Microsoft.AZ-500.v2026-06-13.q208

Exam Code:	AZ-500
Exam Name:	Microsoft Azure Security Technologies
Certification Provider:	Microsoft
Free Question Number:	208
Version:	v2026-06-13
# of views:	110
# of Questions views:	2282
https://www.freecram.net/torrent/Microsoft.AZ-500.v2026-06-13.q208.html	

NEW QUESTION: 1
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: 2
You are implementing an Azure Application Gateway web application firewall (WAF) named WAF1.
You have the following Bicep code snippet.

```
resource AppGW_AppFW_Pol 'Microsoft.Network/ApplicationGatewayWebApplicationFirewallPolicies@2021-08-01' = {
  name: AppGW_AppFW_Pol_name
  location: location
  properties: {
    customRules: [
      {
        name: 'CustRule01'
        priority: 100
        ruleType: 'MatchRule'
        action: 'Block'
        matchConditions: [
          {
            matchVariables: [
              {
                variableName: 'RemoteAddr'
              }
            ]
            operator: 'IPMatch'
            negationConditon: true
            matchValues: [
              '10.10.10.0/24'
            ]
          }
        ]
      }
    ]
    policySettings: {
      requestBodyCheck: true
      maxRequestBodySizeInKb: 128
      state: 'Enabled'
      mode: 'Detection'
    }
    managedRules: {
      managedRuleSets: [
        {
          ruleSetType: 'OWASP'
          ruleSetVersion: '3.2'
        }
      ]
    }
  }
}
```


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
A request to the backend pool from IP address 10.1.1.5 is allowed.	○	○
Incoming requests attempting file path attacks are blocked.	○	○
WAF1 allows a 50-MB file to be uploaded.	○	○

Answer:

Answer Area

Statements	Yes	No
A request to the backend pool from IP address 10.1.1.5 is allowed.	○	○
Incoming requests attempting file path attacks are blocked.	○	○
WAF1 allows a 50-MB file to be uploaded.	○	○

Explanation:

Answer Area

Statements	Yes	No
A request to the backend pool from IP address 10.1.1.5 is allowed.	○	●
Incoming requests attempting file path attacks are blocked.	●	○
WAF1 allows a 50-MB file to be uploaded.	○	●

NEW QUESTION: 3

You have an Azure virtual machine named VM1.

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

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

What should you do?

A. Add the Microsoft Antimalware extension to VM1.

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

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

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

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 4

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: 5

You have an Azure subscription.

You need to deploy an Azure virtual WAN to meet the following requirements:

* Create three secured virtual hubs located in the East US, West US, and North Europe Azure regions.

* Ensure that security rules sync between the regions.

What should you use?

A. Azure Virtual Network Manager

B. Azure Firewall Manager

C. Azure Network Function Manager

D. Azure Front Door

Answer: (SHOW ANSWER)

NEW QUESTION: 6

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

What should you do?

A. Add a membership rule to Group1.

B. Delete Group1. Create a new group named Group1 that has a membership type of Office 365. Add users and devices to the group.

C. Modify the membership rule of Group1.

D. Change the membership type of Group1 to Assigned. Create two groups that have dynamic memberships. Add the new groups to Group1.

Answer: (SHOW ANSWER)

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

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

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

NEW QUESTION: 7
You have an Azure subscription that is linked to a Microsoft Entra tenant. The tenant contains the groups shown in the following table.

Name	Member of
Group1	*None*
Group2	Group1

The tenant contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

The subscription contains the Azure SQL servers shown in the following table.

Name	Assigned server admin	Database
sqlsvr1	User1	DB1
sqlsvr2	Group1	DB2

The servers are configured for Microsoft Entra-only authentication.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

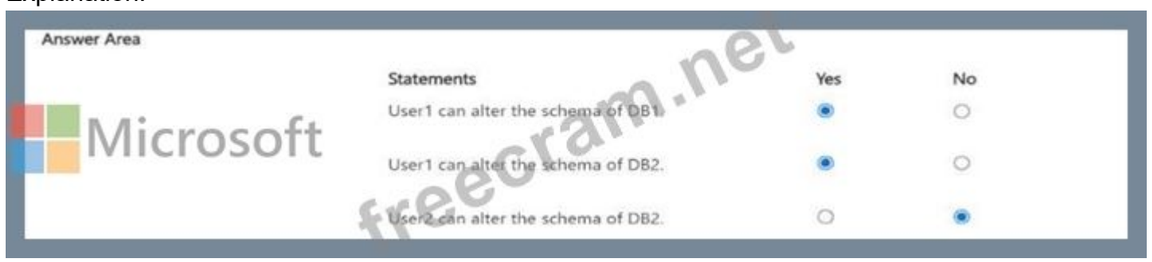
Answer Area

Statements	Yes	No
User1 can alter the schema of DB1.	○	○
User1 can alter the schema of DB2.	○	○
User2 can alter the schema of DB2.	○	○

Answer:

Answer Area

Explanation:



NEW QUESTION: 8

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: 9

You plan to deploy Azure container instances.

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

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

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

What should you include in the deployment?

A. application security groups
B. network security groups (NSGs)
C. management groups
D. container groups
Answer: (SHOW ANSWER)
Azure Container Instances supports the deployment of multiple containers onto a single host using a container group. A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process.
Reference:
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-container-groups

NEW QUESTION: 10
You have an Azure Subscription that is linked to an Azure Active Directory (Azure AD). The tenant contains the users shown in the following table.

Name	Role	Member of
User1	Security administrator	Group1
User2	Network Contributor	Group2
User3	Key Vault Contributor	Group1, Group2

You have an Azure key vault named Vault1 that has Purge protection set to Disabled. Vault1 contains the access policies shown in the following table.

Name	Key permission	Secret permission	Certificate permission
Group1	Purge	Purge	Purge
Group2	Select all	Select all	Select all

You create role assignments for Vault1 as shown in the following table.

Name	Role
User1	None
User2	Key Vault Reader
User3	User Access Administrator

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

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

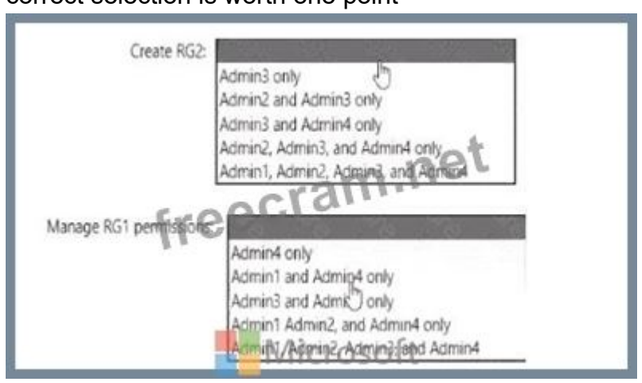
Answer:
Answer Area

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

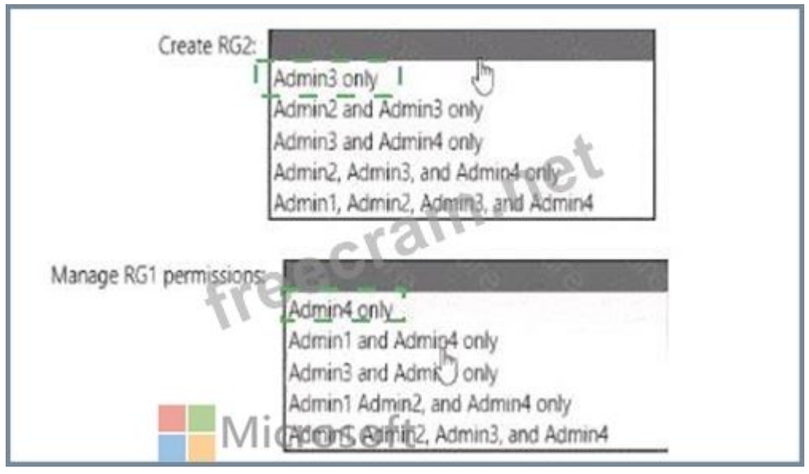
Explanation:

NEW QUESTION: 11

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

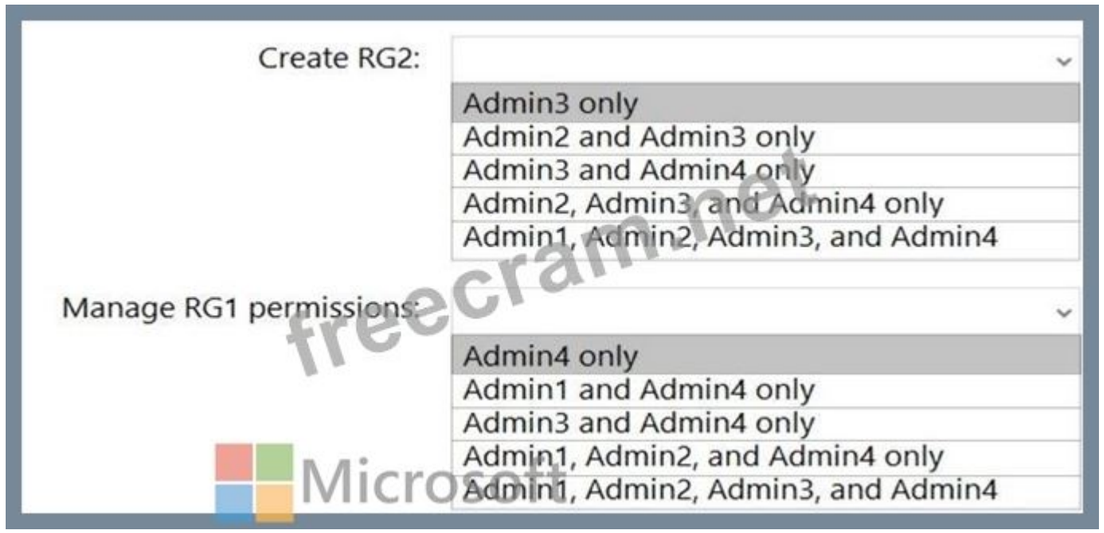


Answer:



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: 12

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

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

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

Answer Area

Answer:

Answer Area

Explanation:

A screenshot of a computer Description automatically generated

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

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

2. Share access signature

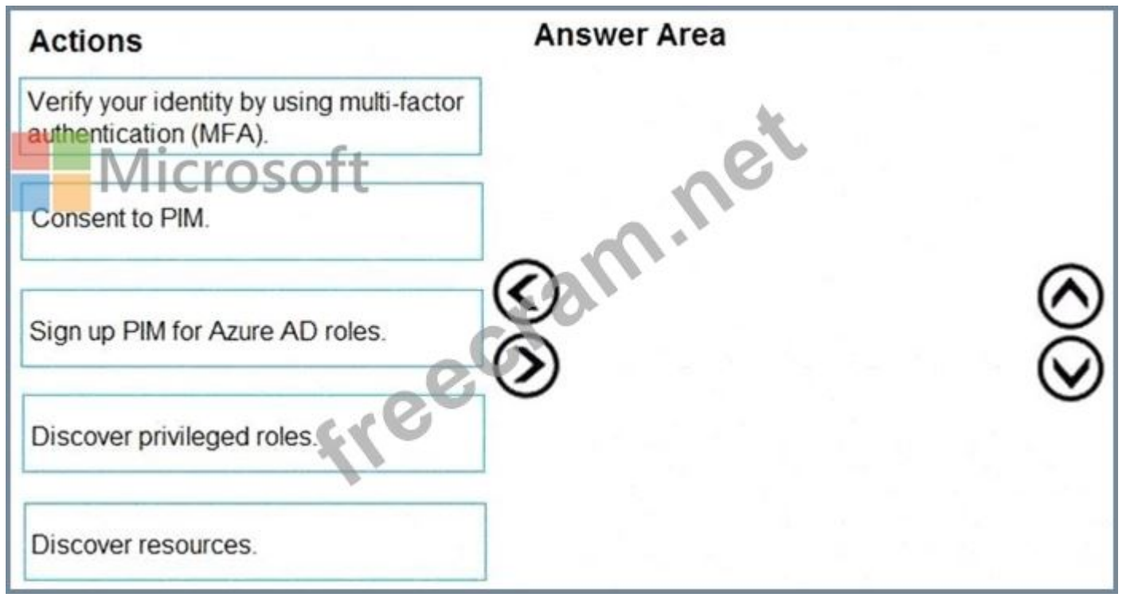
Requirement: Only grant users access to contoso2023 in the year 2023

NEW QUESTION: 13

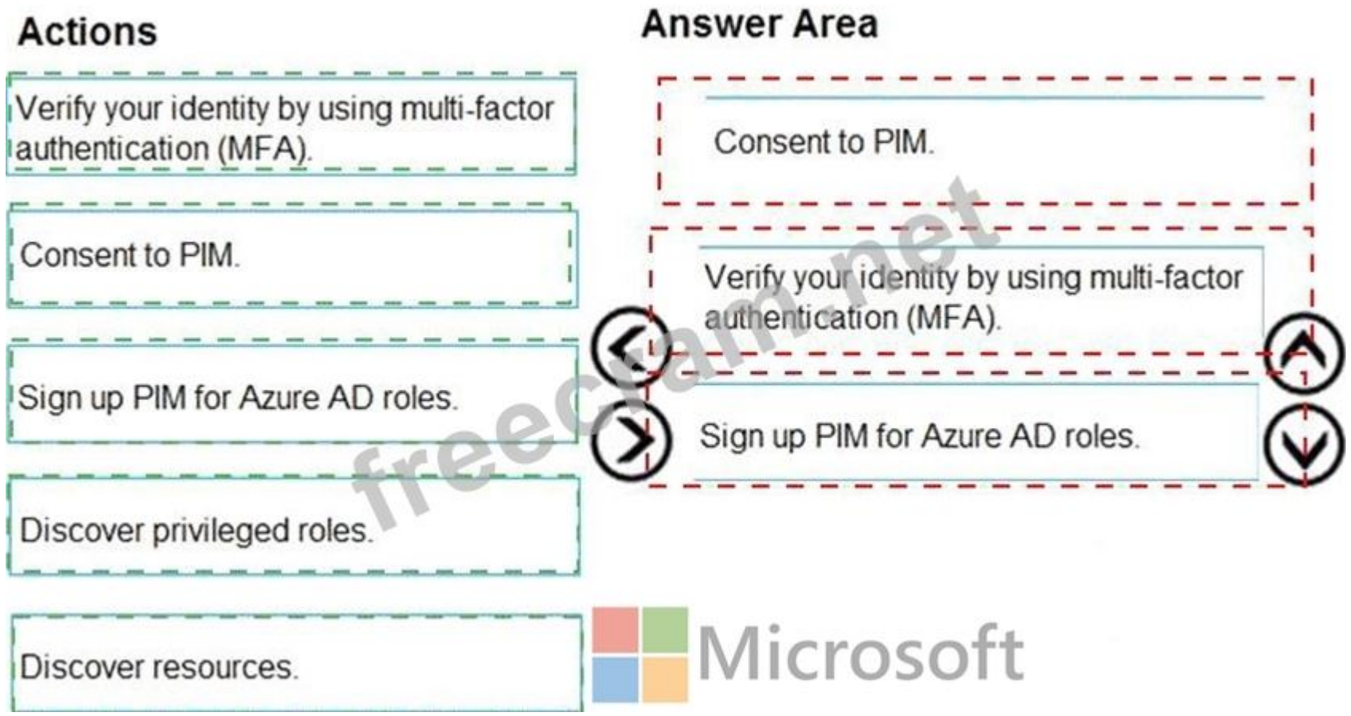
You create an Azure subscription.

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:

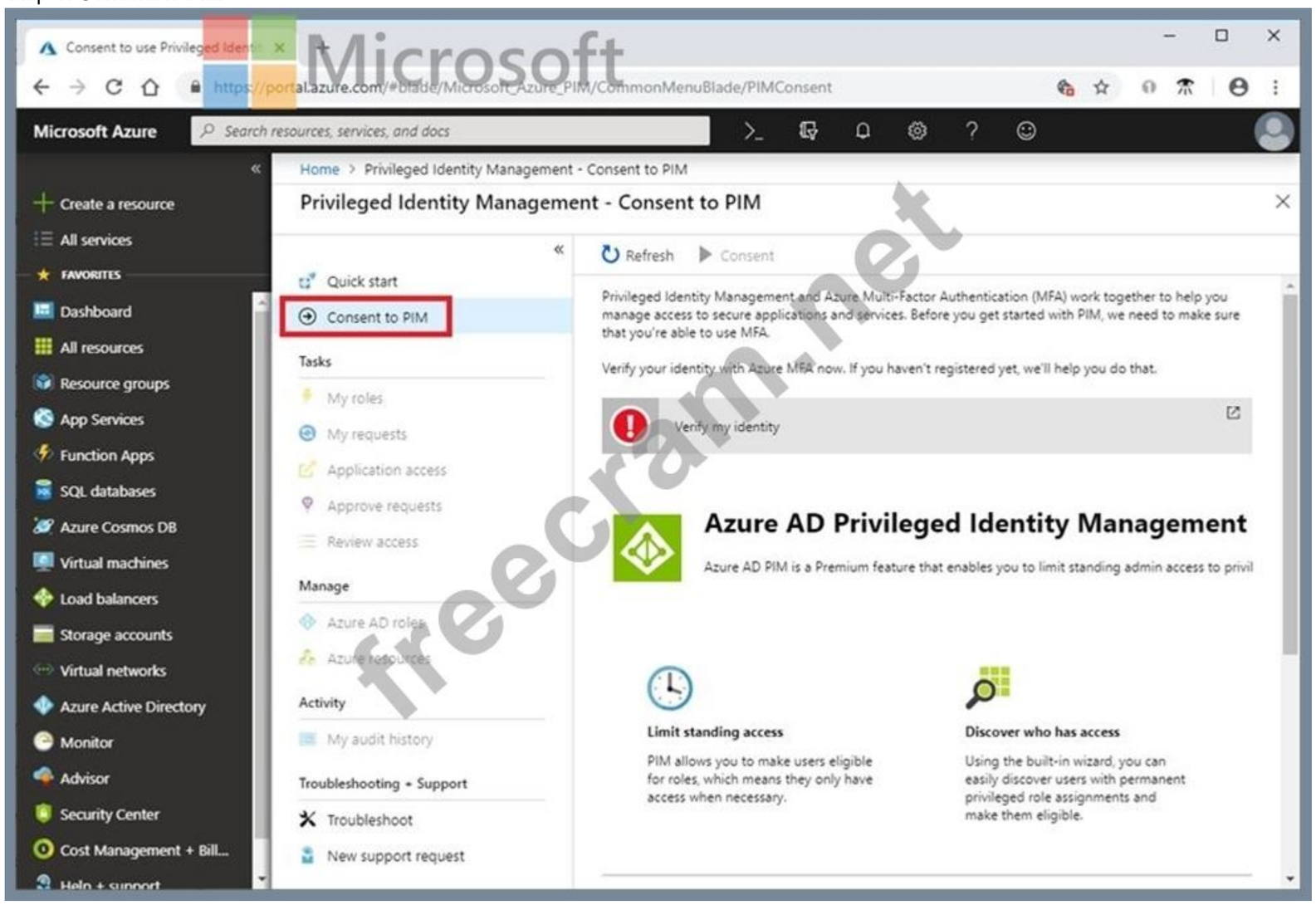
Consent to PIM.

Microsoft

Verify your identity by using multi-factor authentication (MFA).

Sign up PIM for Azure AD roles.

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: 14
You have an Azure subscription that contains the resources shown in the following table.

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

An IP address of 10.1.0.4 is assigned to VM5. VM5 does not have a public IP address.
VM5 has just in time (JIT) VM access configured as shown in the following exhibit.

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

Priority	Name	Port	Protocol	Source	Destination	Action
100	SecurityCenter-JITRule-...	3389	Any	Any	10.1.0.4	Allow
1000	SecurityCenter-JITRule_341...	3389	Any	Any	10.1.0.4	Deny
1001	RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

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

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	○	○
Remote Desktop access to VM5 is blocked.	○	○
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	○	○

Answer:

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	○	○
Remote Desktop access to VM5 is blocked.	○	○
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	○	○

Explanation:

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	○	○
Remote Desktop access to VM5 is blocked.	○	○
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	○	○

NEW QUESTION: 15

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

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

You plan to implement TLS for WebApp1.

You need to add a certificate to WebApp1.

Which certificates from Vault1 can you add to WebApp1?

A. Cert1 and Cert2 only

B. Cert1 and Cert3 only

C. Cert1, Cert2, Cert3, and Cert4

D. Cert3 and Cert4 only

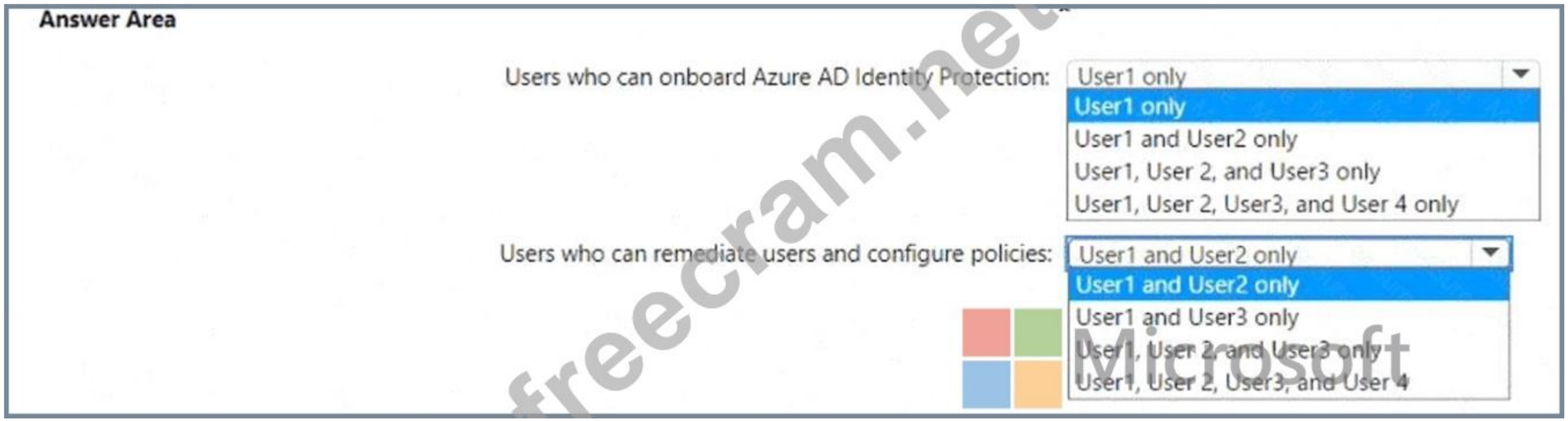
Answer: (SHOW ANSWER)

NEW QUESTION: 16
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: 17
You have an Azure subscription named Sub 1 that is associated to an Azure AD Tenant named contoso.com.
The tenant contains the users shown in the following table.

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

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



Answer:

Explanation:

NEW QUESTION: 18

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

A. From container1, change the access level.

B. From container1 add an access policy.

C. From container1, modify the Access Control (1AM) settings.

D. From storage1 , enable soft delete for blobs.

Answer: B (LEAVE A REPLY)

References:

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

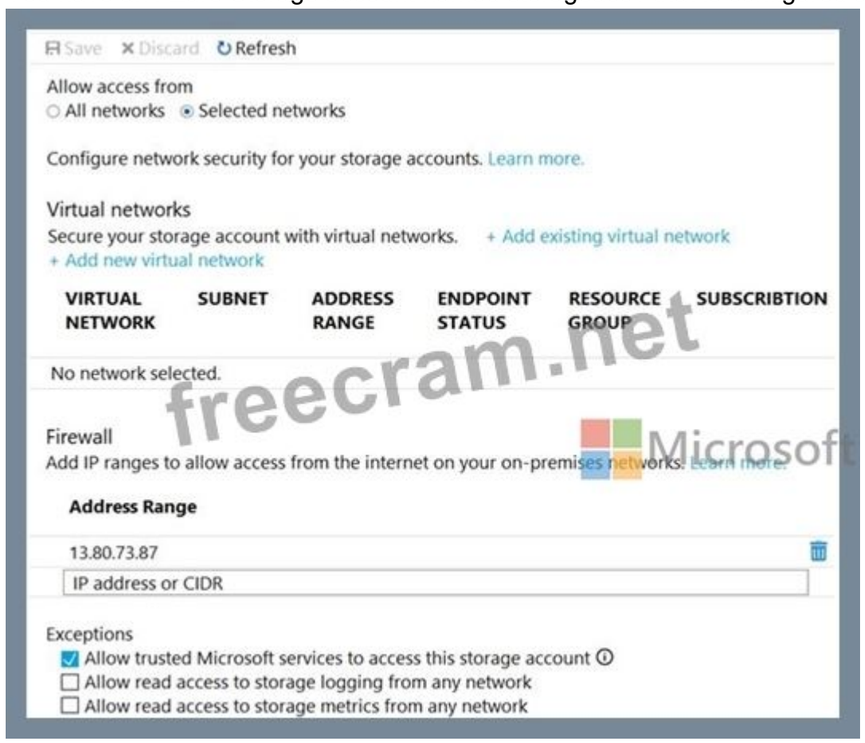
NEW QUESTION: 19

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

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

Subnet1 and Subnet2 have a Microsoft.Storage service endpoint configured.

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



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

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

Answer:

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

Explanation:

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

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

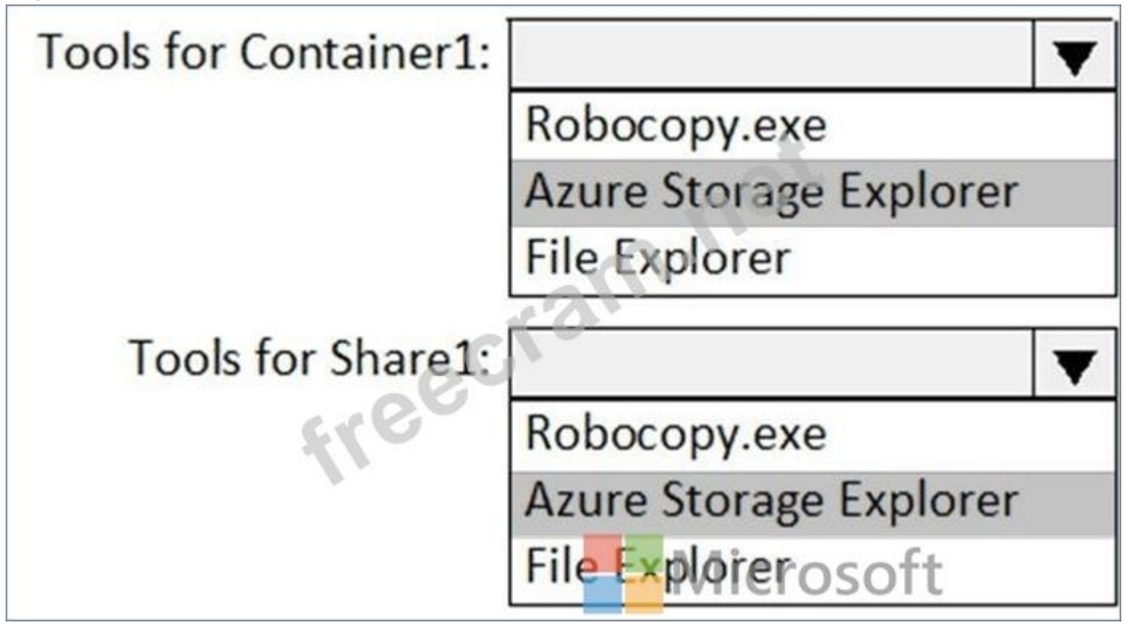
NEW QUESTION: 20
You have an Azure subscription named Sub1. Sub1 has an Azure Storage account named Storage1 that contains the resources shown in the following table.

Name	Type
Container1	Blob container
Share1	File share

You generate a shared access signature (SAS) to connect to the blob service and the file service.
Which tool can you use to access the contents in Container1 and Share! by using the SAS? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:



NEW QUESTION: 21

You have an Azure Active Directory (Azure AD) tenant.

You need to prevent nonprivileged Azure AD users from creating service principals in Azure AD.

What should you do in the Azure Active Directory admin center of the tenant?

A. From the Properties Wade, set Enable Security defaults to Yes.

B. From the User settings blade, set Restrict access to Azure AD administration portal to Yes.
C. From the User settings blade, set Users can register applications to No
D. From the Properties blade, set Access management fen Azure resources to No
Answer: (SHOW ANSWER)

NEW QUESTION: 22
You need to delegate a user to implement the planned change for Defender for Cloud.
The solution must follow the principle of least privilege.
Which user should you choose?
A. Admin2
B. Admin4
C. Admin1
D. Admin3
Answer: (SHOW ANSWER)

NEW QUESTION: 23
You have an Azure web app named WebApp1.
You upload a certificate to WebApp1.
You need to make the certificate accessible to the app code of WebApp1.
What should you do?
A. Add a user-assigned managed identity to WebApp1.
B. Add an app setting to the WebApp1 configuration.
C. Enable system-assigned managed identity for the WebApp1.
D. Configure the TLS/SSL binding for WebApp1.
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate-in-code

NEW QUESTION: 24
You have an Azure subscription.
You plan to create a workflow automation in Microsoft Defender for Cloud that will automatically remediate a security vulnerability.
What should you create first?
A. a managed identity
B. an Azure function app
C. an alert rule
D. an automation account
E. an Azure logic app
Answer: (SHOW ANSWER)

NEW QUESTION: 25
You have an Azure subscription that contains the resources shown in the following table.

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

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

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

You need to configure auditing for SQL1.

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

NOTE: Each correct selection is worth one point.

Answer Area

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

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

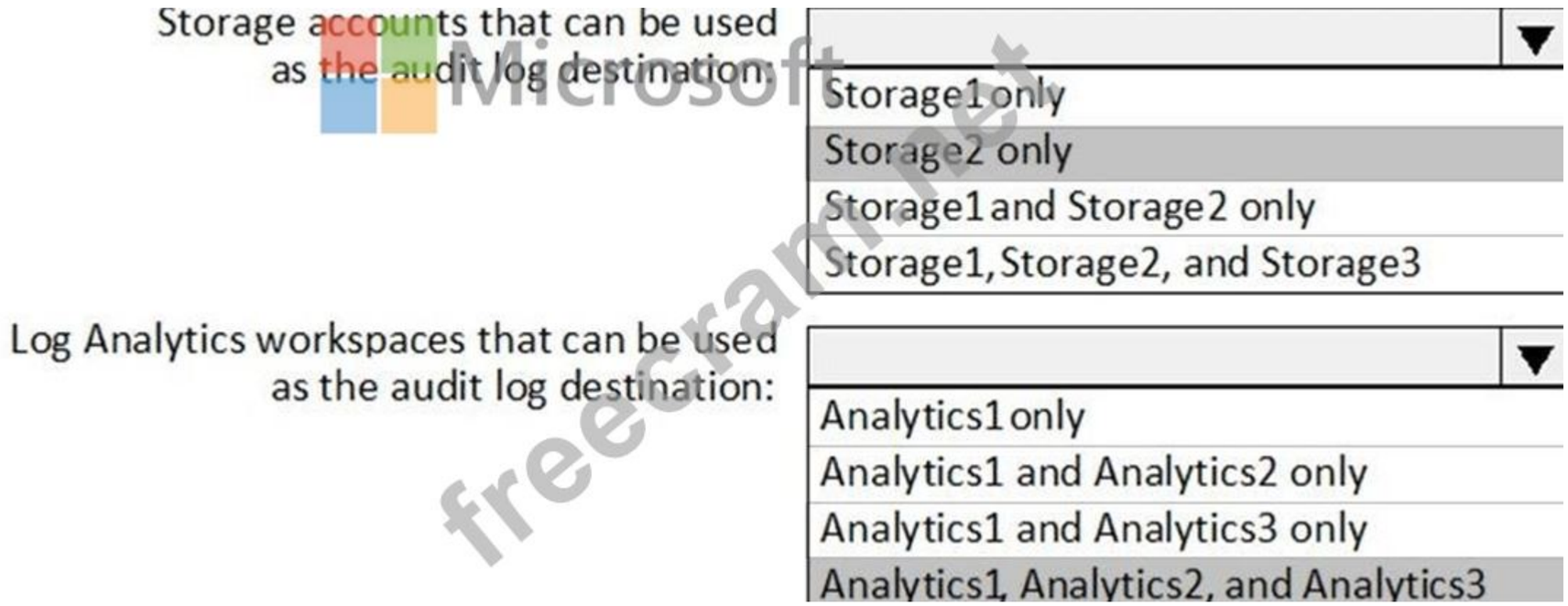
Answer:

Answer Area

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

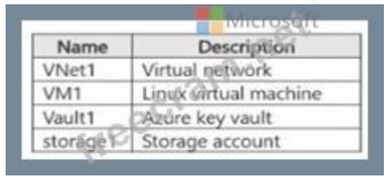
Log Analytics workspaces that can be used as the audit log destination:
- Analytics1 only
- Analytics1 and Analytics2 only
- Analytics1 and Analytics3 only
- Analytics1, Analytics2, and Analytics3

Explanation:



NEW QUESTION: 26

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



Name	Description
VNet1	Virtual network
VM1	Linux virtual machine
Vault1	Azure key vault
storage1	Storage account

You plan to implement Microsoft Defender for Cloud. Which resources can be protected by using Defender for Cloud?

A. VM1 and storage1 only

B. Vault1 and storage1 only

C. VM1, Vault1, and storage1 only

D. VNet1,VM1, Vault1. and storage1

E. VM1 only

Answer: (SHOW ANSWER)

NEW QUESTION: 27

You need to ensure that User2 can implement PIM.

What should you do first?

A. Assign User2 the Global administrator role.

B. Configure authentication methods for contoso.com.

C. Configure the identity secure score for contoso.com.

D. Enable multi-factor authentication (MFA) for User2.

Answer: (SHOW ANSWER)

To start using PIM in your directory, you must first enable PIM.
1. Sign in to the Azure portal as a Global Administrator of your directory.
You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.
Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com References:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started

NEW QUESTION: 28
You have an Azure Active Directory (Azure AD) tenant that contains two administrative units named AU1 and AU2.
Users are assigned to the administrative units as shown in the following table.

User name	Member of
Admin1	AU1
Admin2	AU1
Admin3	AU2
Admin4	AU2
User1	AU1

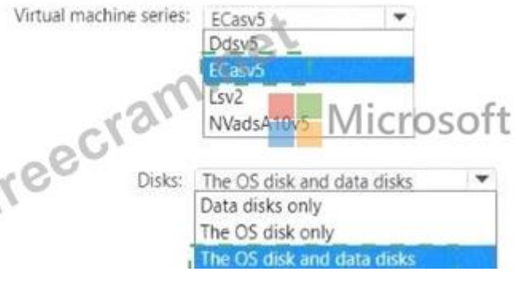
Answer:

Explanation:

NEW QUESTION: 29
You have an Azure subscription.
You plan to deploy a virtual machine named VM1.

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

Answer:



Explanation:

NEW QUESTION: 30

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

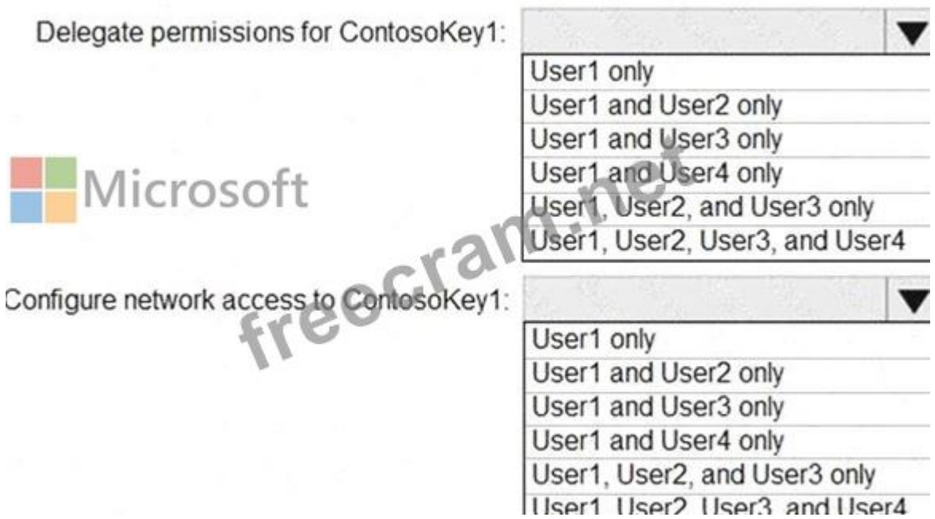
Answer: (SHOW ANSWER)
https://learn.microsoft.com/en-us/azure/app-service/configure-authentication-provider-google

NEW QUESTION: 31
You have an Azure subscription that contains an Azure Files share named share1 and a user named User1.
Identity-based authentication is configured for share1.
User1 attempts to access share1 from a Windows 10 device by using SMB.
Which type of token will Azure Files use to authorize the request?
A. OAuth 20
B. JSON Web Token (JWT)
C. Kerberos
D. SAML
Answer: (SHOW ANSWER)
https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain- service-enable?tabs=azure-portal

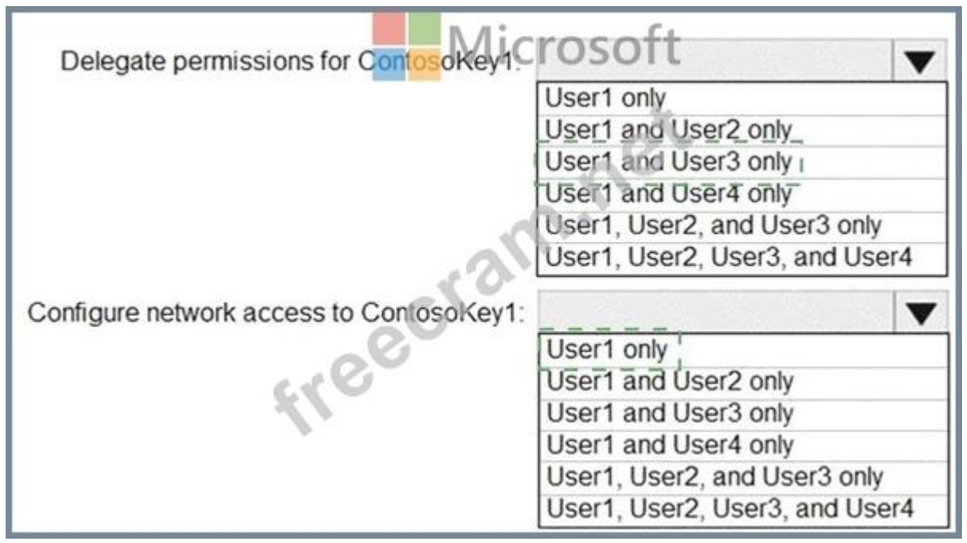
NEW QUESTION: 32
You have an Azure subscription that contains an Azure key vault named ContosoKey1.
You create users and assign them roles as shown in the following table.

Name	Subscription role assignment	ContosoKey1 role assignment
User1	Owner	*None*
User2	Security Admin	*None*
User3	*None*	User Access Administrator
User4	*None*	Key Vault Contributor

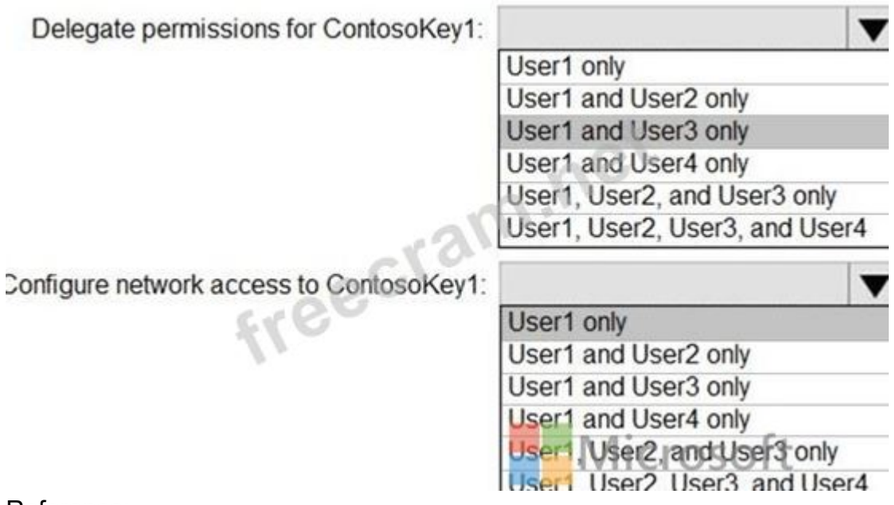
You need to identify which users can perform the following actions:
* Delegate permissions for ContsosKey1.
* Configure network access to ContosoKey1.
Which users should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



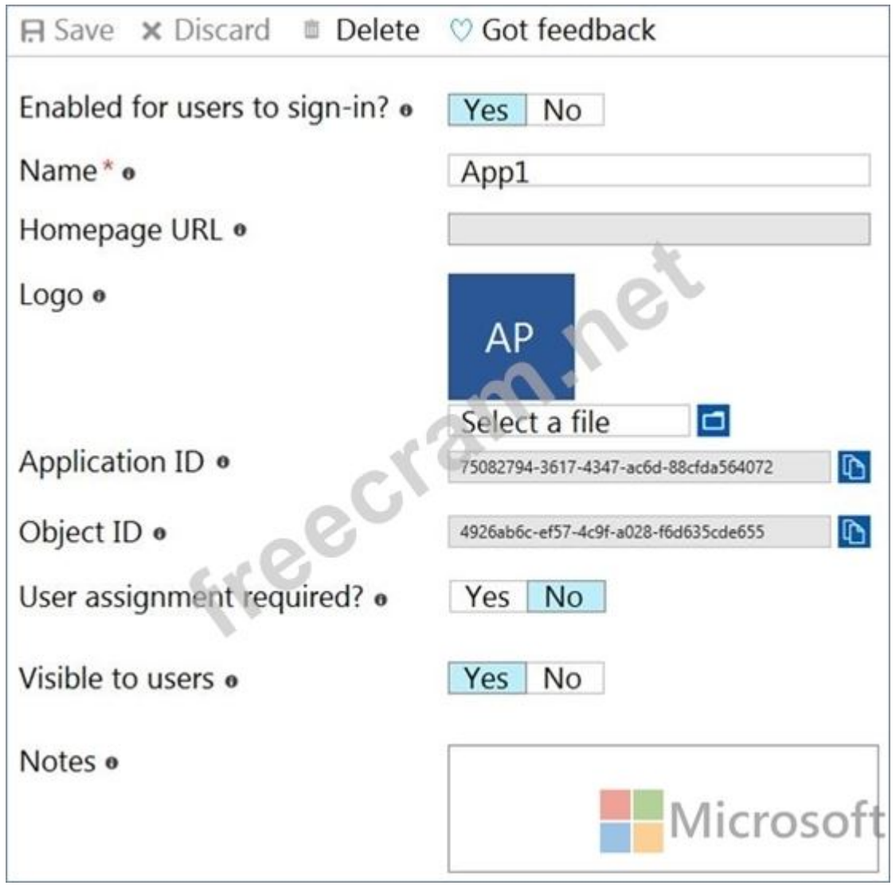
Reference:
https://docs.microsoft.com/en-gb/azure/key-vault/general/rbac-guide

NEW QUESTION: 33
You have an Azure subscription that uses Microsoft Defender for Cloud. The subscription contains an instance of Azure Database for PostgreSQL.
You need to ensure that an email alert is triggered when a suspected brute force attack on the database is detected. The solution must minimize administrative effort.
What should you configure?
A. the Azure Monitor activity log
B. the PostgreSQL Audit extension (pgAudit)
C. an Azure Monitor alert rule
D. Microsoft Defender for open-source relational databases
Answer: (SHOW ANSWER)

NEW QUESTION: 34
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains three security groups named Group1, Group2, and Group3 and the users shown in the following table.

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

Group3 is a member of Group2.
In contoso.com, you register an enterprise application named App1 that has the following settings:
* Owners: User1
* Users and groups: Group2
You configure the properties of App1 as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 has App1 listed on his My Apps portal.	○	○
User2 has App1 listed on her My Apps portal.	○	○
User3 has App1 listed on her My Apps portal.	○	○

Answer:

Explanation:

Text Description automatically generated

Reference:

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

NEW QUESTION: 35

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

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

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

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

The outbound traffic of which app is controlled by using NSG1?

A. App4 only

B. App3 and App4 only
C. App1, App2, App3, andApp4
D. App2, App3, and App4 only
Answer: (SHOW ANSWER)

NEW QUESTION: 36
You have an Azure subscription that contains the resources shown in the following table.

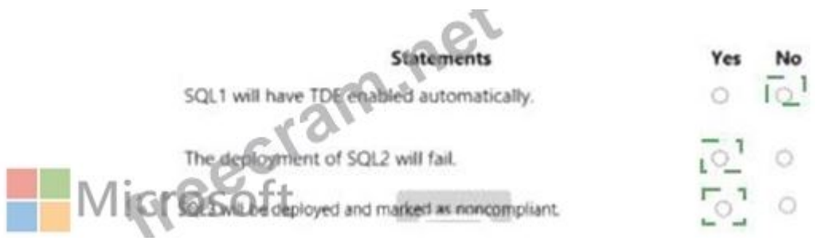
Name	Type	Resource group
RG1	Resource group	**Not applicable**
RG2	Resource group	**Not applicable**
RG3	Resource group	**Not applicable**
SQL1	Azure SQL Database	RG3

Transparent Data Encryption (TDE) is disabled on SQL1.
You assign polices to the resource groups as shown in the following table.

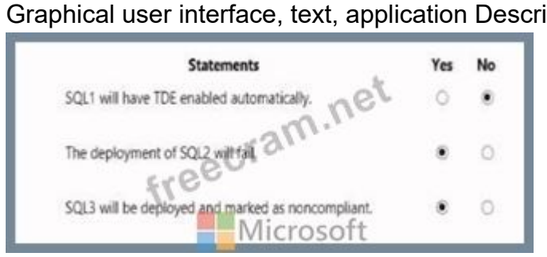
Name	Condition	Effect if condition is false	Assignment
Policy1	TDE enabled	`Deny`	RG1, RG2
Policy2	TDE enabled	`DeployIfNotExists`	RG2, RG3
Policy3	TDE enabled	`Audit`	RG1

You plan to deploy Azure SQL databases by using an Azure Resource Manager (ARM) template. The databases will be configured as shown in the following table.
NOTE: Each correct selection is worth one point.

Answer:
Answer Area



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



NEW QUESTION: 37

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

NEW QUESTION: 38
You have a web app hosted on an on-premises server that is accessed by using a URL of https://www.contoso.
com. You plan to migrate the web app to Azure. You will continue to use https://www.contoso.com. You need to enable HTTPS for the Azure web app. What should you do first?
A. Export the public key from the on-premises server and save the key as a P7b file.
B. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using TripleDES.
C. Export the public key from the on-premises server and save the key as a CER file.
D. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using AES256.
Answer: (SHOW ANSWER)
https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate#private-certificate-requirements

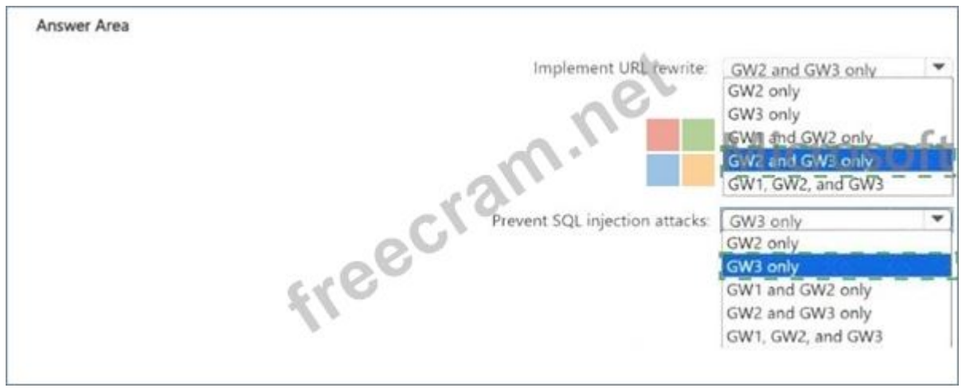
NEW QUESTION: 39
You have an Azure subscription that contains an Azure key vault.
You need to configure maximum number of days for Which new keys are valid. The solution must minimize administrative effort.
What should you use?
A. Key Vault properties
B. Azure Policy
C. Azure Purview
D. Azure Blueprints
Answer: (SHOW ANSWER)

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

Name	Tier
GW1	Basic
GW2	Standard V2
GW3	WAF V2

You need to configure settings to implement URL rewrite and prevent SQL injection attacks.
Which application gateways support each requirement? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.

Answer:



Explanation:

NEW QUESTION: 41

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:

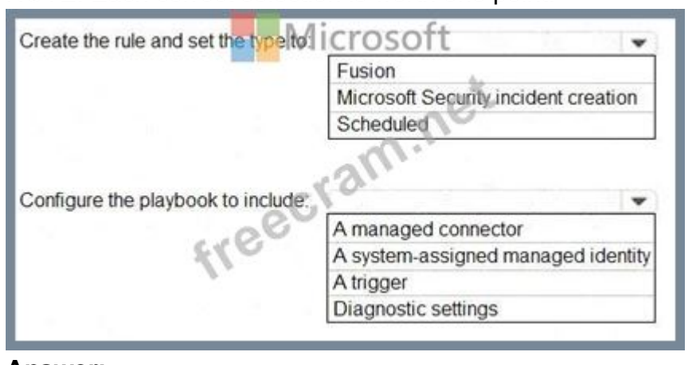
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

NEW QUESTION: 42
You have an Azure subscription that contains the resources shown in the following Table.

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

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

NEW QUESTION: 43
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:

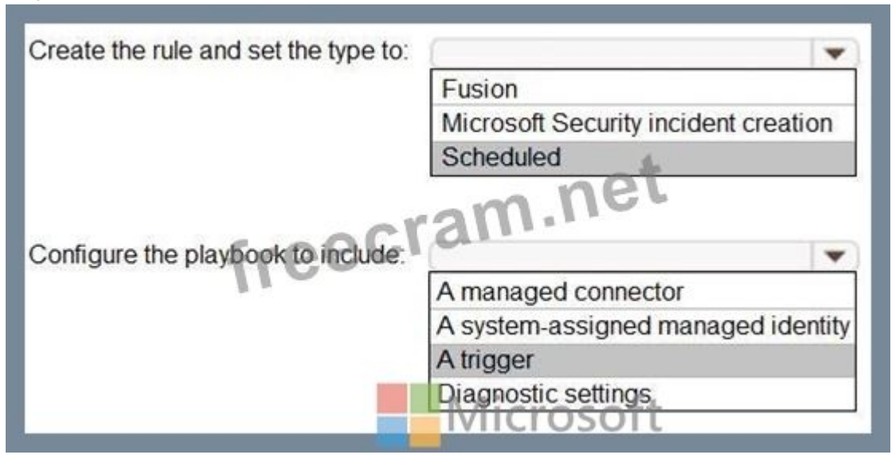
Create the rule and set the type to:

- Fusion
- Microsoft Security incident creation
- Scheduled

Configure the playbook to include:

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

Explanation:



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

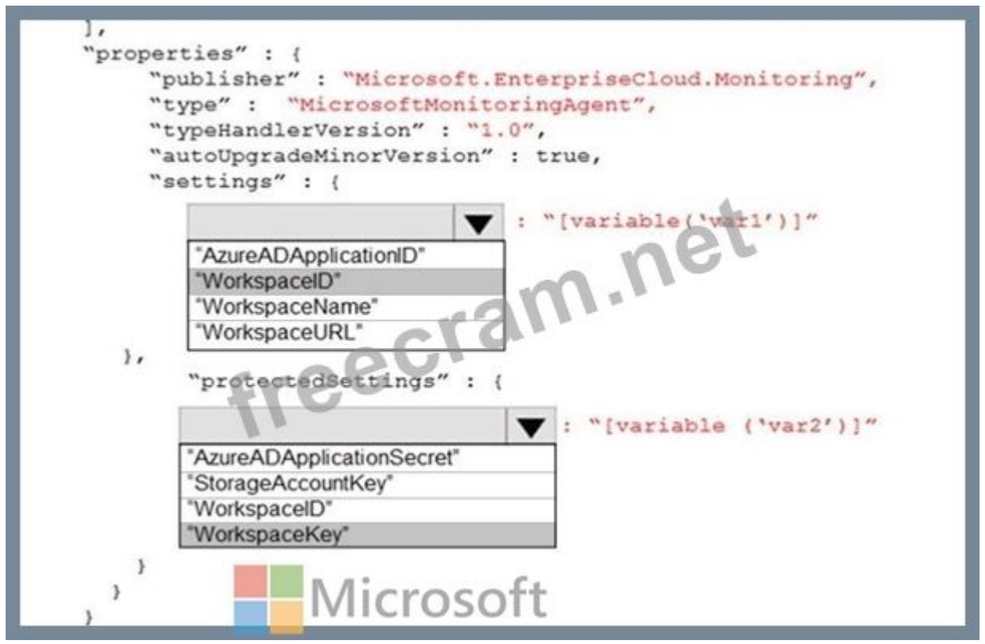
NEW QUESTION: 44
You plan to use Azure Log Analytics to collect logs from 200 servers that run Windows Server 2016.
You need to automate the deployment of the Microsoft Monitoring Agent to all the servers by using an Azure Resource Manager template.
How should you complete the template? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

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


Answer:

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

Explanation:



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

NEW QUESTION: 45

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

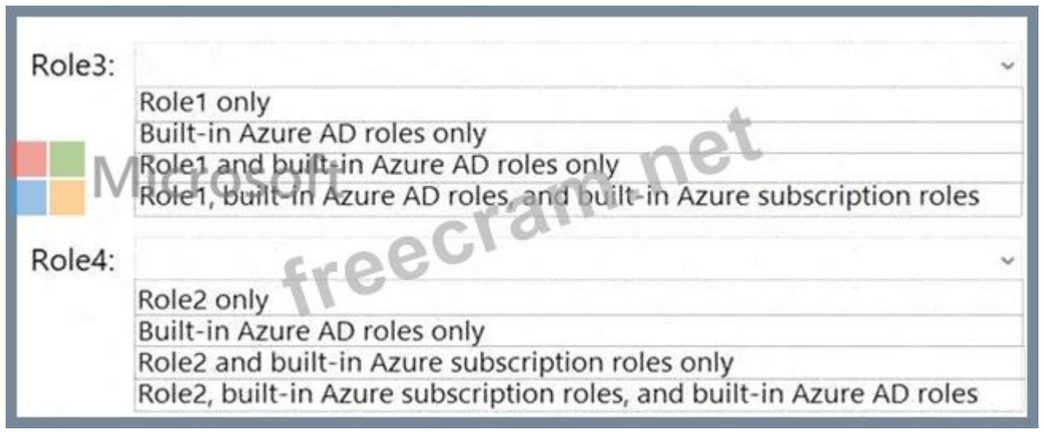
Name	Type
Role1	Azure Active Directory (Azure AD)
Role2	Azure subscription

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

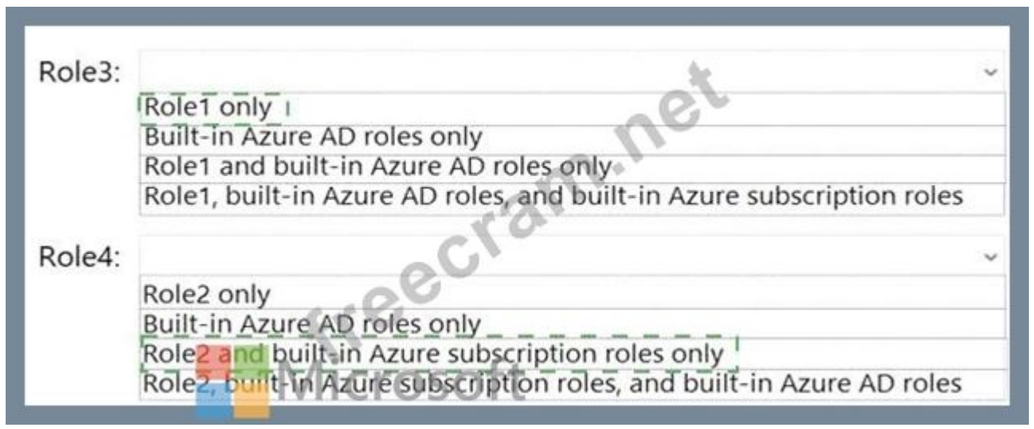
Name	Type
Role3	Azure AD
Role4	Azure subscription

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

NOTE: Each correct selection is worth one point.

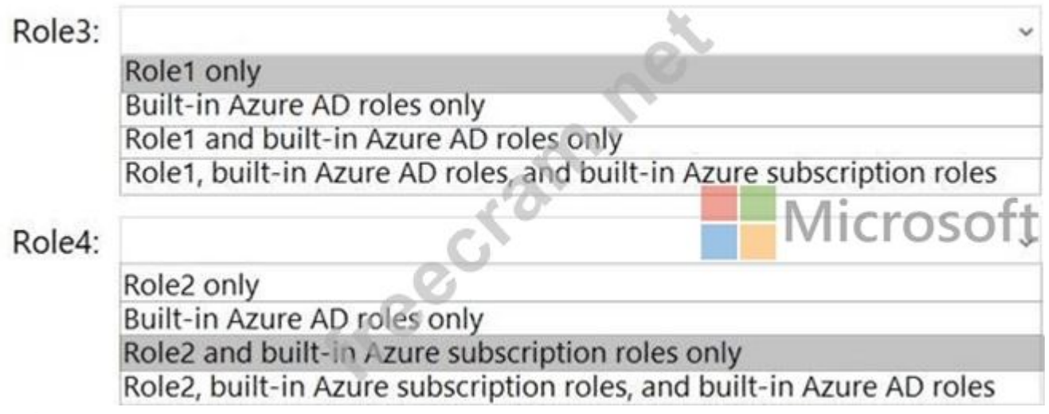


Answer:



Explanation:

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



Reference:

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

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

NEW QUESTION: 46

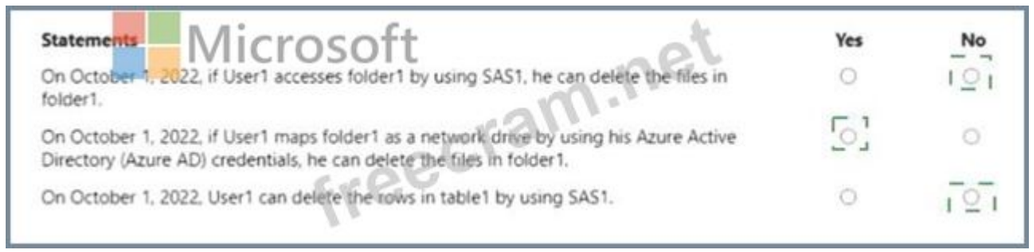
You have an Azure subscription that contains a user named User1 and a storage account named storage 1. The storage1 account contains the resources shown in the following table:

Name	Type
container1	Container
folder1	File share
table1	Table

User1 is assigned the following roles for storage1:

* Storage Blob Data Reader
* Storage Table Data Contributor
* Storage File Data SMB Share Reader

Answer:



Explanation:

No, Yes, No

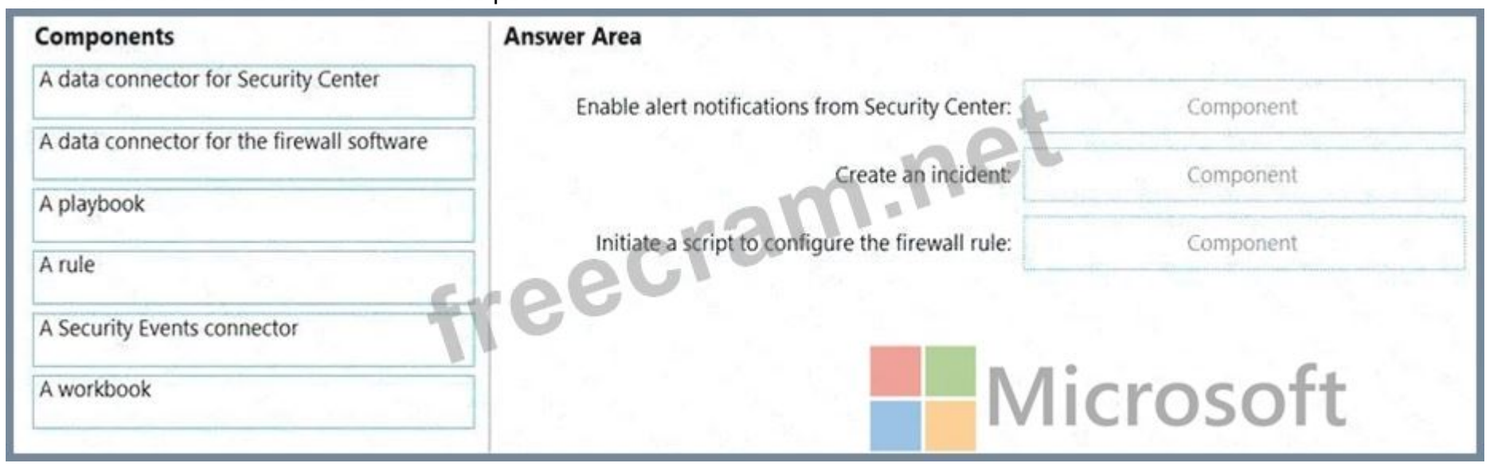
NEW QUESTION: 47

You have an Azure subscription that contains the following resources:

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

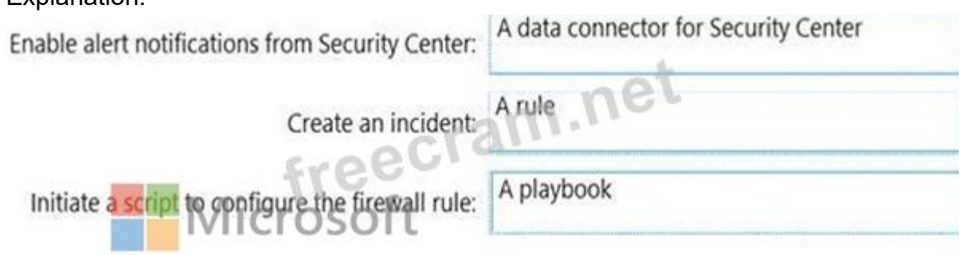
You need to ensure that when a high-priority alert is generated in Security Center for a virtual machine, an incident is created in Azure Sentinel and then a script is initiated to configure a firewall rule for the NVA.

How should you configure Azure Sentinel to meet the requirements? To answer, drag the appropriate components to the correct requirements. Each component may be used once, more than once, or not at all.
You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Answer:

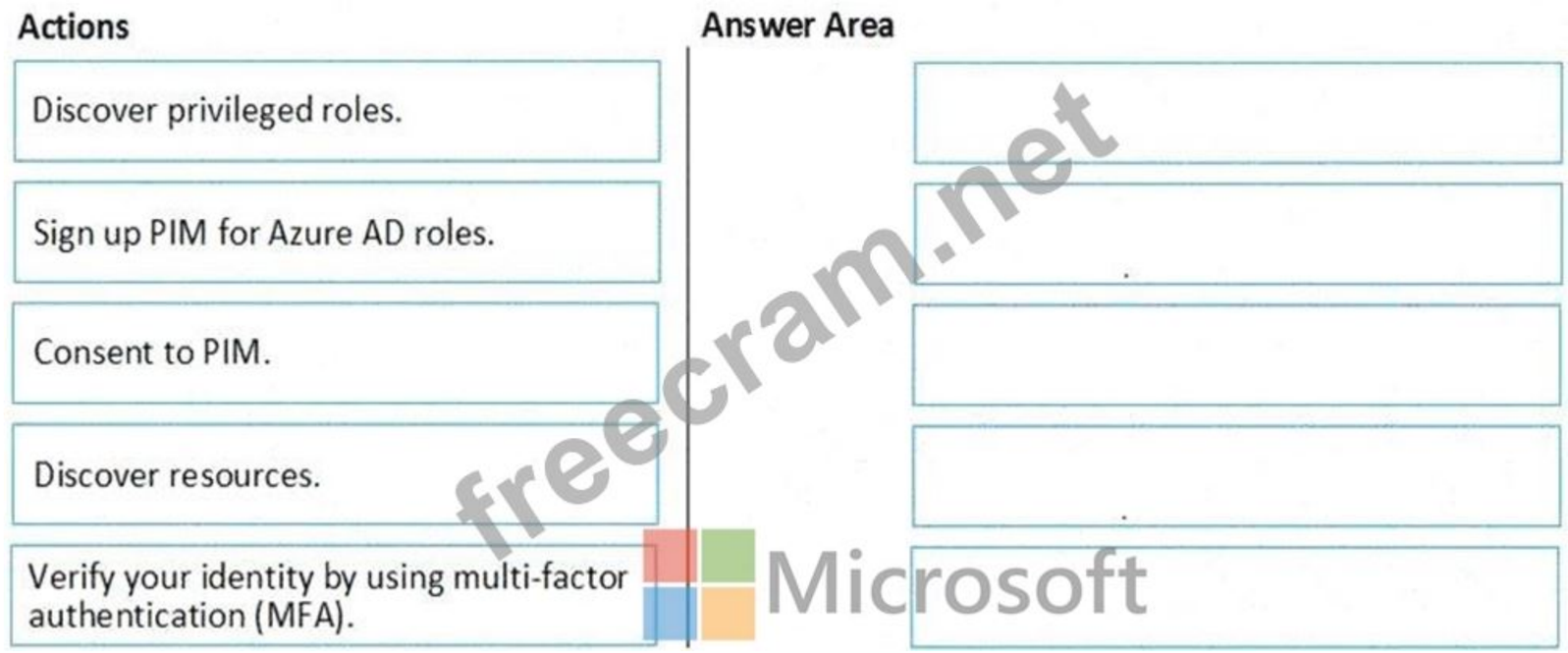
Explanation:



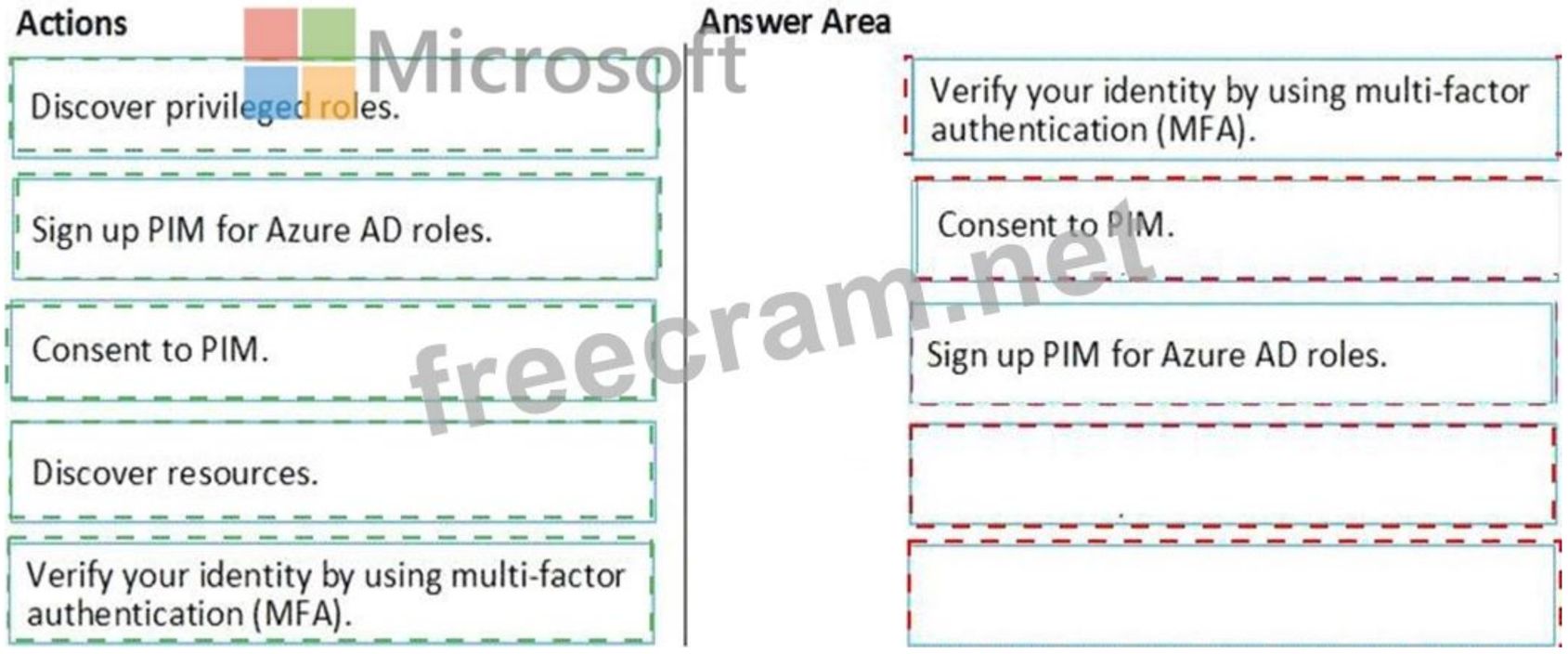
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

NEW QUESTION: 48
You need to implement the planned change for VM1 to access storage1.
The solution must meet the technical requirements.
What should you do first?
A. Configure federated identity credentials for ID1.
B. Assign ID1 to VM1.
C. Configure a system-assigned managed identity on VM1.
D. Assign the Storage Blob Data Reader role to storage 1.
E. Add a role assignment condition to storage1.
Answer: (SHOW ANSWER)

NEW QUESTION: 49
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:



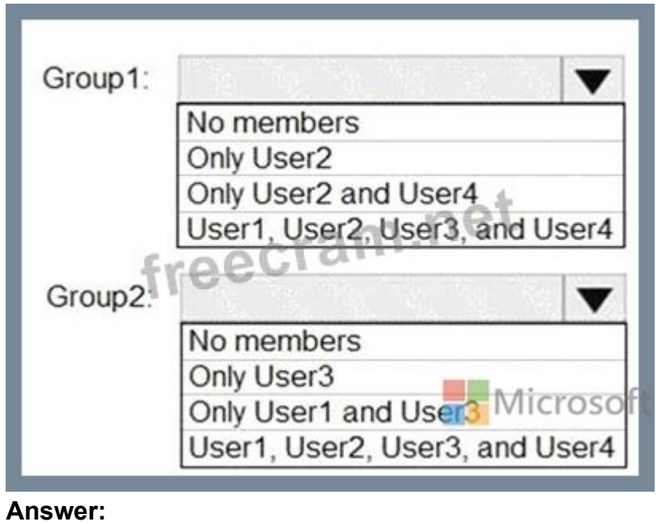
Explanation:

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

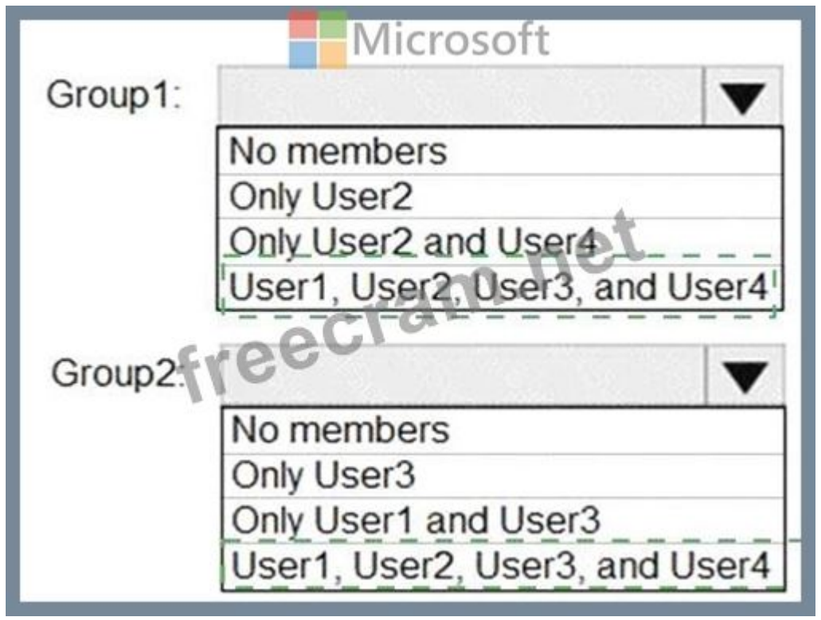
NEW QUESTION: 50

What is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Box 1: User1, User2, User3, User4

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

Box 2: User1, User2, User3, User4

References:

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

NEW QUESTION: 51

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

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

What should you use?

A. device compliance policies in Microsoft Intune

B. Azure Automation State Configuration

C. application security groups

D. Azure Advisor

Answer: (SHOW ANSWER)

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

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

References:

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

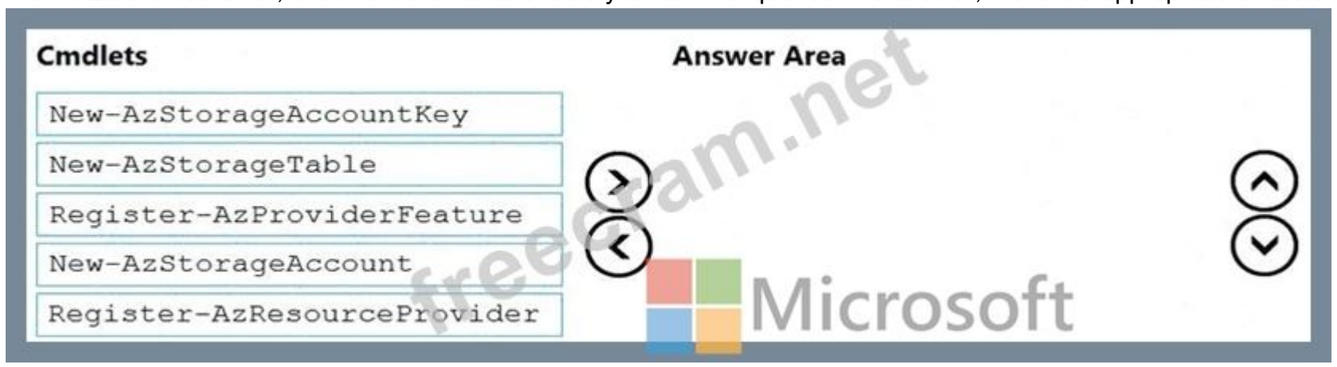
NEW QUESTION: 52

You have an Azure subscription.

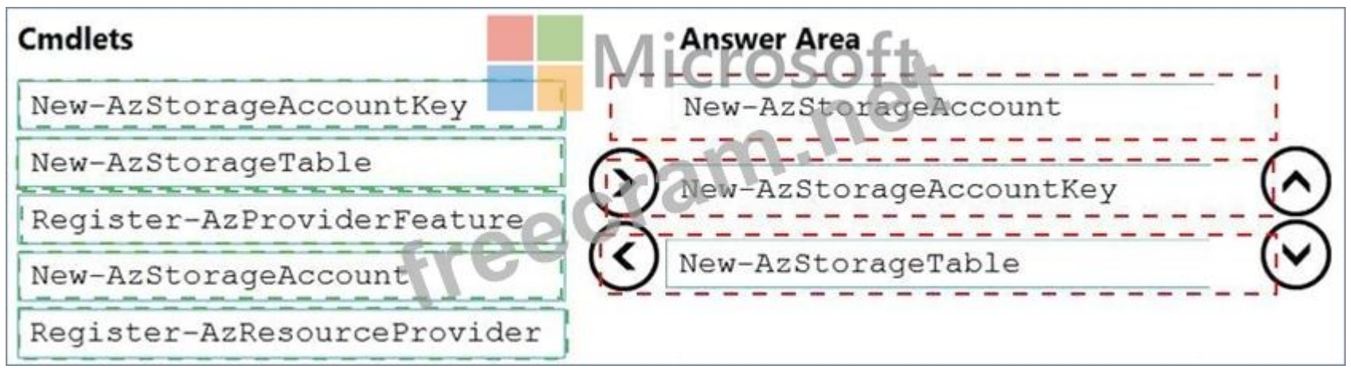
You plan to create a storage account.

You need to use customer-managed keys to encrypt the tables in the storage account.

From Azure Cloud Shell, which three cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.

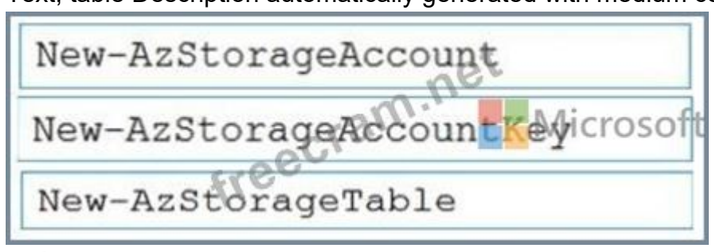


Answer:



Explanation:

Text, table Description automatically generated with medium confidence



Reference:

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

NEW QUESTION: 53

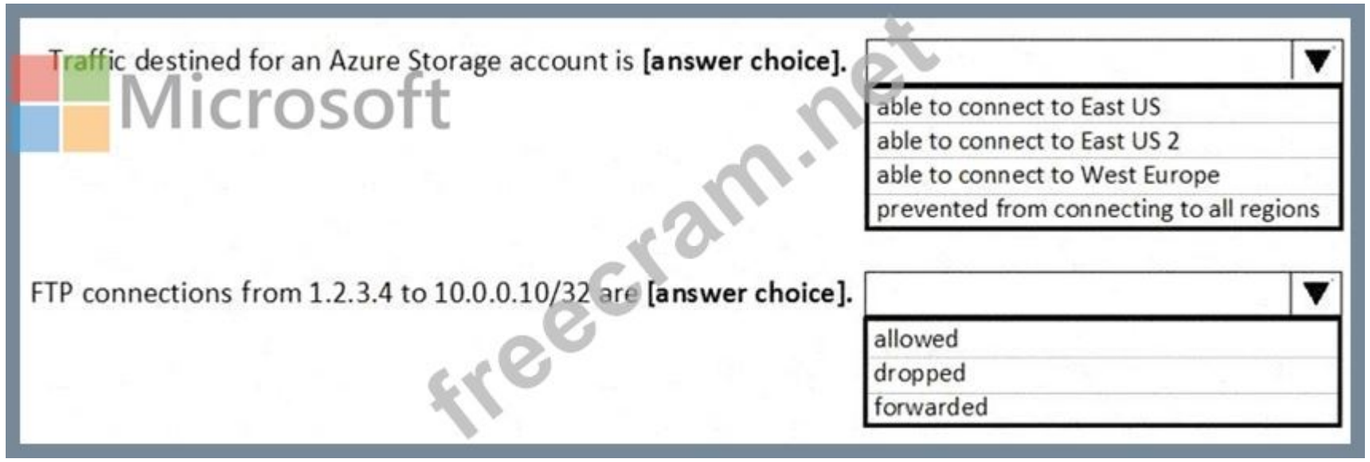
You have a network security group (NSG) bound to an Azure subnet.

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

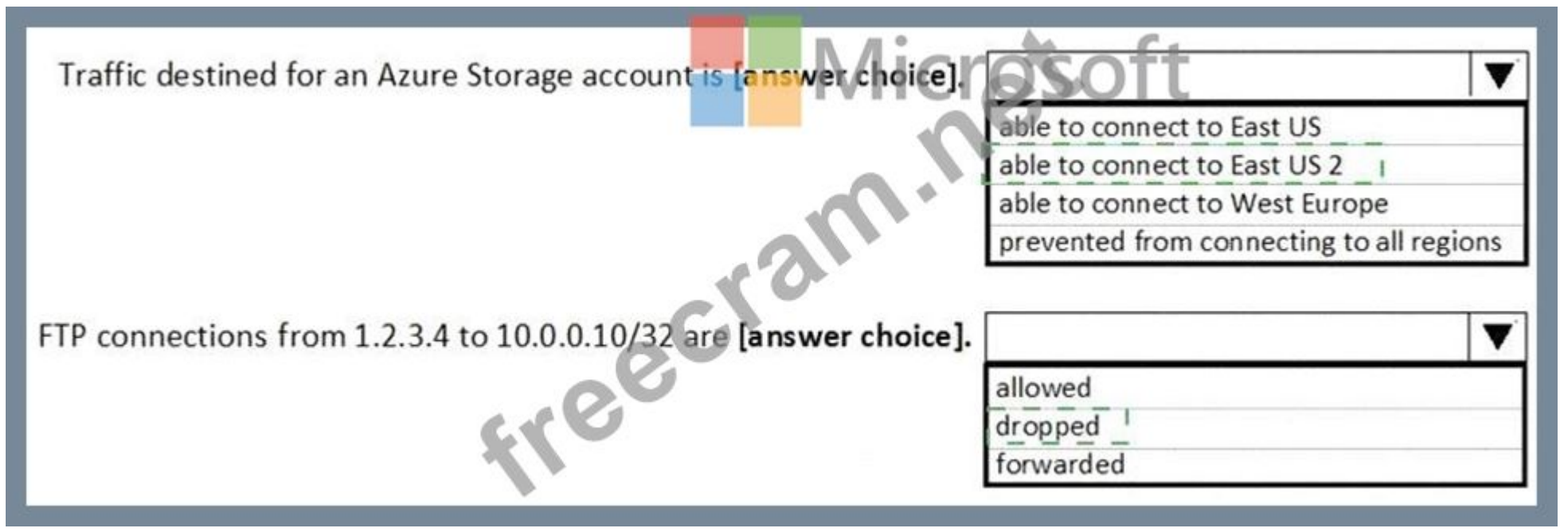
```
Name                                    :  DenyStorageAccess
Description                             :
Protocol                                :  *
SourcePortRange                         :  {*}
DestinationPortRange                    :  {*}
SourceAddressPrefix                     :  {*}
DestinationAddressPrefix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

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


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

NOTE: Each correct selection is worth one point.



Answer:



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

NEW QUESTION: 54
You have an Azure subscription name Sub1 that contains an Azure Policy definition named Policy1. Policy1 has the following settings:
Definition location: Tenant Root Group
Category: Monitoring
You need to ensure that resources that are noncompliant with Policy1 are listed in the Azure Security Center dashboard.
What should you do first?
A. Change the Category of Policy1 to Security Center.

B. Add Policy1 to a custom initiative.
C. Change the Definition location of Policy1 to Sub1.
D. Assign Policy1 to Sub1.
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/overview

NEW QUESTION: 55
You have a management group named MG1 that contains an Azure subscription and a resource group named RG1. RG1 contains a virtual machine named VM1. You have the custom Azure roles shown in the following table.

Name	Scoped to
Role1	MG1
Role2	RG1

The permissions for Role1 are shown in the following role definition file.

```
"permissions": [
        {
                "Microsoft.Compute/virtualMachines/*"
            ],
            "notActions": [
                "Microsoft.Compute/virtualMachines/delete"
            ],
            "dataActions": [],
The permissions for Role2 are shown in the following role definition file.
"permissions": [
        {
            "actions": [
                "Microsoft.Compute/virtualMachines/*"
            ],
            "notActions": [],
            "dataActions": [],
            "notDataActions": []
        }
]
```

You assign the roles to the users shown in the following table.

Name	Role
User1	Role1
User2	Role1, Role2
User3	Role2

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

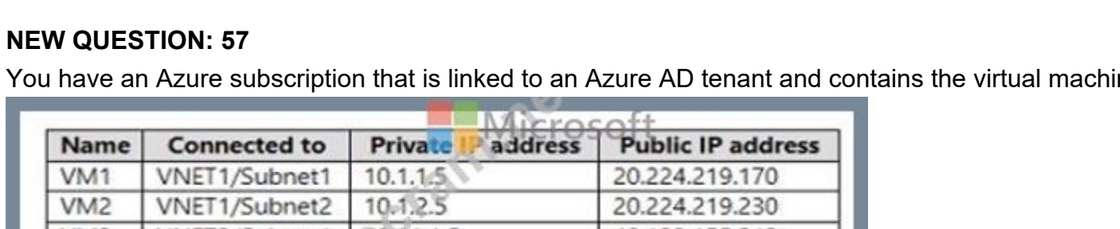
Statements	Yes	No
User1 can delete VM1.	○	○
User2 can delete VM1.	○	○
User3 can delete VM1.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can delete VM1.	○	○
User2 can delete VM1.	○	○
User3 can delete VM1.	○	○

Explanation:



NEW QUESTION: 56

You have the Azure resource shown in the following table.

Name	Type	Parent
Management1	Management group	Tenant Root Group
Subscription1	Subscription	Management1
RG1	Resource group	Subscription1
RG2	Resource group	Subscription1
VM1	Virtual machine	RG1
VM2	Virtual machine	RG2

You need to meet the following requirements:

* Internet-facing virtual machines must be protected by using network security groups (NSGs).
* All the virtual machines must have disk encryption enabled.

What is the minimum number of security that you should create in Azure Security Center?

A. 3
B. 1
C. 4
D. 2

Answer: (SHOW ANSWER)

NEW QUESTION: 57

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

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

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

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

You create the resources shown in the following table.

Name	Type
storage1	Azure Storage account
Vault1	Azure Key Vault

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

Answer:

Explanation:

NEW QUESTION: 58

Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

The company develops an application named App1. App1 is registered in Azure AD.

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

NEW QUESTION: 59
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: 60
You need to implement the function apps to meet the technical requirements.
Which apps should you include in the implementation?

A. Fa1 and Fa3 only
B. Fa1 and Fa2 only
C. Fa1, Fa2, and Fa3
D. Fa2 and Fa3 only
Answer: (SHOW ANSWER)

NEW QUESTION: 61
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: 62
You have an Azure subscription that contains a storage account named storage1 and several virtual machines.
The storage account and virtual machines are in the same Azure region. The network configurations of the virtual machines are shown in the following table.

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

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

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

You configure the following Firewall and virtual networks settings for storage1:
* Allow access from: Selected networks
* Virtual networks: VNET3\Subnet3
* Firewall - Address range: 52.233.129.0/24
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
VM1 can connect to storage1.	○	○
VM2 can connect to storage1.	○	○
VM3 can connect to storage1.	○	○

Answer:

Statements	Yes	No
VM1 can connect to storage1.	○	◉
VM2 can connect to storage1.	◉	○
VM3 can connect to storage1.	○	◉

Explanation:

Box 1: No

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

Box 2: Yes

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

Box 3: No

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

NEW QUESTION: 63

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

Name	Type
storage1	Storage account
storage2	Storage account
VM1	Virtual machine
VM2	Virtual machine
Analytics1	Log Analytics workspace

You need to enable Microsoft Defender for Cloud for storage accounts and virtual machines.

At which levels can you enable Defender for Cloud for the storage accounts and the virtual machines? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point

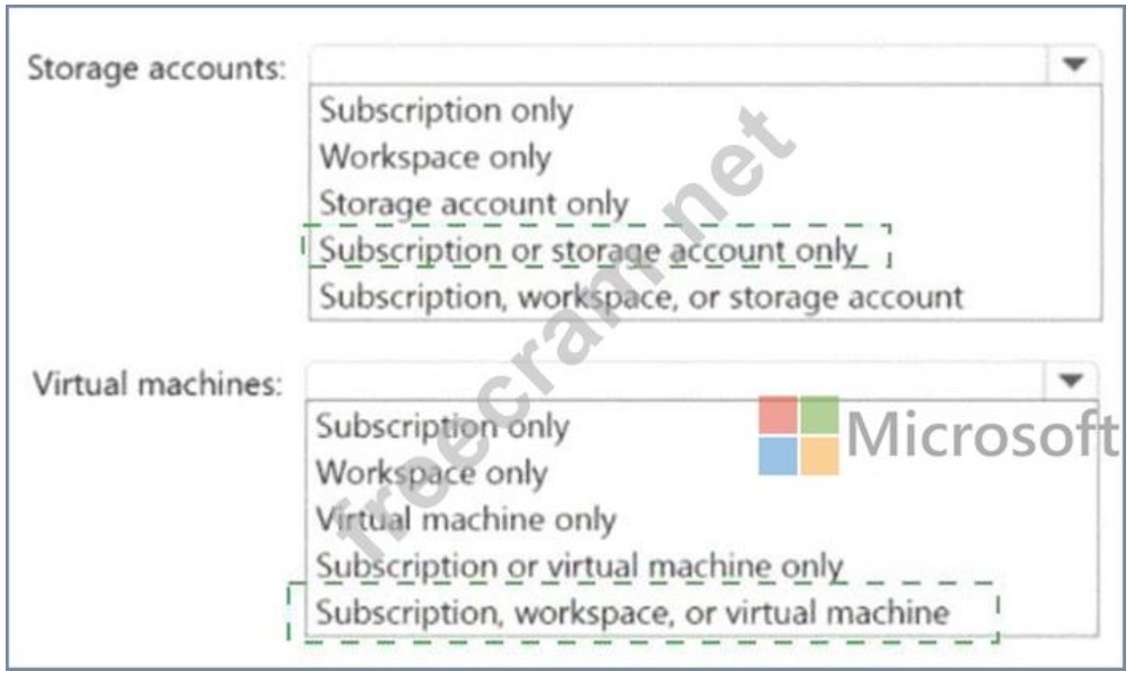
Storage accounts:

- Subscription only
- Workspace only
- Storage account only
- Subscription or storage account only
- Subscription, workspace, or storage account

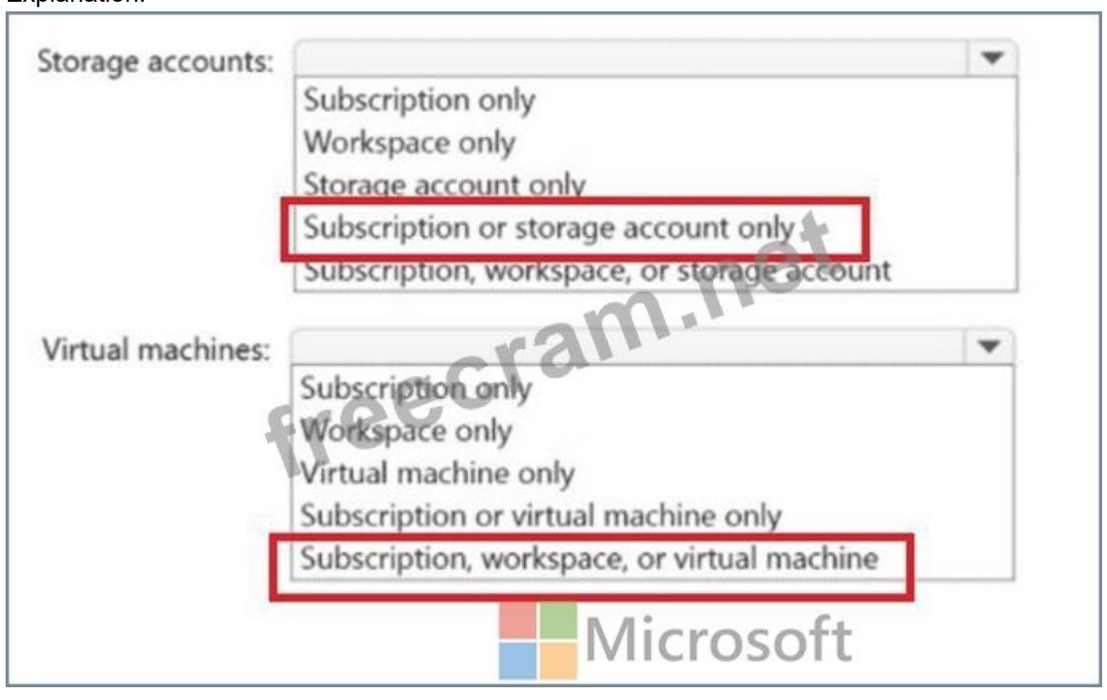
Virtual machines:

- Subscription only
- Workspace only
- Virtual machine only
- Subscription or virtual machine only
- Subscription, workspace, or virtual machine

Answer:



Explanation:



NEW QUESTION: 64

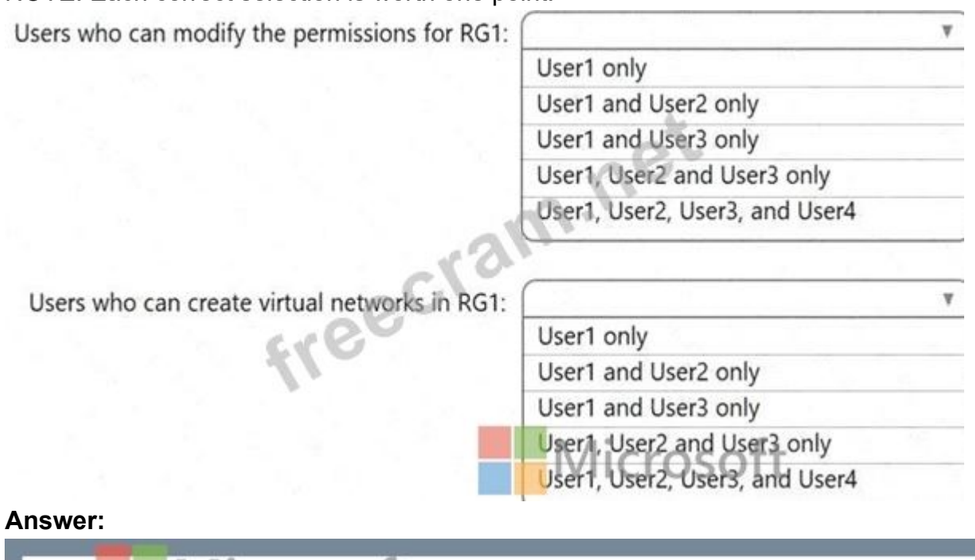
You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

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

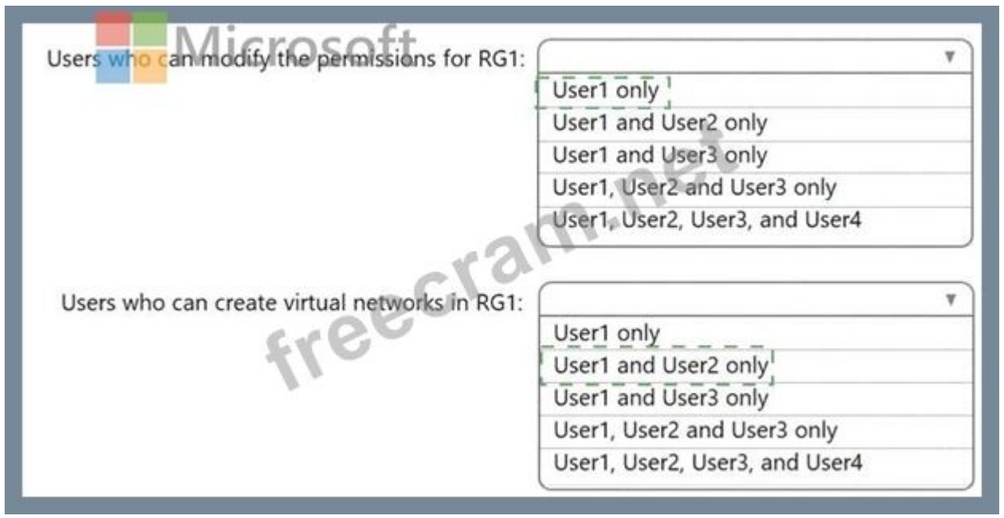
You create a resource group named RG1.

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

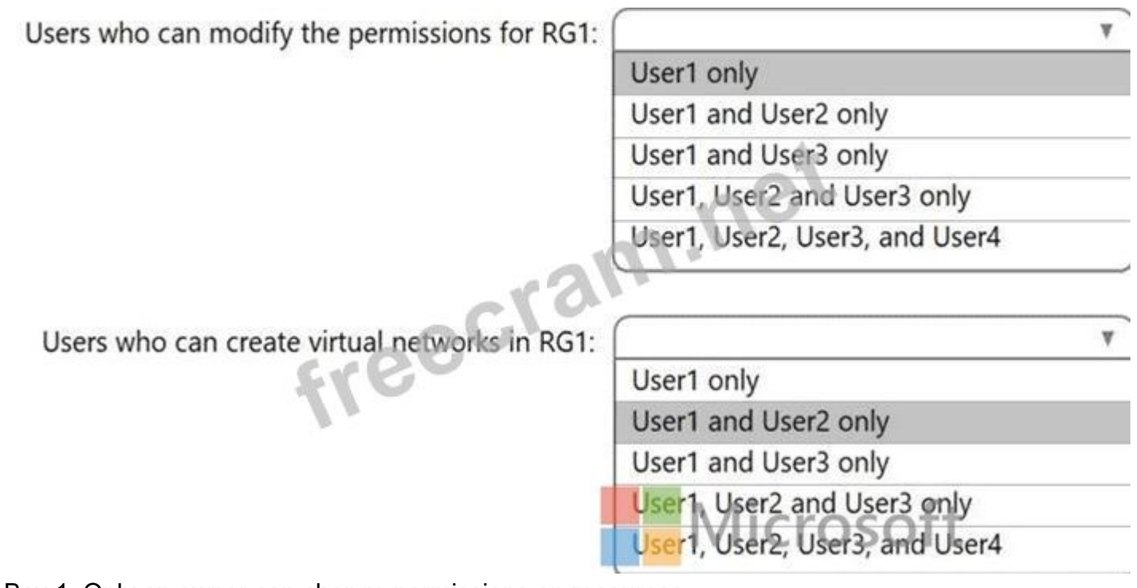
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



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

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

NEW QUESTION: 65

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!.	◉	○

Explanation:

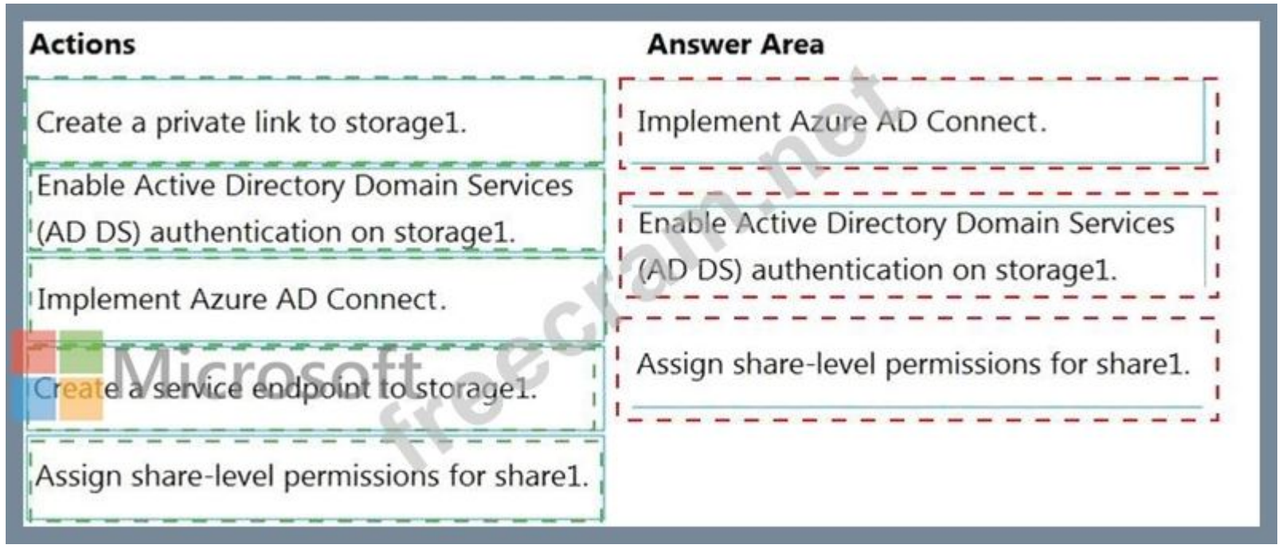
Text Description automatically generated

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: 66
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains a user named User1.
You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains an Azure Storage account named storage1. Storage1 contains an Azure file share named share1.
Currently, the domain and the tenant are not integrated.
You need to ensure that User1 can access share1 by using his domain credentials.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Answer:



Explanation:

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

NEW QUESTION: 67
You have an Azure SQL database.
You implement Always Encrypted.
You need to ensure that application developers can retrieve and decrypt data in the database.
Nantes's of information should you provide to the developers? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. a stored access policy
B. a shared access signature (SAS)
C. the column encryption key
D. user credentials
E. the column master key
Answer: (SHOW ANSWER)
Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.
References:

https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine

NEW QUESTION: 68
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 federated authentication.
B. Configure the Azure AD tenant used by the new subscription to use pass-through authenticate
C. Configure a second instance of Azure AD Connect.
D. Change the Azure AD tenant used by the new subscription.
Answer: (SHOW ANSWER)

NEW QUESTION: 69
You have an Azure subscription that contains an Azure Sentinel workspace.
Azure Sentinel is configured to ingest logs from several Azure workloads. A third-party service management platform is used to manage incidents.
You need to identify which Azure Sentinel components to configure to meet the following requirements:
* When Azure Sentinel identifies a threat, an incident must be created.
* A ticket must be logged in the service management platform when an incident is created in Azure Sentinel.
Which component should you identify for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

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

NEW QUESTION: 70
You have an Azure subscription that contains a resource group named RG1 and the network security groups (NSGs) shown in the following table.

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

You create the Azure policy shown in the following exhibit.

Basics Parameters Remediation Non-compliance messages **Review + create**

Basics

Scope	Azure Pass - Sponsorship/RG1
Exclusions	Azure Pass - Sponsorship/RG1/NSG1
Policy definition	Flow logs should be enabled for every network security group
Assignment name	Flow logs should be enabled for every network security group
Description	Description1
Policy enforcement	Enabled
Assigned by	Admin1

Parameters

effect	Audit

Remediation

Create managed identity	Yes
Managed identity location	westeurope
Create a remediation task	No

Non-compliance messages

Default non-compliance message	Message1

You assign the policy to RG1.

What will occur if you assign the policy to NSG1 and NSG2?

A. Flow logs will be enabled for NSG1 only.

B. Flow logs will be disabled for NSG1 and NSG2.

C. Flow logs will be enabled for NSG1 and NSG2.

D. Flow logs will be enabled for NSG2 only.

Answer: (SHOW ANSWER)

NEW QUESTION: 71

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

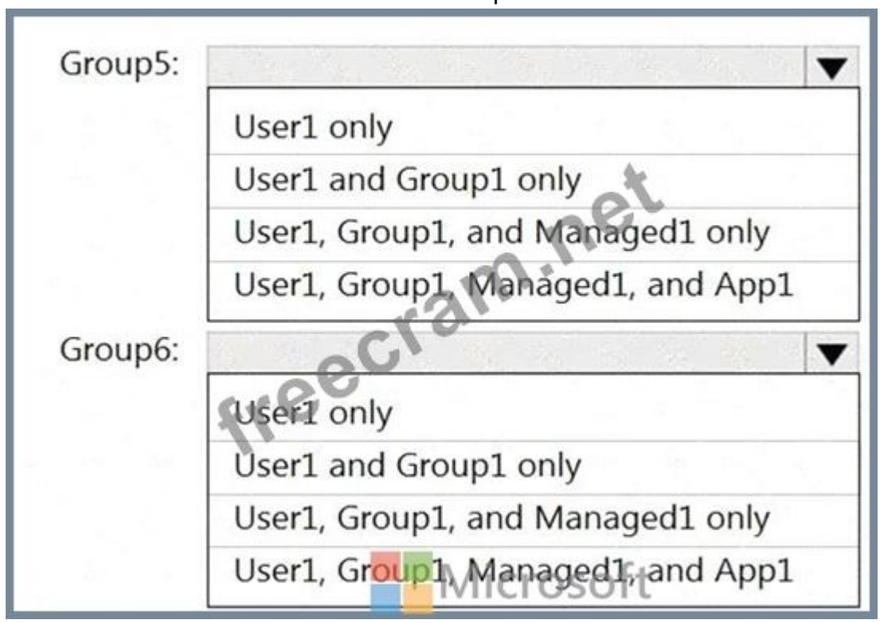
Name	Description
User1	User
Group1	Security group that has a Membership type of Dynamic Device
Managed1	Managed identity
App1	Enterprise application

You create the groups shown in the following table.

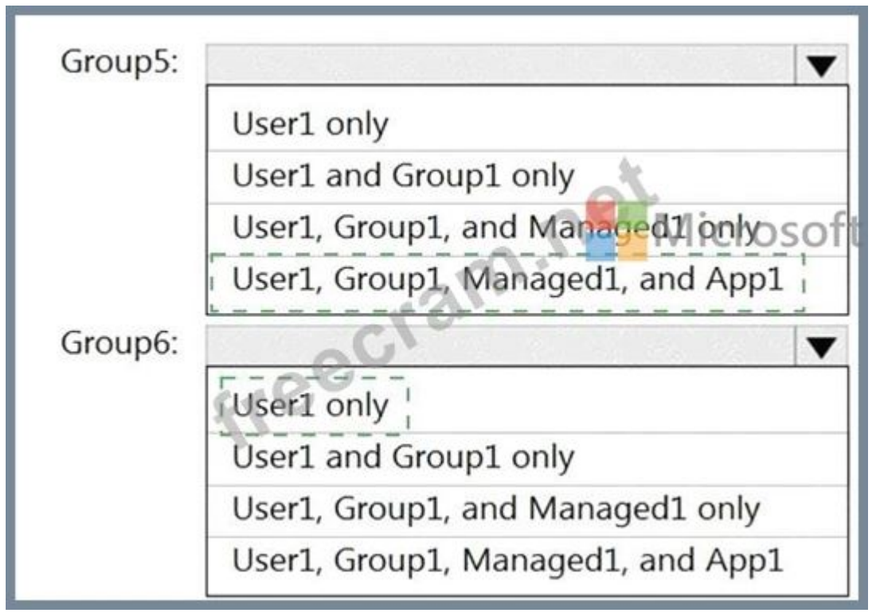
Name	Description
Group5	Security group that has a Membership type of Assigned
Group6	Microsoft 365 group that has a Membership type of Assigned

Which resources can you add to Group5 and Group6? 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

Group5:

- User1 only
- User1 and Group1 only
- User1, Group1, and Managed1 only
- User1, Group1, Managed1, and App1

Group6:

- User1 only
- User1 and Group1 only
- User1, Group1, and Managed1 only
- User1, Group1, Managed1, and App1

NEW QUESTION: 72

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

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

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

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

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

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

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

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


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

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

PS C:\> _
```

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

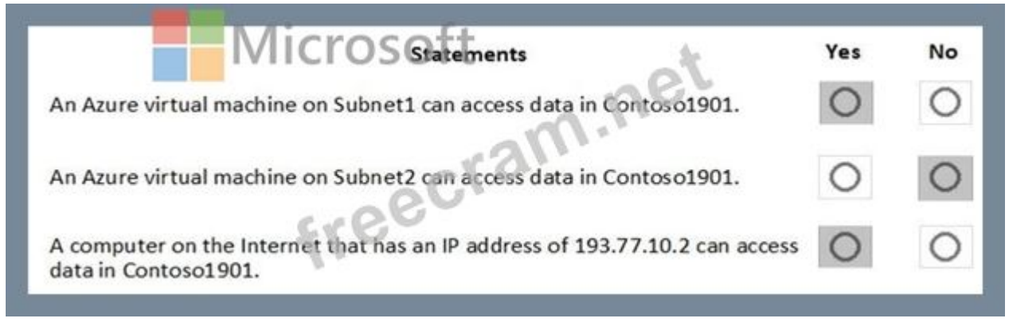
NOTE: Each correct selection is worth one point.

Statements	Yes	No
An Azure virtual machine on Subnet1 can access data in Contoso1901.	○	○
An Azure virtual machine on Subnet2 can access data in Contoso1901.	○	○
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	○	○

Answer:

Statements	Yes	No
An Azure virtual machine on Subnet1 can access data in Contoso1901.	○	○
An Azure virtual machine on Subnet2 can access data in Contoso1901.	○	○
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	○	○

Explanation:



Box 1: Yes

Access from Subnet1 is allowed.

Box 2: No

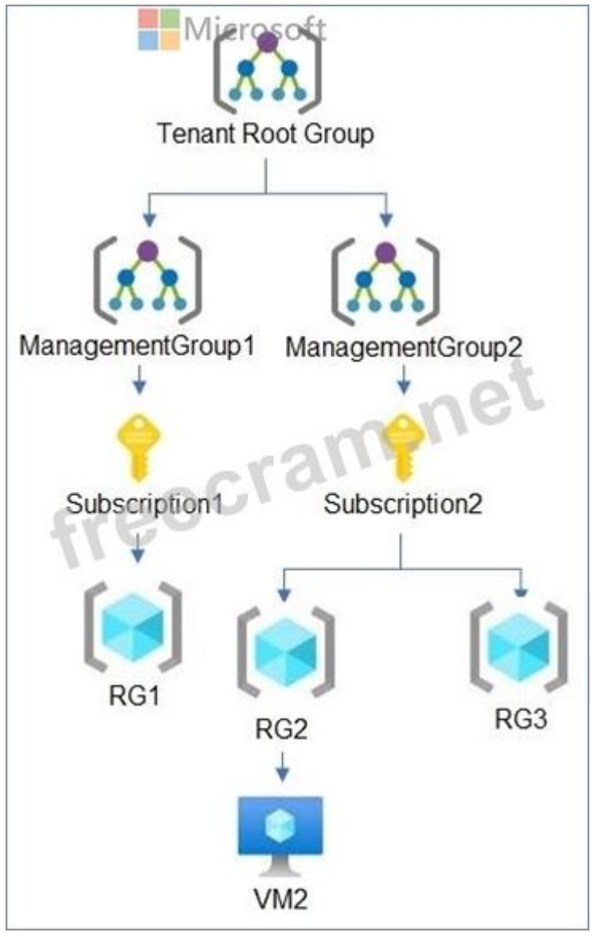
No access from Subnet2 is allowed.

Box 3: Yes

Access from IP address 193.77.10.2 is allowed.

NEW QUESTION: 73

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



RG1, RG2, and RG3 are resource groups.

RG2 contains a virtual machine named VM1.

You assign role-based access control (RBAC) roles to the users shown in the following table.

Name	Role	Added to resource
User1	Contributor	Tenant Root Group
User2	Virtual Machine Contributor	Subscription2
User3	Virtual Machine Administrator Login	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
User1 can deploy virtual machines to RG1.	O	O
User2 can delete VM2.	O	O
User3 can reset the password of the built-in Administrator account of VM2.	O	O

Answer:

Statements	Yes	No
User1 can deploy virtual machines to RG1.	O	O
User2 can delete VM2.	O	O
User3 can reset the password of the built-in Administrator account of VM2.	O	O

Explanation:

Statements	Yes	No
User1 can deploy virtual machines to RG1.	O	O
User2 can delete VM2.	O	O
User3 can reset the password of the built-in Administrator account of VM2.	O	O

NEW QUESTION: 74

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

NOTE: Each correct selection is worth one point.

Virtual networks that User2 can modify:

- VNET4 only
- VNET4 and VNET1 only
- VNET4, VNET3, and VNET1 only
- VNET4, VNET3, VNET2, and VNET1

Virtual networks that User2 can delete:

- VNET4 only
- VNET4 and VNET1 only
- VNET4, VNET3, and VNET1 only
- VNET4, VNET3, VNET2, and VNET1

Answer:

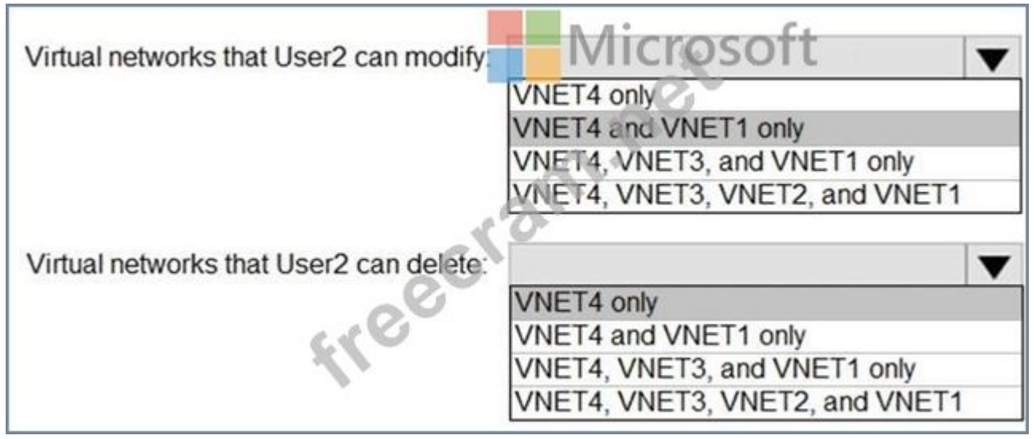
Virtual networks that User2 can modify:

- VNET4 only
- VNET4 and VNET1 only
- VNET4, VNET3, and VNET1 only
- VNET4, VNET3, VNET2, and VNET1

Virtual networks that User2 can delete:

- VNET4 only
- VNET4 and VNET1 only
- VNET4, VNET3, and VNET1 only
- VNET4, VNET3, VNET2, and VNET1

Explanation:



Box 1: VNET4 and VNET1 only

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

RG2 and RG3 both have Read-only locks.

Box 2: VNET4 only

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

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

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

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

Scenario:

User2 is a Security administrator.

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

User2 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

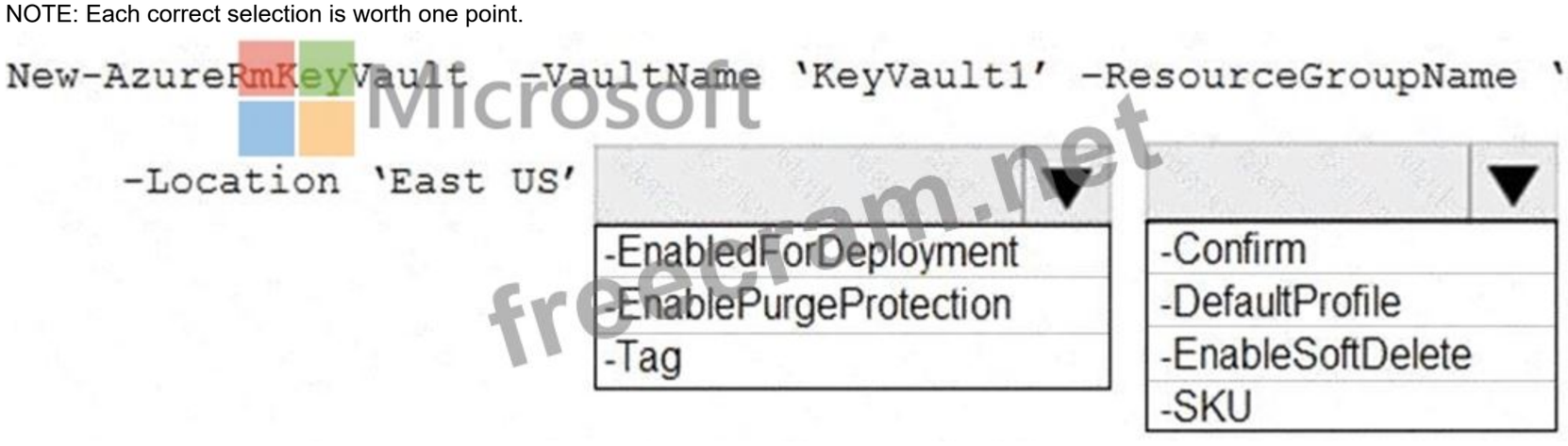
Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

References:

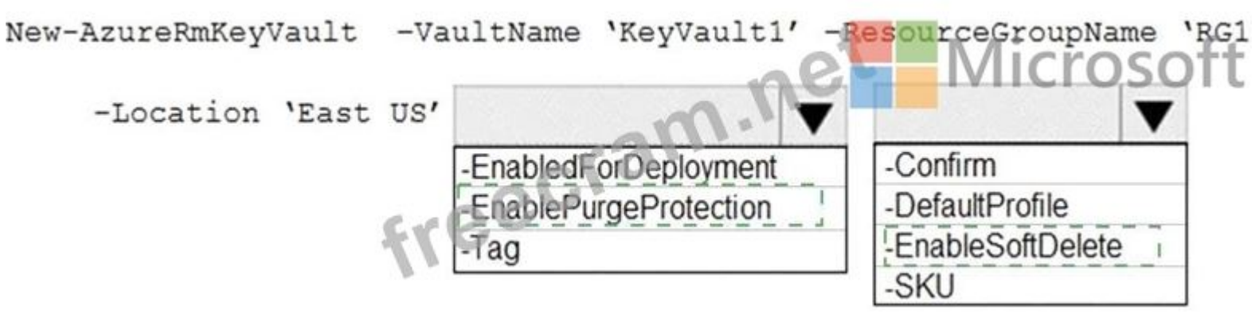
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

NEW QUESTION: 75
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

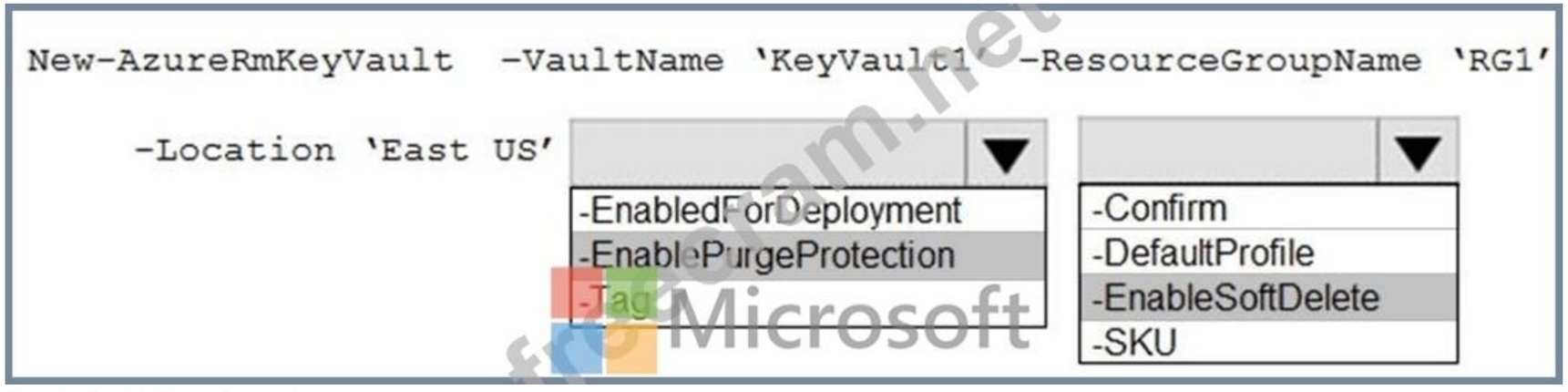
NEW QUESTION: 76
You need to create an Azure key vault. The solution must ensure that any object deleted from the key vault be retained for 90 days.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



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: 77

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

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

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

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

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

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

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 78

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

You purchase an App named App1.
User1 needs to publish App1 by using Azure AD Application Proxy.
Which role should you assign to User1?
A. Cloud Application Administrate
B. Application Administrator
C. Cloud App Security Administrator
D. Hybrid identity Administrator
Answer: (SHOW ANSWER)

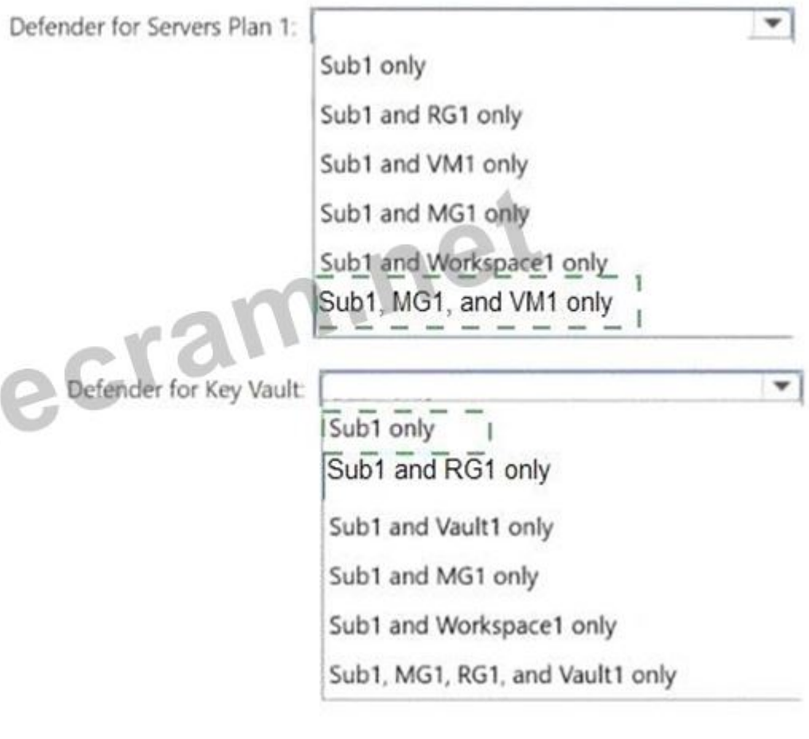
NEW QUESTION: 79
You have a management group named MG1 that contains an Azure subscription named Sub1. Sub1 contains the resources shown in the following table.

Name	Description
RG1	Resource group
VM1	Virtual machine
Vault1	Azure key vault
Workspace1	Log Analytics workspace

You need to protect the resource? in Sub1 by using Microsoft Defender for Servers Plan1 and Microsoft Defender for Key Vault.
From the Azure portal, on which resources can you enable Defender for Servers Plan 1, and on which resources can you enable Defender for Key Vault? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Answer Area



Explanation:

NEW QUESTION: 80

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.

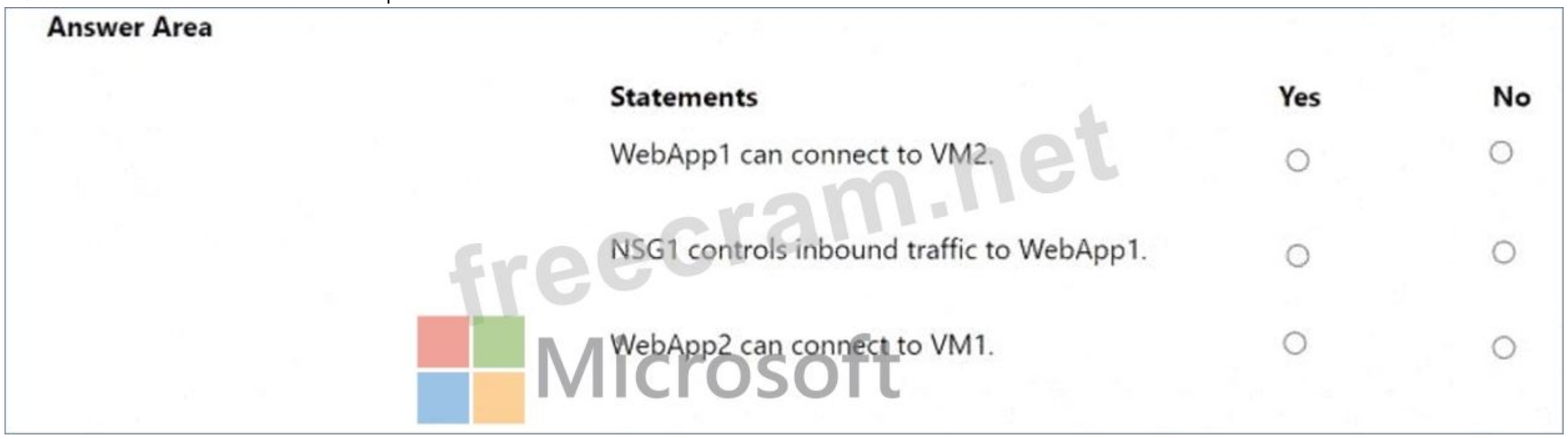
The subscription contains the virtual machines shown in the following table.

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:

Explanation:

NEW QUESTION: 81
You have an Azure subscription that contains two virtual machines named VM1 and VM2 that run Windows Server 2019.
You are implementing Update Management in Azure Automation.
You plan to create a new update deployment named Update1.
You need to ensure that Update! meets the following requirements:
* Automatically applies updates to VM1 and VM2.
* Automatically adds any new Windows Server 2019 virtual machines to Update1.
What should you include in Update1?
A. a dynamic group query
B. a security group that has a Membership type of Assigned
C. a Kusto query language query
D. a security group that has a Membership type of Dynamic Device
Answer: (SHOW ANSWER)

NEW QUESTION: 82
You have a web app named WebApp1.
You create a web application firewall (WAF) policy named WAF1.
You need to protect WebApp1 by using WAF1.
What should you do first?
A. Deploy an Azure Front Door.
B. Add an extension to WebApp1.
C. Deploy Azure Firewall.
Answer: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door

NEW QUESTION: 83

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: 84
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:

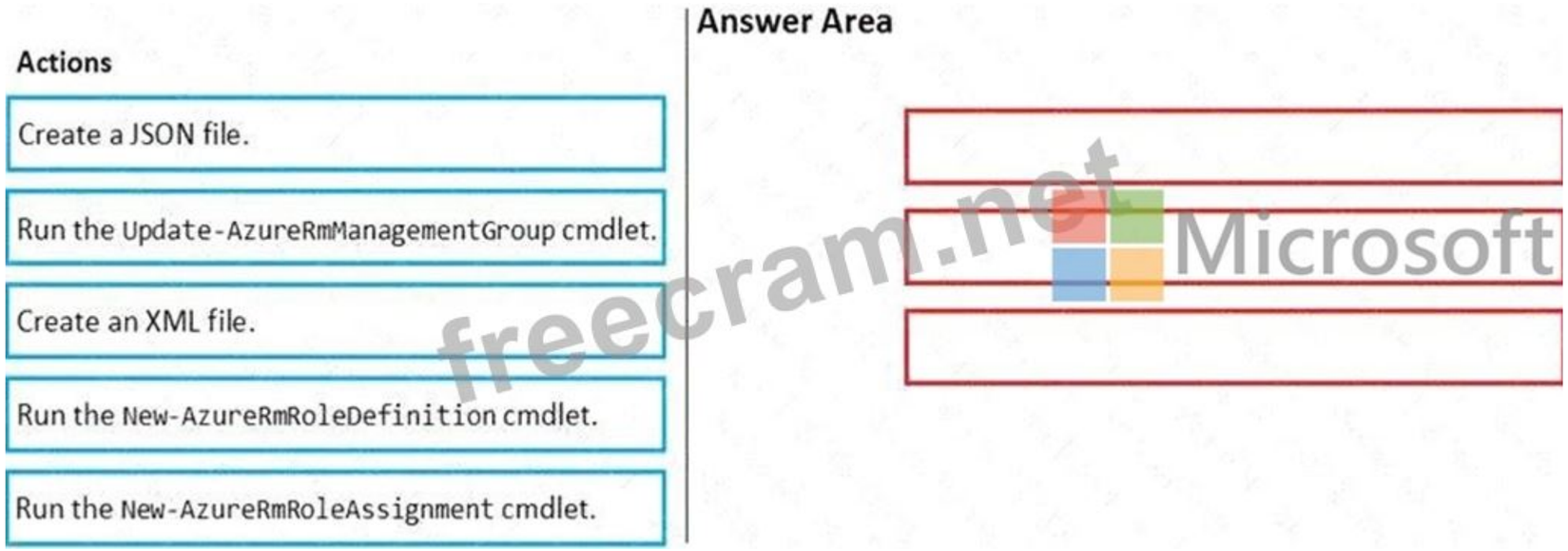
NEW QUESTION: 85

You have an Azure subscription named Sub1.

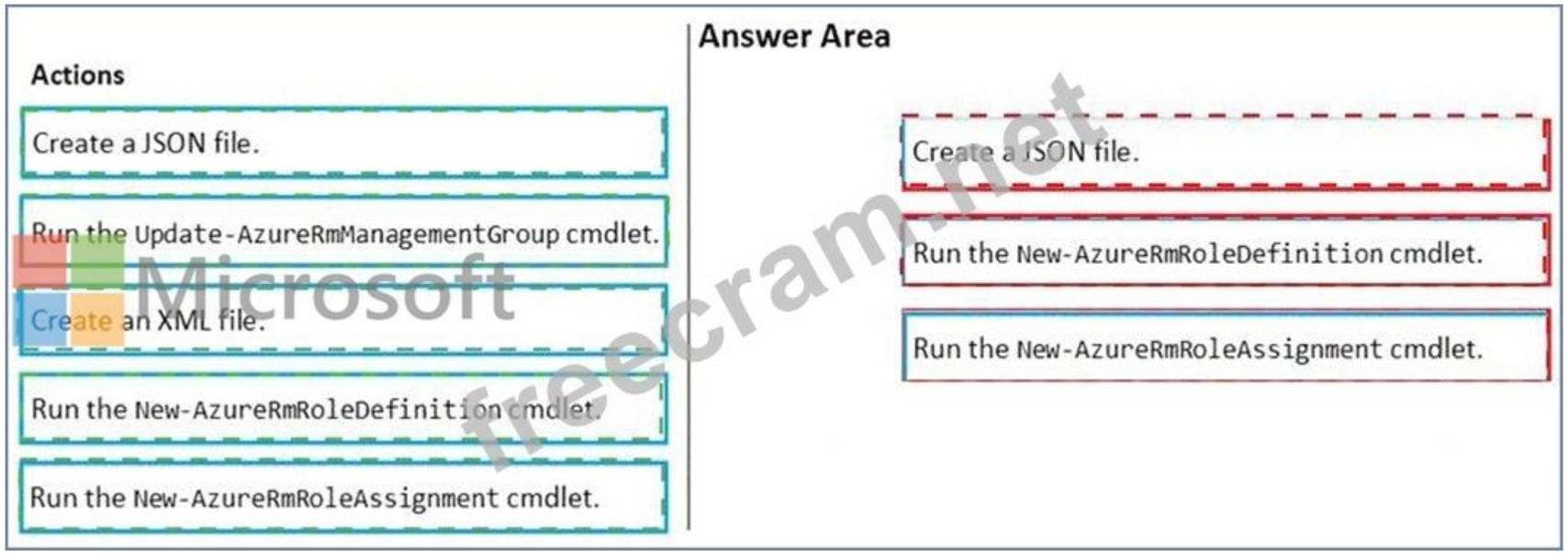
You have an Azure Active Directory (Azure AD) group named Group1 that contains all the members of your IT team.

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

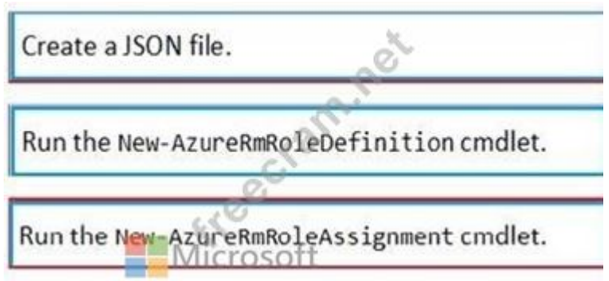
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:



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

NEW QUESTION: 86
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 Area

Add permissions

Microsoft Monitoring Insights Microsoft.SecurityGraph	**Microsoft Monitoring Insights** Enable your workforce to be productive on all their devices, while keeping your organization's information protected.	**Microsoft Monitoring Insights** Microsoft.DynamicsTelemetry	**Microsoft Network** Connect cloud and on-premises infrastructure and services to provide your customers and users the best.
Microsoft Operations Management A simplified management solution for any enterprise	**Microsoft Policy Insights** Summarize policy states for the subscription level policy definition.	**Microsoft Portal** Build, manage, and monitor all Azure products in a single, unified console.	**Microsoft Power BI Dedicated** Manage Power BI Premium dedicated capacities for exclusive use by an organization.
Microsoft Power Platform Microsoft.PowerPlatform	**Microsoft Project Babylon** Microsoft.ProjectBabylon	**Microsoft Purview** Microsoft.Purview	**Microsoft Resource Graph** Powerful tool to query, explore, and analyze your cloud resources at scale.

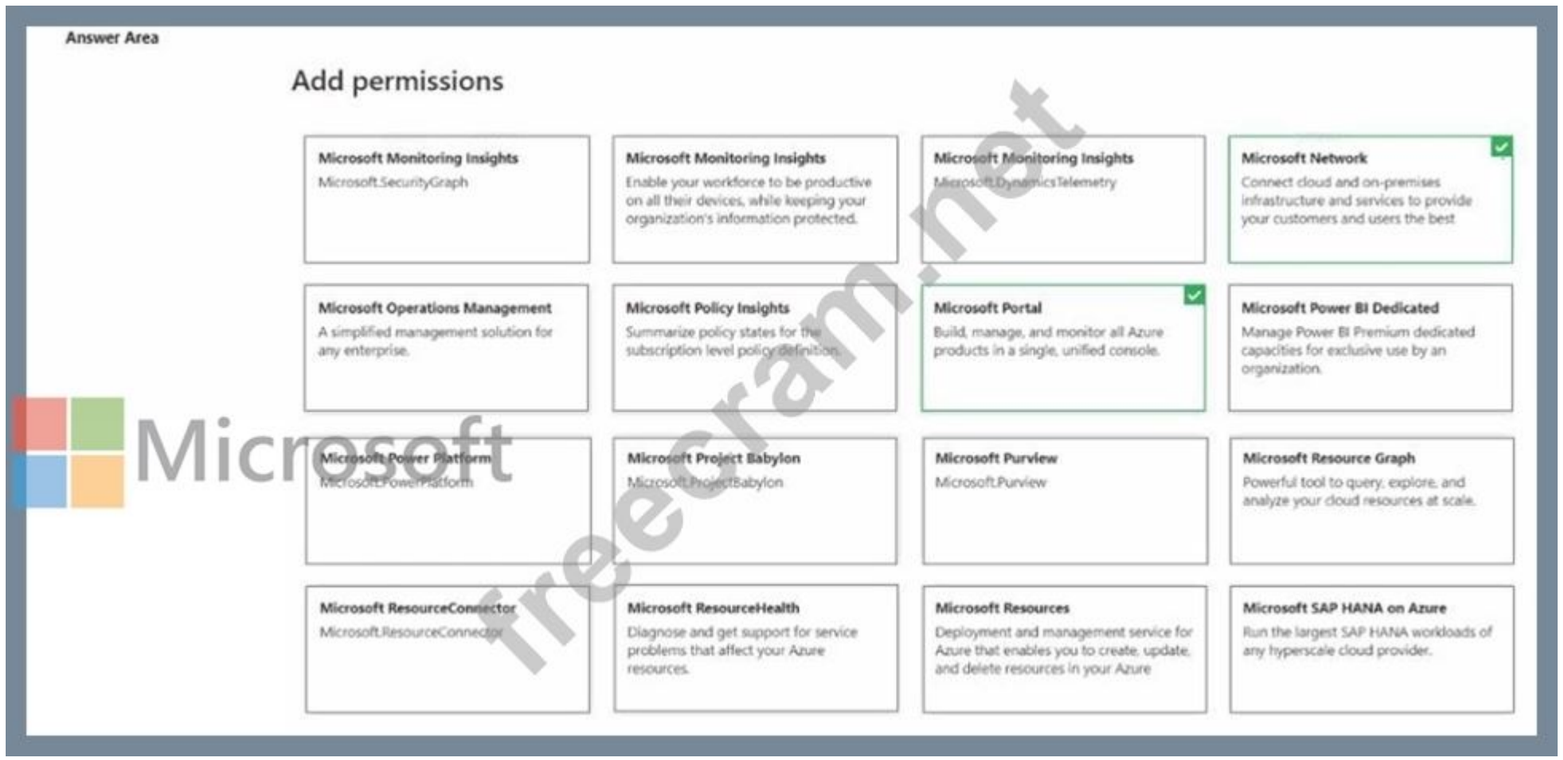
Answer:

Answer Area

Add permissions

Microsoft Monitoring Insights Microsoft.SecurityGraph	**Microsoft Monitoring Insights** Enable your workforce to be productive on all their devices, while keeping your organization's information protected.	**Microsoft Monitoring Insights** Microsoft.DynamicsTelemetry	**Microsoft Network** Connect cloud and on-premises infrastructure and services to provide your customers and users the best.
Microsoft Operations Management A simplified management solution for any enterprise	**Microsoft Policy Insights** Summarize policy states for the subscription level policy definition.	**Microsoft Portal** Build, manage, and monitor all Azure products in a single, unified console.	**Microsoft Power BI Dedicated** Manage Power BI Premium dedicated capacities for exclusive use by an organization.
Microsoft Power Platform Microsoft.PowerPlatform	**Microsoft Project Babylon** Microsoft.ProjectBabylon	**Microsoft Purview** Microsoft.Purview	**Microsoft Resource Graph** Powerful tool to query, explore, and analyze your cloud resources at scale.

Explanation:



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

NEW QUESTION: 87
You have an Azure subscription that contains an Azure Blob storage account bolb1.
You need to configure attribute-based access control (ABAC) for blob1.
Which attributes can you use in access conditions?
A. blob index tags and container names only
B. blob index tags only
C. blob index tags, file extensions, and container names
D. file extensions and container names only
Answer: (SHOW ANSWER)

NEW QUESTION: 88
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

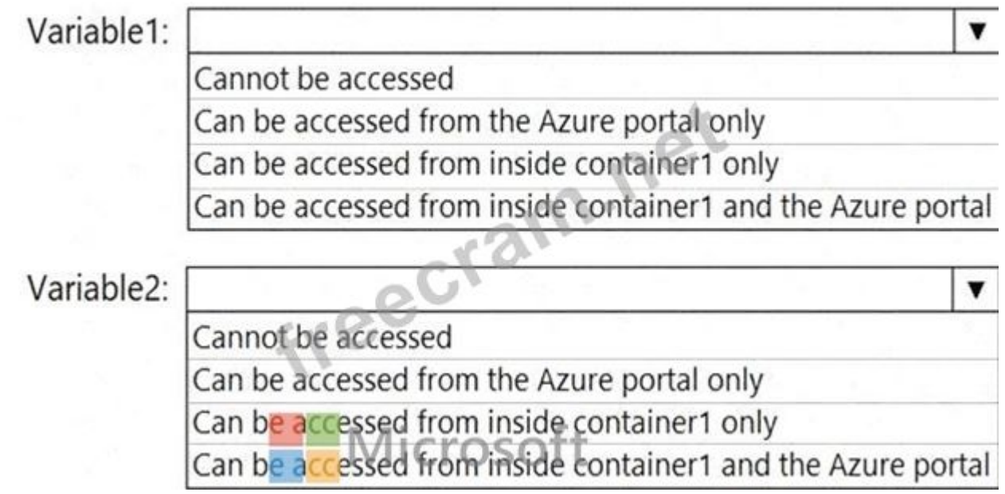
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy
https://docs.microsoft.com/en-us/azure/security-center/policy-reference

NEW QUESTION: 89
You have an Azure subscription that contains an Azure SQL database named SQL1. You need to configure SQL1 to use Always Encrypted. What should you use?
A. pgAdmin
B. the Azure portal
C. MySQL Workbench
D. Microsoft SQL Server Management Studio (SSMS)
Answer: (SHOW ANSWER)

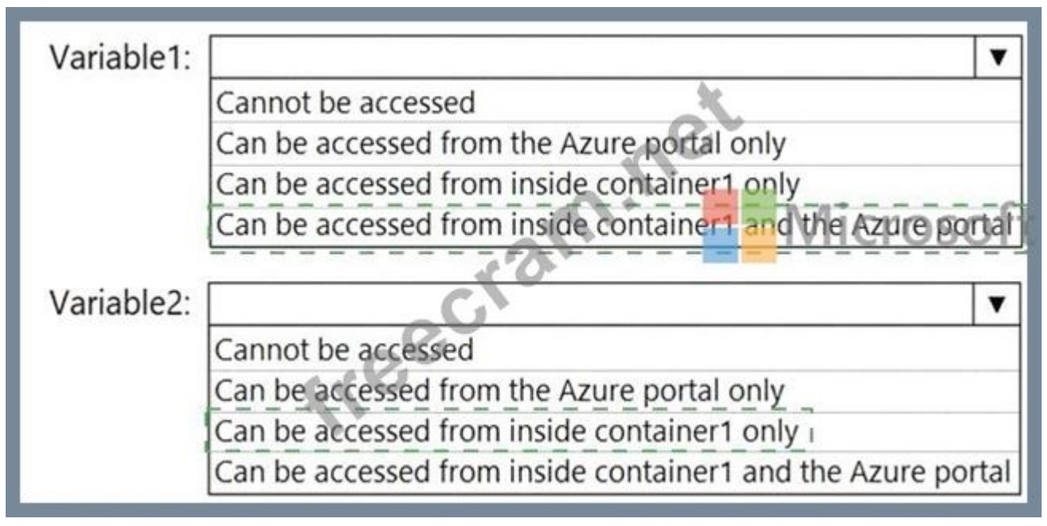
NEW QUESTION: 90
You have a file named File1.yaml that contains the following contents.

```
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
```

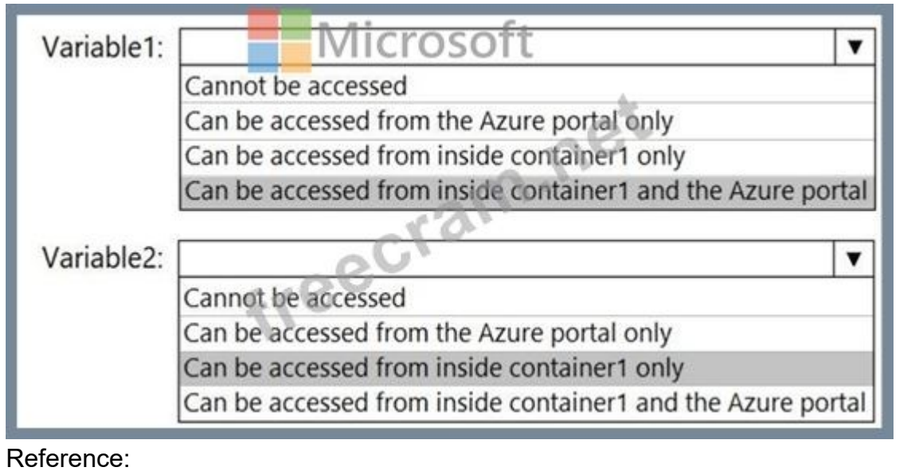

You create an Azure container instance named container1 by using File1.yaml.
You need to identify where you can access the values of Variable1 and Variable2.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



Reference:

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

NEW QUESTION: 91
You need to configure WebApp1 to meet the data and application requirements.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. Upload a public certificate.
B. Turn on the HTTPS Only protocol setting.
C. Set the Minimum TLS Version protocol setting to 1.2.
D. Change the pricing tier of the App Service plan.
E. Turn on the Incoming client certificates protocol setting.
Answer: (SHOW ANSWER)
Refer https://docs.microsoft.com/en-us/azure/app-service/app-service-web-configure-tls-mutual-auth

NEW QUESTION: 92
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 Area

Statements	Yes	No
You can use URL filtering on the network rules for VNet1.	○	○
You can use an intrusion detection and prevention system (IDPS) to monitor malicious activity on VNet2.	○	○
If you configure peering between VNet1 and VNet3, encrypted outbound traffic from VNet3 will be inspected.	○	○

Answer:

Answer Area

Statements	Yes	No
You can use URL filtering on the network rules for VNet1.	○	○
You can use an intrusion detection and prevention system (IDPS) to monitor malicious activity on VNet2.	○	○
If you configure peering between VNet1 and VNet3, encrypted outbound traffic from VNet3 will be inspected.	○	○

Explanation:

Answer Area

Statements	Yes	No
You can use URL filtering on the network rules for VNet1.	○	●
You can use an intrusion detection and prevention system (IDPS) to monitor malicious activity on VNet2.	●	○
If you configure peering between VNet1 and VNet3, encrypted outbound traffic from VNet3 will be inspected.	○	●

NEW QUESTION: 93

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

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

You create and enforce a Microsoft Entra Identity Protection sign-in risk policy that has the following settings:

* Assignments: Include Group1, exclude Group2
* Conditions: Sign-in risk level: Low and above
* Access: Allow access, Require multi-factor authentication

You need to identify what occurs when the users sign in to Microsoft Entra ID.

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:

NEW QUESTION: 94

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]**.

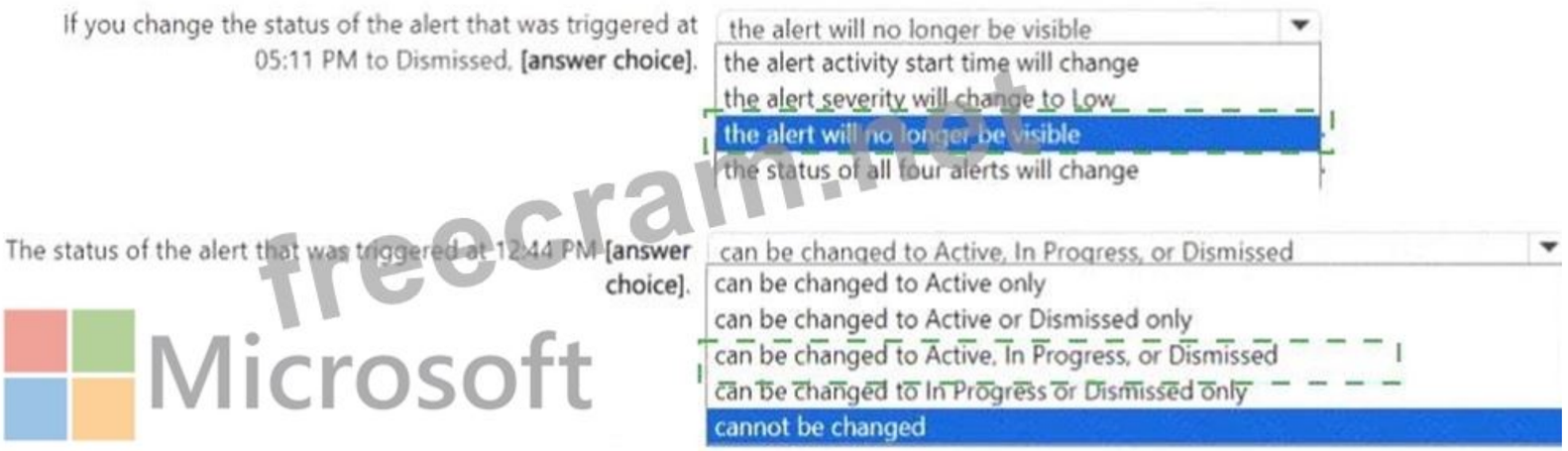
- the alert will no longer be visible
- the alert activity start time will change
- the alert severity will change to Low
- the alert will no longer be visible
- the status of all four alerts will change

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

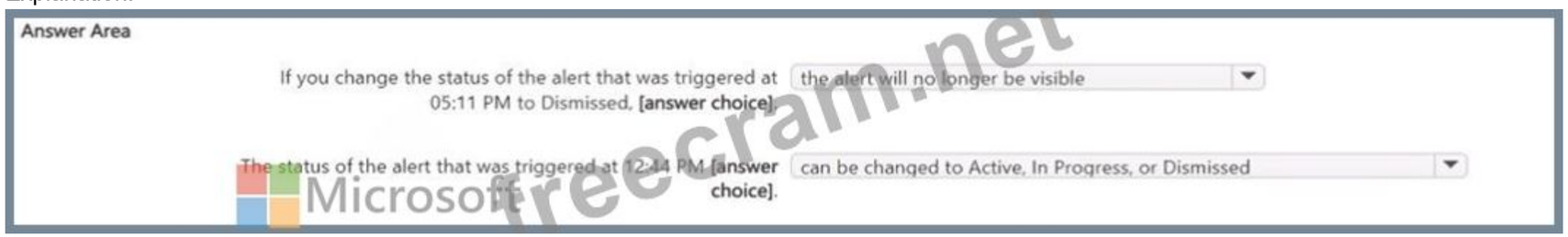
- can be changed to Active, In Progress, or Dismissed
- can be changed to Active only
- can be changed to Active or Dismissed only
- can be changed to Active, In Progress, or Dismissed
- can be changed to In Progress or Dismissed only
- cannot be changed

Answer:

Answer Area



Explanation:

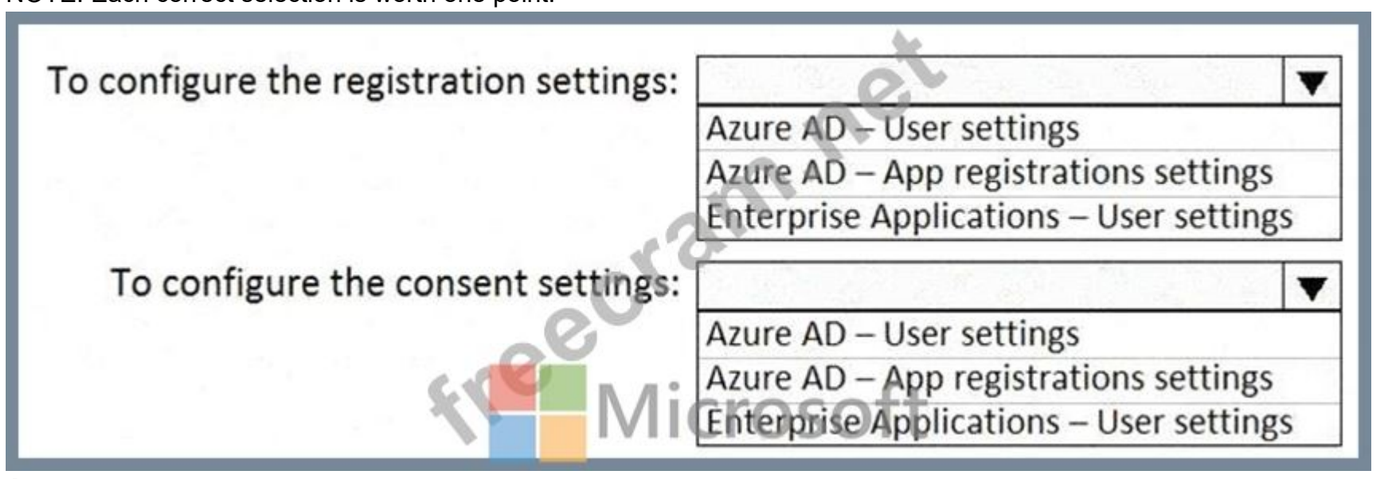


NEW QUESTION: 95

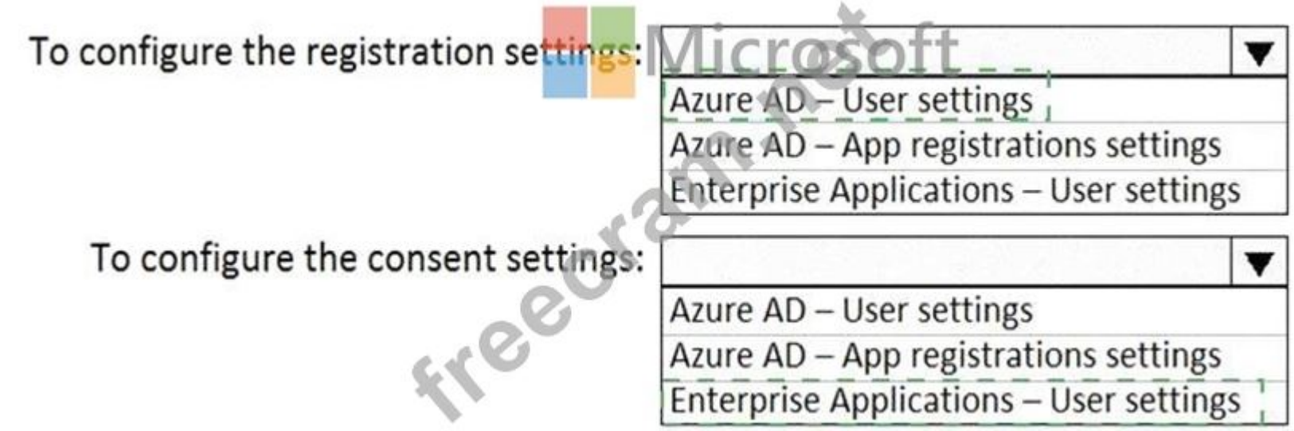
You need to ensure that the Azure AD application registration and consent configurations meet the identity and access requirements.

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

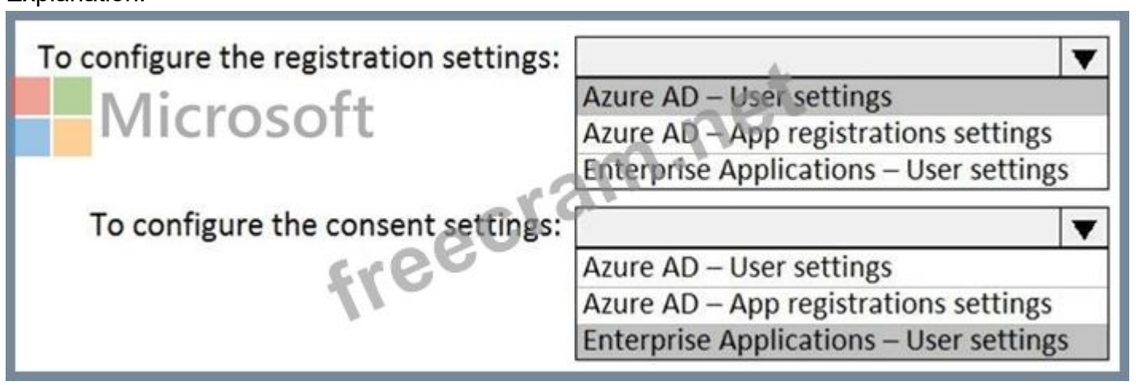
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



Reference:

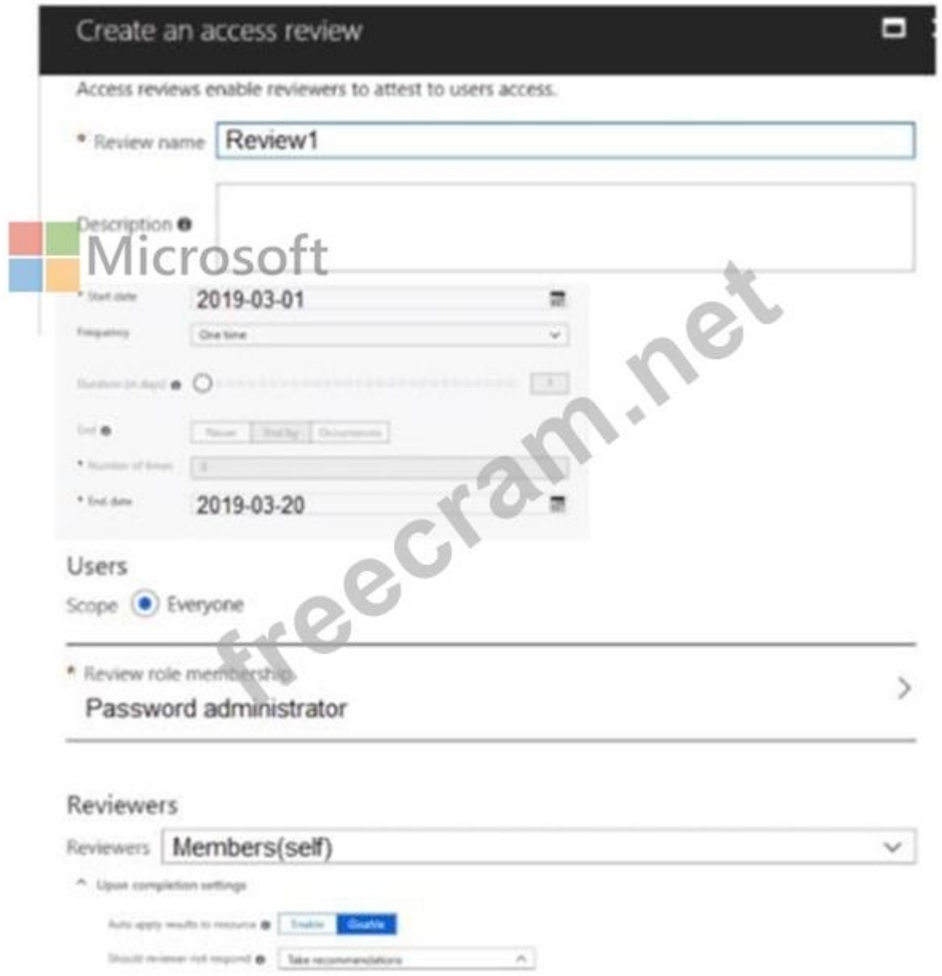
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent

NEW QUESTION: 96

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.

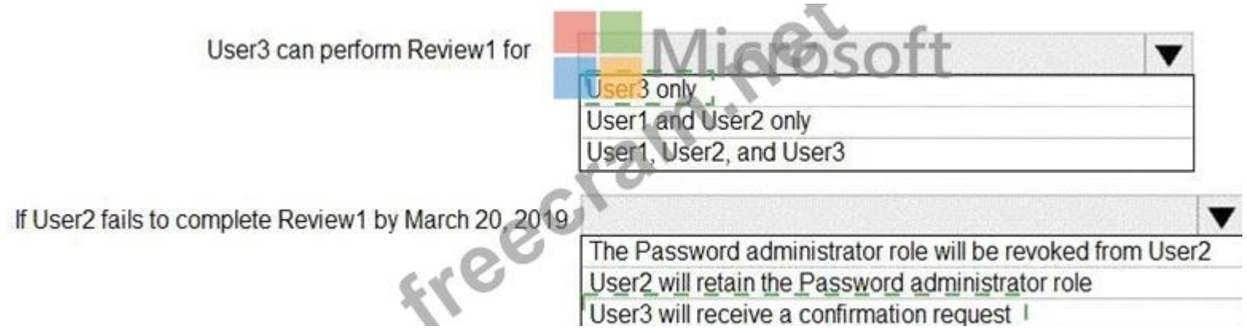
User3 can perform Review1 for

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

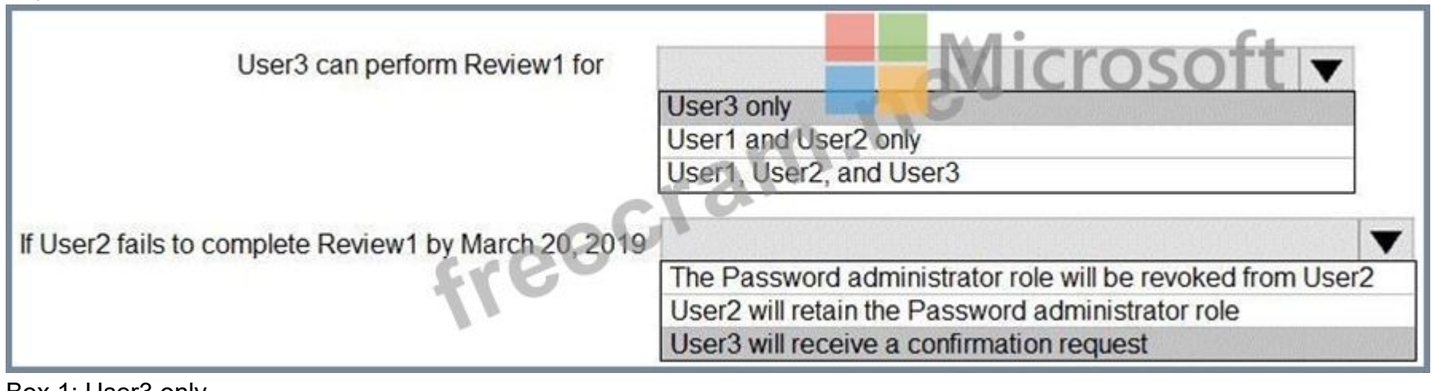
If User2 fails to complete Review1 by March 20, 2019

- The Password administrator role will be revoked from User2
- User2 will retain the Password administrator role
- User3 will receive a confirmation request

Answer:



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: 97

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

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

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

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

NOTE: Each correct selection is worth one point.

Azure Active Directory Identity Protection:

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

Azure Firewall:

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

CEF:

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

Answer:

Azure Active Directory Identity Protection:

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

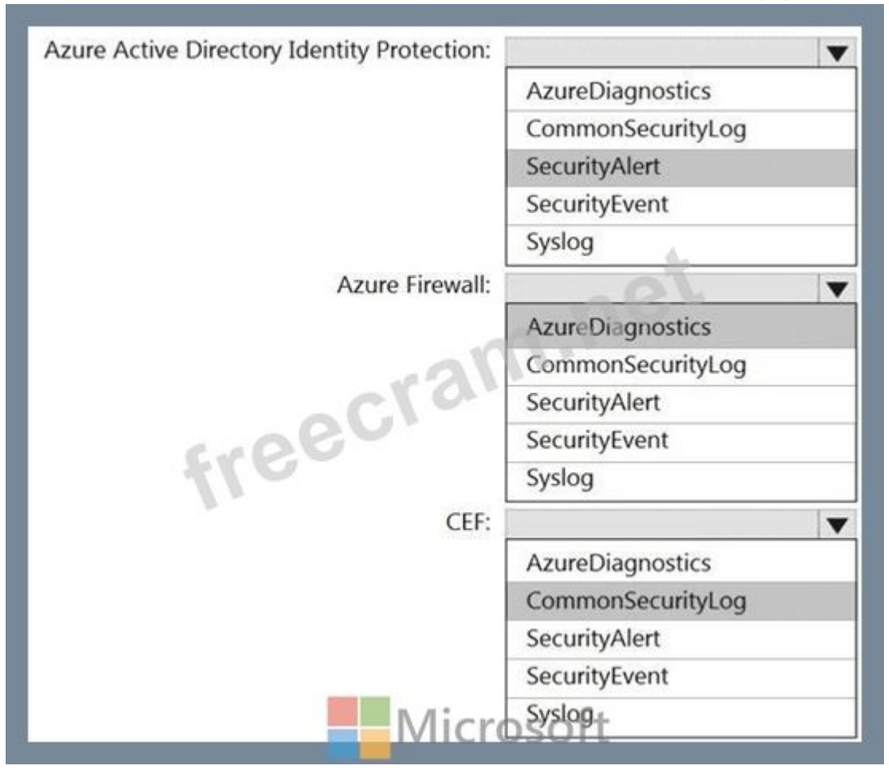
Azure Firewall:

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

CEF:

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

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

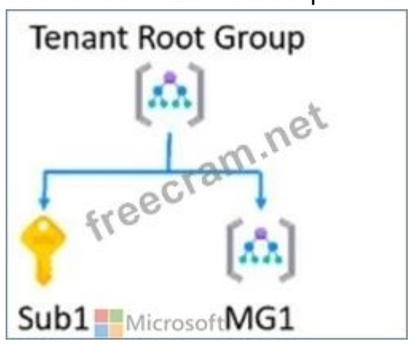


NEW QUESTION: 98
Lab Task
use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password. place your cursor in the Enter password box and click on the password below.
Azure Username: Userl -28681041@ExamUsers.com
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 4
You need to ensure that a user named user2-28681041 can manage the properties of the virtual machines in the RG1lod28681041 resource group. The solution must use the principle of least privilege.
Answer:
Check below steps in explanation for Task
Explanation:
To ensure that a user named user2-28681041 can manage the properties of the virtual machines in the RG1lod28681041 resource group using the principle of least privilege, you can follow these steps:
In the Azure portal, search for and select the resource group named RG1lod28681041.
In the left pane, select Access control (IAM).

Select Add.
In the Add role assignment pane, enter the following information:
Role: Select the appropriate role for your scenario. For example, Virtual Machine Contributor.
Assign access to: Select User, group, or service principal.
Select: Enter the name of the user you want to assign the role to. For example, user2-28681041.
Select Save.
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal

NEW QUESTION: 99
You are troubleshooting a security issue for an Azure Storage account.
You enable the diagnostic logs for the storage account. What should you use to retrieve the diagnostics logs?
A. the Security & Compliance admin center
B. SQL query editor in Azure
C. File Explorer in Windows
D. AzCopy
Answer: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-logging?toc=%2fazure%2fstorage%2fblobs%2ftoc.json

NEW QUESTION: 100
You have an Azure subscription named Sub1 that uses Microsoft Defender for Cloud. You have the management group hierarchy shown in the following exhibit.



You create the definitions shown in the following table.

Name	Location	Type
Policy1	Sub1	Policy
Initiative1	Tenant Root Group	Initiative
Initiative2	Sub1	Initiative
Initiative3	MG1	Initiative

You need to use Defender for Cloud to add a security policy. Which definitions can you use as a security policy?
A. Initiative1 and Initiative2 only
B. Initiative1, Initiative2, and Initiatives only
C. Policy1 and Initiative1 only

D. Policy1, Initiative1, Initiative2, and Initiative3
E. Policy1 only
Answer: (SHOW ANSWER)

NEW QUESTION: 101
You have an Azure subscription that contains the resources shown in the following table.

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

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

Answer Area

Answer:
Answer Area

Explanation:

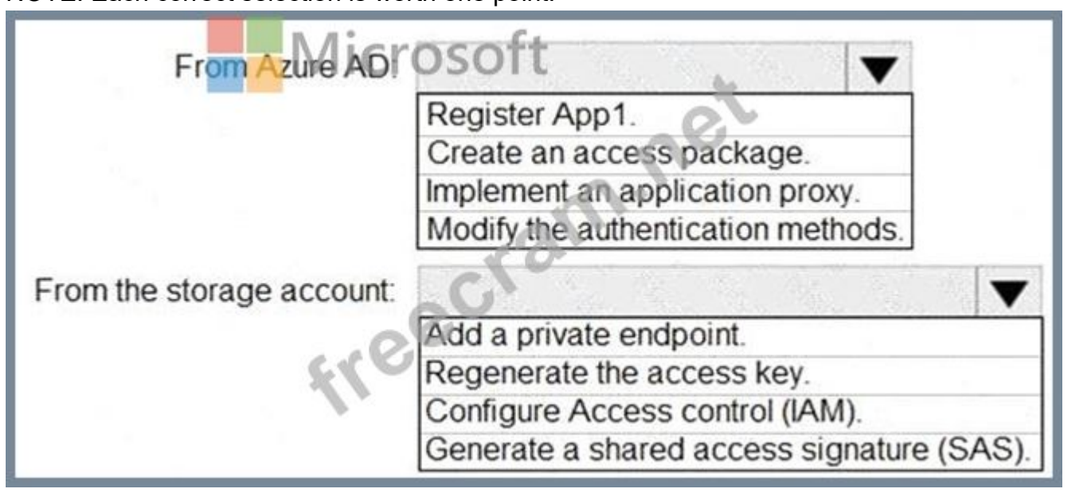
NEW QUESTION: 102

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

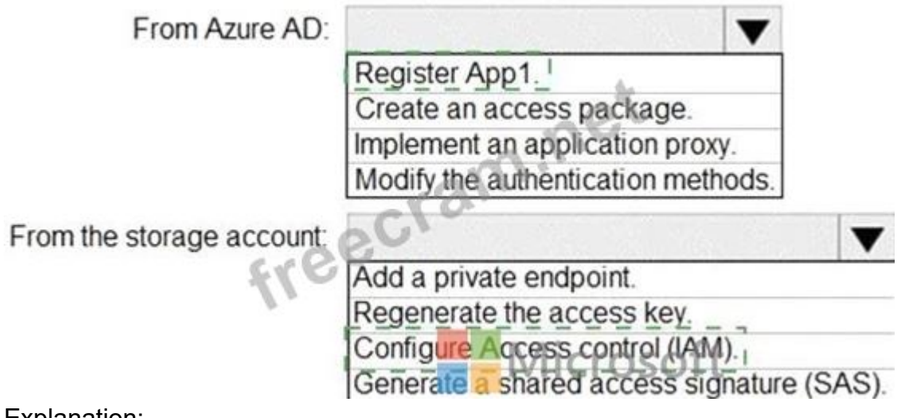
You need to enable App1 access to container1 by using Azure Active Directory (Azure AD) authentication.

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

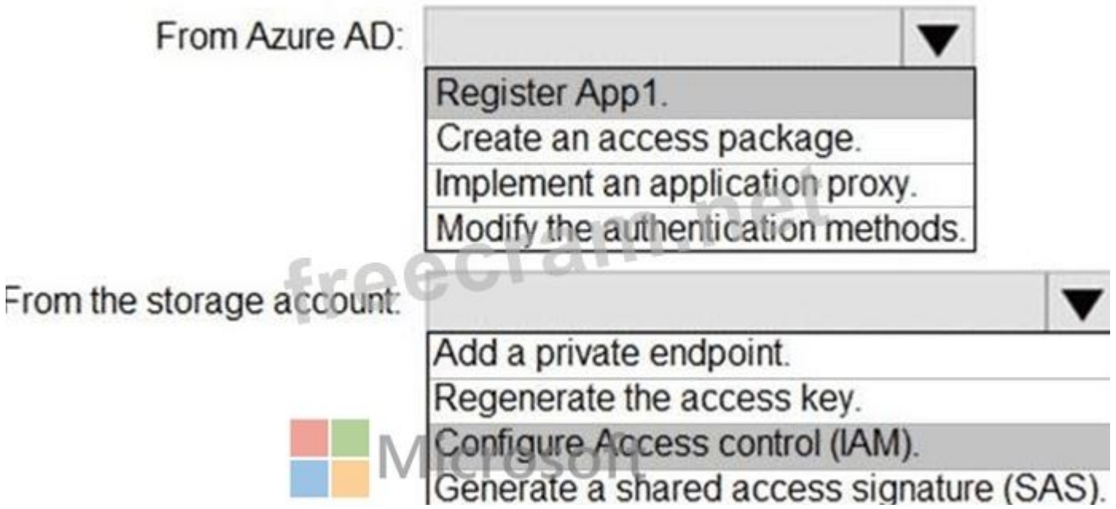
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



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

NEW QUESTION: 103
You have an Azure Container Registry named ContReg1 that contains a container image named image1.
You enable content trust for ContReg1.
After content trust is enabled, you push two images to ContReg1 as shown in the following table.

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

Which images are trusted images?
A. image1 and image2 only
B. image2 only
C. image1, image2, and image3
Answer: (SHOW ANSWER)
Azure Container Registry implements Docker's content trust model, enabling pushing and pulling of signed images.
To push a trusted image tag to your container registry, enable content trust and push the image with docker push.
To work with trusted images, both image publishers and consumers need to enable content trust for their Docker clients. As a publisher, you can sign the images you push to a content trust-enabled registry.
Reference:
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust

NEW QUESTION: 104
You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant.
From the Azure portal, you register an enterprise application.
Which additional resource will be created in Azure AD?
A. a service principal

B. an X.509 certificate
C. a managed identity
D. a user account
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

NEW QUESTION: 105
You have an Azure subscription that is linked to an Azure AD tenant and contains the resources shown in the following table.

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

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

NEW QUESTION: 106
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. VM1 and VM2 only
B. VM2 and VM3 only
C. VM2 and VM4 only
D. VM1, VM2, VM3, and VM4
Answer: (SHOW ANSWER)

NEW QUESTION: 107
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: 108
You have 10 virtual machines on a single subnet that has a single network security group (NSG).
You need to log the network traffic to an Azure Storage account.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. Install the Network Performance Monitor solution.
B. Enable Azure Network Watcher.
C. Enable diagnostic logging for the NSG.
D. Enable NSG flow logs.
E. Create an Azure Log Analytics workspace.
Answer: D (LEAVE A REPLY)
A network security group (NSG) enables you to filter inbound traffic to, and outbound traffic from, a virtual machine (VM). You can log network traffic that flows through an NSG with Network Watcher's NSG flow log capability. Steps include:
* Create a VM with a network security group
* Enable Network Watcher and register the Microsoft.Insights provider
* Enable a traffic flow log for an NSG, using Network Watcher's NSG flow log capability
* Download logged data
* View logged data
Reference:

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal

NEW QUESTION: 109
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:

Explanation:

NEW QUESTION: 110

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: 111
You have an Azure subscription named Sub1 that contains the Azure key vaults shown in the following table.

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

In Sub1, you create a virtual machine that has the following configurations:
* Name:VM1
* Size: DS2v2
* Resource group: RG1
* Region: West Europe
* Operating system: Windows Server 2016
You plan to enable Azure Disk Encryption on VM1.
In which key vaults can you store the encryption key for VM1?
A. Vault1 or Vault3 only
B. Vault1, Vault2, Vault3, or Vault4
C. Vault1 only

D. Vault1 or Vault2 only

Answer: (SHOW ANSWER)

"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: 112

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

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

In KeyVault1 the following events occur in sequence:

* item is deleted.

* Item2 and Policy1 are deleted.

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

NOTE: Each correct selection is worth one point.

ui

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

NEW QUESTION: 113
You have an Azure subscription that contains the virtual machines shown in the following table.

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

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

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

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

NEW QUESTION: 114
You have an Azure subscription that contains virtual machines. The subscription uses Microsoft Defender for Cloud with the Foundational Cloud Security Posture Management (CSPM) plan.
You need to enable agentless scanning for the virtual machines.
What should you do in Defender for Cloud?
A. Enable the Defender CSPM plan.
B. Enable Microsoft Defender for Servers Plan1.
C. Create a custom standard security policy
D. Add a security solution.
Answer: (SHOW ANSWER)

NEW QUESTION: 115
You have been tasked with applying conditional access policies for your company's current Azure Active Directory (Azure AD).
The process involves assessing the risk events and risk levels.
Which of the following is the risk level that should be configured for users that have leaked credentials?
A. None
B. Low
C. Medium
D. High
Answer: (SHOW ANSWER)
These six types of events are categorized in to 3 levels of risks - High, Medium & Low:
Table Description automatically generated

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

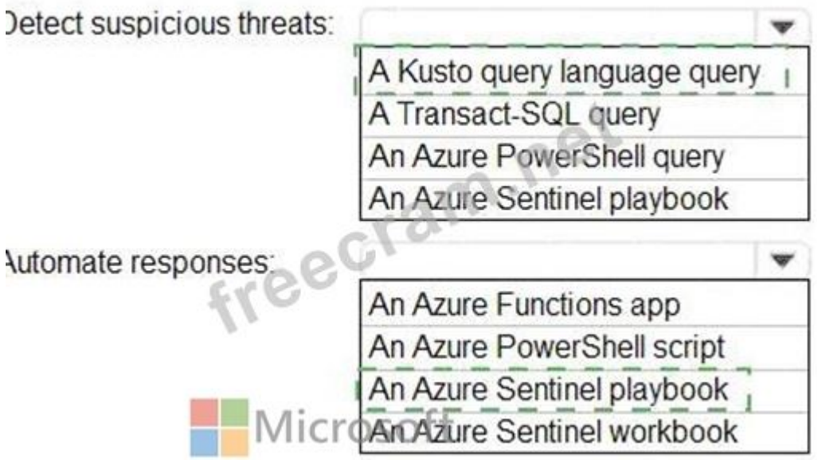
Reference:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/

NEW QUESTION: 116
You have 15 Azure virtual machines in a resource group named RG1.
All virtual machines run identical applications.
You need to prevent unauthorized applications and malware from running on the virtual machines.
What should you do?
A. Configure Azure Active Directory (Azure AD) Identity Protection.
B. From Microsoft Defender for Cloud, configure adaptive application controls.
C. Apply an Azure policy to RGI.
D. Apply a resource lock to RGI.
Answer: (SHOW ANSWER)

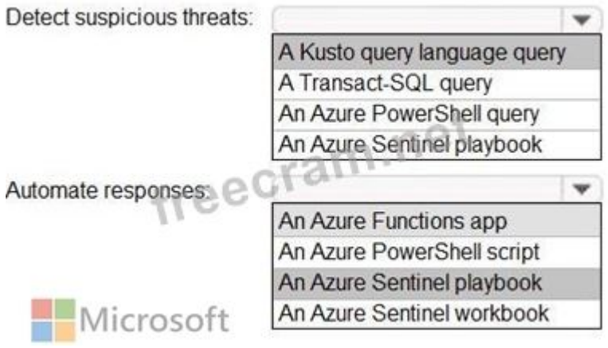
Microsoft Defender for Cloud helps you prevent, detect, and respond to threats. Defender for Cloud gives you increased visibility into, and control over, the security of your Azure resources. It provides integrated security monitoring and policy management across your Azure subscriptions. It helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions.
Defender for Cloud helps you optimize and monitor the security of your virtual machines by:
* Providing security recommendations for the virtual machines. Example recommendations include:
apply system updates, configure ACLs endpoints, enable antimalware, enable network security groups, and apply disk encryption.
* Monitoring the state of your virtual machines.
https://learn.microsoft.com/en-us/azure/security/fundamentals/virtual-machines-overview

NEW QUESTION: 117
You plan to use Azure Sentinel to create an analytic rule that will detect suspicious threats and automate responses.
Which components are required for the rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:



Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

NEW QUESTION: 118
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. Azure Disk Encryption
B. Transparent Data Encryption (TDE) with customer-managed keys
C. Transparent Data Encryption (TDE) with Microsoft-managed keys
D. Always Encrypted
E. TLS
Answer: (SHOW ANSWER)

NEW QUESTION: 119
You have an Azure subscription that contains the storage accounts shown in the following, table.

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

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

Answer:

see the answer below in explanation.

Explanation:

Answer as below.

NEW QUESTION: 120

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

You plan to implement an application that will consist of the resources shown in the following table.

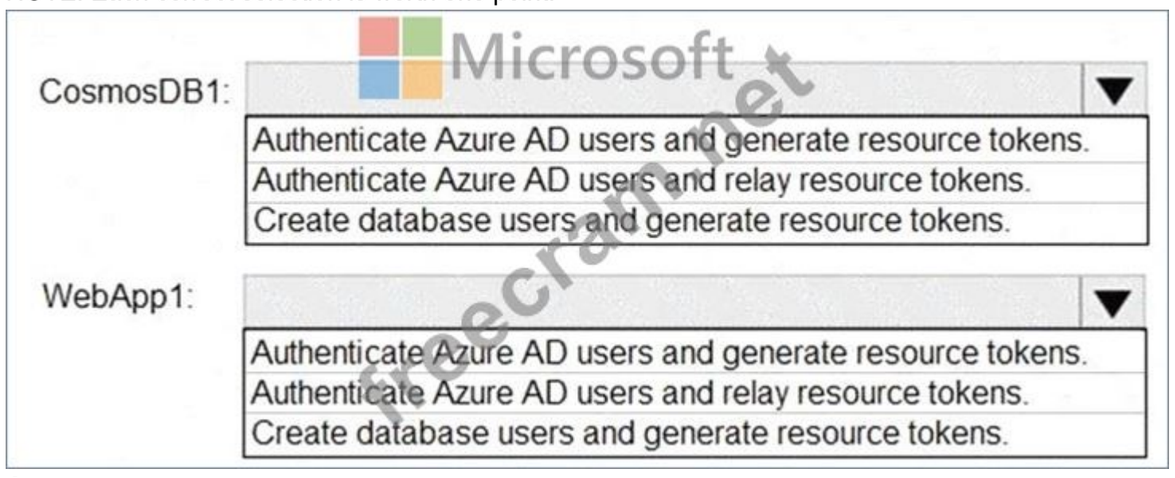
Name	Type	Description
CosmosDBAccount1	Azure Cosmos DB account	A Cosmos DB account containing a database Named CosmosDB1 that serves as a back-end tier of the application
WebApp1	Azure web app	A web app configured to serve as the middle tier of the application

Users will authenticate by using their Azure AD user account and access the Cosmos DB account by using resource tokens.

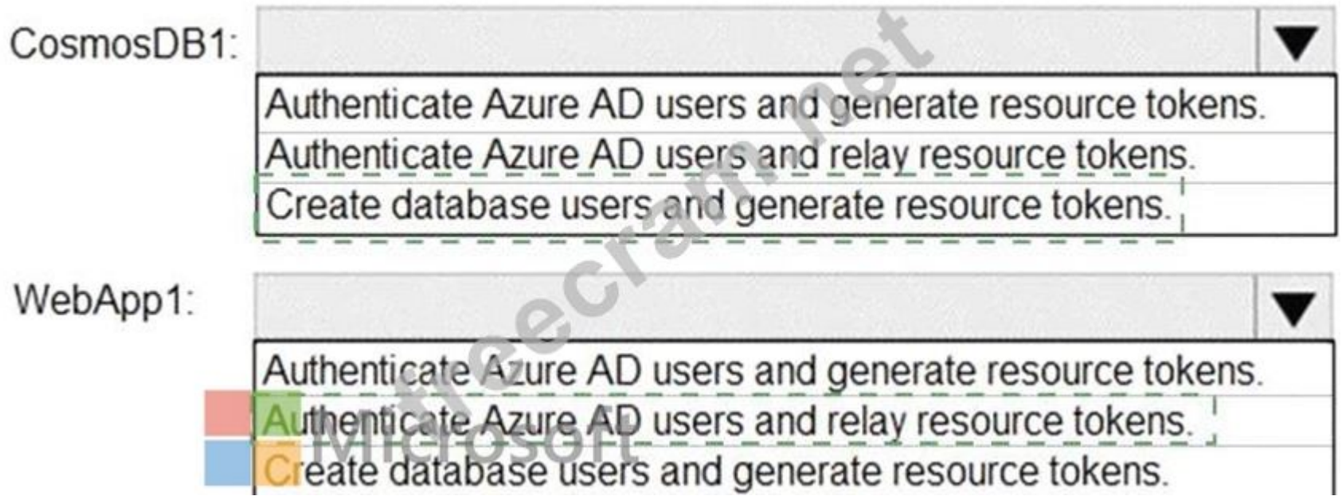
You need to identify which tasks will be implemented in CosmosDB1 and WebApp1.

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

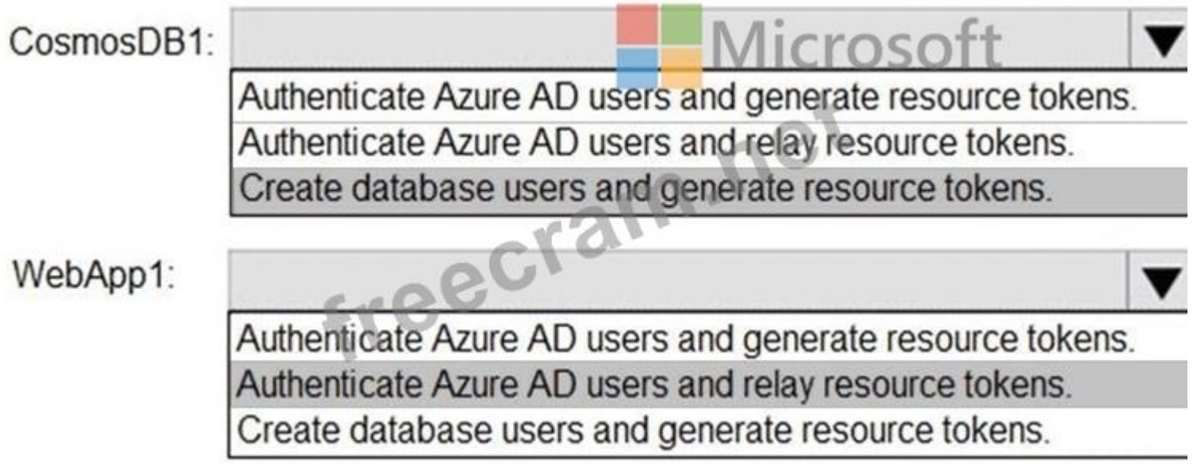
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

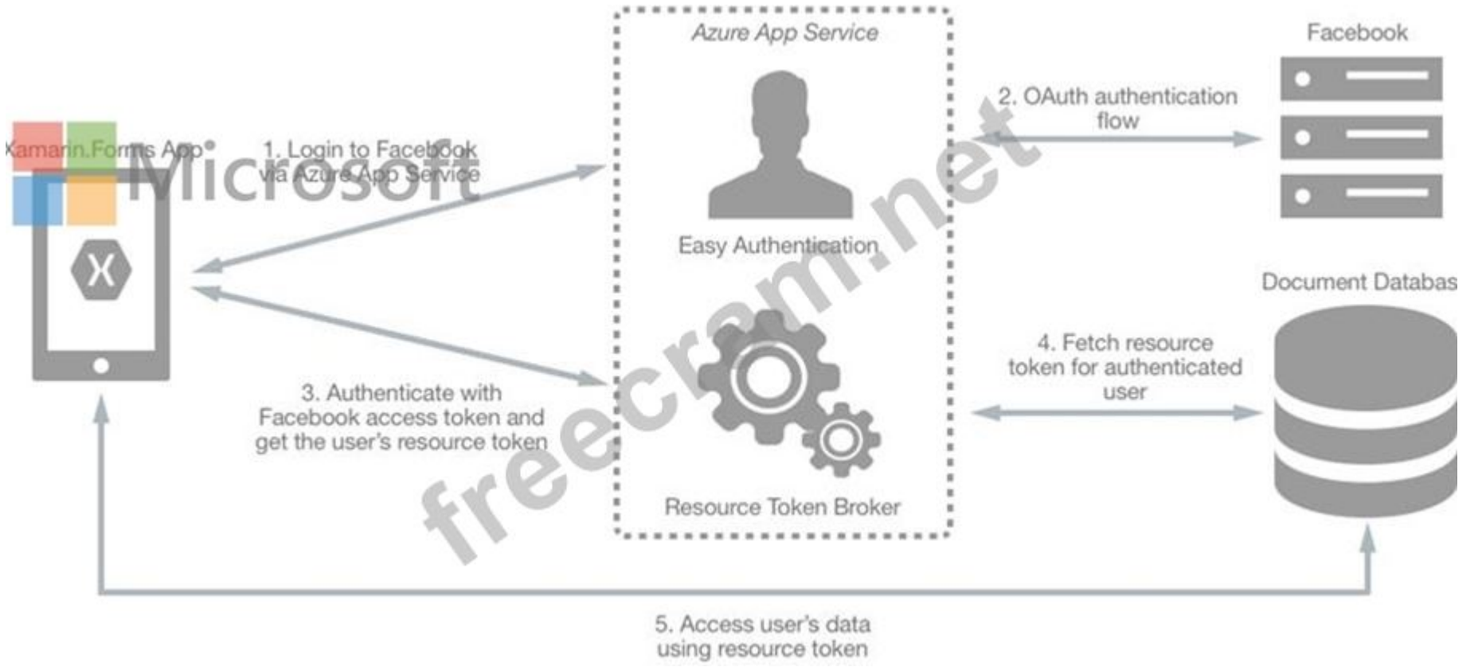


CosmosDB1: Create database users and generate resource tokens.

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

WebApp1: Authenticate Azure AD users and relay resource tokens

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



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

NEW QUESTION: 121
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 1
You need to configure Azure to allow RDP connections from the Internet to a virtual machine named VM1.
The solution must minimize the attack surface of VM1.
Answer:
Check below steps in explanation for Task.
Explanation
To configure Azure to allow RDP connections from the Internet to a virtual machine named VM1, you can follow the steps below:
Create a new inbound security rule in the network security group (NSG) that is associated with the virtual network subnet that contains VM1. The rule should allow RDP traffic from the Internet to the virtual network subnet. You can use the Azure portal, Azure PowerShell, or Azure CLI to create the rule.
Configure the network security group (NSG) to associate it with the virtual network subnet that contains VM1.

Configure the virtual machine to allow RDP traffic. You can use the Azure portal, Azure PowerShell, or Azure CLI to configure the virtual machine.
To minimize the attack surface of VM1, you can use the following best practices:
Use a strong password for the local administrator account on the virtual machine.
Use Network Security Groups (NSGs) to restrict traffic to only the necessary ports and protocols.
Use Azure Security Center to monitor and protect your virtual machines.

NEW QUESTION: 122
You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

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

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

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

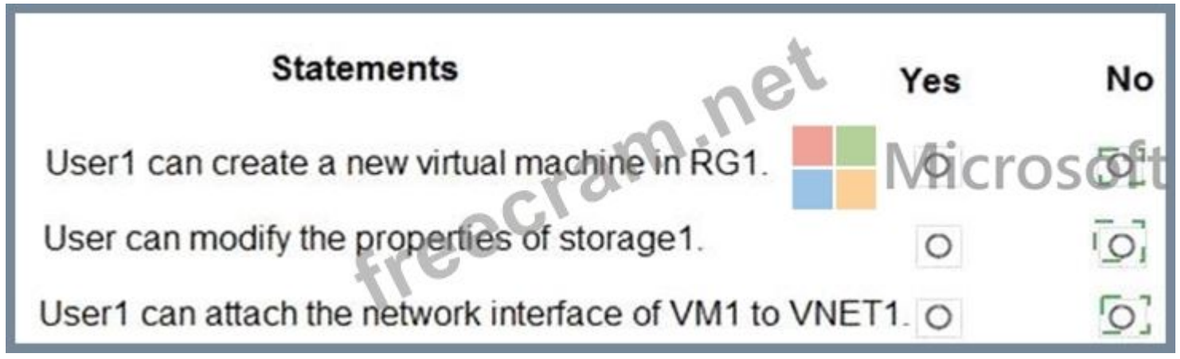

You assign Role1 to User1 for RG1.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can create a new virtual machine in RG1.	○	○
User can modify the properties of storage1.	○	○
User1 can attach the network interface of VM1 to VNET1.	○	○

Answer:



Explanation:

NO

NO

NO

Reference:

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

NEW QUESTION: 123

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: 124
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 customer-managed keys
C. Azure Disk Encryption
D. TLS
E. Transparent Data Encryption (TDE) with Microsoft-managed keys
Answer: (SHOW ANSWER)

NEW QUESTION: 125
You have the Azure Information Protection conditions shown in the following table.

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

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

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

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

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

NOTE: Each correct selection is worth one point.

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

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

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

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

Answer:

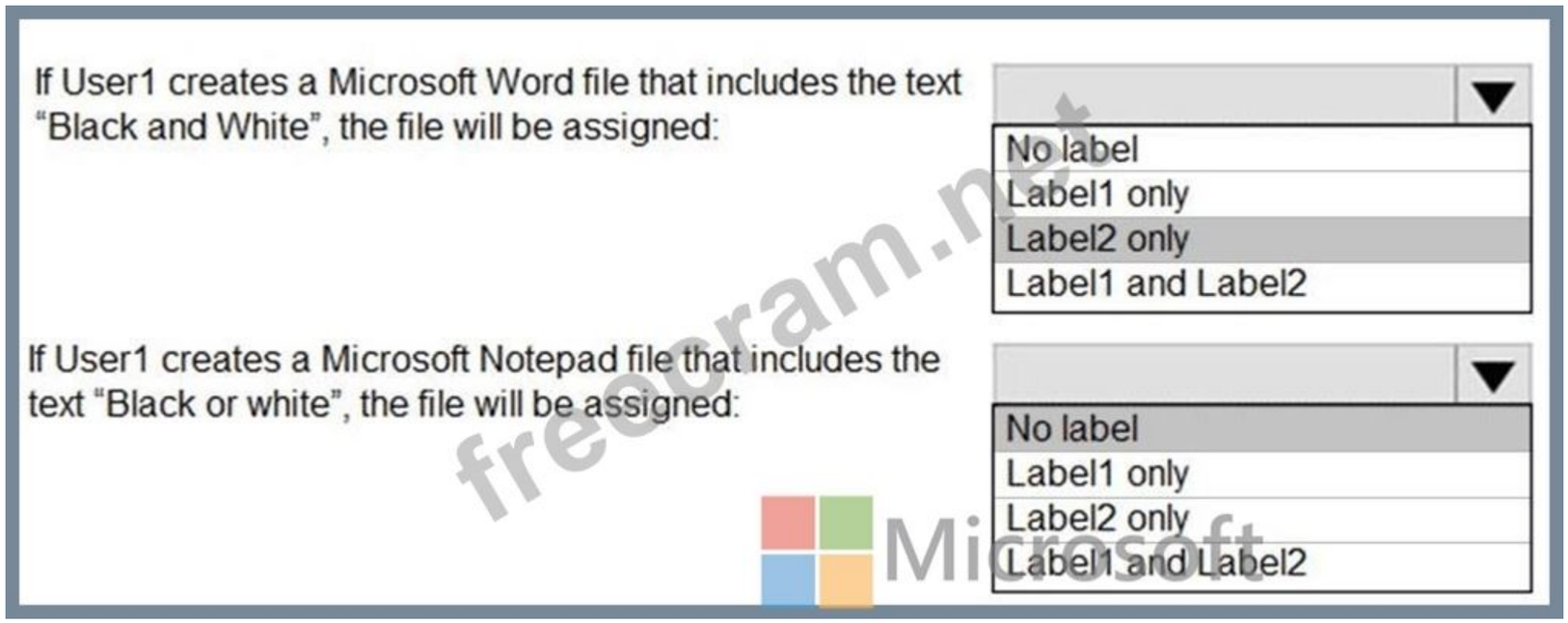
If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

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

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

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

Explanation:



Box 1: Label 2 only

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

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

Box 2: No Label

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

References:

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

NEW QUESTION: 126

You have an Azure subscription that contains a storage account named storage1 and a virtual machine named VM1.

VM1 is connected to a virtual network named VNet1 that contains one subnet and uses Azure DNS.

You need to ensure that VM1 connects to storage1 by using a private IP address. The solution must minimize administrative effort.

What should you do?

A. For storage1, create a new private endpoint.

B. For storage1, disable public network access.

C. Create an Azure Private DNS zone.

D. On VNet1. create a new subnet.

Answer: (SHOW ANSWER)

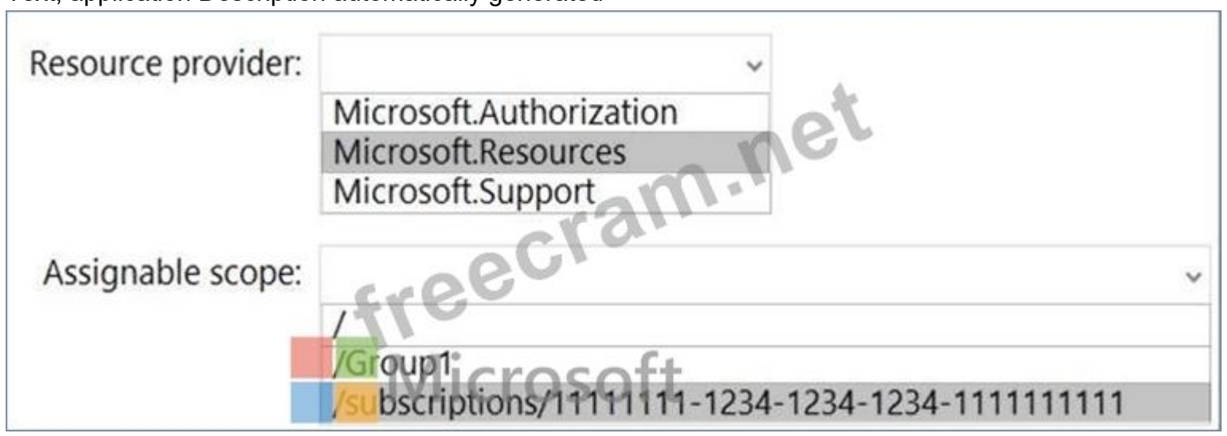
NEW QUESTION: 127

You have a management group named Group1 that contains an Azure subscription named sub1. Sub1 has a subscription ID of 11111111-1234-1234-1234-1111111111.

You need to create a custom Azure role-based access control (RBAC) role that will delegate permissions to manage the tags on all the objects in Group1.
What should you include in the role definition of Role1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:
Text, application Description automatically generated



Note: Assigning a custom RBAC role as the Management Group level is currently in preview only. So, for now the answer to the assignable scope is the subscription level.
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#step-5-assignable- scopes

NEW QUESTION: 128
You create a new Azure subscription.
You need to ensure that you can create custom alert rules in Azure Security Center.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. Onboard Azure Active Directory (Azure AD) Identity Protection.
B. Create an Azure Storage account.
C. Implement Azure Advisor recommendations.
D. Create an Azure Log Analytics workspace.
E. Upgrade the pricing tier of Security Center to Standard.
Answer: (SHOW ANSWER)
D: You need write permission in the workspace that you select to store your custom alert.
References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-custom-alert

NEW QUESTION: 129
You need to implement the planned change for storage2. The solution must meet the technical requirements for storage encryption.
A. Assign an Azure role-based access control (Azure RBAC) role to storage2.
B. Enable purge protection for storage2.
C. Create an encryption scope in storage2.
D. Configure storage2 to use an account encryption key.
Answer: (SHOW ANSWER)

NEW QUESTION: 130
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. storage1 and Function1 only
D. Function1 only
E. SQL1 only
F. storage1, SQL1, and Function1
Answer: (SHOW ANSWER)

NEW QUESTION: 131
You have an Azure subscription that contains an Azure web app named Appl.
You plan to configure a Conditional Access policy for Appl. The solution must meet the following requirements:
* Only allow access to App1 from Windows devices.
* Only allow devices that are marked as compliant to access Appl.
Which Conditional Access policy settings should you configure? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION: 132
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that contains an Azure Kubernetes Service (AKS) cluster named AKS1 and an Azure container registry named AZCR1.
You need to ensure that AKS1 can deploy container images stored in AZCR1.

Solution: You configure AKS1 to use a user-assigned managed identity and assign the Azure Kubernetes Service Cluster Admin Role to the managed identity.
Does this meet the requirement?
A. Yes
B. No
Answer: A (LEAVE A REPLY)

NEW QUESTION: 133
You have Azure Resource Manager templates that you use to deploy Azure virtual machines.
You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.
What should you use?
A. Azure Advisor
B. an Azure Desired State Configuration (DSC) virtual machine extension
C. Azure Logic Apps
D. security policies in Azure Security Center
Answer: (SHOW ANSWER)

NEW QUESTION: 134
You are evaluating the security of the network communication between the virtual machines in Sub2.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	○	○
From VM1, you can successfully ping the private IP address of VM3.	○	○
From VM1, you can successfully ping the public IP address of VM5.	○	○

Answer:

Answer Area

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	○	○
From VM1, you can successfully ping the private IP address of VM3.	○	○
From VM1, you can successfully ping the public IP address of VM5.	○	○

Explanation:
Yes,
Yes
No

NEW QUESTION: 135
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 Private endpoint connections tab, create a private endpoint for 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 Firewalls and virtual networks tab, add VNet1.
D. From the Firewalls and virtual networks tab, add the IP address of VM1.
Answer: (SHOW ANSWER)

NEW QUESTION: 136
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. a policy-specific non-compliance message
B. the remediation task of the policy
C. the effect of the policy
D. the default non-compliance message of the built-in
Answer: (SHOW ANSWER)

NEW QUESTION: 137
You have an Azure subscription that contains an Azure Data Lake Storage Gen2 account named storage1.
You deploy an Azure Synapse Analytics workspace named synapsews1 to a managed virtual network. You need to enable access from synapsews1 to storage1. What should you configure?
A. a network security group (NSG)
B. peering
C. a virtual network gateway
D. a private endpoint
Answer: (SHOW ANSWER)

NEW QUESTION: 138
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: 139

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

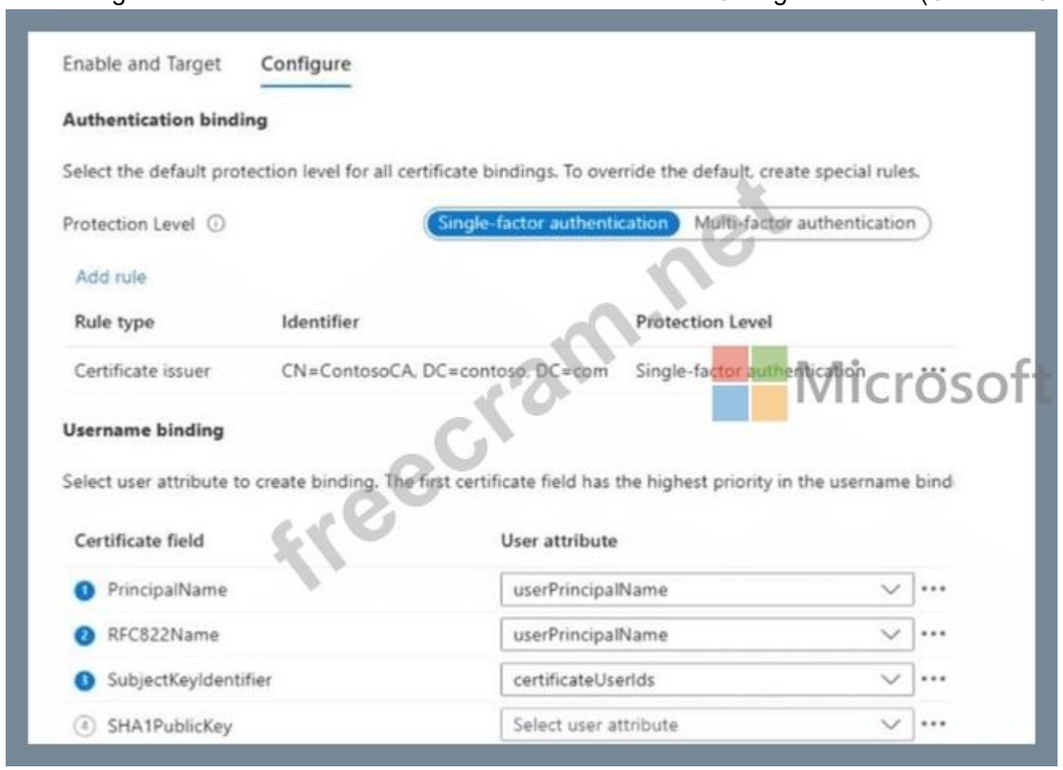
o Access controls

* 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:

Explanation:

NEW QUESTION: 140

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

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

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

Answer:

Explanation:

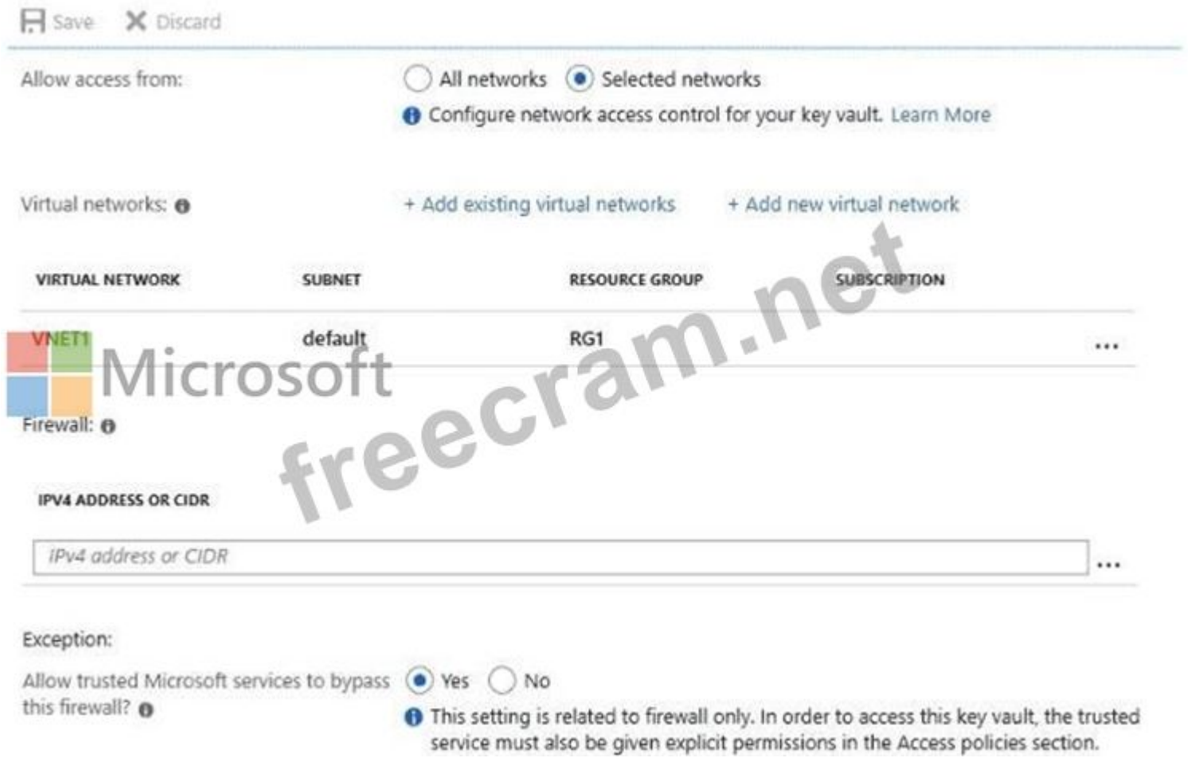
NEW QUESTION: 141
You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.
You need to use automatically generated service principal for the AKS cluster to authenticate to the Azure Container Registry.
What should you create?
A. a secret in Azure Key Vault
B. a role assignment

C. an Azure Active Directory (Azure AD) user
D. an Azure Active Directory (Azure AD) group
Answer: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal

NEW QUESTION: 142
You have an Azure subscription that contains an Azure key vault named KeyVault1 and the virtual machines shown in the following table.

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

You enable the Azure Disk Encryption for volume encryption KeyVault1 setting.
KeyVault1 is configured as shown in the following exhibit.



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

Answer:

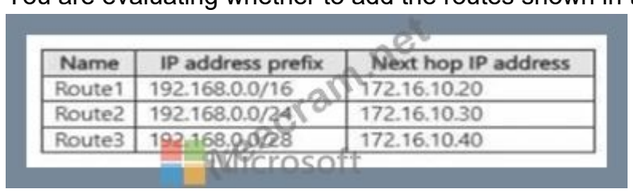
Explanation:

NEW QUESTION: 143

You have an Azure subscription that contains a route table named RT1. RT1 includes a route that has the following configurations:

* Name: RouteA
* IP address prefix: 192.168.0.0/24
* Next hop IP address: 172.16.10.10

You are evaluating whether to add the routes shown in the following table.



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

Which routes can you add to RT1?

A. Route3 only

B. Route1 only

C. Route1 and Route2 only

D. Route2 only
E. Route1 and Route3 only
F. Route2 and Route3 only
Answer: (SHOW ANSWER)

NEW QUESTION: 144
You have an Azure subscription.
You plan to create a custom role-based access control (RBAC) role that will provide permission to read the Azure Storage account.
Which property of the RBAC role definition should you configure?
A. NotActions []
B. DataActions []
C. AssignableScopes []
D. Actions []
Answer: (SHOW ANSWER)
To 'Read a storage account', ie. list the blobs in the storage account, you need an 'Action' permission.
To read the data in a storage account, ie. open a blob, you need a 'DataAction' permission.
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-definitions

NEW QUESTION: 145
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 Identity
B. Microsoft Defender for Cloud
C. Microsoft Sentinel
D. Azure Active Directory (Azure AD) Identity Protection
Answer: (SHOW ANSWER)

NEW QUESTION: 146
You have a Microsoft 365 E5 subscription.
You have an Azure subscription that uses Microsoft Defender for Cloud.
You have an on-premises datacenter that contains the servers shown in the following table.
You enable direct onboarding to Microsoft Defender for Cloud.
Which servers will be onboarded to Defender for Cloud?
A. Server1 and Server3
B. Server1 only
C. Server3 only
D. Server2 only
E. Servei2 and Servet3
F. Server1, Server2, and Server3

Answer: (SHOW ANSWER)

NEW QUESTION: 147
You have an Azure AD tenant.
You plan to implement an authentication solution to meet the following requirements:
* Require number matching.
* Display the geographical location when signing in.
Which authentication method should you include in the solution?
A. Microsoft Authenticator
B. FID02 security key
C. SMS
D. Temporary Access Pass
Answer: (SHOW ANSWER)

NEW QUESTION: 148
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: 149
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. OWASP Top 1O
B. Attack Surface Summary
C. Security Posture
D. GDPR Compliance
Answer: (SHOW ANSWER)

NEW QUESTION: 150

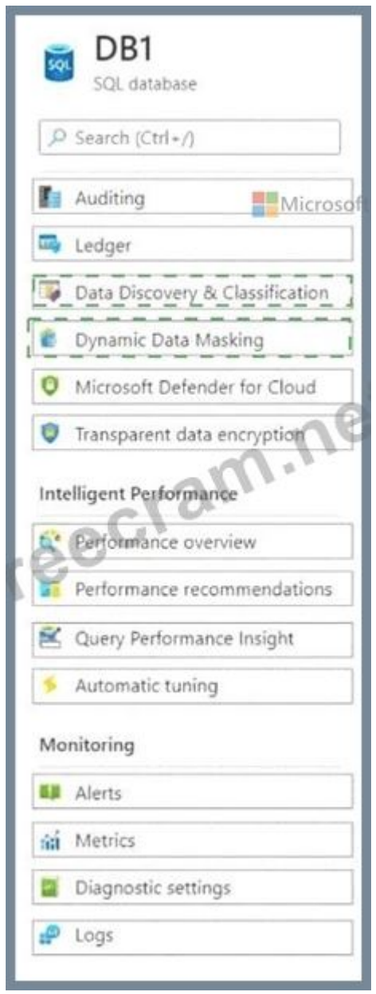
You have an Azure subscription named Sub1.
In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.
You need to modify Play1 to send email messages to a distribution group named Alerts.
What should you use to modify Play1?

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: 151
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:

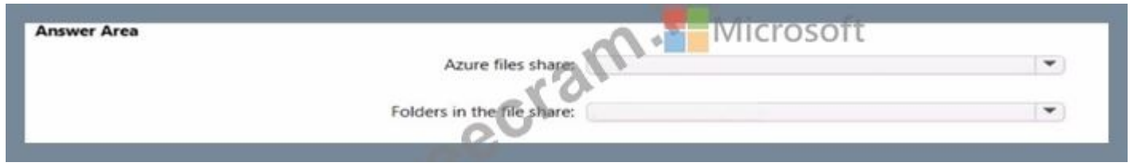
1. Data Discovery & Classification
2. Dynamic Data Masking

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: 152

You have an Azure Active directory tenant that syncs with an Active Directory Domain Services (AD DS) domain.
You plan to create an Azure file share that will contain folders and files.
Which identity store can you use to assign permissions to the Azure file share and folders within the share?
To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



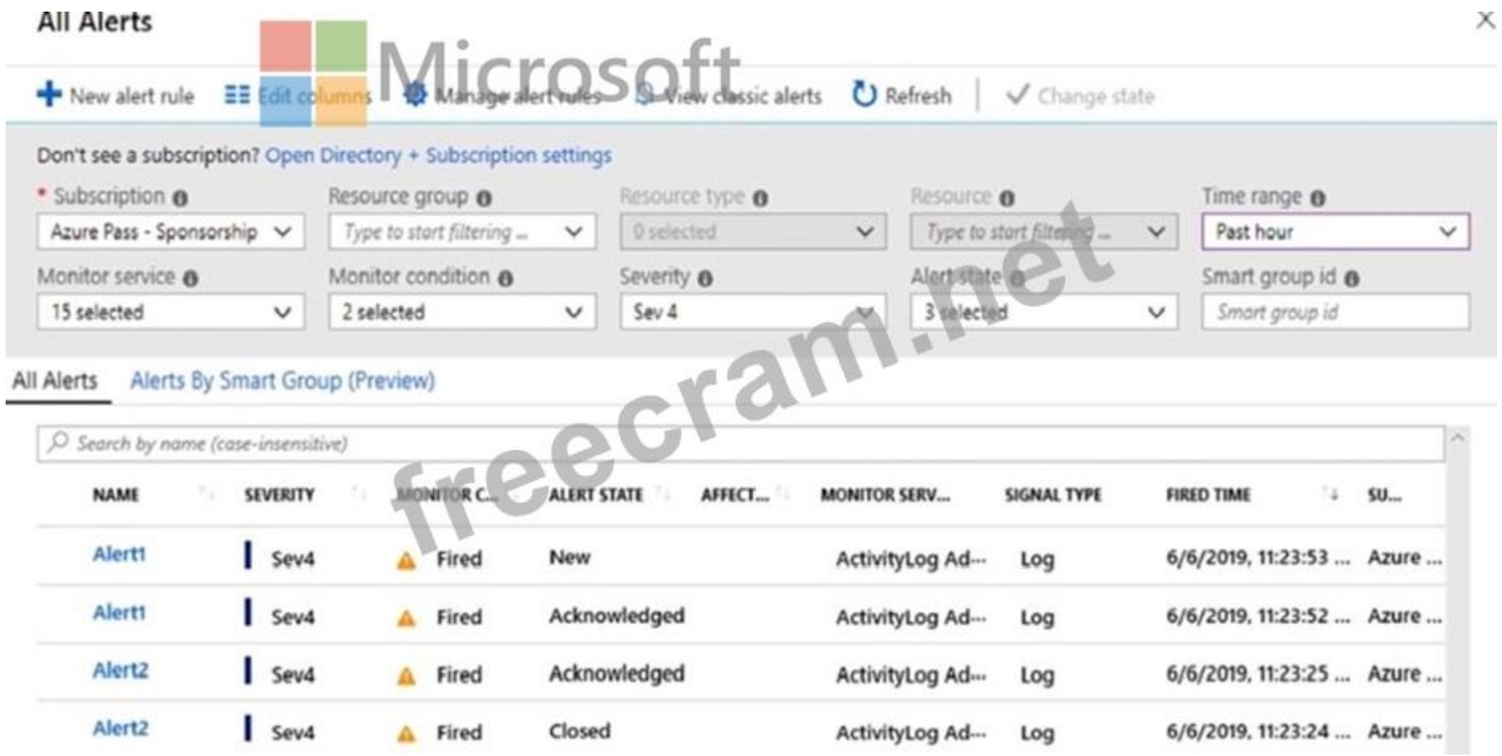
Answer:
See the answer below at Explanation.
Explanation:
Answer is as image below.

NEW QUESTION: 153
You have a Microsoft Entra tenant that uses Microsoft Entra Permissions Management and contains the accounts shown in the following table:

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

Which accounts will be listed as assigned to highly privileged roles on the Azure AD insights tab in the Entra Permissions Management portal?
A. Admin2 and Admin4 only
B. Admin1. Admin2, Admin3. and Admin4
C. Admin2 and Admin3 only
D. Admin1 only
E. Admin1. Admin2, and Admin3 only
F. Admin2. Admin3, and Admin4 only
Answer: (SHOW ANSWER)

NEW QUESTION: 154
You have an Azure subscription that contains the alerts shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

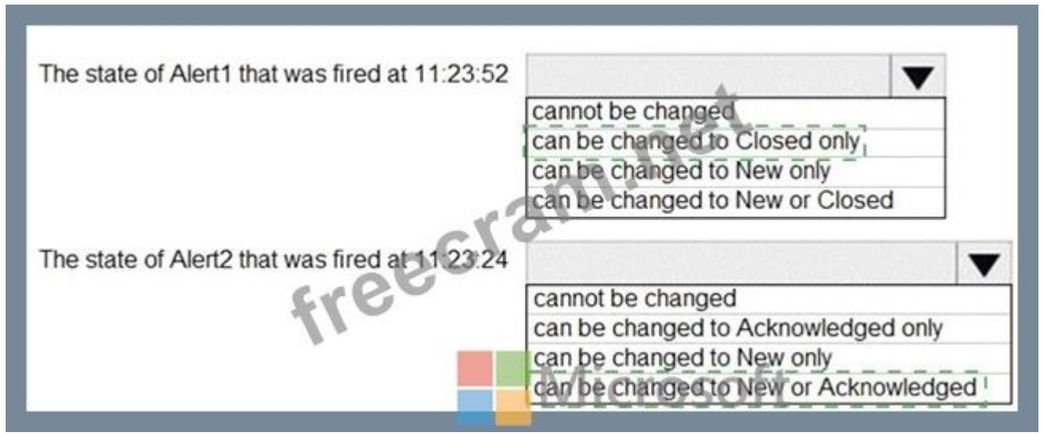
The state of Alert1 that was fired at 11:23:52

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

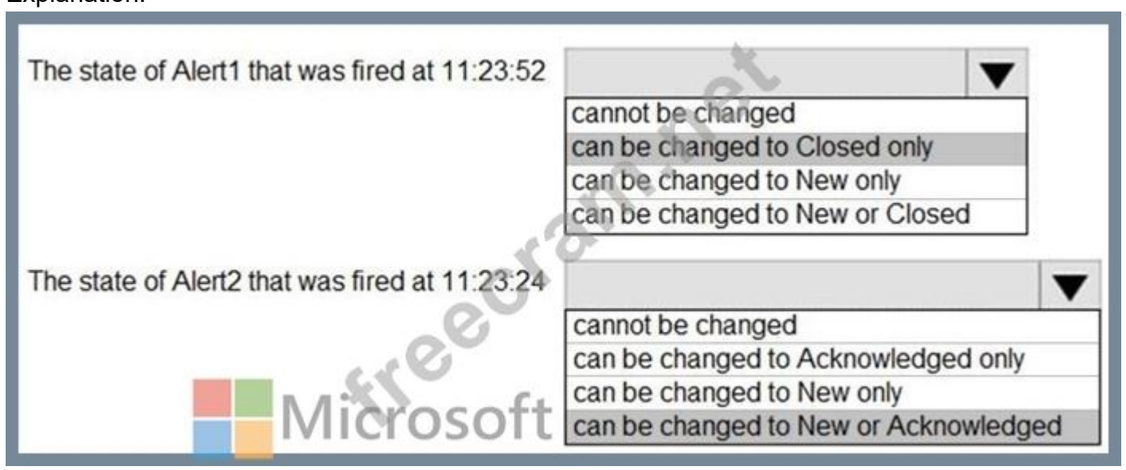
The state of Alert2 that was fired at 11:23:24

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

Answer:



Explanation:



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

NEW QUESTION: 155
You need to recommend an encryption solution for the planned ExpressRoute implementation. The solution must meet the technical requirements.
Which ExpressRoute circuit should you recommend for each type of encryption? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Answer Area

Explanation:

NEW QUESTION: 156

You have an Azure resource group that contains 100 virtual machines.

You have an initiative named Initiative1 that contains multiple policy definitions. Initiative1 is assigned to the resource group.

You need to identify which resources do NOT match the policy definitions.

What should you do?

A. From Azure Security Center, view the Regulatory compliance assessment.

B. From the Policy blade of the Azure Active Directory admin center, select Compliance.

C. From Azure Security Center, view the Secure Score.

D. From the Policy blade of the Azure Active Directory admin center, select Assignments.

Answer: (SHOW ANSWER)

Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/how-to/get-compliance-data#portal

NEW QUESTION: 157
You have an Azure key vault named Vault1 that stores the resources shown in the following table.

Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

Which resources support the creation of a rotation policy?
A. Secret1 and Cert1 only
B. Cert1 only
C. Key 1 only
D. Key1, Secret1, and Cert1
E. Key1 and Secret1 only
F. Key1 and Cert1 only
Answer: (SHOW ANSWER)

NEW QUESTION: 158
You are evaluating the security of the network communication between the virtual machines in Sub2.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Q1: No { and it should not be allowed as only TCP 80 is allowed from the "Internet" service tag Q2: Yes {as it should be for VMs in the same local subnet pinging each other on private IP and no NSG configured} Q3: Yes {VM5 is in subnet where 1st rule of NSG allows any traffic from any source to the destination}

NEW QUESTION: 159
You have an Azure subscription that contains an Azure Data Lake Storage account named sa1.
You plan to deploy an app named App1 that will access sa1 and perform operations, including Read. List, Create Directory, and Delete Directory.
You need to ensure that App1 can connect securely to sa1 by using a private endpoint What is the minimum number of private endpoints required for sa1?
A. 1
B. 2
C. 3
D. 4
E. 5
Answer: (SHOW ANSWER)
A private endpoint is a network interface that connects you privately and securely to a service that's powered by Azure Private Link. By enabling a private endpoint, you're bringing the service into your virtual network.
You only need one private endpoint for each service that you want to access privately, such as Azure Data Lake Storage. You can create a private endpoint for your Azure Data Lake Storage account named sa1 by following the steps in this article.
References:
What is a private endpoint? - Azure Private Link
Private Endpoints for Azure Storage are now Generally Available
Step-by-Step: How to Configure a Private Endpoint to Secure Azure ...

NEW QUESTION: 160
Lab Task
Task 3
You need to ensure that a user named Danny-31330471 can sign in to any SQL database on a Microsoft SQL server named web31330471 by using SQL Server Management Studio (SSMS) and Azure AD credentials.

Answer:
see the task answer with step by step below:
* Create and register an Azure AD application. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to specify a name, such as SQLServerCTP1, and select the supported account types, such as Accounts in this organization directory only.
* Grant application permissions. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to assign the Directory.Read.All permission to the application and grant admin consent for your organization.
* Create and assign a certificate. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to create a self-signed certificate and upload it to the application. You also need to store the certificate in Azure Key Vault and grant access policies to the application and your SQL Server.
* Configure Azure AD authentication for SQL Server through Azure portal. You can use the Azure portal to do this. You need to select your SQL Server resource and enable Azure AD authentication. You also need to select your Azure AD application as the Azure AD admin for your SQL Server.
* Create logins and users. You can use SSMS or Transact-SQL to do this. You need to connect to your SQL Server as the Azure AD admin and create a login for Danny-31330471. You also need to create a user for Danny-31330471 in each database that he needs access to.
* Connect with a supported authentication method. You can use SSMS or SqlClient to do this. You need to specify the Authentication connection property in the connection string as Active Directory Password or Active Directory Integrated. You also need to provide the username and password of Danny-31330471.

NEW QUESTION: 161

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 Area

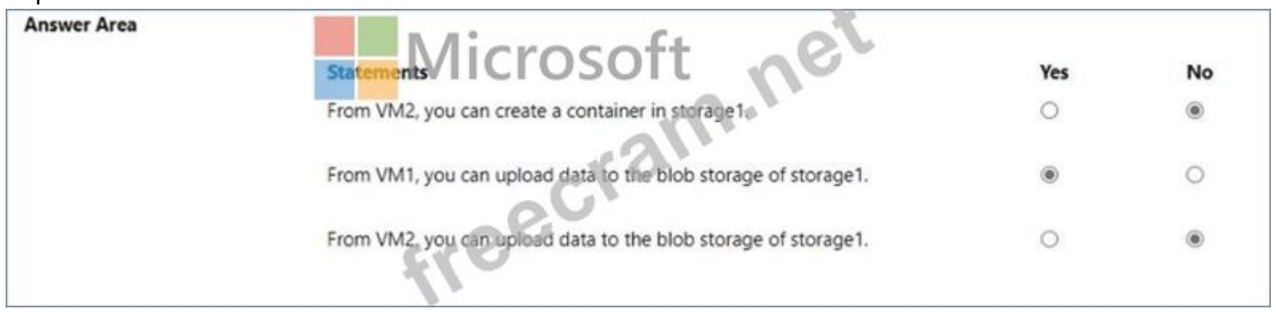
Statements	Yes	No
From VM2, you can create a container in storage1.	○	○
From VM1, you can upload data to the blob storage of storage1.	○	○
From VM2, you can upload data to the blob storage of storage1.	○	○

Answer:

Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1.	○	○
From VM1, you can upload data to the blob storage of storage1.	○	○
From VM2, you can upload data to the blob storage of storage1.	○	○

Explanation:



NEW QUESTION: 162

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

Name	Description
User1	Uses app password authentication for the Mail and Calendar app in Windows 10
User2	Uses Outlook on the web

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. Configure a multi-factor authentication (MFA) registration policy.

B. Create a new app registration.

C. Assign User! the Authentication Policy Administrator role.

D. Enable Azure AD Password Protection.

Answer: (SHOW ANSWER)

NEW QUESTION: 163

Lab Task

use the following login credentials as needed:

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

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

Azure Username: Userl -28681041@ExamUsers.com

Azure Password: GpOAe4@lDg

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 28681041

Task 8

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

Answer:

Check below steps in explanation for Task

Explanation:

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

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

In the left pane, select Firewalls and virtual networks.
In the Firewalls and virtual networks pane, select Selected networks.
In the Selected networks pane, select Add existing virtual network.
In the Add existing virtual network pane, select the virtual network that does not allow HTTP connections.
Select Add.

NEW QUESTION: 164
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 Non-compliant, and the Compliance State of the policy assignment to RG1 is Compliant.
B. The Compliance State of both policy assignments is Non-compliant.
C. The Compliance State of both policy assignments is Compliant.
D. The Compliance State of the policy assignment to Subscription1 is Compliant, and the Compliance State of the policy assignment to RG1 is Non-compliant.
Answer: (SHOW ANSWER)

NEW QUESTION: 165
Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.
After syncing all on-premises identities to Azure AD, you are informed that users with a givenName attribute starting with LAB should not be allowed to sync to Azure AD.
Which of the following actions should you take?
A. You should make use of the Synchronization Rules Editor to create an attribute-based filtering rule.
B. You should configure a DNAT rule on the Firewall.
C. B. You should configure a network traffic filtering rule on the Firewall.
D. You should make use of Active Directory Users and Computers to create an attribute-based filtering rule.
Answer: (SHOW ANSWER)
Use the Synchronization Rules Editor and write attribute-based filtering rule.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

NEW QUESTION: 166
You have two Azure subscriptions named Sub1 and Sub2 that contain the virtual networks shown in the following table.

Name	Subscription	Tag
VNet1	Sub1	*None*
VNet2	Sub1	Red

You have an Azure Virtual Network Manager instance named AVNM1 that has the following configurations:
* Management scope: Sub1
* Network groups:
* NetGrp1: Static membership that includes VNet1
* NetGrp2: Dynamic membership that has the following criteria: Tags that contain Red
* Security admin rule collection: SARule1
* Deployed to all Azure regions

Name	Subscription	Tag
VNet3	Sub1	Red
VNet4	Sub2	Red

You create two new virtual networks as shown in the following table.
Which virtual networks will have SARule1 applied?
A. VNet1, VNet2, and VNet3 only
B. VNet2, VNet3, and VNet4 only
C. VNet1, VNet2, VNet3, and VNet4
D. VNet2 and VNet3 only
E. VNet1 and VNet2 only
Answer: (SHOW ANSWER)

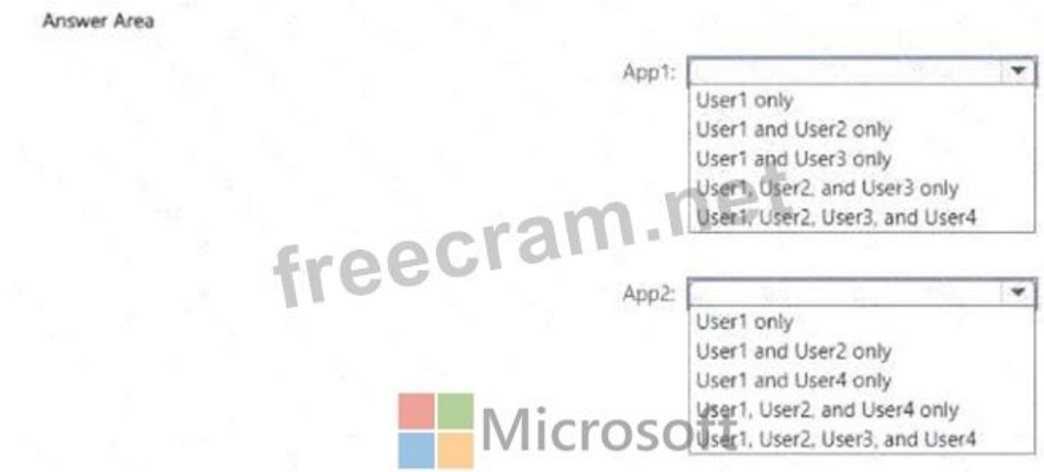
NEW QUESTION: 167
You have a Microsoft Entra tenant named contoso.com that contains the users shown in the following table.

Name	Role
User1	Application Administrator
User2	Application Developer
User3	Azure DevOps Administrator
User4	Security Operator

You add enterprise applications to contoso.com as shown in the following table.

Name	Owner	Users and groups
App1	User3	User4
App2	User4	User3

You need to Identify which users can grant admin consent for App1 and App2.



Answer:

Explanation:

NEW QUESTION: 168

Lab Task

use the following login credentials as needed:

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

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

Azure Username: Userl -28681041@ExamUsers.com

Azure Password: GpOAe4@lDg

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 28681041

Task 9

You need to ensure that the rg1lod28681041n1 Azure Storage account is encrypted by using a key stored in the KeyVault28681041 Azure key vault.

Answer:

Check below steps in explanation for Task

Explanation:

To ensure that the rg1lod28681041n1 Azure Storage account is encrypted by using a key stored in the KeyVault28681041 Azure key vault, you can follow these steps:

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

In the left pane, select Encryption.

In the Encryption pane, select Customer-managed key.

In the Customer-managed key pane, select Select from Key Vault.

In the Select from Key Vault pane, enter the following information:

Key vault: Select the KeyVault28681041 Azure key vault.

Key: Select the key you want to use.

Select Save.

NEW QUESTION: 169

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

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

Save Discard Upload Download

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


```
{
    "id": "d6b00db3-7ef4-4f3c-b1e7-8346f0a59546",
    "acceptMappedClaims": null,
    "accessTokenAcceptedVersion": null,
    "addIns": [],
    "allowPublicClient": null,
    "appId": "88137405-6a75-4c20-903a-f7b18ff7d496",
    "appRoles": [],
    "oauth2AllowUrlPathMatching": false,
    "createdDateTime": "2019-07-15T21:09:20Z",
    "groupMembershipClaims": null,
    "identifierUris": [],
    "informationalUrls": {
        "termsOfService": null,
        "support": null,
        "privacy": null,
        "marketing": null
    },
    "keyCredentials": [],
    "knownClientApplications": [],
    "logoUrl": null,
    "logoutUrl": null,
    "name": "AKSAzureADServer",
    "oauth2AllowIdTokenImplicitFlow": false,
    "oauth2AllowImplicitFlow": false,
    "oauth2Permissions": [],
    "oauth2RequirePostResponse": false,
    "optionalClaims": null,
    "orgRestrictions": [],
    "parentalControlSettings": {
```


You need to ensure that the AKS cluster and Azure Active Directory (Azure AD) are integrated.

Which property should you modify in the manifest?

A. accessTokenAcceptedVersion

B. keyCredentials

C. groupMembershipClaims

D. acceptMappedClaims

Answer: (SHOW ANSWER)

Reference:

https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli
https://www.codeproject.com/Articles/3211864/Operation-and-Maintenance-of-AKS-Applications

NEW QUESTION: 170
You have an Azure subscription.
You have the following custom role-based access control (RBAC) role definition.

```
{
    "properties": {
        "roleName": "CustomRole",
        "assignableScopes": [
            "/subscriptions/<subid>"
        ],
        "permissions": [
            {
                "actions": [
                    "*"
                ],
                "notActions": [
                    "Microsoft.Authorization/*/Delete",
                    "Microsoft.Authorization/*/Write",
                    "Microsoft.Authorization/elevateAccess/Action",
                    "Microsoft.Sql/servers/administrators/write",
                    "Microsoft.Sql/servers/administrators/delete"
                ],
                "dataActions": [],
                "notDataActions": []
            }
        ]
    }
}
```

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
The custom role grants a user permission to delete Azure SQL Database resources.	○	○
The custom role grants a user permission to manage the Microsoft Entra admin settings for an Azure SQL Database server.	○	○
The custom role grants a user permission to reset the administrator password for instances of Azure Database for MariaDB.	○	○

Answer:

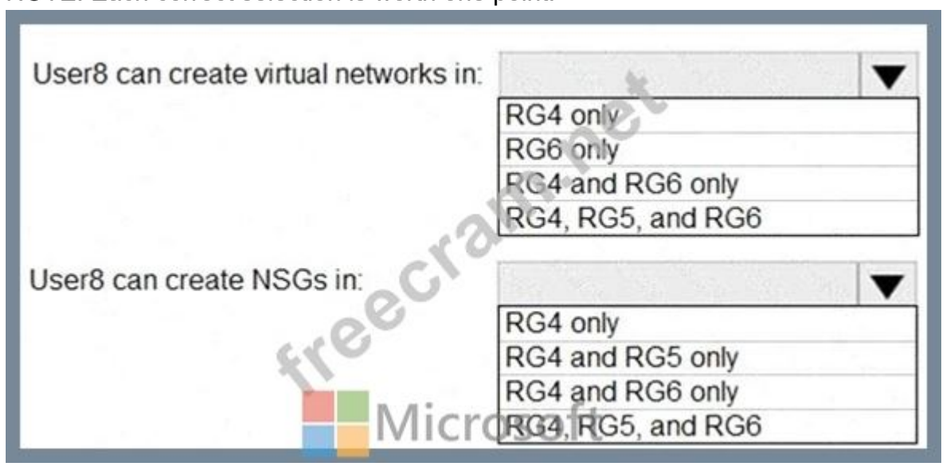
Explanation:

NEW QUESTION: 171

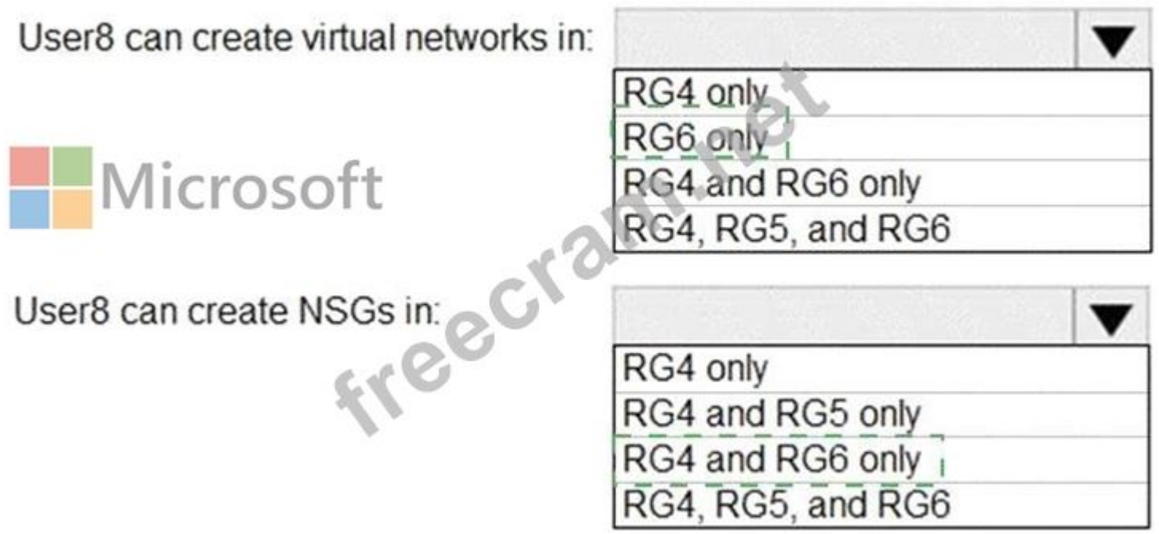
You assign User8 the Owner role for RG4, RG5, and RG6.

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

NOTE: Each correct selection is worth one point.



Answer:



Explanation:
Box1: RG6 only as there is not option for RG5 & RG6 which it should be.
Box2: RG4 & RG6
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: 172

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: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/azure/governance/policy/overview

NEW QUESTION: 173
You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server
2016.
You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.
How should you complete the policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

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

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


Answer:

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

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


Explanation:

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

Box 1: DeployIfNotExists

DeployIfNotExists executes a template deployment when the condition is met.

Box 2: Template

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

Deployment [required]

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

/deployment

References:

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

NEW QUESTION: 174

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: (SHOW ANSWER)

Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin

NEW QUESTION: 175
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: 176
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. App2. App3. and App4 only
D. App3 and App4 only
Answer: (SHOW ANSWER)

NEW QUESTION: 177
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: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory

NEW QUESTION: 178

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

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

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can access App1 from an IP address of 154.12.18.10.	○	○
User2 can access App1 from an IP address of 193.77.10.15.	○	○
User2 can access App1 from an IP address of 154.12.18.34.	○	○

Answer:

Explanation:

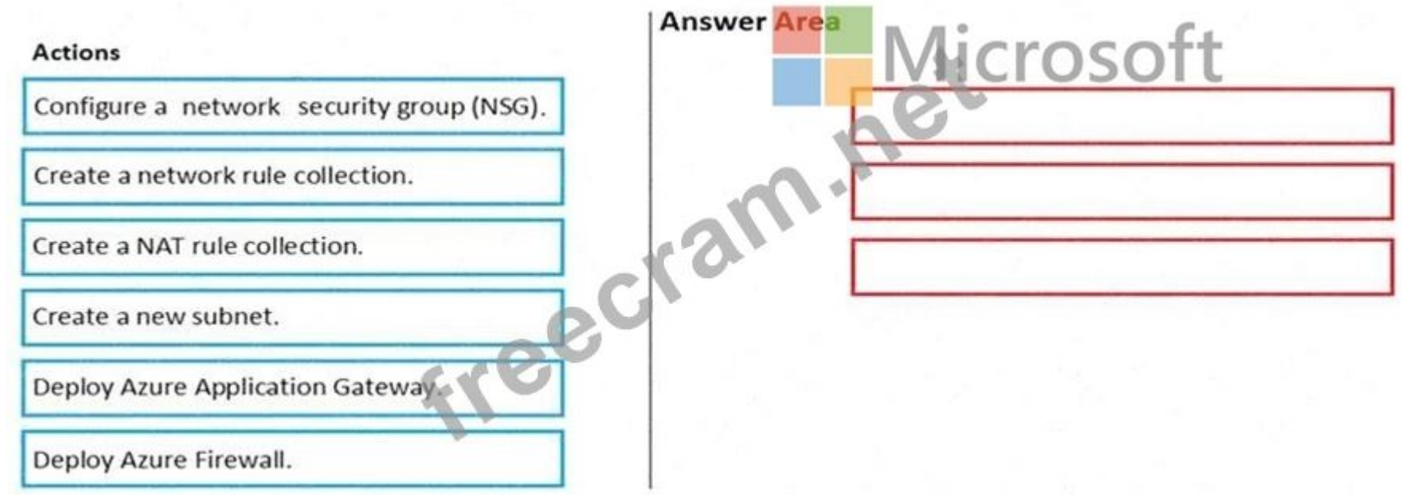
NEW QUESTION: 179

You have an Azure subscription that contains the following resources:

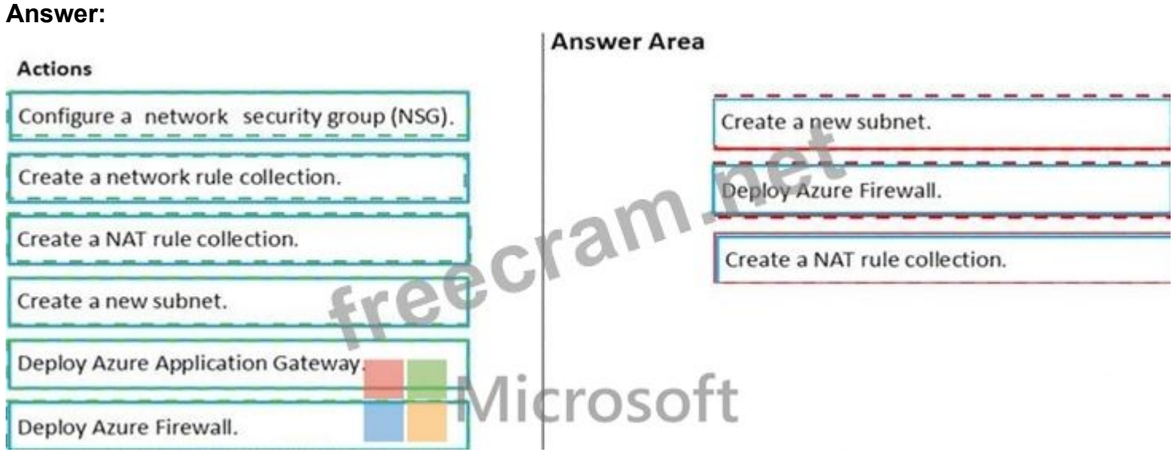
* A virtual network named VNET1 that contains two subnets named Subnet1 and Subnet2.
* A virtual machine named VM1 that has only a private IP address and connects to Subnet1.

You need to ensure that Remote Desktop connections can be established to VM1 from the internet.

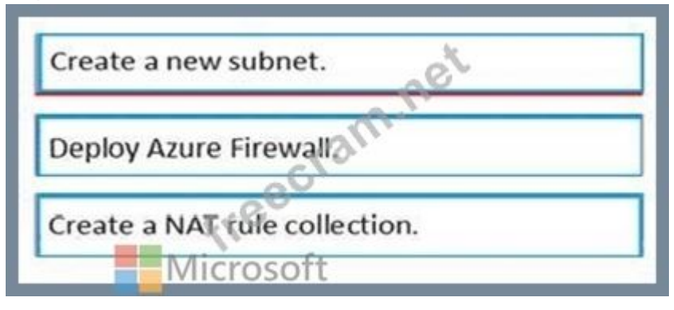
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange then in the correct order.



Answer:



Explanation:



NEW QUESTION: 180

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:

See the answer below at Explanation.

Explanation:

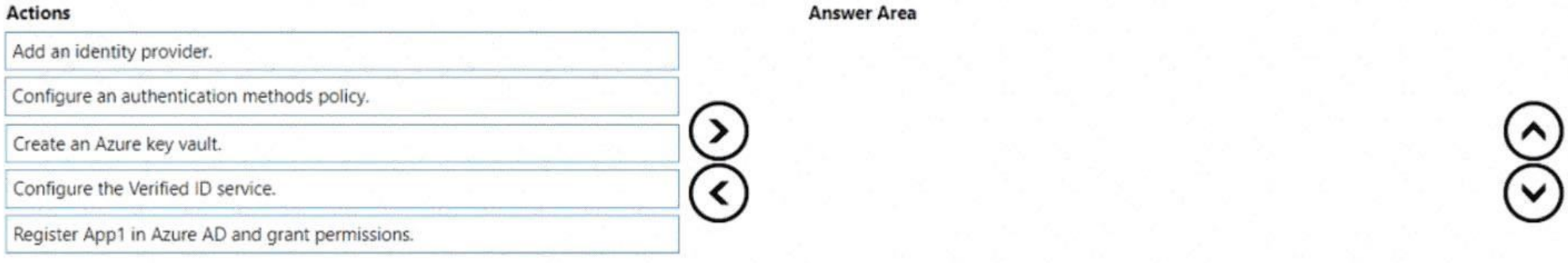
Answer is as image below.

NEW QUESTION: 181

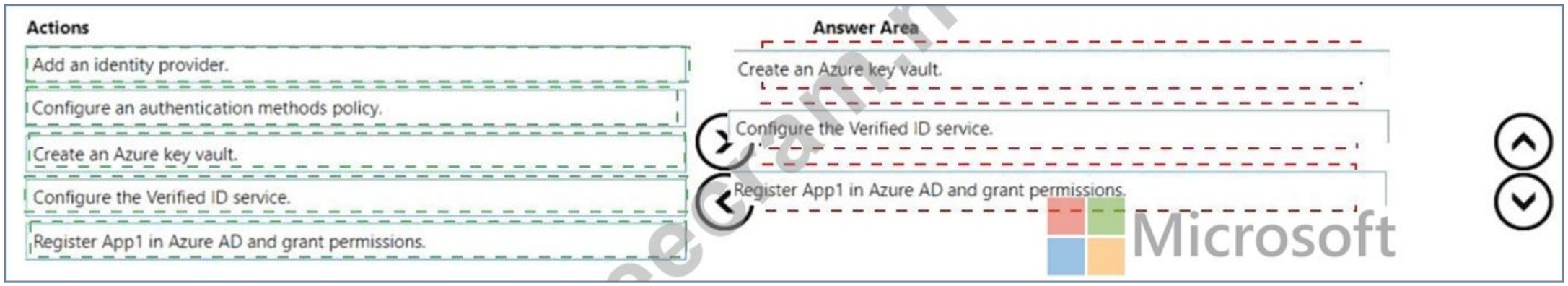
You have an Azure AD Tenant and an application named App1.

You need to ensure that App1 can use Microsoft Entra Verified ID to verify credentials.

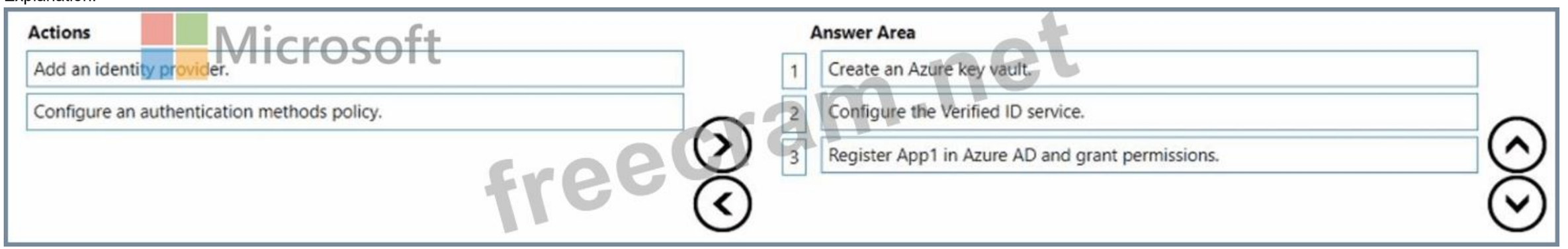
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:



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

NEW QUESTION: 182

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

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

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

Answer:

Explanation:

NEW QUESTION: 183

You have an Azure subscription that contains an Azure SQL database named sql1.

You plan to audit sql1.

You need to configure the audit log destination. The solution must meet the following requirements:

Support querying events by using the Kusto query language.

Minimize administrative effort.

What should you configure?

A. an event hub

B. a storage account

C. a Log Analytics workspace

Answer: (SHOW ANSWER)

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-log-analytics-wizard

NEW QUESTION: 184

You have an Azure subscription that contains an Azure API Management instance named ContosoAPI1.

You need to configure SSL 3.0 support for ContosoAPI1.

What should you do first in the Azure portal?

A. From Protocols + ciphers, select a backend protocol.

B. From Pricing tier, change the pricing tier.

C. From APIs, add an API tag.

D. From Certificates, add a certificate.

Answer: (SHOW ANSWER)

NEW QUESTION: 185

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

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

You create the Azure policies shown in the following table.

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

You create the resource locks shown in the following table.

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

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

NOTE: Each correct selection is worth one point.

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

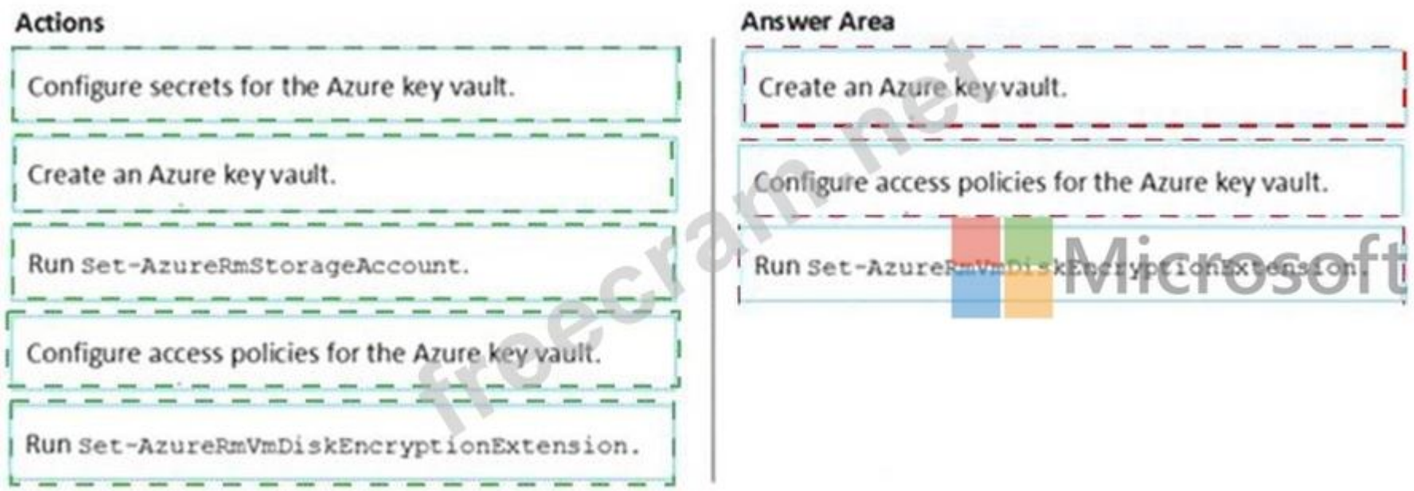
Answer:

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

Explanation:
NO
NO
NO
1.) cannot perform write operation because following scope(s) are locked:
' subscriptions/xxxx/resourceGroups/xxx ' Please remove the lock and try again.
2.) When creating a VM in a resource group with a Read Only lock an error is shown:
" The selected resource group is read only "
3.) Because of the read only lock virtual machines cannot be started nor stopped when the lock is added after the machine started. (not part of this use case, but still good to know.
The article referenced in the answer states different because that is scoped to blueprints.
In the Lock Resources pages is states the following regarding starting VMs:
" A ReadOnly lock on a resource group that contains a virtual machine prevents all users from starting or restarting the virtual machine. These operations require a POST request. "
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

NEW QUESTION: 186
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Subscription named Sub1. Sub1 contains an Azure virtual machine named VM1 that runs Windows Server 2016.
You need to encrypt VM1 disks by using Azure Disk Encryption.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Answer:



Explanation:

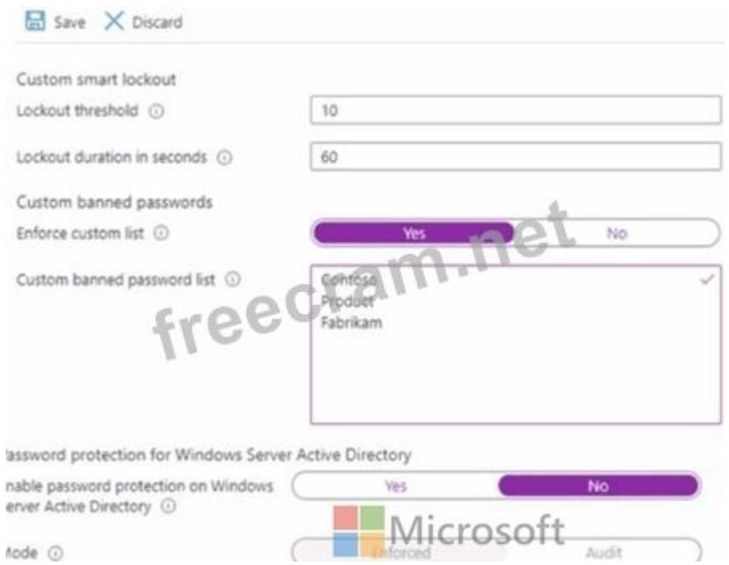
References:

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

NEW QUESTION: 187

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 only
C. User3 only
D. User2only
E. User1 and User3 only
Answer: (SHOW ANSWER)

NEW QUESTION: 188

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

You discover that AKS1 cannot be accessed by using accounts from Contoso.com You need to ensure AKS1 can be accessed by using accounts from Contoso.com The solution must minimize administrative effort.

What should you do first?

A. From Azure recreate AKS1,
B. From AKS1, upgrade the version of Kubermetes.
C. From Azure AD, implement Azure AD Premium P2.
D. From Azure AD, configure the User settings
Answer: (SHOW ANSWER)

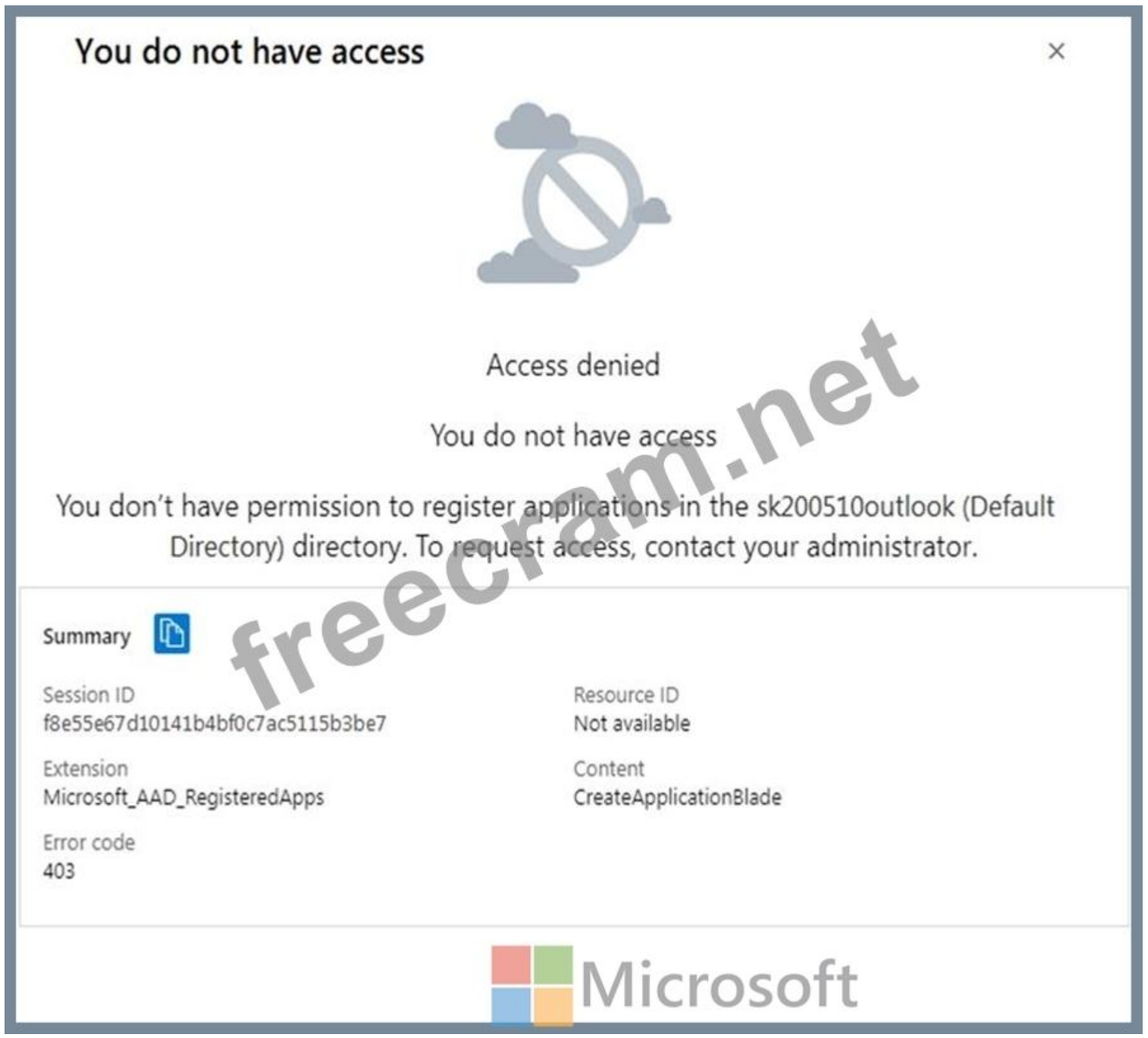
Reference:

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

NEW QUESTION: 189

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: 190
You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant.
When a developer attempts to register an app named App1 in the tenant, the developer receives the error message shown in the following exhibit.



You need to ensure that the developer can register App1 in the tenant.

What should you do for the tenant?

A. Modify the User settings

B. Set Enable Security default to Yes.

C. Modify the Directory properties.

D. Configure the Consent and permissions settings for enterprise applications.

Answer: (SHOW ANSWER)

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

NEW QUESTION: 191
You have an Azure subscription that contains an Azure SQL database named SQLDB1. SQLDB1 contains the columns shown in the following table.

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

For the Email and Birthday columns, you implement dynamic data masking by using the default masking function.
Which value will the users see in each column? To answer, drag the appropriate values to the correct columns.
Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Answer:

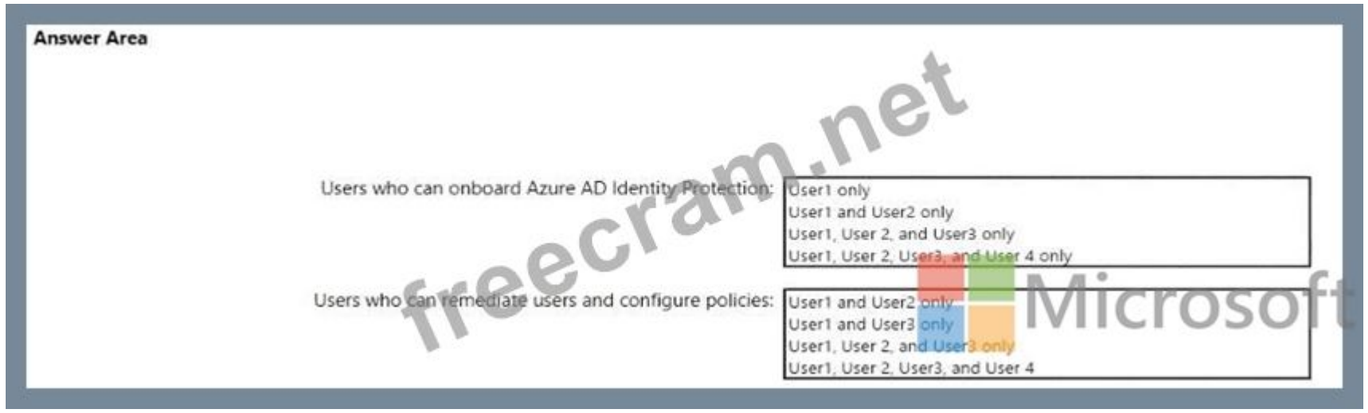
Explanation:

NEW QUESTION: 192
You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

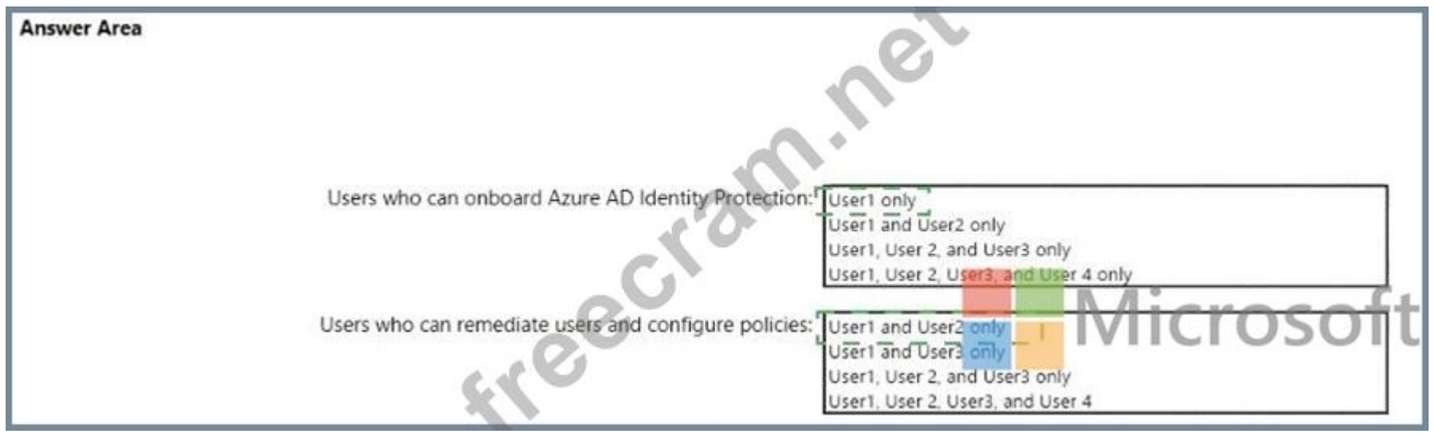
Name	Role
User1	Global administrator
User2	Security administrator
User3	Security reader
User4	License administrator

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

NOTE: Each correct selection is worth one point



Answer:



Explanation:

NEW QUESTION: 193

You have an Azure subscription.

You plan to implement Azure DDoS Protection. The solution must meet the following requirement:

* Provide access to DDoS rapid response support during active attacks.

* Project Basic SKU public IP addresses.

You need to recommend which type of DDoS projection to use for each requirement.

What should you recommend? To answer, drag the appropriate DDoS projection types to the correct requirements. Each DDoS Projection type may be used once, or not at all. You may need to drag the split bar between panes or scroll to view connect.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION: 194

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. Storage

B. Resource Manager

C. Servers

D. APIs

E. App Service

Answer: (SHOW ANSWER)

NEW QUESTION: 195

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

You have a network security group (NSG) named NSG1 that is associated to the network interface of VM1 and is configured as shown in the following exhibit

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
300	RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerI...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Just-in-time (JIT) VM access is enabled on VM1 and has the following configurations:

* Management ports: 3389, 22
* Maximum time range: 3 hours
* Allowed source IP addresses: Any

You activate the JIT rule and connect to VM1 by using SSH.

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

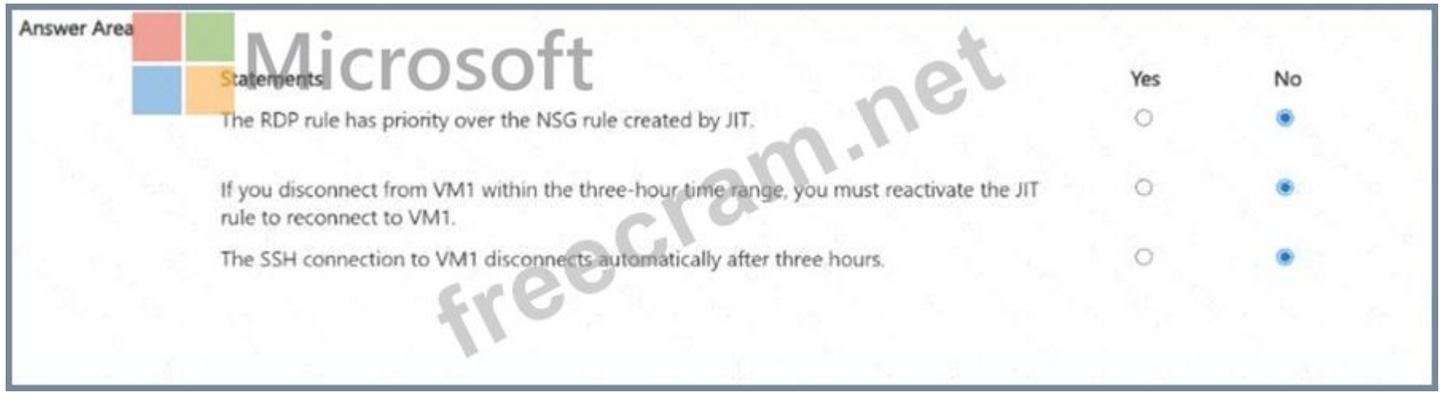
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
The RDP rule has priority over the NSG rule created by JIT.	○	○
If you disconnect from VM1 within the three-hour time range, you must reactivate the JIT rule to reconnect to VM1.	○	○
The SSH connection to VM1 disconnects automatically after three hours.	○	○

Answer:

Explanation:

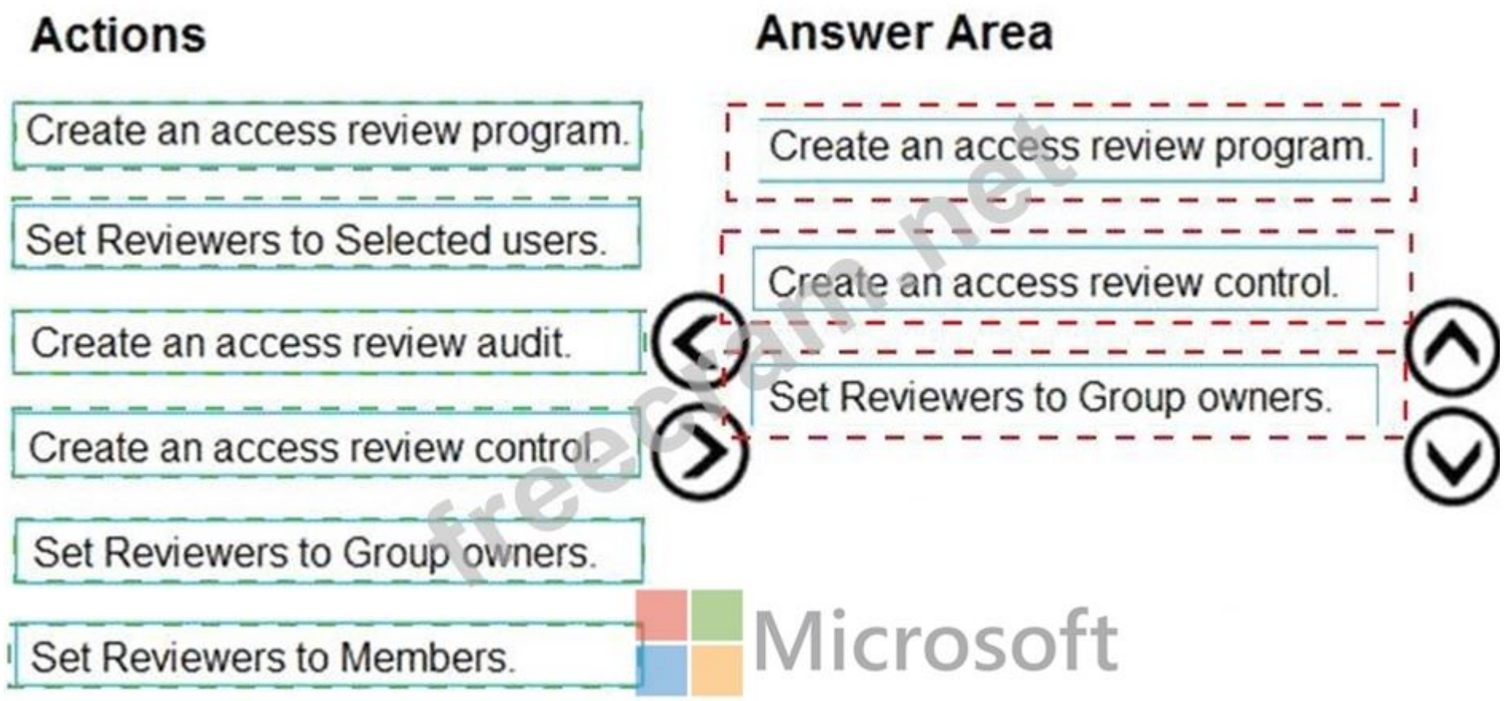


NEW QUESTION: 196

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 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
Topic 2, Contoso
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview
Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.
The company hosts its entire server infrastructure in Azure.
Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
Technical requirements
Contoso identifies the following technical requirements:
* Deploy Azure Firewall to VNetWork1 in Sub2.
* Register an application named App2 in contoso.com.
* Whenever possible, use the principle of least privilege.

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

Existing Environment

Azure AD

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

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

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

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

Sub1

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

User2 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

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

Sub1 contains the Azure policies shown in the following table.

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

Sub2

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

Sub2 contains the virtual machines shown in the following table.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Contoso identifies the following technical requirements:

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

NEW QUESTION: 198

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:

Explanation:

NEW QUESTION: 199

You have an Azure subscription that has a managed identity named identity and is linked to an Azure Active Directory (Azure AD) tenant. The tenant contains the resources shown in the following table.

Which resources can be added to AUI and AU2? To answer, select the appropriate options in the answer area.

Name	Type	Assigned object
AU1	Administrative unit	User1, Group1
AU2	Administrative unit	**None**
User1	User	**Not applicable**
Group1	Security group	**Not applicable**
Group2	Microsoft 365 group	**Not applicable**

Which resources can be added to AU1 and AU2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION: 200

You have a Microsoft Entra tenant.

You need to prevent nonprivileged Microsoft Entra users from creating service principals in Microsoft Entra ID.

A. From the Properties blade, set Enable Security defaults to Yes.

B. From the Properties blade, set Access management for Azure resources to No.

C. From the User settings blade, set Users can register applications to No.

D. From the User settings blade, set Restrict access to Microsoft Entra ID administration portal to Yes.

Answer: (SHOW ANSWER)

NEW QUESTION: 201

Your company has an Azure subscription named Subscription1. Subscription1 is associated with the Azure Active Directory tenant that includes the users shown in the following table.

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

The company is sold to a new owner.

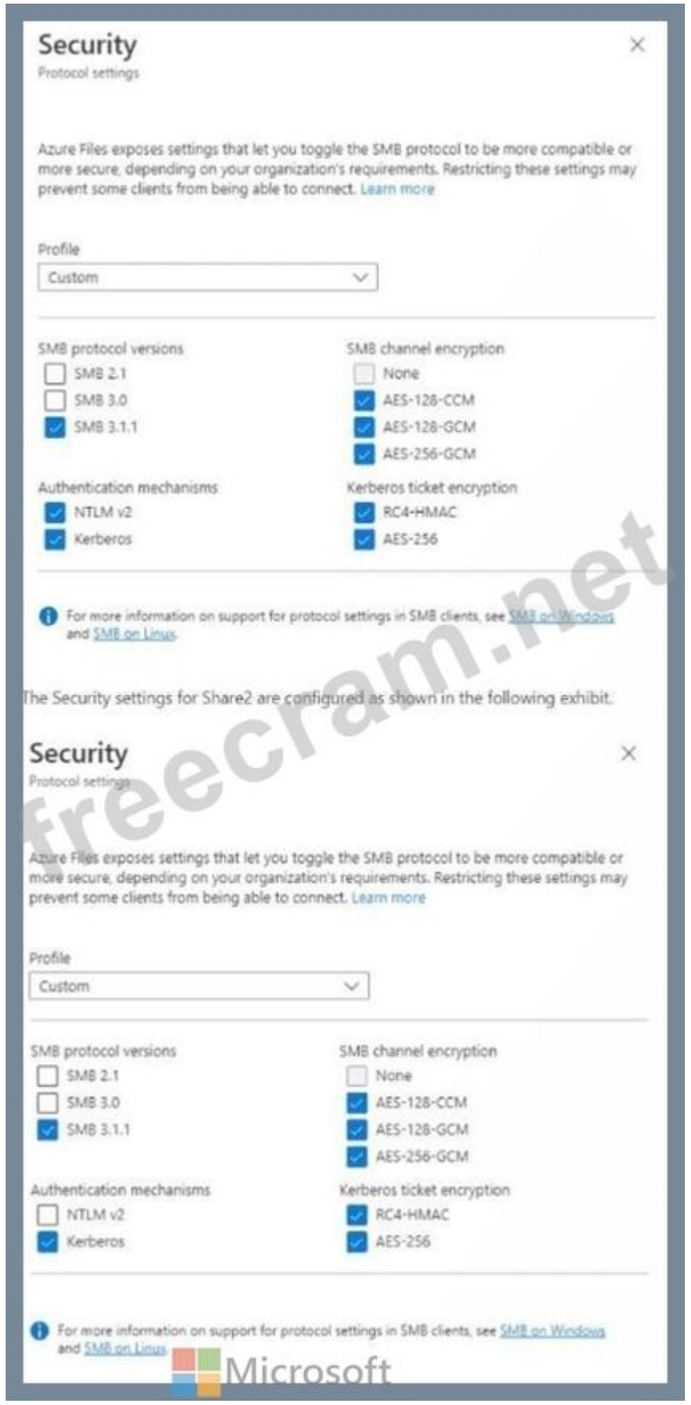
The company needs to transfer ownership of Subscription1.

Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:
Table Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer

NEW QUESTION: 202
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.



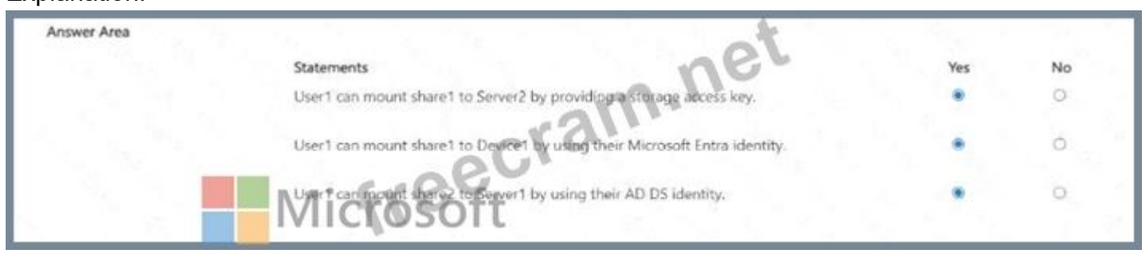
The Security settings for Share2 are configured as shown in the following exhibit.

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: 203

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

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

You need to ensure that App1 can read all user calendars and create appointments. The solution must use the principle of least privilege.

What should you do?

A. Add a new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.

B. Add a new Application API permission for Microsoft.Graph Calendars.ReadWrite.

C. Select Grant admin consent.

D. Add a new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.Shared.

Answer: (SHOW ANSWER)

Reference:

https://docs.microsoft.com/en-us/graph/permissions-reference#calendars-permissions

NEW QUESTION: 204

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

Name	Type	Resource group	Location
RG1	Resource group	**Not applicable**	West US
Managed1	Managed identity	RG1	West US

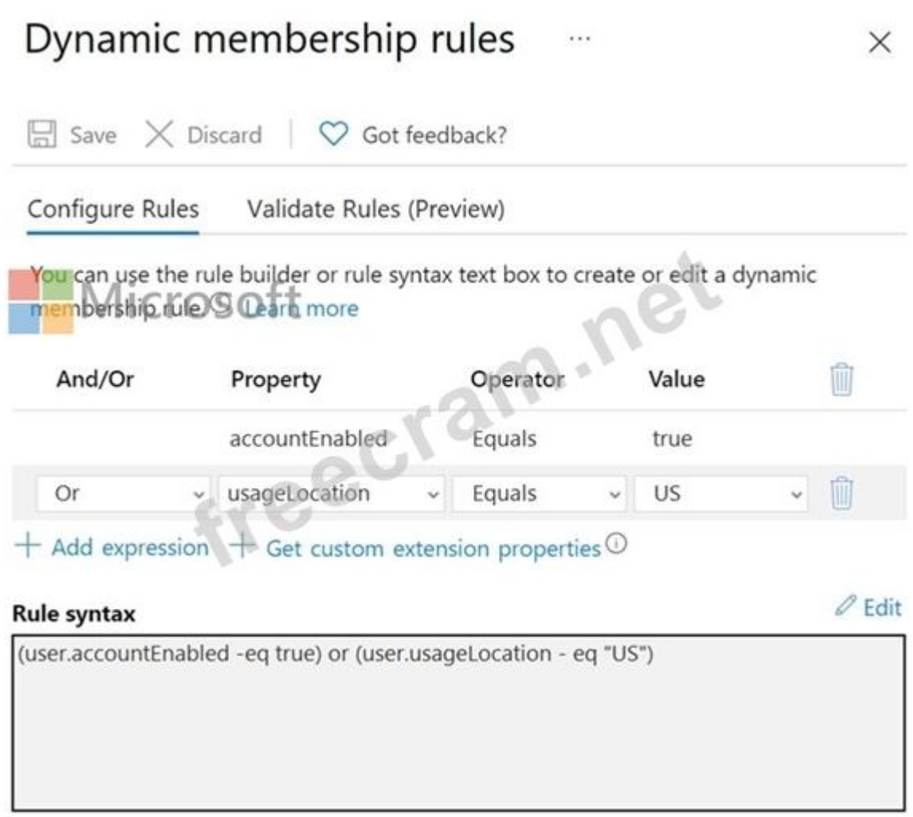
The subscription is linked to an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Usage location
User1	United States
User2	Germany

You create the groups shown in the following table.

Name	Type	Membership type
Group1	Security	Dynamic User
Group2	Microsoft 365	Dynamic User

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



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

Statements	Yes	No
User1 is a member of Group1 and Group2.	○	○
User2 is a member of Group2 only.	○	○
Managed1 is a member of Group1 and Group2.	○	○

Answer:

Statements	Yes	No
User1 is a member of Group1 and Group2.	○	○
User2 is a member of Group2 only.	○	○
Managed1 is a member of Group1 and Group2.	○	○

Explanation:

Text Description automatically generated

Statements	Yes	No
User1 is a member of Group1 and Group2.	○	○
User2 is a member of Group2 only.	○	○
Managed1 is a member of Group1 and Group2.	○	○

Reference:

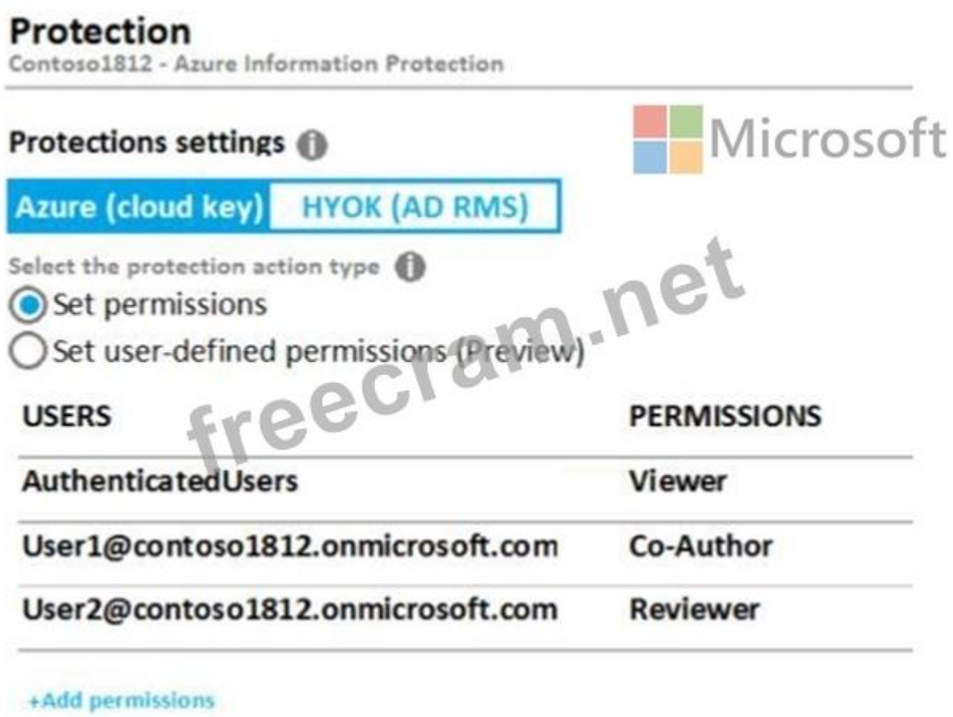
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership

NEW QUESTION: 205

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

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

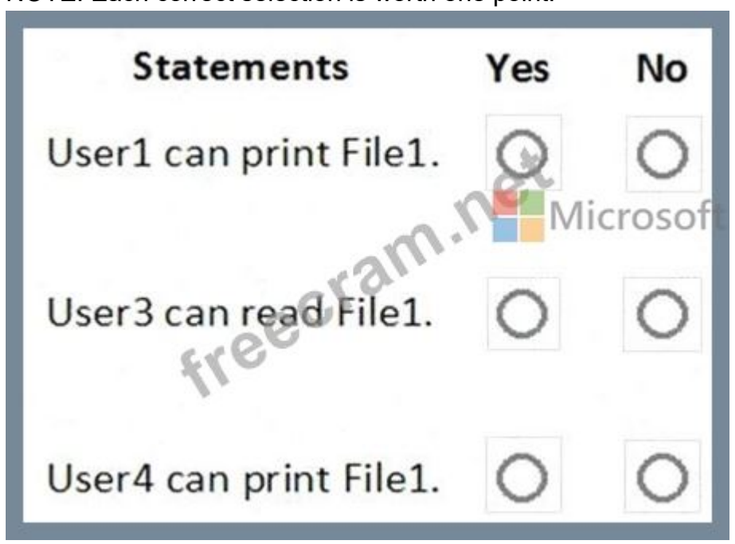
You create an Azure Information Protection label named Label1. The Protection settings for Label1 are configured as shown in the exhibit. (Click the Exhibit tab.)



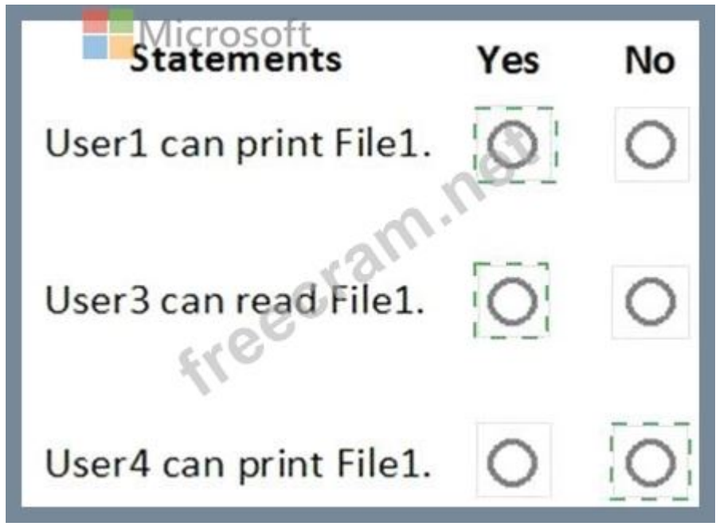
Label1 is applied to a file named File1.

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

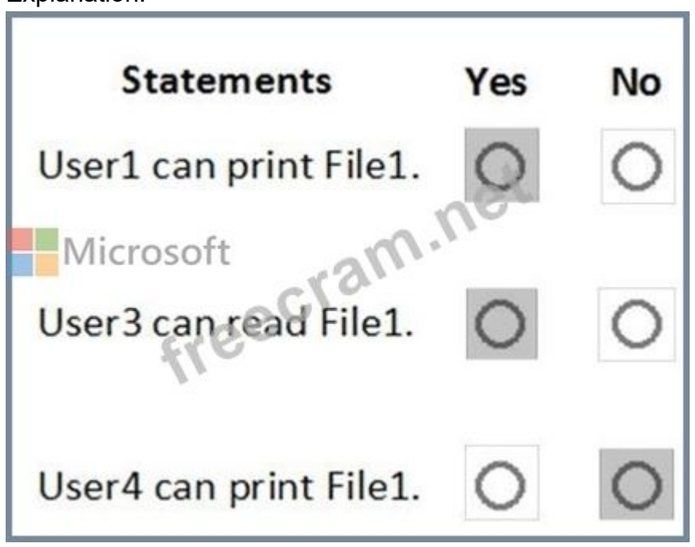
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 206

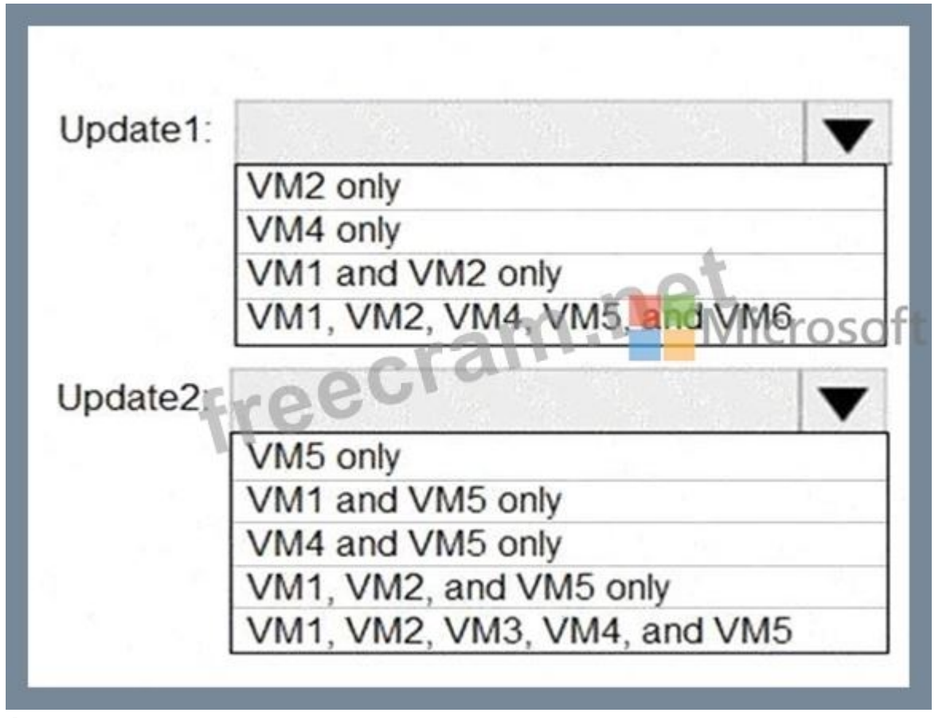
You have Azure virtual machines that have Update Management enabled. The virtual machines are configured as shown in the following table.

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

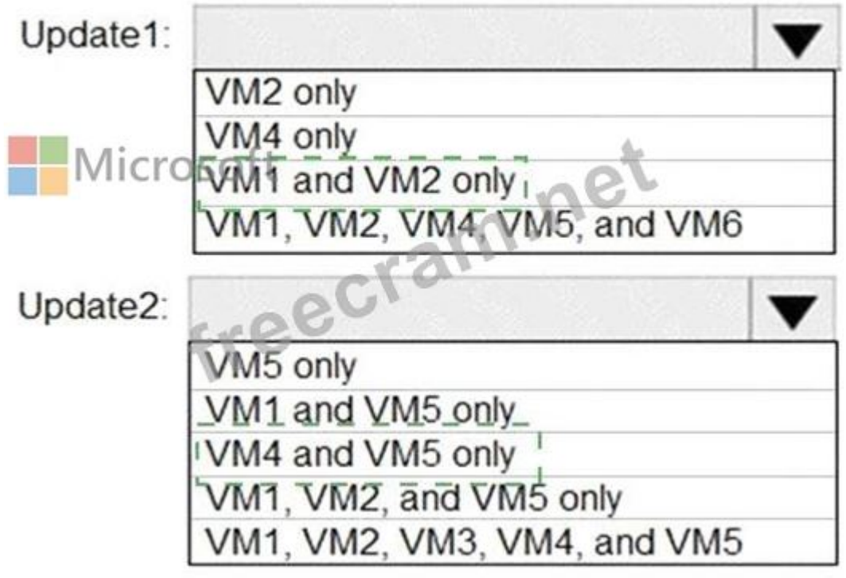
You schedule two update deployments named Update1 and Update2. Update1 updates VM3. Update2 updates VM6.

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

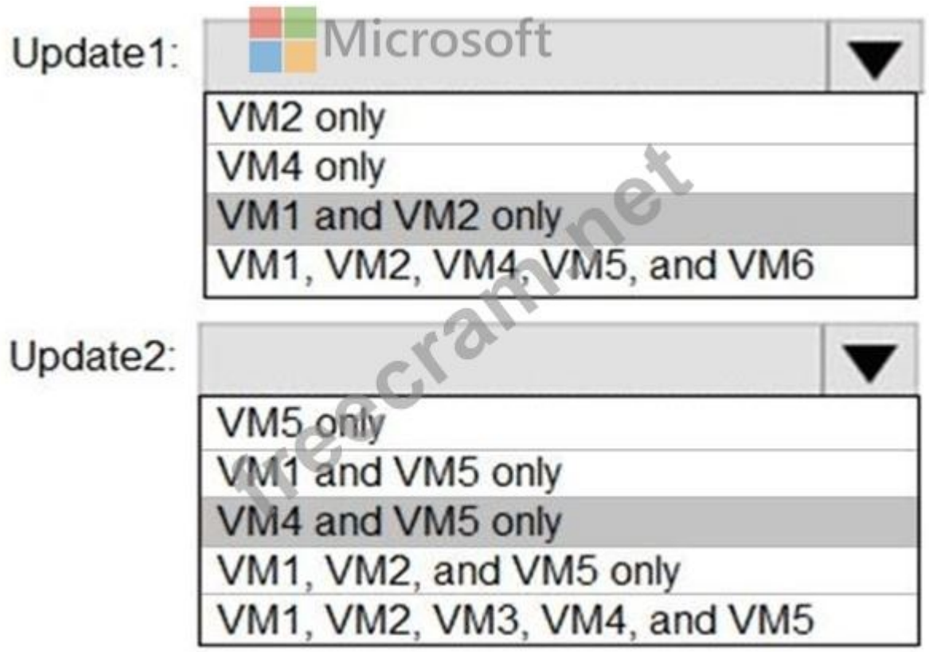
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



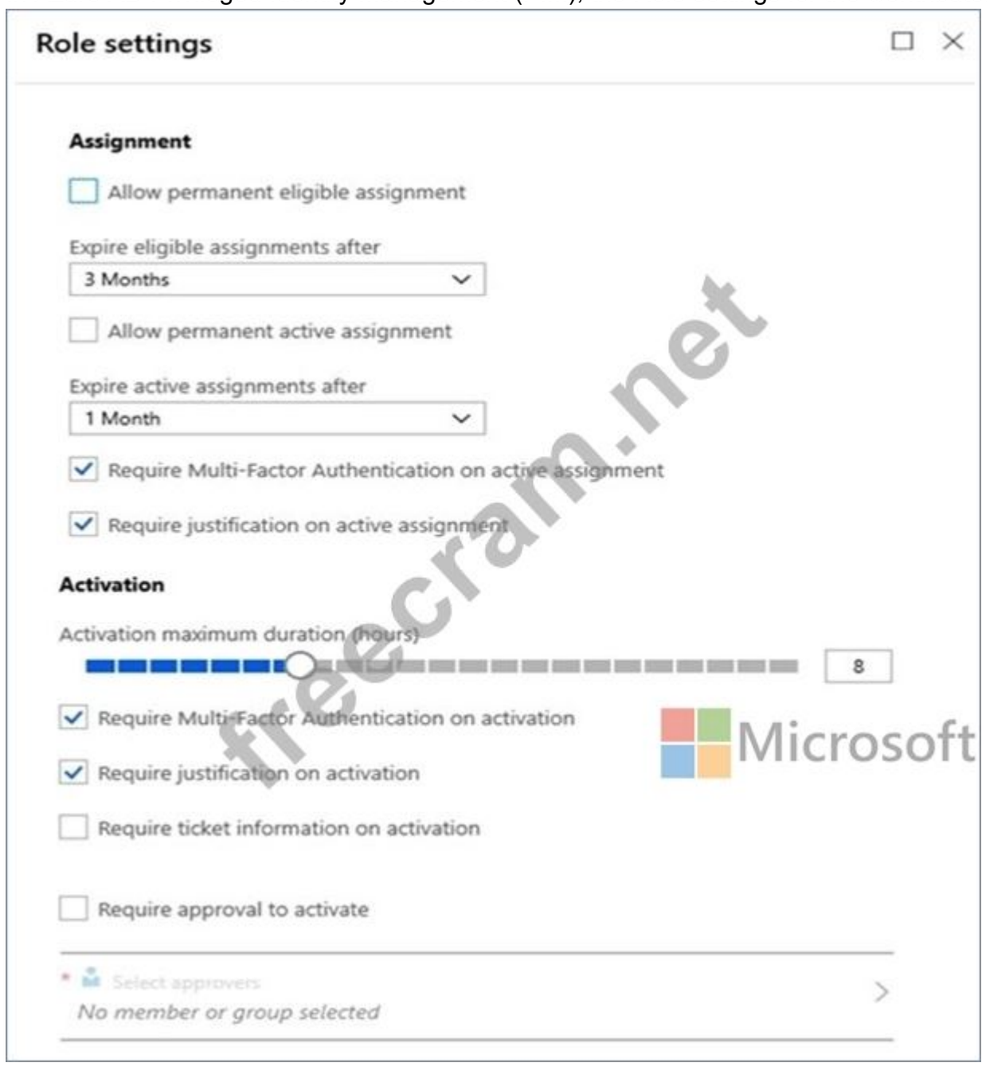
Update1: VM1 and VM2 only
VM3: Windows Server 2016 West US RG2
Update2: VM4 and VM5 only
VM6: CentOS 7.5 East US RG1
For Linux, the machine must have access to an update repository. The update repository can be private or public.
References:
https://docs.microsoft.com/en-us/azure/automation/automation-update-management

NEW QUESTION: 207
You have an Azure subscription that contains a SQL Server on Azure Virtual Machines instance named SQt1 and a Microsoft Sentinel workspace named Sentinel1.
You need to monitor security incidents on SQL1 by using Sentinel1.
What should you do first?
A. On SQL1, enable SQL1 Server audit.
B. From the Azure portal, create a Log Analytics workspace.
C. On SQL1. install the Connected Machine agent for Azure Arc-enabled servers.
D. From Sentinel1, enable VM insights.
Answer: (SHOW ANSWER)

NEW QUESTION: 208
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

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

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



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

Name	Assignment type
User1	Eligible
User2	Active
User3	Active

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

NOTE: Each correct selection is worth one point.

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

Answer:

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

Explanation:

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

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