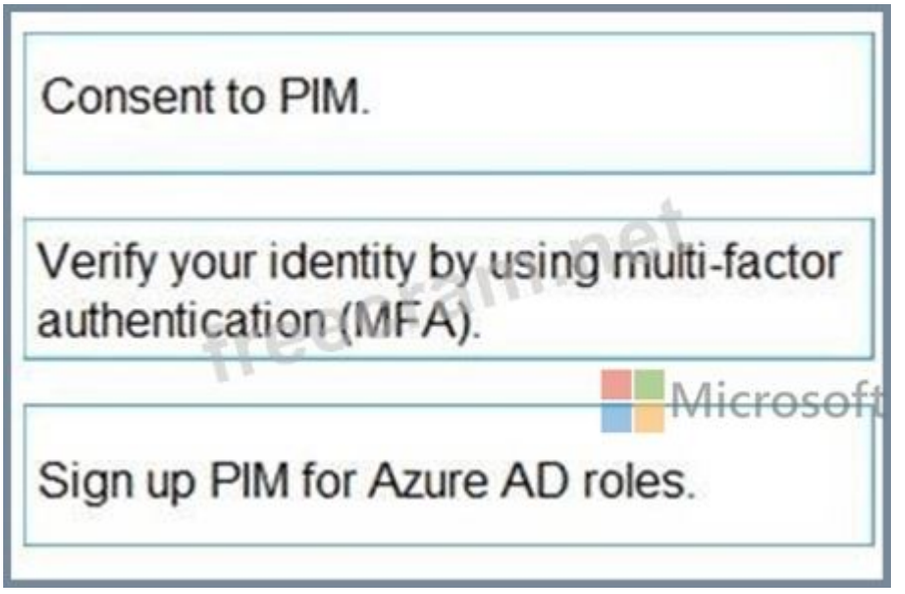
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



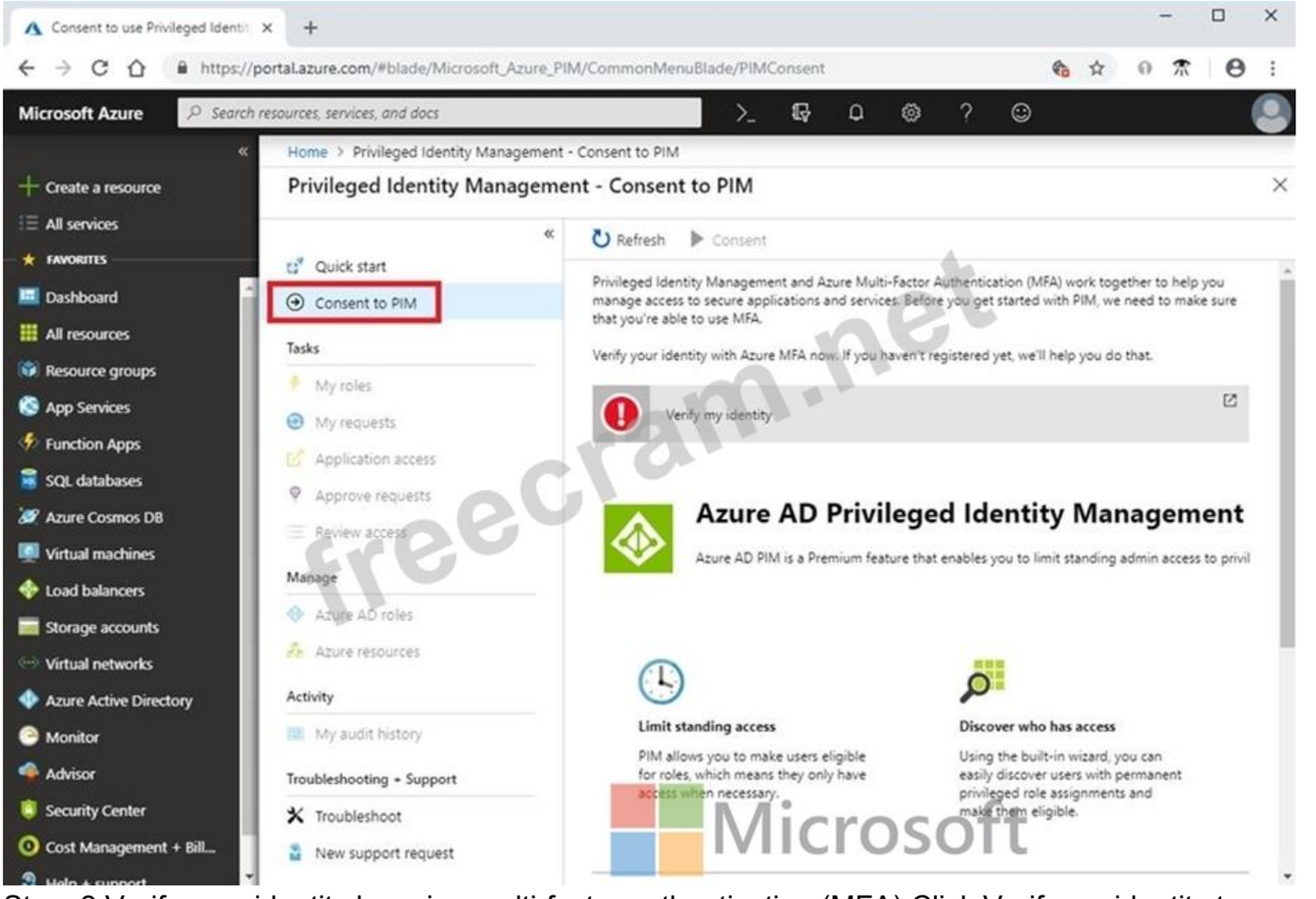
Answer:



Explanation:



Step 1: Consent to PIM



Step: 2 Verify your identity by using multi-factor authentication (MFA) Click Verify my identity to verify your identity with Azure MFA. You'll be asked to pick an account.

Step 3: Sign up PIM for Azure AD roles

Once you have enabled PIM for your directory, you'll need to sign up PIM to manage Azure AD roles.

References:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

NEW QUESTION: 65

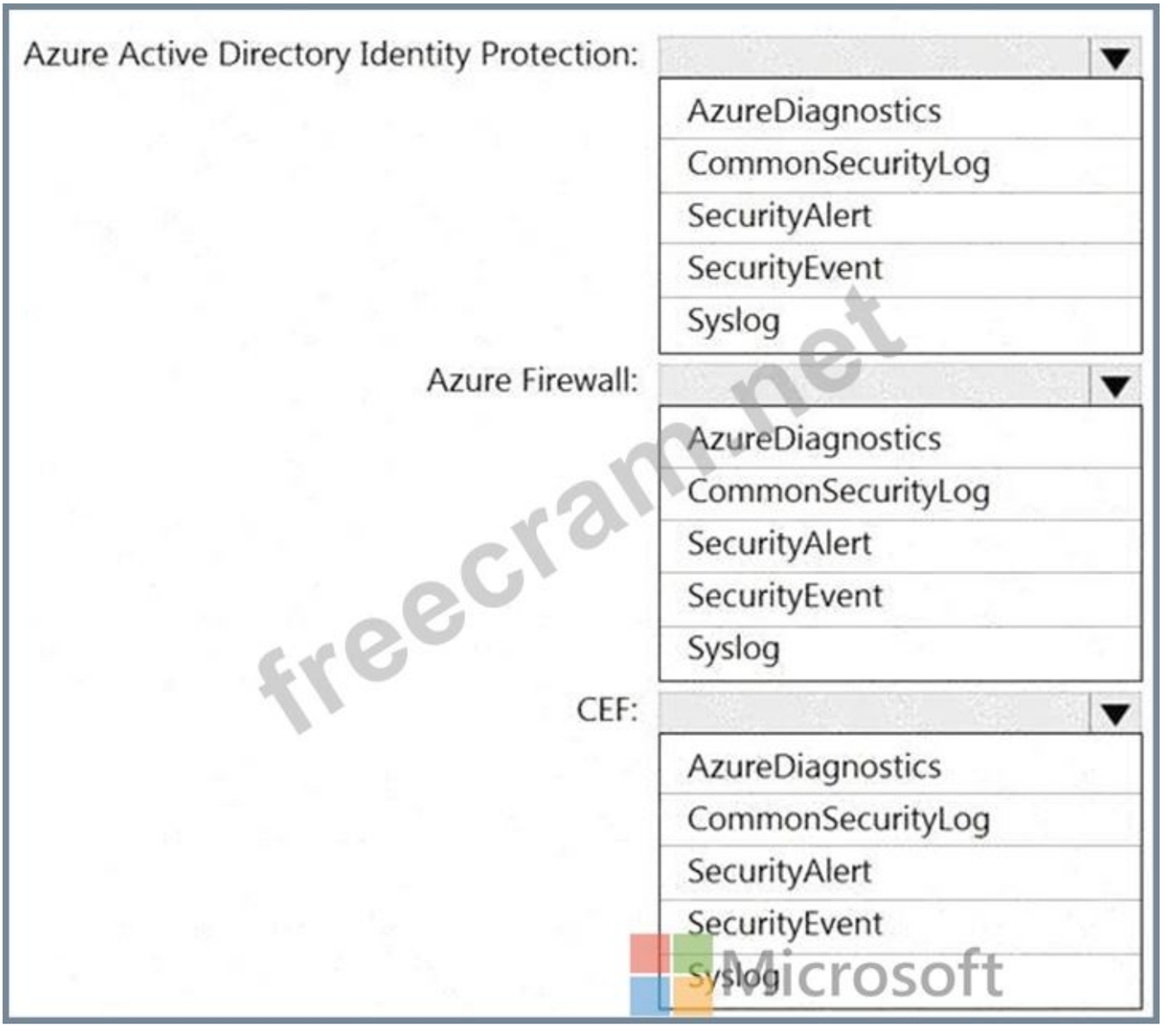
You have an Azure Sentinel workspace that has the following data connectors:

* Azure Active Directory Identity Protection
* Common Event Format (CEF)
* Azure Firewall

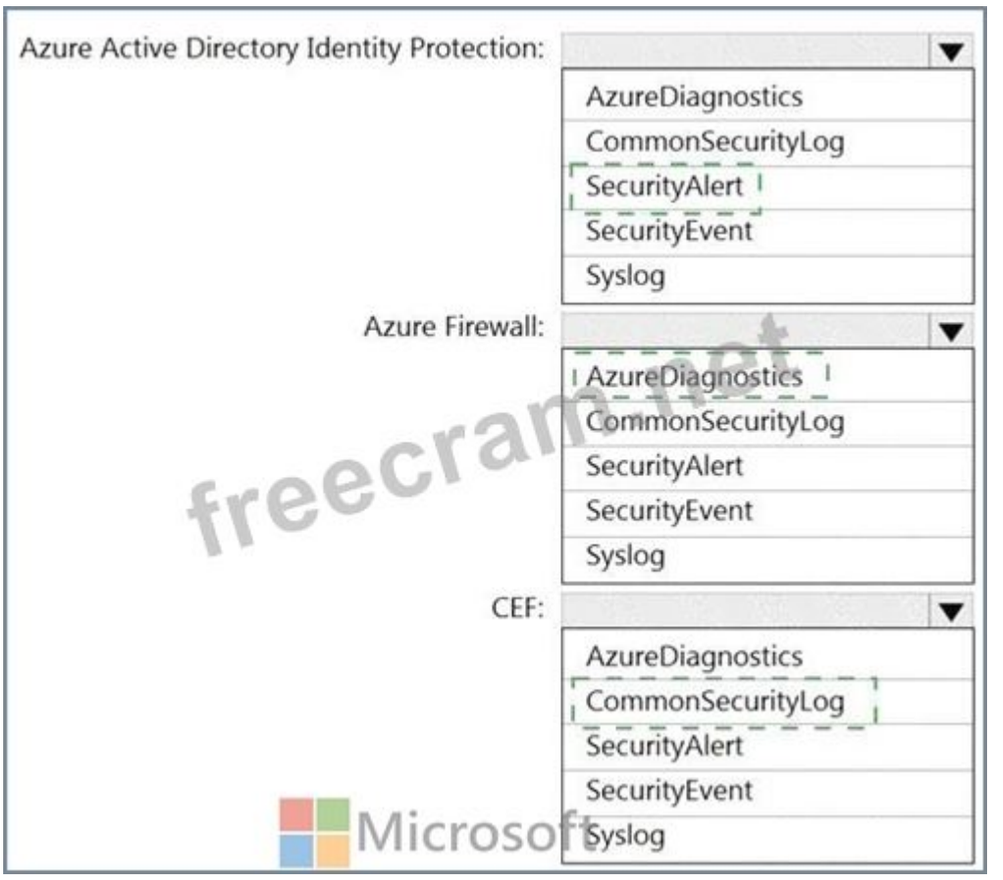
You need to ensure that data is being ingested from each connector.

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

NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 66

Your company uses cloud-based resources from the following platforms:

* Azure
* Amazon Web Services (AWS)
* Google Cloud Platform (GCP)

You plan to implement Microsoft Defender for Cloud.

On which platforms can you use Defender for Cloud to protect containers and storage? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION: 67

You have an Azure Storage account that contains a blob container named container! and a client application named App1. You need to enable App1 access to container1 by using Microsoft Entra authentication. What should you do? lo answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

NEW QUESTION: 68

You have an Azure subscription that contains an Azure key vault named Vault1 and a virtual machine named VM1. VM1 has the Key Vault VM extension installed.

For Vault1, you rotate the keys, secrets, and certificates.

What will be updated automatically on VM1?

A. the keys and secrets only

B. the secrets and certificates only

C. the keys only

D. the keys, secrets, and certificates

E. the certificates only

F. the secrets only

Answer: (SHOW ANSWER)

NEW QUESTION: 69
You have an Azure subscription that contains the resources shown in the following table.
You need to configure storage1 to regenerate keys automatically every 90 days. Which cmdlet should you run?
A. Add-A:StorogcAccountmanagementPolicyAction
B. Set-A;StorageAccountimanagementPolicy
C. set -A=StorageAccount
D. Add-AsKeyVaultmanageStorageAccount
Answer: (SHOW ANSWER)

NEW QUESTION: 70
Your network contains an Active Directory forest named contoso.com. The forest contains a single domain.
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant.
You need to recommend an integration solution that meets the following requirements:
Ensures that password policies and user logon restrictions apply to user accounts that are synced to the Tenant Minimizes the number of servers required for the solution.
Which authentication method should you include in the recommendation?

A. federated identity with Active Directory Federation Services (AD FS)
B. password hash synchronization with seamless single sign-on (SSO)
C. pass-through authentication with seamless single sign-on (SSO)
Answer: (SHOW ANSWER)
1. Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant
>> Pass-Through Authentication enforce on-premises user account states, password policies, and sign-in hours.
2. Minimizes the number of servers required for the solution.
>> Pass-through needs a lightweight agent to be installed one (or more) on-premises servers.
>> PW Hash also require installing Azure AD Connect on your existing DC.

NEW QUESTION: 71
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:

Answer Area

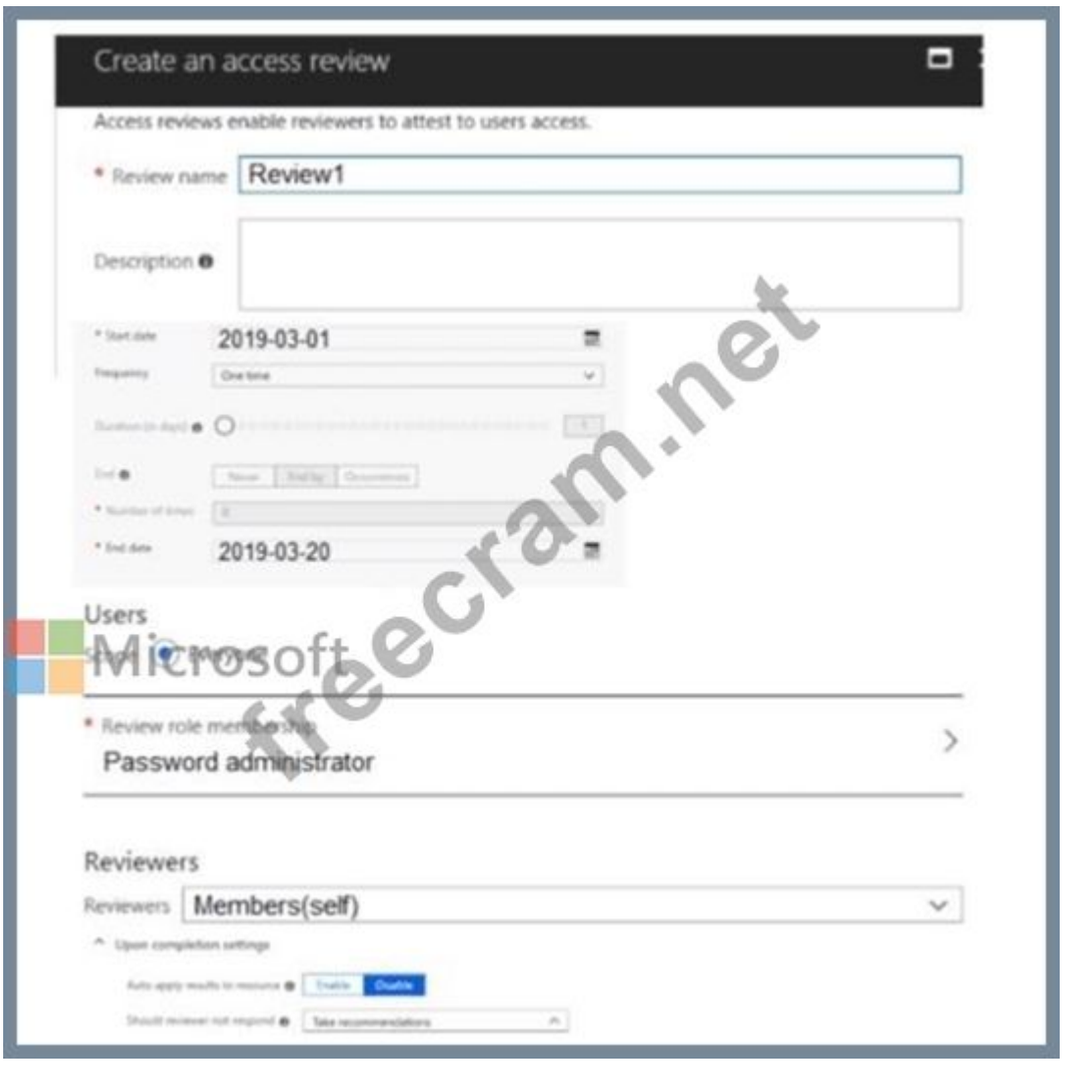
Statements	Yes	No
User1 can sign in without providing a password.	○	○
User2 can choose to use a certificate or a smart card to sign in.	○	○
User3 must use a certificate during sign-in.	○	○

NEW QUESTION: 72
You have an Azure Active Directory (Azure AD) tenant that contains a group named Group1 You need to ensure that the members of Group1 sign in by using passwordless authentication What should you do?
A. Configure the Microsoft Authenticator authentication method policy.
B. Configure the sign-in risk policy.
C. Configure the certificate-based authentication (CBA) policy.
D. Create a Conditional Access policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 73
You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

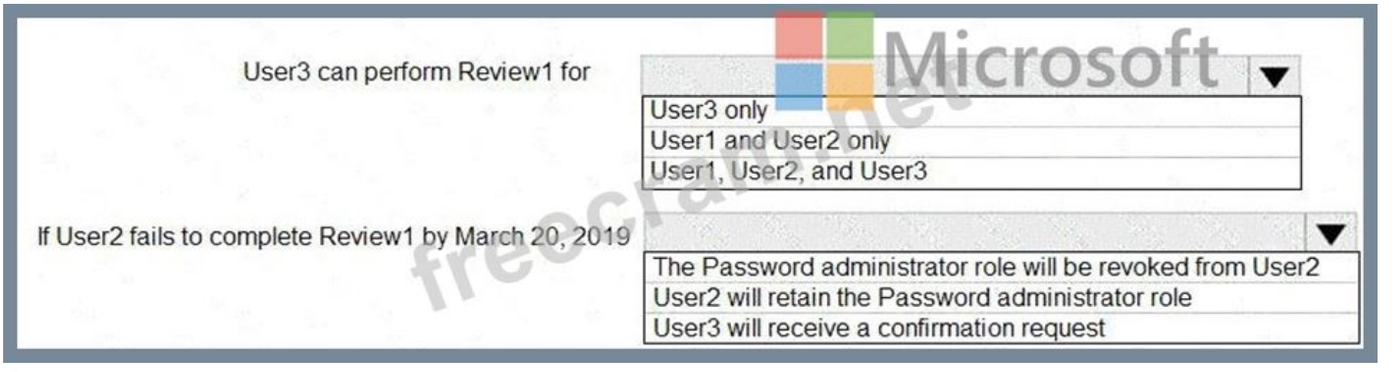
Name	Role	Sign in frequency
User1	Password administrator	Sign in every work day
User2	Password administrator	Sign in bi-weekly
User3	Global administrator, Password administrator	Signs in every month

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

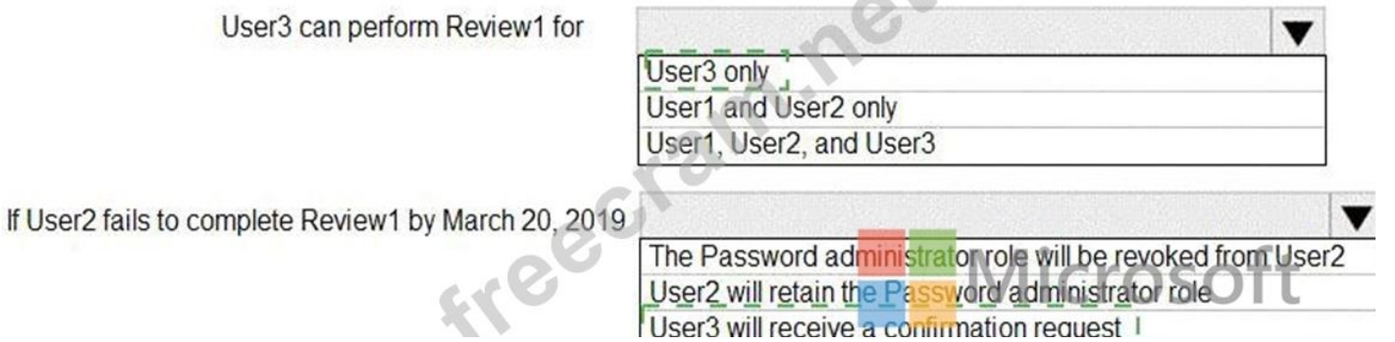


Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

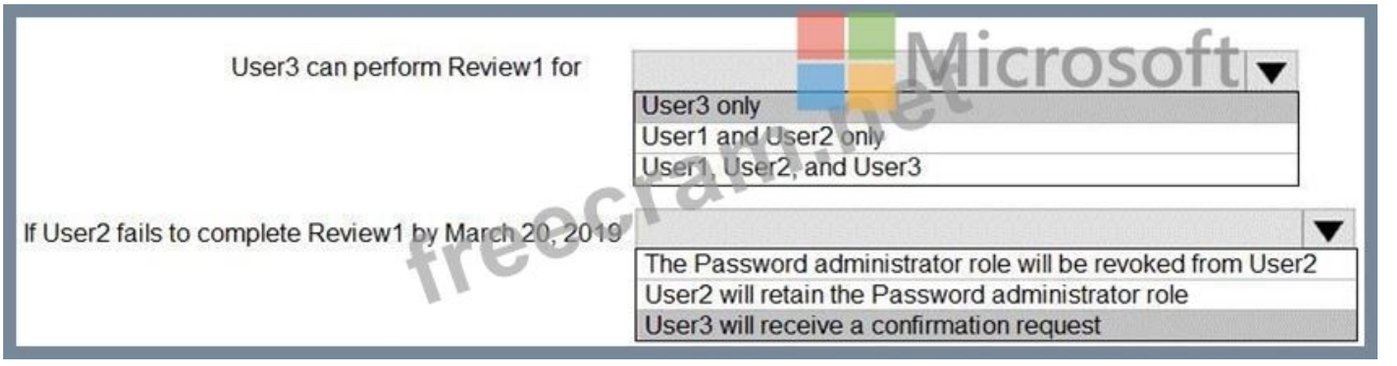
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



Box 1: User3 only

Use the Members (self) option to have the users review their own role assignments.

Box 2: User3 will receive a confirmation request

Use the Should reviewer not respond list to specify what happens for users that are not reviewed by the reviewer within the review period. This setting does not impact users who have been reviewed by the reviewers manually. If the final reviewer's decision is Deny, then the user's access will be removed.

No change - Leave user's access unchanged

Remove access - Remove user's access

Approve access - Approve user's access

Take recommendations - Take the system's recommendation on denying or approving the user's continued access References:

https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to- start-security-review

NEW QUESTION: 74

You have an Azure subscription that contains the following resources:

* An Azure key vault
* An Azure SQL database named Database1
* Two Azure App Service web apps named AppSrv1 and AppSrv2 that are configured to use system-assigned managed identities and access Database1 You need to implement an encryption solution for Database1 that meets the following requirements:
* The data in a column named Discount in Database1 must be encrypted so that only AppSrv1 can decrypt the data.

* AppSrv1 and AppSrv2 must be authorized by using managed identities to obtain cryptographic keys.

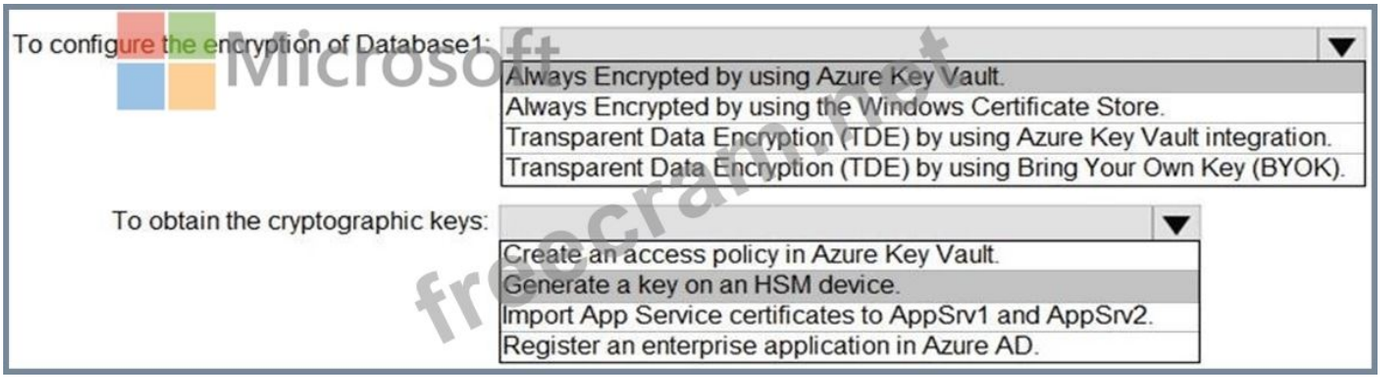
How should you configure the encryption settings fa Database1 To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Answer:

Explanation:

Text Description automatically generated with medium confidence



Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/always-encrypted-azure-key-vault-configure?

tabs=azure-powershell

NEW QUESTION: 75

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

Answer: (SHOW ANSWER)

NEW QUESTION: 76

You have an Azure subscription named Subscription1 that contains a resource group named RG1 and a user named User1. User1 is assigned the Owner role for RG1.

You create an Azure Blueprints definition named Blueprint1 that includes a resource group named RG2 as shown in the following exhibit.

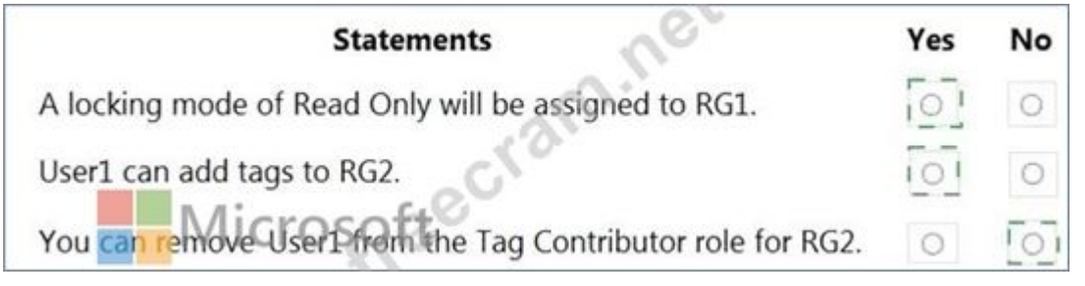
You assign Blueprint1 to Subscription1 by using the following settings:

* Lock assignment: Read Only
* Managed Identity: System assigned

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

NOTE: Each correct selection is worth one point.

Answer:



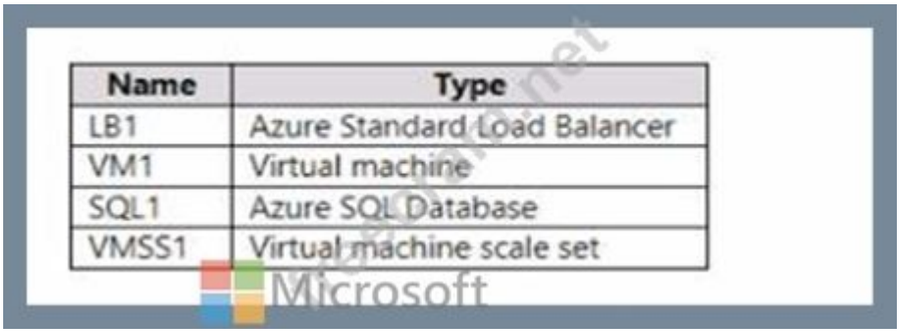
Explanation:
Graphical user interface, text, application Description automatically generated

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

NEW QUESTION: 77
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: (SHOW ANSWER)
https://docs.microsoft.com/en-us/azure/azure-arc/servers/onboard-service-principal

NEW QUESTION: 78

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. LB1

B. VM1

C. VMSS1

D. SQL

Answer: (SHOW ANSWER)

NEW QUESTION: 79

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

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:

NEW QUESTION: 80

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

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: 81
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: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-log-analytics-wizard

NEW QUESTION: 82
You have an Azure key vault named Vault1 that stores the resources shown in the following table.
Which resources support the creation of a rotation policy?
A. Key1 and Cert1 only
B. Key1, Secret1, and Cert1
C. Secret1 and Cert1 only
D. Cert1 only
E. Key 1 only
F. Key1 and Secret1 only
Answer: (SHOW ANSWER)

NEW QUESTION: 83
You have an Azure subscription that contains an instance of Azure Firewall Standard named AzFWL You need to identify whether you can use the following features with AzFW1:
* TLS inspection
* Threat intelligence
* The network intrusion detection and prevention systems (IDPS)

What can you use?

A. TLS inspection, threat intelligence, and the IDPS

B. threat intelligence only

C. threat intelligence and the IDPS only

D. TLS inspection and the IDPS only

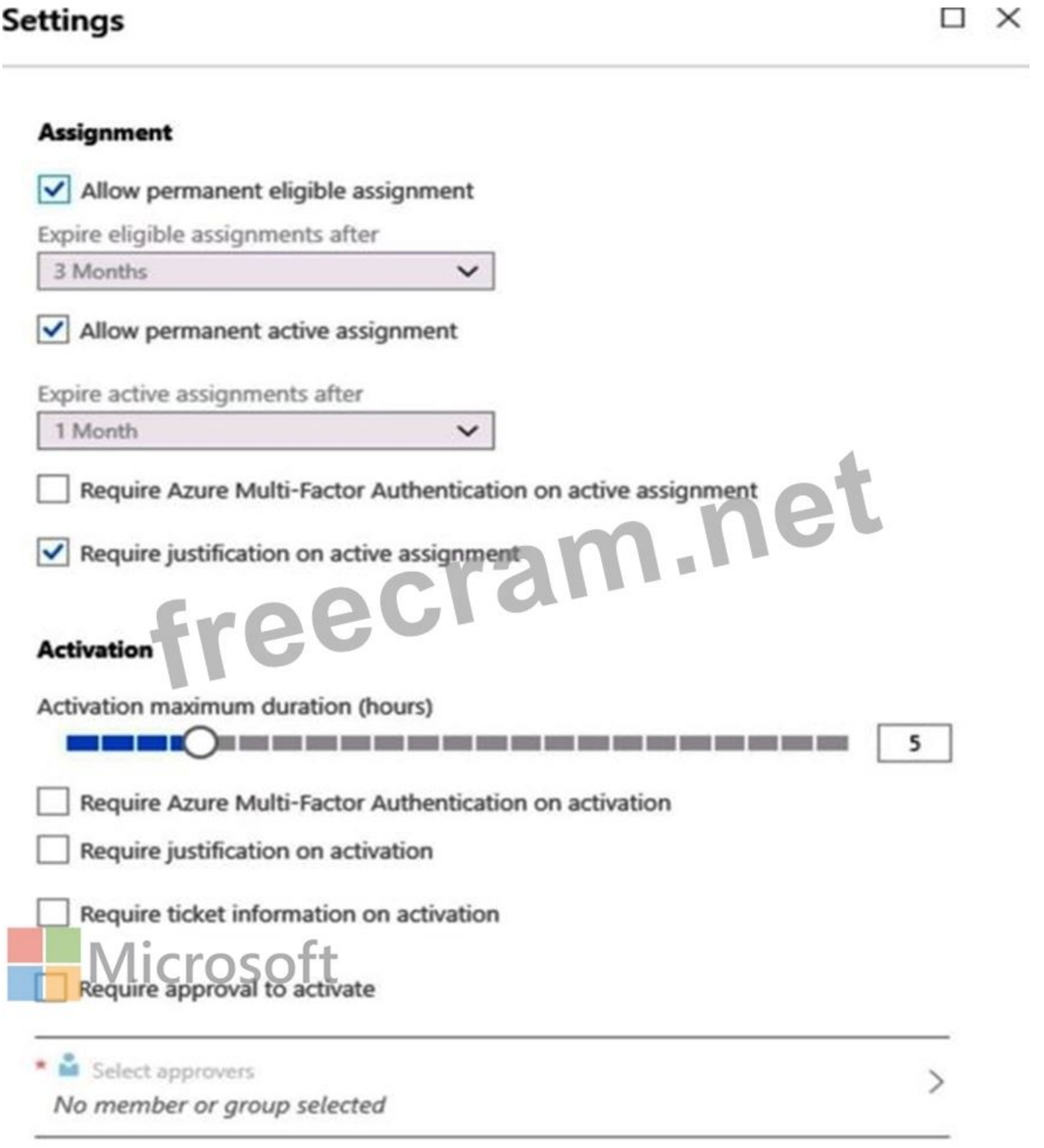
E. TLS inspection only

Answer: (SHOW ANSWER)

NEW QUESTION: 84

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

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.

Answer:

Explanation:

Box 1: Yes

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

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

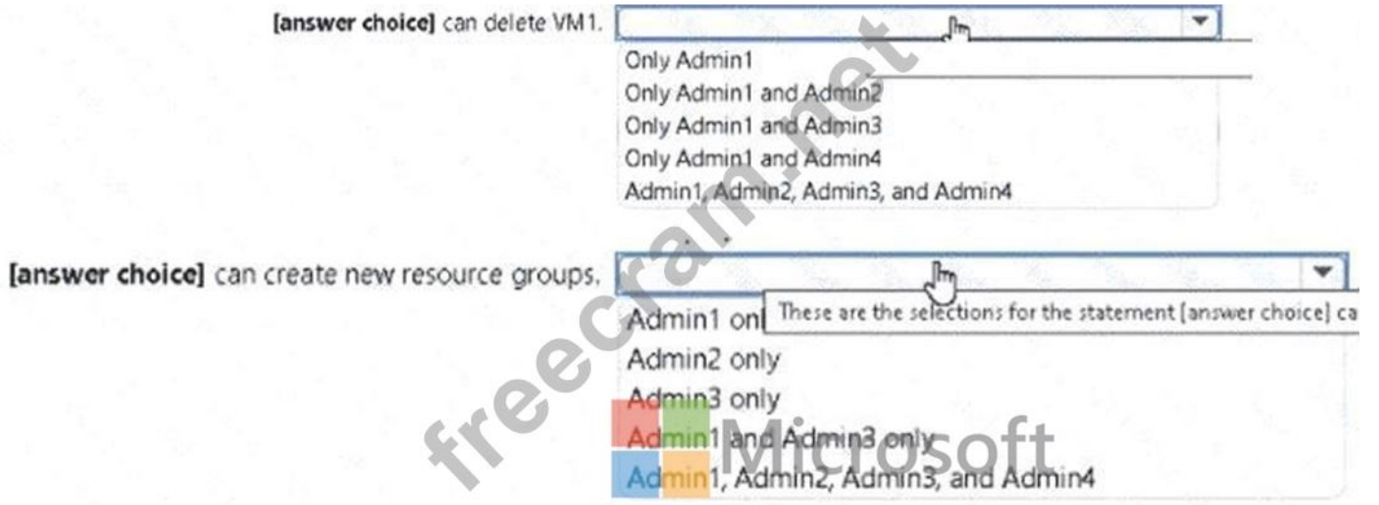
Use the Activation maximum duration slider to set the maximum time, in hours, that a role stays active before it expires. This value can be from one to 24 hours.

Box 2: Yes

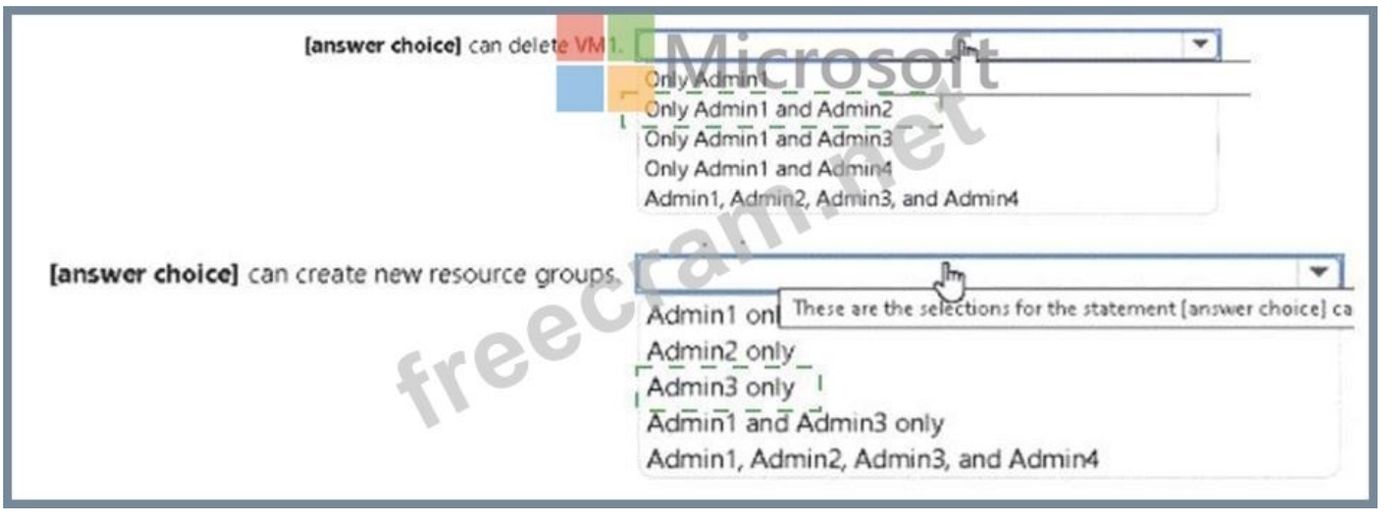
Active Type: A role assignment that doesn't require a user to perform any action to use the role. Users assigned as active have the privileges assigned to the role Box 3: Yes User3 is member of Group2.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure
https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource- roles-configure-role-settings

NEW QUESTION: 85
You have the role assignments shown in the following exhibit.

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



Answer:



NEW QUESTION: 86

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

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

You plan to deploy an app named App1.

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

Which role should you assign to User1?

A. App Configuration Data Owner for the subscription

B. Managed Application Contributor for the subscription

C. Cloud application administrator in Azure AD

D. Application developer in Azure AD.

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 87

You have an Azure Active Directory (Azure AD) tenant. The tenant contains users that are assigned Azure AD Premium Plan 2 licenses.

You have an partner company that has a domain named The fabrikam.com domain contains a user named user'. User' has an email address of userl@tabrikam.com.

You to provide User1 with to the resources in the tenant The solution must meet the following requirements:

* user1 must be able to sign in by using the userl@fabrikam.com credentials
* You must be able to grant User1 access to the resources in the tenant
* Administrative effort must be minimized.

What should you do?

A. To the tenant add fabrikamcom as a custom domain

B. Set Enable guest self-service sign up via user flows to Yes for the tenant.

C. Create a user account for user1.

D. Create an invite for User1.

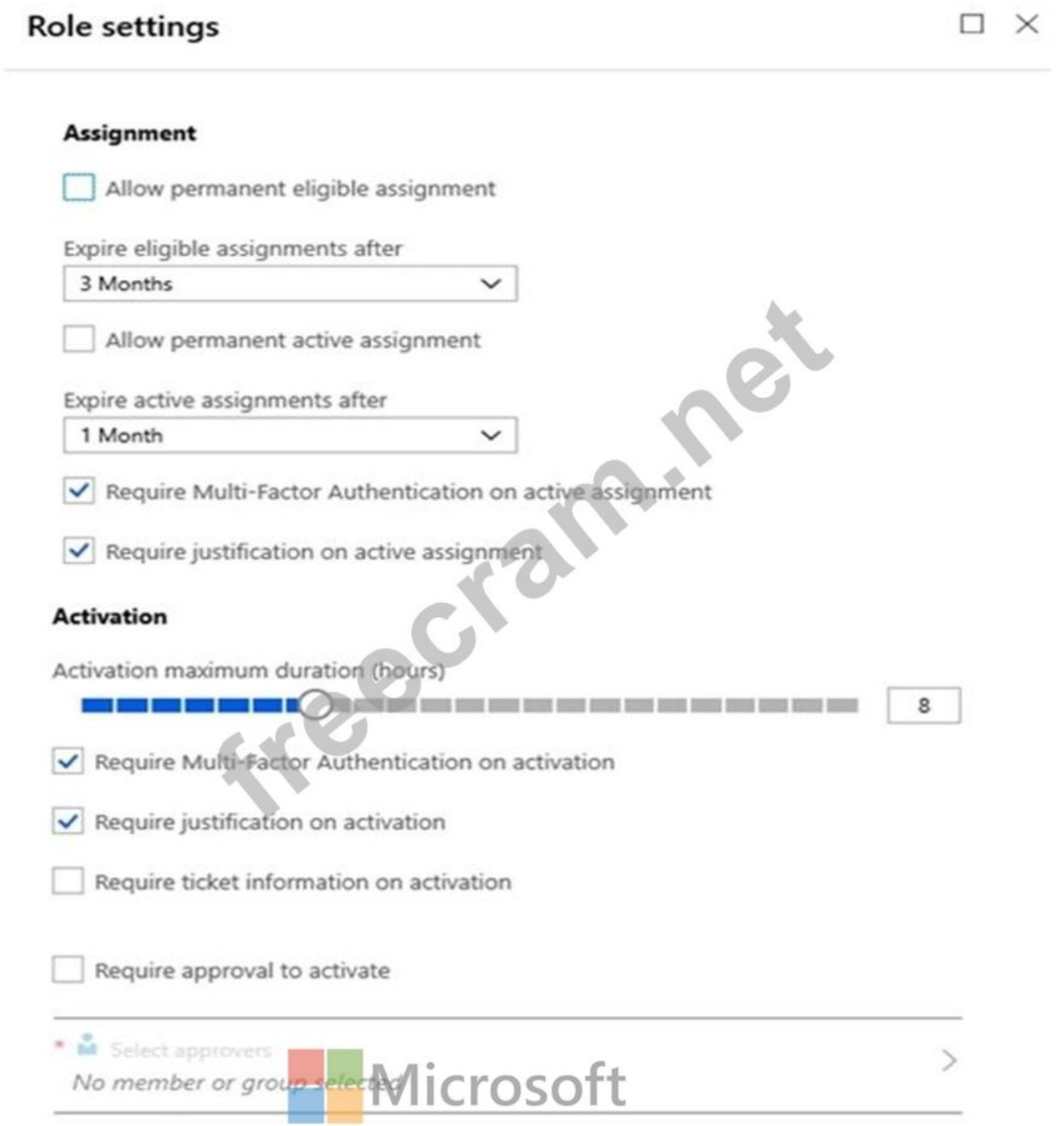
Answer: (SHOW ANSWER)

NEW QUESTION: 88

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.

Answer:

Name	Assignment type
User1	Eligible
User2	Active
User3	Active

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

NEW QUESTION: 89
You have an Azure subscription.
You plan to deploy a new Conditional Access policy named CAPolicy1.
You need to use the What If tool to evaluate how CAPolicy1 will affect uter1. The solution must minimize the impact of CAPolicy1 on the users.
To what should you set the Enable policy setting for CAPolicy1?
A. Oft
B. Report only
C. On
Answer: B (LEAVE A REPLY)

NEW QUESTION: 90
Your on-premises network contains an Active Directory Domain Services (AD DS) domain and the devices shown in the following table.
You have a hybrid Microsoft Entra tenant that contains a synced user named User1.
You have an Azure subscription that contains the Azure Files shares shown in the following table.
Used is assigned the Storage File Data SMB Share Contributor role tor storage1 and storage2.
The Security settings for Share! are configured as shown in the following exhibit.

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

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION: 91

You have an Azure subscription that contains a user named User1 and a storage account named storage 1. The storage1 account contains the resources shown in the following table:

User1 is assigned the following roles for storage1:

* Storage Blob Data Reader
* Storage Table Data Contributor

* Storage File Data SMB Share Reader

Answer:

No, Yes, No

NEW QUESTION: 92

You have 20 Azure subscriptions and a security group named Group1. The subscriptions are children of the root management group.

Each subscription contains a resource group named RG1.

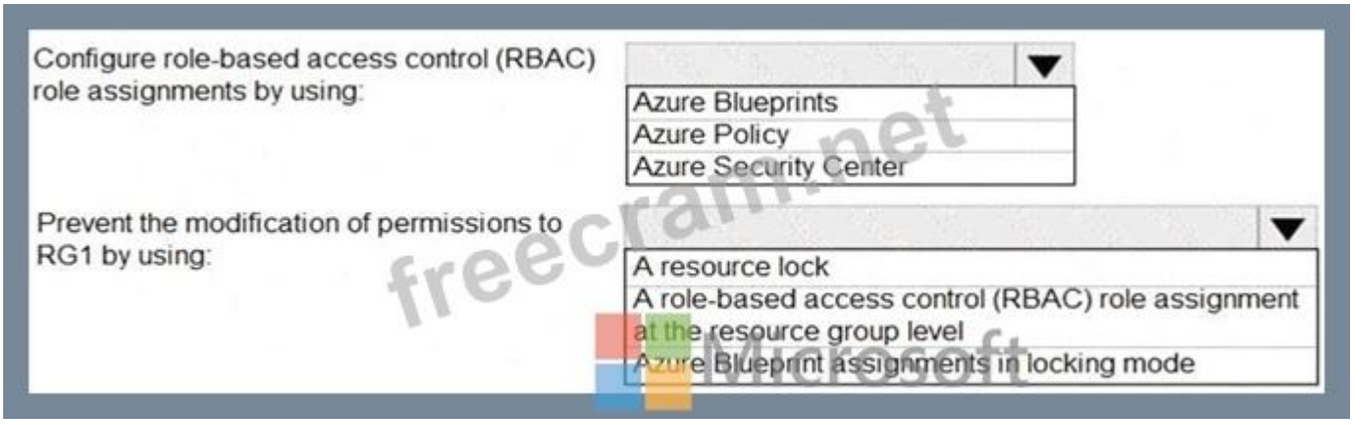
You need to ensure that for each subscription RG1 meets the following requirements:

* The members of Group1 are assigned the Owner role.

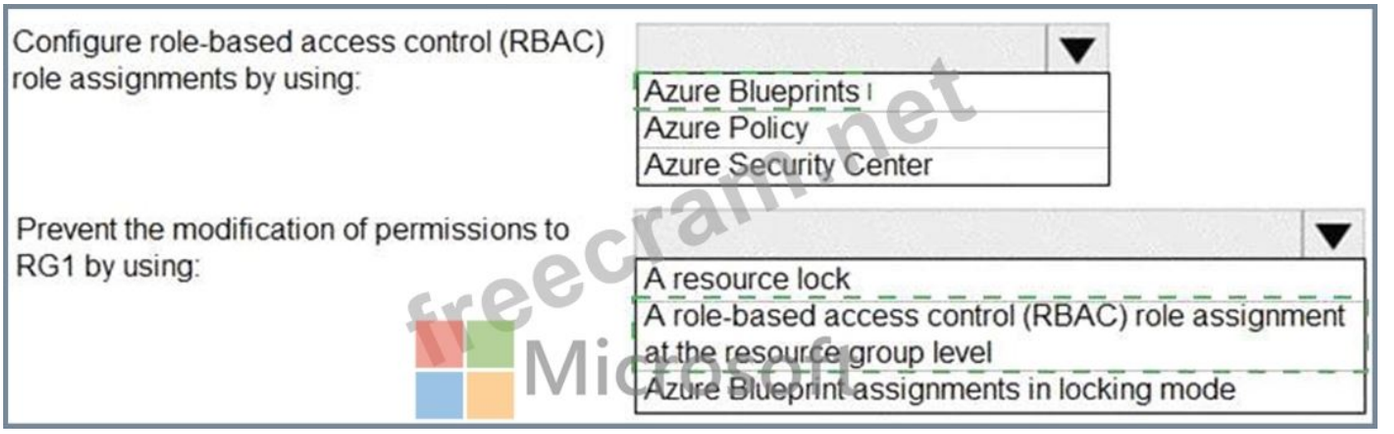
* The modification of permissions to RG1 is prevented.

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

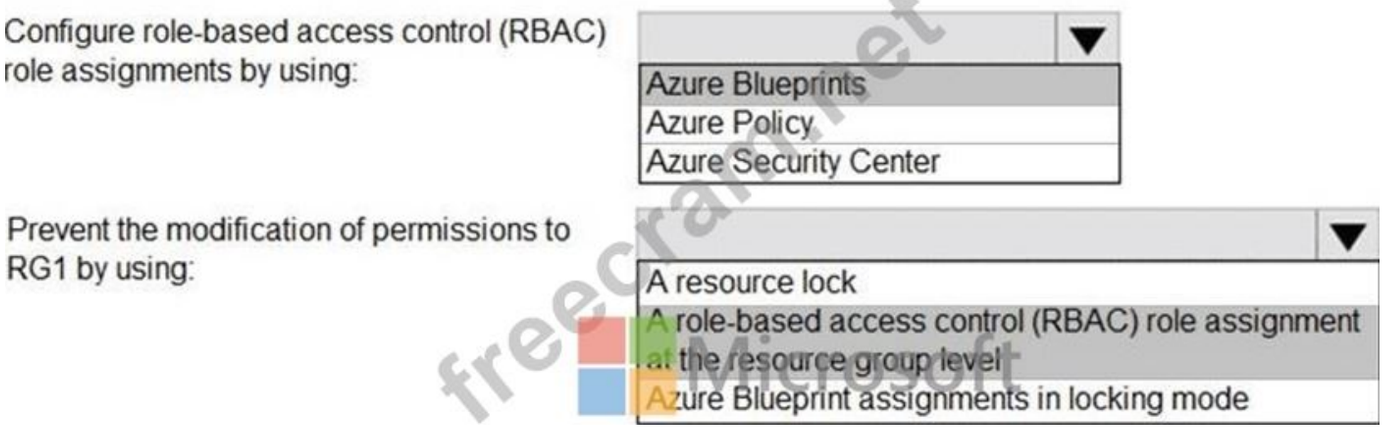
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 93

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:

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: 94

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: (SHOW ANSWER)

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:

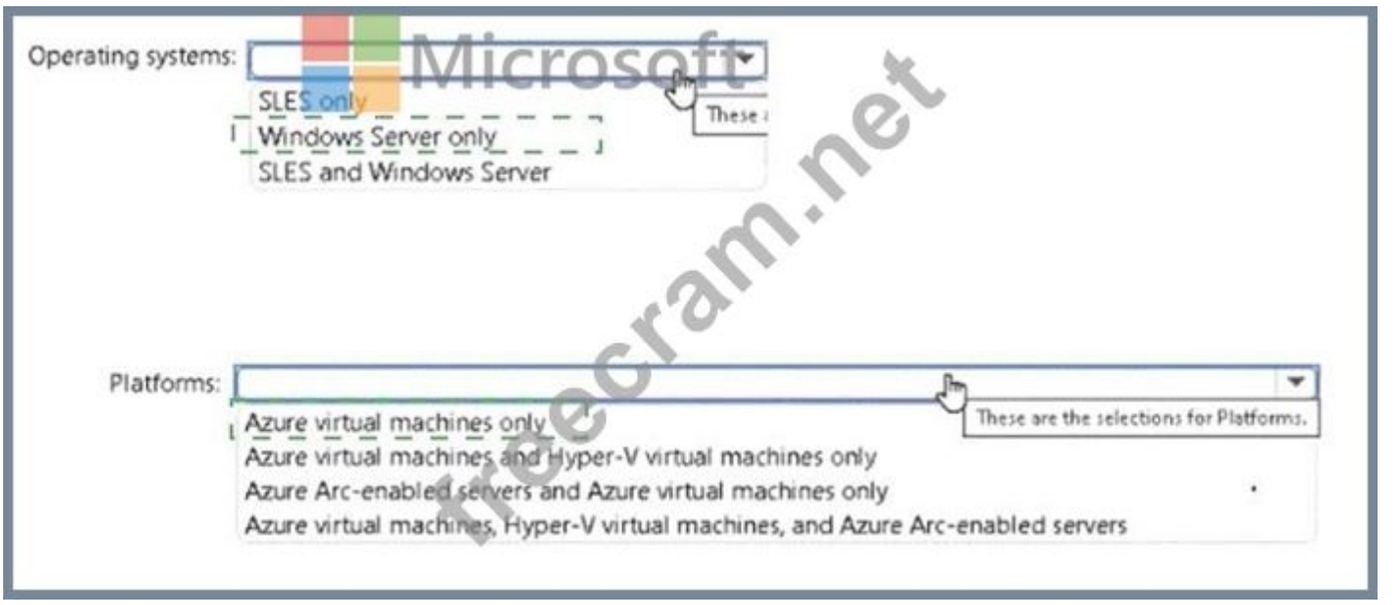
https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview

NEW QUESTION: 95

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

You have an Azure subscription that contains multiple virtual machines that run either Windows Server 2019 or SLES. You plan to implement adaptive application controls in Microsoft Defender for Cloud. Which operating systems and platforms can you monitor? To answer, select the appropriate options in the answer area.

Answer:



NEW QUESTION: 96
You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.
Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 20.04.
You create a service endpoint for Microsoft. Storage in Subnet1.
You need to ensure that when you deploy Docker containers to VM1, the containers can access Azure Storage resources by using the service endpoint.
What should you do on VM1 before you deploy the container?
A. Create an application security group and a network security group (NSG).
B. Edit the docker-compose.ym1 file.
C. Install the container network interface (CNI) plug-in.
Answer: (SHOW ANSWER)

NEW QUESTION: 97
From the Azure portal, you are configuring an Azure policy.
You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects.
Which effect requires a managed identity for the assignment?
A. AuditIfNotExist
B. Append
C. DeployIfNotExist
D. Deny
Answer: (SHOW ANSWER)
When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.
References:
https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources

NEW QUESTION: 98
You have an Azure Active Directory (Azure AD) tenant that contains a user named Admin1.
Admin1 is assigned the Application developer role.
You purchase a cloud app named App1 and register App1 in Azure AD.
Admin1 reports that the option to enable token encryption for App1 is unavailable.
You need to ensure that Admin1 can enable token encryption for App1 in the Azure portal.
What should you do?
A. Upload a certificate for App1.
B. Modify the API permissions of App1.
C. Add App1 as an enterprise application.
D. Assign Admin1 the Cloud application administrator role.
Answer: (SHOW ANSWER)
This is a tricky one because uploading a certificate is also required. However, the question states that the Token Encryption option is unavailable. This is because the app is not added as an enterprise application.
When the app is added as an enterprise application, the Token Encryption option will be available. Then you can upload the certificate.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/howto-saml-token-encryption

NEW QUESTION: 99
You network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.

Name	Source
User1	Azure AD
User2	Azure AD
User3	On-premises Active Directory

The tenant contains the groups shown in the following table.

Name	Members
Group1	User1, User2, User3
Group2	User2

You configure a multi-factor authentication (MFA) registration policy that and the following settings:
* Assignments:
* Include: Group1
* Exclude Group2
Controls: Require Azure MFA registration

Enforce Policy: On

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

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	○	○
User2 must configure MFA during the user's next Azure AD authentication.	○	○
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	○	○

Answer:

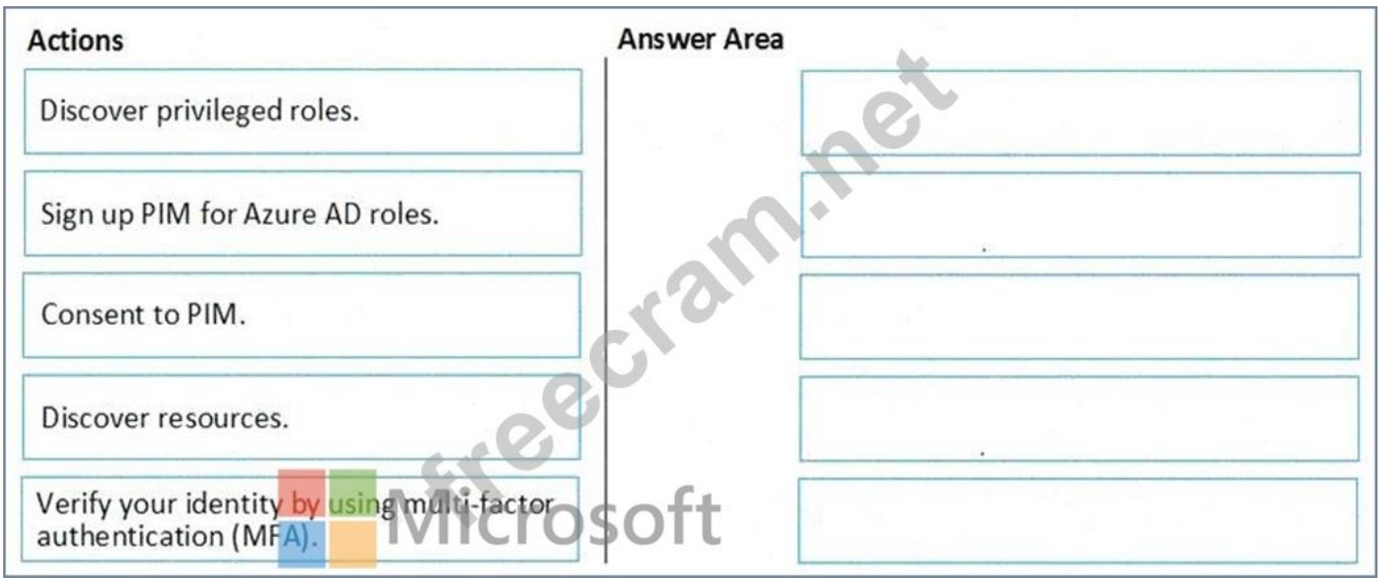
Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	○	○
User2 must configure MFA during the user's next Azure AD authentication.	○	○
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	○	○

NEW QUESTION: 100

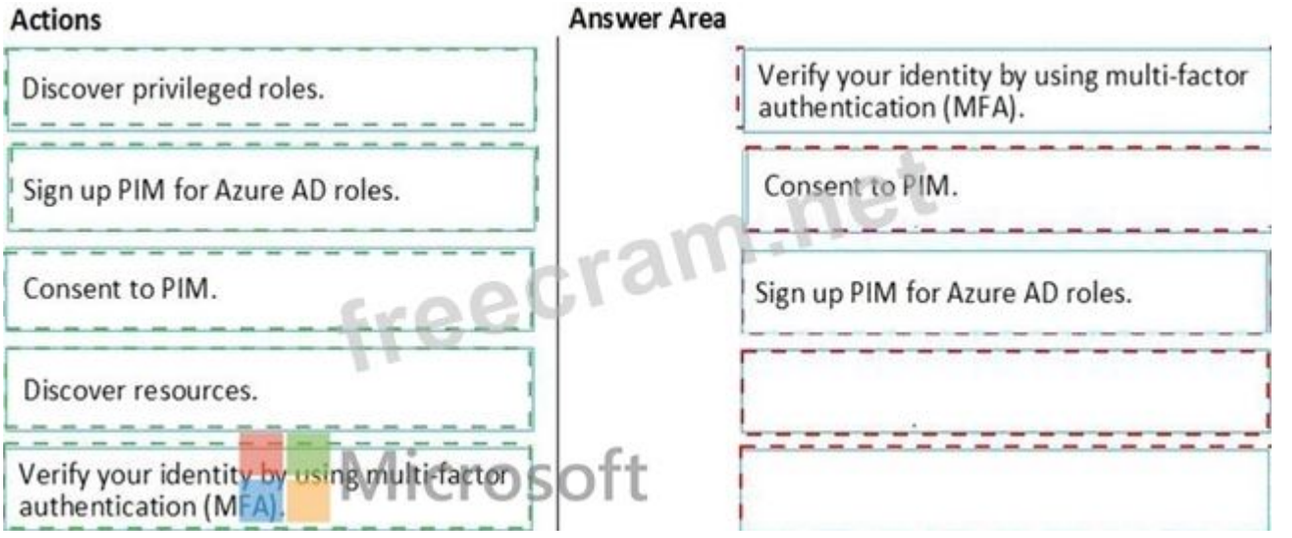
You create an Azure subscription with Azure AD Premium P2.

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: 101

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: (SHOW ANSWER)

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: 102
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: (SHOW ANSWER)
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: 103
You have a Microsoft Sentinel deployment.
You need to connect a third-party security solution to the deployment.
The third-party solution will send Common Event Format (CER-formatted messages.

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

NOTE: Each correct selection is worth one point.

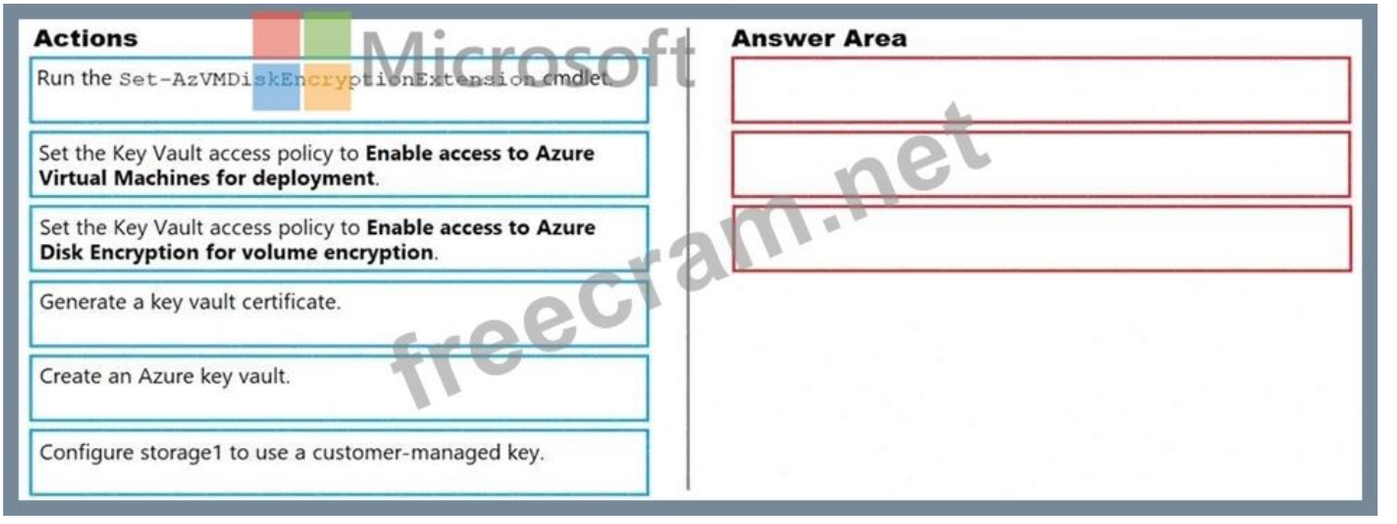
Answer:

NEW QUESTION: 104

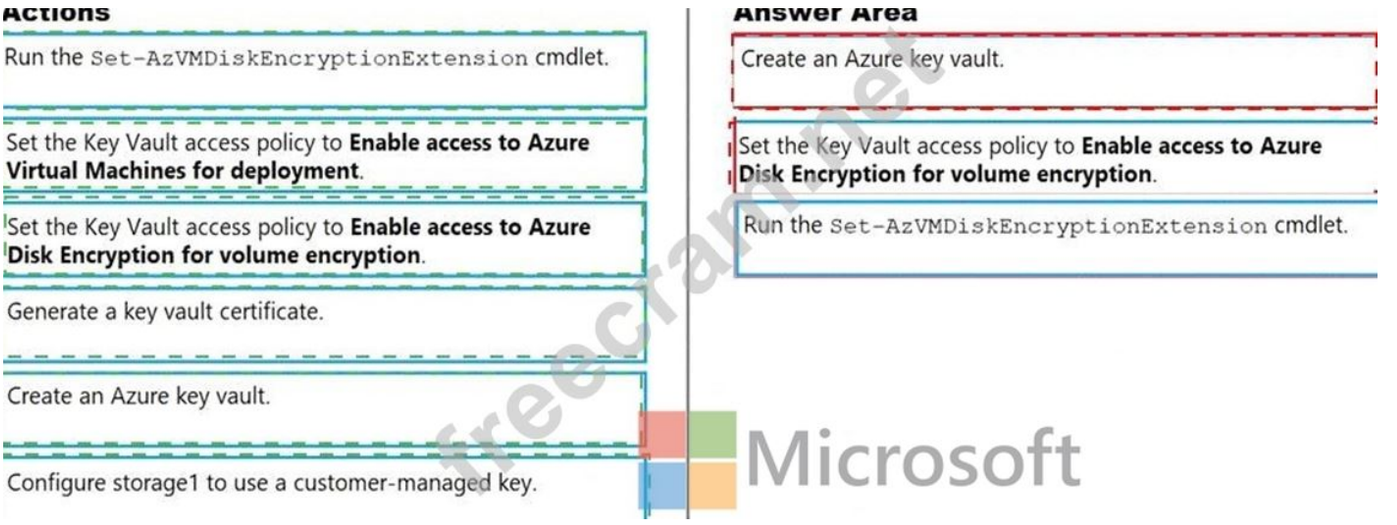
You have an Azure Storage account named storage1 and an Azure virtual machine named VM1. VM1 has a premium SSD managed disk.

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.



Answer:



Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

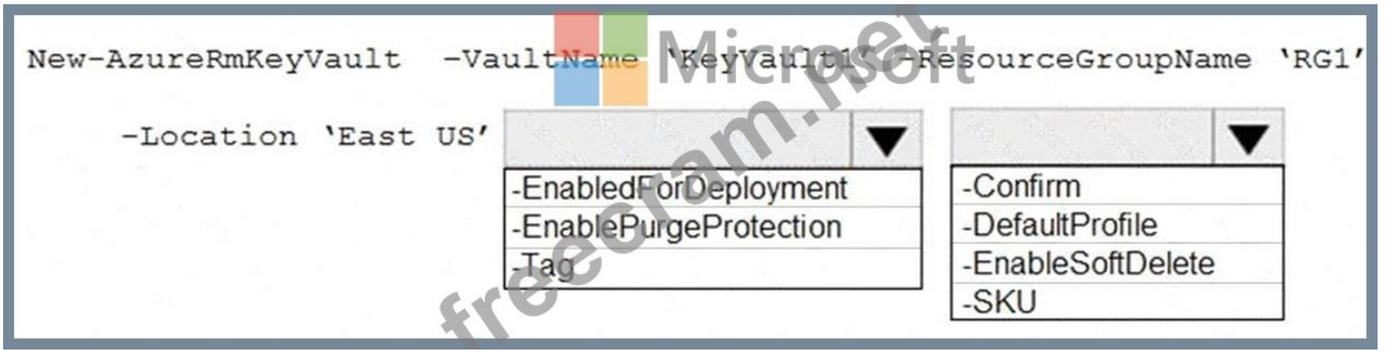
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault

NEW QUESTION: 105

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: 106

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,azurewebsites,net

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

C. Endpoint1. Privatelink,documents,azure,com

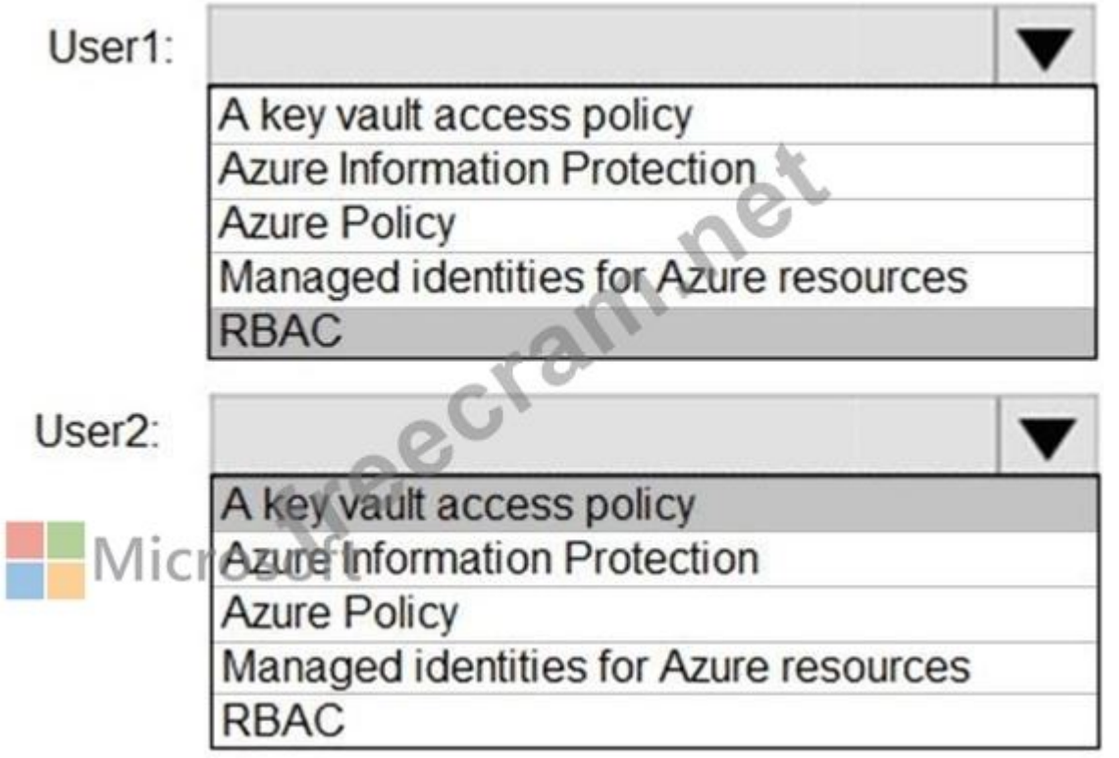
D. Endpoint1. Privatelink,database,azure,com

Answer: (SHOW ANSWER)

NEW QUESTION: 107

You have an Azure key vault.

You need to delegate administrative access to the key vault to meet the following requirements:
* Provide a user named User1 with the ability to set advanced access policies for the key vault.
* Provide a user named User2 with the ability to add and delete certificates in the key vault.
* Use the principle of least privilege.
What should you use to assign access to each user? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Answer:



User1: RBAC
RBAC is used as the Key Vault access control mechanism for the management plane. It would allow a user with the proper identity to:
* set Key Vault access policies
* create, read, update, and delete key vaults
* set Key Vault tags
Note: Role-based access control (RBAC) is a system that provides fine-grained access management of Azure resources. Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs.
User2: A key vault access policy
A key vault access policy is the access control mechanism to get access to the key vault data plane. Key Vault access policies grant permissions separately to keys, secrets, and certificates.
References:
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

NEW QUESTION: 108

You have an Azure subscription.
You configure the subscription to use a different Azure Active Directory (Azure AD) tenant.
What are two possible effects of the change? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. Role assignments at the subscription level are lost.
B. Virtual machine managed identities are lost.
C. Virtual machine disk snapshots are lost.
D. Existing Azure resources are deleted.
Answer: A,B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory

NEW QUESTION: 109
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 machines in RG1 only.
* Connect the virtual machines to the existing virtual networks 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. a custom RBAC role for RG2
B. the Network Contributor role for RG2
C. the Contributor role for the subscription
D. a custom RBAC role for the subscription
E. the Network Contributor role for RG1
F. the Virtual Machine Contributor role for RG1
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

NEW QUESTION: 110
You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Category
Initiative1	Initiative definition	Security Center
Initiative2	Initiative definition	My Custom Category
Policy1	Policy definition	Security Center
Policy2	Policy definition	My Custom Category

You need to identify which initiatives and policies you can add to Subscription1 by using Azure Security Center.
What should you identify?
A. Policy1 and Policy2 only
B. Initiative1 only
C. Initiative1 and Initiative2 only
D. Initiative1, Initiative2, Policy1, and Policy2
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/security-center/custom-security-policies

NEW QUESTION: 111
You have an Azure subscription named Subscription1.
You deploy a Linux virtual machine named VM1 to Subscription1.
You need to monitor the metrics and the logs of VM1.
D18912E1457D5D1DDCBD40AB3BF70D5D
What should you use?
A. Linux Diagnostic Extension (LAD) 3.0
B. Azure HDInsight
C. the AzurePerformanceDiagnostics extension
D. Azure Analysis Services
Answer: (SHOW ANSWER)

NEW QUESTION: 112
You have an Azure subscription that uses Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
A PIM user that is assigned the User Access Administrator role reports receiving an authorization error when performing a role assignment or viewing the list of assignments.
You need to resolve the issue by ensuring that the PIM service principal has the correct permissions for the subscription. The solution must use the principle of least privilege.
Which role should you assign to the PIM service principle?
A. Resource Policy Contributor
B. User Access Administrator
C. Contributor
D. Managed Application Operator

Answer: (SHOW ANSWER)

NEW QUESTION: 113
You have an Azure subscription that contains an Azure SQL server named sqlsrv1 and an Azure SQL database named DB1. Sqlsrv1 is configured for Microsoft Entra authentication only.
You have the Microsoft Entra identities shown in the following table.

Name	Type	Description	Role for DB1
User1	User	*None*	db_owner
User2	User	Member of Group1	*None*
User3	User	Member of Group2	*None*
Group1	Group	User2 and Group2 are members	db_owner
Group2	Group	Member of Group1	*None*

Which users can create scoped credentials for DB1?
A. User1, User2, and User3
B. User1 only
C. User1 and User2 only
Answer: (SHOW ANSWER)

NEW QUESTION: 114
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: (SHOW ANSWER)
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: 115
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 Security Center
B. Azure Monitor
C. Azure Policy
D. Azure Service Health
Answer: C (LEAVE A REPLY)

NEW QUESTION: 116
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.
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: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall

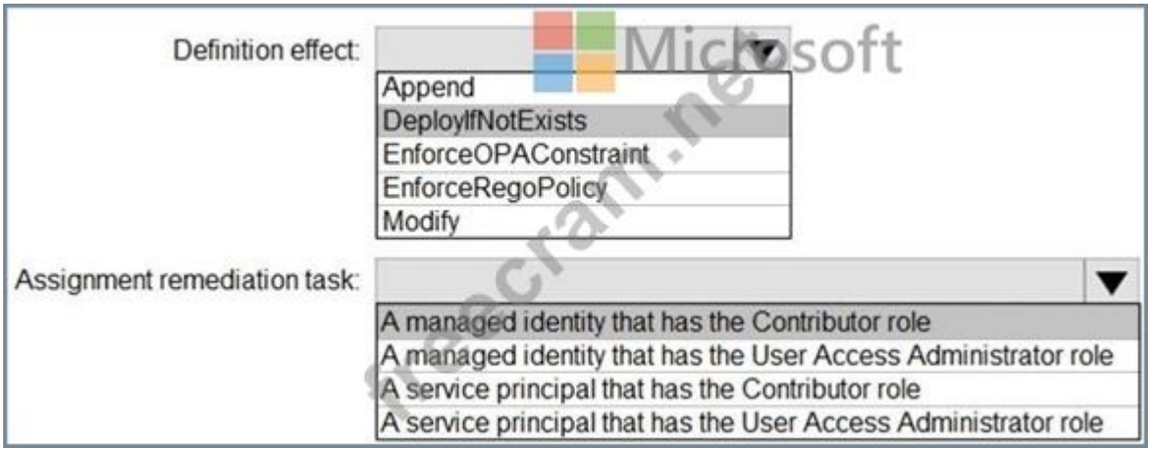
NEW QUESTION: 117
You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit.
(Click the Exhibit tab.)
BASICS

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

You plan to deploy the cluster to production. You disable HTTP application routing.
You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address.
What should you do?
A. Create an AKS Ingress controller.

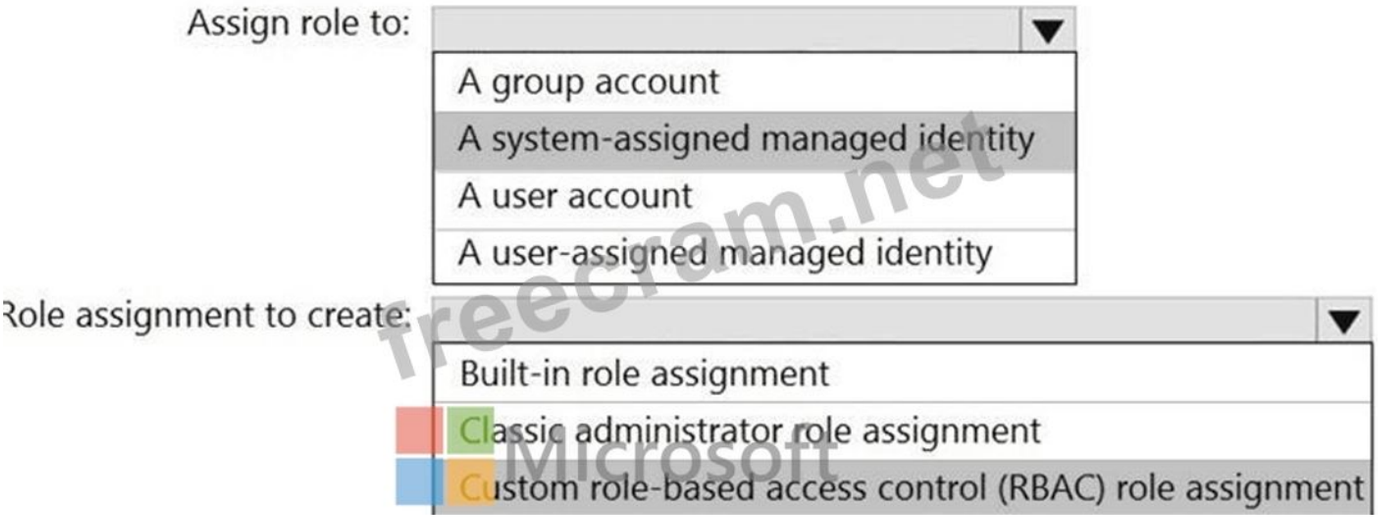
B. Install the container network interface (CNI) plug-in.
C. Create an Azure Standard Load Balancer.
D. Create an Azure Basic Load Balancer.
Answer: (SHOW ANSWER)
An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.
References:
https://docs.microsoft.com/en-us/azure/aks/ingress-tls

NEW QUESTION: 118
You have an Azure subscription.
You need to create and deploy an Azure policy that meets the following requirements:
* When a new virtual machine is deployed, automatically install a custom security extension.
* Trigger an autogenerated remediation task for non-compliant virtual machines to install the extension.
What should you include in the policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Answer:



Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources

NEW QUESTION: 119
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:



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: 120
You are implementing an Azure Application Gateway web application firewall (WAF) named WAF1.
You have the following Bicep code snippet.
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:

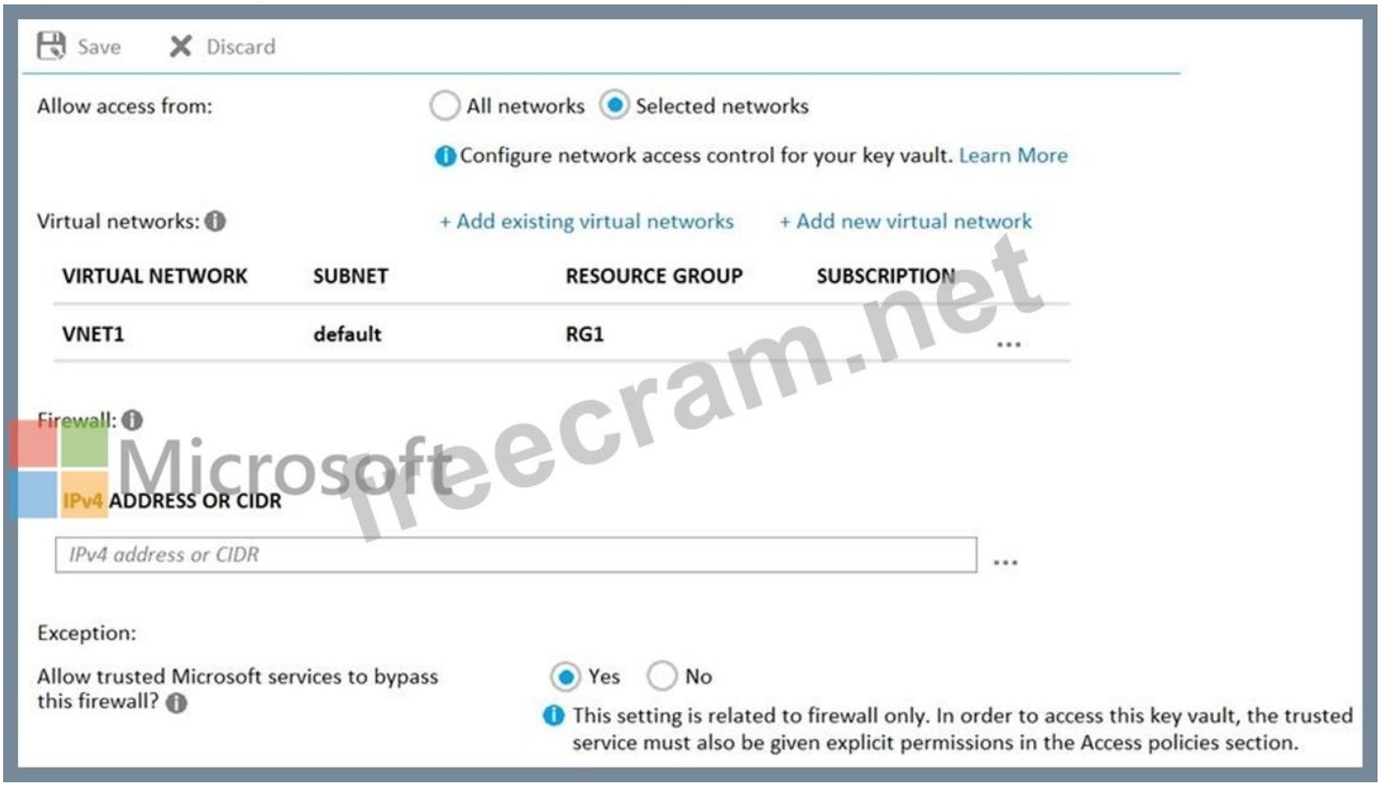
Explanation:

NEW QUESTION: 121
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Subscription. The subscription contains 50 virtual machines that run Windows Server
2012 R2 or Windows Server 2016.
You need to deploy Microsoft Antimalware to the virtual machines.
Solution: You add an extension to each virtual machine.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)
You can use Visual Studio to enable and configure the Microsoft Antimalware service. This entails selecting Microsoft Antimalware extension from the dropdown list under Installed Extensions and click Add to configure with default antimalware configuration.
References:
https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

NEW QUESTION: 122
You have an Azure subscription named Subcription1 that contains an Azure Active Directory (Azure AD) tenant named contosos.com and a resource group named RG1.

You create a custom role named Role1 for contoso.com.
You need to identify where you can use Role1 for permission delegation.
What should you identify?
A. contoso.com only
B. contoso.com and RGT only
C. contoso.com and Subscription1 only
D. contoso.com, RG1, and Subcription1
Answer: (SHOW ANSWER)
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

NEW QUESTION: 123
You have an Azure subscription that contains an Azure key vault named KeyVault1 and the virtual machines shown in the following table.
You set the Key Vault access policy to Enable access to Azure Disk Encryption for volume encryption.
KeyVault1 is configured as shown in the following exhibit.



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

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

Answer:

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

NEW QUESTION: 124

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. App roles

B. Roles and administrators

C. Users and groups

D. API permissions

Answer: (SHOW ANSWER)

NEW QUESTION: 125

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

You create users and assign them roles as shown in the following table.

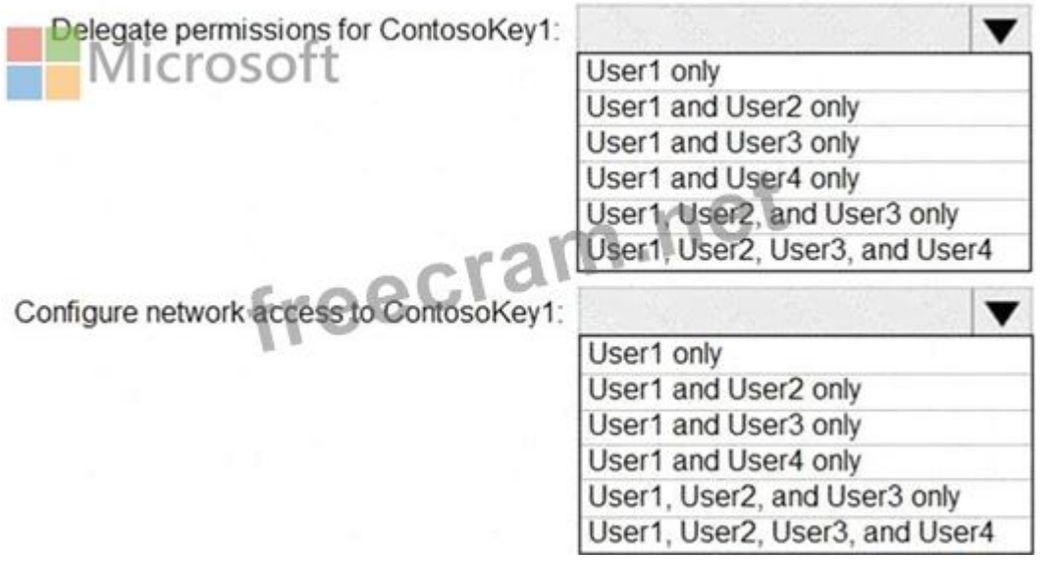
You need to identify which users can perform the following actions:

* Delegate permissions for ContsosKey1.

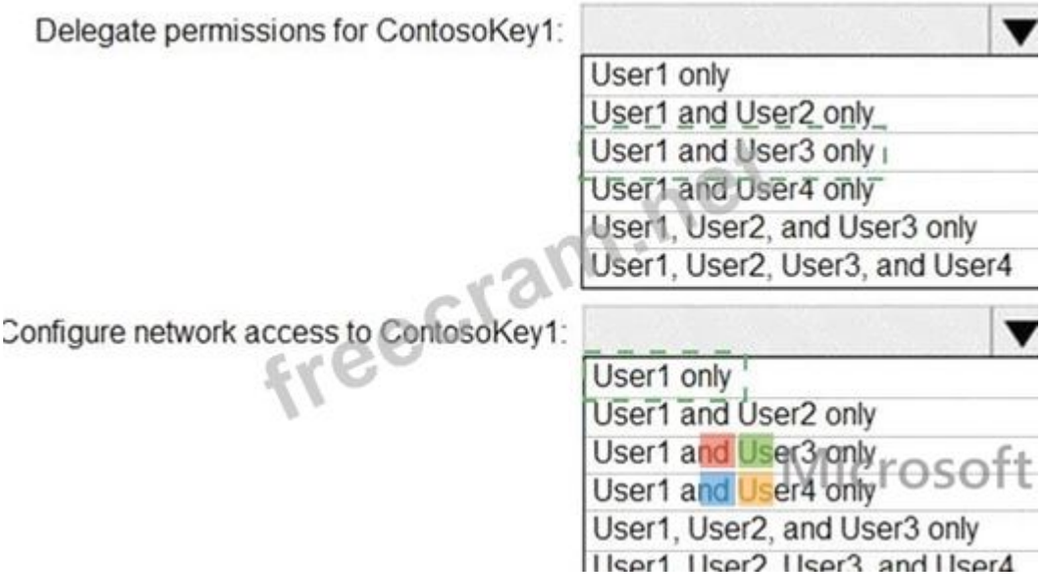
* Configure network access to ContosoKey1.

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

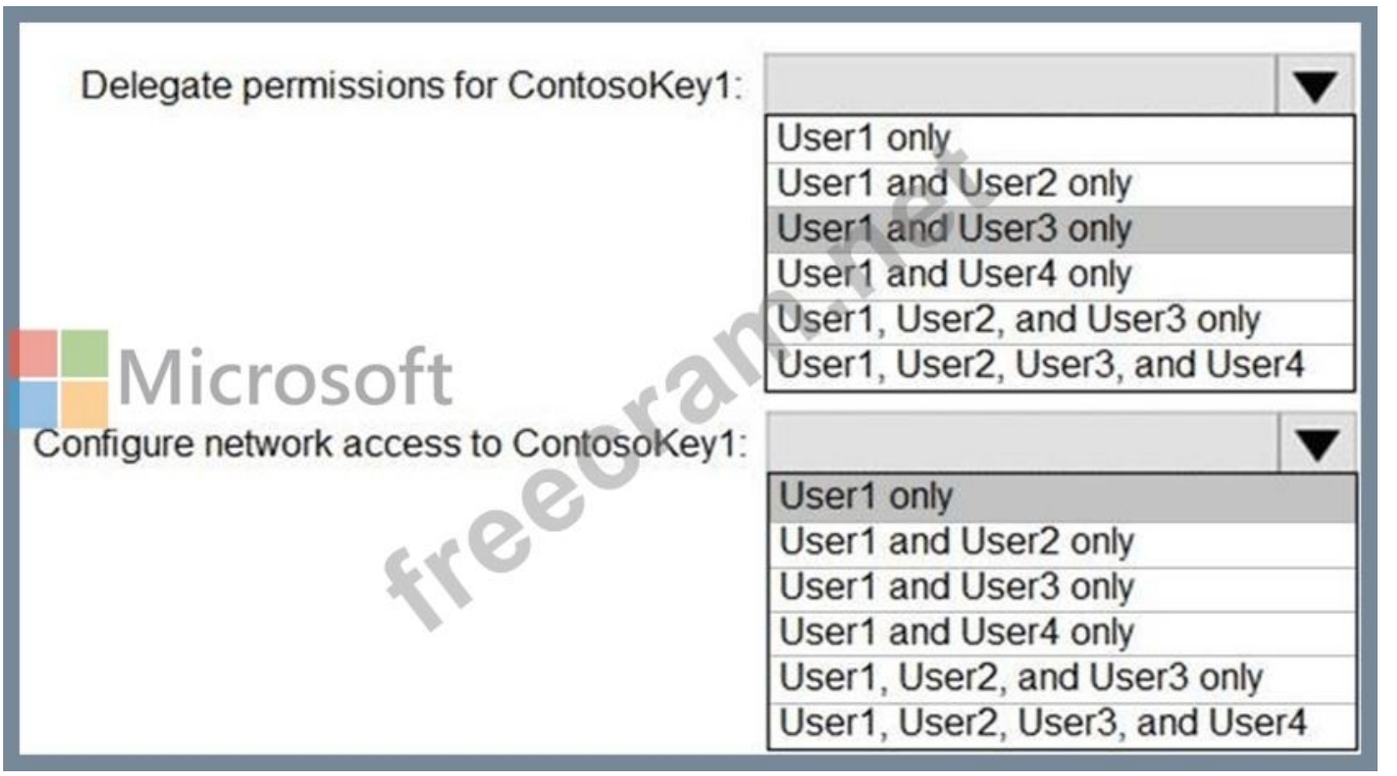
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



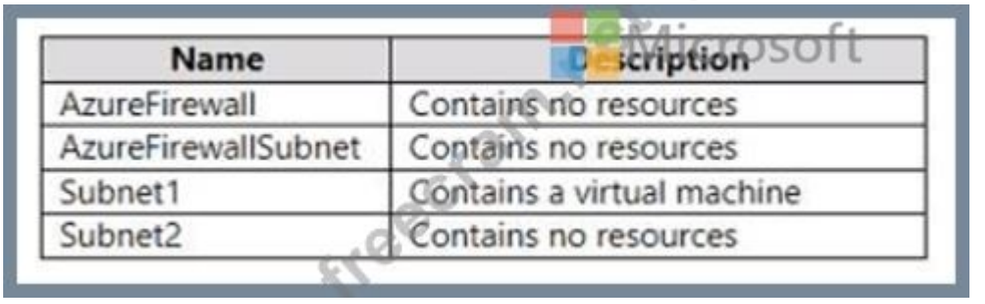
Reference:
https://docs.microsoft.com/en-gb/azure/key-vault/general/rbac-guide

NEW QUESTION: 126

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

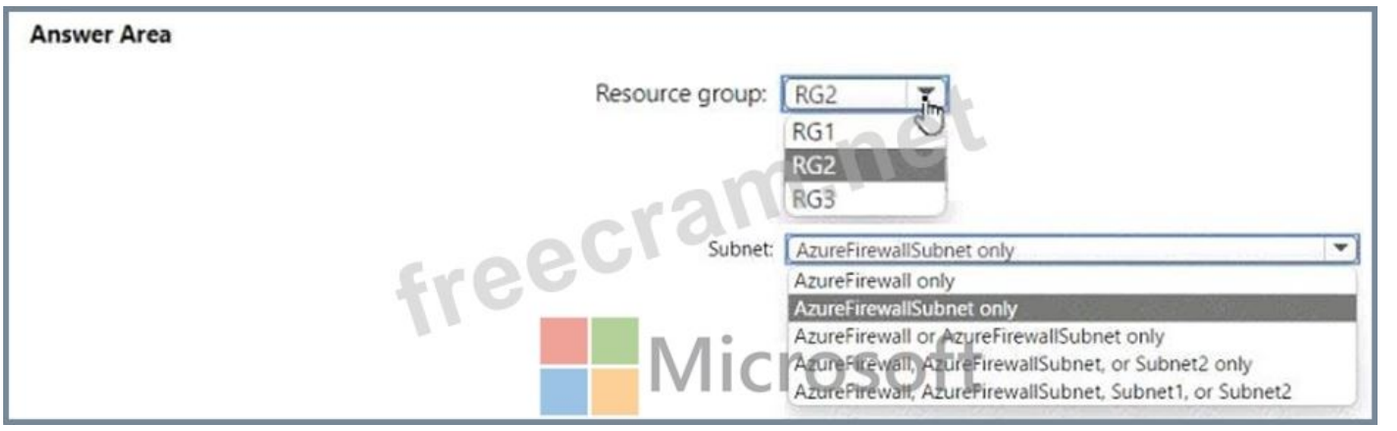
Name	Type	Location	In resource group
RG1	Resource group	East US	*Not applicable*
RG2	Resource group	West US	*Not applicable*
RG3	Resource group	Central US	*Not applicable*
VNet1	Virtual network	Central US	RG2

VNet1 contains the subnets shown in the following table.

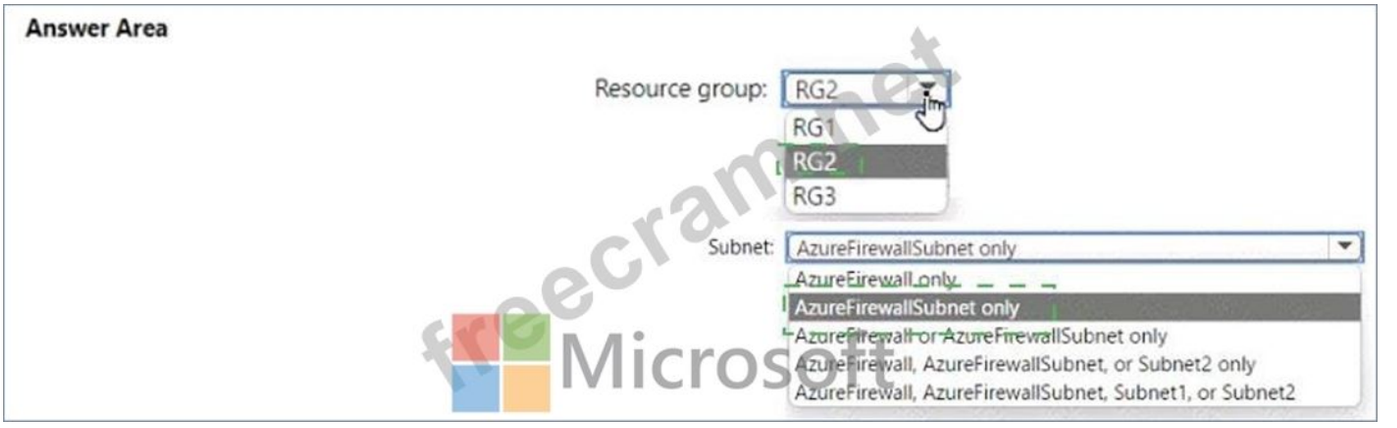


Name	Description
AzureFirewall	Contains no resources
AzureFirewallSubnet	Contains no resources
Subnet1	Contains a virtual machine
Subnet2	Contains no resources

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:



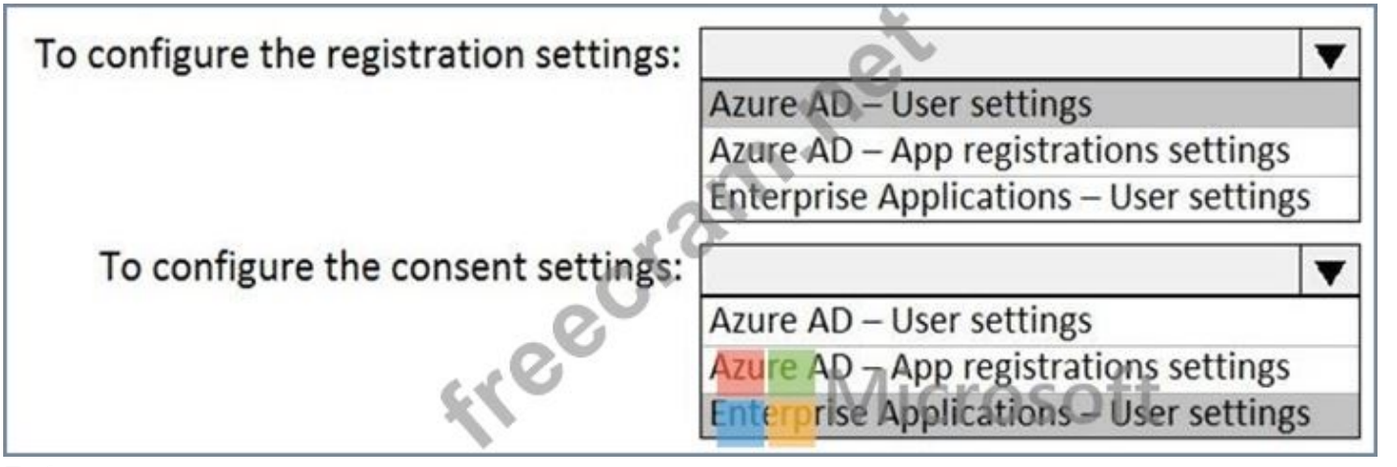
NEW QUESTION: 127

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.

Answer:



Reference:

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

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: 128

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: (SHOW ANSWER)

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime

NEW QUESTION: 129

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: 130
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:

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

Explanation:

NEW QUESTION: 131

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 regenerate the Azure storage account access keys.

Does this meet the goal?

A. Yes

B. No

Answer: A (LEAVE A REPLY)

Generating new storage account keys will invalidate all SAS's that were based on the previous keys.

NEW QUESTION: 132

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

You have an Amazon Web Services (AWS) account.

You need to ensure that when you deploy a new AWS Elastic Compute Cloud (EC2) instance, the Microsoft Defender for Servers agent installs automatically.
What should you configure first?
A. the log Analytics agent
B. the Azure Monitor agent
C. the classic cloud connector
D. the native cloud connector
Answer: (SHOW ANSWER)

NEW QUESTION: 133
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: (SHOW ANSWER)

NEW QUESTION: 134
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 function app
C. a playbook
D. a runbook
Answer: (SHOW ANSWER)

NEW QUESTION: 135
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center for the centralized policy management of three Azure subscriptions.
You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create an initiative and an assignment that is scoped to a management group.
Does this meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
References:
https://docs.microsoft.com/en-us/azure/governance/policy/overview

NEW QUESTION: 136
You have three on-premises servers named Server1, Server2, and Server3 that run Windows Server1 and Server2 and located on the Internal network. Server3 is located on the premises network. All servers have access to Azure.
From Azure Sentinel, you install a Windows firewall data connector.
You need to collect Microsoft Defender Firewall data from the servers for Azure Sentinel.
What should you do?
A. Create an event subscription from Server1, Server2 and Server3
B. Install the On-premises data gateway on each server.
C. Install the Microsoft Agent on each server.
D. Install the Microsoft Agent on Server1 and Server2 install the on-premises data gateway on Server3.
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall

NEW QUESTION: 137
Lab Task
Task 4
You need to ensure that when administrators deploy resources by using an Azure Resource Manager template, the deployment can access secrets in an Azure key vault named KV31330471.
Answer:
see the task answer with step by step below:

* Grant permission to the application that is used to deploy the resources to access the secrets in the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to assign the Key Vault Secrets User role to the application at the scope of the key vault or individual secrets.
* Enable template deployment for the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to set the enabledForTemplateDeployment property of the key vault to true.
* Reference the secrets in the template by using their resource ID. You can use the listSecrets function to get the resource ID of a secret in the key vault. You need to specify the name of the key vault and the name of the secret as parameters.
* Deploy the template by using Azure PowerShell, Azure CLI, or REST API. You can use the New- AzResourceGroupDeployment cmdlet, the az deployment group create command, or the Deployments - Create Or Update REST API to do this. You need to provide the template file or URI and any required parameters.

NEW QUESTION: 138
You create resources in an Azure subscription as shown in the following table.

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

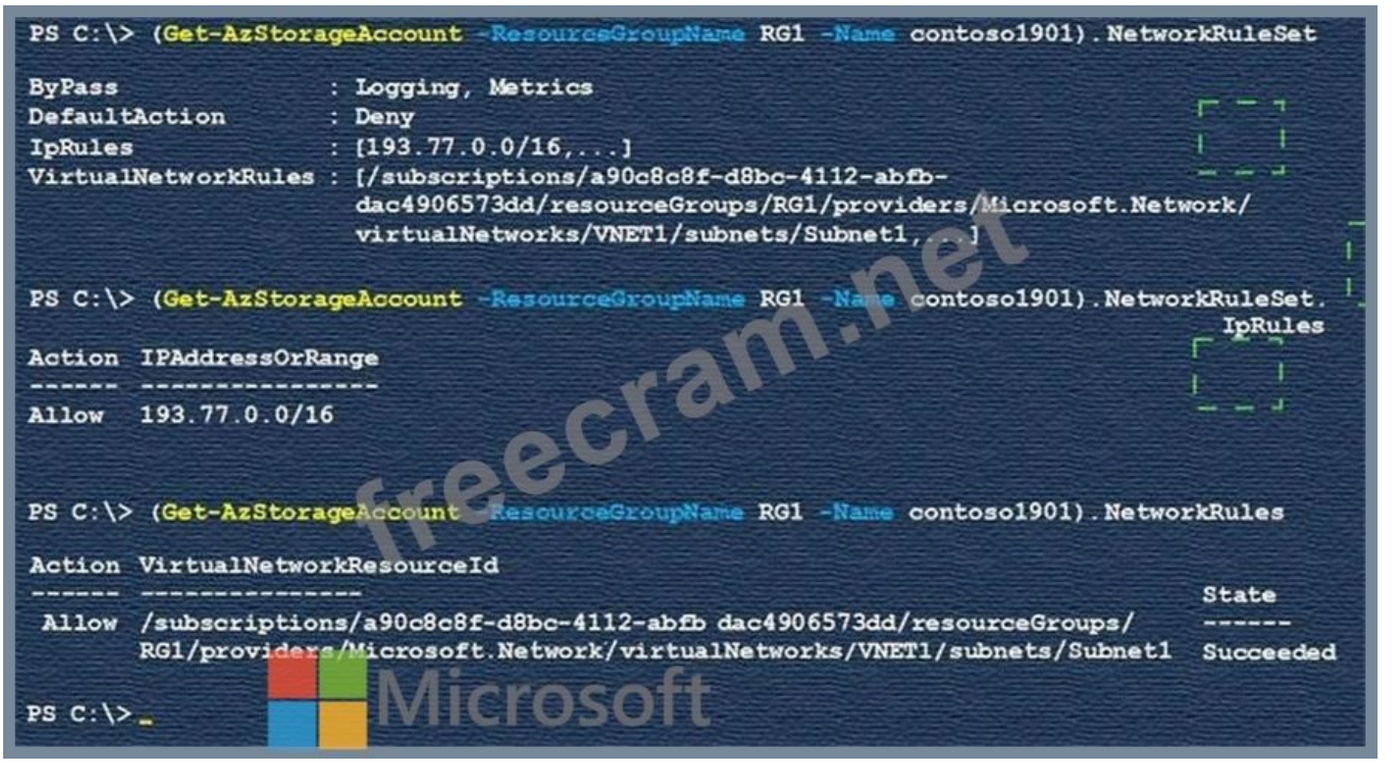
VNET1 contains two subnets named Subnet1 and Subnet2. Subnet1 has a network ID of 10.0.0.0/24. Subnet2 has a network ID of 10.1.1.0/24.
Contoso1901 is configured as shown in the exhibit. (Click the Exhibit tab.)

```
PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet

ByPass              : Logging, Metrics
DefaultAction       : Deny
IpRules             : [193.77.0.0/16,...]
VirtualNetworkRules : [/subscriptions/a90c8c8f-d8bc-4112-abfb-
                      dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/
                      virtualNetworks/VNET1/subnets/Subnet1,...]

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet.
                                                                          IpRules

Action  IPAddressOrRange
------  ----------------
Allow   193.77.0.0/16


PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRules

Action  VirtualNetworkResourceId                                                  State
------  --------------------------------------------------------------------------------
 Allow  /subscriptions/a90c8c8f-d8bc-4112-abfb dac4906573dd/resourceGroups/      ------
        RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1   Succeeded

PS C:\>_
```

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

NOTE: Each correct selection is worth one point.

Answer:



Explanation:

Box 1: Yes

Access from Subnet1 is allowed.

Box 2: No

No access from Subnet2 is allowed.

Box 3: Yes

Access from IP address 193.77.10.2 is allowed.

NEW QUESTION: 139

You have an Azure subscription named Sub1.

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

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

What should you use to modify WF1?

A. Azure Application Insights
B. Azure Monitor
C. Azure Logic Apps Designer
D. Azure DevOps
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation
https://docs.microsoft.com/en-us/learn/modules/resolve-threats-with-azure-security-center/6-exerciseconfigure-playbook

NEW QUESTION: 140
Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD).
The Azure AD tenant contains the users shown in the following table.

Name	Source	Password
User1	Azure AD	Adatum123
User2	Azure AD	N3w3rT0Gue33
User3	On-premises Active Directory	ComplexPassword33

You configure the Authentication methods - 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.

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!.	○	○

Answer:

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!.	○	○

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

NEW QUESTION: 141
You have an Azure subscription that is linked to an Azure AD tenant and contains the resources shown in the following table.

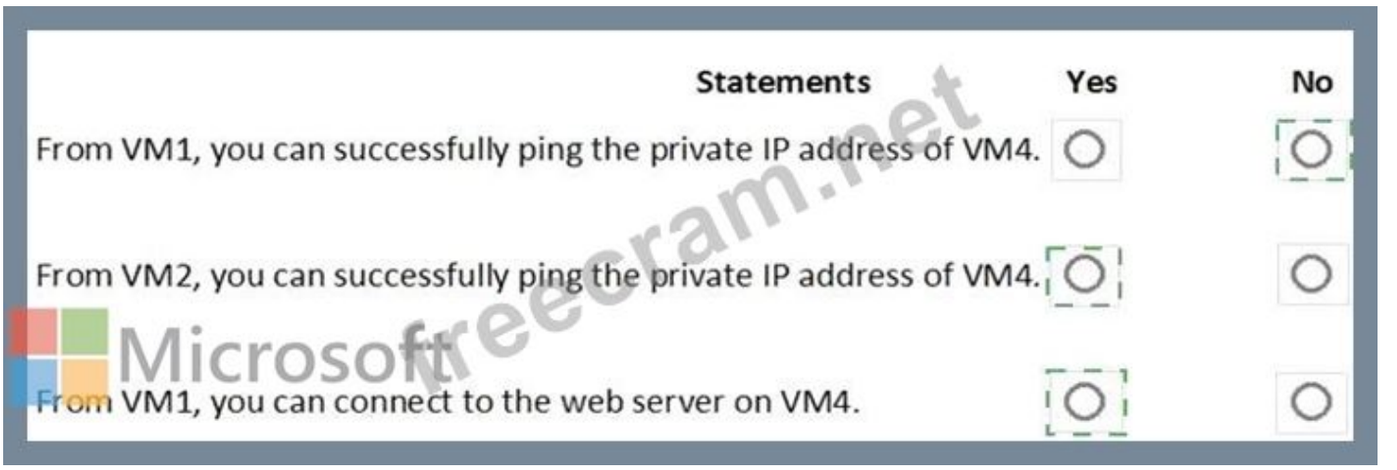
Name	Location	Description
Group1	*Not applicable*	Dynamic device security group in Azure AD
Managed1	East US	Managed identity
VM1	West US	Virtual machine that has a system-assigned managed identity
VM2	Central US	Virtual machine
App1	*Not applicable*	Enterprise application in Azure AD

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

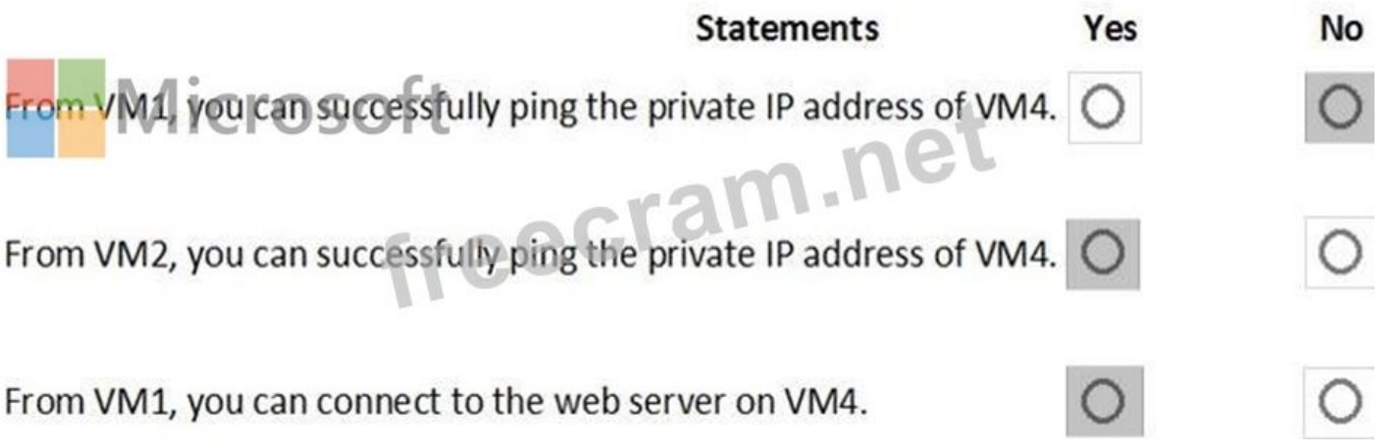
NEW QUESTION: 142
You are evaluating the effect of the application security groups on the network communication between the virtual machines in Sub2.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
From VM1, you can successfully ping the private IP address of VM4.	○	○
From VM2, you can successfully ping the private IP address of VM4.	○	○
From VM1, you can connect to the web server on VM4.	○	○

Answer:



Explanation:



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

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

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

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

Box 2: Yes.

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

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

NEW QUESTION: 143

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. Assign a built-in compliance standard.

B. Create a new custom standard.

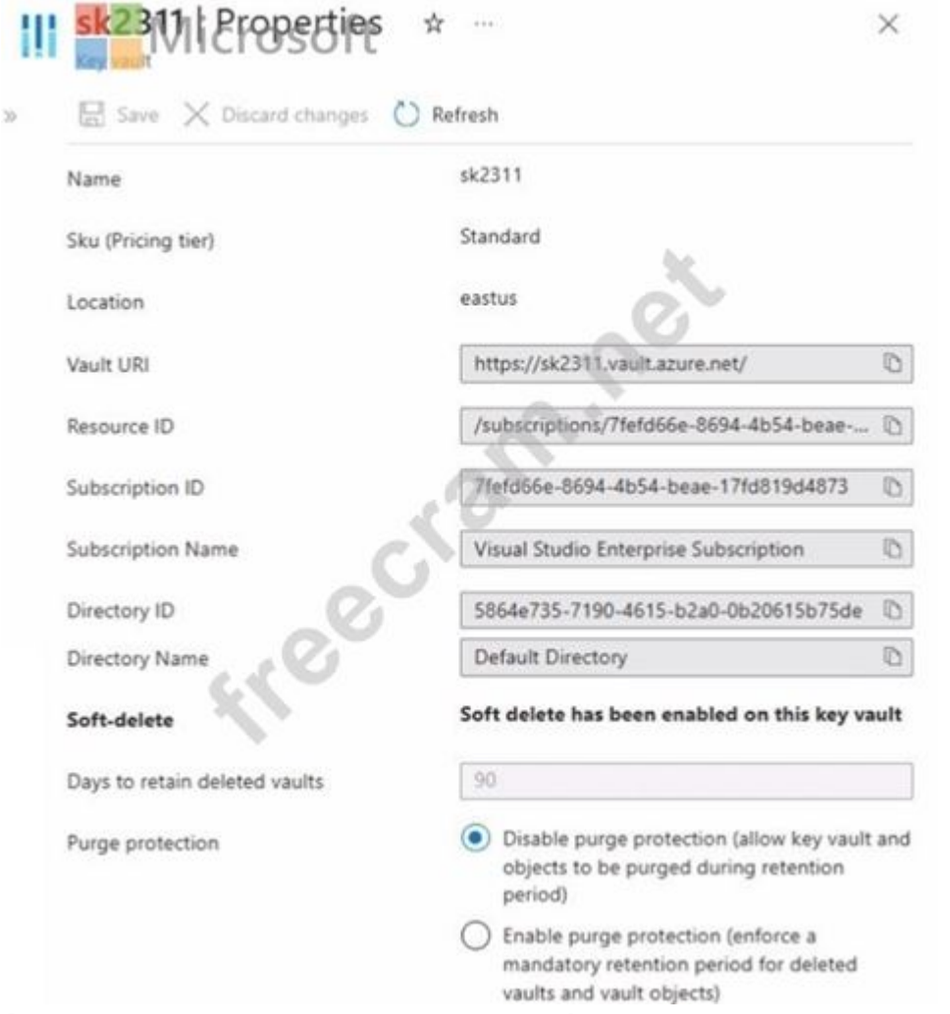
C. Assign a built-in assessment.

D. Create a new customer assessment.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 144

You have an Azure key vault named sk2311 configured as shown in the following exhibit.



Sk2311 contains the items shown in the following table.

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

In sk2311, the following events occur in sequence:

* Item1 is deleted.

* Item2 and Policy1 ate deleted.

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

Answer:

Explanation:

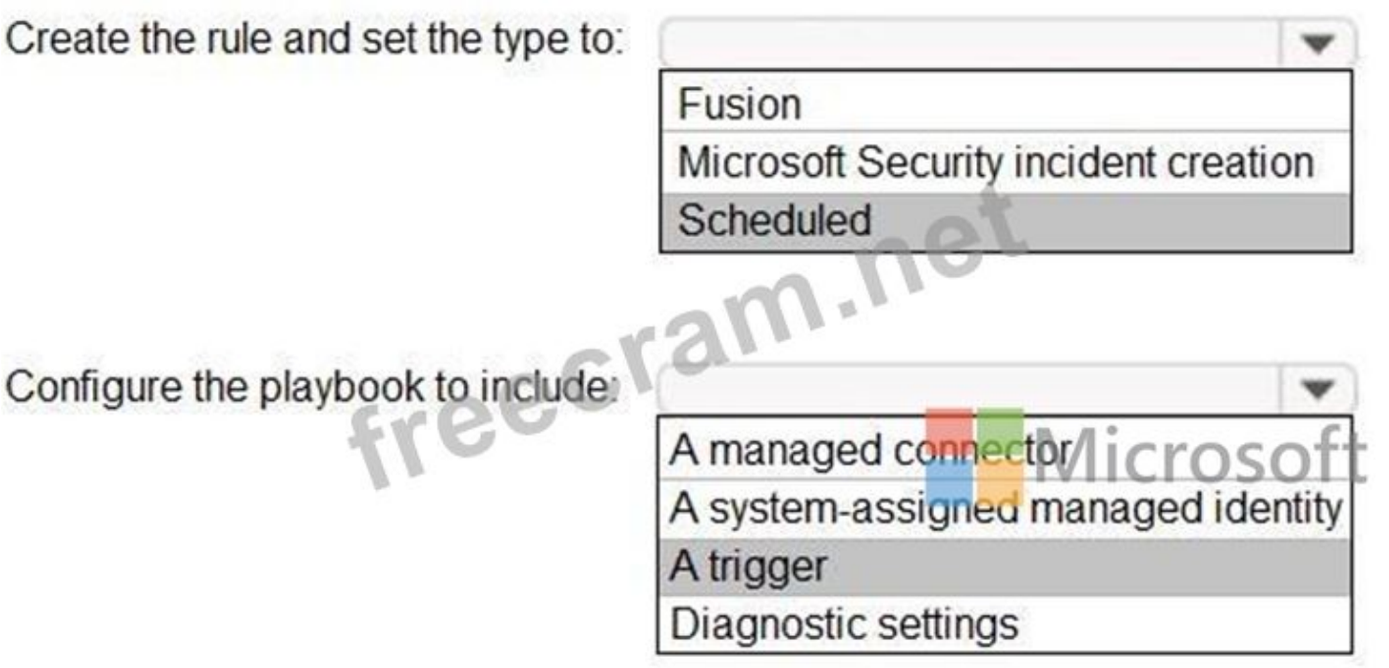
NEW QUESTION: 145
You have an Azure subscription that contains an Azure key vault. The role assignments for the key vault are shown in the following exhibit.
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Answer:
See the answer below at Explanation.
Explanation:
Answer is as image below.

NEW QUESTION: 146

You have an Azure subscription and the computers shown in the following table.
You need to perform a vulnerability scan of the computers by using Microsoft Defender for Cloud.
Which computers can you scan?
A. Server1 and VMSS1.0 only
B. VM1, VM2, and Server1 only
C. VM1 and VM2 only
D. VM1 only
E. VM1, VM2, Server1, and VMSS1.0
Answer: (SHOW ANSWER)

NEW QUESTION: 147
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:



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: 148
From Azure Security, you create a custom alert rule.
You need to configure which users will receive an email message when the alert is triggered.

What should you do?
A. From Azure Monitor, create an action group.
B. From Security Center, modify the Security policy settings of the Azure subscription.
C. From Azure Active Directory (Azure AD). modify the members of the Security Reader role group.
D. From Security Center, modify the alert rule.
Answer: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups

NEW QUESTION: 149
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: (SHOW ANSWER)
https://learn.microsoft.com/en-us/azure/app-service/configure-authentication-provider-google

NEW QUESTION: 150
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:

Explanation:

NEW QUESTION: 151
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: (SHOW ANSWER)
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/

NEW QUESTION: 152
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: 153
You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1. EASM1 has discovery enabled and contains several inventory assets.
You need to identify which inventory assets are vulnerable to the most critical web app security risks.
Which Defender EASM dashboard should you use?
A. GDPR Compliance
B. Attack Surface Summary
C. OWASP Top 1O
D. Security Posture
Answer: (SHOW ANSWER)

NEW QUESTION: 154
Your network contains an Active Directory forest named contoso.com. You have an Azure Directory (Azure AD) tenant named contoso.com.
You plan to configure synchronization by using the Express Settings installation option in Azure AD Connect.
You need to identify which roles and groups are required to perform the planned configurations. The solution must use the principle of least privilege.
Which two roles and groups should you identify? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. the Domain Admins group in Active Directory
B. the Security administrator role in Azure AD
C. the Global administrator role in Azure AD
D. the User administrator role in Azure AD
E. the Enterprise Admins group in Active Directory
Answer: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

NEW QUESTION: 155
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.
Azure AD Privileged Identity Management (PIM) is enabled for the tenant.
In PIM, the Password Administrator role has the following settings:
* Maximum activation duration (hours): 2
* Send email notifying admins of activation: Disable
* Require incident/request ticket number during activation: Disable

* Require Azure Multi-Factor Authentication for activation: Enable
* Require approval to activate this role: Enable
* Selected approver: Group1

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

Name	Assignment type
User1	Active
User2	Eligible
user3	Eligible

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

Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	○	○
User2 can request to activate the Password Administrator role.	○	○
If User3 wants to activate the Password Administrator role, the user can approve their own request.	○	○

Answer:

Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	○	○
User2 can request to activate the Password Administrator role.	○	○
If User3 wants to activate the Password Administrator role, the user can approve their own request.	○	○

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: 156
You have an Azure subscription linked to an Azure Active Directory Premium Plan 1 tenant.
You plan to implement Azure Active Directory (Azure AD) Identity Protection.
You need to ensure that you can configure a user risk policy and a sign-in risk policy.
What should you do first?
A. Purchase Azure Active Directory Premium Plan 2 licenses for all users.
B. Register all users for Azure Multi-Factor Authentication (MFA).

C. Enable security defaults for Azure AD.
D. Upgrade Azure Security Center to the standard tier.
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa

NEW QUESTION: 157
You have an Azure subscription named Sub1 that contains the Azure key vaults shown in the following table.
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: 158
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. Microsoft Defender for App Service
B. Microsoft Defender for APIs
C. Foundational Cloud Security Posture Management (CSPM)
D. Defender Cloud Security Posture Management (CSPM)
Answer: (SHOW ANSWER)

NEW QUESTION: 159

Lab Task
Task 5
A user named Debbie has the Azure app installed on her mobile device.
You need to ensure that debbie@contoso.com is alerted when a resource lock is deleted.
Answer:
see the task answer with step by step below:
Create an Azure Resource Manager service principal. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to specify a name and a role for the service principal, such as Contributor.
Grant permission to the service principal to access the secrets in the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to assign the Key Vault Secrets User role to the service principal at the scope of the key vault or individual secrets.
Enable template deployment for the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to set the enabledForTemplateDeployment property of the key vault to true.
Reference the secrets in the template by using their resource ID. You can use the listSecrets function to get the resource ID of a secret in the key vault. You need to specify the name of the key vault and the name of the secret as parameters.
Deploy the template by using Azure PowerShell, Azure CLI, or REST API. You can use the New-AzResourceGroupDeployment cmdlet, the az deployment group create command, or the Deployments - Create Or Update REST API to do this. You need to provide the template file or URI and any required parameters. You also need to provide the credentials of the service principal.

NEW QUESTION: 160
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 Azure Defender for the subscription.
Which resources can be protected by using Azure Defender?
A. VM1, VNET1, storage1, and Vault1
B. VM1, VNET1, and storage1 only
C. VM1, storage1, and Vault1 only
D. VM1 and VNET1 only
E. VM1 and storage1 only
Answer: (SHOW ANSWER)

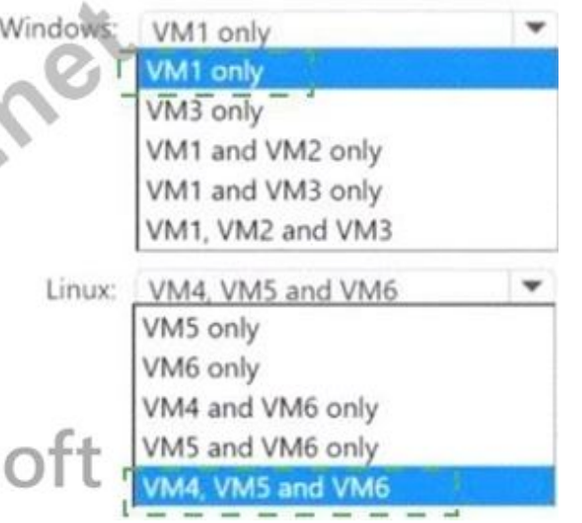
Reference:
https://docs.microsoft.com/en-us/azure/security-center/azure-defender

NEW QUESTION: 161
You have an Azure subscription.
You plan to deploy the virtual machines shown in the following table.

Name	Size	Operating system
VM1	DC4ads_v5	Windows Server 2022 Datacenter: Azure Edition
VM2	D2ads_v5	Windows Server 2022 Standard
VM3	EC4ads_v5	Windows Server 2019 Datacenter
VM4	D2ads_v5	Debian
VM5	EC4ads_v5	Ubuntu Server
VM6	DC4ads_v5	SUSE Linux Enterprise Server

You need to identify the virtual machines and operating systems that can be deployed as confidential virtual machines?
Which Windows virtual machines and which Linux virtual machines should you identify?
Answer Area

Answer:
Answer Area



Explanation:

Answer Area

NEW QUESTION: 162

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

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 Area

Answer:

Answer Area

NEW QUESTION: 163

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 subscription contains the subnets shown in the following table.

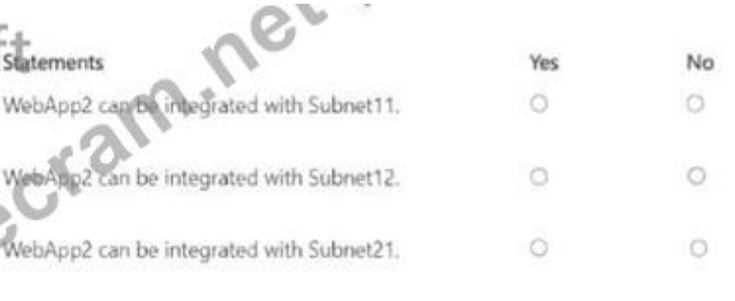
You plan to create an Azure web app named WebApp2 that will have the following configurations:

* Region: East US
* VNet integration: Enabled
* Scale out; Autoscale to up to 10 instances

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



Answer:

NEW QUESTION: 164

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, Cert2, Cert3, and Cert4

B. Cert1 and Cert3 only

C. Cert1 and Cert2 only

D. Cert3 and Cert4 only

Answer: (SHOW ANSWER)

NEW QUESTION: 165

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.

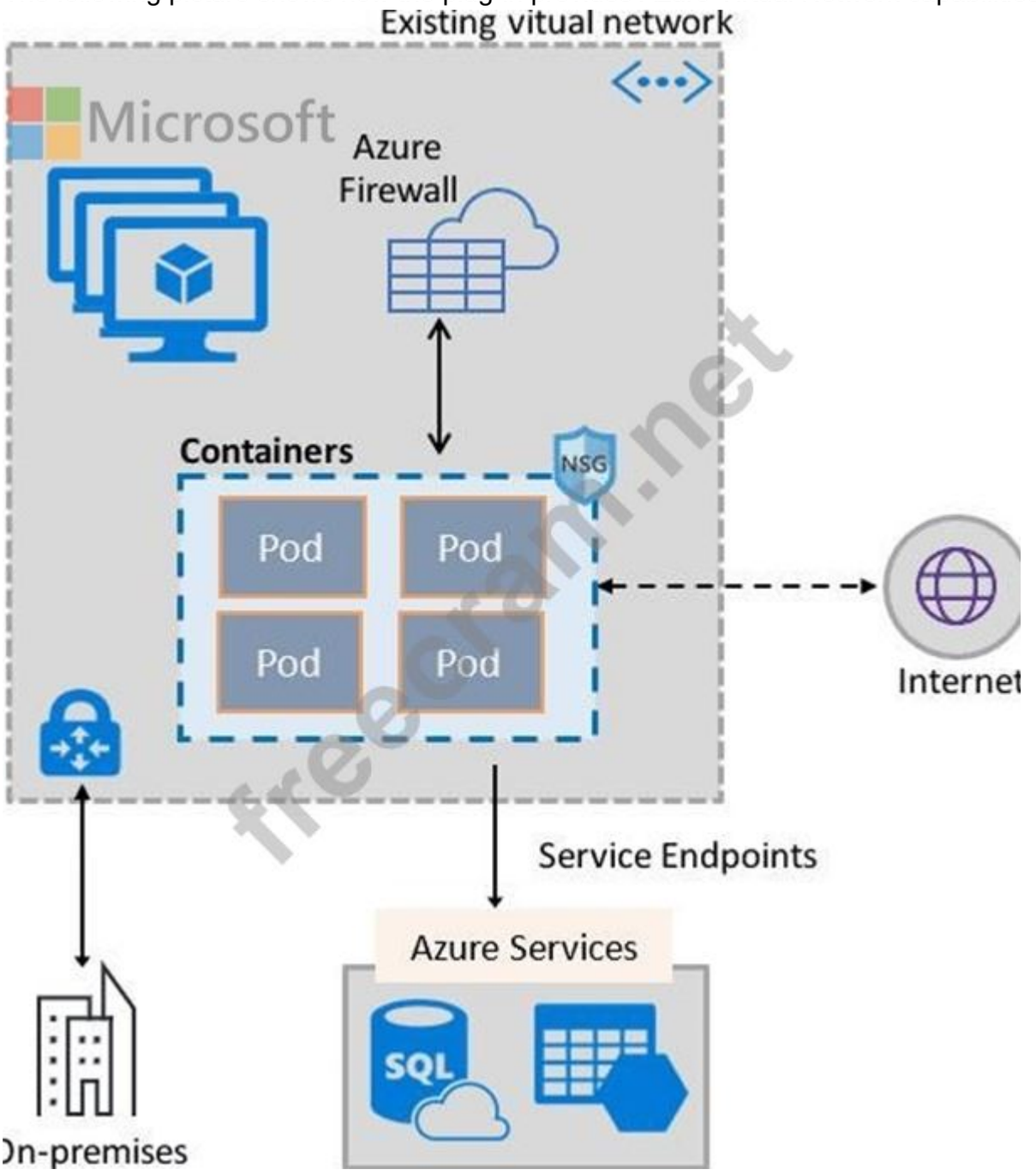
C. Install the container network interface (CNI) plug-in.

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: 166
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:

Explanation:

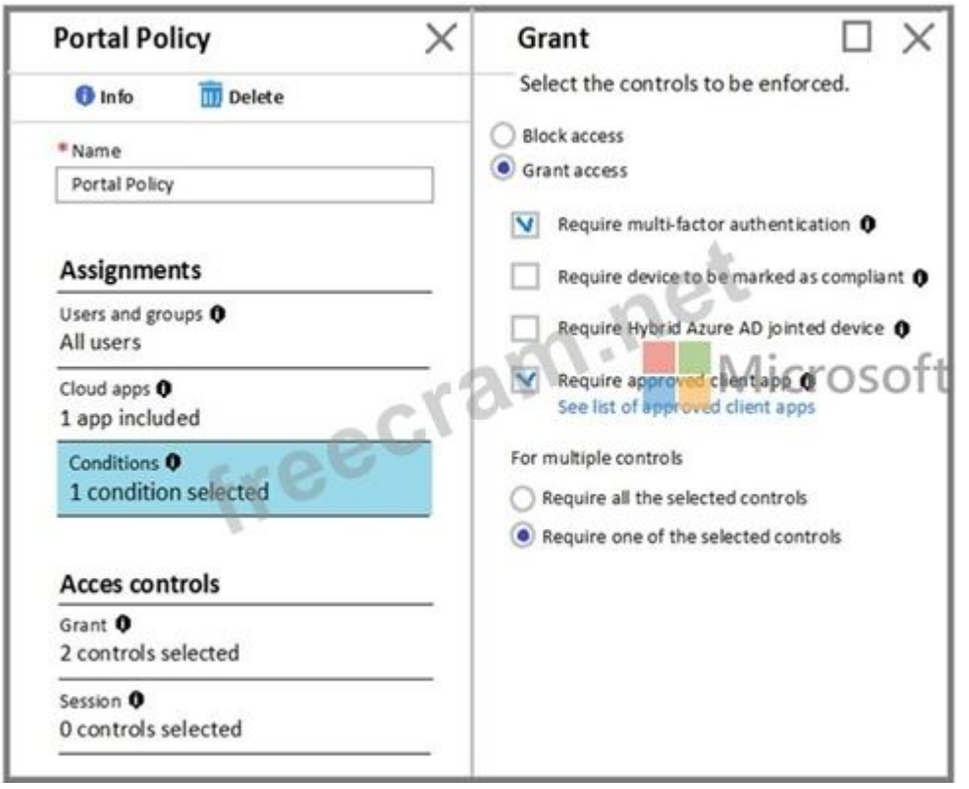
NEW QUESTION: 167
You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Operating system
VM1	Windows Server 2019
VM2	Windows Server 2022
VM3	Server Core installation of Windows Server 2022
VM4	Windows Server 2022 configured with an AppLocker policy

You are configuring Microsoft Defender for Servers.
You plan to enable adaptive application controls to create an allowlist of known-safe apps on the virtual machines. Which virtual machines support the use of adaptive application controls?
A. VM2 and VM4 only
B. VM2 and VM3 only
C. VM1, VM2, VM3, and VM4
D. VM1 and VM2 only
Answer: (SHOW ANSWER)

NEW QUESTION: 168
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: (SHOW ANSWER)
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: 169
You create a new Azure subscription that is associated to a new Azure Active Directory (Azure AD) tenant.
You create one active conditional access policy named Portal Policy. Portal Policy is used to provide access to the Microsoft Azure Management cloud app.
The Conditions settings for Portal Policy are configured as shown in the Conditions exhibit. (Click the Conditions tab.) The Grant settings for Portal Policy are configured as shown in the Grant exhibit. (Click the Grant tab.)



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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	○
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	○	○
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	○

Answer:

Statements	Yes	No
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	○
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	○	○
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	○

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

NEW QUESTION: 170
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: 171
You have an Azure subscription.
You create an Azure web app named Contoso1812 that uses an S1 App service plan.
You create a DNS record for www.contoso.com that points to the IP address of Contoso1812.
You need to ensure that users can access Contoso1812 by using the https://www.contoso.com URL.

Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. Turn on the system-assigned managed identity for Contoso1812.
B. Add a hostname to Contoso1812.
C. Scale out the App Service plan of Contoso1812.
D. Add a deployment slot to Contoso1812.
E. Scale up the App Service plan of Contoso1812.
F. Upload a PFX file to Contoso1812
Answer: (SHOW ANSWER)
B: You can configure Azure DNS to host a custom domain for your web apps. For example, you can create an Azure web app and have your users access it using either www.contoso.com or contoso.com as a fully qualified domain name (FQDN). To do this, you have to create three records:
A root "A" record pointing to contoso.com
A root "TXT" record for verification
A "CNAME" record for the www name that points to the A record
F: To use HTTPS, you need to upload a PFX file to the Azure Web App. The PFX file will contain the SSL certificate required for HTTPS.
References: https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom- Domain

NEW QUESTION: 172
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.

```
{
  "mode": "All",
  "policyRule": {
    "if": {
      "anyOf": [
        {
          "field": "location",
          "notEquals": "[resourceGroup().location]"
        },
        {
          "field": "name",
          "notContains": "obj"
        }
      ]
    },
    "then": {
      "effect": "deny"
    }
  },
  "parameters": {}
}
```


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:

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

Explanation:

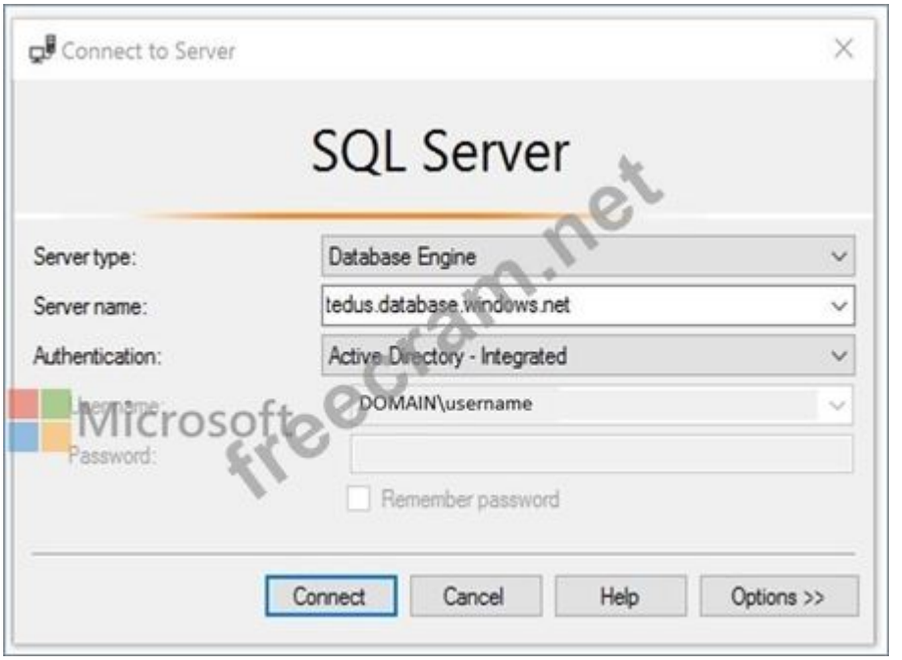
NEW QUESTION: 173

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: 174
You are collecting events from Azure virtual machines to an Azure Log Analytics workspace.
You plan to create alerts based on the collected events
You need to identify which Azure services can be used to create the alerts.
Which two services should you identify? Each correct answer presents a complete solution
NOTE: Each correct selection is worth one point.
A. Azure Monitor
B. Azure Security Center
C. Azure Analytics Services
D. Azure Sentinel
E. Azure Advisor
Answer: (SHOW ANSWER)
https://docs.microsoft.com/en-us/azure/analysis-services/analysis-services-overview

NEW QUESTION: 175
You have an Azure subscription that contains a virtual machine named VM1.
You create an Azure key vault that has the following configurations:
Name: Vault5
Region: West US
Resource group: RG1
You need to use Vault5 to enable Azure Disk Encryption on VM1. The solution must support backing up VM1 by using Azure Backup.
Which key vault settings should you configure?
A. Access policies
B. Secrets
C. Keys
D. Locks
Answer: A (LEAVE A REPLY)
References:
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

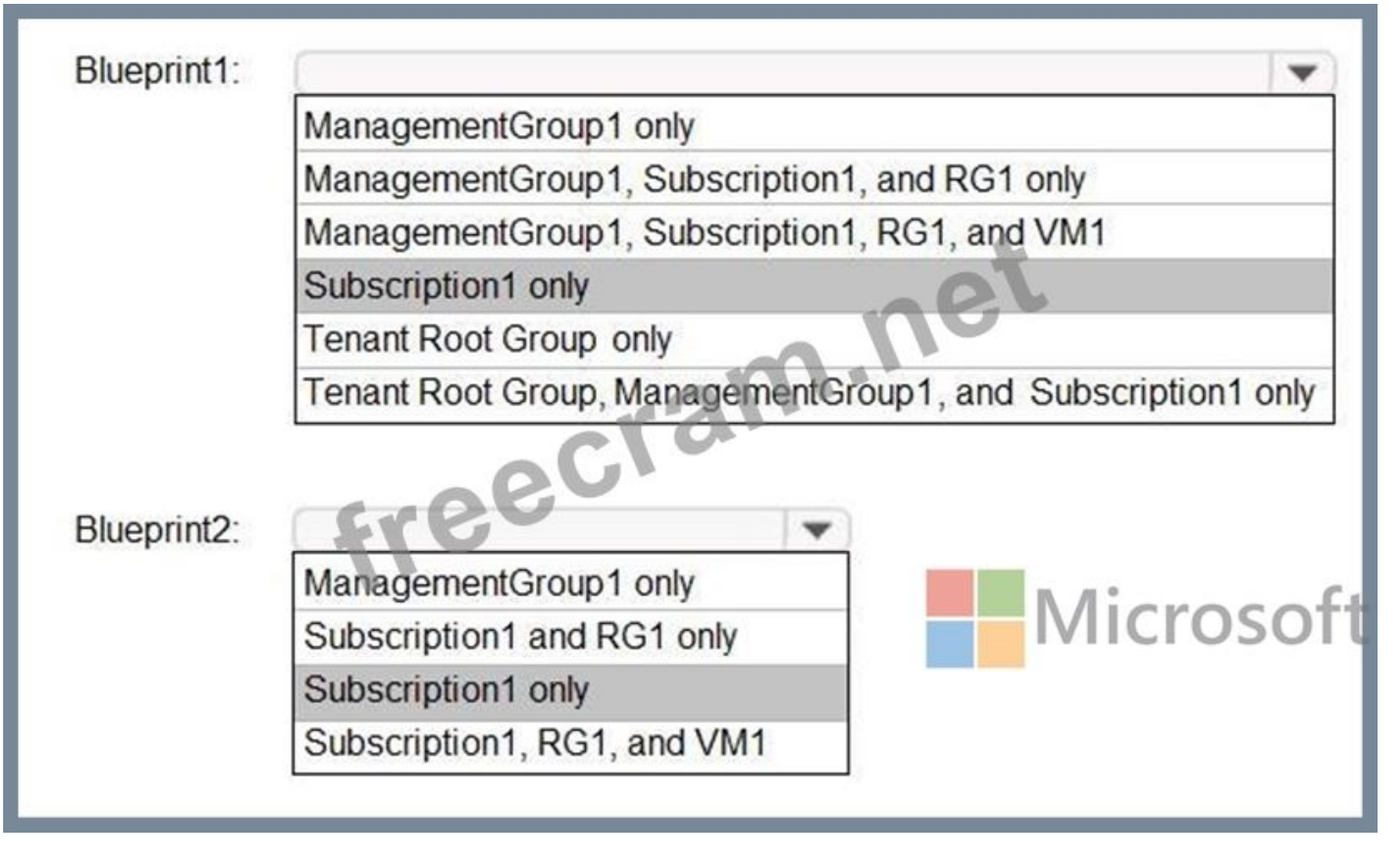
NEW QUESTION: 176
You have an on-premises datacenter that contains multiple servers.
You have an Azure subscription.
You plan to onboard the on-premises servers to Microsoft Defender for Cloud by using a script.
You need to create an identity to enable the script to run without prompting for Microsoft Entra credentials.
Which type of identity should you create?

A. service principal
B. group account
C. user-assigned managed identity
D. user account
E. system-assigned managed identity
Answer: (SHOW ANSWER)

NEW QUESTION: 177
You have the hierarchy of Azure resources shown in the following exhibit.

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

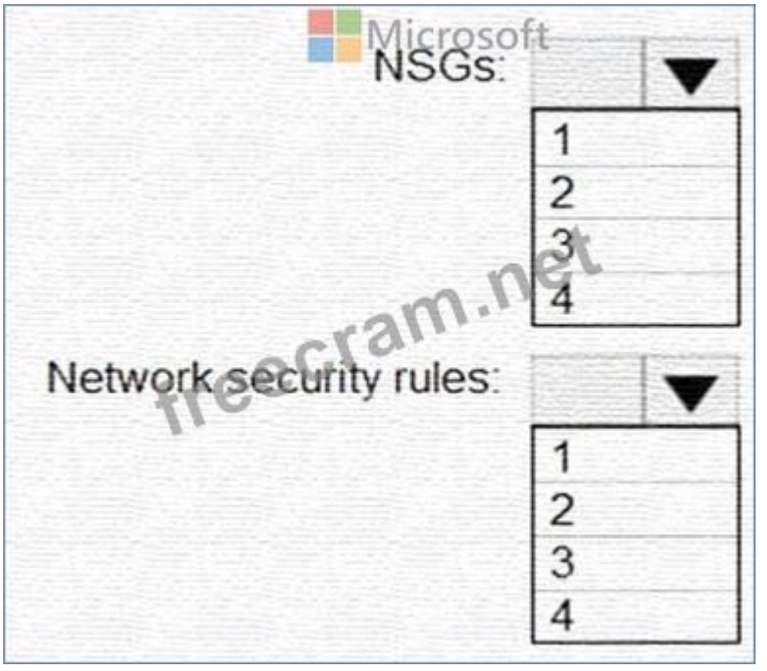
Explanation:



Blueprints can only be assigned to subscriptions.

NEW QUESTION: 178
You plan to configure Azure Disk Encryption for VM4 Which key vault can you use to store the encryption key?
A. KeyVault1
B. KeyVault3
C. KeyVault2
Answer: (SHOW ANSWER)
The key vault needs to be in the same subscription and same region as the VM.
VM4 is in West US. KeyVault1 is the only key vault in the same region as the VM.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault

NEW QUESTION: 179
You have an Azure subscription named Sub1.
You create a virtual network that contains one subnet. On the subnet, you provision the virtual machines shown in the following table.
Currently, you have not provisioned any network security groups (NSGs).
You need to implement network security to meet the following requirements:
* Allow traffic to VM4 from VM3 only.
* Allow traffic from the Internet to VM1 and VM2 only.
* Minimize the number of NSGs and network security rules.
How many NSGs and network security rules should you create? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

NSGs: 1

Network security rules: 3

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

References:

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

NEW QUESTION: 180

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

A. Add a user-assigned managed identity to WebApp1.

B. Add an app setting to the WebApp1 configuration.

C. Enable system-assigned managed identity for the WebApp1.

D. Configure the TLS/SSL binding for WebApp1.

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 181

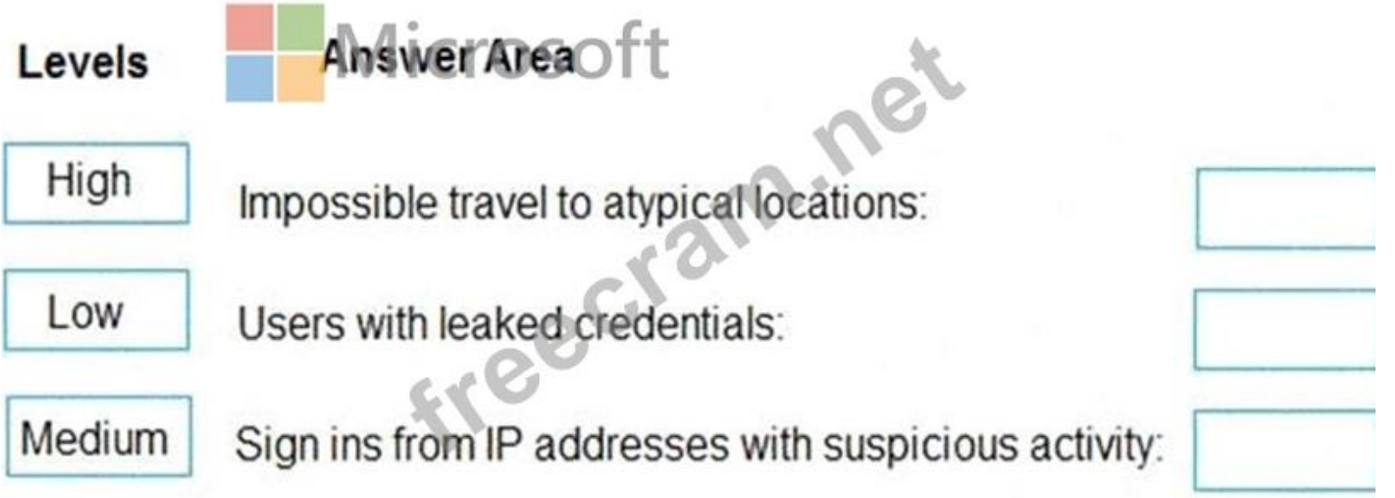
You are implementing conditional access policies.

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

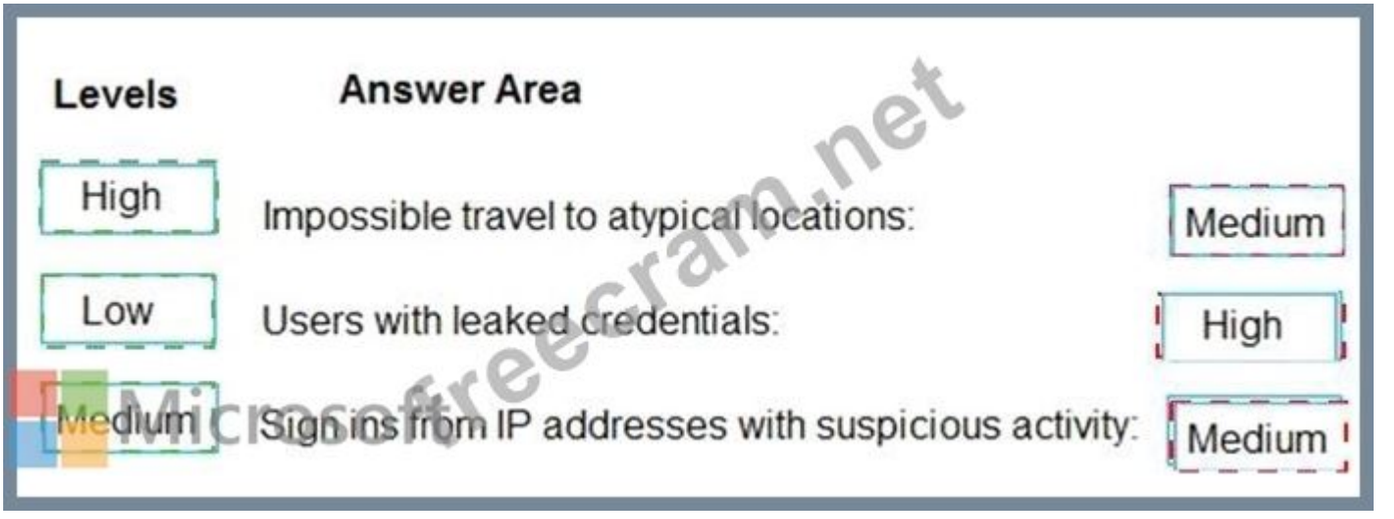
You need to identify the risk level of the following risk events:

* 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.



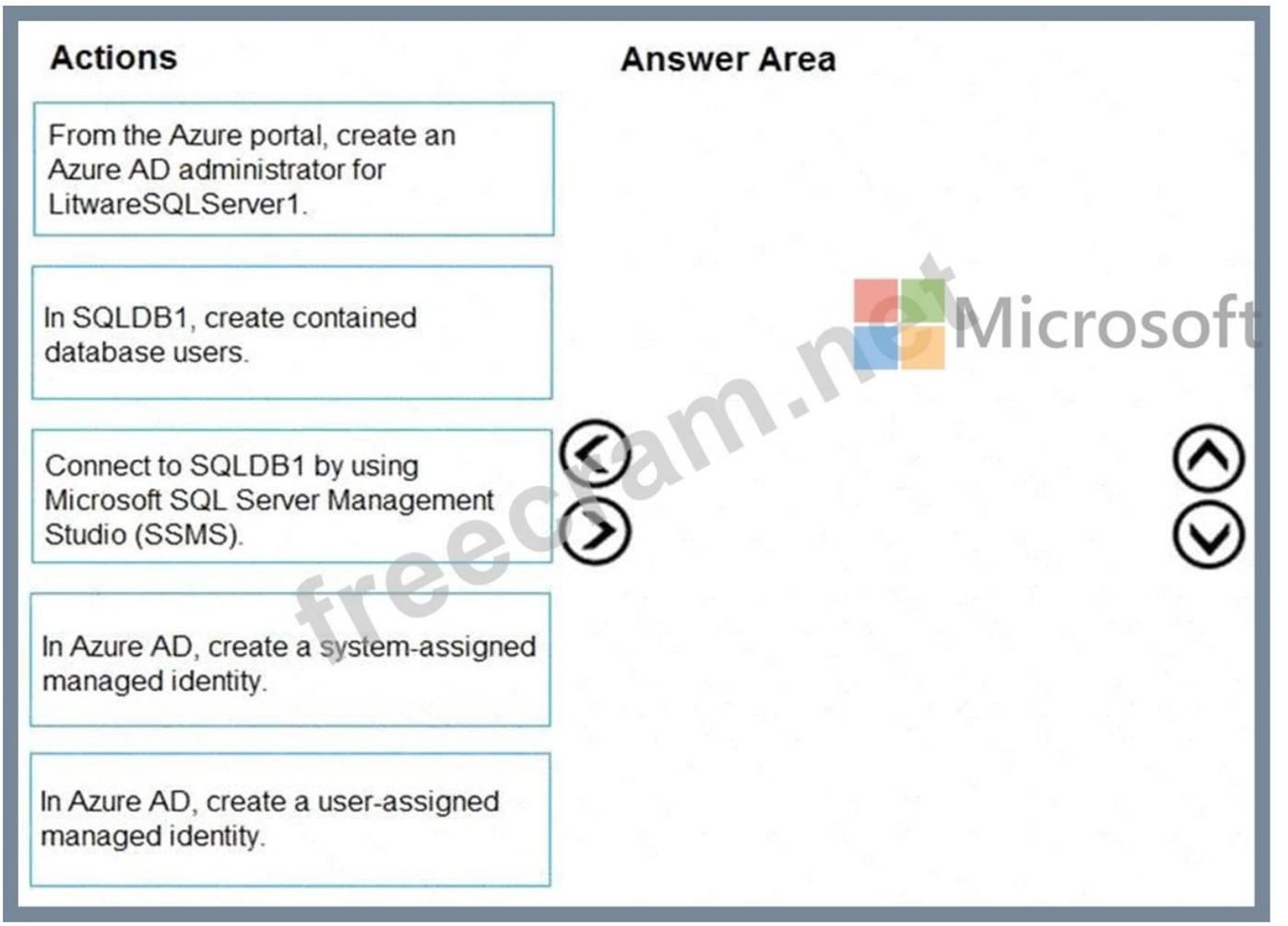
Answer:



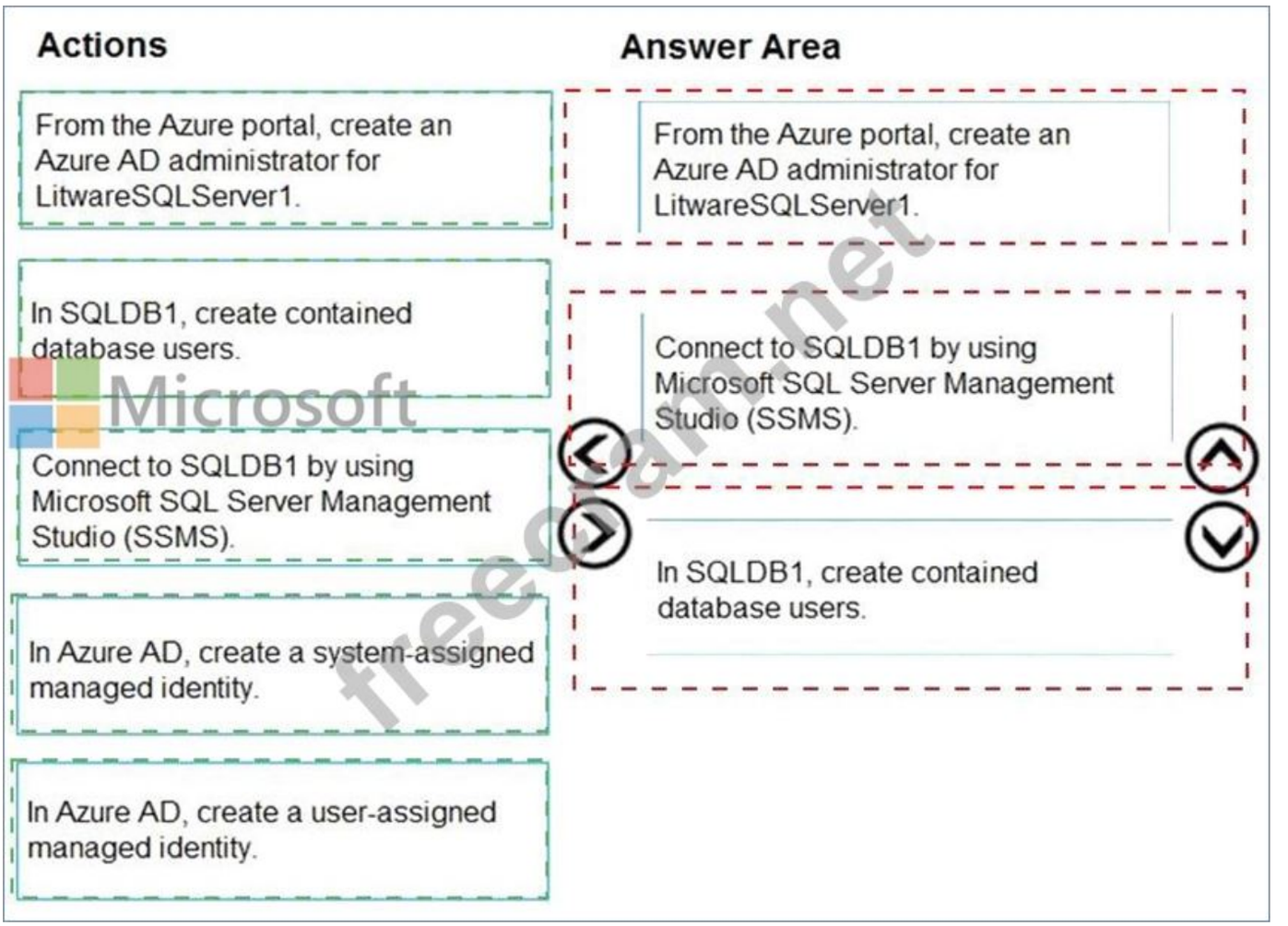
Explanation:
Medium
High
Medium
Refer https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events#sign- ins-from-ip-addresses-with-suspicious-activity

NEW QUESTION: 182
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: 183
You need to configure SQLDB1 to meet the data and application requirements.
Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.


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

Answer:



Explanation:

From the Azure portal, create an Azure AD administrator for LitwareSQLServer1 Connect to SQLDB1 by using SSMS In SQLDB1, create contained database users

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

NEW QUESTION: 184

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

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

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

On which other network interfaces can you configure ASG1?

A. NIC2 only

B. NIC2, NIC3, NIC4, and NIC5

C. NIC2 and NIC3 only

D. NIC2, NIC3, and NIC4 only

Answer: (SHOW ANSWER)

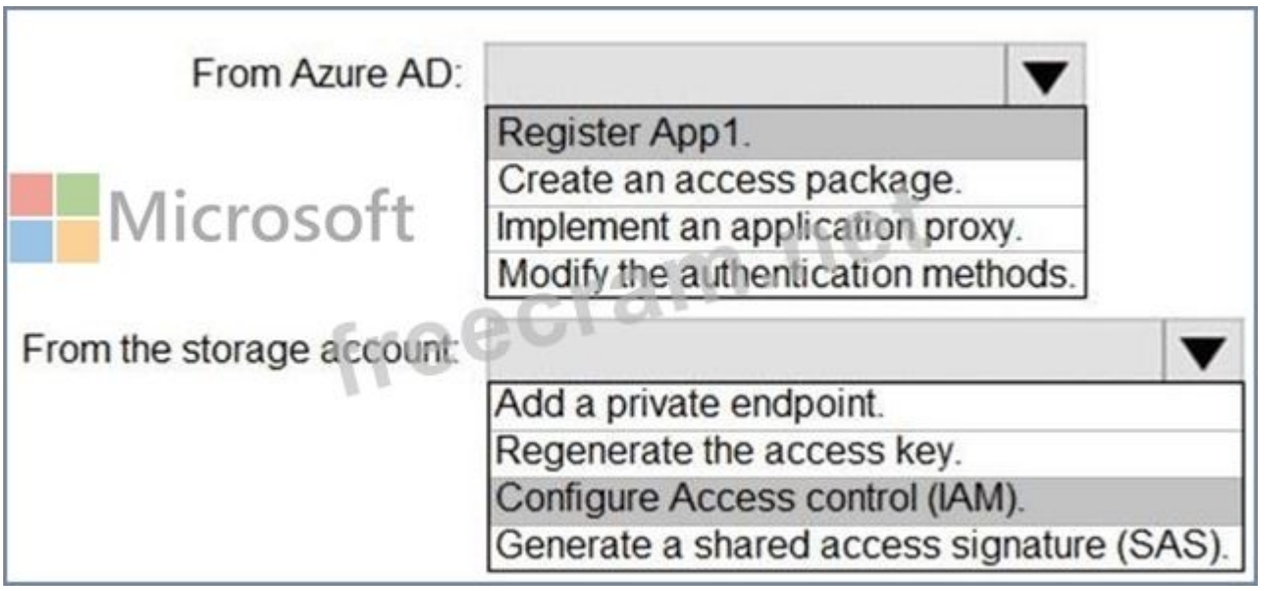
Only network interfaces in NVET1, which consists of Subnet11 and Subnet12, can be configured in ASG1, as all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.

Reference:

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

NEW QUESTION: 185
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: (SHOW ANSWER)
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: 186
You have an Azure Storage account that contains a blob container named container1 and a client application named App1.
You need to enable App1 access to container1 by using Azure Active Directory (Azure AD) authentication.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Answer:



Reference:
https://azure.microsoft.com/en-in/blog/announcing-the-preview-of-aad-authentication-for-storage/
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/storage/common/storage-auth-aad-rbac- portal.md

NEW QUESTION: 187
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: 188
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.

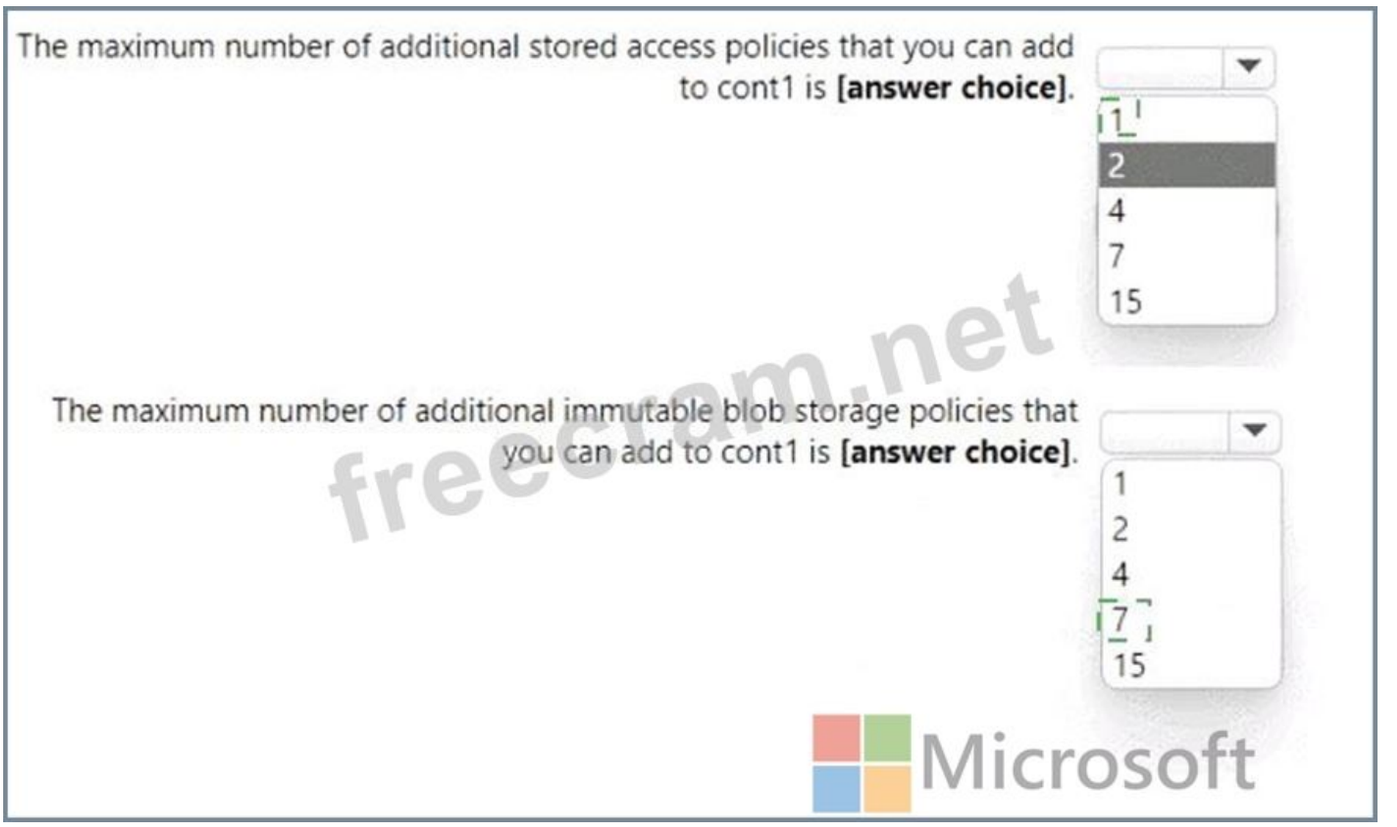
The maximum number of additional stored access policies that you can add to cont1 is **[answer choice]**.

1
2
4
7
15

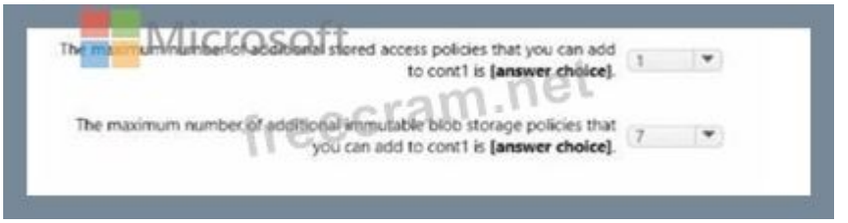
The maximum number of additional immutable blob storage policies that you can add to cont1 is **[answer choice]**.

1
2
4
7
15

Answer:



Explanation:



NEW QUESTION: 189

You have an Azure AD tenant that contains 500 users and an administrative unit named AU1.

From the Azure Active Directory admin center, you plan to add the users to AU1 by using Bulk add members.

You need to create and upload a file for the bulk add.

What should you include in the file?

A. only the user principal name (UPN) of each user

B. only the user principal name (UPN) and object identifier of each user

C. only the object identifier of each user

D. Only the user principal name (UPN) and display name of each user

E. only the display name of each user

Answer: (SHOW ANSWER)

NEW QUESTION: 190

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

Name	Description
App1	Azure App Service app in a Premium plan
SQL1	Azure SQL managed instance
storage1	Azure Storage account
Function1	Azure Functions function in a Consumption plan

App1 uses Function 1, SQL1, and storage 1.

You need to secure the traffic between App1, Function1, SQL1. and storage1, by using private endpoints.

With which resources can App1 communicate by using a private endpoint?

A. storage1 only

B. SQL1 and storage1 only

C. SQL1 only

D. Function1 only

E. storage1 and Function1 only

F. storage1, SQL1, and Function1

Answer: F (LEAVE A REPLY)

NEW QUESTION: 191

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. Edit the role activation settings.

B. Create a new access review.

C. Update the end date of the user assignment

D. Edit the role assignment settings.

Answer: (SHOW ANSWER)

NEW QUESTION: 192

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

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

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

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

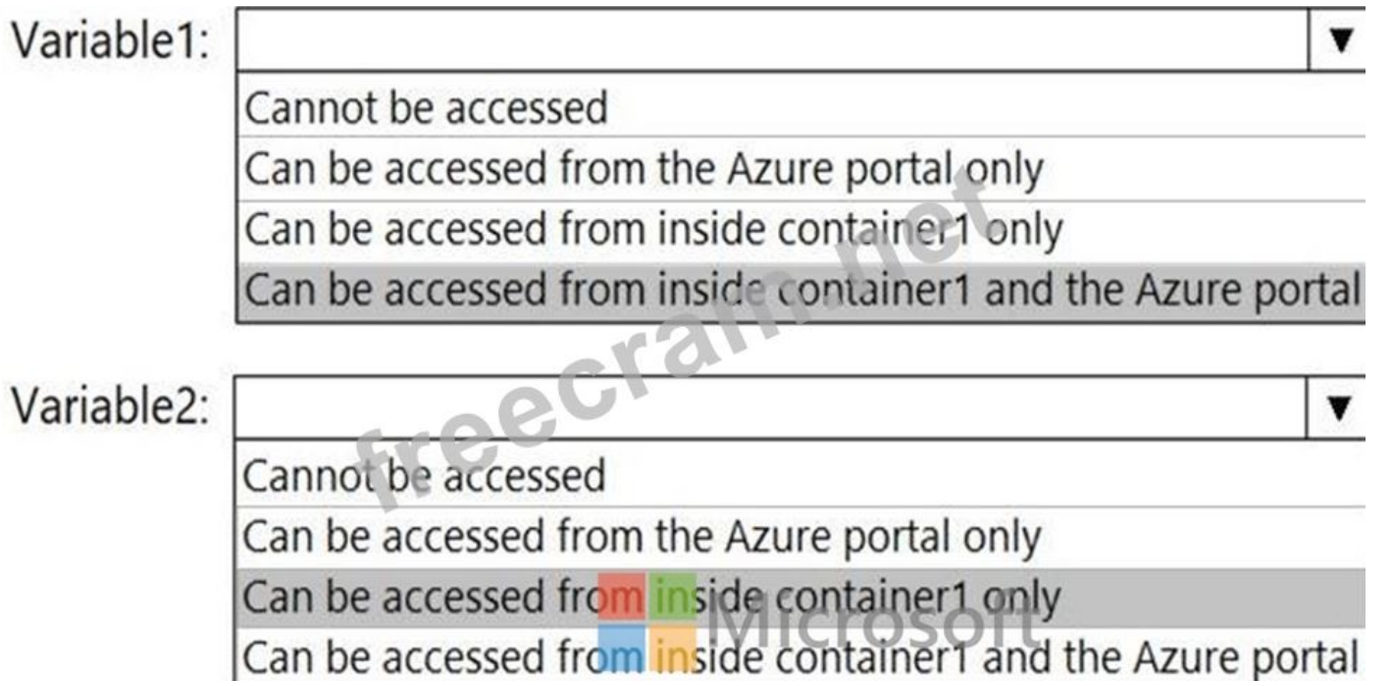
What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

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

Explanation:



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

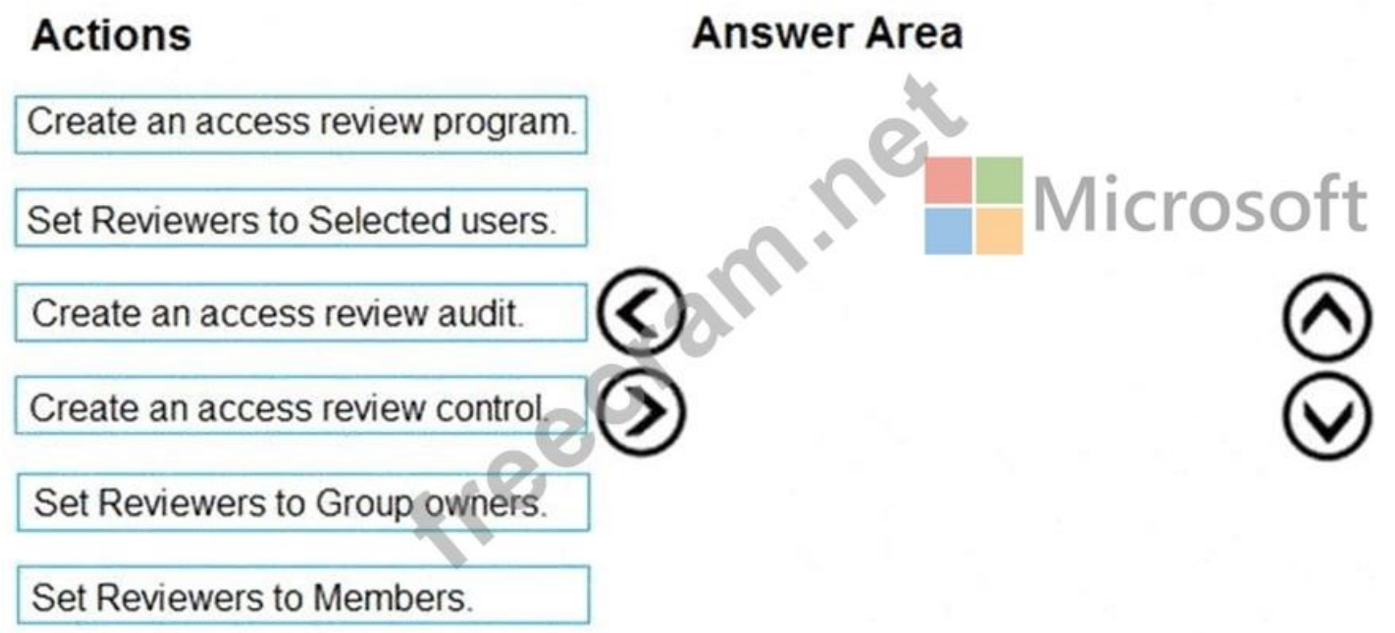
NEW QUESTION: 193
You have multiple development teams that will create apps in Azure.
You plan to create a standard development environment that will be deployed for each team.
You need to recommend a solution that will enforce resource locks across the development environments and ensure that the locks 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: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

NEW QUESTION: 194
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

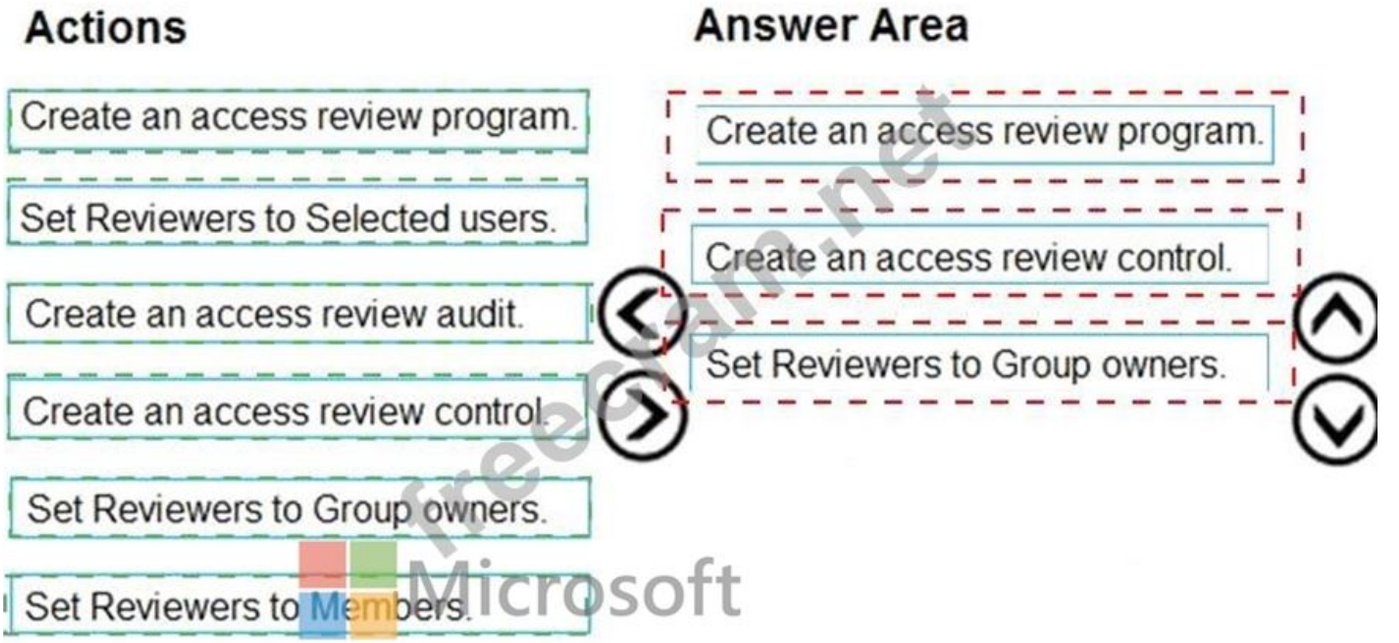
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:
Lab Instance: 28681041
Task 7
You need to collect all the audit failure data from the security log of a virtual machine 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: 195
You have an Azure subscription that contains the virtual machines shown in the following table.
All the virtual networks are peered.
You deploy Azure Bastion to VNET2.
Which virtual machines can be protected by the bastion host?
A. VM1, VM2, VM3, and VM4
B. VM1, VM2, and VM3 only
C. VM2 and VM4 only
D. VM2 only
Answer: (SHOW ANSWER)
https://docs.microsoft.com/en-us/azure/bastion/vnet-peering

NEW QUESTION: 196
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: 197
You have an Azure subscription that contains an Azure key vault named Vault1 and a virtual machine named VM1.
VM1 is connected to a virtual network named VNet1.
You need to allow access to Vault1 only from VM1.
What should you do in the Networking settings of Vault1?
A. From the Firewalls and virtual networks tab, add the IP address of VM1.
B. From the Firewalls and virtual networks tab, set Allow trusted Microsoft services to bypass this firewall to Yes for Vault1.
C. From the Private endpoint connections tab, create a private endpoint for VM1.
D. From the Firewalls and virtual networks tab, add VNet1.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 198
You company has an Azure Active Directory (Azure AD) tenant named contoso.com.
You plan to create several security alerts by using Azure Monitor.
You need to prepare the Azure subscription for the alerts.
What should you create first?
A. An Azure Storage account
B. an Azure Log Analytics workspace
C. an Azure event hub

D. an Azure Automation account

Answer: (SHOW ANSWER)

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

NEW QUESTION: 199

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 6

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

Answer:

Check below steps in explanation for Task

Explanation:

To email an alert to a user named adminl@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes, you can follow these steps:

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

In the left pane, select Alerts.

Select New alert rule.

In the New alert rule pane, enter the following information:

Name: Enter a name for the alert rule.

Description: Enter a description for the alert rule.

Condition: Select Metric measurement.

Resource: Select the virtual machine named VM1.

Metric: Select Percentage CPU.

Operator: Select Greater than.

Threshold: Enter 70.

Aggregation type: Select Average.

Period: Select 15 minutes.

In the Actions pane, select Add action group.

In the Add action group pane, enter the following information:

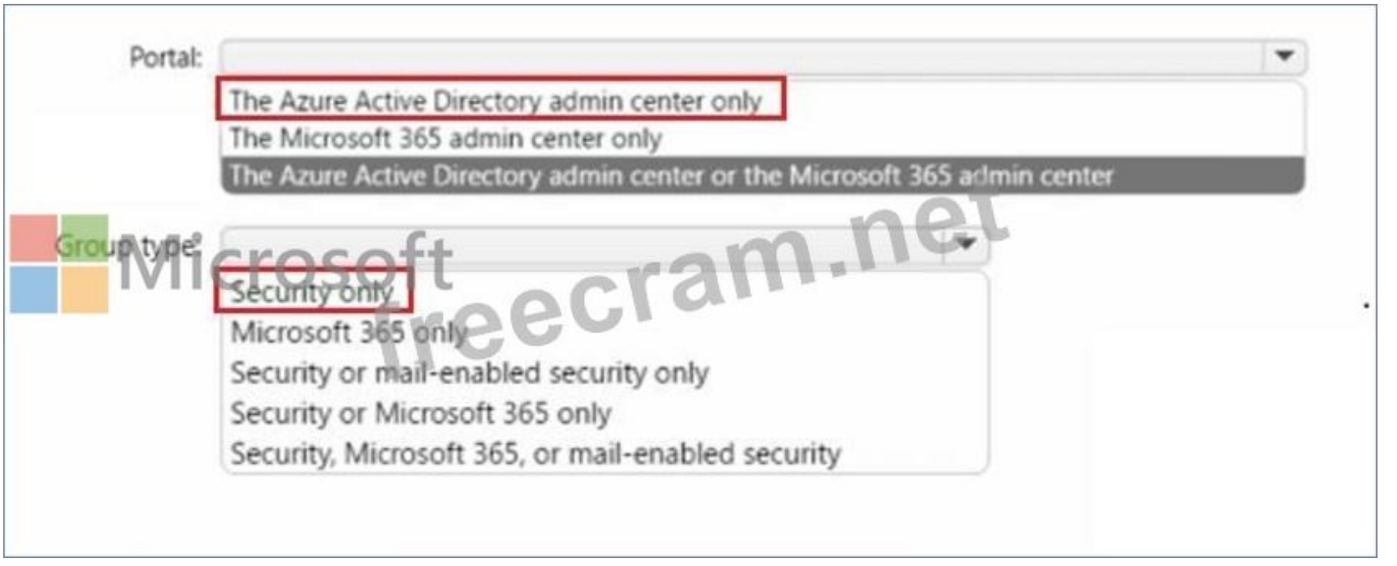
Name: Enter a name for the action group.

Short name: Enter a short name for the action group.
Email recipient: Enter the email address of the user you want to receive the alert. For example, adminl@contoso.com.
Select OK.

NEW QUESTION: 200

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:



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

NEW QUESTION: 201

You have an Azure subscription.
You need to ensure that you receive notifications regarding suspicious Azure DNS activity.
Which Microsoft Defender plan for Cloud Workload Protection (CWP) should you enable?

A. APIs
B. Servers
C. Storage
D. Resource Manager
E. App Service

Answer: (SHOW ANSWER)

NEW QUESTION: 202

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

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

You create a resource group named RG1.

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

NOTE: Each correct selection is worth one point.

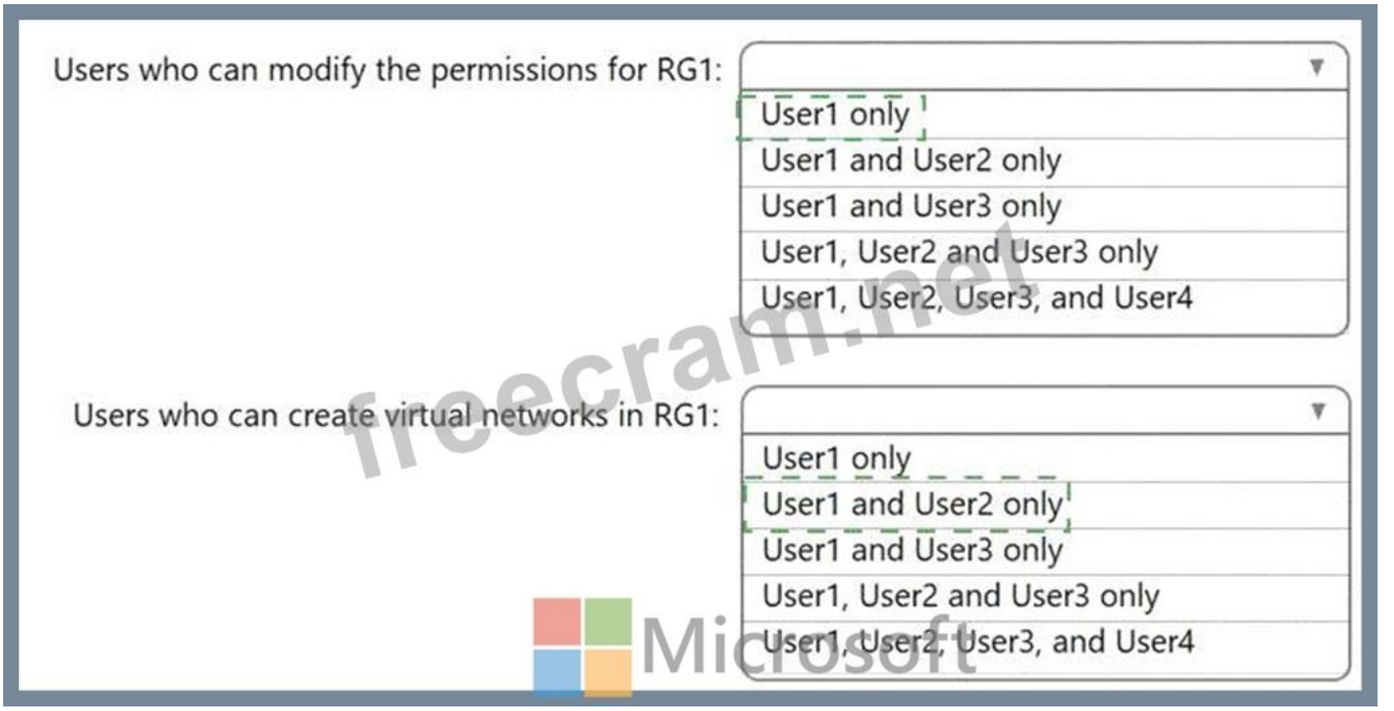
Users who can modify the permissions for RG1:

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

Users who can create virtual networks in RG1:

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

Answer:



Explanation:

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

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

NEW QUESTION: 203

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: (SHOW ANSWER)

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

NEW QUESTION: 204

You have an Azure AD tenant that contains the users shown in the following table.

You need to ensure that the users cannot create app passwords. The solution must ensure that User1 can continue to use the Mail and Calendar app.

What should you do?

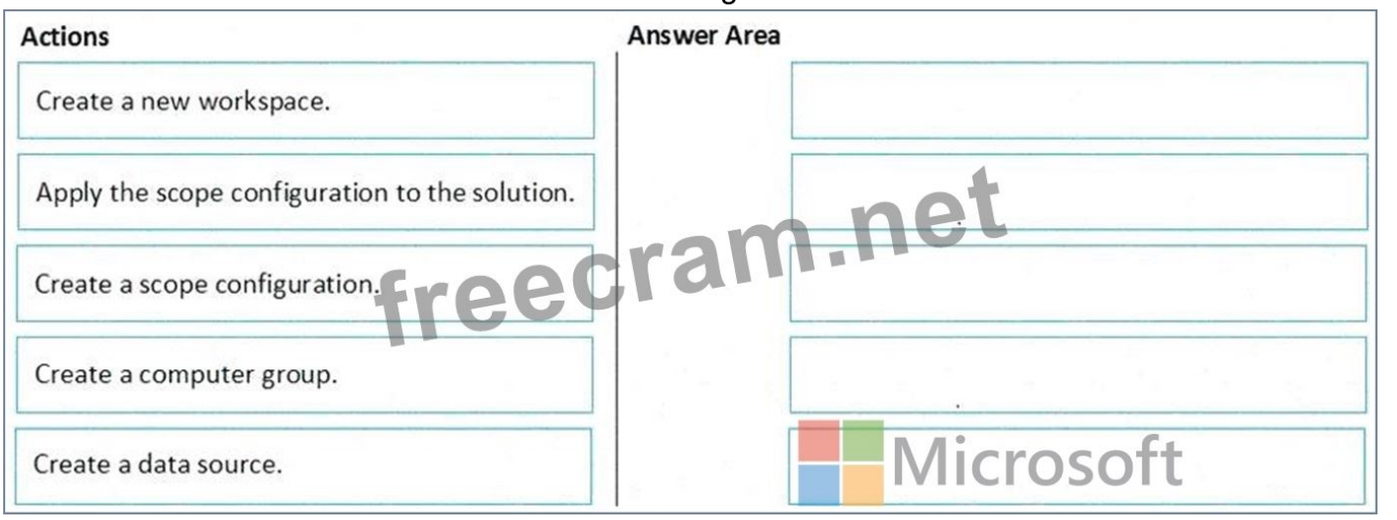
A. Assign User! the Authentication Policy Administrator role.

B. Configure a multi-factor authentication (MFA) registration policy.
C. Create a new app registration.
D. Enable Azure AD Password Protection.
Answer: (SHOW ANSWER)

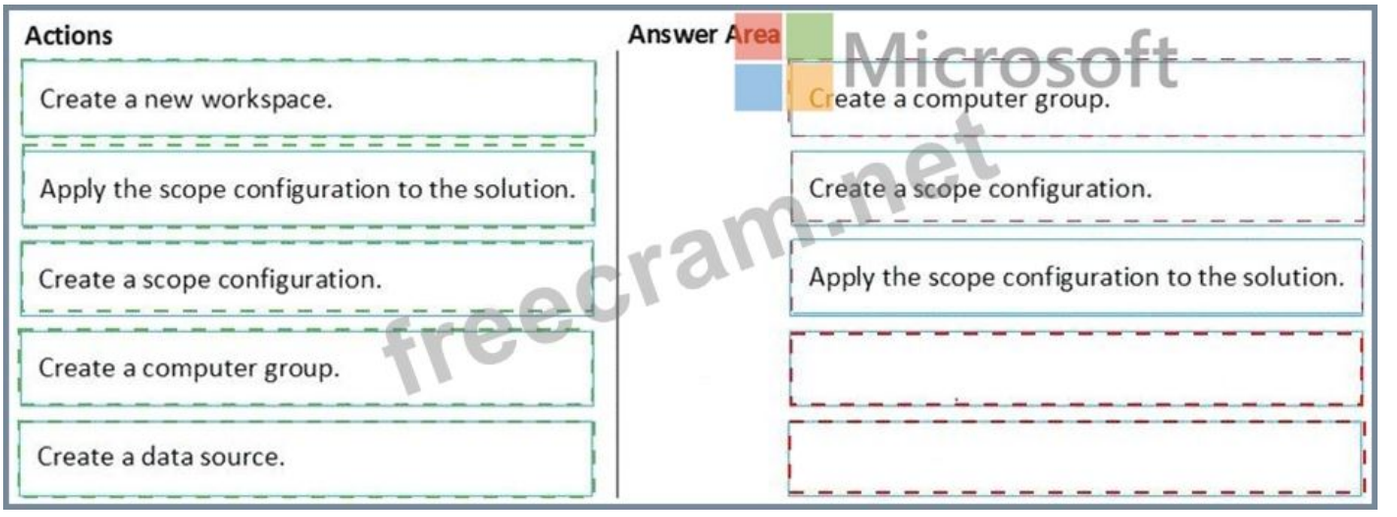
NEW QUESTION: 205
Lab Task
use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password. place your cursor in the Enter password box and click on the password below.
Azure Username: Userl -28681041@ExamUsers.com
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 5
You need to ensure that only devices connected to a 131-107.0.0/16 subnet can access data in the rg1lod28681041 Azure Storage account.
Answer:
Check below steps in explanation for Task
Explanation:
To ensure that only devices connected to a 131-107.0.0/16 subnet can access data in the rg1lod28681041 Azure Storage account, you can follow these steps:
In the Azure portal, search for and select the storage account named rg1lod28681041.
In the left pane, select Firewalls and virtual networks.
In the Firewalls and virtual networks pane, select Selected networks.
In the Selected networks pane, select Add existing virtual network.
In the Add existing virtual network pane, select the virtual network that contains the 131-107.0.0/16 subnet.
Select Add.
https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

NEW QUESTION: 206
You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.
You have 500 Azure virtual machines that run Windows Server 2016 and are enrolled in LAW1.
You plan to add the System Update Assessment solution to LAW1.
You need to ensure that System Update Assessment-related logs are uploaded to LAW1 from 100 of the virtual machines only.

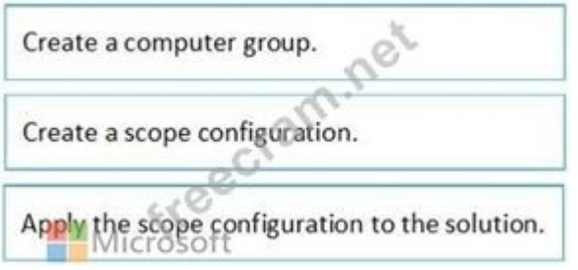
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:



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

NEW QUESTION: 207
You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.
You have 100 on-premises servers that run Windows Server 2012 R2 and Windows Server 2016. The servers connect to LAW1. LAW1 is configured to collect security-related performance counters from the connected servers.

You need to configure alerts based on the data collected by LAW1. The solution must meet the following requirements:
* Alert rules must support dimensions.
* The time it takes to generate an alert must be minimized.
* Alert notifications must be generated only once when the alert is generated and once when the alert is
* resolved.
Which signal type should you use when you create the alert rules?
A. Log
B. Log (Saved Query)
C. Metric
D. Activity Log
Answer: (SHOW ANSWER)
Metric alerts in Azure Monitor provide a way to get notified when one of your metrics cross a threshold.
Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights standard and custom metrics.
Note: Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric

NEW QUESTION: 208
You have an Azure subscription named Sub1.
In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.
You need to modify Play1 to send email messages to a distribution group named Alerts.
What should you use to modify Play1?
A. Azure DevOps
B. Azure Application Insights
C. Azure Monitor
D. Azure Logic Apps Designer
Answer: (SHOW ANSWER)
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: 209

You have a Microsoft 365 tenant that uses an Azure Active Directory (Azure AD) tenant The Azure AD tenant syncs to an on-premises Active Directory domain by using an instance of Azure AD Connect.
You create a new Azure subscription
You discover that the synced on-premises user accounts cannot be assigned rotes in the new subscription.
You need to ensure that you can assign Azure and Microsoft 365 roles to the synced Azure AD user accounts.
What should you do first?
A. Configure the Azure AD tenant used by the new subscription to use pass-through authenticate
B. Configure a second instance of Azure AD Connect.
C. Change the Azure AD tenant used by the new subscription.
D. Configure the Azure AD tenant used by the new subscription to use federated authentication.
Answer: (SHOW ANSWER)

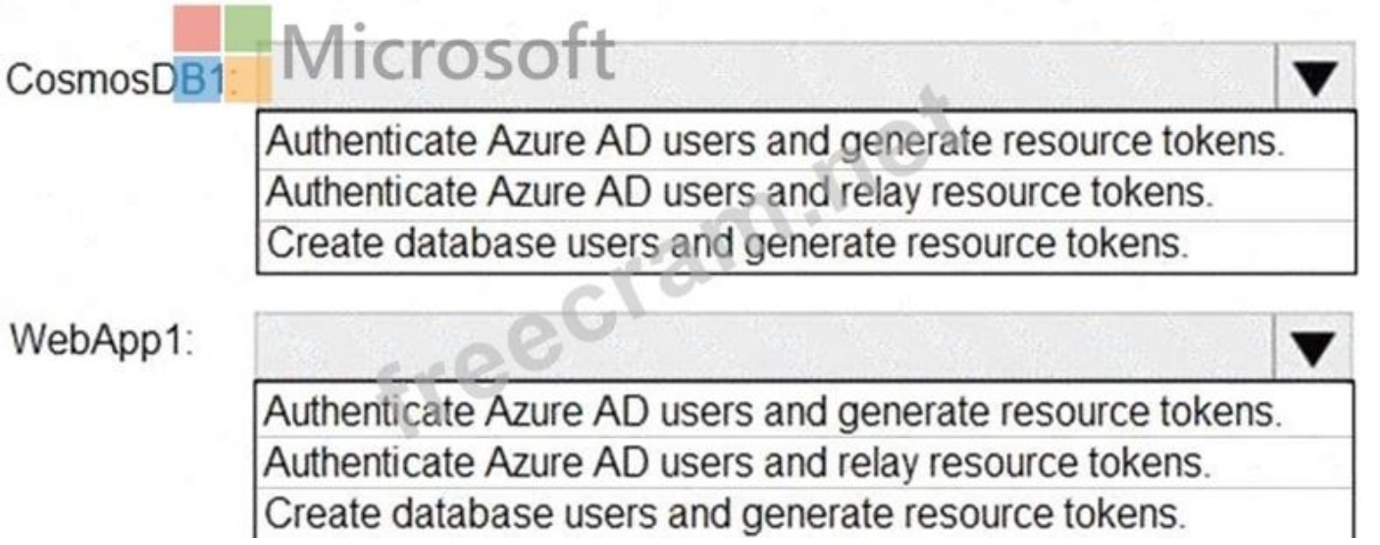
NEW QUESTION: 210
You have an Azure subscription named Sub1 that contains the virtual machines shown in the following table.

Name	Resource group
VM1	RG1
VM2	RG2
VM3	RG1
VM4	RG2

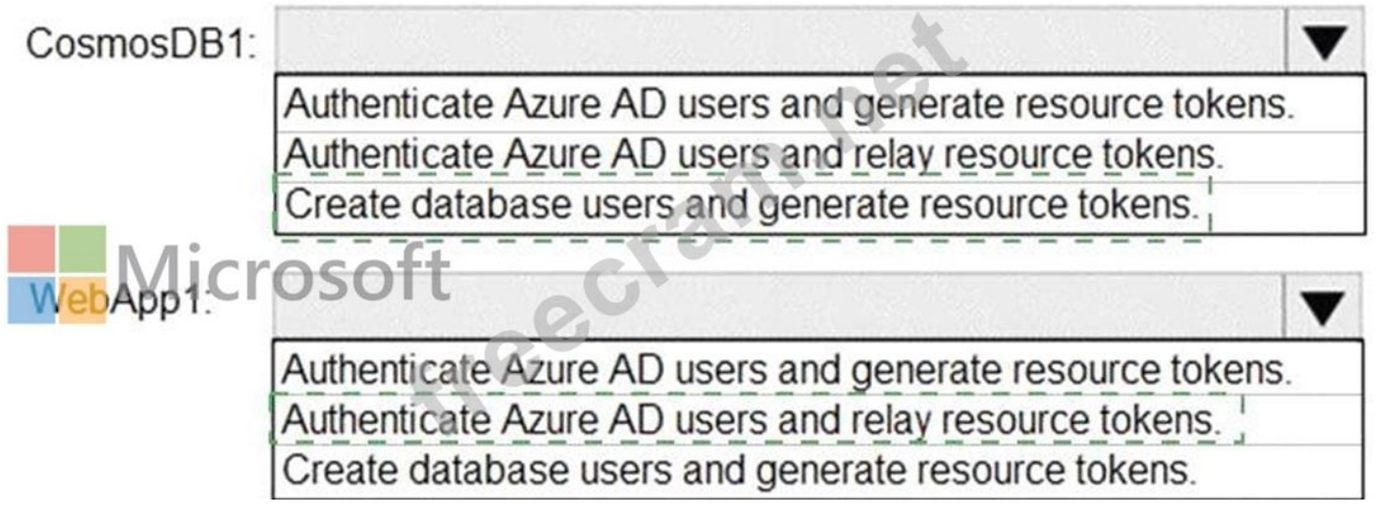
You need to ensure that the virtual machines in RG1 have the Remote Desktop port closed until an authorized user requests access.
What should you configure?
A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
B. an application security group
C. Azure Active Directory (Azure AD) conditional access
D. just in time (JIT) VM access
Answer: (SHOW ANSWER)
Just-in-time (JIT) virtual machine (VM) access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.
Note: When just-in-time is enabled, Security Center locks down inbound traffic to your Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the just-in-time solution.
When a user requests access to a VM, Security Center checks that the user has Role-Based Access Control (RBAC) permissions that permit them to successfully request access to a VM. If the request is approved, Security Center automatically configures the Network Security Groups

(NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the amount of time that was specified. After the time has expired, Security Center restores the NSGs to their previous states. Those connections that are already established are not being interrupted, however.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

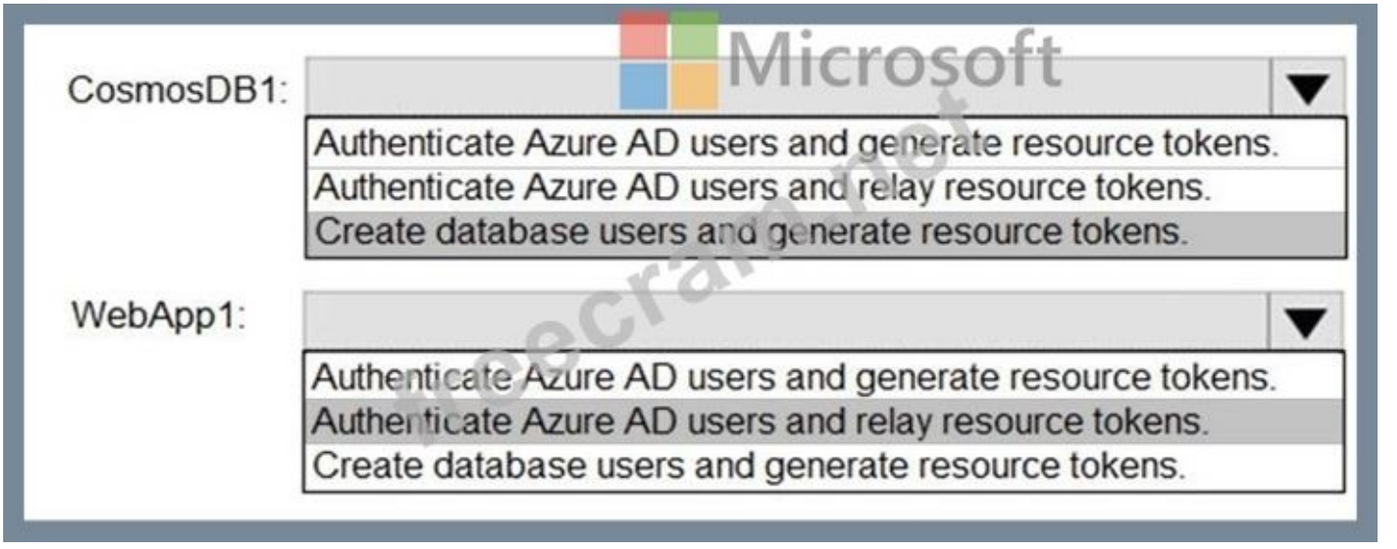
NEW QUESTION: 211
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
You plan to implement an application that will consist of the resources shown in the following table.
Users will authenticate by using their Azure AD user account and access the Cosmos DB account by using resource tokens.
You need to identify which tasks will be implemented in CosmosDB1 and WebApp1.
Which task should you identify for each resource? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

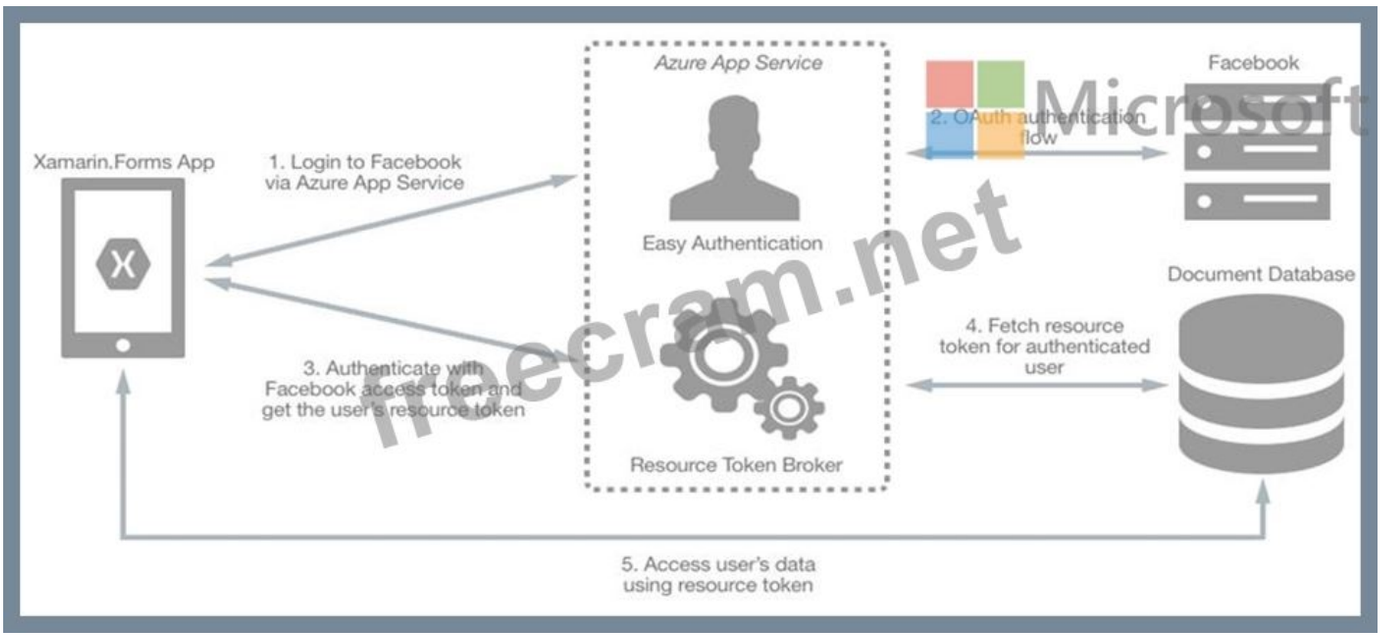


CosmosDB1: Create database users and generate resource tokens.

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

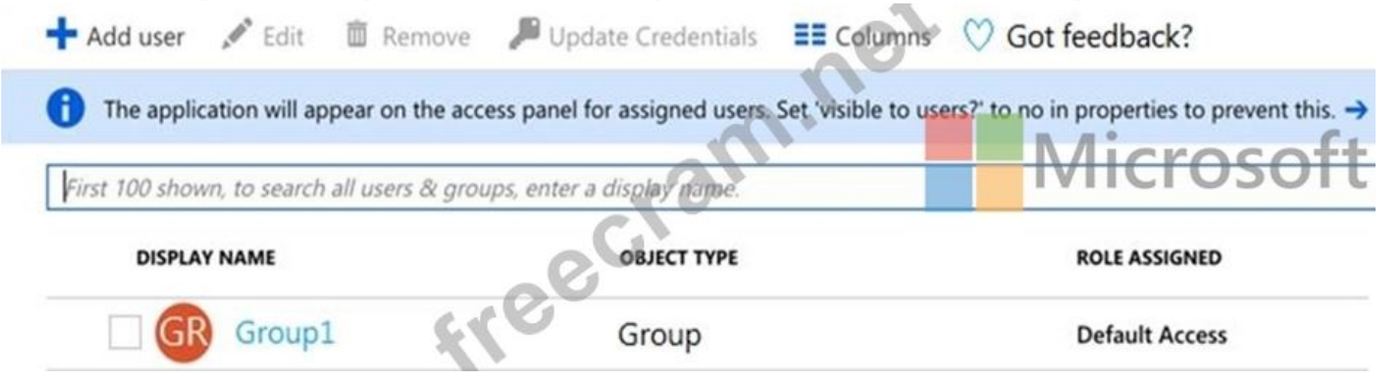
WebApp1: Authenticate Azure AD users and relay resource tokens

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



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

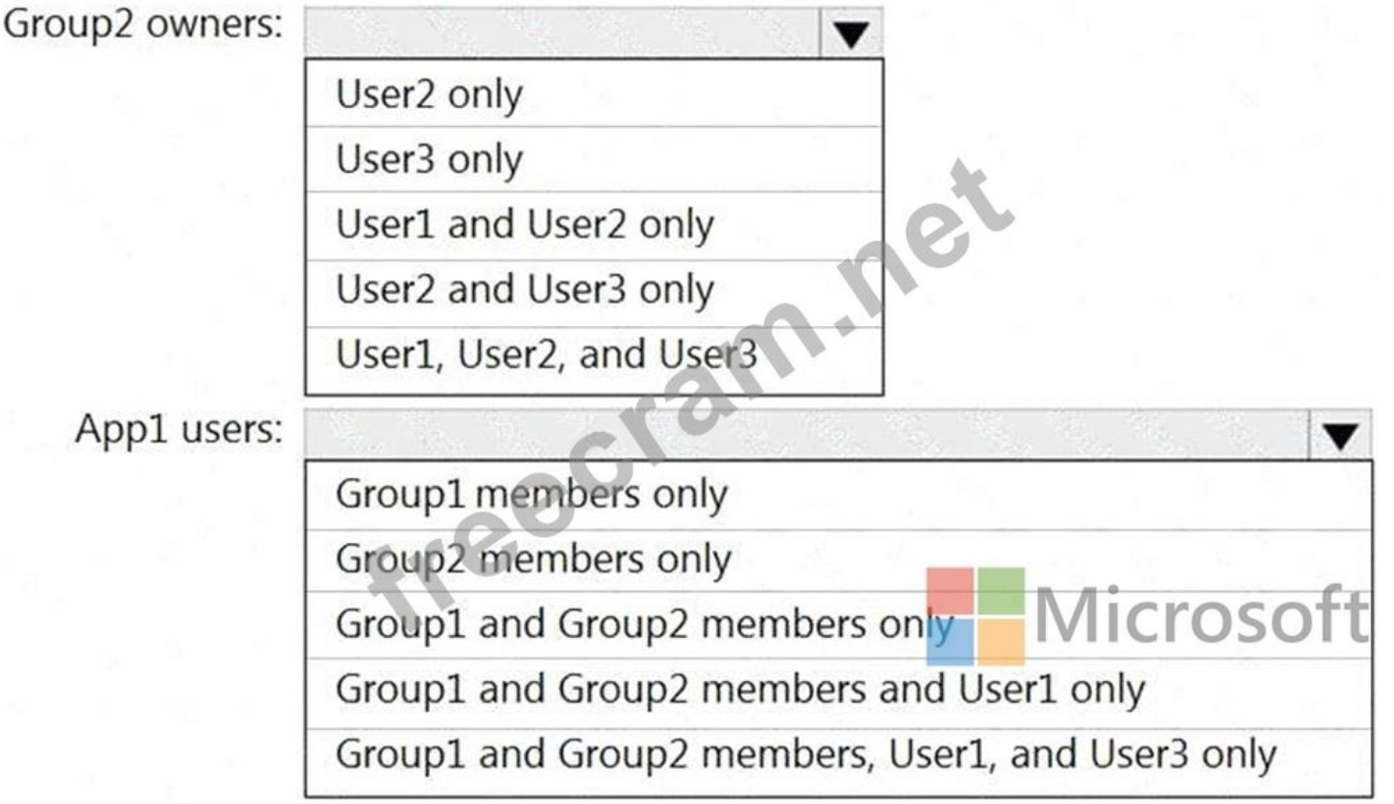
NEW QUESTION: 212
You have an Azure Active Directory (Azure AD) tenant that contains the resources shown in the following table.
User2 is the owner of Group2.
The user and group settings for App1 are configured as shown in the following exhibit.



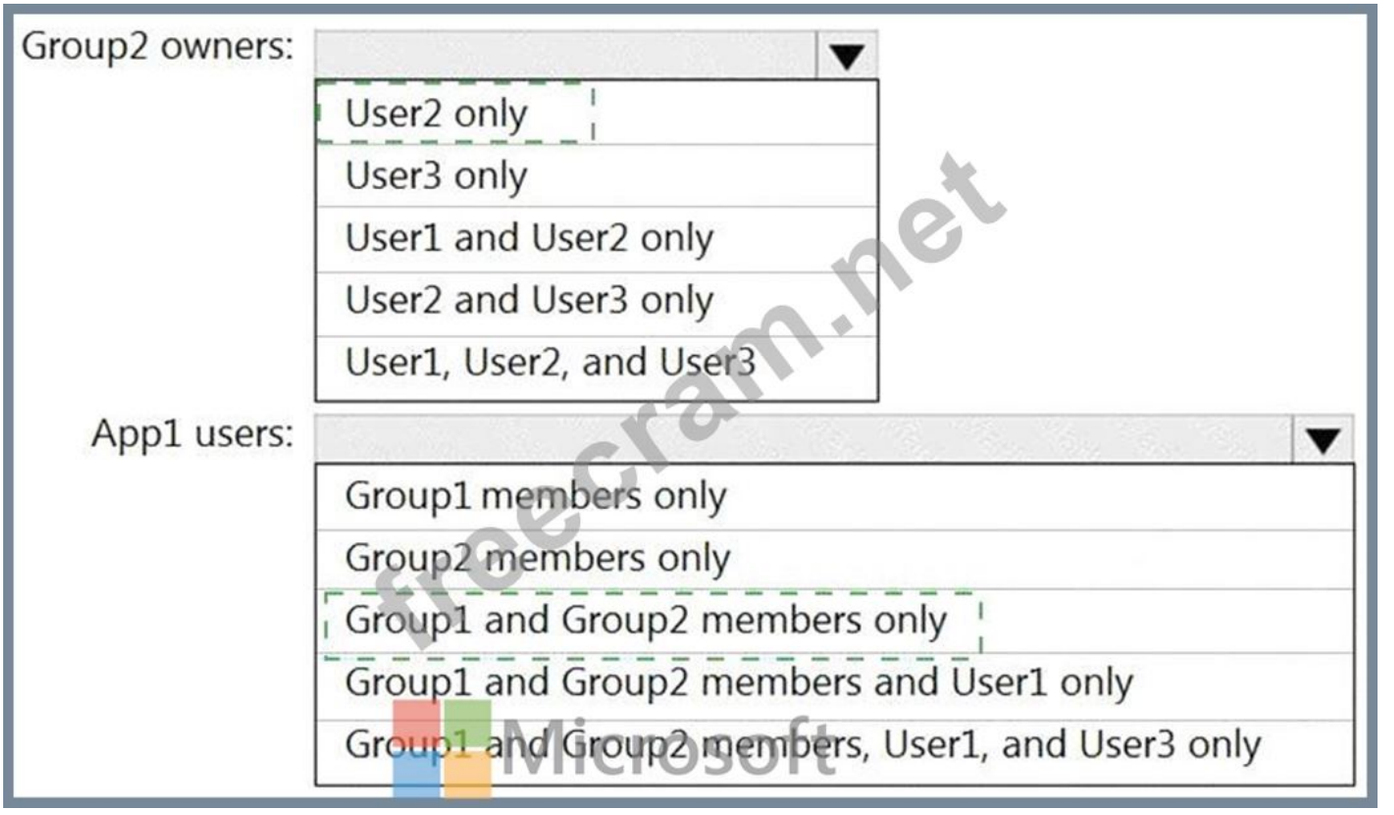
You enable self-service application access for App1 as shown in the following exhibit.
User3 is configured to approve access to Appl.
You need to identify the owners of Group2 and the users of Appl.

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

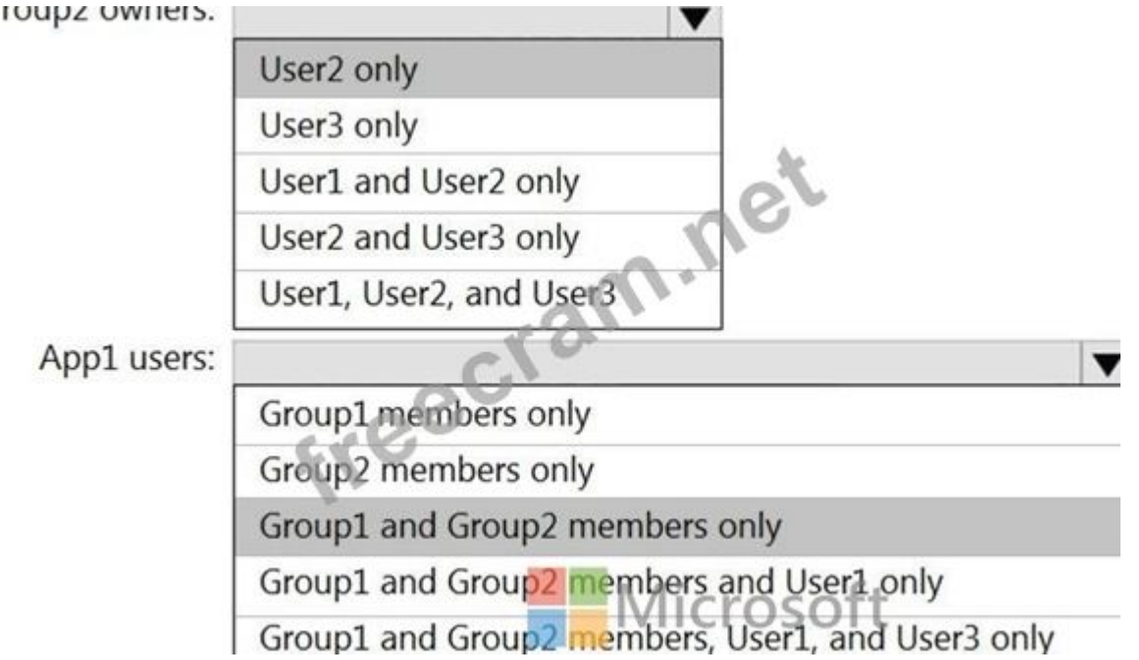
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



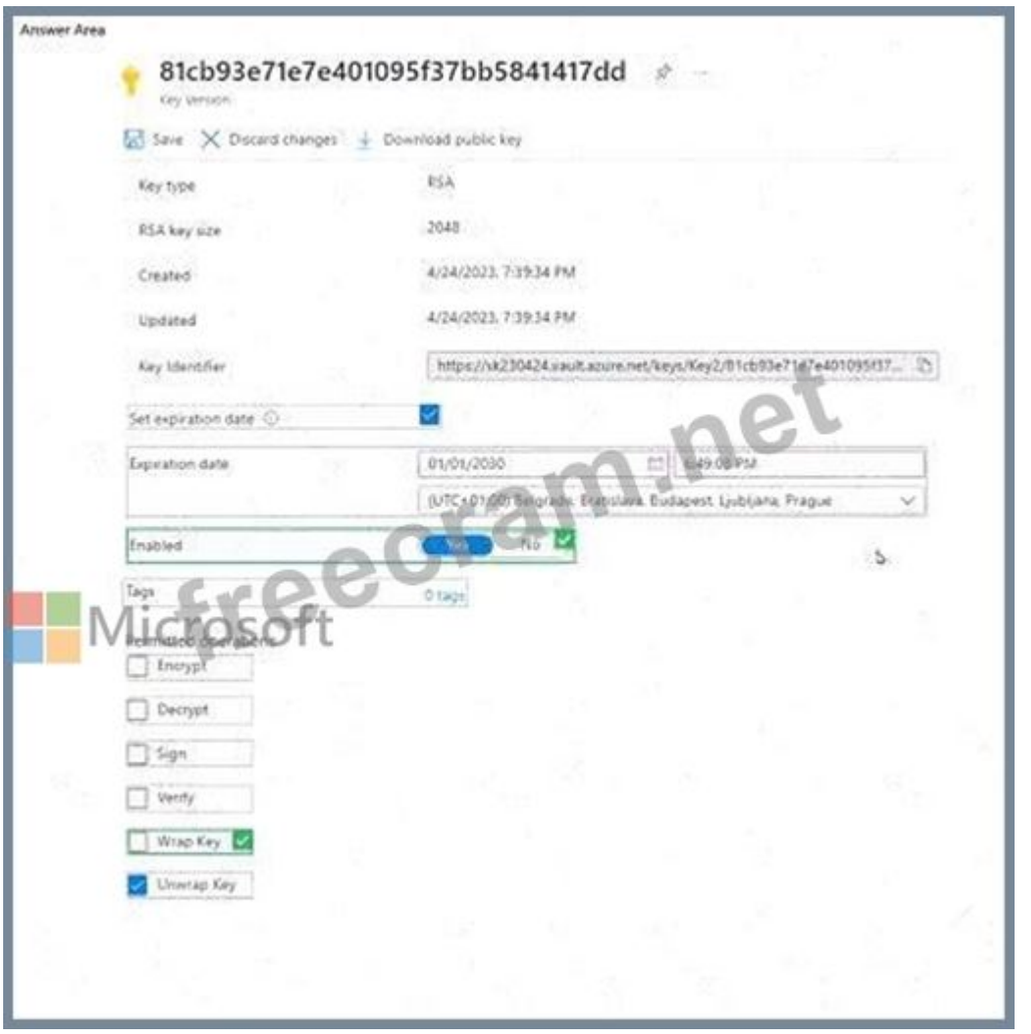
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access

NEW QUESTION: 213
You have an Azure subscription that contains the Azure App Service apps shown in the following table.

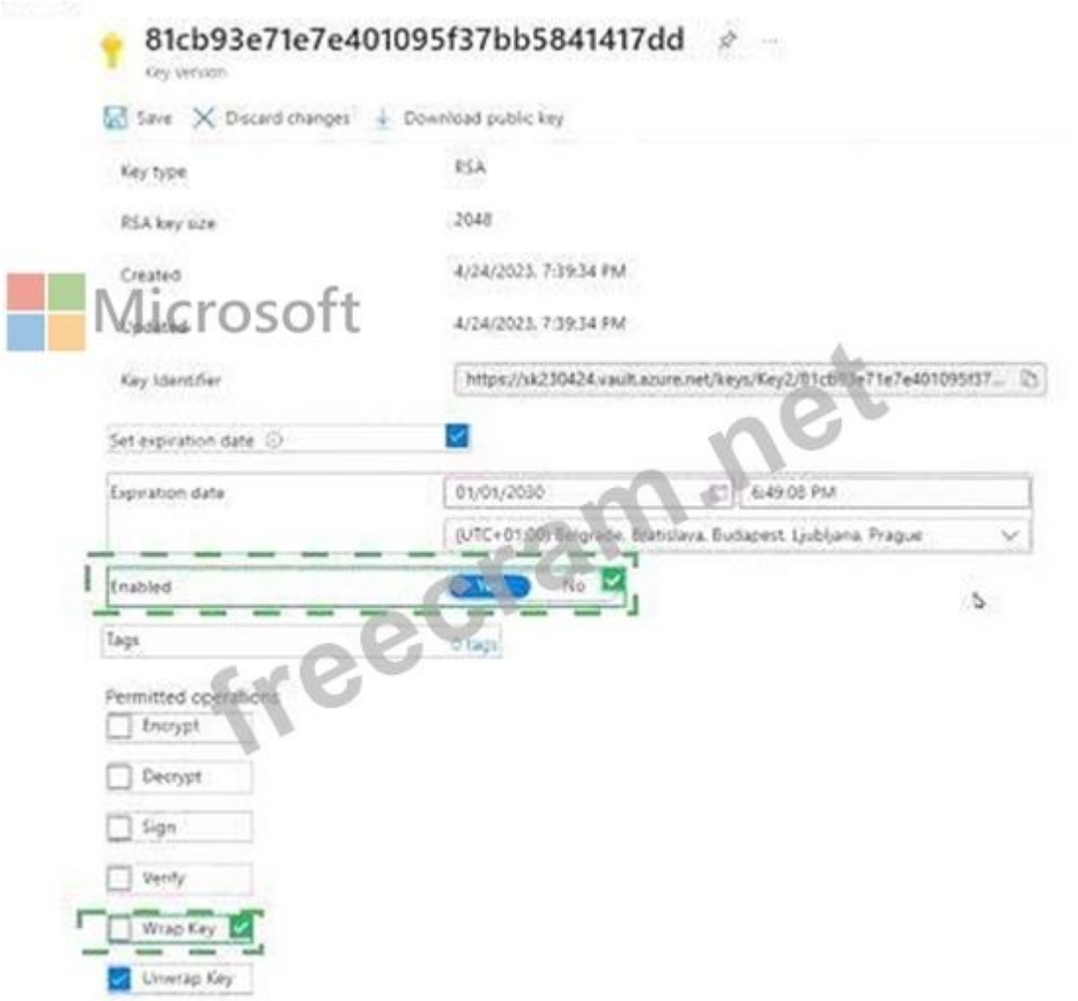
Name	App Service plan
App1	Free
App2	Shared
App3	Basic
App4	Standard

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

NEW QUESTION: 214
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:



NEW QUESTION: 215

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

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

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

The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

A. the Contributor role for the subscription

B. the Network Contributor role for RG1.

C. A custom RBAC role for the subscription

D. the Network Contributor role for RG2

E. the Virtual Machine Contributor role for RG1.

F. a custom RBAC role for RG2

Answer: (SHOW ANSWER)