Microsoft.AZ-500-KR.v2026-06-04.q213

□□□□:	AZ-500-KR
□□□□:	Microsoft Azure Security Technologies (AZ-500 Korean Version)
□□□:	Microsoft
□□ □□ □□□:	213
□□:	v2026-06-04
# □□ □:	162
# □□ □□□:	2130
https://www.krdump.com/Microsoft.AZ-500-KR.v2026-06-04.q213.html	

NEW QUESTION: 1
VNet1□□□ □□ □□□□□ □□□ Azure □□□ □□□□. VNet1□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

□□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.

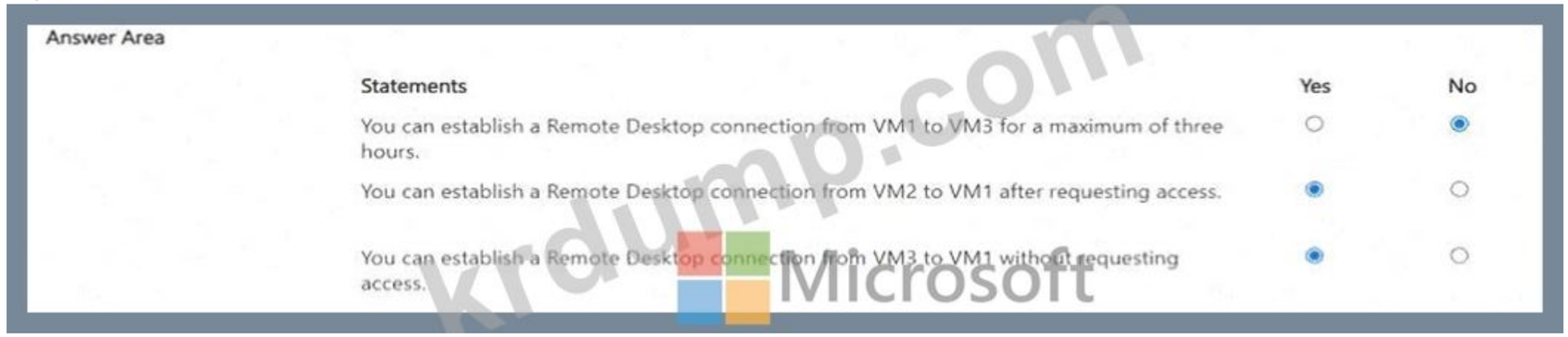
Name	Connected to
VM1	Subnet1
VM2	Subnet2
VM3	Subnet3

VM3□□ □□ 8080□□ □□□ □□□□ □□□□ □□□□ □□□□.
VM1□ □□ □□ □□□ □□ JIT(Just-In-Time) VM □□□□ □□□□□.

□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□□□: □□ 1□□ 1□□□□.

Answer:

Explanation:



NEW QUESTION: 2

contoso□□ Azure Active Directory(Azure AD) □□□□ □□□ Azure □□□ □□□□.

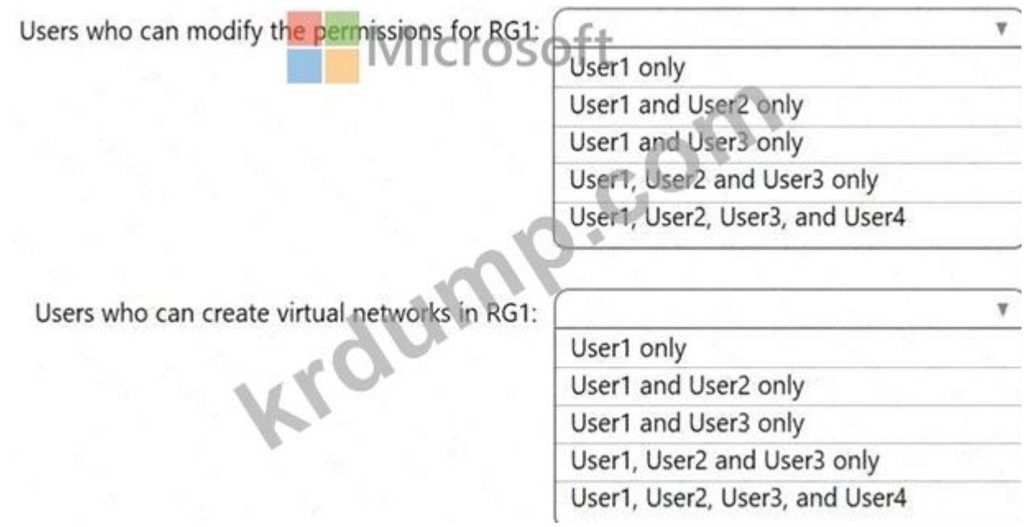
□□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

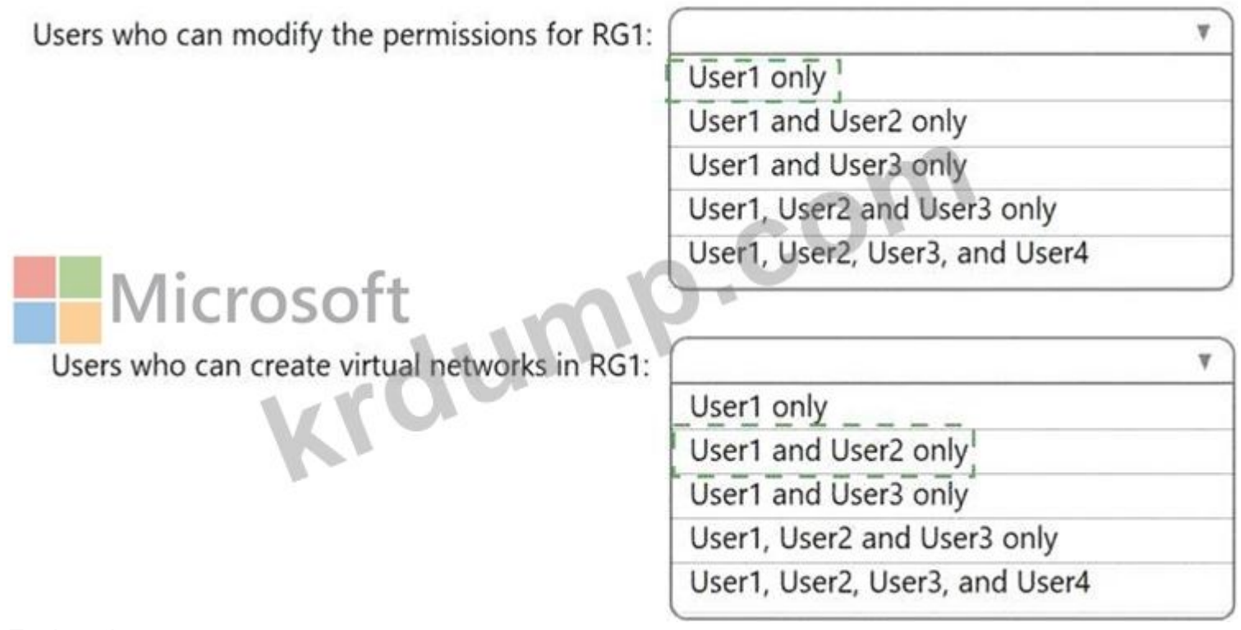
RG1□□□ □□□ □□□ □□□□.

RG1□ □□ □□□ □□□ □ □□ □□□□ □□□□, RG1□ □□ □□□□□ □□□ □ □□ □□□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

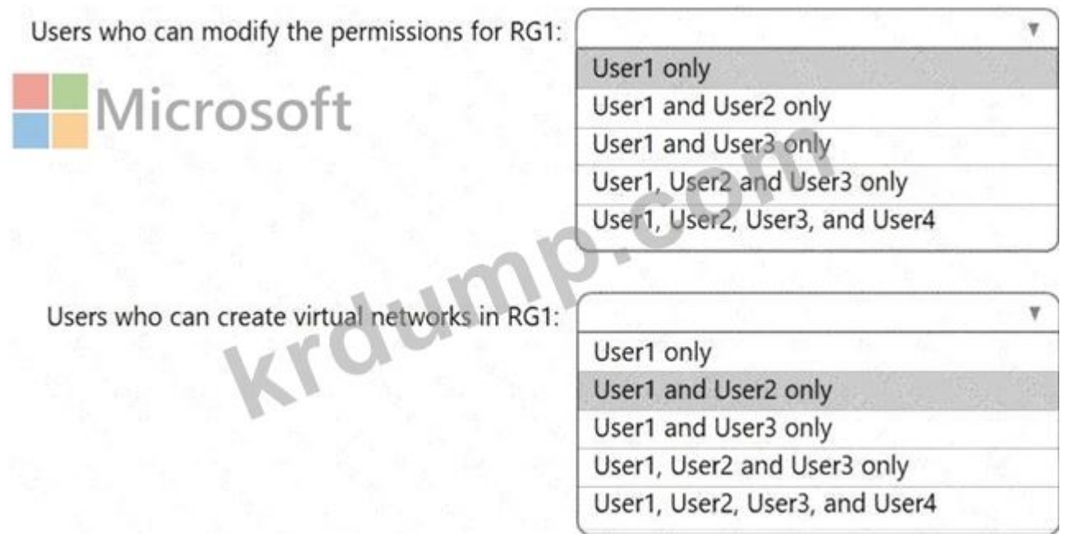
□□: □□ 1□□ 1□□□□.



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: 3

□□□□□ contoso.com□□□ Active Directory □□□□□ □□□□. contoso.com□□□ Azure □□□□(Azure AD) □□□□ □□□□.

Azure AD Connect□ Express □□ □□ □□□ □□□□ □□□□ □□□□□ □□□.

□□□ □□□ □□□□ □ □□□ □□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

□□ □ □□ □□□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.

□□: □□ 1□□ 1□□□□.

A. Active Directory□ □□□ □□□ □□

B. Azure AD□ □□ □□□ □□

C. Azure AD□ □□□ □□□ □□

D. Azure AD□ □□□ □□□ □□

E. Active Directory□ Enterprise Admins □□

Answer: C,E (LEAVE A REPLY)

References:

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

NEW QUESTION: 4

User2□ PIM□ □□□ □ □□□ □□□□ □□□.

□□ □□ □□□ □□ □□□?

A. User2□□ □□□ □□□ □□□ □□□□□.

B. contoso.com□ □□ □□ □□□ □□□□□.

C. contoso.com□ □□ ID □□ □□□ □□□□□.

D. User2□ □□ □□ □□ □□(MFA)□ □□□□□□.

Answer: D (LEAVE A REPLY)

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

1. Sign in to the Azure portal as a Global Administrator of your directory.
You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.
Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com References:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting- started
Topic 3, Fabrikam inc
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
General Overview
Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.
Existing Environment
Network Environment
Fabrikam has a Microsoft 365 subscription and an Azure subscription named subscription1.
The network contains an on-premises Active Directory domain named Fabrikam.com. The domain contains two organizational units (OUs) named OU1 and OU2. Azure AD Connect cloud sync syncs only OU1.
The Azure resources hierarchy is shown in the following exhibit.

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

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

Azure AD contains the resources shown in the following table.

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

Subscription1 Resources

Subscription1 contains the virtual networks shown in the following table.

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

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

Name	Location
NSG2	West US
NSG3	Central US
NSG4	West US

Subscription1 contains the virtual machines shown in the following table.

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

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

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

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

Planned Changes and Requirements

Planned Changes

Fabrikam plans to implement the following changes:

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

Name	Location
ASG1	West US
ASG2	Central US

* Associate the network interface of VM1 to ASG1.
* Deploy SecPol1 by using Azure Security Center.
* Deploy a third-party app named App1. A version of App1 exists for all available operating systems.
* Create a resource group named RG2.
* Sync OU2 to Azure AD.
* Add User1 to Group1.

Technical Requirements

Fabrikam identifies the following technical requirements:

* The finance department users must reauthenticate after three hours when they access SharePoint Online.
* Storage1 must be encrypted by using customer-managed keys and automatic key rotation.
* From Sentinel1, you must ensure that the following notebooks can be launched:
* Entity Explorer - Account
* Entity Explorer - Windows Host
* Guided Investigation Process Alerts

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

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

App1 must use a secure connection string stored in KeyVault1.
KeyVault1 traffic must NOT travel over the internet.

NEW QUESTION: 5
Azure □□□ □□□□ MG1□□□ □□ □□□ RG1□□□ □□□ □□□ □□□□. RG1□□ VM1□□□ □□ □□□ □□□□. □□ □□ □□ □□ □□□ □□ Azure □□□ □□□□.

Name	Scoped to
Role1	MG1
Role2	RG1

Role1□ □□ □□□ □□ □□ □□ □□□ □□□□□.

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

□□ □□ □□□ □□□□□ □□□ □□□□□.

Name	Role
User1	Role1
User2	Role1, Role2
User3	Role2

□□ □ □□□ □□, □□□ □□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□. □□: □□□ 1□□□□.

Answer Area

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

Answer:

Explanation:

NEW QUESTION: 6

□□□ □□

□□ 7

Homepage-AGW□□ Azure Application Gateway□ □□ □□□ □□ □□□ □□ □□□□□ □□□□ □□□.

Answer:

see the task answer with step by step below:

* Enable Web Application Firewall (WAF) for the application gateway. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select a WAF policy and a WAF mode for the application gateway. You can choose a predefined policy or create a custom policy with your own rules and exclusions.
* Configure WAF policy settings. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select the managed rulesets and rule groups that you want to enable or disable for the WAF policy. You can also configure custom rules to match specific patterns or conditions and take actions such as blocking or logging requests.
* Monitor WAF logs. You can use different types of logs in Azure to manage and troubleshoot the application gateway and the WAF policy. You can access some of these logs through the portal, such as metrics and health probes. You can also export the logs to Azure Storage, Event Hubs, or Log Analytics and view them in different tools, such as Azure Monitor, Excel, or Power BI.

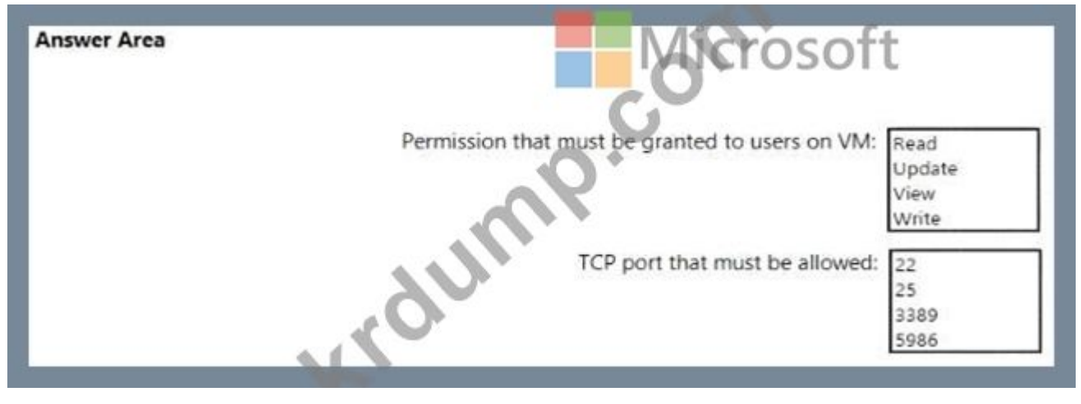
NEW QUESTION: 7

Azure □□ □□ □□□ □□ JIT(Just-in-Time) VM □□□□ □□□□ □□□□.

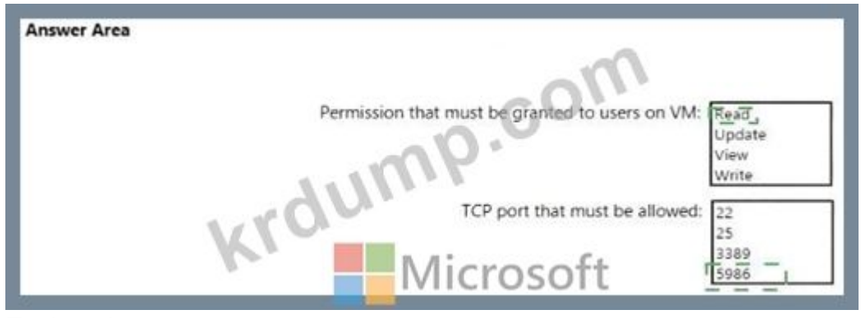
JIT VM □□□□ □□□□ □□□□□ □□ □□□ □□ PowerShell □□□ □□□ □□□□ □□□.

□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ 1□□ 1□□□□.



Answer:



Explanation:

1. Read permission

2. 5986

https://docs.microsoft.com/en-us/azure/security-center/just-in-time-explained#what-permissions-are-needed- to-configure-and-use-jit

NEW QUESTION: 8

Vault1□□□ Azure Key Vault□ VM1□□□ □□ □□□ □□□ Azure □□□ □□□□.

VM1□ VNet1□□□ □□ □□□□□ □□□□□.

VM1□□□ Vault1□ □□ □□□□ □□□□ □□□.

Vault1□ □□□□ □□□□ □□□ □□ □□□?

A. □□ □□□□□ □□ □□□ VM1□ □□ □□ □□□□□□ □□□□.

B. □□□ □ □□ □□□□ □□□ VM1□ IP □□□ □□□□□.

C. □□□ □ □□ □□□□ □□□ VNet1□ □□□□□.

D. □□□ □ □□ □□□□ □□□ Vault1□ □□ □□□ □ □□ Microsoft □□□□ □ □□□□ □□□□□ □□□ □□ □□□□□.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 9

□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

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

ServerAdmins□ □□ □□□ □□□ □ □□□ □□□□ □□□.

RG2□ □□ □□ □□□□□□ □□ □□□ □□□□□.

□□□□ □□ □□□ □□□ □□□□ □□□.

ServerAdmins□□ □□ □ □□ □□ □□ □□□ □□(RBAC) □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.

□□: □□ 1□□ 1□□□□.

A. □□□ □□ □□□ □□

B. RG2□ □□□□ □□□ □□

C. RG1□ □□ □□ □□□ □□□□□.

D. RG2□ □□□ □□ RBAC □□

E. RG1□ □□□□ □□□ □□.

F. □□□ □□ □□□ □□ RBAC □□

Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 10
□□□□□ □ □□□□ □□□ □□□ □□ □□□□□. □ □□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□□.
□ □□□ □□□ □□ □□□ □□□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. Azure □□ □□
B. Azure □□
C. Azure AD □□ □□ ID □□(PIM)
D. Azure □□□
Answer: (SHOW ANSWER)
Just as a blueprint allows an engineer or an architect to sketch a project ' s design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization ' s standards, patterns, and requirements.
Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:
* Role Assignments
* Policy Assignments
* Azure Resource Manager templates
* Resource Groups
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

NEW QUESTION: 11
ContReg1□□□ Azure Container Registry□ □□□, □□□□ image1□□□ □□□ □□□□ □□□□ □□□□ □□□□.
ContReg1□ □□ □□□ □□□ □□□□□□.
□□□ □□□ □□□□ □ □□ □□ □□□ □□ □ □□ □□□□ ContReg1□ □□□□□.

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

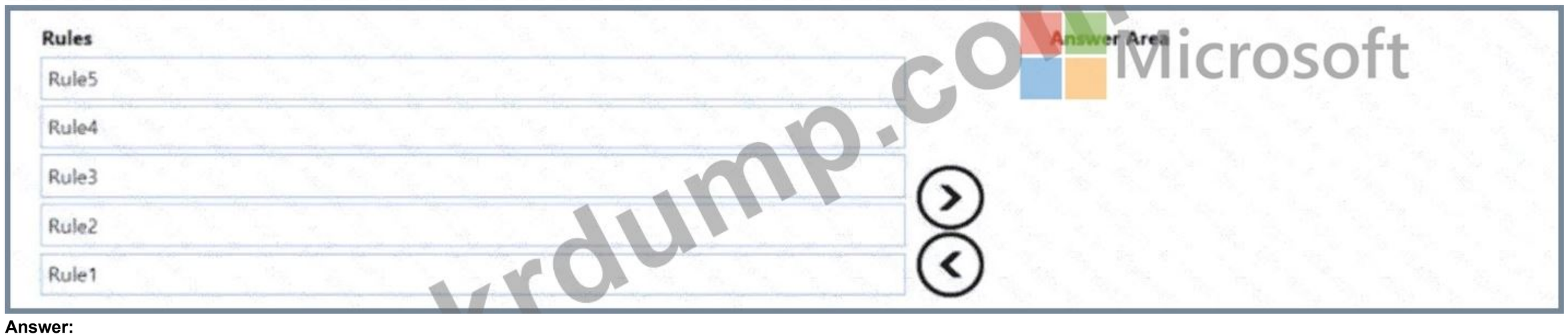
□□ □□□□ □□□ □ □□ □□□□□□?
A. image1□ image2□
B. image2□
C. image1, image2, image3
Answer: B (LEAVE A REPLY)
Azure Container Registry implements Docker ' s content trust model, enabling pushing and pulling of signed images.
To push a trusted image tag to your container registry, enable content trust and 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: 12
□□□□□□ □□□□□ Active Directory □□□ □□□(AD DS) □□□□ □□□□ □□□□. □□ □□ □□□□ □□□□□ Microsoft Entra □□□□ □□□□.
App1□□□ □□□□ □ □□□ □□□□□.
App1□ □□□ □□ □□ □□□ □□□□ □□□□□ □□□□ □□ □□ objectID □□□ □□□□□ □□□□ □□□.
□□ □□□ □□□□ □□□?
A. □□ □ □□□
B. □ □□
C. □□ □□
D. □□□ □ □□
Answer: (SHOW ANSWER)

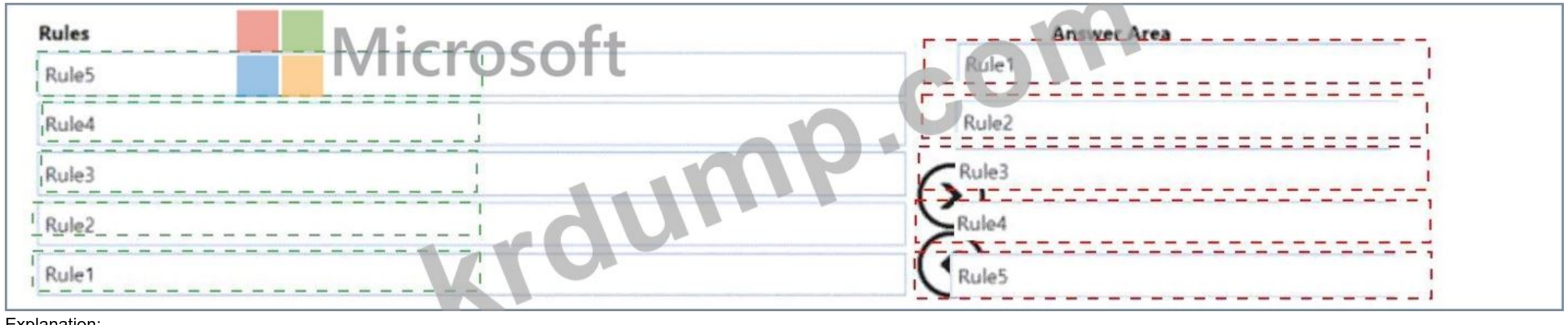
NEW QUESTION: 13
Azure □□□ □□□□.
□□ □□ □□□ □□□ □□□ Azure □□□ □□□ □□□□.

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

□□□ □□ □□□ □□□□ □□□? □□□□ □□ □□□ □□ □□ □□□ □□ □□□□ □□□ □□□ □□□□ □□□□□.



Answer:



Explanation:

The rules should be processed in the following order:

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

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

NEW QUESTION: 14

Sub1□□□ Azure □□□ □□□□.

Azure Security Center□□ WF1□□□ □□□□ □□□□ □□□□. WF1□ User1□□□ □□□□□ □□□ □□□□ □□□□ □□□□ □□□□.

Alerts□□ □□□ □□ □□□ □□□ □□□□ □□□□ WF1□ □□□□ □□□.

WF1□ □□□□□ □□□ □□□□ □□□?

A. Azure □□□□□□ □□□□

B. Azure □□□

C. Azure Logic Apps □□□□

D. Azure DevOps

Answer: (SHOW ANSWER)

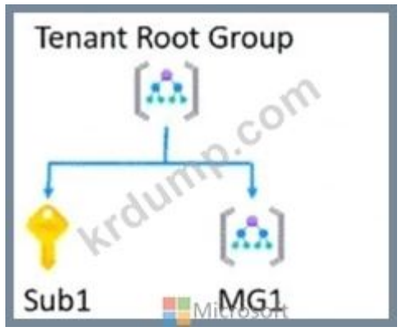
Reference:

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

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

NEW QUESTION: 15

Microsoft Defender for Cloud□ □□□□ Sub1□□□ Azure □□□ □□□□. □□ □□□ □□ □□ □□ □□ □□□ □□□□.



□□ □□ □□□ □□□ □□□□□.

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

□□ □□□ □□□□□ Defender for Cloud□ □□□□ □□□. □□ □□□ □□ □□□□ □□□ □ □□□?

A. □□1, □□□□□1, □□□□□2, □□□□□3

B. □□1 □ □□□□□1□

C. Initiative1, Initiative2 □ Initiatives□

D. □□1□

E. Initiative1 □ Initiative2□

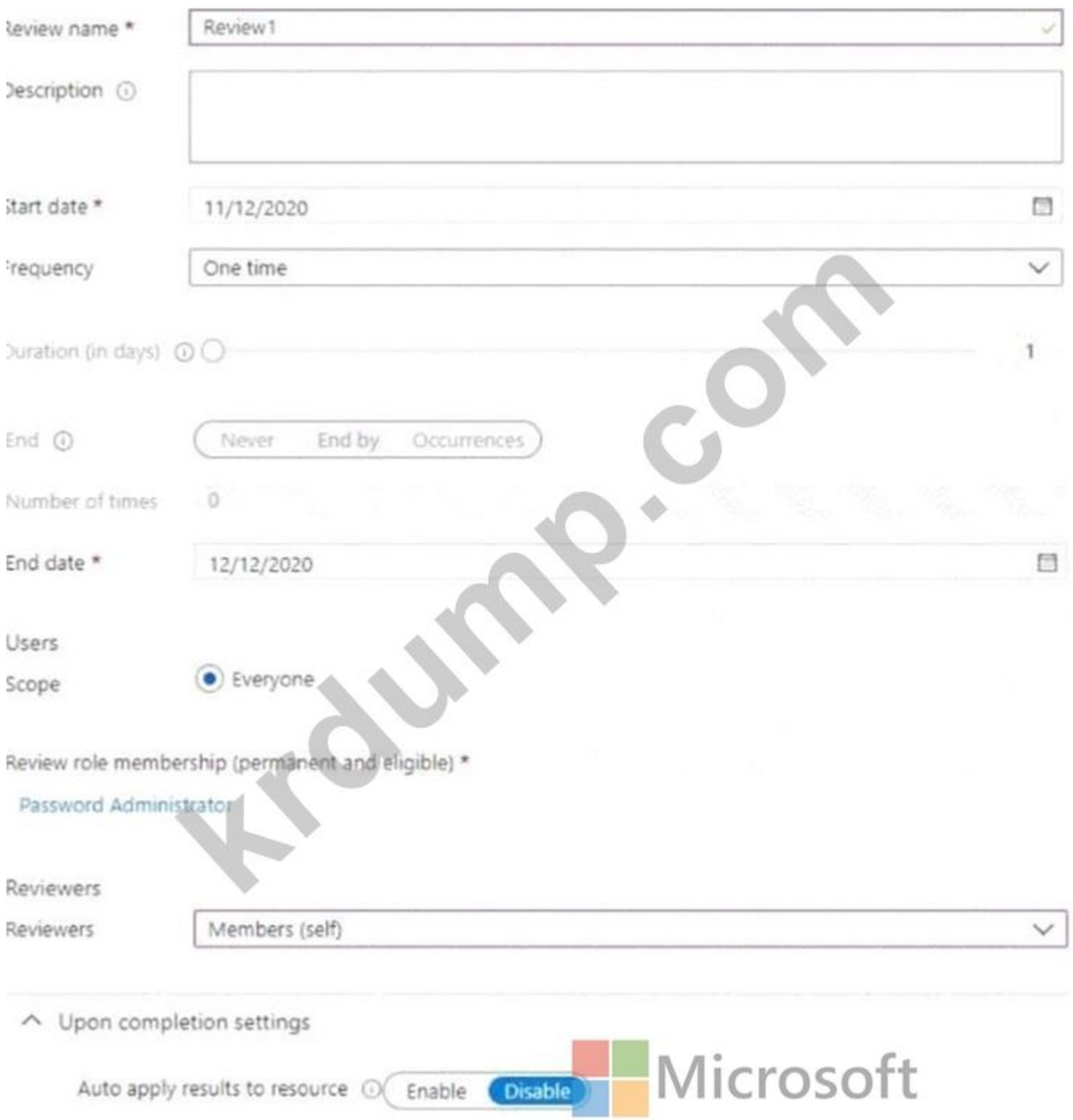
Answer: B (LEAVE A REPLY)

NEW QUESTION: 16

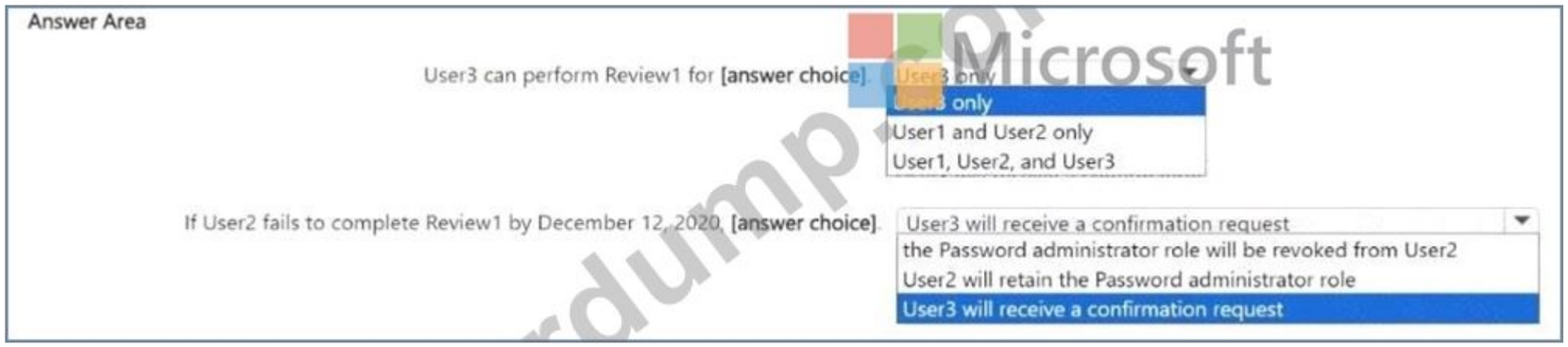
contoso.com□□□ Microsoft Entra □□□□ □□□□. □ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

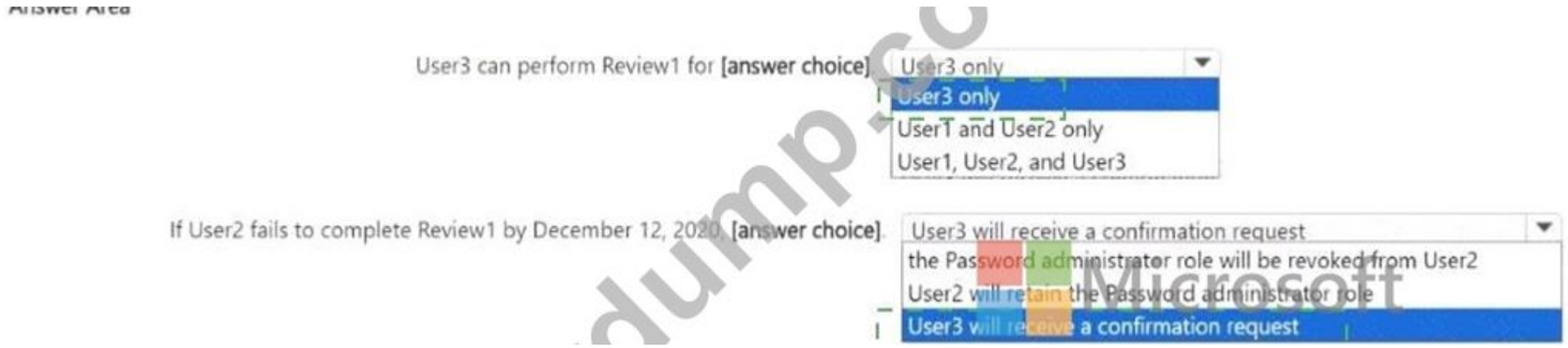
□□ □□ □□□ □□□ Review1□□□ □□□ □□□ □□□ □□□□□. □□ □□□ MM/DD/YYYY □□□□□.


Review name *
Review1
Description
Start date *
11/12/2020
Frequency
One time
Duration (in days)
1
End
Never
End by
Occurrences
Number of times
0
End date *
12/12/2020
Users
Scope
Everyone
Review role membership (permanent and eligible) *
Password Administrator
Reviewers
Reviewers
Members (self)
Upon completion settings
Auto apply results to resource
Enable
Disable

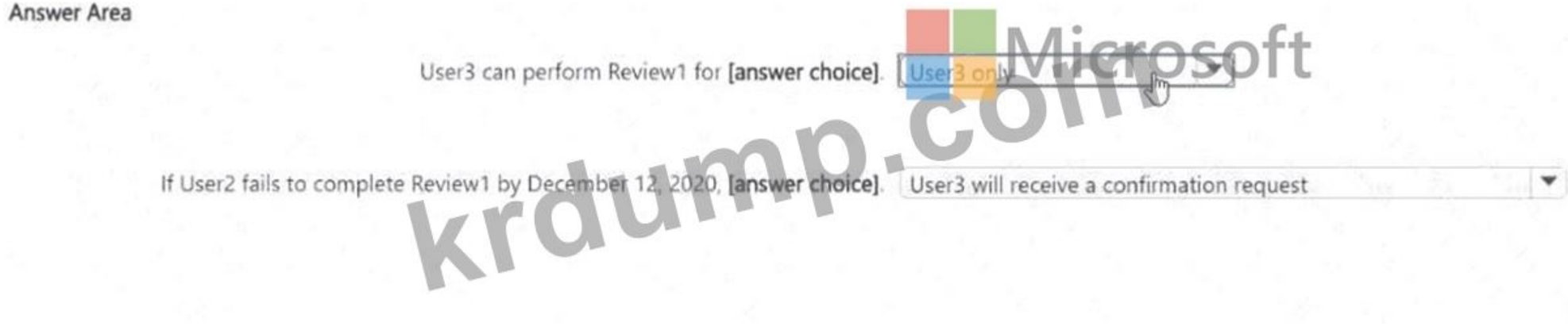
□□□□ □□□ □□□ □□□□ □ □□□ □□□□ □□ □□□ □□□□□ □□□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 17

□□ □□□□ □□ □□□□ □□ □□(NSG)□ □□ 10□□ □□ □□□ □□□□.

Azure Storage □□□ □□□□ □□□□ □□□□ □□□.

□□ □ □□ □□□ □□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.
A. □□□□ □□ □□□ □□□□ □□□□□.
B. Azure Network Watcher□ □□□□□□.
C. NSG□ □□ □□ □□□ □□□□□□.
D. NSG □□ □□□ □□□□□□.
E. Azure Log Analytics □□ □□□ □□□□.
Answer: (SHOW ANSWER)
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: 18
WAF1□ □□ □□□ □□ □□□ □□□□ □□□.
□□□□ □□ □□□ □□□□□ □□□.
□□□ □□ □□□?
A. Azure □□□ □□□□.
B. Bot Manager 1.1 □□ □□□ □□□□□.
C. □□□ □□ □□□ □□□□□.
D. Azure□□ □□□□ DRS□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 19
□□ □□ Azure □□ □□□ □□ □□□□.

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

□□ □□ □□□ RG1□ Analytics1□□□ Azure Log Analytics □□ □□□ □□□□.
Analytics1□ □□□ □ □□ □□ □□□ □□□□□?
A. VM1□
B. VM1, VM2 □ VM3□ □□

C. VM1, VM2, VM3 □ VM4
D. VM1 □ VM4□ □□
Answer: C (LEAVE A REPLY)
Note: Create a workspace
* In the Azure portal, click All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics.
* Click Create, and then select choices for the following items:
Provide a name for the new Log Analytics workspace, such as DefaultLAWorkspace. OMS workspaces are now referred to as Log Analytics workspaces.
Select a Subscription to link to by selecting from the drop-down list if the default selected is not appropriate.
For Resource Group, select an existing resource group that contains one or more Azure virtual machines.
Select the Location your VMs are deployed to. For additional information, see which regions Log Analytics is available in.
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-access

NEW QUESTION: 20
□□ □□ □□□ □□□□ □□□ contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□□□.

Name	Role
Admin1	Global administrator
Admin2	Group administrator
Admin3	User administrator

Contoso.com□□ □□ □□ □□□ □□□□ □□□□. □ □□□□ 'Contoso'□□ □□□ □□□□ □□□ □□ □□ □□ □□ □□□ □□□□.
contoso.com□□ Contoso Sales□□ □□□ □□ □ □□ □□□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.

Users who can create a security group named Contoso Sales:
- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3

Users who can create an Office 365 group named Contoso Sales:
- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3

Answer:

Explanation:

Reference:

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

NEW QUESTION: 21

□□ □□ □□ □□ □□□□ □□□ Subscription1□□□ Azure □□□ □□□□.

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

Azure Security Center□ □□□□ Subscription1□ □□□ □ □□ □□□□□□ □□□ □□□□ □□□.

□□□ □□□□ □□□?

A. Policy1 □ Policy2□

B. □□□□□1□

C. Initiative1 □ Initiative2□

D. □□□□□1, □□□□□2, □□1, □□2

Answer: D (LEAVE A REPLY)

Reference:

https://docs.microsoft.com/en-us/azure/security-center/custom-security-policies

NEW QUESTION: 22
Azure □□□ □□□□.
VM1□□□ □□ □□□ □□□ □□□□□.
VM1□□ □□ □□□ □□□□ □□□□ □□□.
VM1□ □□ □□ □□ □□□□ □□□□ □□, □□ □□□ □□□□ □□□□ □□□□ □ □□ □□□ □□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 23
WebApp1□□□ Azure App Services □□□ □□□ Azure □□□ □□□□. WebApp1□ □□ Azure □□□ □□□□ □□□□□□.
WebApp1□ □□ □□□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* □□□□ □ □□□□□□□ □□□□□.

* □□□ □□□ □□□ □□□ □□□□□□.
□□□ □□□□ □□□?
A. Azure □□□□□□ □□□□□
B. Azure □□□ □□ □□□□(CDN)
C. Azure □□□
D. Azure Front Door □□□□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 24
Azure □□□□ Vault1□□□ Azure Key Vault□ □□□□ □□□□. Vault1□ key1□□□ 2048□□ RSA □□ □□□□□□.
key1□ 90□□□ □□□□□ □□ □□□.
□□ □□ □□□ □□ □□□?
A. □ □□ □□□ □□□□□.
B. Vault1□ Key Vault Premium□□ □□□□□□□□.
C. Vault1□ □□□ □□ □□□ □□□□□.
D. key1□ EC □□ □□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 25
□□ □□□ □□□ Azure □□□ □□□□.
□□ □□ □□□ □□ JIT(Just-In-Time) VM □□□□ □□□□□□.
□□ □□□□□ □□□□ □□ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. Azure Directory(Azure AD) Privileged Identity Management(PIM)□□ □□ □□□ □□□ □□□ □□□□□□.
B. Azure Active Directory(Azure AD) Privileged Identity Management(PIM)□□ □□ □□□ □□□ □□□ □□□□□□.
C. Azure Portal□□ □□ □□□ □□□□ □□□ □□□ □□ □□□ □□□ □□□□□.
D. Azure Portal□□ □□ □□□ □□□□ Network Watcher Agent □□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/connect-logon

NEW QUESTION: 26
□□: □ □□□□ □□□ □□□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□. □ □□□ □□ □□□ □□ □□□ □□□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□ □ □□□.
□□□ □□ □ □ □□□ □□ □□□ □□□ □ □□□□. □□ □□□ □□ □ □ □□□□ □□□ □□□□ □□ □□ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

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

□□ □□ □□□□ □□ □□□□.

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

SQL1□□□ □□□ Azure SQL □□ □□□□□ □□□ Microsoft Entra □□ □□□ □□□□□□.
User1□ User2□ □□ SQL1□ □□ Microsoft Entra □□□□ □□□□ □□□ □□□□ □□□.
□□ □□: App1□ SQL1□ Microsoft Entra □□□□ □□□□□.
□□□ □□□ □□□□□?

A. □□□

B. □

Answer: A (LEAVE A REPLY)

NEW QUESTION: 27

Microsoft Defender for Cloud□ □□ □□□ □□ □□ □□□□□□ □□□ □□□□□.
□□ □□□ □□ □□ □□□ □□□ □□□□ □□□.
□□ □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.

Answer Area

Answer:

Explanation:

A screenshot of a computer Description automatically generated

Answer Area

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

NEW QUESTION: 28
Defender for Cloud□ □□ □□□ □□ □□□ □□□□ □□ □□□□ □□□□ □□□.
□□□□ □□ □□□ □□□ □□□ □□□.
□□ □□□□ □□□□ □□□?
A. □□□3
B. □□□4
C. □□□1
D. □□□2
Answer: D (LEAVE A REPLY)

NEW QUESTION: 29

□□ □□ Azure □□□ DB1□□□ Azure SQL □□□□□□□ □□□ Azure □□□ □□□□. □□ □□ □□ □□ □□□ □□□ □□□□.

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

DB1□ □□ □□□ □□□□ □□□□□.

DB1□ □□ □□□□ □□ □□□□ □□□ □□□ □ □□□?

A. Storage2 □ storage3□

B. storage1 □ storage4□

C. storage1□

D. storage1, storage2 □ storage3□

Answer: A (LEAVE A REPLY)

NEW QUESTION: 30

□□□ □□□□ □□□ □□ □□□ □□□□ □□□.

□□ CAPolicy1 □□□ □□□□ □□□?

A. □□□□ □ □□ □□

B. □□

C. □□□

D. □□

Answer: D (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 31

contoso.com□□□ Azure AD □□□□ □□□ Sub 1□□□ Azure □□□ □□□□.

□□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

□ □□□□□ Azure AD Premium P2 □□□□□ □□□□□.

Azure AD Identity Protection□ □□□□□ □□□ □□□□□.

□□ □□□□ Azure AD Identity Protection□ □□□□□, □□□□ □□□□, □□□ □□□ □ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ 1□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 32

□ □□ □□ □□□ Azure SQL Server□ □□□ Azure □□□ □□□□.T DE(□□ □□□ □□□)□ □□ □□ □□
□□□□ Azure SQL □□□□□□□ □□□□ □□□ .
□□□□□□□ □□□□ □□ □□□ □□□□ □□□?

A. □ □□
B. SQL □□ □□□ □□□ □□□ □□□ □□
C. □□□□ □□□ □□ ID
D. □□ □□ □□ v2 □□□□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 33
□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

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

□□ □□ □□□ Azure Storage □□□ □□□□.

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

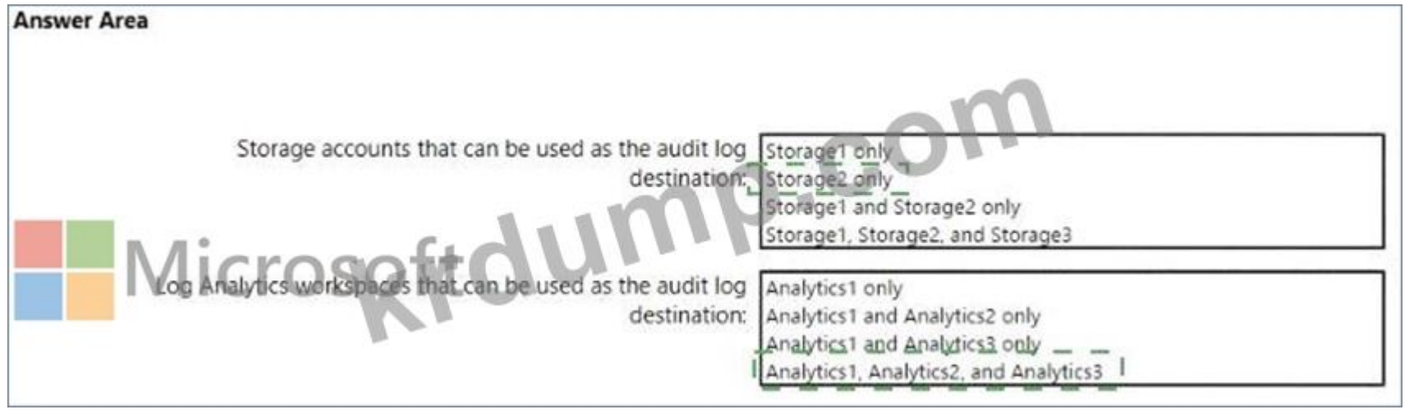
SQL1□ □□ □□□ □□□□ □□□.
□□ □□ □□□□ □□□ □ □□ □□□□ □□□ Log Analytics □□ □□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.

Answer Area

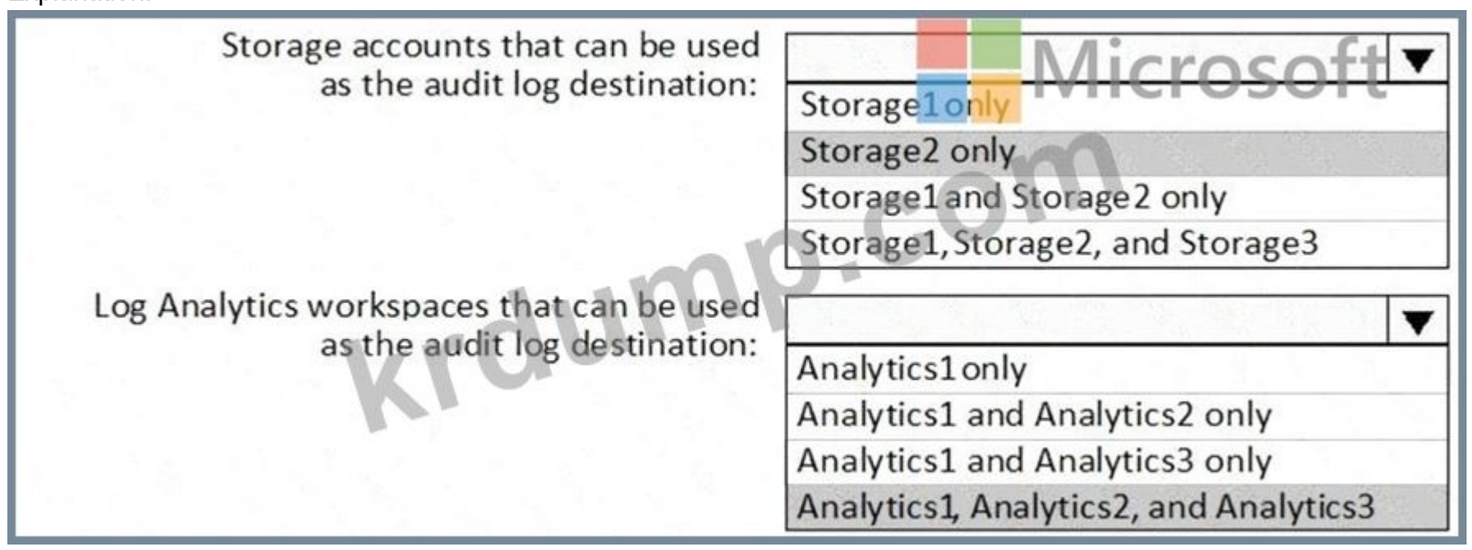
Storage accounts that can be used as the audit log destination:
- Storage1 only
- Storage2 only
- Storage1 and Storage2 only
- Storage1, Storage2, and Storage3

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:



Explanation:



NEW QUESTION: 34

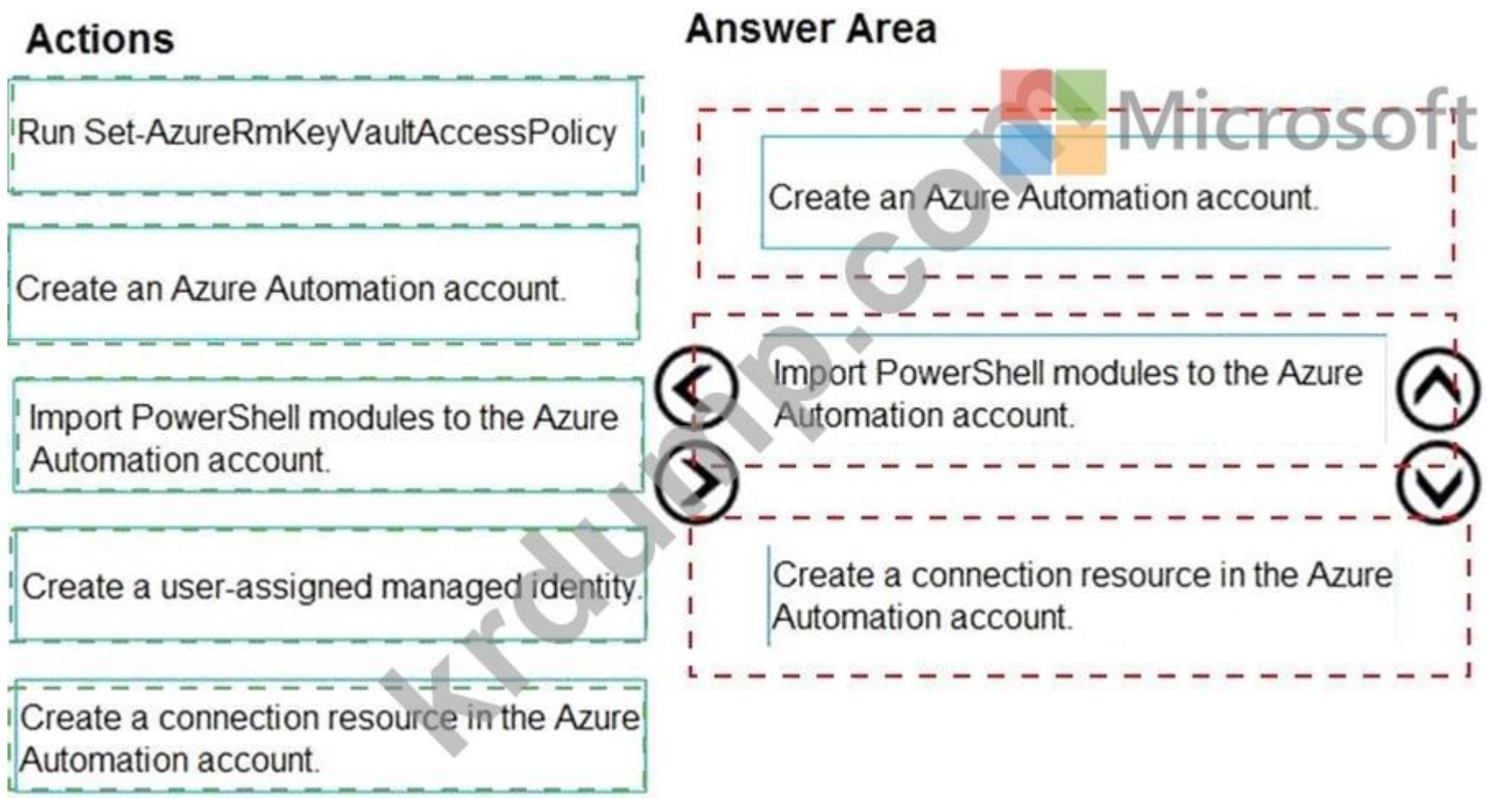
Contosostorage1□□□ Azure Storage □□□ Contosokeyvault1□□□ Azure Key Vault□ □□□□ Sub1□□□ Azure □□□ □□□□.

Contosostorage1□ □□ □□□□ Contosokeyvault1□ □□□□ Azure Automation □□□ □□ □□□□□.

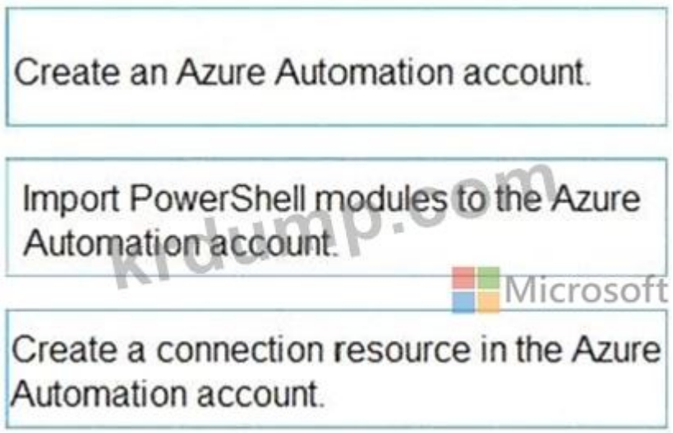
□□□ □□□□□ □□ □□□ □□□□ □□□.

□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.

Answer:



Explanation:



Step 1: Create an Azure Automation account
Runbooks live within the Azure Automation account and can execute PowerShell scripts.
Step 2: Import PowerShell modules to the Azure Automation account
Under 'Assets' from the Azure Automation account Resources section select 'to add in Modules to the runbook. To execute key vault cmdlets in the runbook, we need to add AzureRM.profile and AzureRM.key vault.
Step 3: Create a connection resource in the Azure Automation account
You can use the sample code below, taken from the AzureAutomationTutorialScript example runbook, to authenticate using the Run As account to manage Resource Manager resources with your runbooks. The AzureRunAsConnection is a connection asset automatically created when we created 'run as accounts' above.
This can be found under Assets - > Connections. After the authentication code, run the same code above to get all the keys from the vault.

```
$connectionName = " AzureRunAsConnection "
try
{
# Get the connection " AzureRunAsConnection "
$servicePrincipalConnection=Get-AutomationConnection -Name $connectionName
" Logging in to Azure... "
Add-AzureRmAccount `
-ServicePrincipal `
-TenantId $servicePrincipalConnection.TenantId `
-ApplicationId $servicePrincipalConnection.ApplicationId `
-CertificateThumbprint $servicePrincipalConnection.CertificateThumbprint
}
```

References:
https://www.rahulpnath.com/blog/accessing-azure-key-vault-from-azure-runbook/

NEW QUESTION: 35
□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

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

VM5□ IP □□ 10.1.0.4□ □□□□□□□. VM5□□ □□ IP □□□ □□□□.

VM5□ □□ □□□□ □ □ □□□ JIT(Just-in-Time) VM □□□□ □□□□□□.

VM5□ □□ JIT VM □□□□ □□□□□□.

NSG1□□ □□ □□ □□□ □□□□ □□□ □□□□.

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

□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.

□□: □□ 1□□ 1□□□□.

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: 36

□□□ □□□ □□□ □□□□ □□□□.

□□□ □□□□ □□□□□ □□ Azure Active Directory(Azure AD) □□ □□□□ □□ □□□ □□□□ □□□.

□□ □□ □□□ □□ □□□ □□□□ □□□.

* □□ □□□ □□□ □□□

* □□□□□ □□□□ □□□ □□□□□□.

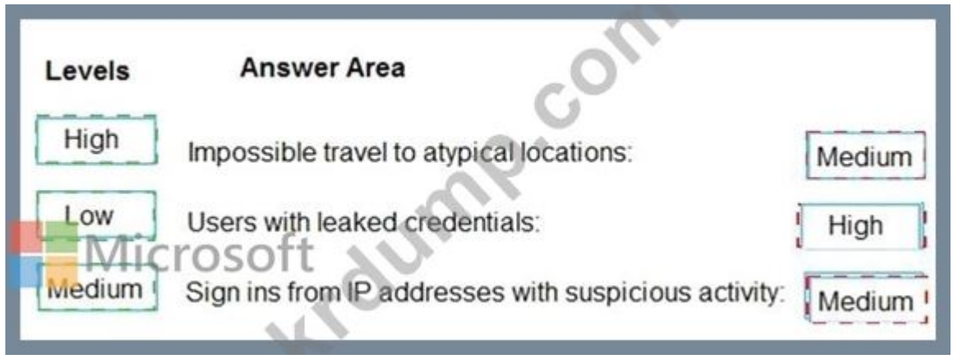
* □□□□□ □□□ □□ IP □□□□ □□□

□ □□ □□□□ □□ □□ □□□ □□□□ □□□? □□ □□□□ □□ □□□ □□ □□ □□□□ □□□□□□. □ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □□□ □□ □□□ □□□□□□ □□□□□ □ □□ □□□□.

□□: □□ 1□□ 1□□□□.

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

Answer:



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

NEW QUESTION: 37
storage1□□□ □□□ □□□ □□□ VM1□□□ □□□ □□ □□□ □□□ Azure □□□ □□□□.
VM1□ □□□ □□□□ □□□□ Azure DNS□ □□□□ VNet1□□□ □□ □□□□□ □□□□□.
VM1□ □□ IP □□□ □□□□ storage1□ □□□□□ □□ □□□. □□□□ □□ □□□ □□□□□ □□□.
□□□ □□ □□□?
A. storage1□ □□ □□□ □□ □□□□□□ □□□□.
B. storage1□ □□ □□ □□□□ □□□□ □□□□□□□.
C. VNet1□□ □□□ □□□□ □□□□.
D. Azure □□ DNS □□□ □□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 38
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□,
□□ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
Azure Security Center□ □□□□ □ □□ Azure □□□ □□ □□ □□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□ □□ □□ □□ □□□ □□□□□.
□ □□ □□ □□□ □□ □□□ □□□□ □□□□ □□□.
□□□: □□□ □□□ □□□ □□□ □□ □□□□□□ □□□ □□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
Instead use a management group.
Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously.
Reference:

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

NEW QUESTION: 39
Admin1□□□ □□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□. Admin1□□□ □□□□□□ □□□ □□□ □□□□□□□.
App1□□□ □□□□ □□ □□□□ Azure AD□ App1□ □□□□□.
Admin1□ App1□ □□ □□ □□□□ □□□□□ □□□ □□□ □ □□□ □□□□□.
Azure Portal□□ Admin1□ App1□ □□ □□ □□□□ □□□□ □ □□□ □□□□ □□□.
□□□ □□ □□□?
A. App1□ □□ □□□□ □□□□□□.
B. App1□ API □□□ □□□□□.
C. App1□ □□□□□□ □□□□□□□□ □□□□□.
D. Admin1□□ □□□□ □□□□□□ □□□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
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: 40
□□□□□ □□□ □□□ □□□□. VM1□ VNet1□□□ □□ □□□□□ □□□□ □□□□. VNet1□ S2S(□□□ □) VPN□ □□□□ □-□□□□ □□□ □□□ □□□□ □□□ □.
storage1 □ App1□□□ □□□ Azure □□□□ □□□ □□ □□□□□.
□ □□□□ □□ □□□□ □□□ □□ □□ □□□ □□□□□ □□□□ □□□.
* App1□ □□ □□□ □□ □□□□ NAT □□□□□ □□□□□ □□□.
* VNet1□□ storage1□□ □□□ Microsoft □□ □□□□□ □□□□ □□□.
* □□□□ □□□ □□□□□ □□□.
□ □□□□ □□ □□□ □□□□ □□□? □□□ □□□ □□ □□□ □□ □□□□ □□□□□ □□□□. □ □□ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □ □□ □□ □□□ □□□□□□ □□□□□ □ □□ □□□□.
□□: □□ 1□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 41

□□□ □□

□□ 4

□□□□ Azure Resource Manager □□□□ □□□□ □□□□ □□□□ □□ □□□ KV31330471□□□ Azure Key Vault□ □□□ □□□□ □ □□□ □□□□ □□□.

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.

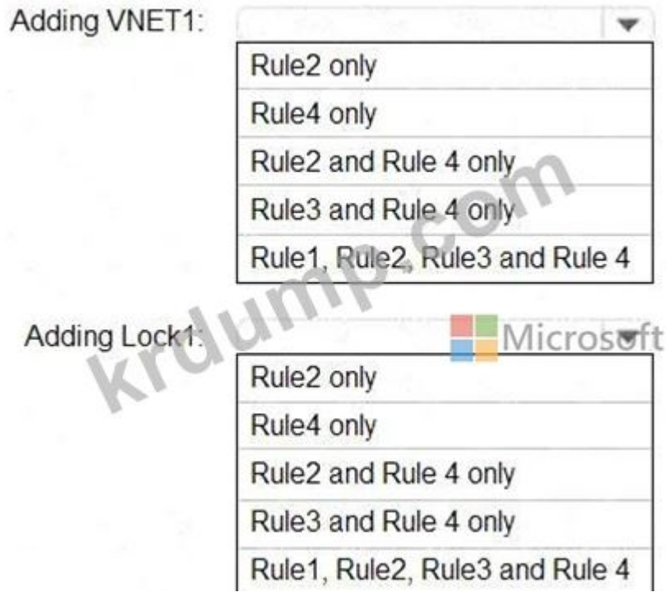
* Reference the secrets in the template by using their resource ID. You can use the listSecrets function to get the resource ID of a secret in the key vault. You need to specify the name of the key vault and the name of the secret as parameters.
* Deploy the template by using Azure PowerShell, Azure 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: 42
Microsoft Enterprise PIM(Privileged Identity Management)□ □□□□ Azure □□□ □□□□. User1□□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□□. □ □□□ □□ 2□□ □□□ □□ □ □□□□ □□□□ □□□. □□□ □□ □□□?
A. □ □□□ □□□ □□□□□.
B. □□□ □□ □□□□ □□□□□□□.
C. □□ □□□ □□□ □□□□□.
D. □□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)

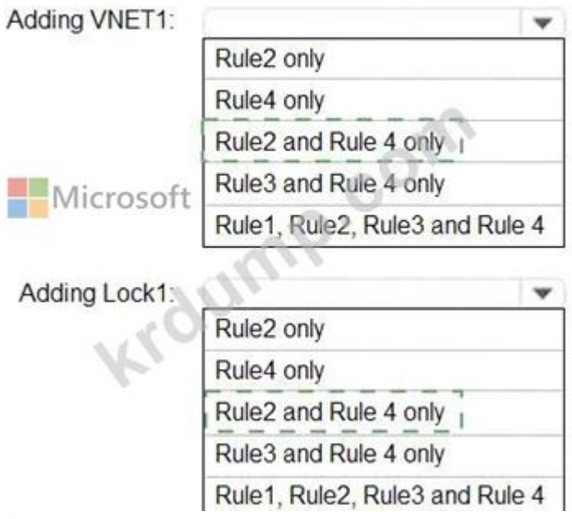
NEW QUESTION: 43
Admin1□□□ □□□□ RG1□□□ □□□ □□□ □□□□ Azure □□□ □□□□.
Azure Monitor□□ □□ □□ □□□ □□ □□□ □□□□.

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

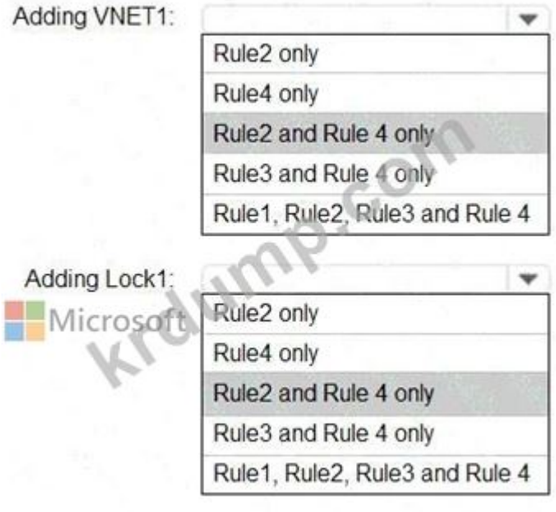
Admin1□ RG1□ □□ □□ □□□ □□□□□.
* VNET1□□□ □□ □□□□□ □□□□□.
* Lock1□□□ □□□ □□ □□□ □□□□□.
Admin1□ □□□□ □□ □□ □□□□ □□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 44

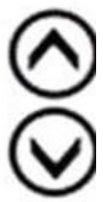
□□□ □ □□□□□□ □□ □□□ □□□□□ SQLDB1□ □□□□ □□□.

□□ □ □□ □□□ □□□□ □□□□ □□ □□□□? □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.

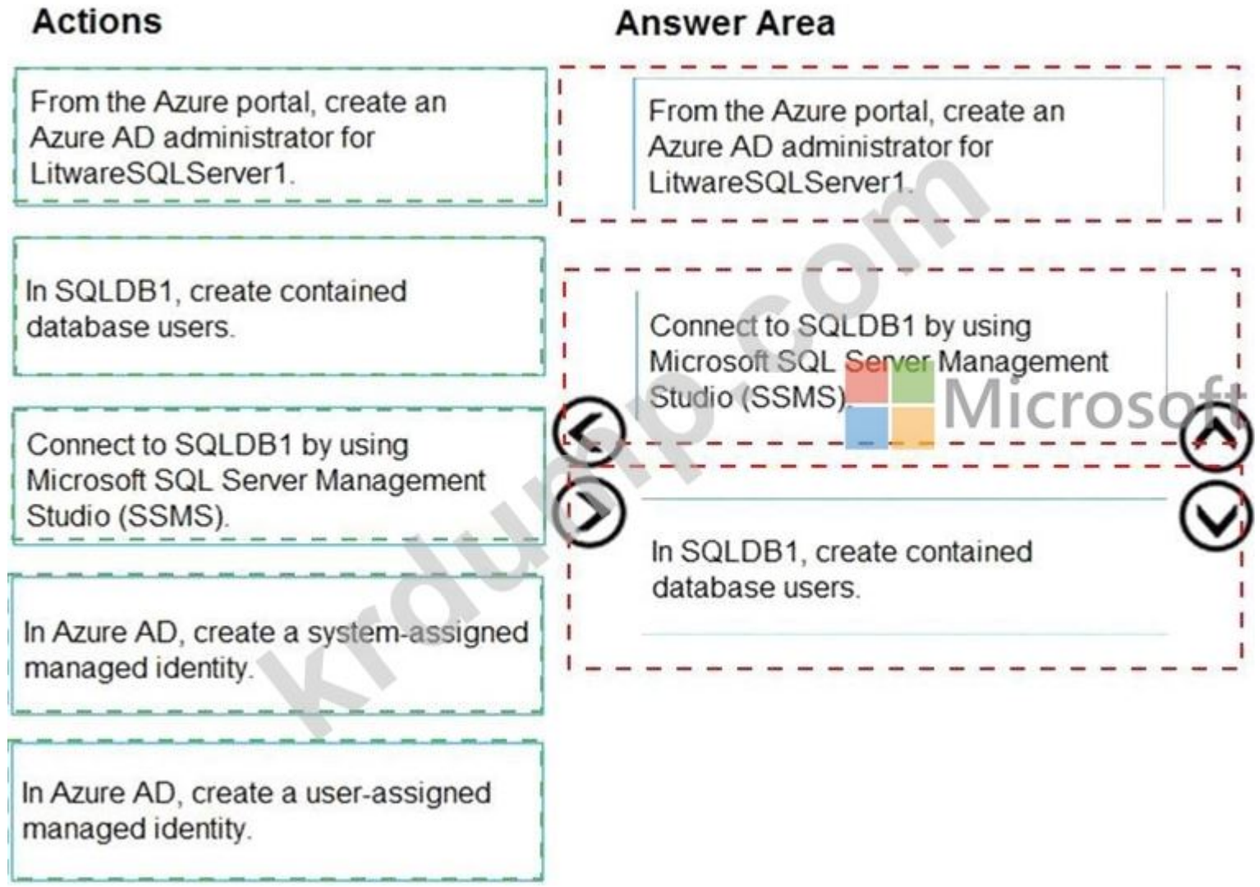
Actions

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

Answer Area



Answer:



Explanation:
From the Azure portal, create an Azure AD administrator for LitwareSQLServer1 Connect to SQLDB1 by using SSMS In SQLDB1, create contained database users
https://www.youtube.com/watch?v=pEPyPsGEevw

NEW QUESTION: 45
Azure □□□ □□□□.
□□ □□ □□□ □□□□□ Azure □□ WAN□ □□□□ □□□.
* □□ □□, □□ □□, □□ □□ Azure □□□ □□□ 3□□ □□ □□ □□□ □□□□.
* □□ □□□ □ □□ □□ □□□□□□ □□□□□.
□□□ □□□□ □□□?
A. Azure □□□□ □□ □□□
B. Azure □□ □□□□ □□□
C. Azure □□
D. Azure □□□ □□□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 46
VM1□□□ □□ □□□ □□□ Azure □□□ □□□□.

VM1□□ □□□□ □□□□ DCR1□□□ □□□ □□ □□(DCR)□ □□□ □□□□.
ID□ 4798□ □□□□ □□□□□ □□ □□□.
DCR1□□□ □□□ □□□□ □□□?
A. aT-SQL□□
B. PowerShell □□□□
C. KQL □□
D. XPath □□
Answer: (SHOW ANSWER)

NEW QUESTION: 47
□□ □□□ □□□□ □□ Azure Sentinel □□ □□□ □□□□.
* Azure Active Directory ID □□
* □□ □□□ □□(CEF)
* Azure □□□
□ □□□□□ □□□□ □□□□□ □□□□ □□□.
□□ □□ □□□ □ □□□□ □□ □□ □□□□ □□□□ □□□? □□ □□□□ □□□ □□□ □□□□ □□□□□.
□□: □□ 1□□ 1□□□□.

Azure Active Directory Identity Protection:

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

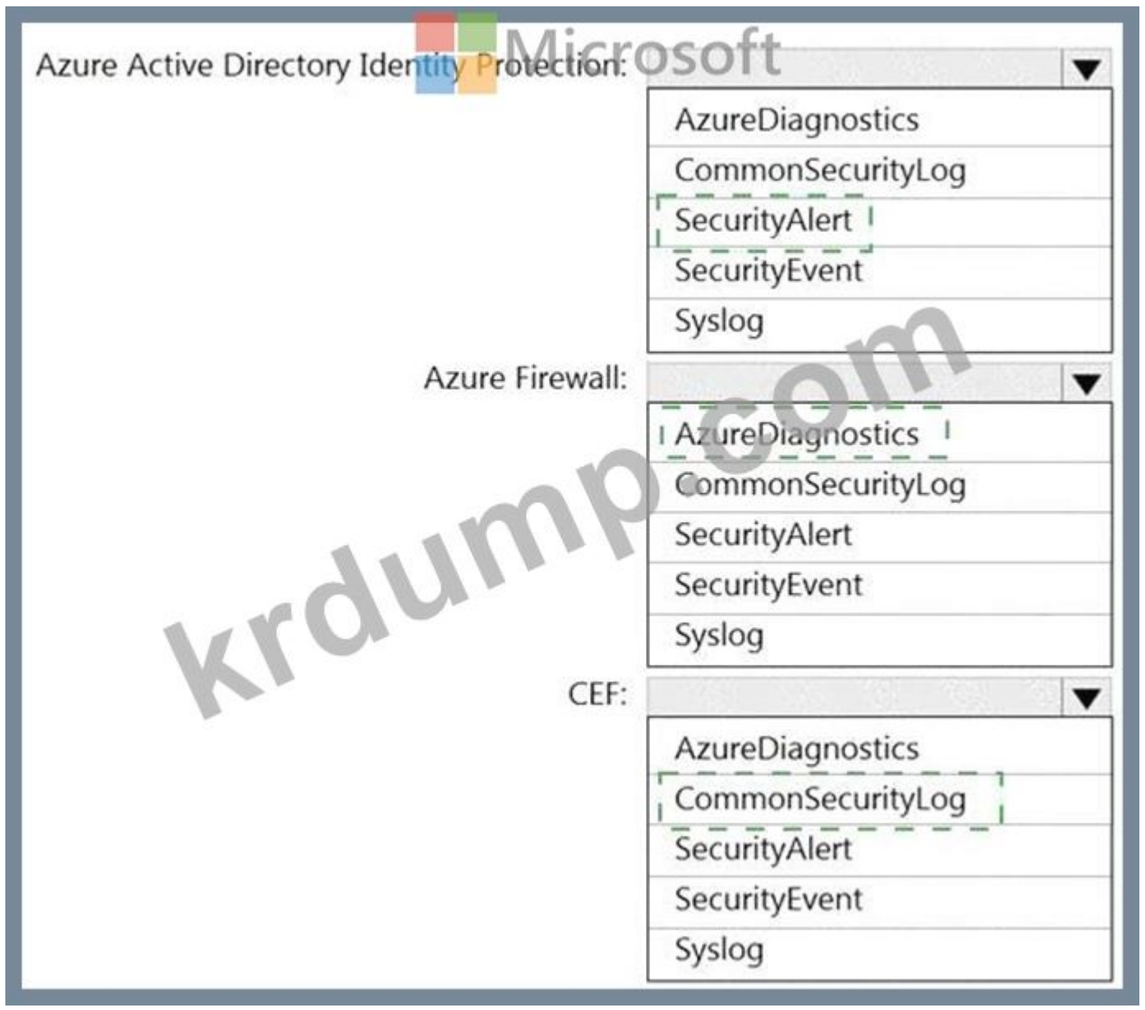
Azure Firewall:

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

CEF:

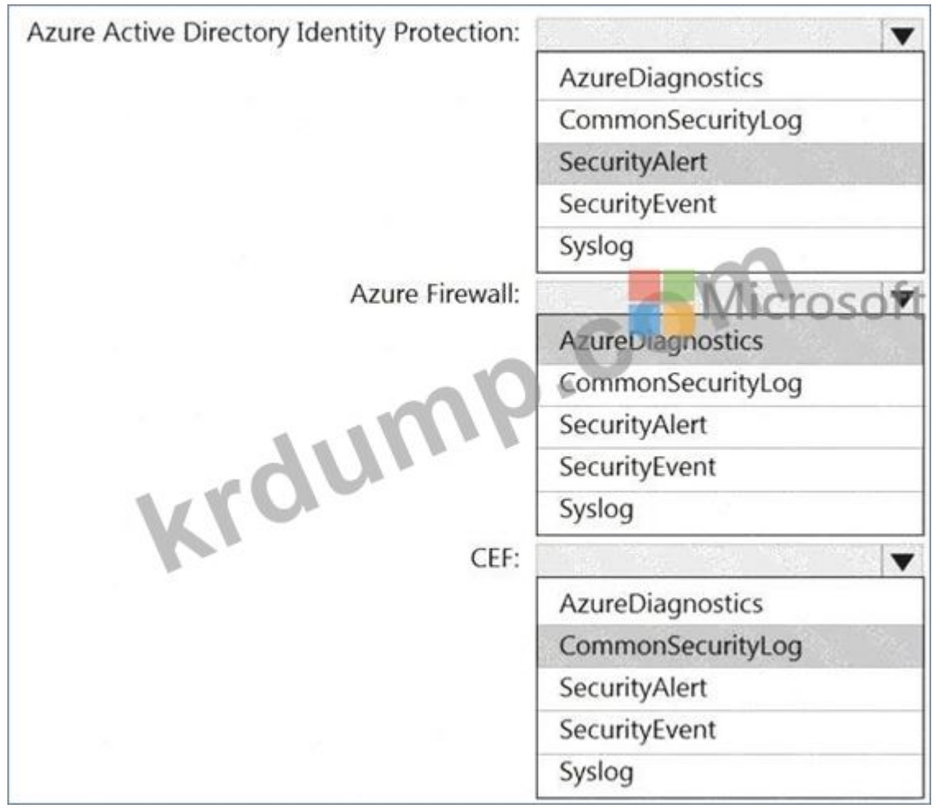
- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

Answer:



Explanation:

Graphical user interface, application, table Description automatically generated



NEW QUESTION: 48

webapp1□□□ Azure □□□ □□□□.

Azure Repo□ □□□□ webapp1□ □□ □□□□ □□□ □□□□ □□□.

□□ □□ □□□ □□□□ □□□?

A. Azure DevOps □□

B. Azure Storage □□

C. Azure Application Insights □□

D. Azure DevTest Labs □

Answer: (SHOW ANSWER)

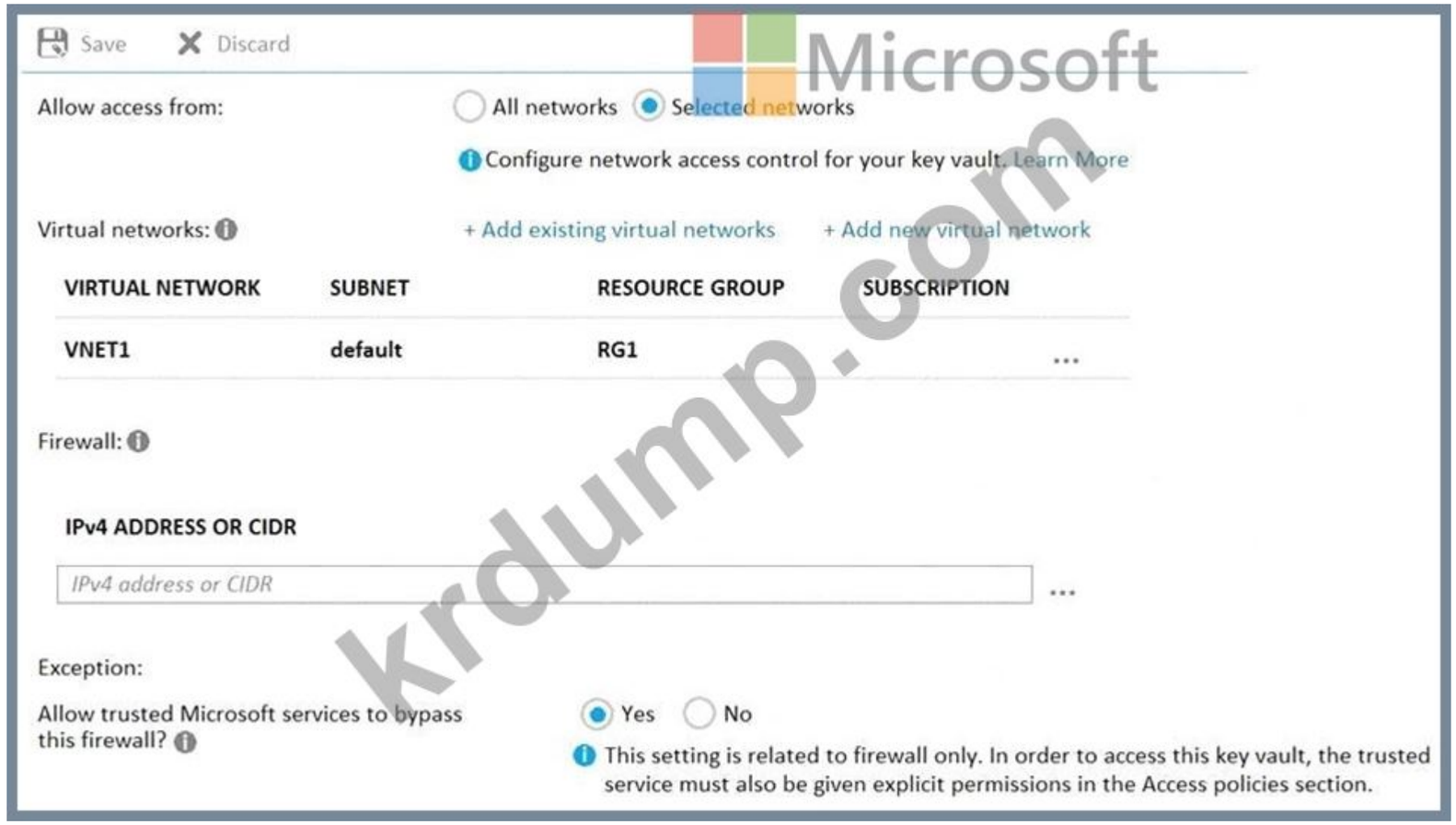
NEW QUESTION: 49

KeyVault1□□□ Azure Key Vault□ □□ □□ □□□ □□ □□□ □□□□ Azure □□□ □□□□.

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

□□ □□□□ □□ Azure Disk Encryption□ □□ □□□□ □□□□□□ Key Vault □□□ □□□ □□□□□.

KeyVault1□ □□ □□□ □□ □□□□□.



□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.

□□: □□ 1□□ 1□□□□.

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

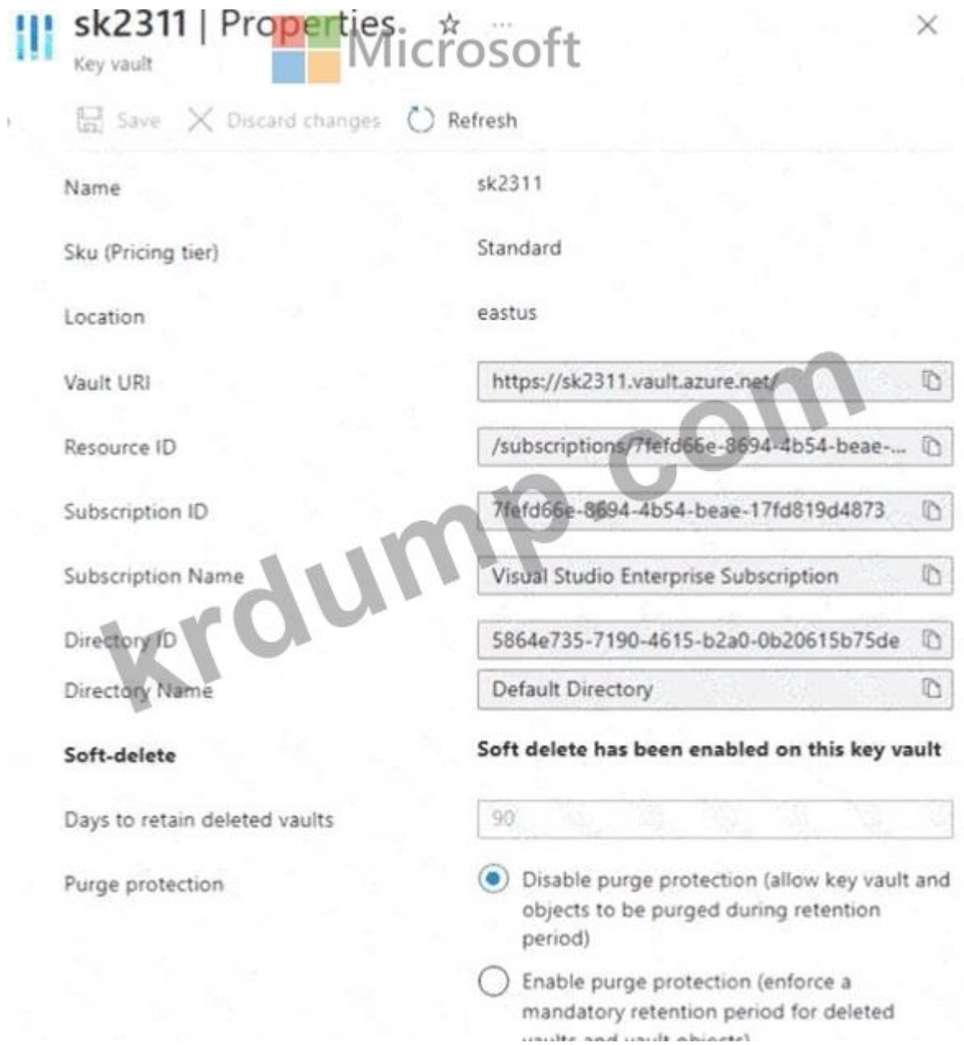
Answer:

Explanation:

Answer Area

NEW QUESTION: 50

□□ □□□ □□ sk2311□□□ Azure Key Vault□ □□□□ □□□□.



Sk2311□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

sk2311□□□ □□ □□□□ □□□□ □□□□□.

* Item1□ □□□□□□□.
* □□2□ □□1□ □□□□□□□.

□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.

□□: □□ 1□□ 1□□□□.

Answer Area

Answer:

Answer Area

Explanation:

NEW QUESTION: 51

RT1□□□ □□ □□□□ □□□ Azure □□□ □□□□. RT1□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□.

* □□ : RouteA
* IP □□ □□□: 192.168.0.0/24
* □□ □ IP □□: 172.16.10.10

□□ □□ □□□ □□□ □□□□ □□□ □□□□ □□□□.

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

RT1□ □□ □□□ □□□ □ □□□?

A. Route2□

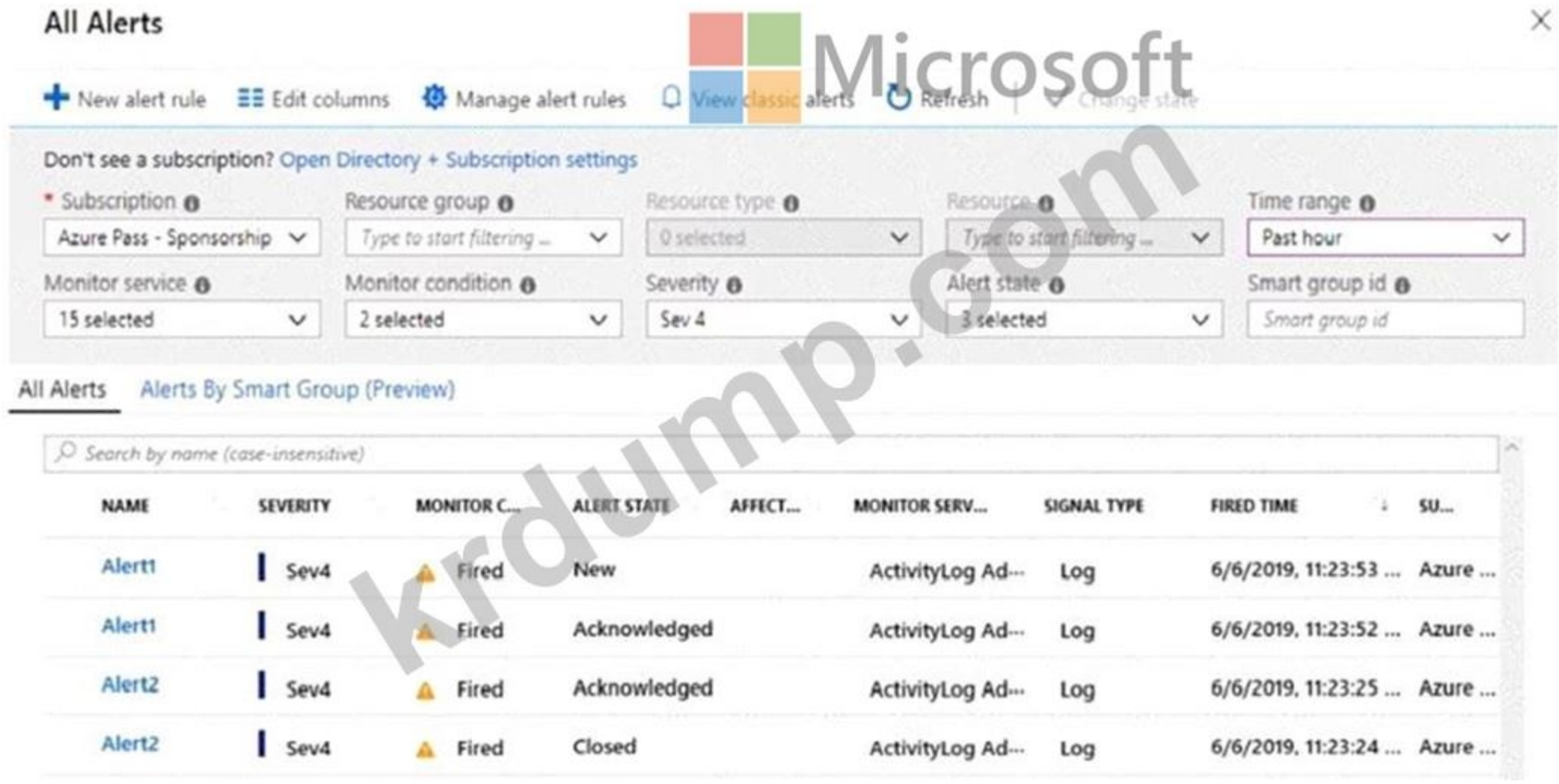
B. Route1□

C. Route1□ Route2□

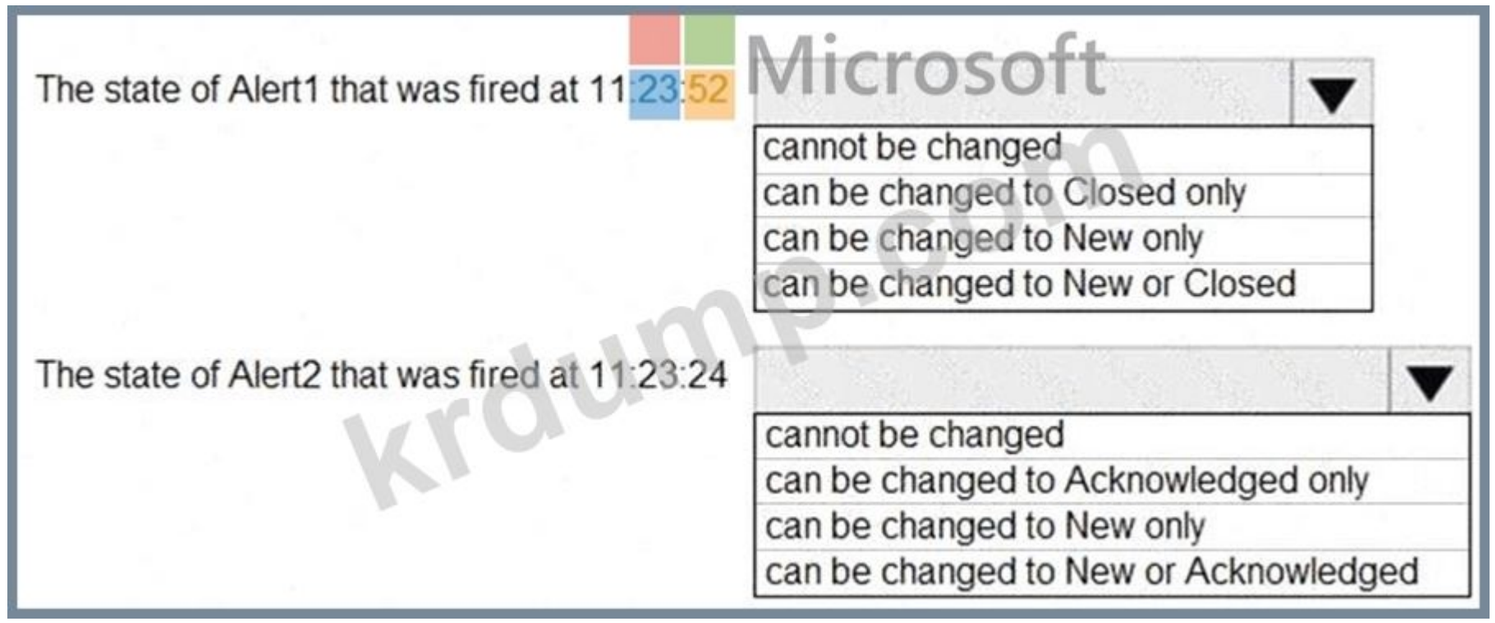
D. Route1□ Route3□

E. Route2□ Route3□
F. Route3□
Answer: D (LEAVE A REPLY)

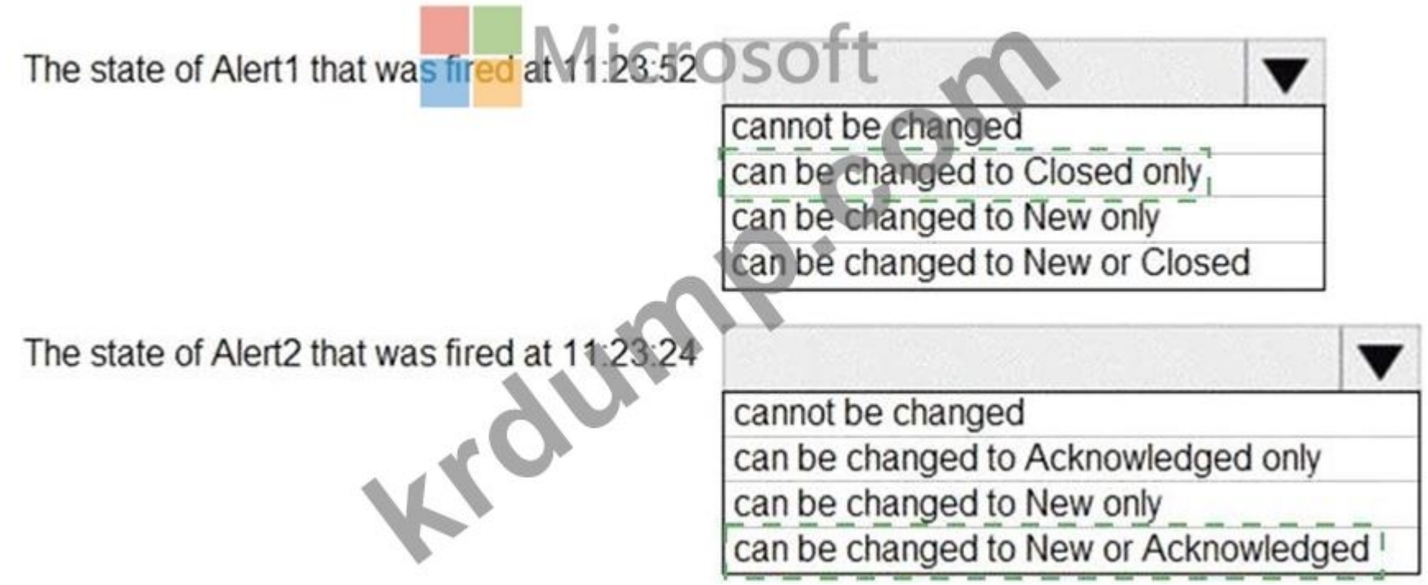
NEW QUESTION: 52
□□ □□□ □□□ □□□ □□□ Azure □□□ □□□□.



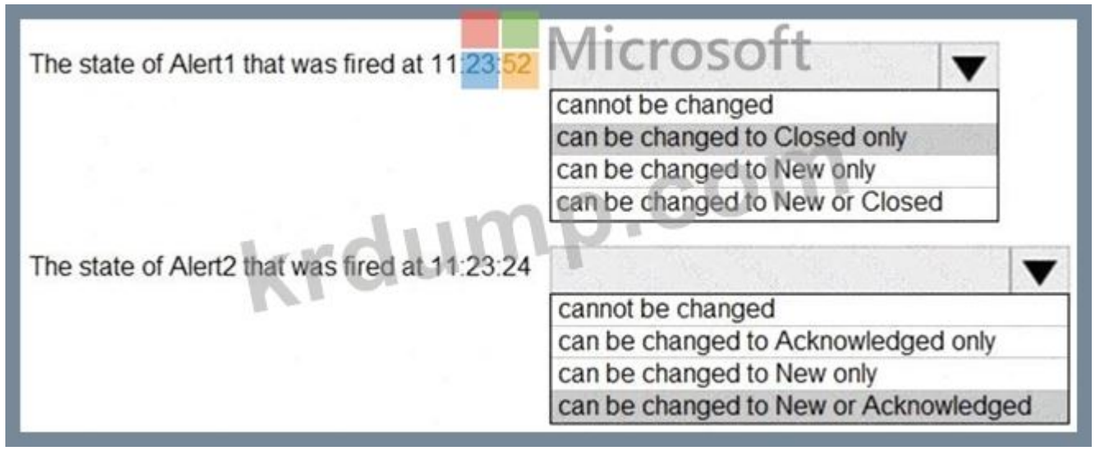
□□□□ □□□ □□□ □□□□ □ □□□ □□□□ □□ □□□ □□□□□ □□□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.



Answer:

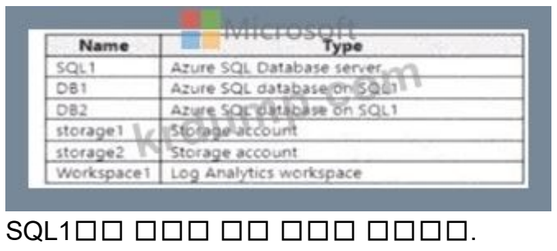


Explanation:



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

NEW QUESTION: 53
□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.



Name	Type
SQL1	Azure SQL Database server
DB1	Azure SQL database on SQL1
DB2	Azure SQL database on SQL1
storage1	Storage account
storage2	Storage account
Workspace1	Log Analytics workspace

SQL1□□ □□□ □□ □□□ □□□□.
* □□: □□□□
* □□ □□ □□: storage1, Workspace1
DB1□□ □□□ □□ □□□ □□□□.
* □□: □□□□
* □□ □□ □□: storage2
DB2□□ □□ □□□ □□□□□□□□□.
DB1□ DB2□ □□ □□□ □□□ □□□□□? □□□□ □□ □□□□ □□□ □□□ □□□□□. □□: □□ □□□ 1□□□□.
Answer Area

Answer:

Answer Area

Explanation:

NEW QUESTION: 54

Azure SQL □□□□□□□ □□□□ □□ □□□□.

□□□□□□□ □□ SQL □□ □□□ □□□ □□ □□□ □□□ □□□.

□□□ □□ □□□?

A. Azure Monitor□ SQL Health Check □□□□ □□□□□.

B. □□□□□□□ □□ □□ □□ □□□ □□□□□□.

C. □□□□□□□ □□ □□□ □□□□□.

D. □□□□□□□ □□ Azure Defender for SQL□ □□□□□□.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 55

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.

□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.

Sub1□□□ Azure □□□ □□□□.

RG1□□□ □□□ □□□ sa1□□□ Azure Storage □□□ □□□□.

□□□□ □□□□□□□ □□ □□ □□ □□□ □□(SAS)□ □□□ □□□ □□□ □□□□ sa1□ Blob □□□□ □□ □□□□ □□□□□□.

□□□ □□ □□□□ □□ □□□□ Blob □□□□ □□ □□□□ □□ □□□□□□.

sa1□ □□ □□ □□ □□□ □□□□ □□□.

□□ □□: Azure Storage □□ □□□ □□ □□ □□□□□.

□□□ □□□ □□□□□?

A. □
B. □□□
Answer: A (LEAVE A REPLY)
Generating new storage account keys will invalidate all SAS's that were based on the previous keys.

NEW QUESTION: 56
□□ □□ □□□ □□ □□ □□ □□□ □□□ Azure □□□ □□□□.

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

□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

6□ 1□□ □□ □□□ □□□□□.
* KeyVault1□□ key1□□□ □□ □□□□□.
* KeyVault2□□ secret 1□□□ □□□ □□□ □□□□□.
□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.

Statements	Yes	No
Admin1 can recover key1 on June 5.	○	○
Admin2 can purge secret1 on June 12.	○	○
Admin3 can recover key1 on June 17.	○	○

Answer:

Statements	Yes	No
Admin1 can recover key1 on June 5.	○	○
Admin2 can purge secret1 on June 12.	○	○
Admin3 can recover key1 on June 17.	○	○

Explanation:
Yes
Yes
No

NEW QUESTION: 57

User1□□□ □□□□ storage1□□□ □□□ □□□ □□□ Azure □□□ □□□□. storage1 □□□□ □□ □□ □□ □□ □□□□ □□□□ □□□□.

Name	Type
container1	Container
folder1	File share
table1	Table

User1□□ storage1□ □□ □□ □□□ □□□□□.

* □□□□ Blob □□□ □□
* □□ □□□ □□□ □□□
* □□ □□ □□□ SMB □□ □□

Statements	Yes	No
On October 1, 2022, if User1 accesses folder1 by using SAS1, he can delete the files in folder1.	○	○
On October 1, 2022, if User1 maps folder1 as a network drive by using his Azure Active Directory (Azure AD) credentials, he can delete the files in folder1.	○	○
On October 1, 2022, User1 can delete the rows in table1 by using SAS1.	○	○

Answer:

Statements	Yes	No
On October 1, 2022, if User1 accesses folder1 by using SAS1, he can delete the files in folder1.	○	○
On October 1, 2022, if User1 maps folder1 as a network drive by using his Azure Active Directory (Azure AD) credentials, he can delete the files in folder1.	○	○
On October 1, 2022, User1 can delete the rows in table1 by using SAS1.	○	○

Explanation:

No, Yes, No

NEW QUESTION: 58

□□ □□ □□□ □□ □□□ □□□ Azure □□□ □□□□.

□□□ 1□ □□□ 2□□ □□□□ □□ □□(NSG)□ □□□□. NSG□□ □□□ □□ □□□ □□ □□□□□ □□□ □□□□.

* □□; □□
* □□ : Any
* □□□□: 100
* □□: □□
* □□□□: □□
* □□□: □□□

□□□□ storage1□□□ □□□ □□□ □□□ □□□□ □□□□.

□□ □□□ □□□□ Private1□□□ □□ □□□□□□ □□□□.

* □□□ □□: Microsoft.Storage/storageAccounts

* □□□: storage1
* □□ □□ □□□: blob
* □□ □□□□: VNet1
* □□□: Subnet1

□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.

□□: □□ 1□□ 1□□□□.

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:

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.	○	◉

NEW QUESTION: 59

□□□ □□

□□□ □□ □□ □□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□ □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
□□□□□ □□□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□□□.
Azure □□□ □□: Userl -28681041@ExamUsers.com
Azure □□□□: GpOAe4@lDg
Azure Portal□ □□□□□ □□□□□ □□□□ □□□ CTRL-K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
□□□ □□□□: 28681041
□□ 5
rg1lod28681041 Azure Storage □□□ □□□□ □□□□ □ □□□ 131-107.0.0/16 □□□□ □□□ □□□ □□□□ □□□.
Answer:
Check below steps in explanation for Task.
Explanation:
To ensure that only devices connected to a 131-107.0.0/16 subnet can access data in the rg1lod28681041 Azure Storage account, you can follow these steps:
* In the Azure portal, search for and select the storage account named rg1lod28681041.
* In the left pane, select Firewalls and virtual networks.
* In the Firewalls and virtual networks pane, select Selected networks.
* In the Selected networks pane, select Add existing virtual network.
* In the Add existing virtual network pane, select the virtual network that contains the 131-107.0.0/16 subnet.
* Select Add.
https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

NEW QUESTION: 60
AKS1□□□ □□□ Azure Kubernetes Service(AKS) □□□□□ □□□ Azure □□□ □□□□.
Azure DevOps Microsoft □□□ □□□□□ □□□□ □□□ □□□□ □□□□ □□□□ Azure □□□□ □□□□□□ □□□□.
□□□□ □□ □□□□□□□ AKS1□ □□□□ □ □□□ □□□□ □□□. □□□□ □□ □□□ □□□□□ □□□.
AKS1□ □□ □□□ □□□□ □□□?
A. □□□ IP □□ □□
B. □□□□□□ □□□□□ □□□□ □□□□(AGIC)
C. □□ □□□□
D. □□ □□□□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 61
Azure Active Directory(Azure AD) □□□□ □□□□.
□□ □□□ □□□ □□□ □□ □□□□.

Name	Type	Deleted on
Group1	Security group	April 5, 2020
Group2	Office 365 group	April 5, 2020
User1	User	March 25, 2020
User2	User	April 30, 2020

2020□ 5□ 4□□ Azure Active Directory □□ □□□ □□□□ □□□ □□□ □□□□□ □□□□□.

□□ □ □□ □□□ □□□ □ □□□? □□□ □□ □□□ □□□□ □□□□□.
□□: □□ 1□□ 1□□□□.
A. □□1
B. □□2
C. □□□2
D. □□□1
Answer: B,C (LEAVE A REPLY)
Deleted users and deleted Office 365 groups are available for restore for 30 days.
You cannot restore a deleted security group.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-restore-deleted

NEW QUESTION: 62
Microsoft Defender for Cloud□ □□□□ Azure □□□ □□□□.
Amazon Web Services(AWS) □□□ □□□□.
□□□ AWS Elastic Compute Cloud(EC2) □□□□□ □□□ □ Microsoft Defender for Servers □□□□□ □□□□ □□□□□ □□□□ □□□.
□□ □□□ □□□□ □□□?
A. □□□□ □□□□ □□□
B. □□□ □□□□ □□□
C. Azure Monitor □□□□
D. □□ □□ □□□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 63
Windows Server 2019□ □□□□ □□□□□ □□□ 10□ □□□□.
□□□ □□ Azure Security Center □□□ □□□□ □□□ □□□□□.
□□□ □□ □□□ □□□□ □□□?
A. Azure Sentinel□ □□ □□□ □□□ □□□
B. Microsoft Endpoint Configuration Manager □□□□□
C. Azure Arc □□ □□ Connected Machine □□□□
D. Endpoint□ Microsoft Defender □□□□
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: 64

Sub1□□□ Azure □□□ □□□□ MG1□□□ □□ □□□ □□□□.

Sub1□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

□□ □□□ □□ AVNM1□□□ Azure Virtual Network Manager □□□□□ □□□□.

* Management scope: MG1

* Network groups:

o Name: Group1

Group members: VNet1

* Security admin configuration:

o Name: SAT

o Rule collections:

Name: SACollection1

Target network groups: Group1

Security admin rules:

Name: SARule1

Priority: 500

Action: Deny

Direction: Inbound

Source type: Any

Source port *

SA1 is deployed to all Azure regions.

You create a Virtual Network Manager instance named AVNM2 that has the following configurations:

* Management scope: Sub1

* Network groups:

o Name: Group2

Group members: VNet1

* Security admin configuration:

o Name: SA2

o Rule collections:

Name: SACollection2
Target network groups: Group2
Security admin rules:
Name: SARule2
Priority: 500
Action: Always allow
Direction: Inbound
Source type: Any
Source port: *
SA2□ □□ Azure □□□ □□□□□.
□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□: □□ 1□□ 1□□□□.

Answer Area

Statements	Yes	No
If you change Priority for NSGRule1 to **100**, NSG1 will be processed before SA1 and SA2.	○	○
Internet traffic is blocked to the public IP address of VM1.	○	○
If you change Action for SARule1 to **Allow**, internet traffic to the public IP address of VM1 will be enabled automatically.	○	○

Answer:

Answer Area

Statements	Yes	No
If you change Priority for NSGRule1 to **100**, NSG1 will be processed before SA1 and SA2.	○	○
Internet traffic is blocked to the public IP address of VM1.	○	○
If you change Action for SARule1 to **Allow**, internet traffic to the public IP address of VM1 will be enabled automatically.	○	○

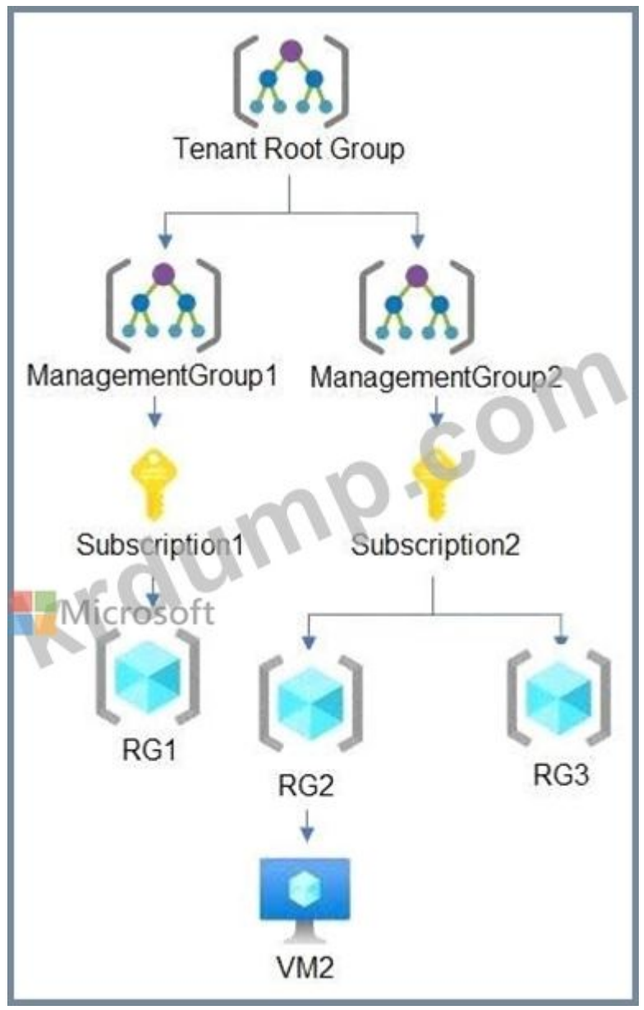
Explanation:

Answer Area

Statements	Yes	No
If you change Priority for NSGRule1 to **100**, NSG1 will be processed before SA1 and SA2.	○	●
Internet traffic is blocked to the public IP address of VM1.	○	●
If you change Action for SARule1 to **Allow**, internet traffic to the public IP address of VM1 will be enabled automatically.	●	○

NEW QUESTION: 65

□□ □□□□ Azure □□□□ □□ □□□ □□□□□.



RG1, RG2, RG3□ □□□ □□□□□.

RG2□□ VM1□□□ □□ □□□ □□□□ □□□□.

□□ □□ □□□ □□□□□ □□ □□ □□□ □□(RBAC) □□□ □□□□□.

Name	Role	Added to resource
User1	Contributor	Tenant Root Group
User2	Virtual Machine Contributor	Subscription2
User3	Virtual Machine Administrator Login	RG2

□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□: □□ 1□□ 1□□□□.

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

Answer:

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

Explanation:

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

NEW QUESTION: 66
□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

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

□□□ □□□□□□ □□□ □□□□□ □□□ □□□ □□□□□.

□□□ □□□□□□ □□□□ □□□□ □ □□ □□□□ □□□□, □□□ □□□□□ □□□ □□□□ □□□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ 1□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 67
Microsoft Sentinel□ □□□□ □□□□.
□□□ □□ □□ □□□□ □□□□ □□□. □□ □□□□ CER(Common Event Format) □□□ □□□□ □□□□□.
□□□ □□□ □□□□ □□□? □□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.

Answer:

See the answer below at Explanation.

Explanation:

Answer is as image below.

NEW QUESTION: 68

□□ □□□ Azure □□ □□□ □□ □□□□.

Name	Operating system	State
VM1	Windows Server 2008 R2 Service Pack 1 (SP1)	Running
VM2	Windows Server 2012 R2	Running
VM3	Windows Server 2016	Stopped
VM4	Ubuntu Server 18.04 LTS	Running

□□ □□ □□□ □□□□ □□□ □□□□ □ □□□?

A. VM2 □ VM3□ □□

B. VM2, VM3 □ VM4□ □□

C. VM1, VM2 □ VM4□ □□

D. VM1, VM2, VM3 □ VM4

E. VM1, VM2 □ VM3□ □□

Answer: (SHOW ANSWER)

References:

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

NEW QUESTION: 69

□□□□□ contoso.com□□□ Active Directory □□□□□ □□□□. □ □□□□□□ □□ □□□□ □□□□.

contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□□ Sub1□□□ Azure □□□ □□□□.

Azure AD Connect□ □□□□ Active Directory□ Azure AD □□□□ □□□ □□□□□.

□□ □□ □□□ □□□□ □□ □□□□ □□□□ □□□.

□□□□ □□□□ □□□ □□□ □□ □□□ □□□ □□□ □□□ □□□□□ □□□□□. □□□□ □□□ □□ □□ □□□□□□.
□□ □□ □□□ □□□ □□□□ □□□?

A. Active Directory Federation Services(AD FS)□ □□□ □□□□□ ID

B. □□□ SSO(Single Sign-On)□ □□ □□□□ □□ □□□

C. □□□ SSO(Single Sign-On)□ □□ □□□□ □□

Answer: C (LEAVE A REPLY)

1. Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant
> > Pass-Through Authentication enforce on-premises user account states, password policies, and sign-in hours.
2. Minimizes the number of servers required for the solution.
> > Pass-through needs a lightweight agent to be installed one (or more) on-premises servers.
> > PW Hash also require installing Azure AD Connect on your existing DC.

NEW QUESTION: 70

Azure □□□ □□□□.
□□ □□ □□□ □□ □□□ □□□ □□□□□.

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

□□ □□ □□□□ □□□ □ □□ □□ □□□ □□ □□□ □□□□ □□□?
□□ Windows □□ □□□ □□ Linux □□ □□□ □□□□ □□□?

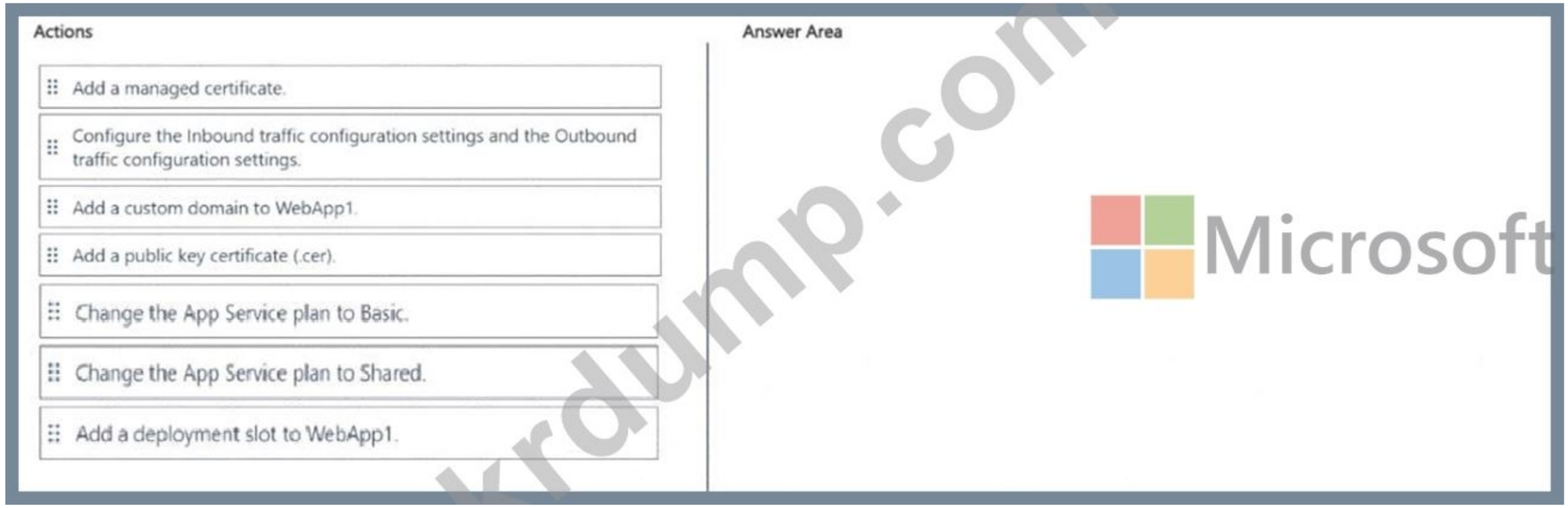
Answer Area

Answer:

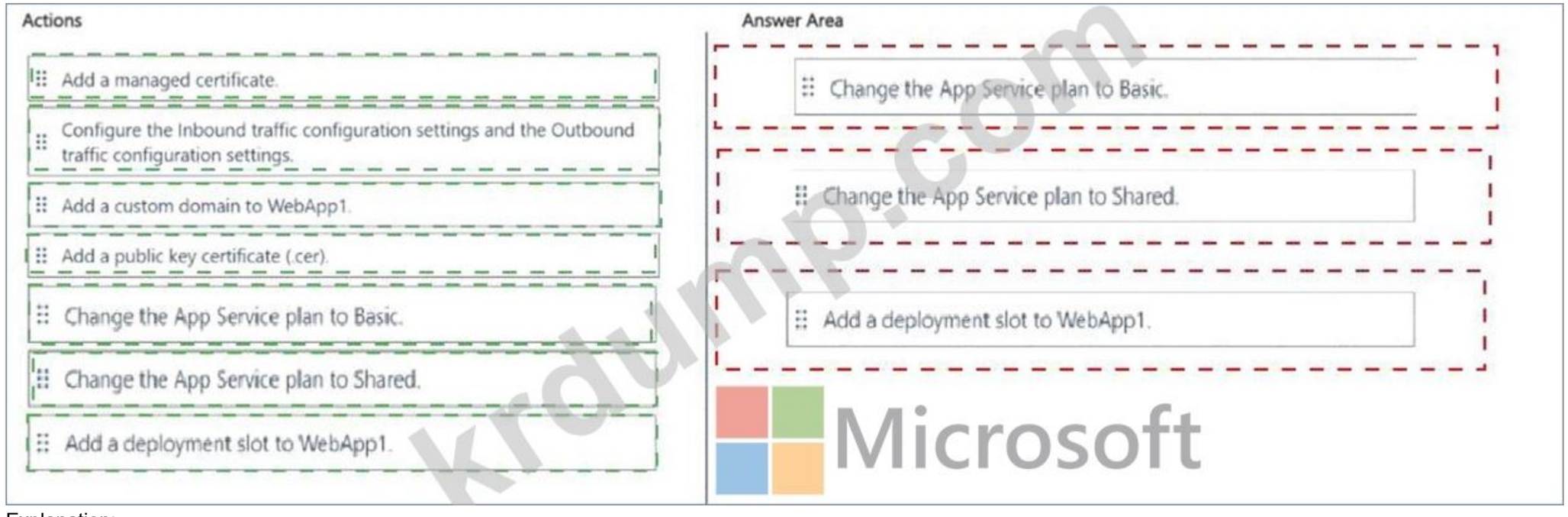
Explanation:

NEW QUESTION: 71
Azure Key Vault□ □□□ Azure □□□ □□□□.
storage1□□□ □□□ □□□□ □□□ □□□□□.
□□□ □□ □□□□1 □□□□ □□□□ □□□ □□□□□.
* Azure □□
* Azure Blob □□□□
* Azure □□□ □□□□
* Azure Queue □□□□
□ □□□□ □□□ □□ □□□□ □□□ □□□□ □□□ □ □□ □□□□ □□□□□? □ □□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.
A. □ □□□
B. □□ □□□□
C. Azure □□
D. □□□ □□□
Answer: B,C (LEAVE A REPLY)

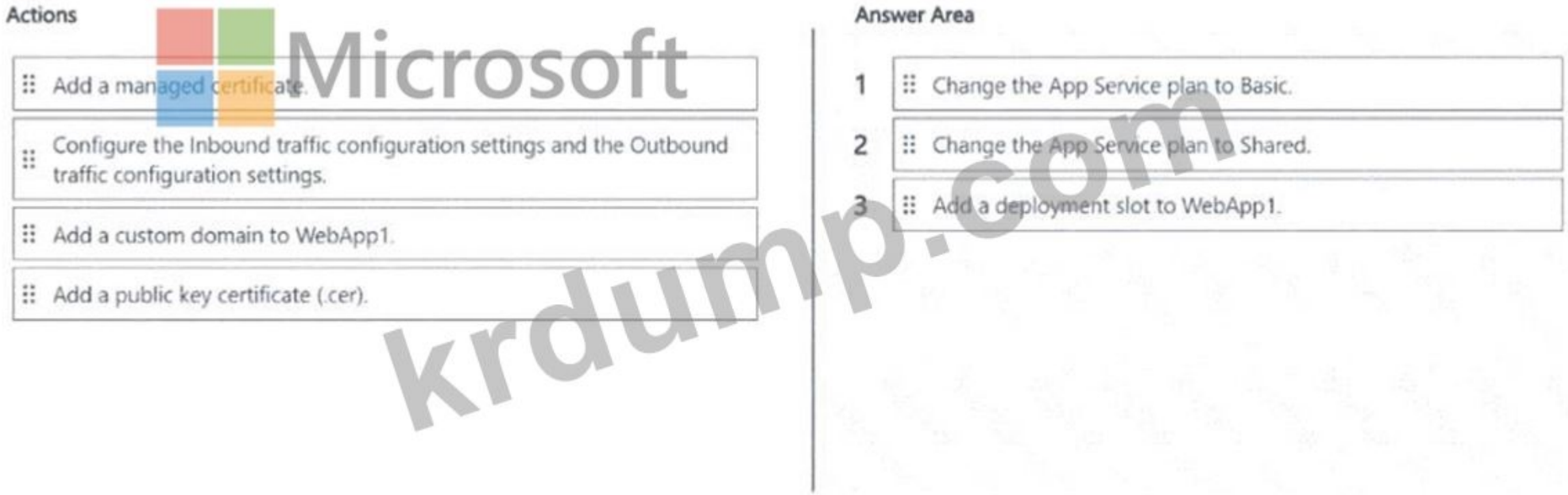
NEW QUESTION: 72
□□□□ Azure □□□□ □□□ □□ Azure App Service □ □□ □□□□ □□□□.
* □□: WebApp1
* □ □□□ □□□: □□
WebApp1□ App Service □□□ □□□□ □□□□□ □□□□ □□□. □□□□ □□□ □□□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□ □□□□□, □□ □□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:



NEW QUESTION: 73
Azure AD □□□□ □□□□.
□□ □□ □□□ □□□□ □□ □□ □□□□ □□□ □□□□□.
* □□ □□□ □□□□□.
* □□□ □ □□□ □□□ □□□□□.
□□□□ □□ □□ □□□ □□□□ □□□?
A. FID02 □□ □
B. Microsoft □□□
C. □□ □□□
D. □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 74
□□ □□□ Azure □□□□ □□ □□□□.

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

□□ □□ □□□ □□□□ □□□.
* □□□□ □□□ □□ □□□ NSG(□□□□ □□ □□)□ □□□□ □□□□ □□□.
* □□ □□ □□□□ □□□ □□□□ □□□□□ □□□ □□□.
Azure Security Center□□ □□□□ □□ □□ □□ □□ □□□□□?
A. 3
B. 4

C. 1
D. 2
Answer: B (LEAVE A REPLY)

NEW QUESTION: 75
Azure Storage □□□ □□ □□□ □□□□ □□□□. Azure Storage □□ □□□ □□□□□ □□□ □□□ □□□□□. □□ □□□ □□□□□ □□□ □□□□ □□□?
A. Azure □□□
B. Azure□ SQL □□ □□□
C. Azure □□□ □□□
D. Azure Cosmos DB □□□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 76
□□□ □□
□□□ □□ □□ □□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□ □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
□□□□□ □□□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□□□.
Azure □□□ □□: Userl -28681041@ExamUsers.com
Azure □□□□: GpOAe4@lDg
Azure Portal□ □□□□□ □□□□□ □□□□ □□□ CTRL-K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
□□□ □□□□: 28681041
□□ 4
user2-28681041□□□ □□□□ RG1lod28681041 □□□ □□□ □□ □□ □□□ □□□ □□□ □ □□□ □□□□ □□□. □ □□□□ □□ □□ □□□ □□□□ □□□.
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: 77

Azure Container Registry□ □□□ Azure Kubernetes Service(AKS) □□□□□ □□□□ □□□□.

Azure Container Registry□ □□□□□ □□ □□□ □□□ □□□ □□□□ □□□.

□□□ □□□□ □□□?

A. Azure Active Directory(Azure AD) □□

B. Azure Active Directory(Azure AD) □□ □□

C. Azure Active Directory(Azure AD) □□□

D. Azure Key Vault□ □□

Answer: B (LEAVE A REPLY)

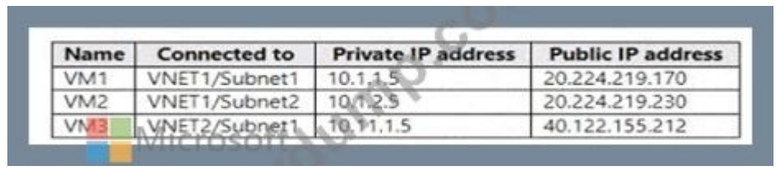
When you create an AKS cluster, Azure also creates a service principal to support cluster operability with other Azure resources. You can use this auto-generated service principal for authentication with an ACR registry. To do so, you need to create an Azure AD role assignment that grants the cluster ' s service principal access to the container registry.

References:

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

NEW QUESTION: 78

Azure AD □□□□ □□□ Azure □□□ □□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.



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

□□ □□□□□ □□□□□ □□ □□ □□□ □□□ □□□□□□ □□□□.

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

□□ □□ □□□ □□□□ □□□□□.

Name	Type
storage1	Azure Storage account
Vault1	Azure Key Vault

□□ □ □□□ □□, □□□ □□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□. □□: □□□ 1□□□□.

Answer:

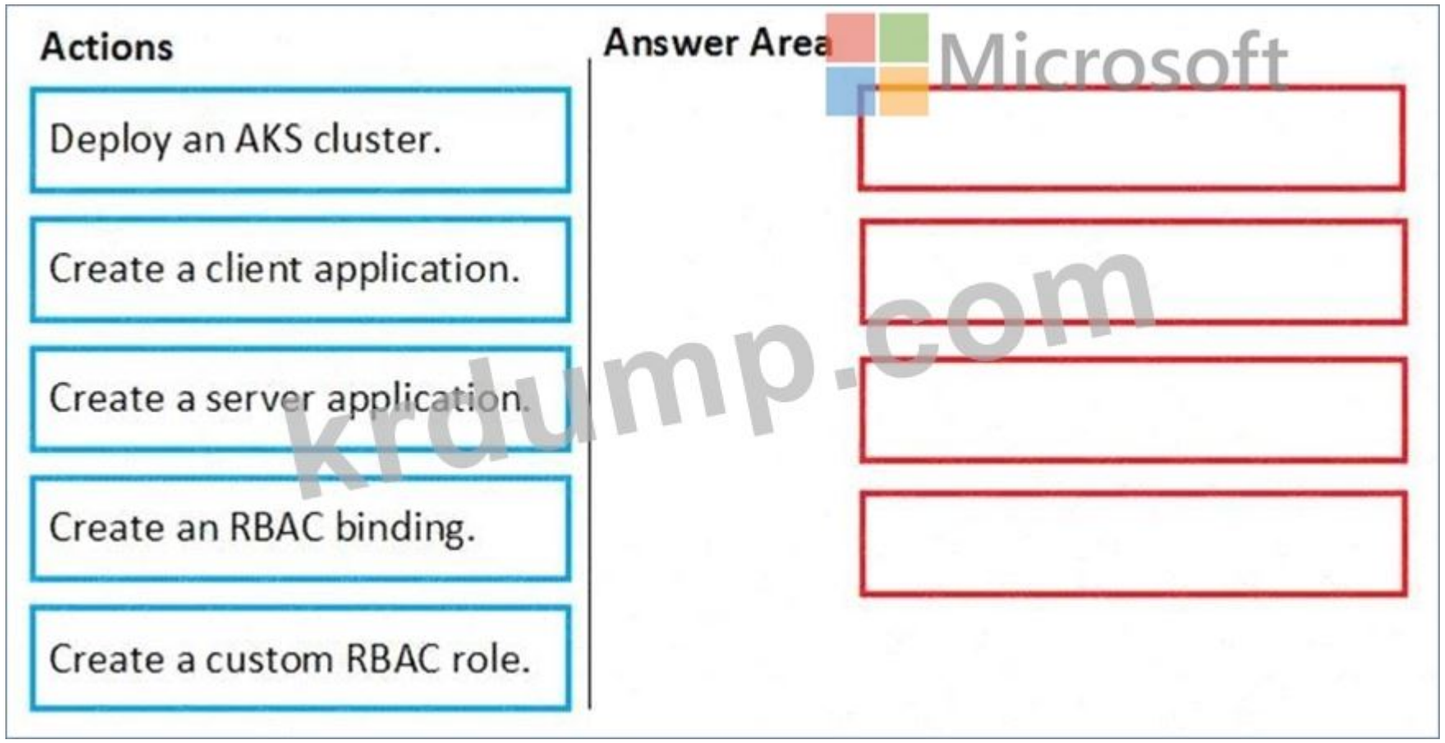
Explanation:

NEW QUESTION: 79

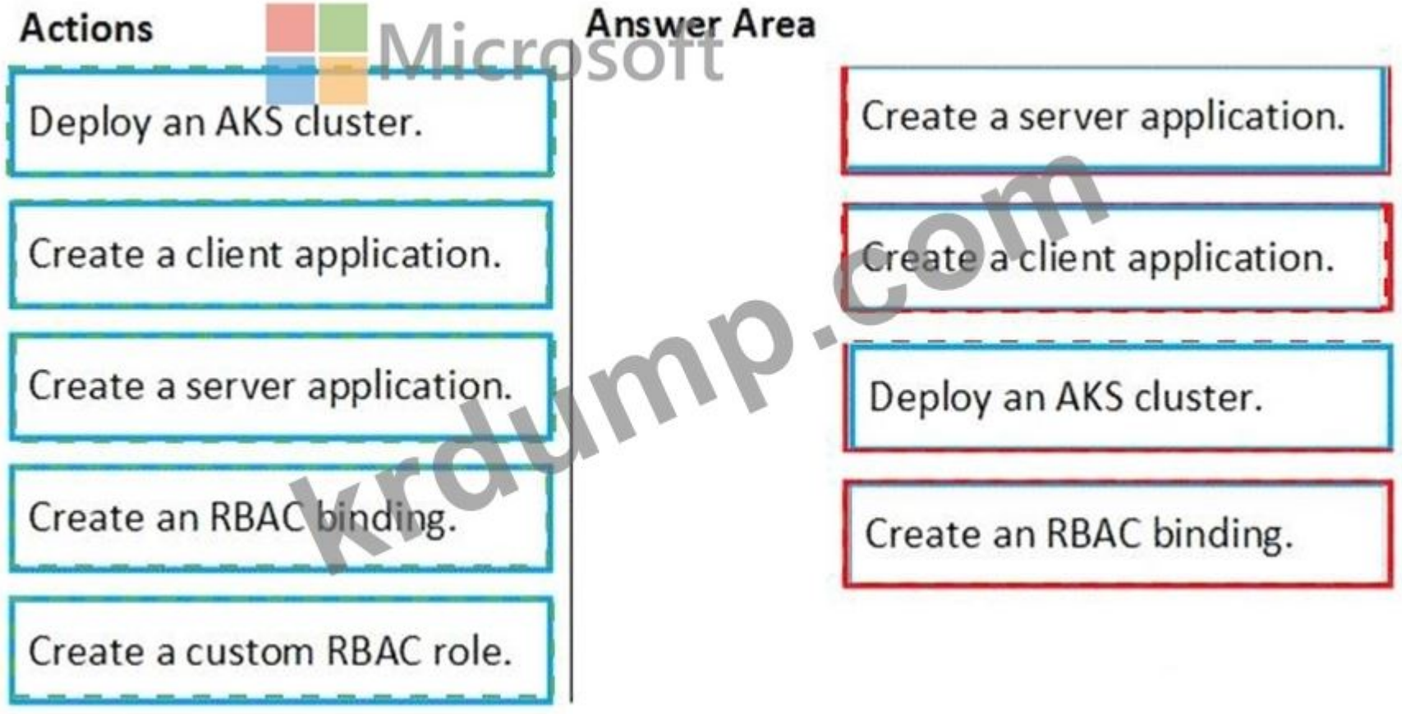
□□□ □□ □□ □□□ □□□□□ AKS1□ □□□□ □□□.

□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.

□□: □□ □□□ □ □ □□□ □ □□□□. □□ □□□ □□□□ □□ □□ □□□□ □□□□□.



Answer:



Explanation:

Scenario: Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.
Litewire plans to deploy AKS1, which is a managed AKS (Azure Kubernetes Services) cluster.
Step 1: Create a server application
To provide Azure AD authentication for an AKS cluster, two Azure AD applications are created. The first application is a server component that provides user authentication.
Step 2: Create a client application
The second application is a client component that ' s used when you ' re prompted by the CLI for authentication. This client application uses the server application for the actual authentication of the credentials provided by the client.
Step 3: Deploy an AKS cluster.
Use the az group create command to create a resource group for the AKS cluster.
Use the az aks create command to deploy the AKS cluster.
Step 4: Create an RBAC binding.
Before you use an Azure Active Directory account with an AKS cluster, you must create role-binding or cluster role-binding. Roles define the permissions to grant, and bindings apply them to desired users. These assignments can be applied to a given namespace, or across the entire cluster.
Reference:
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration

NEW QUESTION: 80
□□□□□ □□□□□□ Active Directory □□□ □□□(AD DS) □□□□ □□ □□ □□□ □□□ □□□□ □□□□.
User1□□□ □□□□ □□□□ □□□ □□□□□ Microsoft Entra □□□□ □□□□.
□□ □□ □□□ Azure Files □□□ □□□ Azure □□□ □□□□.
storage1□ storage2□ □□ □□ □□□ SMB □□ □□□ □□□ □□□□□□□.
Share!□ □□ □□□ □□ □□□ □□ □□□□□.


Security
Protocol settings
Azure Files exposes settings that let you toggle the SMB protocol to be more compatible or more secure, depending on your organization's requirements. Restricting these settings may prevent some clients from being able to connect. Learn more
Profile
Custom
SMB protocol versions
SMB 2.1
SMB 3.0
SMB 3.1.1
SMB channel encryption
None
AES-128-CCM
AES-128-GCM
AES-256-GCM
Authentication mechanisms
NTLM v2
Kerberos
Kerberos ticket encryption
RC4-HMAC
AES-256
For more information on support for protocol settings in SMB clients, see SMB on Windows and SMB on Linux
Security
Custom
SMB protocol versions
SMB 2.1
SMB 3.0
SMB 3.1.1
SMB channel encryption
None
AES-128-CCM
AES-128-GCM
AES-256-GCM
Kerberos ticket encryption
RC4-HMAC
AES-256
For more information on support for protocol settings in SMB clients, see SMB on Windows and SMB on Linux

□□ □ □□□ □□, □□□ □□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□: □□ 1□□ 1□□□□.

Answer Area

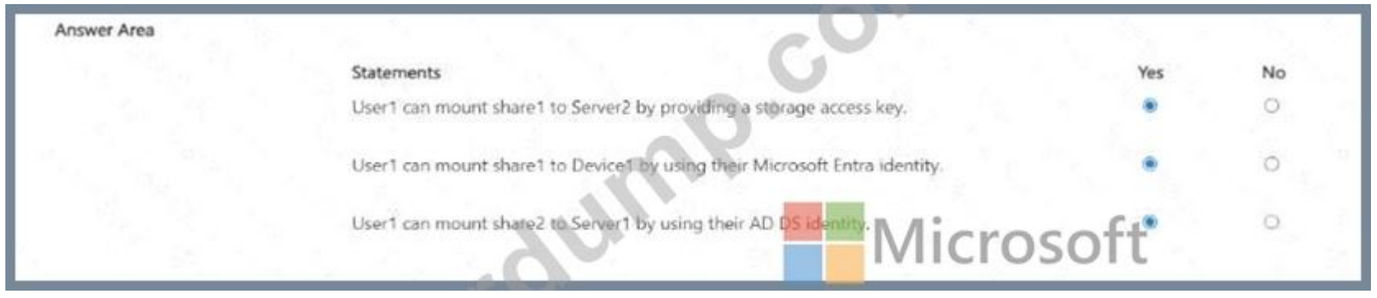
Statements	Yes	No
User1 can mount share1 to Server2 by providing a storage access key.	○	○
User1 can mount share1 to Device1 by using their Microsoft Entra identity.	○	○
User1 can mount share2 to Server1 by using their AD DS identity.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can mount share1 to Server2 by providing a storage access key.	○	○
User1 can mount share1 to Device1 by using their Microsoft Entra identity.	○	○
User1 can mount share2 to Server1 by using their AD DS identity.	○	○

Explanation:



NEW QUESTION: 81

□□□ User1□ User2□□ □ □□ □□□□ App1□□□ □□□ □□ □□ Azure Active Directory(Azure AD) □□□□ □□□□.

□□ □□□ Role1□□□ □□□□ □□□□□.

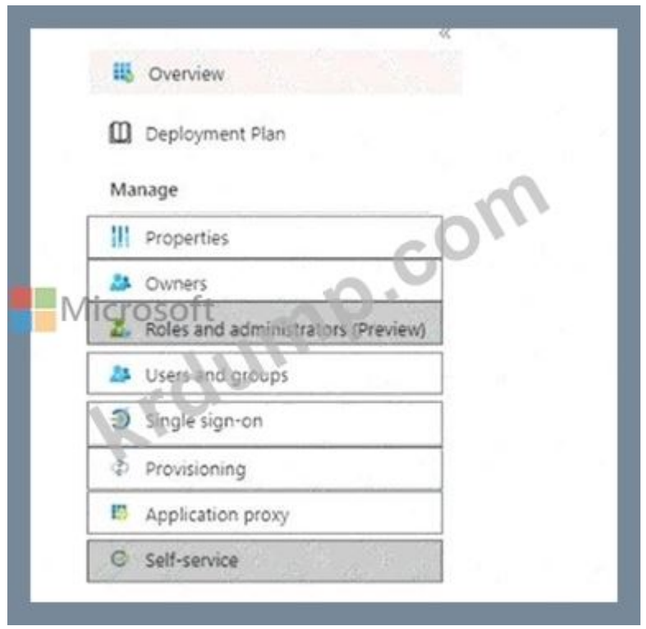
User1□□ Role1□ □□□□ User2□ App1□ □□ □□□ □□□ □□□ □ □□□ □□□□ □□□.

□□ □ □□ □□□ □□□□ □□□? □□□ □□□□□ □□□□□ □□□ □□□ □□□□. □□: □ □□□ 1□□□□.

Answer:

Explanation:

Graphical user interface, application Description automatically generated



NEW QUESTION: 82
contoso.onmicrosoft.com□□□ Azure Active Directory(Azure AD) □□□□ □□□□.
□□□ □□□ □□□ Admin1□□□ □□□□□ □□□□□.
□□ □□□□ user1@outlook.com □□□□ □□□□ Microsoft □□□ □□□ □□□□.
Admin1□ □□ □□□□ □□□□ Azure AD □□□□ □□□□□□ □□□□□ □□□ □□ □□ □□□□ □□□□□. "user1@outlook.com □□□□ □□□ □ □□□□. □□ □□ □□ □□□ □□ □□□□." Admin1□ □□ □□□□ □□□□ Azure AD □□□□ □□□□ □ □□□ □□□□ □□□.
□□□ □□ □□□?
A. □□ □ □□□ □□□□□□ Admin1□ □□ □□□ □□□ □□□□□.
B. □□ □□ □□□□□□ ID □□□□ □□□□□.
C. □□□ □□ □□□ □□ □□□□□□ □□□ □□ □□□□ □□□□□.
D. □□□ □□□□□□ □□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
You need to allow guest invitations in the External collaboration settings.

NEW QUESTION: 83
Microsoft 365 E5 □□□ □□□□.
Microsoft Defender for Cloud□ □□□□ Azure □□□ □□□□.
□□ □□ □□□ □□□ □□□ □□□□□ □□□ □□□ □□□□.
Microsoft Defender for Cloud□ □□ □□□□ □□□□□□.
□□ □□□ Defender for Cloud□ □□□□□□?
A. □□2□
B. Servei2□ Servet3
C. Server3□
D. □□1□

E. □□1, □□2, □□3
F. □□1□ □□3
Answer: (SHOW ANSWER)

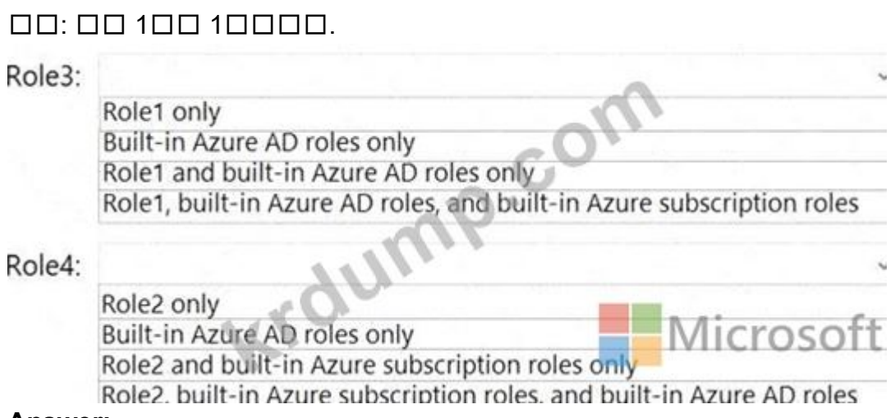
NEW QUESTION: 84
□□ □□ □□□ □□□ □□ □□□ □□□ Azure □□□ □□□□.

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

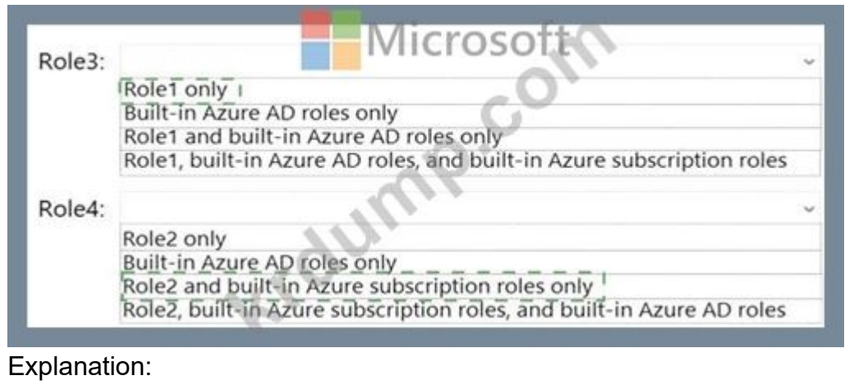
Azure Portal□□ □□ □□□ □□□□ □ □□□ □□ □□□ □□ □□□□□. □ □□□ □□ □□ □□ □□□□□.

Name	Type
Role3	Azure AD
Role4	Azure subscription

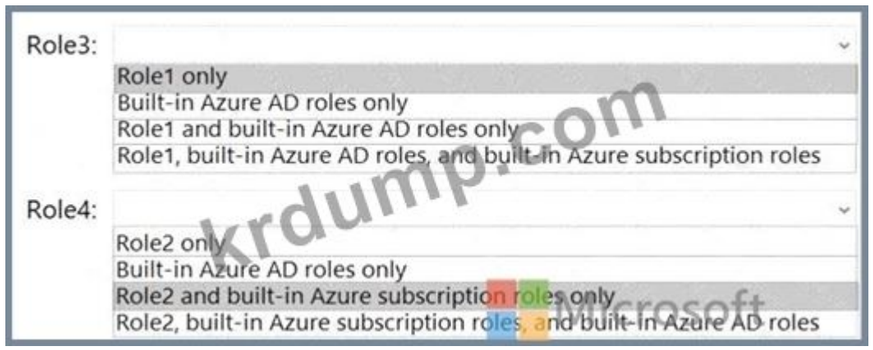
□□ □□□ □□□□ □□□ □□□ □□ □ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.



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: 85
Azure Sentinel □□ □□□ □□□ Azure □□□ □□□□.
Azure Sentinel□ □□ Azure □□□□□ □□□ □□□□□ □□□□ □□□□. □□□□ □□□□ □□ □□□ □□ □□□□ □□□□□.
□□ □□ □□□ □□□□□ □□□ Azure Sentinel □□ □□□ □□□□ □□□.
* Azure Sentinel□ □□□ □□□□ □□□□□ □□□□ □□□.
* Azure Sentinel□□ □□□□□ □□□□ □□□ □□ □□□□ □□□ □□□□ □□□.
□ □□ □□□ □□ □□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.

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: 86
□□□□2□ □□ □□□ □□ □□□ □□□□ □□□. □□□□ □□□□ □□□□ □□ □□ □□ □□□ □□□□ □□□.
A. □□ □□□ □□ □□□□□ storage2□ □□□□□.
B. storage2□ □□□ □□□ □□□□□.
C. storage2□ Azure □□ □□ □□□ □□(Azure RBAC) □□□ □□□□□.
D. storage2□ □□ □□ □□□ □□□□□□.
Answer: B (LEAVE A REPLY)

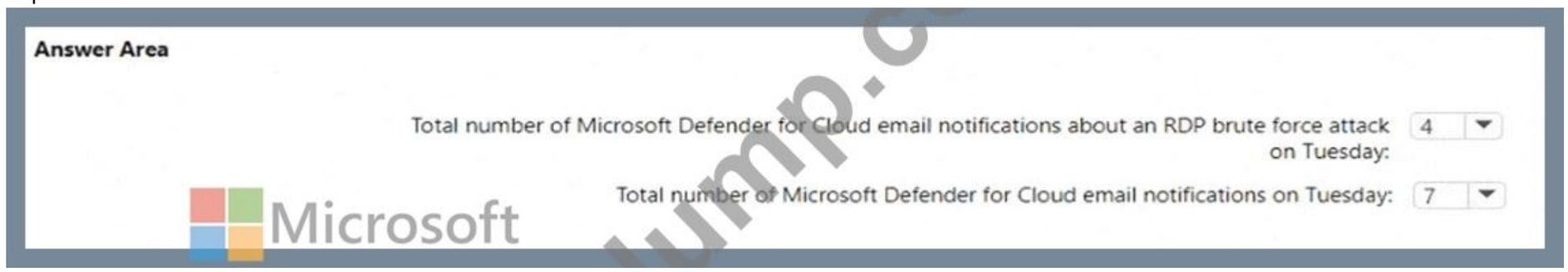
NEW QUESTION: 87
□□□□ Microsoft Defender for Cloud□□ □□□ □□□ □□□□ user1 @contoso□□ □□□□.
□□□□ □□, □□, □□□ □□□ □□ □□□ com□□ □□□□□. □□□, Microsoft Defender for Cloud□ □□ □□ □□□ □□ □□□ □□□□□.

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

user1@contoso.com□ □□□□ □□□ □□□ □ □ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□. □□: □□ □□□ 1□□□□.

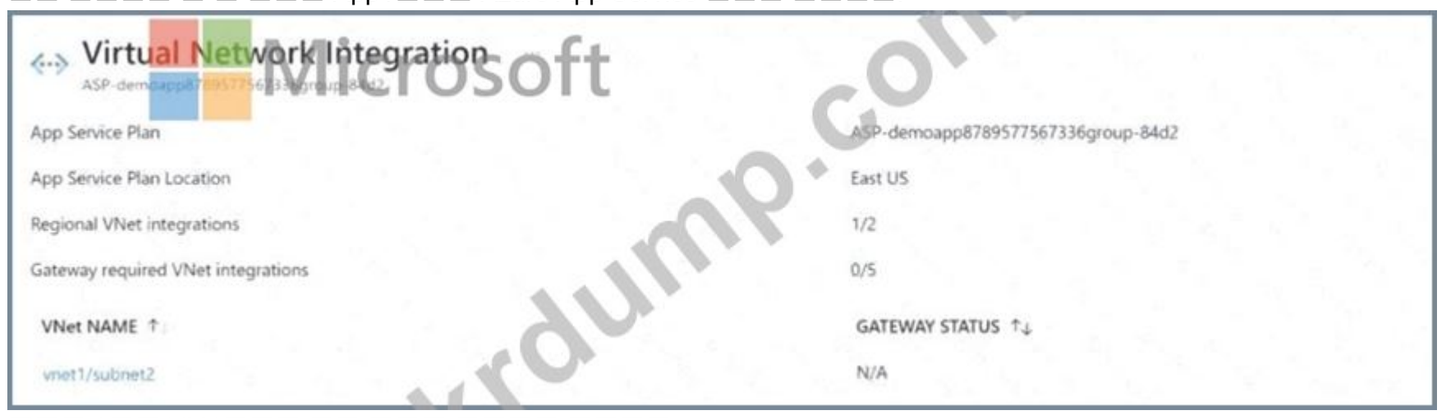
Answer:

Explanation:



NEW QUESTION: 88

□□ □□□□ □ □ □□□ App1□□□ Azure App Service □□□ □□□□.



□□□ 2□□ VM1□□□ □□ □□□ □□□□ □□□□.

□□□□ □□□ □□□□ □□□□ □□□ □□□ □□□□ □ □□□ □□□□ □□ □□□ □□□□□. □□: □□ □□□ 1□□ □□□□□.

Answer:

Explanation:

NEW QUESTION: 89

Azure □□□ □□□□.

Azure Security Center□□ □□ □□□□ □□□□ □□□□ □□□□ □□□□ □□ □□□□□.

□□ □□ □□□ □□□□ □□□?

A. □□□□ ID

B. □□□ □□

C. Azure □□ □

D. □□ □□

E. Azure □□ □

Answer: E (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 90
Vault1□□□ □□□ Azure Key Vault□ □□□ Azure □□□ □□□□.
Vault1□□ Secret1□□□ □□□ □□□ □□□□□.
□□□□□□ □□□□ Azure Active Directory(Azure AD)□ □□□□□□□ □□□□□.
□□□□□□□ Secret1□ □□□ □ □□□ □□□□ □□□.
□□□ □□ □□□?
A. Azure AD□□ □□□ □□□□.
B. Azure Key Vault□□ □□ □□□□.
C. Azure Key Vault□□ □□□ □□□ □□□□.
D. Azure AD□□ Azure AD □□□□□□ □□□□ □□□□□□.
Answer: C (LEAVE A REPLY)
" You may need to configure the target resource to allow access from your application. For example, if you request a token to Key Vault, you need to make sure you have added an access policy that includes your application ' s identity. Otherwise, your calls to Key Vault will be rejected, even if they include the token "
https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet

NEW QUESTION: 91
Azure □□□ RG1□□□ □□□ □□□ □□□□. RG1□□ storage1□□□ □□□□ □□□ □□□□.
RG1□ □□□ □□□ Role1 □ Role2□□ □ □□ □□□ □□ Azure □□□ □□□□.
Role1□ □□ □□□ □□ JSON □□□ □□ □□□□.

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


Role2□ □□ □□□ □□ JSON □□□ □□ □□□□.

Name	Role
User1	Role1
User2	Role2
User3	Role1, Role2

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 92

Azure Active Directory(Azure AD) □□□□ User1□□□ □□□□ □□□ Azure □□□ □□□□.

□□□□ □□ □ □□ □□□ □□ □□ □□□ □□ □□□□□.

App1□□□ □□ □□□ □□□□□.
User1□ Azure AD□ App1□ □□□ □ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
User1□□ □□ □□□ □□□□ □□□?
A. □□□ □□ □ □□ □□□ □□□
B. □□□ □□ □□□ □□□□□□ □□□
C. Azure AD□ □□□□ □□□□□□ □□□
D. Azure AD□ □□□□□□ □□□.
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task

NEW QUESTION: 93
Azure □□□ □□□□ □□ □□□□ □□□□ □□□□.
□□□ □□ □□□ □□□ □□□ □□□ □□ Azure □□ □□□ □□ □□□□ □□□□ □□□.
□□□□ □□□□ □□ □□□□ □□□□ □□ □□□ □□□□ □□□□ □□ □□□.
□□□ □□□□ □□□?
A. Azure □□□
B. Azure □□□ □□
C. Azure □□
D. Azure □□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 94
□□□ weylandindustries.com□□□ □□ □□□□ □□□□ Active Directory □□□□□ □□□□ □□□□. □□ □□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□.
□+□□□□ ID□ □□ Azure AD□ □□□□ □, LAB□ □□□□ givenName □□□ □□ □□□□ Azure AD□ □□□□ □ □□□ □□□ □□ □□□.
□□ □ □□ □□□ □□□ □□□?
A. □□□ □□ □□□□ □□□□ □□ □□ □□□ □□□ □□□□ □□□.
B. □□□□□ DNAT □□□ □□□□ □□□.
C. □□□□□ □□□□ □□□ □□□ □□□ □□□□ □□□.
D. Active Directory □□□ □ □□□□ □□□□ □□ □□ □□□ □□□ □□□□ □□□.
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: 95

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□,
□□ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
Azure □□□ □□□□. □ □□□□ Windows Server□ □□□□ 50□□ □□ □□□ □□□□ □□□□.
2012 R2 □□ Windows Server 2016.
□□ □□□ Microsoft Antimalware□ □□□□ □□□.
□□ □□: □ □□ □□□ □□□□ Windows □□□ □□□□□.
□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

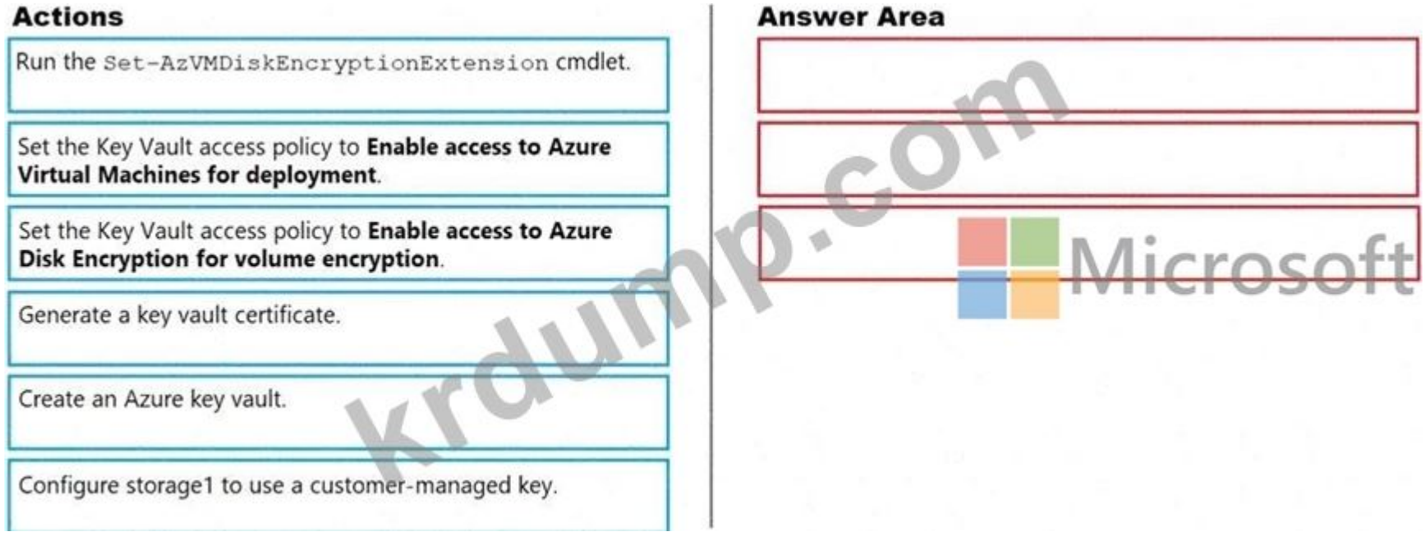
Microsoft Antimalware is deployed as an extension and not a feature.

References:

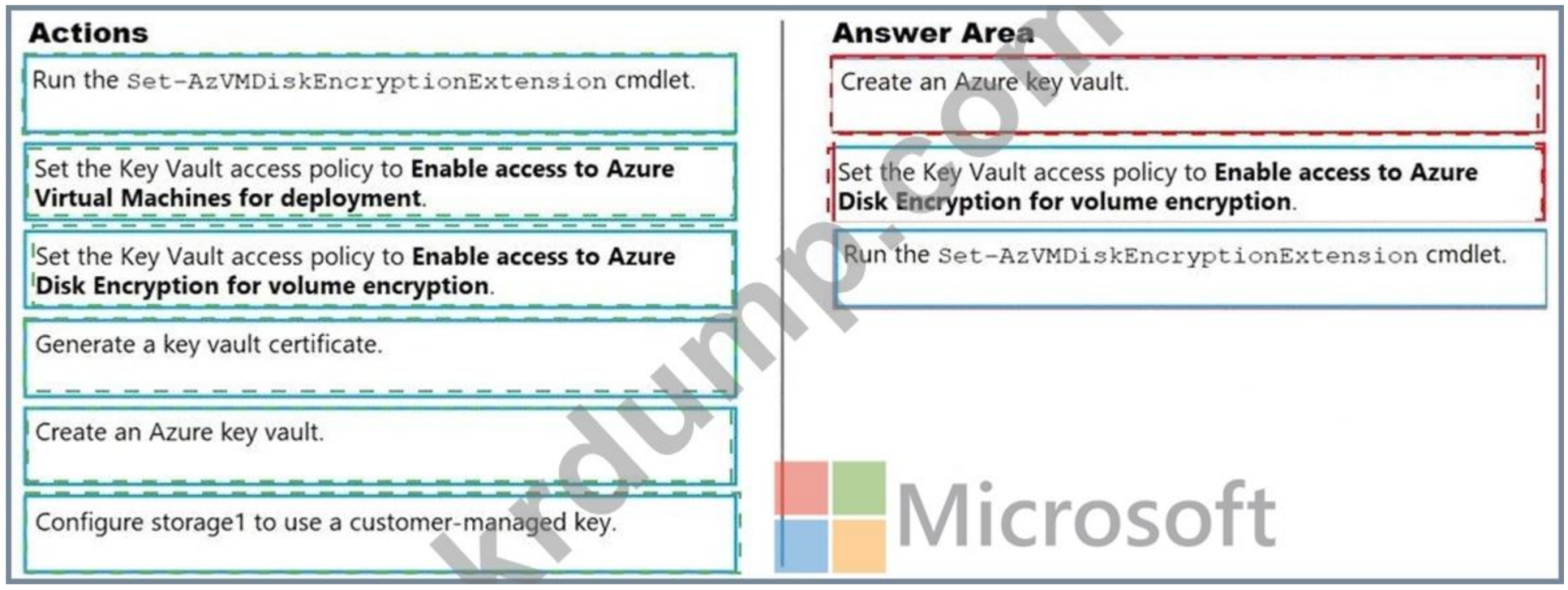
https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

NEW QUESTION: 96

storage1□□□ Azure Storage □□□ VM1□□□ Azure □□ □□□ □□□□. VM1□□ □□□□ SSD □□ □□□□ □□□□.
VM1□ □□ Azure Disk Encryption□ □□□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

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

NEW QUESTION: 97

□□□ Sub1□□□ Azure □□□ □□□□. Sub1□□ Azure Application Insights□ □□□□ WebApp1□□□ Azure □□□ □□□□ □□□□. WebApp1□ □□□□□ □□□□ OAuth 2.0 □□□□ □ □□□□□ □□□□ □□□□ □□□.

□ □□□ □□□□□ □ □1□ □□ □□□ □□□□ □□□□□□□ □□ □□□□□ □□□□ □□□ □ □□□ □□ □□ □□□□□.

□ □□□□ □□□□ □□□ □ □□□ □□ □□□.

□□ □□ □□□ □□ □□□?

A. Microsoft Visual Studio□□ .webtest □□□ □□□□□.

B. .webtest □□□ Application Insights□ □□□□□□.

C. Azure AD□ □ □□□ □□ □□□□□.

D. □ □□□ □□ □□□□□ □□□□□.
Answer: (SHOW ANSWER)
https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep

NEW QUESTION: 98
RG1□□□ □□□ □□□ Azure □□ □□□ 15□ □□□□.
□□ □□ □□□ □□□ □□□□□□□ □□□□□.
□□ □□□□ □□□□ □□ □□□□□□□ □□□□ □□□□ □□ □□□□ □□□.
□□□ □□ □□□?
A. Azure Active Directory(Azure AD) ID □□□ □□□□□.
B. Microsoft Defender for Cloud□□ □□□ □□□□□□ □□□ □□□□□.
C. RGI□ Azure □□□ □□□□□.
D. 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

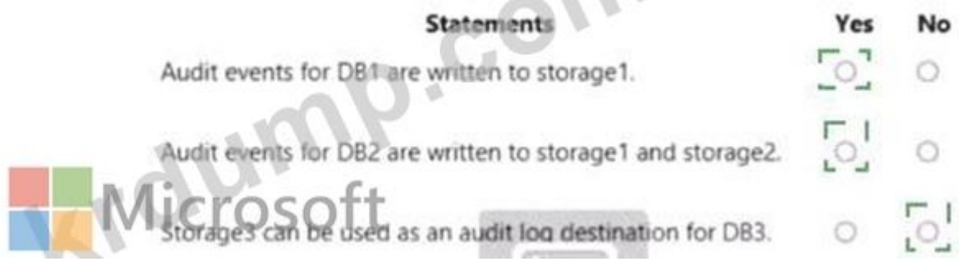
NEW QUESTION: 99
User1□□□ □□□□ □□□ Microsoft Entra □□□□ □□□□.
□□□□ □□ □□ □□ □□□ □□□□ □□□□□.
User1□ □□ □□ □□□ □□□□ □ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
User1□□ □□ □□□ □□□□ □□□?
A. □□ □□□
B. □□□ □□ □□ □□□
C. □□ □□□
D. □□□ □□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 100
Vault1□□□ Azure Key Vault□ VM1□□□ □□ □□□ □□□ Azure □□□ □□□□. VM1□□ Key Vault VM □□□ □□□□ □□□□.
Vault1□ □□ □, □□, □□□□ □□□□□.
VM1□ □□□□ □□□□□□ □□□ □□□□□?
A. □□ □□□
B. □, □□ □ □□□
C. □□

D. □□□
E. □□□ □□□□
F. □□□□
Answer: F (LEAVE A REPLY)

NEW QUESTION: 101
□ □□ □□□ □□, SQL□□□ □□□ Azure SQL □□□ □□□□, □□□ □ □□ Azure SQL □□□□□□□ □□□ Azure □□□ □□□□. □□□ □□□ □□ □□ □□ □□□□ □□□□.
SQ11□ □□□ □□□ □□□□.
* □□: □□
* □□ □□: storage1
Azure SQL □□□□□□□ □□ □□ □□ □□□□□.

Answer:
Answer Area



Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/auditing-configure
https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview

NEW QUESTION: 102
Azure Firewall Standard□ AzFWL □□□□□ □□□ Azure □□□ □□□□. AzFW1□□ □□ □□□ □□□ □ □□□ □□□□ □□□.
* TLS □□
* □□ □□□□□
* □□□□ □□ □□ □ □□ □□□(IDPS)

□□□ □□□ □ □□□?
A. TLS □□□ □□
B. □□ □□□□□ □ IDPS□
C. TLS □□ □ IDPS□
D. TLS □□, □□ □□□□□ □ IDPS
E. □□ □□□□□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 103
□□: □ □□□ □□□ □□□ □□ □□ □□ □ □□□ □□□□ □□□□. □□□ □ □□□□ □□□ □□□ □□□□. □□ □□ □□□ □□□□□ □□□□□.
□□□ weylandindustries.com□□□ □□ □□□□ □□□□ Active Directory □□□□□ □□□□ □□□□. □□ □□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□.
Active Directory□ Azure AD □□□□ □□□□ □□□ □□□□□. Azure AD Connect□ □□□□□ □□□.
□□□ □□ □□□□□ □□ □□□ □□□ □□□ □□□ Azure AD □□□□ □□□□ □□□ □□□ □□□ □□□ □□□ □□ □□ □□□□□ □□ □□□.
□□□: □□□□ □□ □□□□ □□□ SSO□ □□□□ □□ □□□□.
□□□□ □□□ □□□□□?
A. □□□
B. □
Answer: A (LEAVE A REPLY)

NEW QUESTION: 104
□□□ □□
□□□ □□ □□ □□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□ □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
□□□□□ □□□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□□□.
Azure □□□ □□: Userl -28681041@ExamUsers.com
Azure □□□□: GpOAe4@lDg
Azure Portal□ □□□□□ □□□□□ □□□□ □□□ CTRL-K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
□□□ □□□□: 28681041
□□ 10
28681041.onmicrosoft.com□□□ □ Azure AD □□□□□ □□□□ □□□. □ □□□□□□ user1@28681041.onmicrosoft.com□□□ □ □□□□ □□□ □□□.
Answer:
Check below steps in explanation for Task.
Explanation:
To create a new Azure AD directory named 28681041.onmicrosoft.com that contains a new user named user1@28681041.onmicrosoft.com, you can follow these steps:
* In the Azure portal, search for and select Azure Active Directory.
* In the left pane, select Domains.
* Select Add domain.
* In the Add a custom domain pane, enter the following information:
* Domain name: Enter the domain name you want to use. For example, 28681041.onmicrosoft.com.
* Add domain: Select Add domain.

* In the left pane, select Users.
* Select New user.
* In the New user pane, enter the following information:
* User name: Enter the user name you want to use. For example, user1@28681041.onmicrosoft.
com.
* Name: Enter the name of the user.
* Password: Enter a password for the user.
* Groups: Select the groups you want the user to be a member of.
* Select Create.
You can find more information on these topics in the following Microsoft documentation:
* Add a custom domain name to Azure Active Directory
* Create a new user in your organization - Azure Active Directory

NEW QUESTION: 105
□□ □□ □□□ □□ □□□ □□□ Azure □□□ □□□□.

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

□□ □□ □□□□□ □□□□□□.
Azure Bastion□ VNET2□ □□□□□.
□□ □□ □□□ □□□ □□□□ □□□ □ □□□?
A. VM1, VM2, VM3 □ VM4
B. VM1, VM2 □ VM3□ □□
C. VM2 □ VM4□ □□
D. VM2□ □□
Answer: A (LEAVE A REPLY)
https://docs.microsoft.com/en-us/azure/bastion/vnet-peering

NEW QUESTION: 106
App1□□□ □□ □□□ Azure □□□ □□□□. App1□□ □□ □□ □□ □□ □ □□□ □□□□.

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

App1□ □□ □□□ □□□□ □□ □□□ □□□ □ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
□□□ □□ □□□?
A. Microsoft.Graph Calendars.ReadWrite□ □□ □□□ □□ API □□□ □□□□□.
B. Microsoft.Graph Calendars.ReadWrite□ □□ □□□ □□□□□□ API □□□ □□□□□.
C. □□□ □□ □□□ □□□□□.
D. Microsoft.Graph Calendars.ReadWrite.Shared□ □□ □□□ □□ API □□□ □□□□□.

Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/graph/permissions-reference#calendars-permissions

NEW QUESTION: 107
□□ □□ □□ □□ □□□□ □□□□ Vault1□□□ Azure Key Vault□ □□□□.

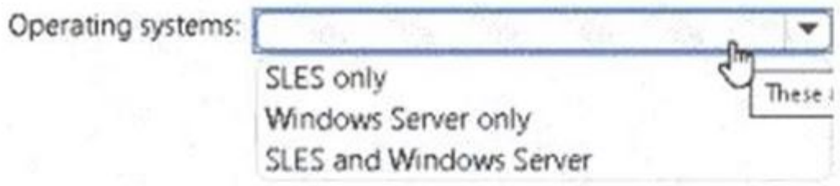
Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

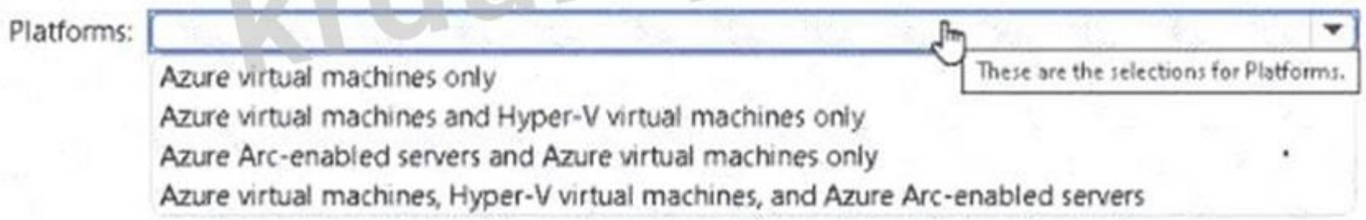
□□ □□□□ □□ □□ □□□ □□□□□?
A. □ 1□
B. Cert1□
C. Key1 □ Cert1□
D. Secret1 □ Cert1□
E. Key1, Secret1 □ Cert1
F. Key1□ Secret1□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 108
□□□□□ □□□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

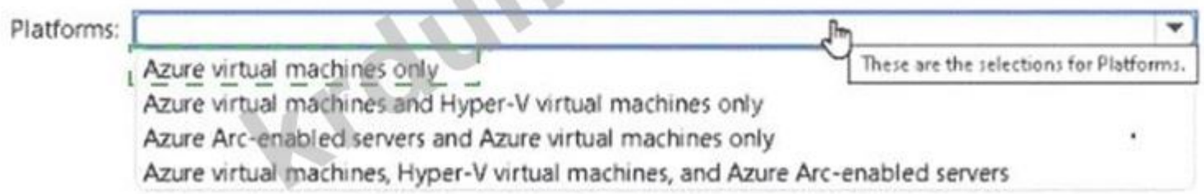
Name	Operating system	Description
Server1	Windows Server 2019	Hyper-V host hosting four virtual machines that run Windows Server 2022
Server2	Windows Server 2019	File server that has the Azure Arc agent installed
Server3	SUSE Linux Enterprise Server (SLES)	Database server that has the Azure Arc agent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

Windows Server 2019 □□ SLES□ □□□□ □□ □□ □□□ □□□ Azure □□□ □□□□. Microsoft Defender for Cloud□□ □□□ □□□□□□ □□□ □□□ □□□□□. □□ □□ □□□ □ □□□ □□□□□ □ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.





Answer:



NEW QUESTION: 109

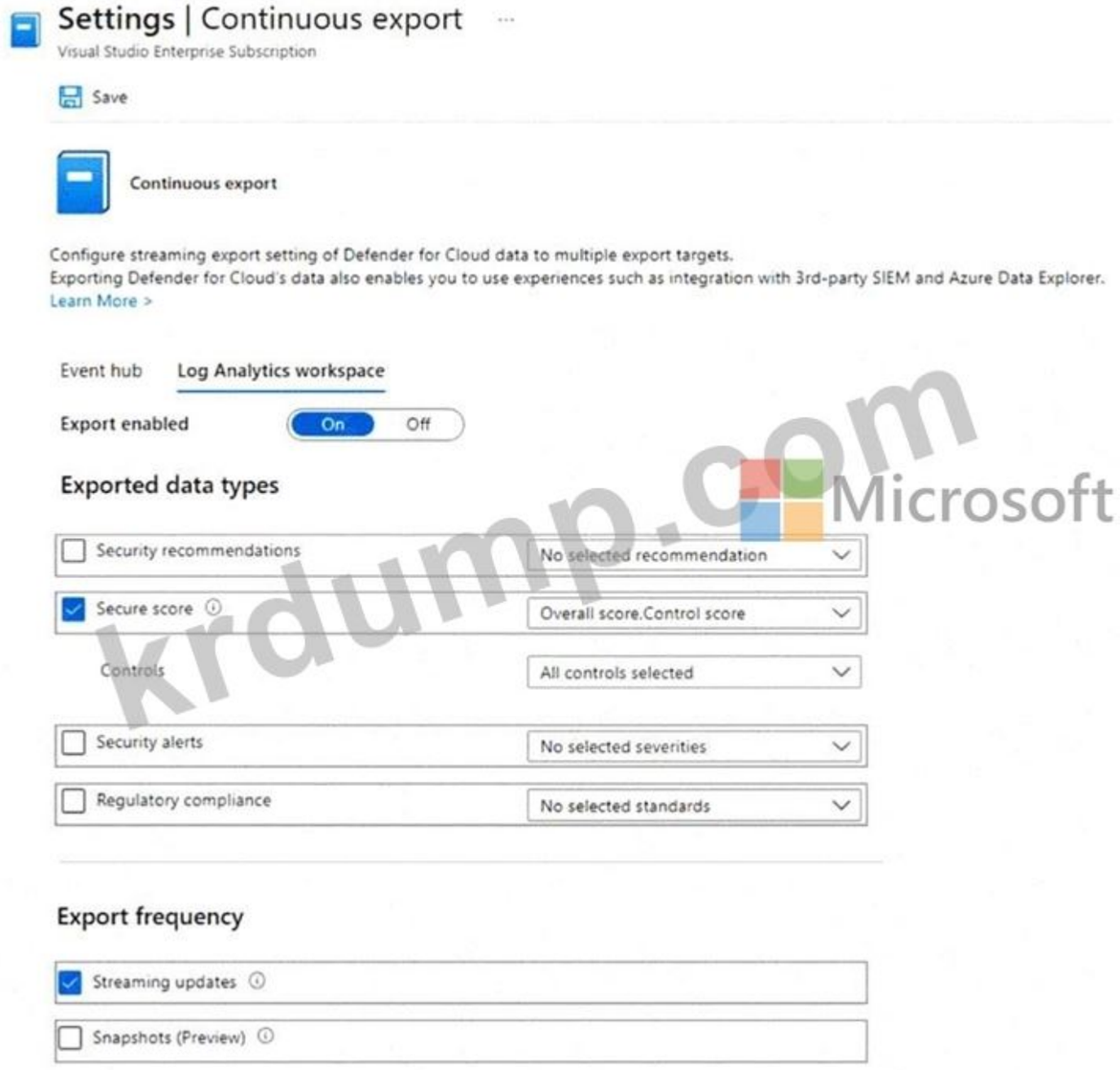
Microsoft Defender for Cloud□ □□□□ Azure □□□ □□□□.

□□ □□□ □□ □□ □□ □□□□ □□□ □□□□□.

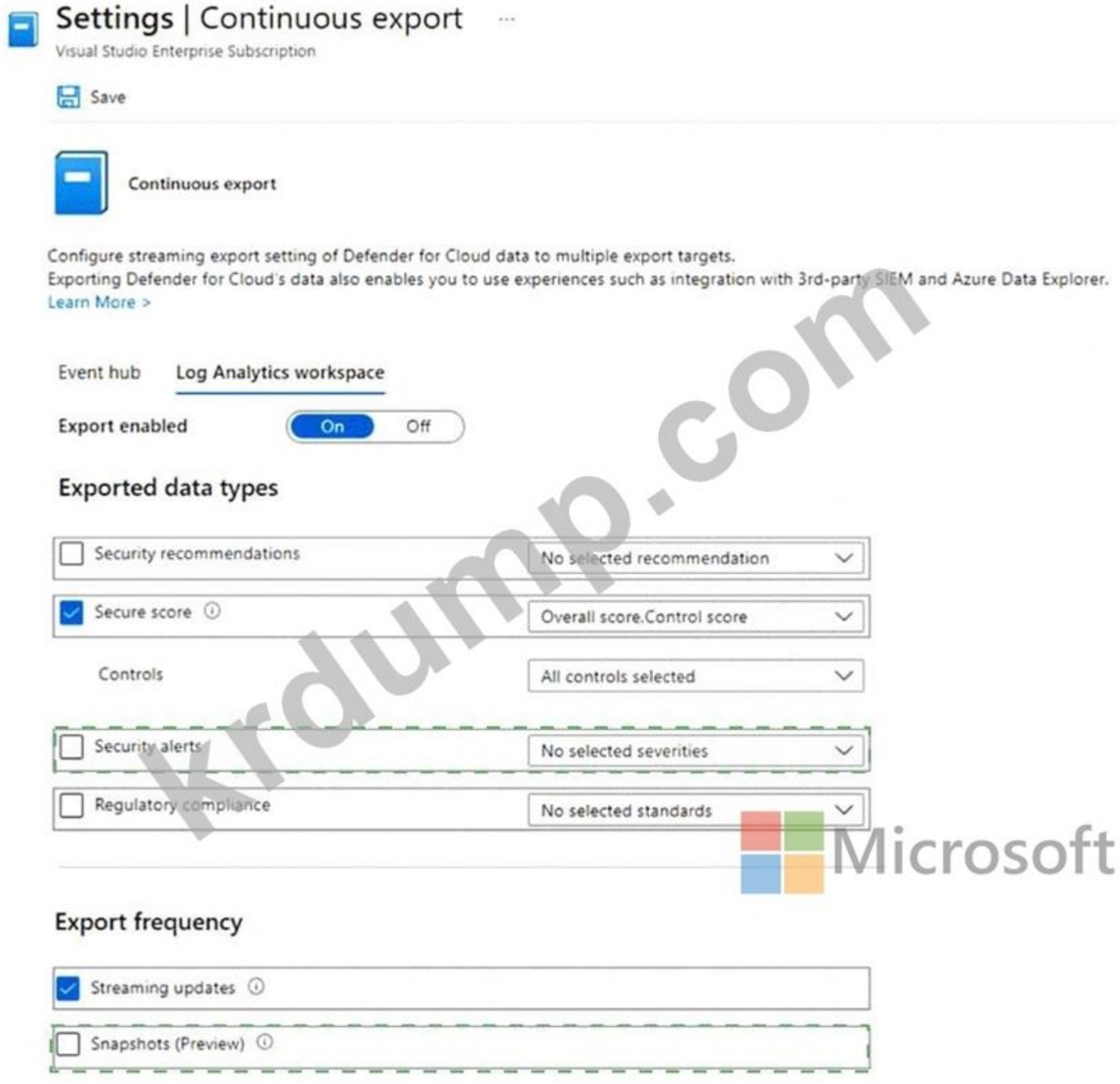
Defender for Cloud □□□□ □□ □□□□ □□□□ □□□ □□□□ □□□.

□□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

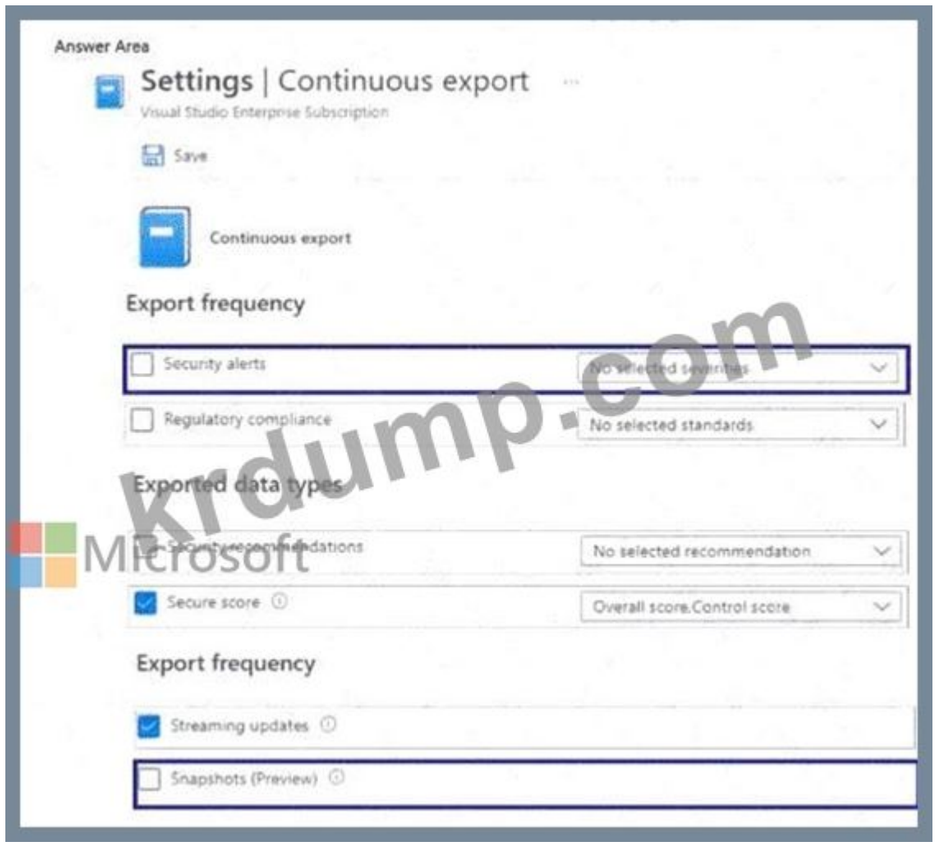
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 110

□□ □□ □□□ □□□□ □□□ contoso.com□□□ Microsoft Entra □□□□ □□□□.

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

□□ □□ □□□ □□ contoso.com□ □□□□□□ □□□□□□□ □□□□□.

Name	Owner	Users and groups
App1	User3	User4
App2	User4	User3

App1□ App2□ □□ □□□ □□□ □□□ □ □□ □□□□ □□□□ □□□.

Answer:

Explanation:

NEW QUESTION: 111

Sub1□□□ Azure □□□ □□□□. Sub1□□ VNet1□□□ □□ □□□□□ □□□, □ □□ □□□□□□ Subnet1□□□ □□□ □□□ □□□□.

Subnet1□□ Ubuntu Server 20.04□ □□□□ VM1□□□ Azure □□ □□□ □□□□ □□□□.

Microsoft□ □□ □□□ □□□□□□ □□□□. Subnet1□ □□□□ □□□□.

Docker □□□□□ VM1□ □□□ □ □□□□□ □□□ □□□□□□ □□□□ Azure Storage □□□□ □□□□ □ □□□ □□□□ □□□.

□□□□□ □□□□ □□ VM1□□ □□□ □□ □□□?

A. □□□□ □□□□ □□□□□(CNI) □□□□□ □□□□□.

B. □□□□□□ □□ □□□ □□□□ □□ □□(NSG)□ □□□□□.

C. docker-compose.ym1 □□□ □□□□□.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 112

□□ □□ □□□ □□ □□□ □□□ Azure □□□ □□□□.

Name	Azure region	Connected to	Associated network security group (NSG)
VM1	West US	VNET1/Subnet1	None
VM2	West US	VNET1/Subnet2	NSG2
VM3	Central US	VNET2/Subnet1	NSG3
VM4	West US	VNET2/Subnet1	NSG4

VNET1, VNET2, VNET3□ □□ □□□□□ □□□□. □□ □□□ □□□□□.

* □□ □□ □□□ ASG1□ ASG2□□ □ □□ □□□□□□ □□ □□□ □□□□.

* VM1□ □□□□ □□□□□□ ASG1□ □□□□□.

Answer:

see the answer below in explanation.

Explanation:

Answer as below.

NEW QUESTION: 113

contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□□ Sub1□□□ Azure □□□ □□□□.

□□□□ □□□ □□□ □□□ □□□□□□□. Azure Security Center □□□ □□□ □□□ □□□□.

□□□ □□ □□□ □□□ □□□□ □□□.

□□ □□ □□□ □□ □□□?

A. □□□ □□ □□ □□ □□□ □□□□.

B. Azure AD□□ □□□ □□□□ □□□ □□□ □□□□.

C. □□ □□□ □□ □□□ □□□□ □□□□□□□□.

D. Microsoft Cloud App Security□□ □□□ □□□□□□.

Answer: A (LEAVE A REPLY)

First, you need to create a new sensitive information type because you can ' t directly modify the default rules.

References:

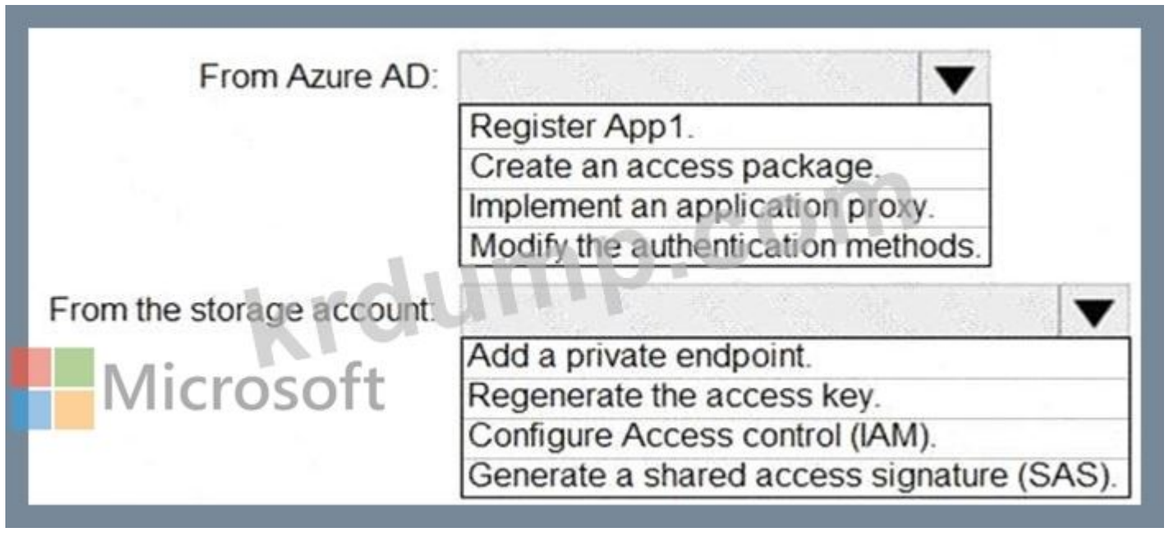
https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information- type

NEW QUESTION: 114

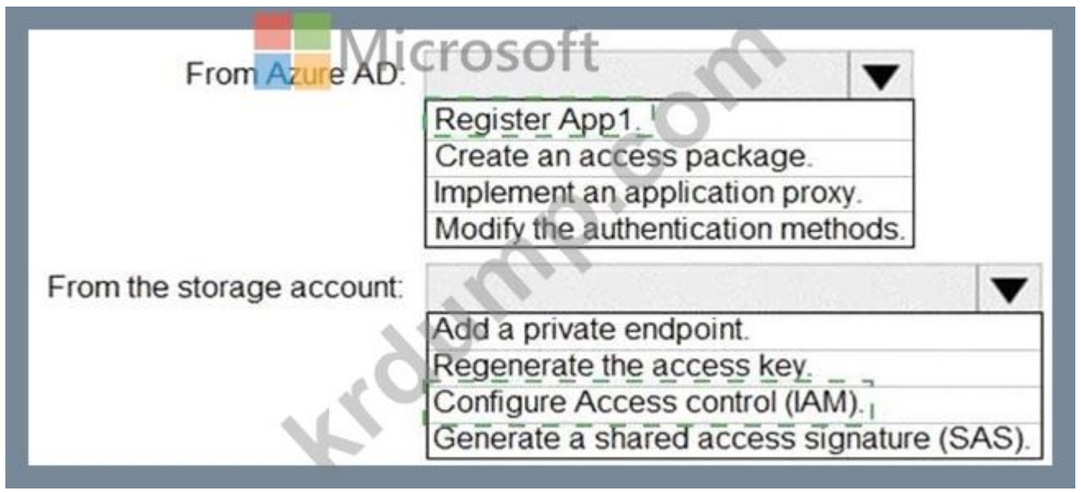
container1□□□ □□□ Blob □□□□□ App1□□□ □□□ □□□□□ □□□□□□□ □□□ Azure Storage □□□ □□□□.

Azure Active Directory(Azure AD) □□□ □□□□ App1□ container1□ □□□□ □ □□□ □□ □□□.

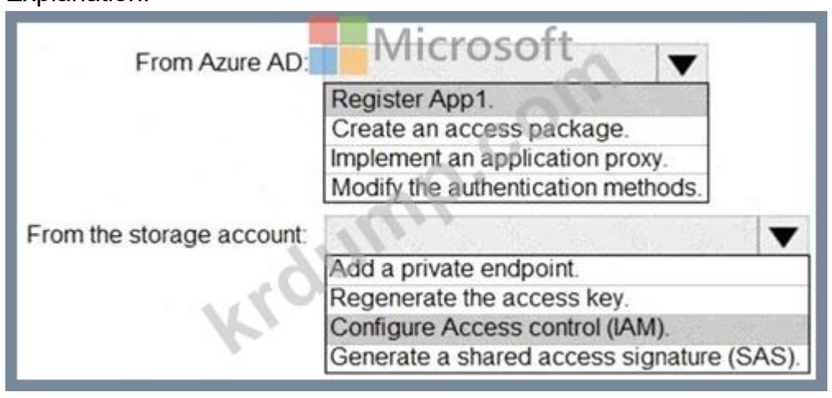
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□□ □□□□□.
□□: □□ 1□□ 1□□□□.



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: 115

Azure □□□ □□□□. □□ □□□□ □□ □□ □□ □□ □□□□ □□□□ VNet1□□□ □□ □□□□□ □□□□ □□□□.

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

□□□□ □□ □□ □□□ □□ □□ □□□□ □□□□.

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

NSG1□ □□□□ □□ □□ □□□□□ □□□□ □□□□□?

A. App4□ □□

B. App2, App3, App4□ □□

C. App3 □ App4□ □□

D. App1, App2, App3, App4

Answer: D (LEAVE A REPLY)

NEW QUESTION: 116

□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

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

APL1□□□ Azure Private Link □□□□ □□□ □□□□□.

APL1□ □□ □ □□ □□□□ □□□□ □□□?

A. SQL

B. LB1

C. VM1

D. VMSS1

Answer: B (LEAVE A REPLY)

NEW QUESTION: 117

□□□ □□

□□□ □□ □□ □□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□ □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
□□□□□ □□□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□□□.
Azure □□□ □□: Userl -28681041@ExamUsers.com
Azure □□□□: GpOAe4@lDg
Azure Portal□ □□□□□ □□□□□ □□□□ □□□ CTRL-K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
□□□ □□□□: 28681041
□□ 7
VM1□□□ □□ □□□ □□ □□□□ □□ □□ □□ □□□□ Azure Storage □□□□ □□□□ □□□. □ □□□ □□□□□ Azure Portal□ □□□□□□.
Answer:
Check below steps in explanation for Task.
Explanation:
To collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account, you can follow these steps:
* In the Azure portal, search for and select the virtual machine named VM1.
* In the left pane, select Diagnostic settings.
* Select Add diagnostic setting.
* In the Add diagnostic setting pane, enter the following information:
* Name: Enter a name for the diagnostic setting.
* Destination: Select Storage account.
* Storage account: Select the storage account you want to use.
* Logs: Select Windows Event Logs.
* Categories: Select Security.
* Event types: Select Audit Failure.
* Select Save.

NEW QUESTION: 118
□□ □□ □□□ □□ □□□□□ □□□ □□□ □□□□.
Azure □□□ □□□□.
□□□□□ □□□□ □Ł□□□□ □□□ Microsoft Defender for Cloud□ □□□□ □□□□□.
Microsoft Entra □□ □□□ □□ □□ □□□□□ □□□□□ ID□ □□□□ □□□.
□□ □□□ □□□□□□ □□□□ □□□?
A. □□ □□
B. □□□ □□
C. □□□□ □□□ □□ ID
D. □□□ □□
E. □□□□□ □□□ □□ ID
Answer: D (LEAVE A REPLY)

NEW QUESTION: 119
Azure □□□ □□□□.

□□□ □□ □□□ □□ □□ □□ □□□ □□(RBAC) □□ □□□ □□□□.

```
{
    "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": []
            }
        ]
    }
}
```

□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□□□: □□ 1□□ 1□□□□.

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:

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.	○	○

Explanation:

NEW QUESTION: 120

Azure Active Directory(Azure AD) □□□□ □□□ Azure □□□ □□□□.

Azure Portal□□ □□□□□□ □□□□□□□ □□□□□.

Azure AD□□ □□ □□ □□□□ □□□□□?

A. □□□ □□

B. X.509 □□□

C. □□□□ ID

D. □□□ □□

Answer: A (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 121

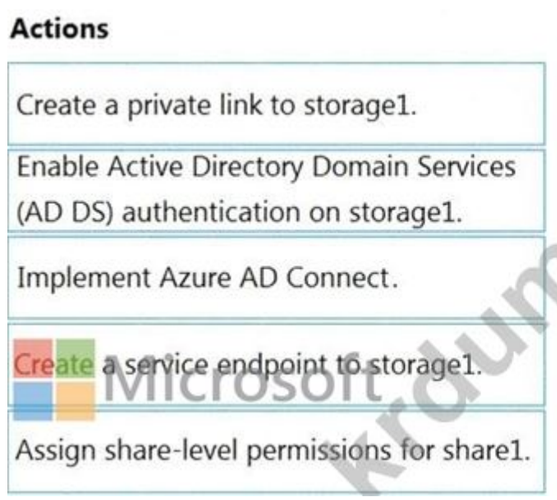
□□□□□ contoso.com□□□ □□□□□ Active Directory □□□□ □□□□. □ □□□□□ User1□□□ □□□□ □□□□.

contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□□ Azure □□□ □□□□. □□ □□□□□ storage1□□□ Azure Storage □□□ □□□□ □□□□. Storage1□□ share1□□□ Azure □□ □□□ □□□□ □□□□.

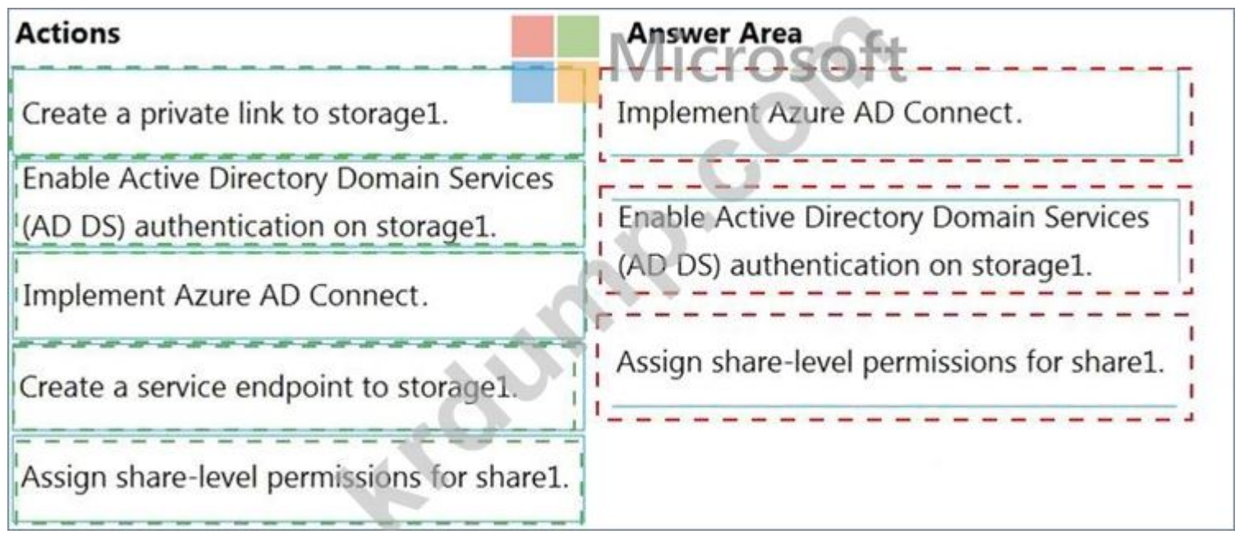
□□ □□□□ □□□□ □□□□ □□□□□.

User1□ □□□ □□□ □□ □□□ □□□□ share1□ □□□□ □ □□□ □□□□ □□□.

□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:

Reference:

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

NEW QUESTION: 122

100□□ □□ □□□ □□□ Azure □□□ □□□ Azure Security Center□ □□□□□ □□□□. □□ □□□ □□□□□ □□□□.
□ □□ □□□ □□□ □□□ □□□ □□□□□.
Azure Resource Manager □□□□ □□□□ □□□ □□□ □□□ □□ □□□ □□□□ □□□.
□□ □□□ □□ □□□□□ □□□□ □□□□□ □□□ □□ □ □□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.

A. □□□□□ □□□ □□ ID
B. Key Vault □□ □□□□ □□ □
C. Azure Active Directory(Azure AD) ID
D. □□□□□ □□□ □□ ID
E. □□ □□ □
F. □□ □□ ID

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

NEW QUESTION: 123

Azure □□□ □□□□. □□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.

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

Microsoft Defender for Cloud□□ □□ □□□ □□□□□ □□□□□ □□□. □□ □□□□ □□ □□□ □□□□□ □□□□□?

A. □□□ 1□ □□□ 2□
B. □□□ □□
C. □□□ □ □□□□
D. □□□1, □□□2, □□□3

Answer: D (LEAVE A REPLY)

NEW QUESTION: 124

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ rt□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
Sub1□□□ Azure □□□ □□□□.
RG1□□□ □□□ □□□ Sa1□□□ Azure Storage □□□ □□□□.
□□□□ □□□□□□□ □□ □□ □□ □□□ □□(SAS)□ □□□ □□□ □□□ □□□□ Sal□ Blob □□□□ □□ □□□□ □□□□□□.

□□□ □□ □□□□ rile □□□□ blob □□□ □□□ □□□□ □□ □□□□□□.
Sa1□ □□ □□ □□ □□□ □□□□ □□□.
□□ □□: □□□ □□ □□ □□□□□.
□□□ □□□ □□□□□?

A. □

B. □□□

Answer: A (LEAVE A REPLY)

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

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

References:

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

NEW QUESTION: 125

□□ □□ □□□ □□ □□□ □□□ Azure □□□ □□□□.

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

□□ □□ □□□ Azure □□□ □□□□.

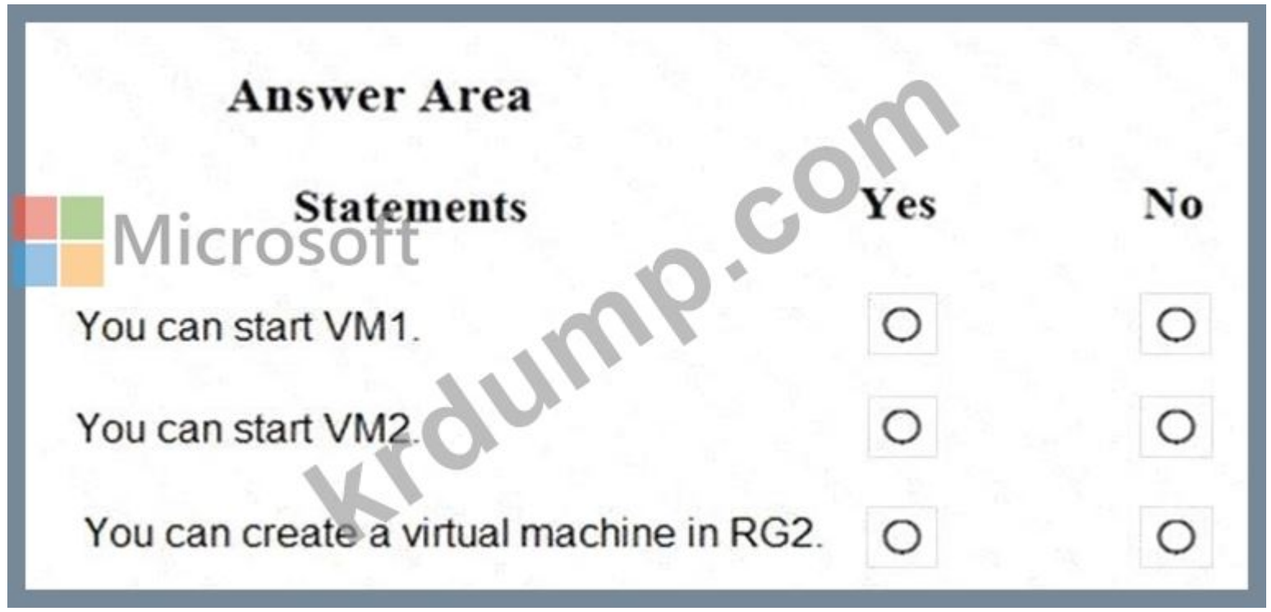
Policy definition	Resource type	Scope
Not allowed resource types	virtualMachines	RG1
Allowed resource types	virtualMachines	RG2

You create the resource locks shown in the following table.

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

□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.

□□: □□ 1□□ 1□□□□.

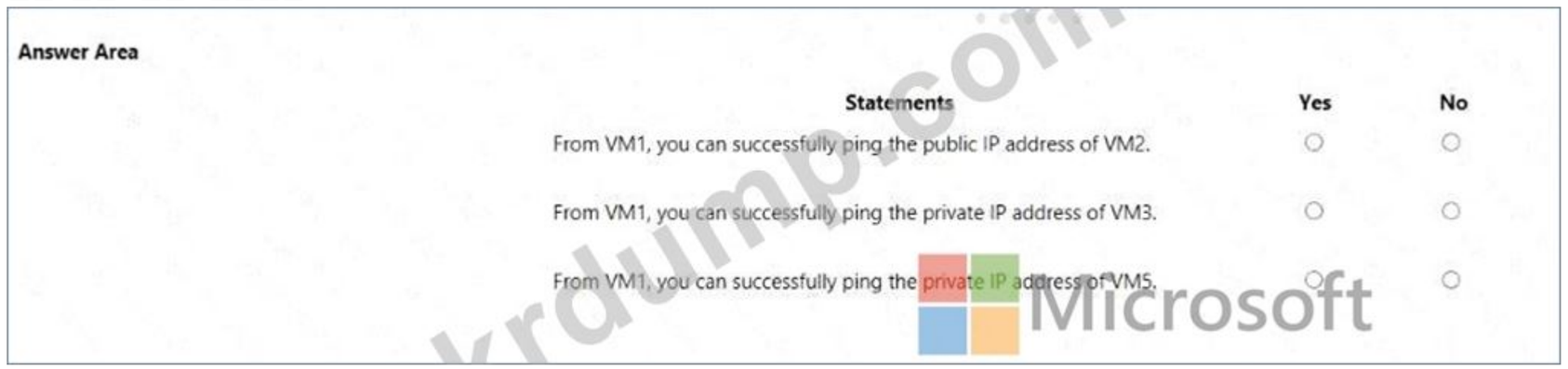


Answer:

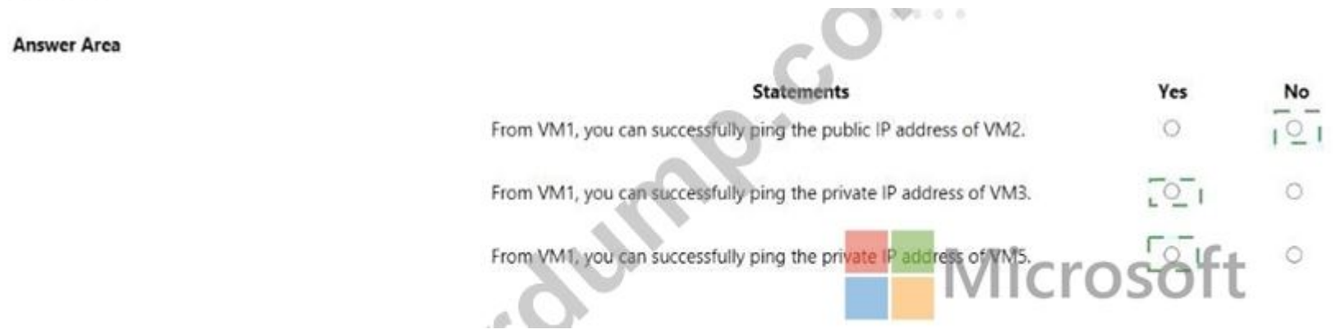
Explanation:

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

NEW QUESTION: 126
Sub2□ □□ □□ □ □□□□ □□□ □□□ □□□□ □□□□.
□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□: □□ 1□□ 1□□□□.



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: 127
Azure Active Directory(Azure AD)□ □□□ Azure □□□ □□□□. □□ □□□□□ □□ □□ □□ □□ □□□□ □□□□ □□□□.

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

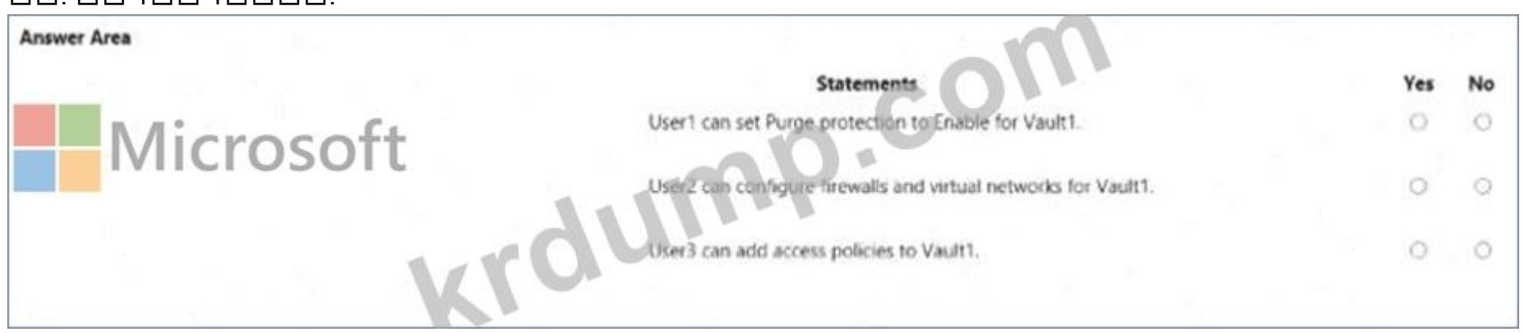
Vault1□□□ Azure Key Vault□ □□□, □□ □□□ □□ □ □□□ □□□□ □□□□. Vault1□□ □□ □□ □□ □□ □□□ □□□ □□□□ □□□□.

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

□□ □□ □□□ □□ Vault1□ □□ □□ □□□ □□□□.

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

□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□.
□□: □□ 1□□ 1□□□□.



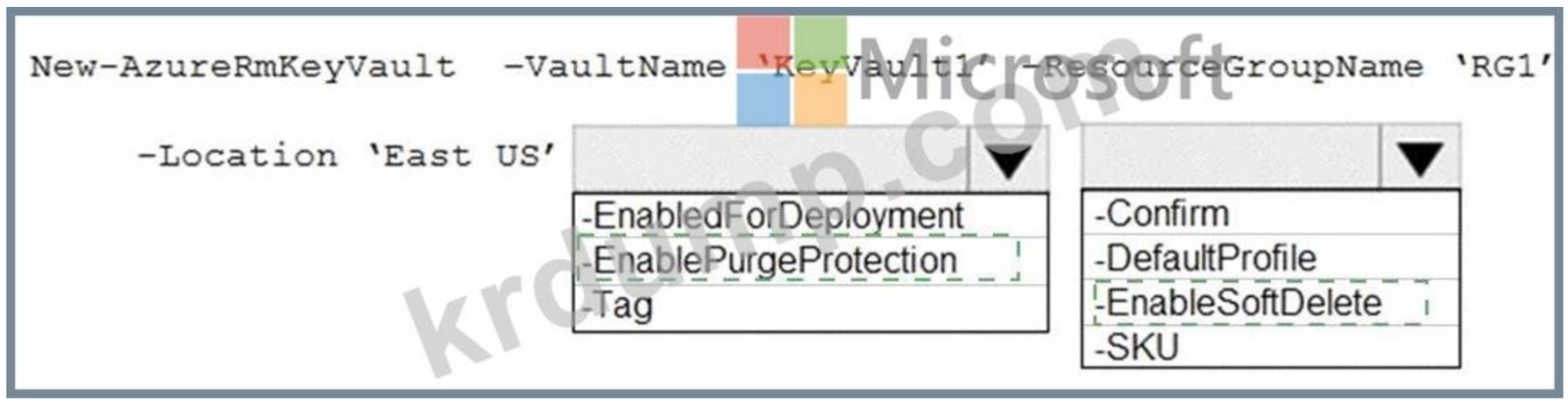
Answer:

Explanation:

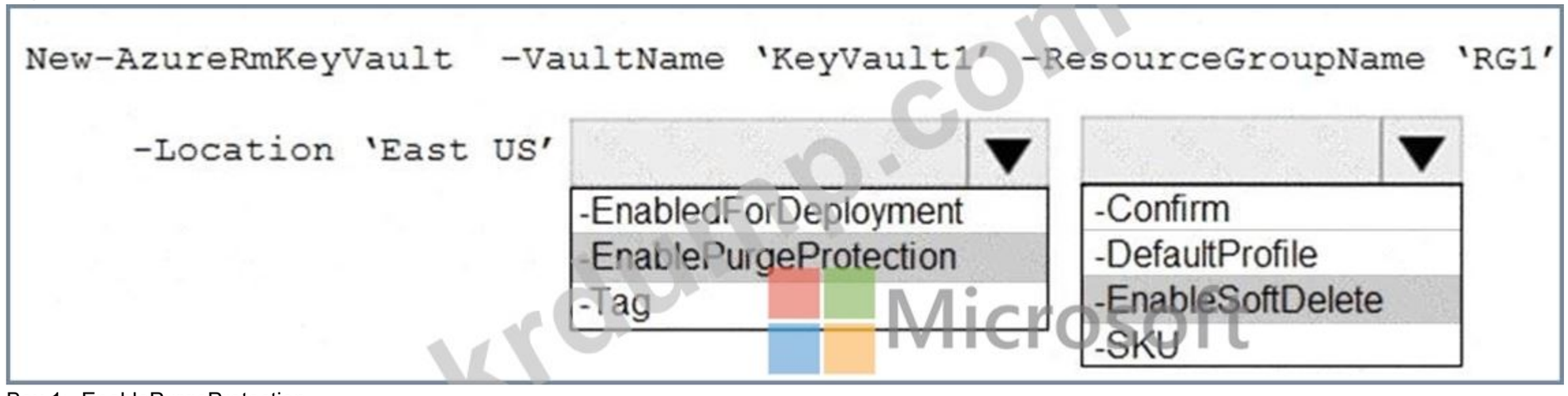
NEW QUESTION: 128
Azure Key Vault□ □□□□ □□□. □□□□ Key Vault□□ □□□ □□ □□□ 90□ □□ □□□□ □□□.
□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ 1□□ 1□□□□.

Answer:



Explanation:



Box 1: -EnablePurgeProtection

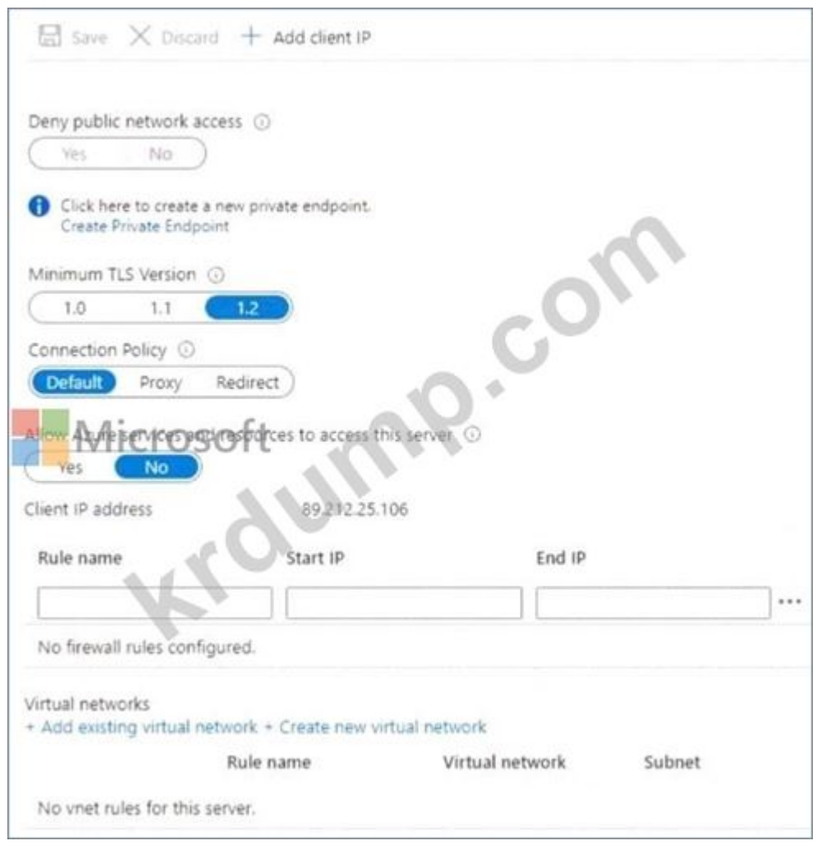
If specified, protection against immediate deletion is enabled for this vault; requires soft delete to be enabled as well.

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: 129
SQL!□□□ Azure SQL Database □□ □□□ VM1□□□ Azure □□ □□□ □□□ Azure □□□ □□□□. VM1□ □□ IP □□□ □□□□□.
SQL1□ □□□ □ □□ □□□□ □□□ □□ □□□ □□□□.



VM1□ SQL1□ □□□ □ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
□□□ □□ □□□?
A. □□ □□ □□□□□ □□□□□.
B. □□ □□□ □□□□ □□□□□.
C. Azure □□□ □ □□□□ □ □□□ □□□□□□ □□□ □□ □□□□□.
D. □□□ □□□ □□□ □□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 130
WAF1□□□ Azure Application Gateway □ □□□□□□ □□□(WAF)□ □□□□ □□□□.
□□□ □□ Bicep □□ □□□ □□□□.

```
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'
        }
      ]
    }
  }
}
```

□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□: □□ 1□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 131

Microsoft Defender for Cloud□ □□□□ Azure □□□ □□□□. □ □□□□ Azure Database for PostgreSQL □□□□□ □□□□ □□□□.
□□□□□□□ □□ □□□ □□ □□□ □□□□ □□ □□□ □□□ □□□□ □□□. □□□□ □□ □□□ □□□□□ □□□.
□□□ □□□□ □□□?

A. Azure Monitor □□ □□

B. Azure Monitor □□ □□

C. □□ □□ □□□ □□□□□□□ Microsoft Defender

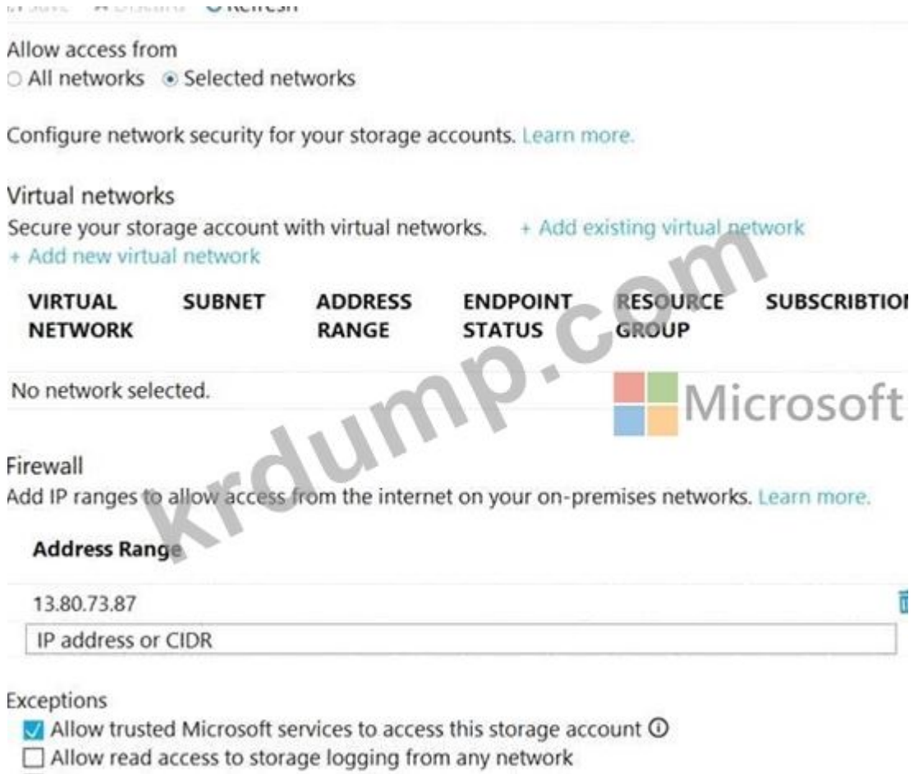
D. PostgreSQL Audit □□(pgAudit)
Answer: (SHOW ANSWER)

NEW QUESTION: 132
500□□ □□□□ AU1□□□ □□ □□□ □□□ Azure AD □□□□ □□□□.
Azure Active Directory □□ □□□□ □□ □□□ □□□ □□□□ AU1□ □□□□ □□□ □□□□□.
□□ □□□ □□□□ □□□ □□□ □□□□□ □□□.
□□□ □□□ □□□□ □□□?
A. □ □□□□ □□□ □□ □□(UPN)□
B. □ □□□□ □□ □□□□
C. □ □□□□ UPN(□□□ □□ □□) □ □□ □□□
D. □ □□□□ □□ □□□
E. □ □□□□ □□□ □□ □□(UPN) □ □□ □□□□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 133
□□ □□ □□□ □□ □□□ □□□ Azure □□□ □□□□.

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□ Subnet2□□ Microsoft.Storage □□□ □□□□□□ □□□□ □□□□.
□□ □□□ □□ □□□ storageacc1□□□ Azure Storage □□□ □□□□.



□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.

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

Answer:

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

Explanation:

Box 1: Yes

The public IP of VM1 is allowed through the firewall.

Box 2: No

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

Box 3: No

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

Reference:

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

NEW QUESTION: 134

□□ □□ □□□ □□ □□□□□ □□□ Azure □□□ □□□□.

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

□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	IP address space	Virtual network	Description
Subnet11	10.1.1.0/24	VNet1	Contains a virtual machine named VM1
Subnet12	172.16.1.0/27	VNet1	Contains no resources
Subnet21	192.168.10.0/24	VNet2	Contains an integrated Azure web app named WebApp1

□□ □□□ □□ WebApp2□□ Azure □□□ □□ □□□□□.

* □□: □□ □□

* VNet □□: □□□□

* □□ □□; □□ 10□ □□□□□□ □□ □□ □□

□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.

□□: □□ 1□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 135

Azure □□□ SQL1□□□ Azure SQL □□□□□□□ □□□□. SQL1□ Always Encrypted□ □□□□□ □□□□ □□□. □□ □□□ □□□□ □□□?

A. MySQL Workbench

B. Microsoft SQL Server Management Studio(SSMS)

C. Azure □□

D. pgAdmin

Answer: B (LEAVE A REPLY)

NEW QUESTION: 136

sqlsrv1□□□ Azure SQL □□□ DB1□□□ Azure SQL □□□□□□□ □□□ Azure □□□ □□□□. Sqlsrv1□ Microsoft Entra □□□□□□ □□□□ □□□□. □□ □□ Microsoft Entra ID□ □□ □□□□.

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

□□ □□□□ DB1□ □□ □□□ □□□ □□ □□□ □□ □ □□□□?

A. User1□ User2□

B. User1□

C. User1, User2, User3

Answer: (SHOW ANSWER)

NEW QUESTION: 137
□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

Microsoft Defender for Cloud□ □□□ □□□□□. Defender for Cloud□ □□□□ □□ □□□□ □□□ □ □□□□?
A. Vault1 □ storage1 □□
B. VM1 □□
C. VNet1, VM1, Vault1 □ storage1
D. VM1 □ storage1□ □□
E. VM1, Vault1 □ storage1□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 138
□□□ □□
□□ 2
VNETOI-Subnet0-NSG □□□□ □□ □□(NSG)□ NetworkSecurityGroupRuleCounter □□□ □□ □□□□ logs31330471 Azure Storage □□□ 30□ □□ □□□□□ □□ □□□.
Answer:
see the task answer with step by step below:
* Enable diagnostic resource logging for the NSG. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select the Rule counter category under Logs and choose the logs31330471 storage account as the destination.
* Configure the retention policy for the storage account to keep the logs for 30 days. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to specify the days parameter as
30 for the Set-AzStorageServiceProperty cmdlet or the az storage logging update command.
* View and analyze the logs in the storage account. You can use any tool that can read JSON files, such as Azure Storage Explorer or Visual Studio Code. You can also export the logs to any visualization tool, SIEM solution, or IDS of your choice

NEW QUESTION: 139
SQLdb1□ □□ □□□ □□ □□□ □□□□ □□□.
□□ □ □□ □□□ □□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.
A. □□□ □□□ □□□ □□□□.
B. SQLdb1□ □□ □□□□□ □□□□□ ID□ □□□□□.
C. SQLdb1□ □□ □□□ □□ □□ ID□ □□□□□.

D. □□ □□ □□□ □□□□.
E. SQLServer1□ □□ Microsoft Entra □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 140
Azure □□□□ □□□□ □□ 3□, SQL1□□□ □□□ Azure SQL □□□ □□□□ 1□, Azure SQL □□□□□□ 3□□ □□□□ □□□□.
□□□□ □□□ □□ □□ □□□ □□ □□□□□.

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

SQL1□□ □□□ □□ □□□ □□□□.
* □□: □□
* □□ □□ □□ □□: □□□!
Azure SQL □□□□□□□ □□ □□ □□□ □□ □□□□□.

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

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.
Answer Area

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

Answer:
Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 141
□□ □□ □□□ □□ □□□ □□□ Azure □□□ □□□□.

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

Azure Security Center□□ □□ □□□□□□ □□□.
□□ □□ □□□ □□ □□□ □□□□□.

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

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

NEW QUESTION: 142
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□,
□□ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
Azure Security Center□ □□□□ □ □□ Azure □□□ □□ □□ □□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□ □□ □□ □□ □□□ □□□□□.
□ □□ □□ □□□ □□ □□□ □□□□ □□□□ □□□.
□□ □□: □□□ □□ □□ □□ □□□ □□□ □□□ □□□□□□ □□□ □□□□.
□□□ □□□ □□□□□?
A. □

B. □□□

Answer: A (LEAVE A REPLY)

Reference:

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

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

NEW QUESTION: 143

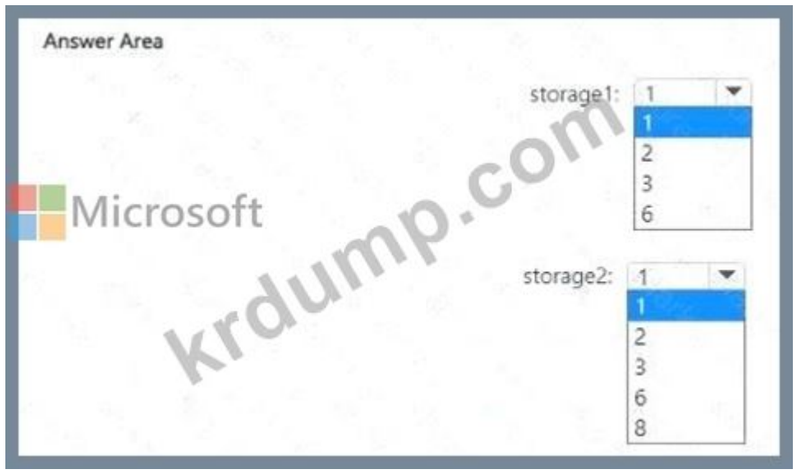
□□ □□ □□□ □□□ □□□ □□□ Azure □□□ □□□□.

Name	Performance	Premium account type	Redundancy	Sub-resource
storage1	Standard	*Not applicable*	Locally-redundant storage (LRS)	Two Azure Files shares
storage2	Premium	Page blobs	Locally-redundant storage (LRS)	Three containers

□□□ □□□ □□ □□ □□□□ □□ □□□□ □□□□□□ □□□□ □□□. □□□□ □□□□ □□□□□□ □□□□ □□ □□ □□ □□□□ □□□□ □ □□□ □□ □□□.

□ □□□□ □□□ □□ □□□□ □□ □□ □□ □□□□□ □□ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

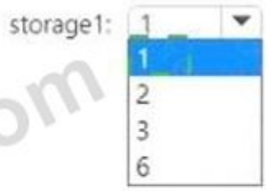
□□: □□ 1□□ 1□□□□.



□□

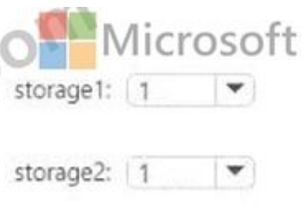
Answer:

Answer Area



Explanation:

Answer Area



NEW QUESTION: 144

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.

□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.

AKS1□□□ Azure Kubernetes Service(AKS) □□□□□ AZCR1□□□ Azure □□□□ □□□□□□ □□□□ Azure □□□ □□□□.

AKS1□ AZCR1□ □□□ □□□□ □□□□ □□□ □ □□□ □□□□ □□□.

□□ □□: □□□□ □□□ □□ ID□ □□□□□ AKS1□ □□□□ □□ ID□ Azure Kubernetes Service □□□□ □□□ □□□ □□□□□.

□□□ □□ □□□ □□□□□?

A. □□□

B. □

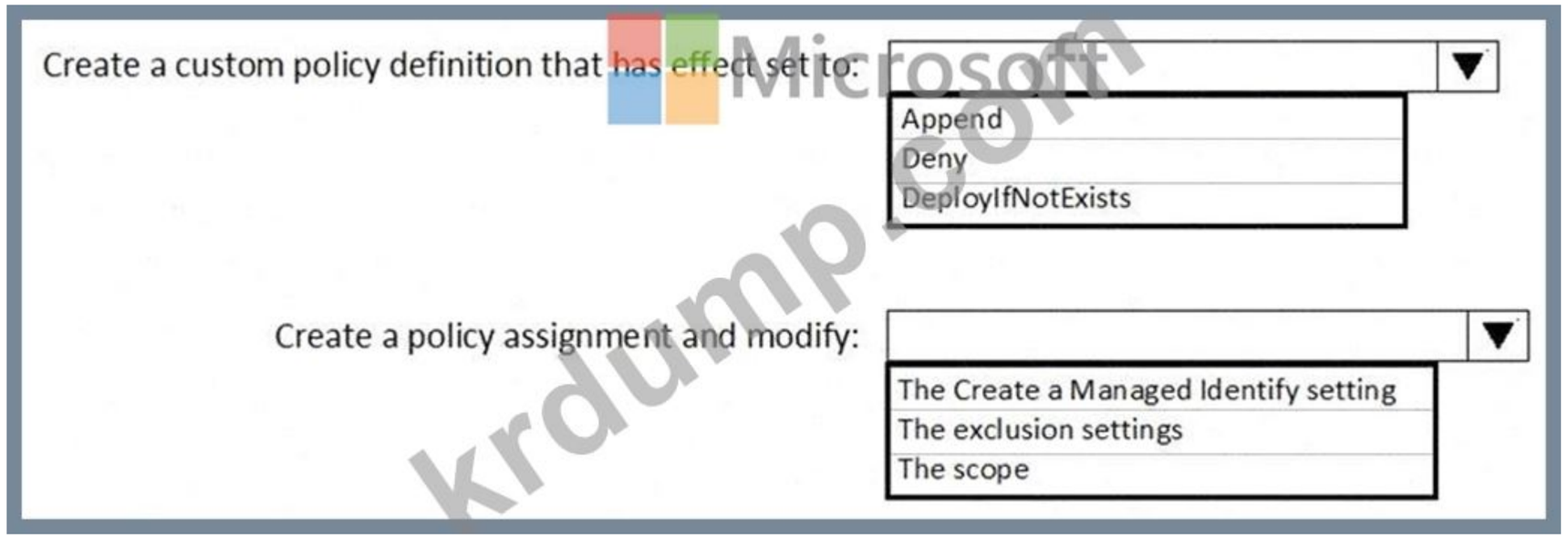
Answer: B (LEAVE A REPLY)

NEW QUESTION: 145

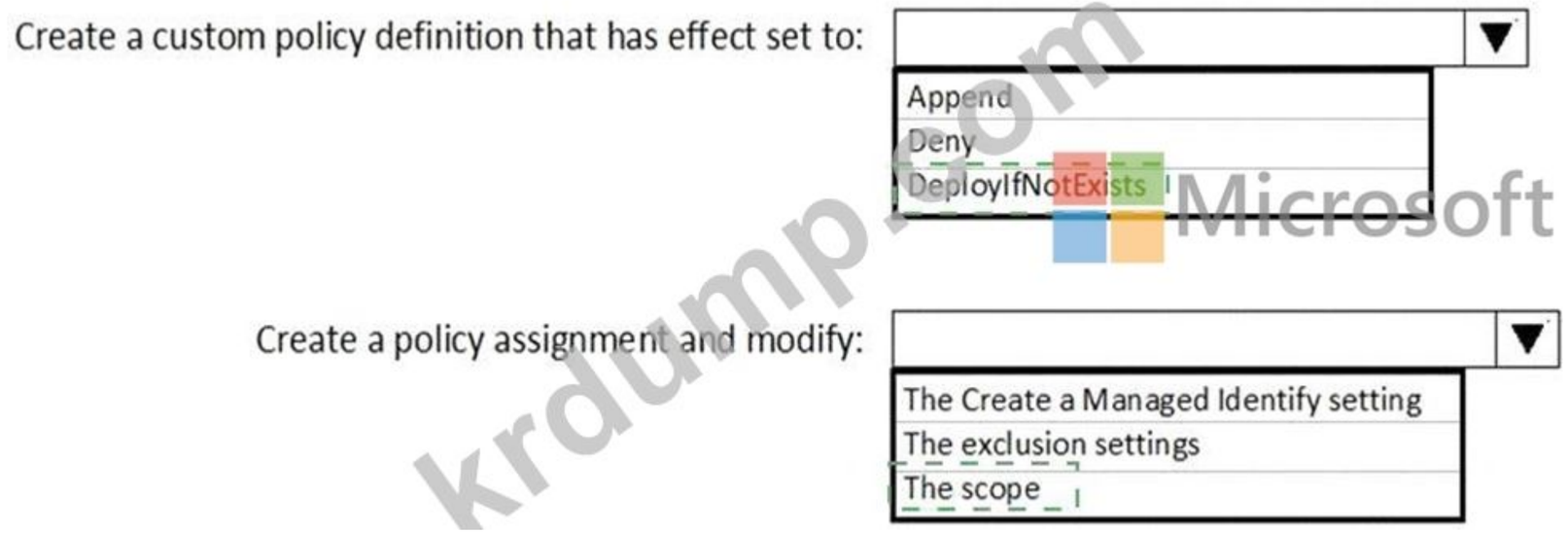
□□□ □□ □□ □□□ □□□□□ Microsoft Antimalware□ □□□□ □□□.

□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□□ □□□□□.

□□: □□ 1□□ 1□□□□.



Answer:



Explanation:

1. DeployifNotExists
2. Scope

NEW QUESTION: 146

AD DS(Active Directory Domain Services) □□□□ □□□□□ Azure Active Directory □□□□ □□□□.

□□□ □□□ □□□□ Azure □□ □□□ □□ □□□□□.

Azure □□ □□ □ □□ □ □□□ □□□ □□□□ □ □□□ □ □□ ID □□□□ □□□□□?

□□□□□ □□ □□□□ □□□ □□□ □□□□□.

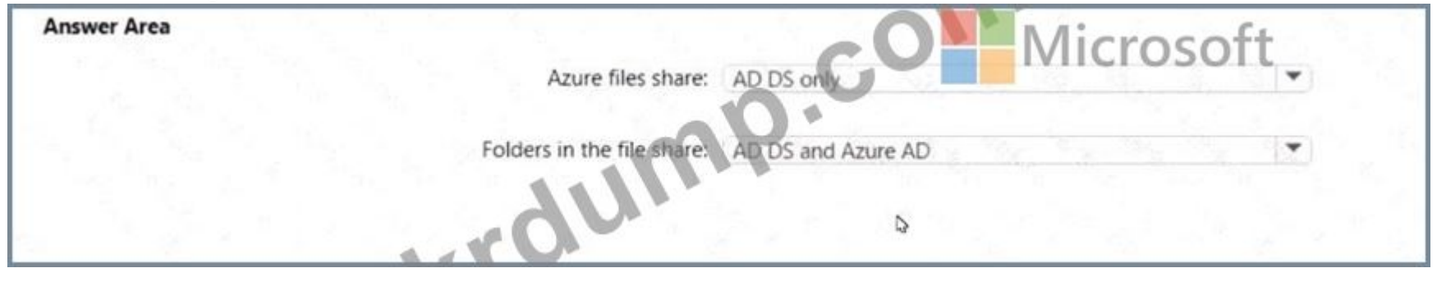
□□: □□ 1□□ 1□□□□.

Answer:

See the answer below at Explanation.

Explanation:

Answer is as image below.



NEW QUESTION: 147

Azure Active Directory Premium Plan 1 □□□□ □□□ Azure □□□ □□□□.

Azure Active Directory(Azure AD) ID □□□ □□□ □□□□□.

□□□ □□ □□□ □□□ □□ □□□ □□□ □ □□□ □□□□ □□□.

□□ □□ □□□ □□ □□□?

A. □□ □□□□ □□ Azure Active Directory Premium Plan 2 □□□□□ □□□□□.

B. □□ □□□□ Azure Multi-Factor Authentication(MFA)□ □□□□□.

C. Azure AD□ □□ □□ □□□□ □□□□□□.

D. Azure Security Center□ □□ □□□□ □□□□□□□□.

Answer: A (LEAVE A REPLY)

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa

NEW QUESTION: 148

□□ □□ □□□ □□ □□□ □□□ Sub1□□□ Azure □□□ □□□□.

Name	Resource group
VM1	RG1
VM2	RG2
VM3	RG1
VM4	RG2

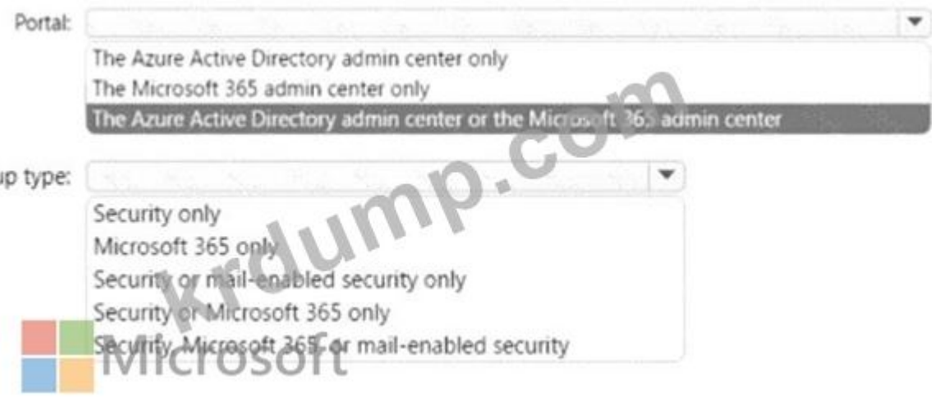
□□□ □□ □□□□ □□□□ □□□ □□□ RG1□ □□ □□□□ □□ □□□□ □□□ □□ □□□ □□□□ □□□.

□□□ □□□□ □□□?

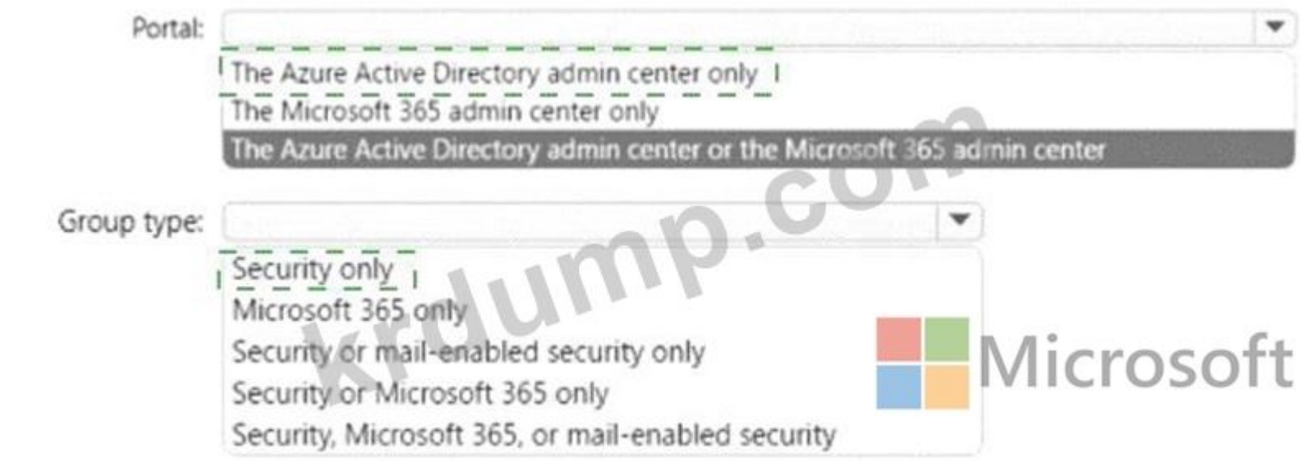
A. Azure Active Directory(Azure AD) □□ □□ ID □□(PIM)

B. □□□□□□ □□ □□
C. Azure Active Directory(Azure AD) □□□ □□□
D. JIT(Just-in-Time) VM □□□
Answer: D (LEAVE A REPLY)
Just-in-time (JIT) virtual machine (VM) access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.
Note: When just-in-time is enabled, Security Center locks down inbound traffic to your Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the just-in-time solution.
When a user requests access to a VM, Security Center checks that the user has Role-Based Access Control (RBAC) permissions that permit them to successfully request access to a VM. If the request is approved, Security Center automatically configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the amount of time that was specified. After the time has expired, Security Center restores the NSGs to their previous states. Those connections that are already established are not being interrupted, however.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

NEW QUESTION: 149
contoso.com□□□ Azure AD □□□□ □□ Azure AD Premium P1 □□□□□ □□□□.
□□□ □□ □□□ □□□ Group1□□□ □□□ □□□□ □□□.
□□1□ □□□□ □□ □□□ □□□□ □□, □□ □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□□ □□ □□□□ 1□□ □□□ □□□□.



Answer:



Explanation:

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

NEW QUESTION: 150

□□ □□ □□□ Azure □ □□ □□ □□□ □□□□ Sub1□□□ Azure □□□ □□□□.

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

Sub1□□□ □□ □□□ □□ □□ □□□ □□□□.

* □□: VM1

* □□: DS2v2
* □□□ □□: RG1
* □□: □□□
* □□□□ : □□□ □□ 2022

VM1□□ Azure Disk Encryption□ □□□□ □□□□□.

VM1□ □□□ □□ □□ □ □□□□ □□□ □ □□□?

A. Vault1 □□ Vault3□ □□

B. Vault1, Vault2, Vault3 □□ Vault4

C. Vault1□ □□

D. Vault1 □□ Vault2□ □□

Answer: A (LEAVE A REPLY)

In order to make sure the encryption secrets don't cross regional boundaries, Azure Disk Encryption needs the Key Vault and the VMs to be co-located in the same region. Create and use a Key Vault that is in the same region as the VM to be encrypted.

Reference:

https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites

NEW QUESTION: 151

□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

Name	Type
VM1	Virtual machine
VNet1	Virtual network
AFW1	Azure firewall

VM1□□ □□ □□ Azure □□□ □□□□ □□□□□ □□□□ □□□□□ AFW1□ □□□□ □□□. □□□□ □□ □□□ □□□□□ □□□.

□□□ □□□□ □□□?

A. □□ □□□□ □□

B. □□□□ □□

C. DNAT □□

D. SNAT □□ IP □□ □□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 152

Azure □□□□ □□□□□ □□□ □□□□□.

□□□□ □□□ □□□ □□ □□□□□□ □□□□□□□ □□□□. □ □□□□□□□ □□□□□□ □□□□□ □□□ □□ □□□□, □□□ □ □□ □□□□□ □□□□□.

□□□□□□ □□□□□ □□ □□□□□ □□ □□□□□□□. □□ □□□□□ □□□□□□ □□□□□ □□□ □□□ □ □□□□ □ □□□ □□□□ □□□□ □□ □□□ □□□□□.

□□□□□□ □□□□□ □□ □□□□□ □□ □□□□□ □□□□ □□□. □□□□□ □□□ □□□□ □□ □□□ □□□□ □□ □□□□ □□□.

□□□ □□□ □□□□ □□□?
A. □□□□□□ □□ □□
B. □□□□ □□ □□(NSG)
C. □□ □□
D. □□□□ □□
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: 153
Azure □□□ □□□□.
AzSQL1□□□ Azure SQL □□□ □□□□□ □□□ □□□□□.
AzSQL1□ □□ □□□ □□□□ □□□□ □□□.
□□□□ □□ □□ □□□ □□□□ □□□.
* □□□□□□ □□□ □ □□□□□, □□□ □□□, □□ □□ □□□ □□□□ □□□□ □□ □□□.
* □□□□□□ □□□□ □□□□ □□□□ □□ □□□□ □ □ □□□ □□□.
□□□□□ □□□ □□□□ □□□?
A. TLS
B. □□ □□ □□ □□□ □□□ □□□ □□□(TDE)
C. Microsoft □□ □□ □□□ □□ □□□ □□□(TDE)
D. Azure □□□ □□□
E. □□ □□□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 154
LAW1□□□ Azure Log Analytics □□ □□□ □□□□ Sub1□□□ Azure □□□ □□□□.
Windows Server 2012 R2 □ Windows Server 2016□ □□□□ □□□□□ □□ 100□□ □□□□. □ □□□□ LAW1□ □□□□□. LAW1□ □□□ □□□□ □□ □□ □□ □□□□ □□□□□ □ □□□ □□□□.
LAW1□□ □□□ □□□□ □□□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* □□ □□□ □□□ □□□□ □□□.
* □□ □□□ □□□ □□□ □□□□□ □□□.
* □□ □□□ □□□ □□□ □□ □□□ □□□ □ □ □□ □□□□□ □□□.
* □□□.
□□ □□□ □□ □ □□ □□ □□□ □□□□ □□□?
A. □□
B. □□(□□□ □□)
C. □□□
D. □□ □□

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: 155

□□ □□ □□□ □□□□□ AKS1 □ ID1 □□ ID□ □□□□ □□□. □□□□ □□ □□ □□□ □□□ □□□.

□ ID□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ 1□□ 1□□□□.

Answer Area

Answer:

Explanation:

Answer Area

AKS1: AcrPull

ID1: AcrPush

NEW QUESTION: 156

User1□□□ □□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.

User1□ □□ □□□ □□□□ □□□ □ □□□ □□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

User1□□ □□ □□□ □□□□ □□□?

A. □□□ □□□

B. □□□□□ □□□

C. □□□ □□ □□ □□□

D. □□ □□□

Answer: C (LEAVE A REPLY)

NEW QUESTION: 157

□□ □□ □□ □□ □□□ □□□ □□□□ Sub1□□□ Azure □□□ □□□□.

Name	Location
RG1	West US
RG2	East US

□□ □□□ □□□ Azure Policy □□□ □□□□.

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


Sub1□ □□□ □□□□□.

□□ □□ □□□ □□□□ □□ □□□□□.

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

□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□: □□ 1□□ 1□□□□.

Answer Area

Statements	Yes	No
You can create IPobject1.	○	○
You can create obj1.	○	○
You can create OBJ3.	○	○

Answer:

Answer Area

Statements	Yes	No
You can create IPobject1.	○	○
You can create obj1.	○	○
You can create OBJ3.	○	○

Explanation:

Statements	Yes	No
You can create IPobject1.	○	●
You can create obj1.	○	●
You can create OBJ3.	○	●

NEW QUESTION: 158
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
AKS1□□□ Azure Kubernetes Service(AKS) □□□□□ AZCR1□□□ Azure □□□□ □□□□□□ □□□□ Azure □□□ □□□□.
AKS1□ AZCR1□ □□□ □□□□ □□□□ □□□ □ □□□ □□□□ □□□.
□□ □□: AKS1□ □□□□ □□ □□ □□□□ □□□ □□ ID□ Kubernetes Agentless Operator □□□ □□□□□.
□□□ □□ □□□ □□□□□?

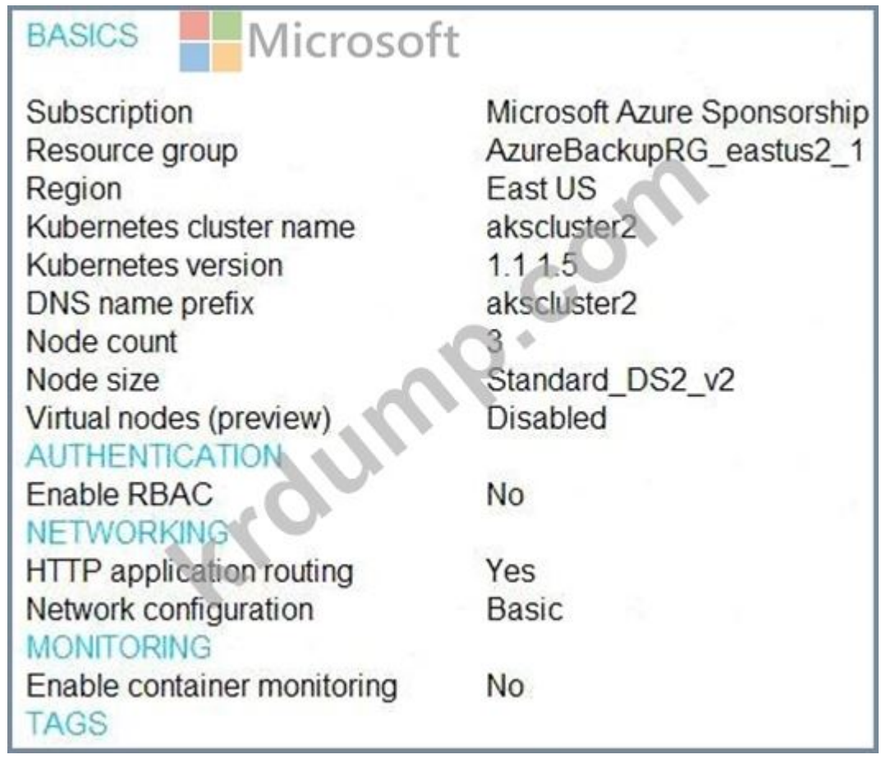
A. □
B. □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 159
Azure Storage □□□ □□ □□□ □□□□ □□□□.
□□□ □□□ □□ □□ □□□ □□□□□□.
□□ □□□ □□□□□ □□□ □□□□ □□□?
A. Azure □□□ □□□
B. Azure□ SQL □□ □□□
C. Windows□ □□ □□□
D. Azure □□ □□
Answer: A (LEAVE A REPLY)
If you want to download the metrics for long-term storage or to analyze them locally, you must use a tool or write some code to read the tables. You must download the minute metrics for analysis. The tables do not appear if you list all the tables in your storage account, but you can access them directly by name. Many storage-browsing tools are aware of these tables and enable you to view them directly (see Azure Storage Client Tools for a list of available tools).
Microsoft provides several graphical user interface (GUI) tools for working with the data in your Azure Storage account. All of the tools outlined in the following table are free.

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

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

NEW QUESTION: 160
Azure Kubernetes Service(AKS) □□□□□ □□□□□ □□□□. □□□□□ □□□ □□ □□□□ □□□□.
(□□ □□ □□□□□.)



□□□□□ □□□□ □□□ □□□ □□□□□. HTTP □□□□□□ □□□□ □□□□□□□.
□□ IP □□□ □□□□ AKS □□□□ □□ □□□ □□□ □ TLS □□□ □□□□ □□□□□□ □□□□ □□□□ □□□.
□□□ □□ □□□?

A. AKS Ingress □□□□□ □□□□□.
B. □□□□ □□□□ □□□□□(CNI) □□□□□ □□□□□.
C. Azure □□ □□ □□ □□□ □□□□.
D. Azure □□ □□ □□ □□□ □□□□.

Answer: (SHOW ANSWER)

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

NEW QUESTION: 161

Azure □□ □□□ □□□□ □ □□□□ Azure Resource Manager □□□□ □□□□.
□□ □□ □□□□□ □□□□□□□ □□ □□□□ □□ Windows □□□ □□□□ □□□□□□ □□□.
□□□ □□□□ □□□?

A. Microsoft Intune□ □□ □□ □□ □□
B. Azure Automation □□ □□
C. □□□□□□ □□ □□
D. Azure □□□□□

Answer: B (LEAVE A REPLY)

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: 162
contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□ □ □□□□ User1□□□ □□□□ □□□□.
□□□□ □□ □□ □□ □□□ □□□□□.
User1□ □□□ □□ □□ □□□ □□□ □□□ □ □□□ □□□□ □□□.
□ □□□ □□□□ □□ User!□ □□ □ □□ □□□ □□□ □□□ □ □□□□? □ □□□ □□□ □□□□ □□□□□.
□□: □□ 1□□ 1□□□□.
A. □□□□□□ □□□
B. □□ □□□
C. □□□□□□ □□□
D. □□□ □□□
E. □□□□ □□□□□□ □□□
Answer: C,E (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent

NEW QUESTION: 163
Azure □□□ □□□□.
Azure Active Directory(Azure AD) □□ □□ □□(PIM)□ □□□□□□.
□□□ □□□ □□□ □□ □□ □□□□ □□□ □□ □□□ □□□□.
* □□□ □□ □□(MFA)□ □□□□ □□□.
* □□□□ 20□□□ □□□ □□□□□ □□□□ □□□.
* □□□□□ 180□□□ □□□□ □□□.
* □□□ PIM□ □□□□ □□□□ □□□.
□□ 90□ □□ □□□□□ □□□□ □□ □□□□ □□ □□□ □□ □□□.
□□□ □□□ □□ □□□□□ □□□.
□□ PIM □□□ □□□□ □□□?
A. □□ □□□□ □□ □□ □□ □□□ □□□□ □□□□.
B. □□□□ □□ □□ □□□ □□□□ □□□□.
C. □□□ □□ □□ ID □□ □□□□ □□□□ □□□□.
D. □□ □□□ □□□□ □□ □□□□□.
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to- configure-security-alerts?tabs=new

NEW QUESTION: 164

Azure Active Directory(Azure AD) □□□□ □□□□. □ □□□□□ Azure AD Premium Plan 2 □□□□□ □□□ □□□□ □□□□ □□□□.
fabrikam.com□□□ □□□□ □□□□ □□□ □□□ □□□□. □ □□□□□ 'user'□□ □□□□ □□□□. 'user'□ □□□ □□□ userl@tabrikam.com□□□.
User1□□ □□□□ □□□□ □□□□□ □□□□ □□ □□ □□□ □□□□ □□□.
* user1□ userl@fabrikam.com □□ □□□ □□□□ □□□□ □ □□□ □□□.
* User1□□ □□□□ □□□□ □□ □□□ □□□ □□□ □ □□□ □□□.
* □□□ □□□ □□□□□ □□□.
□□□ □□ □□□?

A. user1□ □□ □□□ □□□ □□□□□.
B. □□□□ □□ □□□ □□□ □□ □□□ □□ □□□ □□ □□□□ □□ □□□□□.
C. □□□□ fabrikamcom□ □□□ □□ □□□□□ □□□□□.
D. User1□ □□ □□□□ □□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 165
Sub2□ □□ □□ □ □□□□ □□□ □□ □□□□□□ □□ □□□ □□□ □□□□ □□□□.
□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□: □□ 1□□ 1□□□□.

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

Answer:

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

Explanation:

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

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

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

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

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

Box 2: Yes.

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

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

NEW QUESTION: 166

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.

□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.

Sub1□□□ Azure □□□ □□□□. Sub1□□ Windows Server 2016□ □□□□ VM1□□□ Azure □□ □□□ □□□□ □□□□.

Azure Disk Encryption□ □□□□ VM1 □□□□ □□□□□ □□□.

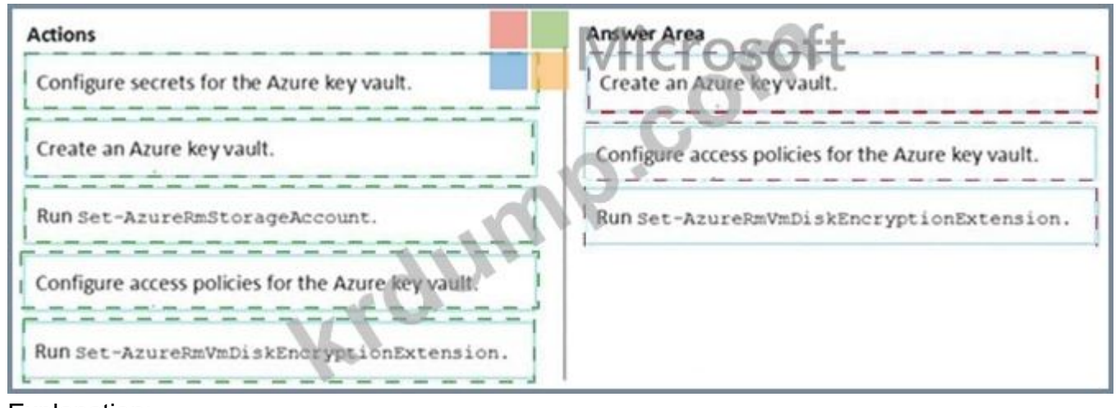
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.

Actions

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

Answer Area

Answer:



Explanation:

References:

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

NEW QUESTION: 167

contoso.com□□□ □□□□□ Microsoft Entra □□□□ □□, □□□□ Uset1□□□ □□□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	Operating system	Configuration
Server1	Windows Server 2016	Domain-joined
Server2	Windows Server 2022	Domain-joined

□□□□ storage1□□□ □□□ □□□ □□□ Azure □□□ □□□□ □□□□. storage1 □□□□ shares1□□□ □□ □□□ □□□□ □□□□.
User1□□□ storages1□ □□ □□□ □□ □□□ SMB □□ □□□ □□□ □□□□□.
storage1□ □□ □□□ □□ □□ □□□□ □□□ □□ □□ □□□ □□ □□□□□.

□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□□□: □□ 1□□ 1□□□□.

Answer:

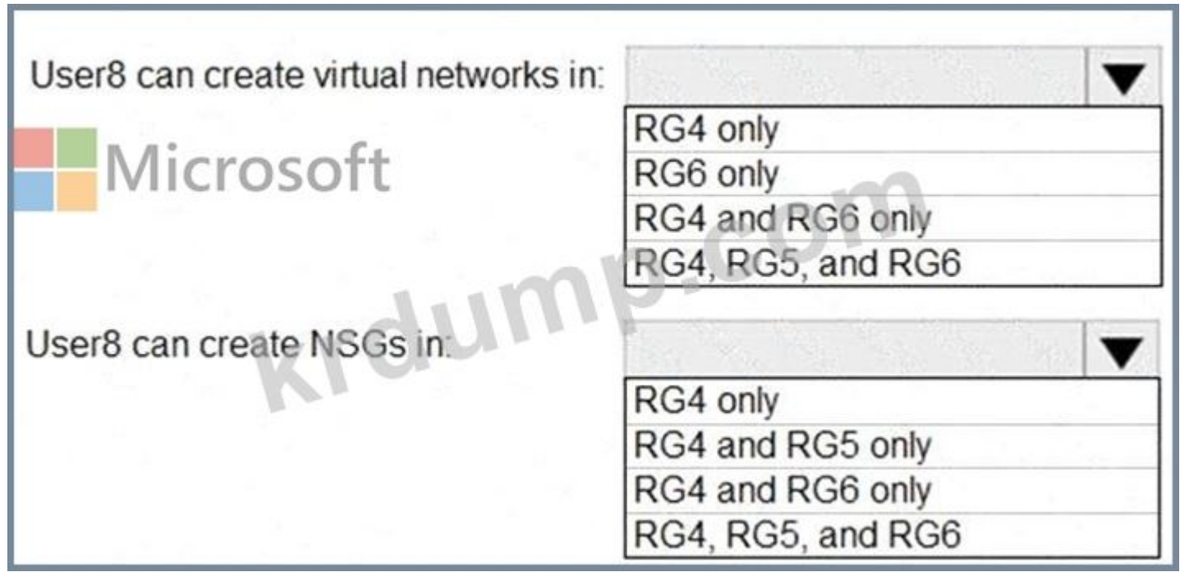
Explanation:

NEW QUESTION: 168

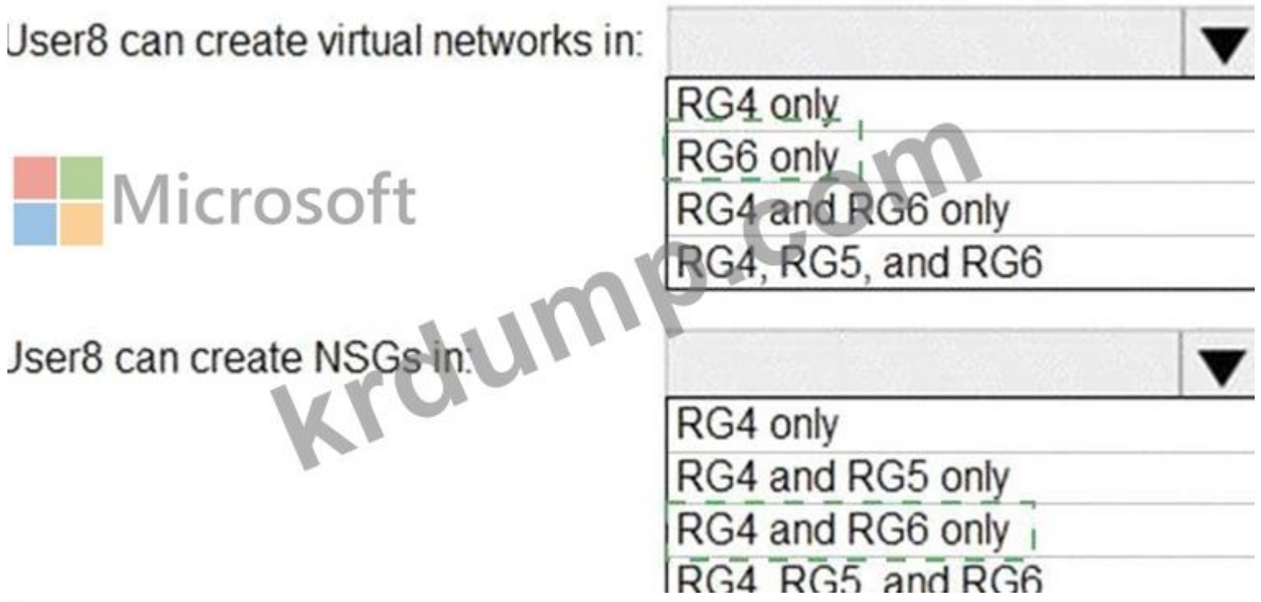
User8□□ RG4, RG5, RG6□ □□□ □□□ □□□□□.

User8□ □□ □□□ □□□ □□ □□□□□ NSG□ □□□ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ 1□□ 1□□□□.



Answer:



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

NEW QUESTION: 169
□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

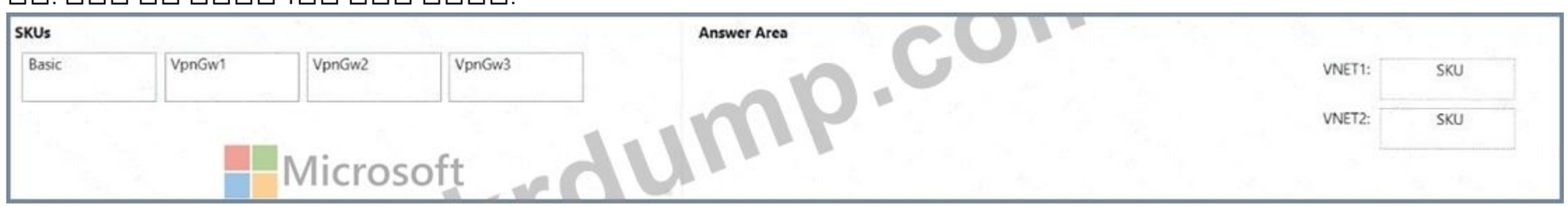
Name	Virtual network	Location
Subnet11	VNet1	West US
Subnet12	VNet1	West US
Subnet21	VNet2	West US

□□□□ □□ □□□ □□ WebApp1□□□ Azure □□□ □□□□ □□□□.
* □□ □□ □□
* □□ □□□□ VNet1
* VNet □□: □□□□
* □□□□□ □□□: Subnet11
* Windows □□(□□ □□): ASP1
□□ □□□ □□ WebApp2□□ Azure □□□ □□□ □□□□□.
* □□: □□ □□
* VNet □□ □□□
* □□□ □□(West UAS): WebApp2?
□□ □□□□ WebApp2□ □□□ □ □□□?
A. □□□2□
B. Subnet2 □□ Subnet21□
C. Subnet11□
D. Subnet11 □□ subnet12□
E. Subnet11, subnet2 □□ Subnet21

Answer: (SHOW ANSWER)

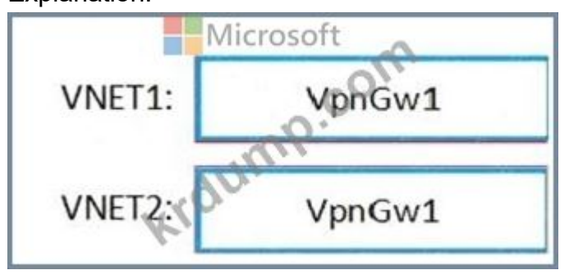
NEW QUESTION: 170
Microsoft Entra □□□□ □□□□.
□□□ □□ Microsoft Entra □□□□ Microsoft Entra ID□□ □□□ □□□ □□□□ □□□□ □□□□ □□□.
A. □□ □□□□□□ □□ □□□ □□□ □□ □□□□□.
B. □□□ □□ □□□□□□ Microsoft Entra ID □□ □□□ □□ □□□ □□□ □□ □□□□□.
C. □□□ □□ □□□□□□ □□□□ □□□□□□□ □□□ □ □□□ □□□□ □□□□□.
D. □□ □□□□□□ Azure □□□□ □□ □□□ □□□ □□□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 171
VNET1□ VNET2□□ □ □□ Azure □□ □□□□□ □□ □□□□ □□□ □□□□ □□□□.
□□ □□ □□□ □□□□□ □□ □□□□□ VPN □□□□□□ □□□□ □□□.
* VNET1□□ BGP□ □□□□ 6□□ □□□ □ □□□ □□□ □□□.
* VNET2□□ BGP□ □□□□ 12□□ □□□ □ □□□ □□□ □□□.
* □□□ □□□□□ □□□.
□ □□ □□□□□ □□ VPN □□□□□(SKI)□ □□□□ □□□? □□ □□□□ □□ SKU□ □□ □□□□□ □□□□□□. □ SKU□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □□□ □□ □□□ □□□□□□ □□□□□ □ □□ □□□□.
□□: □□□ □□ □□□□ 1□□ □□□ □□□□.



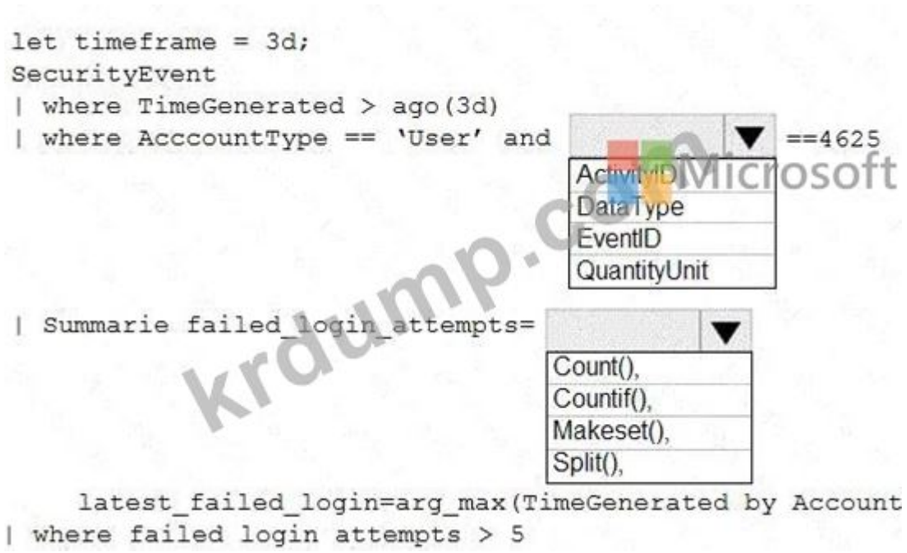
Answer:

Explanation:

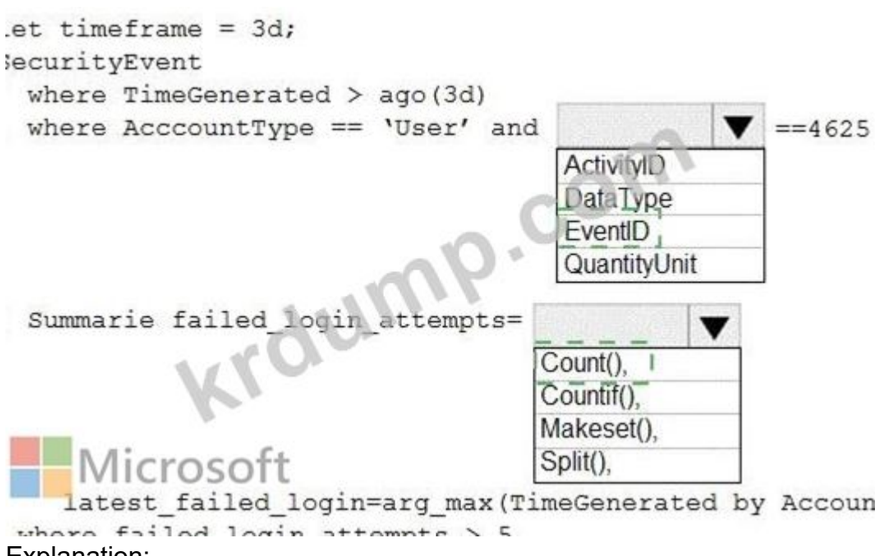


References:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku

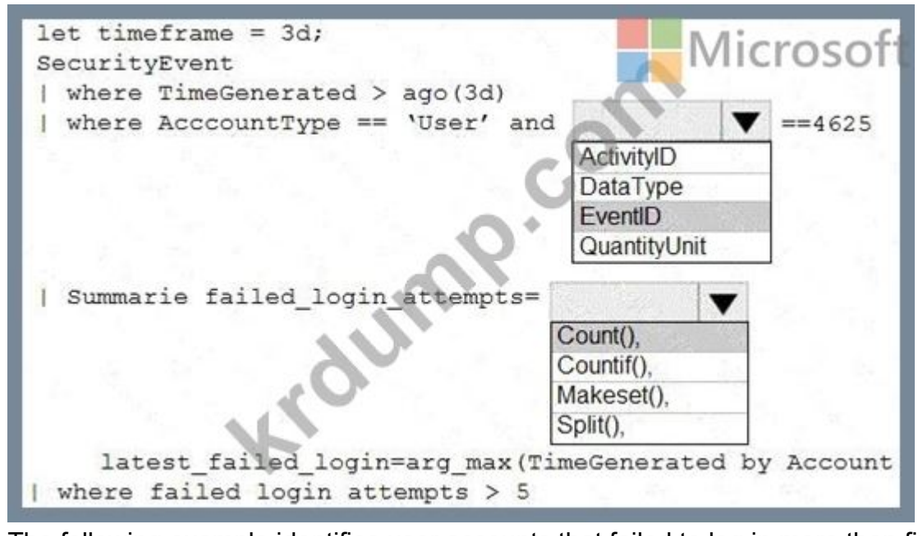
NEW QUESTION: 172
□□□□ □□□□ □ □□ □□□□ □□□□ □□□□ □□□ □□□□□.
□□ 3□□ □□□ □□□ □□□ □□□ □□□□ □□ Azure Log Analytics □□□ □□□□ □□□. □□□□ 5□ □□ □□□ □□□ □□□ □□□□ □□□□□ □□□.
□□□ □□□ □□□□ □□□? □□ □□□□ □□□ □□□ □□□□ □□□□□.
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:



The following example identifies user accounts that failed to log in more than five times in the last day, and when they last attempted to log in.

let timeframe = 1d;

SecurityEvent

| where TimeGenerated > ago(1d)

| where AccountType == ' User ' and EventID == 4625 // 4625 - failed log in

| summarize failed_login_attempts=count(), latest_failed_login=arg_max(TimeGenerated, Account) by Account

| where failed_login_attempts > 5

| project-away Account1

References:

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

NEW QUESTION: 173

□□ □□ □□□ □□ □□□□□ □□□ Azure □□□ □□□□.

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

NSG1□ NSG2□ □ □ □□ □□□ □□□ □□□□.

□□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.

Name	Connected to
VM1	Subnet1
VM2	Subnet2

□□□□ □□ □□ □□□ □ □□ □□□□ □□□□.

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

□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□: □□ 1□□ 1□□□□.

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 174
contoso.com□□□ Microsoft Entra □□□□ □□□□.
□□□ fabrikam.com□□□ Microsoft Entra □□□□ □□□ □□□ □□□ □□□□□.
com□ □□ □□□□ □□ □□ □□ □□(MFA)□ □□□□□□□.
Contoso.com□ □□ □□□ □□□ □□□ □□ □□□ □□□ □□ □□ □□□ □□ □□□□ □□□□. (□□ □□□ □□□ □□□ □□□□□.

Inbound access settings

Edit inbound defaults

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

Outbound access settings

Edit outbound defaults

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

Contoso.com□ □□ □□ □□□ □□ □□ □□ □□ □□□ □□ □□□□ □□□□. (□□ □□ □□ □□ □□□□□.)

□□ □□□ □□□□ □□□ □□□ □□□ □□□□.
* □□: CAPolicy1
* □□
o □□□ □□ □□ □□□: B2B □□ □□□ □□□
o □□ □□
□□: □□ □□□□ □ o □□□ □□
□□ □□ □□
□□□ □□□ □□□□ □□□ □□□□□ □
□□ □□ □□ □□
□□ □□□: □□
□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□.
□□: □□□ □□ □□ □□□ 1□□□□.

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 175

□□ □□□ Azure □□ □□□□□ □□ □□□□.

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

□□ □□□ Azure □□ □□□ □□ □□□□.

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

□□ □□ □□□ □□□□ ping □□□□ □□□□□.

NSG1□ □□ □□□ □□ □□□□ □□□□.

□□□□ □□ □□

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

□□□□□ □□ □□

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

□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.

□□: □□ 1□□ 1□□□□.

Statements	Yes	No
VM1 can ping VM3 successfully.	○	○
VM2 can ping VM4 successfully.	○	○
VM3 can be accessed by using Remote Desktop from the internet.	○	○

Answer:

Statements	Yes	No
VM1 can ping VM3 successfully.	○	○
VM2 can ping VM4 successfully.	○	○
VM3 can be accessed by using Remote Desktop from the internet.	○	○

Explanation:

Statements	Yes	No
VM1 can ping VM3 successfully.	○	○
VM2 can ping VM4 successfully.	○	○
VM3 can be accessed by using Remote Desktop from the internet.	○	○

Box 1: Yes

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

Box 2: No

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

Box 3: Yes

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

NEW QUESTION: 176

□□ □□ □□□ Azure Log Analytics □□ □□□ □□□ Azure □□□ □□□□.

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

□□ □□ □□□ □□ □□□ □□□□□.

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

Azure Sentinel□ □□□□ □□ □□□ Windows Defender □□□□ □□□□□ □□□□□.

Azure Sentinel□ □□□ □ □□ □□ □□□ □□□□□?
A. VM1 □ VM3□ □□
B. VM1 □□
C. VM1 □ VM2□ □□
D. VM1, VM2, VM3 □ VM4
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall

NEW QUESTION: 177
□□ □□ □□ □□ □□ ID□ Identity1□ Azure Key Vault□ □□□ Azure □□□ □□□□.

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

Key Vault1□□ Identity1□ □□□ □□ □ □□□ □□□□ □□□ □□□ □□□□ □□□□.
* □□
* □□
* □□□□
* □□
KeyVault2□ □□□□ Identity1□ □□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
Identity1□ □□ □□□ □□□□ □□□?
A. Key Vault □□□ □□□
B. □ □□ □□
C. Key Vault Crypto □□□ □□□ □□□
D. Key Vault □□□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 178
□□ □□ □□ □□ □□□□ □□□□ Vault1□□□ Azure Key Vault□ □□□□.

Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

□□ □□□□ □□ □□ □□□ □□□□□?
A. Cert1□
B. Key1, Secret1 □ Cert1
C. Secret1 □ Cert1□
D. Key1□
E. Key1□ Secret1□
F. Key1 □ Cert1□

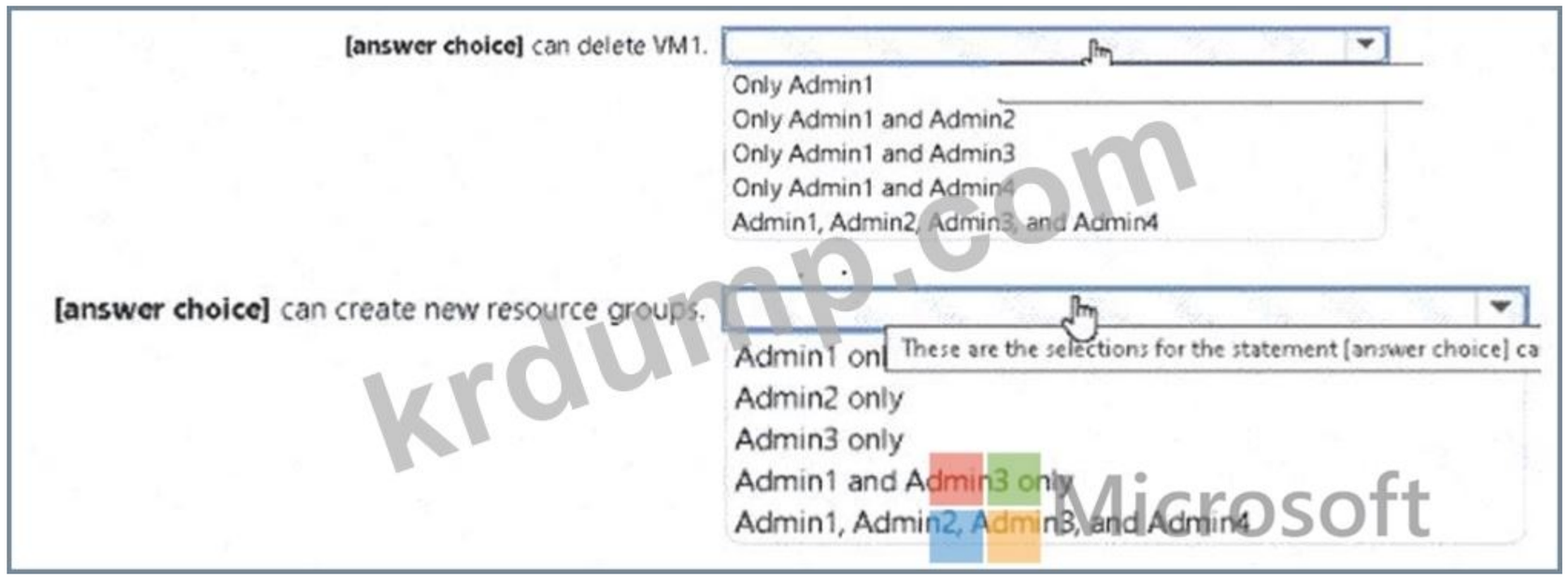
Answer: (SHOW ANSWER)

NEW QUESTION: 179

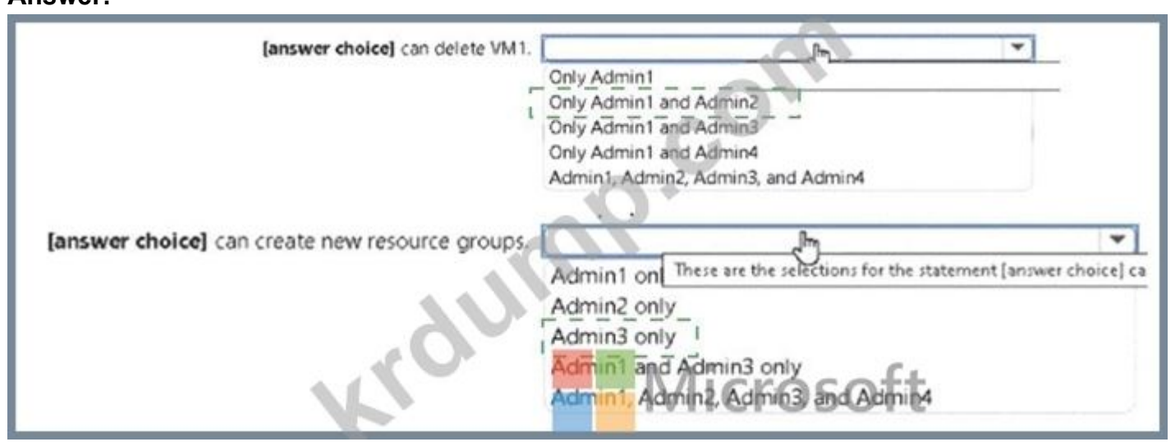
□□ □□□□ □□ □□□ □□ □□□.

□□□□ □□□ □□□ □□□□ □ □□□ □□□□ □□ □□□ □□□□□ □□□□ □□□ □□□□□.

□□: □□ 1□□ 1□□□□.



Answer:



NEW QUESTION: 180

Azure Storage □□□ □□ □□□ □□□□ □□□□.
□□□ □□□ □□ □□ □□□ □□□□□□. □□ □□□ □□□□□ □□□ □□□□ □□□?
A. □□ □ □□ □□ □□ □□
B. Azure□ SQL □□ □□□
C. Windows□ □□ □□□
D. AzCopy
Answer: D (LEAVE A REPLY)
References:
https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-logging?toc=%2fazure%2fstorage%2fblobs%2ftoc.json

NEW QUESTION: 181
App1□□□ □□□ □□□ Azure □□□ □□□□.
□□□□ App1□ □□□ □ Google ID□ Microsoft ID □□□ □□□ □ □□□ □□□.
Azure AD□□ Google□ ID □□□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□ □□□ 1□□□□.
A. □□□ □□
B. □□□ ID
C. □□□□□□□ □□□□□ URL
D. □□□□□ ID
E. □□□□□ □□
Answer: D,E (LEAVE A REPLY)
https://learn.microsoft.com/en-us/azure/app-service/configure-authentication-provider-google

NEW QUESTION: 182
Microsoft Entra □□□□ □□□ Azure □□□ □□□□. □□ □□□□□ □□ □□ □□ □□ □□□ □□□□ □□□□.

Name	Member of
Group1	*None*
Group2	Group1

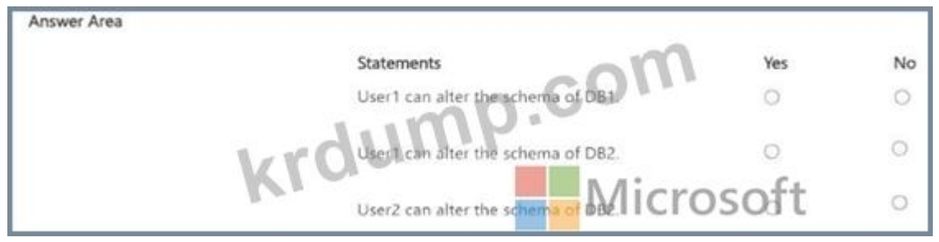
□□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Member of
User1	Group1
User2	Group2

□□□□ □□ □□ □□□ Azure SQL □□□ □□□□ □□□□.

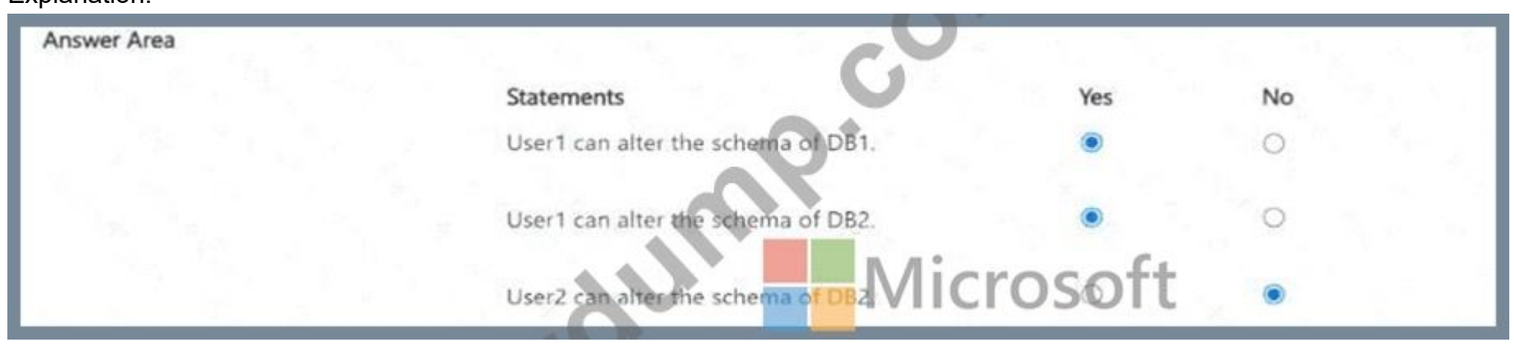
Name	Assigned server admin	Database
sqlsvr1	User1	DB1
sqlsvr2	Group1	DB2

□□□ Microsoft Entra □□ □□□□ □□□□ □□□□.
□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□: □□ 1□□ 1□□□□.



Answer:

Explanation:

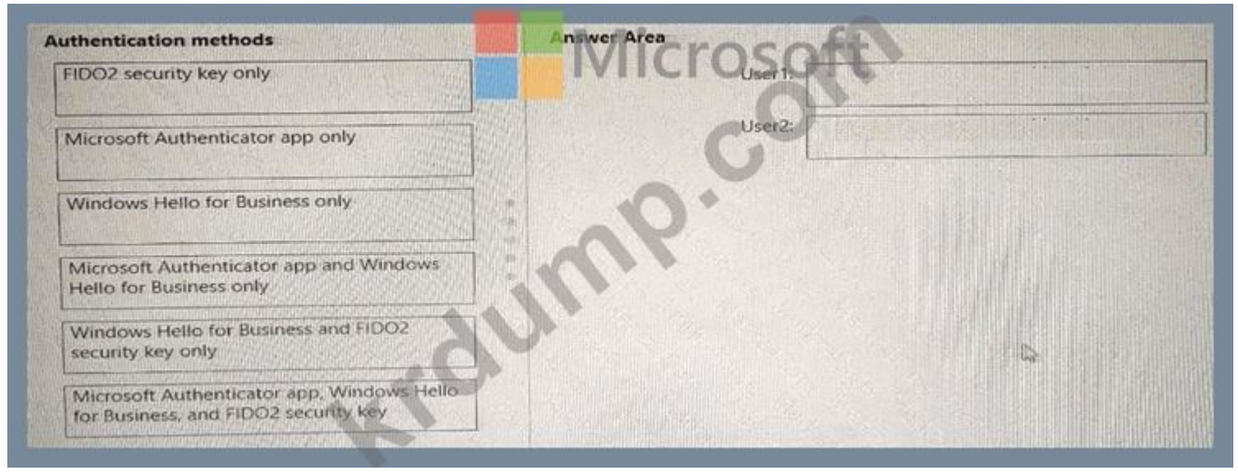


NEW QUESTION: 183
□□ □□ □□□ □□□□ □□□ Azure AD □□□□ □□□□.

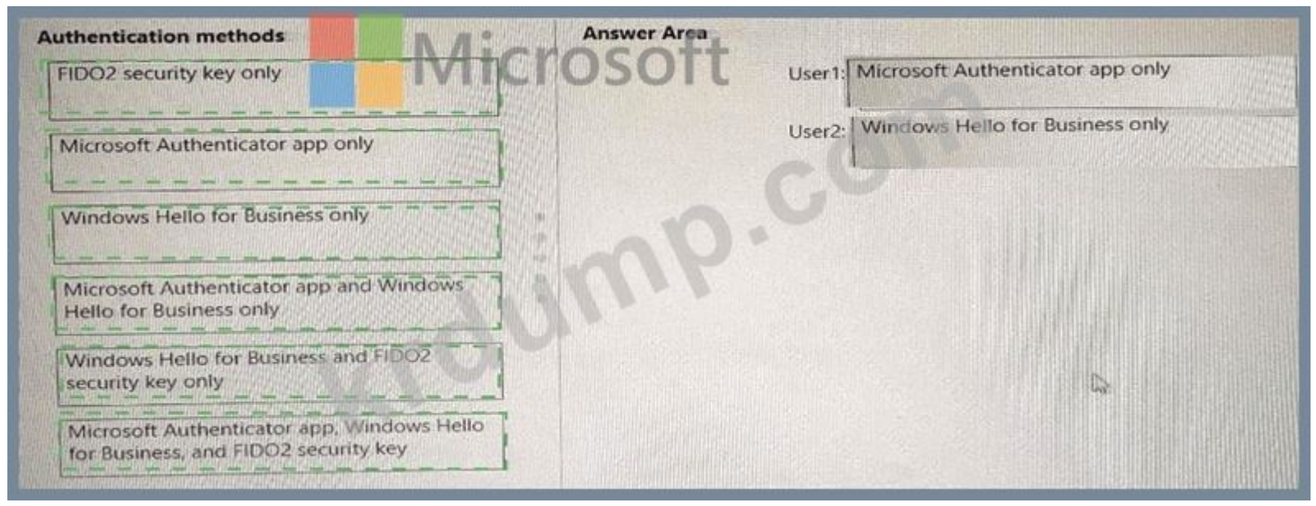
Name	User device
User1	Android mobile device with facial recognition
User2	Windows device with Windows Hello for Business-compatible hardware

□□□□ □□ □□ □□ □□□ □□□□□□.
□ □□□□ □□□□ □□ □□□ □□ □□ □□□ □□□ □ □□□? □□□□ □□ □□ □□□ □□ □□□□□ □□□□□□. □ □□ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□.
□□□□ □□□ □ □□□ □□ □□□ □□□□□□ □□□□□ □ □□ □□□□.

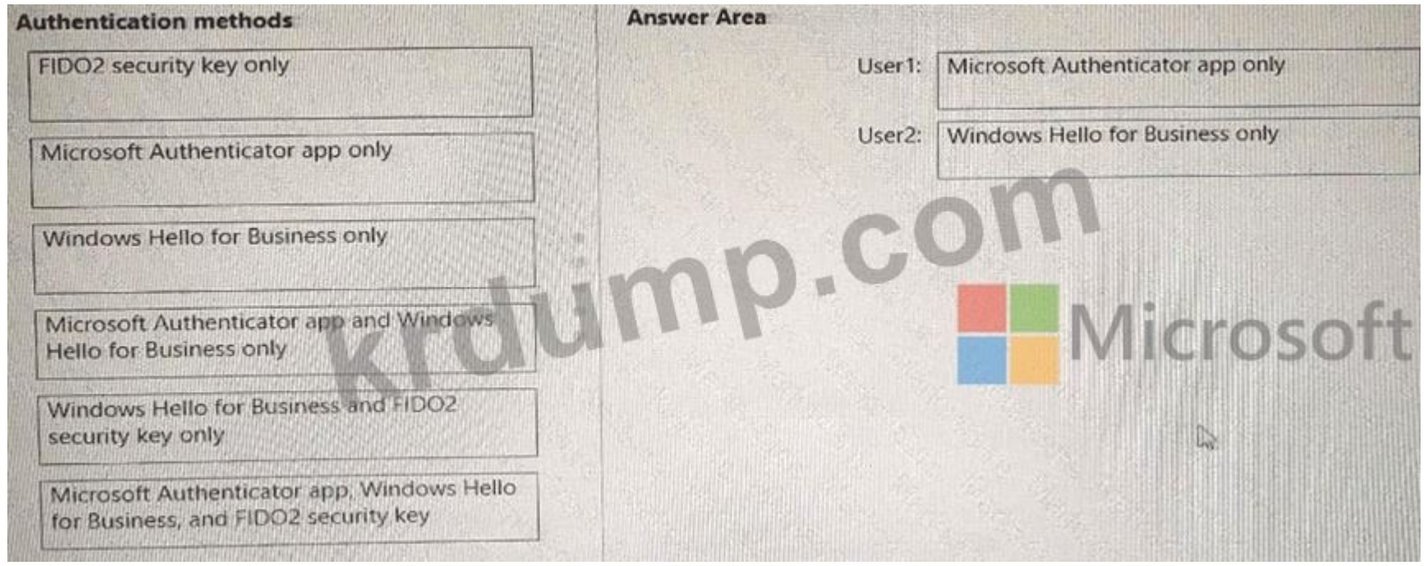
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 184

□□ □□ □□ □□ Azure Active Directory(Azure AD) □□□□ □□□ Azure □□□ □□□□.

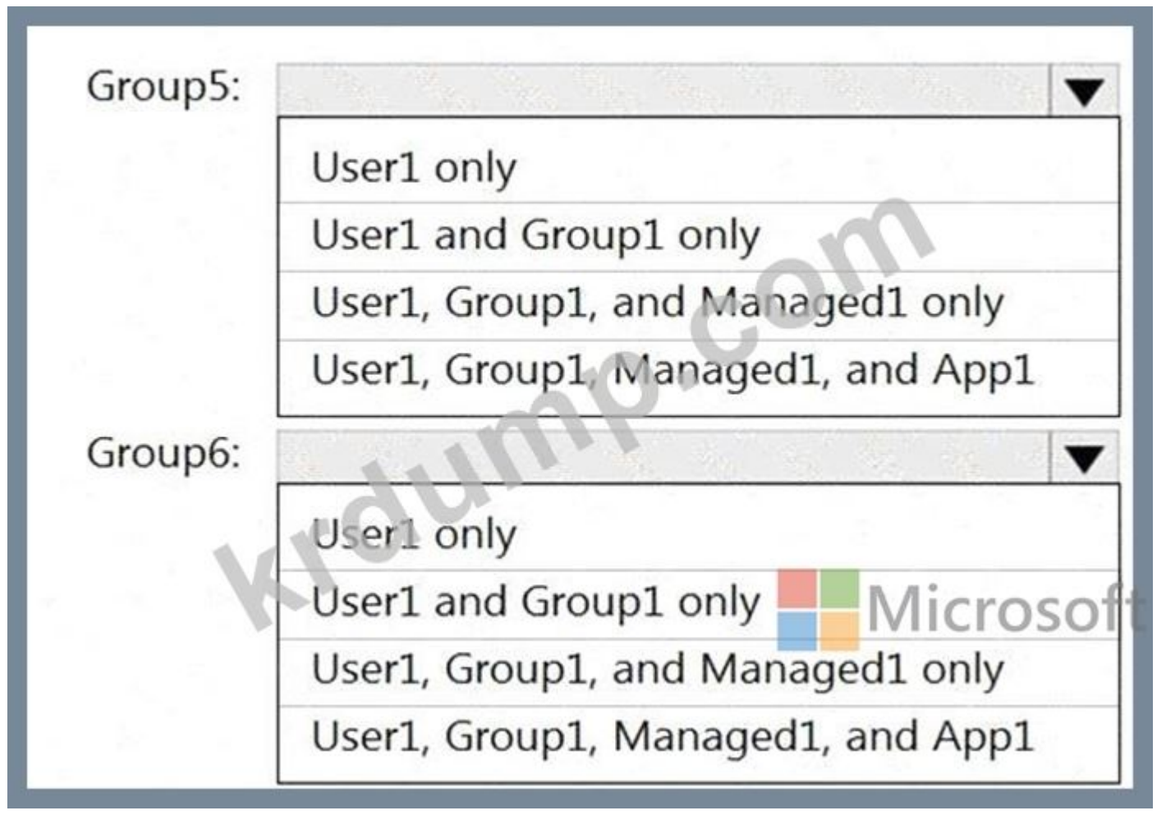
Name	Description
User1	User
Group1	Security group that has a Membership type of Dynamic Device
Managed1	Managed identity
App1	Enterprise application

□□ □□ □□□ □□□ □□□□.

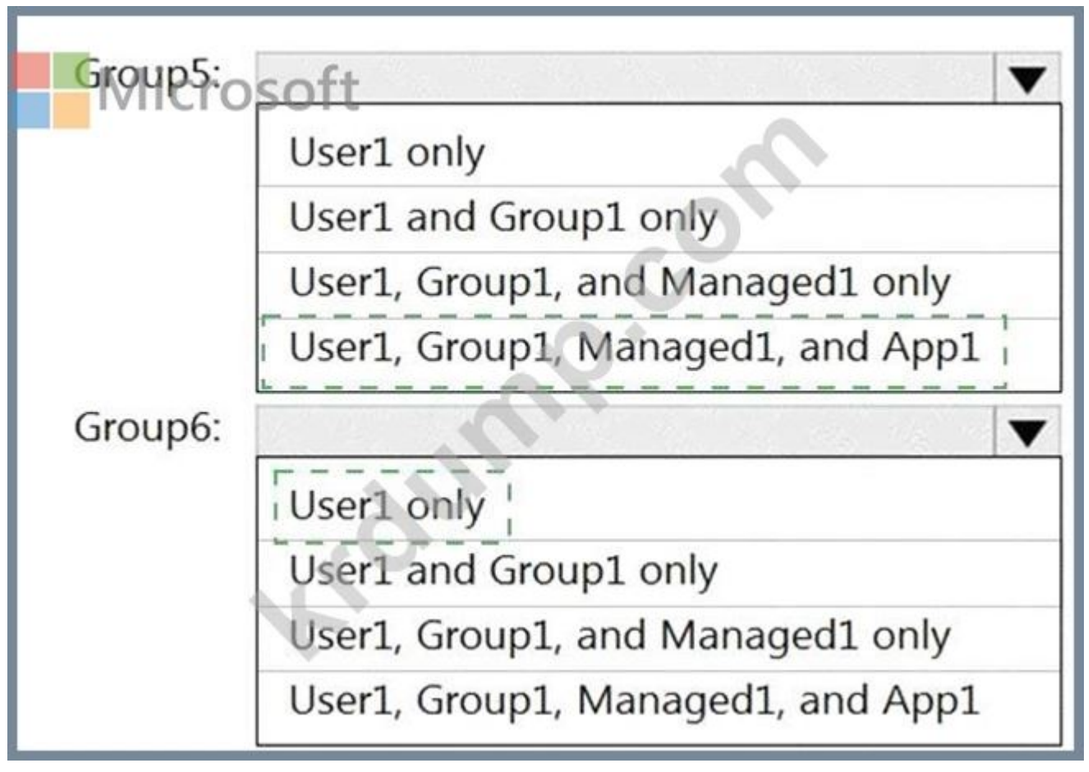
Name	Description
Group5	Security group that has a Membership type of Assigned
Group6	Microsoft 365 group that has a Membership type of Assigned

□□ 5□ □□ 6□ □□ □□□ □□□ □ □□□? □□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ 1□□ 1□□□□.

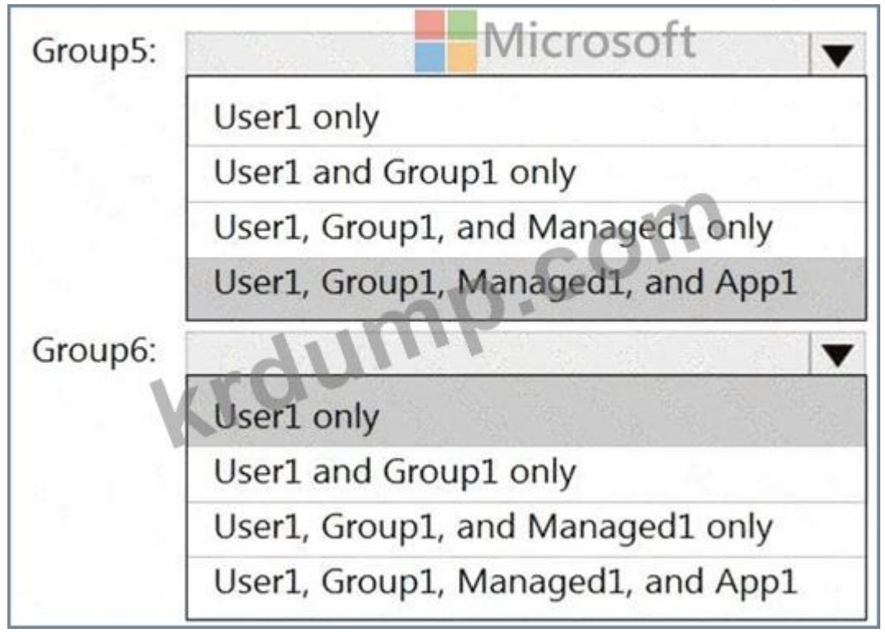

Group5:
User1 only
User1 and Group1 only
User1, Group1, and Managed1 only
User1, Group1, Managed1, and App1
Group6:
User1 only
User1 and Group1 only
User1, Group1, and Managed1 only
User1, Group1, Managed1, and App1

Answer:


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

Explanation:

Graphical user interface, text, application Description automatically generated



NEW QUESTION: 185

Azure □□□ □□□□.

S1 □ □□□ □□□ □□□□ Contoso1812□□ Azure □□□ □□□□.

www.contoso.com□ □□ DNS □□□□ □□□□ Contoso1812□ IP □□□ □□□□□.

□□□□ https://www.contoso.com URL□ □□□□ Contoso1812□ □□□□ □ □□□ □□□□ □□□.

□□ □ □□ □□□ □□□ □□□? □ □□□ □□□□ □□□ □□□□□.

□□: □□ 1□□ 1□□□□.

A. Contoso1812□ □□ □□□□ □□□ □□ ID□ □□□.

B. Contoso1812□ □□□ □□□ □□□□□.

C. Contoso1812□ App Service □□□ □□□□□.

D. Contoso1812□ □□ □□□ □□□□□.

E. Contoso1812□ App Service □□□ □□□□□.

F. Contoso1812□ PFX □□ □□□

Answer: B,F (LEAVE A REPLY)

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

A root " A " record pointing to contoso.com

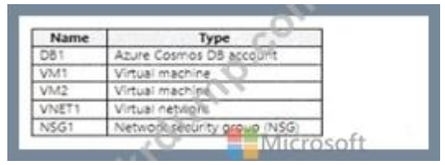
A root " TXT " record for verification

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

F: To use HTTPS, you need to upload a PFX file to the Azure Web App. The PFX file will contain the SSL certificate required for HTTPS.

References: https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom- Domain

NEW QUESTION: 186
□□ □□ □□ □□ □□□□ □□□ Azure □□□ □□□□.



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

VM1□ VM2□ □□ VNET1□ □□□□ NSG1□ □□□□□ □□□□□.
VM1□ VM2□ DB1□ □□□□ □ □□□ □□ □□□.
□□□ □□ □□□?
A. NSG1□ □□ □□□ □□□ □□ □□□ □□□□□.
B. VNET1□ IP □□ □□□ DB1□ □□□ □□□ □□□□□.
C. VNET1□□□ □□□□ □□□□□ DB1□ □□□□□.
D. □□□□□□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 187
VM1□□□ □□□ □□ □□□ □□□ Azure □□□ □□□□.
VM1□ □□□□ □□□□□□ □□□ NSG1□□□ □□□□ □□ □□(NSG)□ □□□, □□ □□□ □□ □□□□ □□□□.

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

VM1□□ Just-in-Time(JIT) VM □□□□ □□□□□ □□□ □□□ □□ □□□ □□ □□□□.
* □□ □□: 3389, 22
* □□ □□ □□: 3□□
* □□□□ □□ IP □□: □□

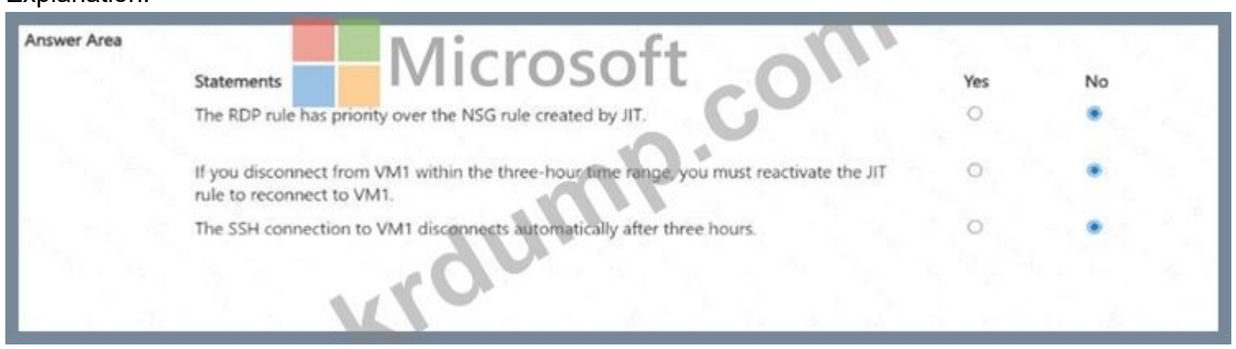
JIT □□□ □□□□□ SSH□ □□□□ VM1□ □□□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

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: 188
contoso.com□□□ Microsoft Enterprise □□□□ □□□ Azure □□□ □□□□. contoso.com□ App1□□□ □□□□□□□ □□□□□□. App1 □□□ Android □□□□□□□ □□□ □□□ □□ □□ □□□. Azure □□□□ □□□ □□□□ □□□?
A. □□□□□
B. □□
C. □□ □□

D. □□□ □ □□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 189

□□□ ExpressRoute □□□ □□ □□□ □□□□ □□□□ □□□. □□ □□□□ □□ □□ □□□ □□□□ □□□.

□ □□□ □□□ □□ □□ ExpressRoute □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ 1□□ 1□□□□.

Answer Area

Answer:

Answer Area

Explanation:

NEW QUESTION: 190

100□□ □□ □□□ □□□ Azure □□□ □□□ □□□□.

□□ □□ □□□ □□□□ Initiative1□□□ □□□□□□ □□□□. Initiative1□ □□□ □□□ □□□□ □□□□.

□□ □□□ □□□□ □□ □□□□ □□□□ □□□.

□□□ □□ □□□?

A. Azure Security Center□□ □□ □□ □□□ □□□□□.
B. Azure Active Directory □□ □□□ □□ □□□□□□ □□ □□□ □□□□□.
C. Azure Security Center□□ □□ □□□ □□□□□.
D. Azure Active Directory □□ □□□ □□ □□□□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/how-to/get-compliance-data#portal

NEW QUESTION: 191
□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

Name	Subscription role	Azure Active Directory (Azure AD) user role	Multi-factor authentication (MFA) status
User1	Owner	Authentication administrator	Enabled
User2	*None*	Global administrator	Enforced
User3	*None*	Global administrator	Disabled

□□ □□□□ Azure AD Privileged Identity Management(PIM)□ □□□□ □ □□□?
A. User2□ User3□
B. User1□ User2□
C. User2□
D. User1□
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

NEW QUESTION: 192
storage 1□□□ □□□ Azure Storage □□□ □□ □□□□□.
storage1□ □□ □□□□ □□ □□□ □□ □□□□ □□□□ □□□□□ □□□. □□, □□ □□□ □□□□□ □□□□□□ □□□.
storage1□ □□□ □ □□□ □□□□ □□□?
A. □□ TLS □□
B. □□□ □□□ □□
C. □□□ □□ □□
D. □□ □□
Answer: (SHOW ANSWER)

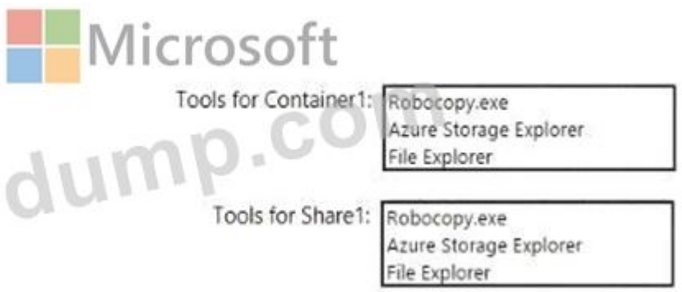
NEW QUESTION: 193
Azure Security□□ □□□ □□ □□ □□□ □□□□.
□□□ □□□□ □□ □□□□□ □□□ □□□□ □□□ □□□□ □□□.
□□□ □□ □□□?
A. Azure Monitor□□ □□ □□□ □□□□.

B. □□ □□□□ Azure □□□ □□ □□ □□□ □□□□□.
C. Azure Active Directory(Azure AD)□□ □□ □□ □□ □□□ □□□ □□□□□.
D. □□ □□□□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups

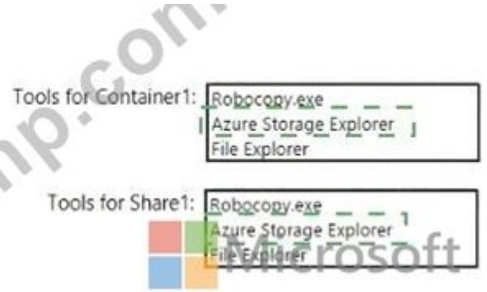
NEW QUESTION: 194
Sub1□□□ Azure □□□ □□□□. Sub1□□ □□ □□ □□ □□ □□□□ □□□ Storage1□□□ Azure Storage □□□ □□□□.

Name	Type
Container1	Blob container
Share1	File share

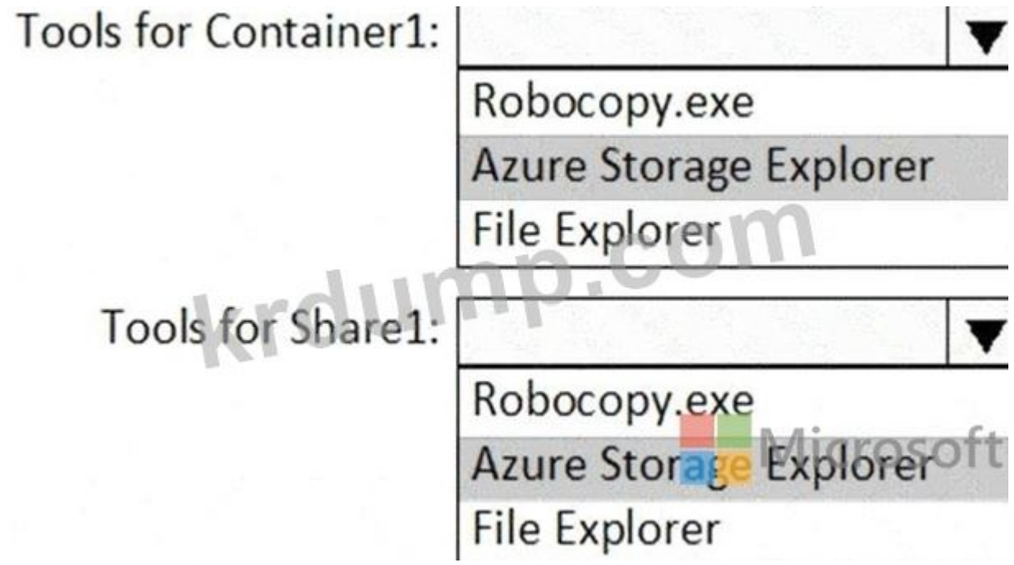
Blob □□□□ □□ □□□□ □□□□□ □□ □□□ □□(SAS)□ □□□□□.
SAS□ □□□□ Container1□ Share!□ □□□□ □□□□□□ □□ □□□ □□□ □ □□□? □□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.
Answer Area



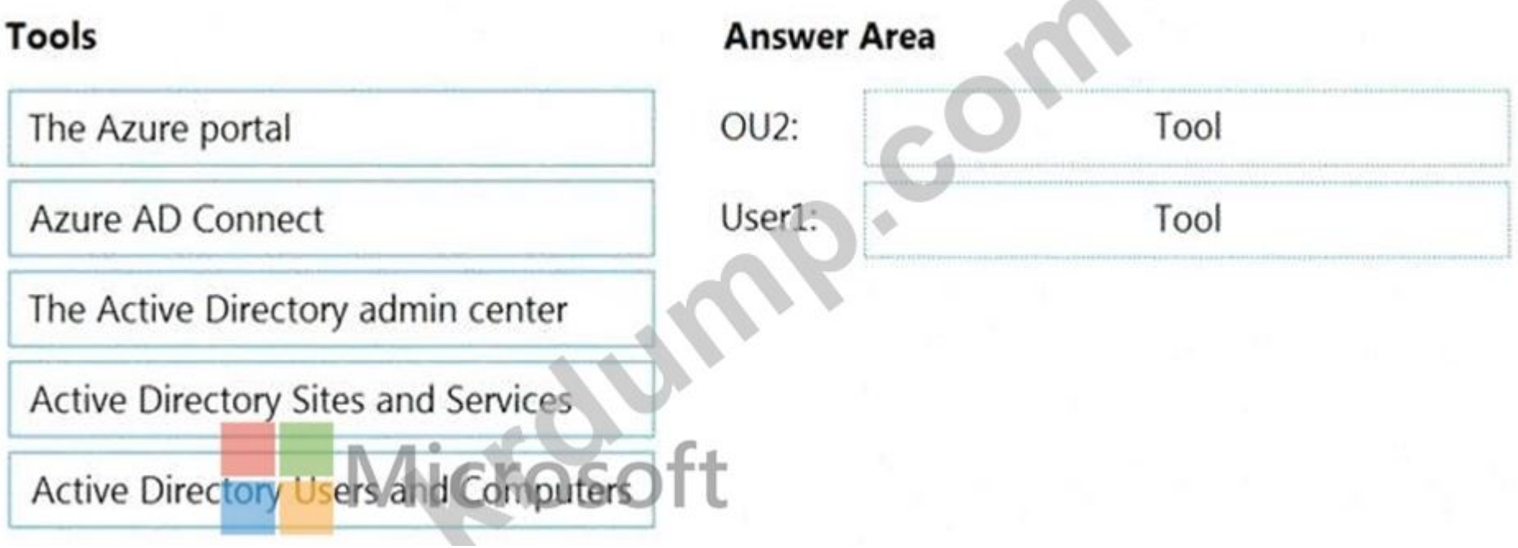
Answer:
Answer Area



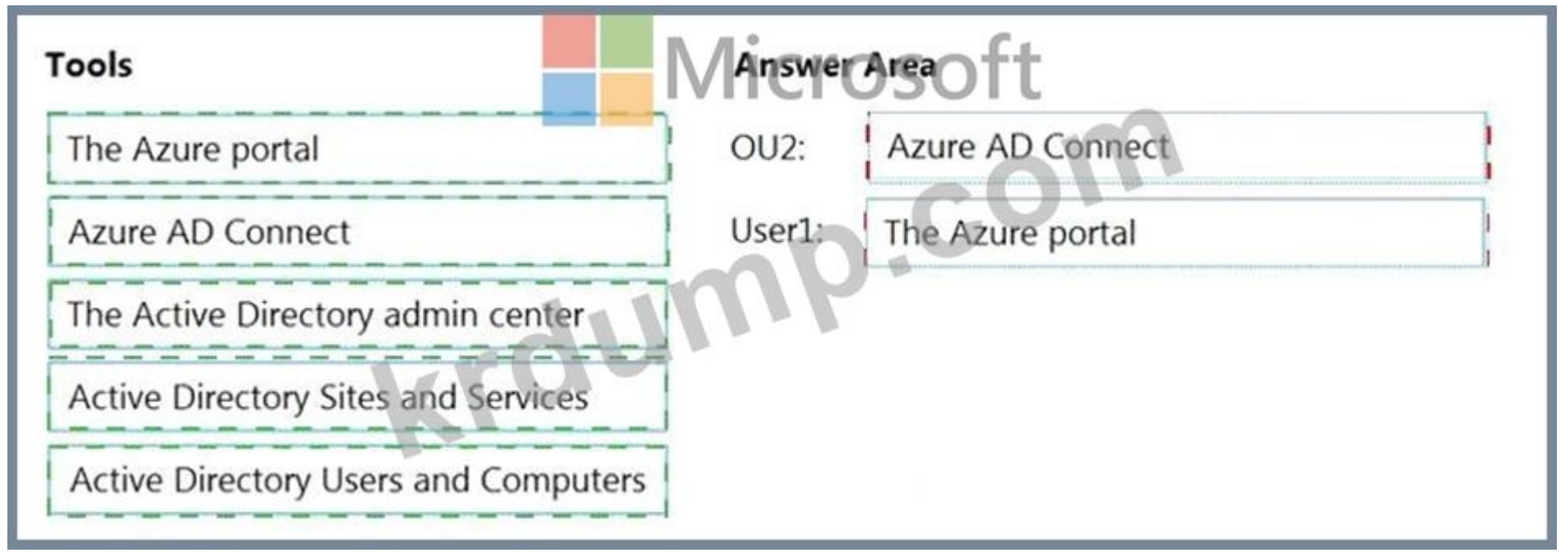
Explanation:



NEW QUESTION: 195
OU2□ User1□ □□ □□□ □□□ □□□□ □□□.
□□ □□□ □□□□ □□□? □□ □□□□ □□□ □□□ □□ □□□□ □□□□□□. □ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □□□ □□ □□□ □□□ □□□ □□□□□ □ □□ □□□□.
□□: □□ 1□□ 1□□□□.

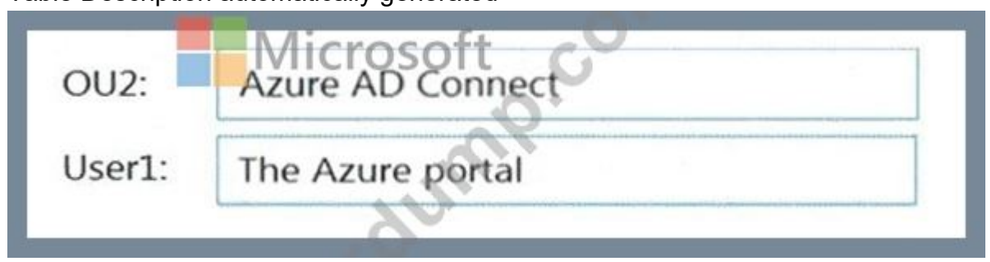


Answer:



Explanation:

Table Description automatically generated



NEW QUESTION: 196

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□,
□□ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
Azure Active Directory(Azure AD)□ □□□□□ □□□ □□□□.
□□ □□□□□ Azure HDInsight □□□□□ □□□□.
□□□□ □ł□□□□ Active Directory □□ □□□ □□□□ □□□□□ □□□□□ □□□ □□□□□.
□□□ □□□ □□□□□ □□□ □□□□ □□□.
□□ □□: Azure □□□ Azure Active Directory Domain Services(Azure AD DS)□ □□□□□.
□□□ □□□ □□□□□?

A. □

B. □□□

Answer: A (LEAVE A REPLY)

References:

https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-configure-using-azure- adds

NEW QUESTION: 197

storage1, storage2, storage3□□□ □ □□ □□□ □□, Analytics1, Analytics2, Analytics3□□□ □ □□ Log Analytics □□ □□, EventHub1, EventHub2, EventHub3□□□ □ □□ Azure □□□ □ □□ □□□ Azure □□□ □□□□.

Microsoft Entra ID□ □□ □□ □□ □□□ □□ □□□ □□□□.

Name	Log	Storage account	Log Analytics workspace	Event hub
Setting1	AuditLogs	storage1	Analytics1	*None*
Setting2	ServicePrincipalSignInLogs, ManagedIdentitySignInLogs	*None*	Analytics2	*None*
Setting3	SignInLogs	storage2	*None*	EventHub1
Setting4	AuditLogs, ProvisioningLogs	*None*	Analytics3	EventHub2
Setting5	NonInteractiveUserSignInLogs	storage3	*None*	EventHub3

□□ □ □□□ □□, □□□ □□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□. □□: □□□ 1□□□□.

Answer Area

Statements	Yes	No
You can create additional Microsoft Entra diagnostic settings.	○	○
You can configure retention for locations where Setting4 stores logs.	○	○
You can configure Setting2 to have Analytics1 and Analytics2 as destinations.	○	○

Answer:

Answer Area

Statements	Yes	No
You can create additional Microsoft Entra diagnostic settings.	○	○
You can configure retention for locations where Setting4 stores logs.	○	○
You can configure Setting2 to have Analytics1 and Analytics2 as destinations.	○	○

Explanation:

NEW QUESTION: 198

□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

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□ Function 1, SQL1, storage 1□ □□□□□.

□□ □□□□□□ □□□□ App1, Function1, SQL1 □ storage1 □□ □□□□ □□□□ □□□.

App1□ □□ □□□□□□ □□□□ □□ □□□□ □□□ □ □□□□?

A. storage1□

B. storage1, SQL1 □ Function1

C. SQL1□

D. Function1□

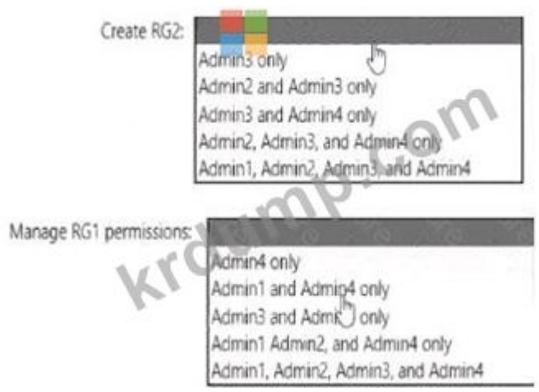
E. SQL1 □ storage1□

F. storage1□ Function1□

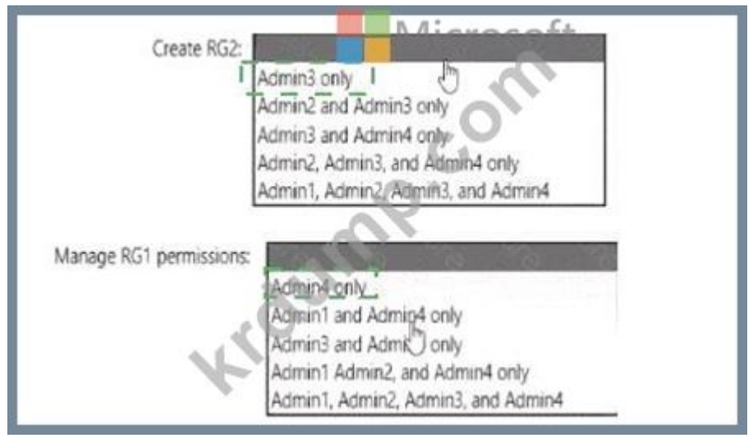
Answer: B (LEAVE A REPLY)

NEW QUESTION: 199

RG2 □□ □ RG1 □□ □□□ □□□□ □□□. □ □□□ □□□ □ □□ □□□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□. □□: □□□ 1□□□□.

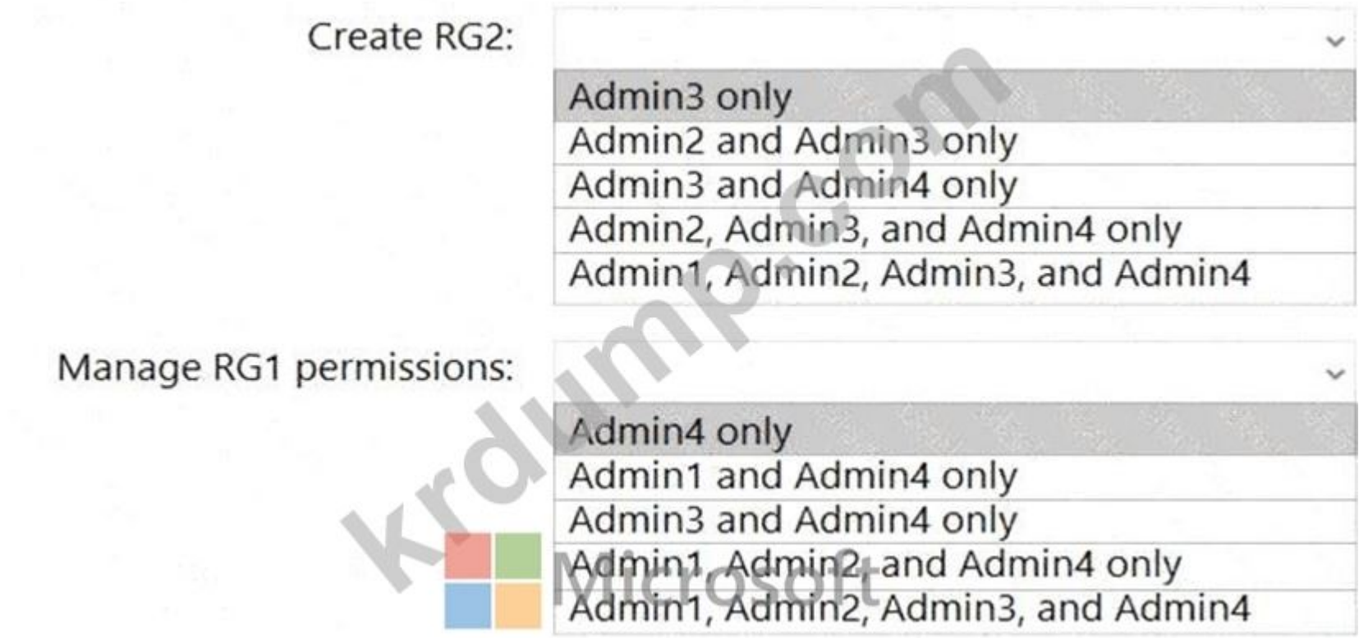


Answer:



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: 200

Azure Active Directory(Azure AD) □□□, Query1□□□ Azure Log Analytics □□, Playbook1□□□ □□□□□ □□□ Azure Sentinel □□ □□□ □□□□.

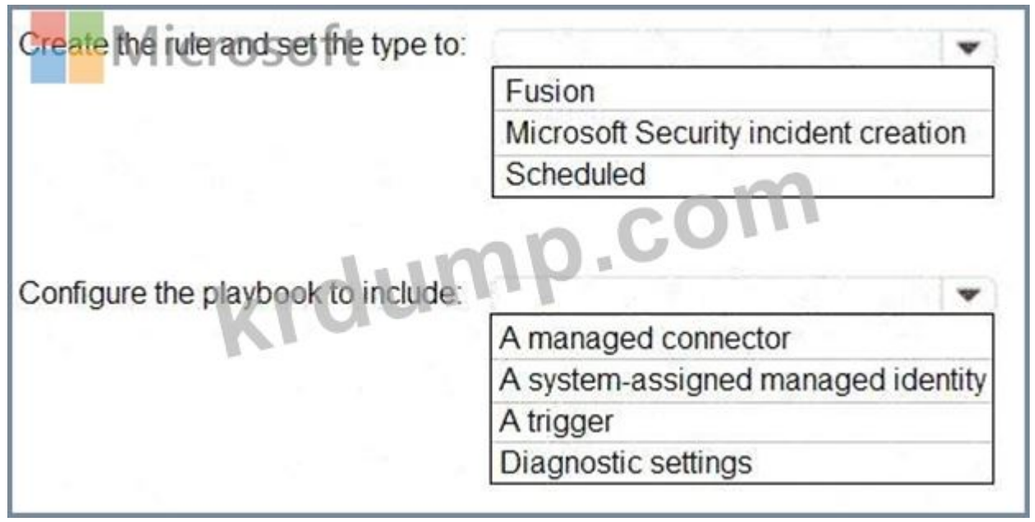
Query1□ Azure AD□□ □□□ □□ □□□□ □□ □□□ □□□□□.

Query1□ □□□□ Playbook1□ □□□□□ Azure Sentinel □□ □□□ □□ □□□□□.

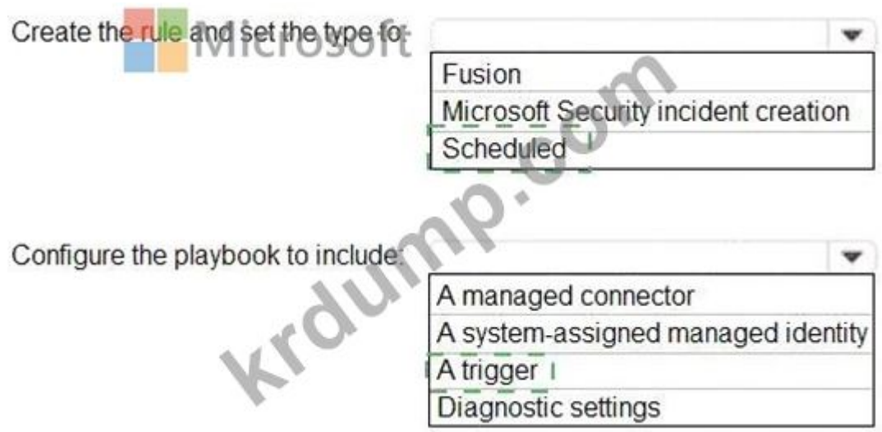
□ □□□ Playbook1□ □□□ □ □□□ □□□□ □□□.

□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□□ □□□□□.

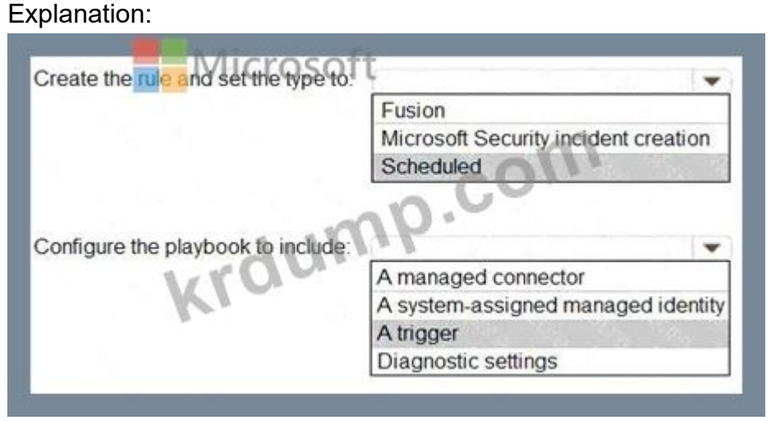
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:

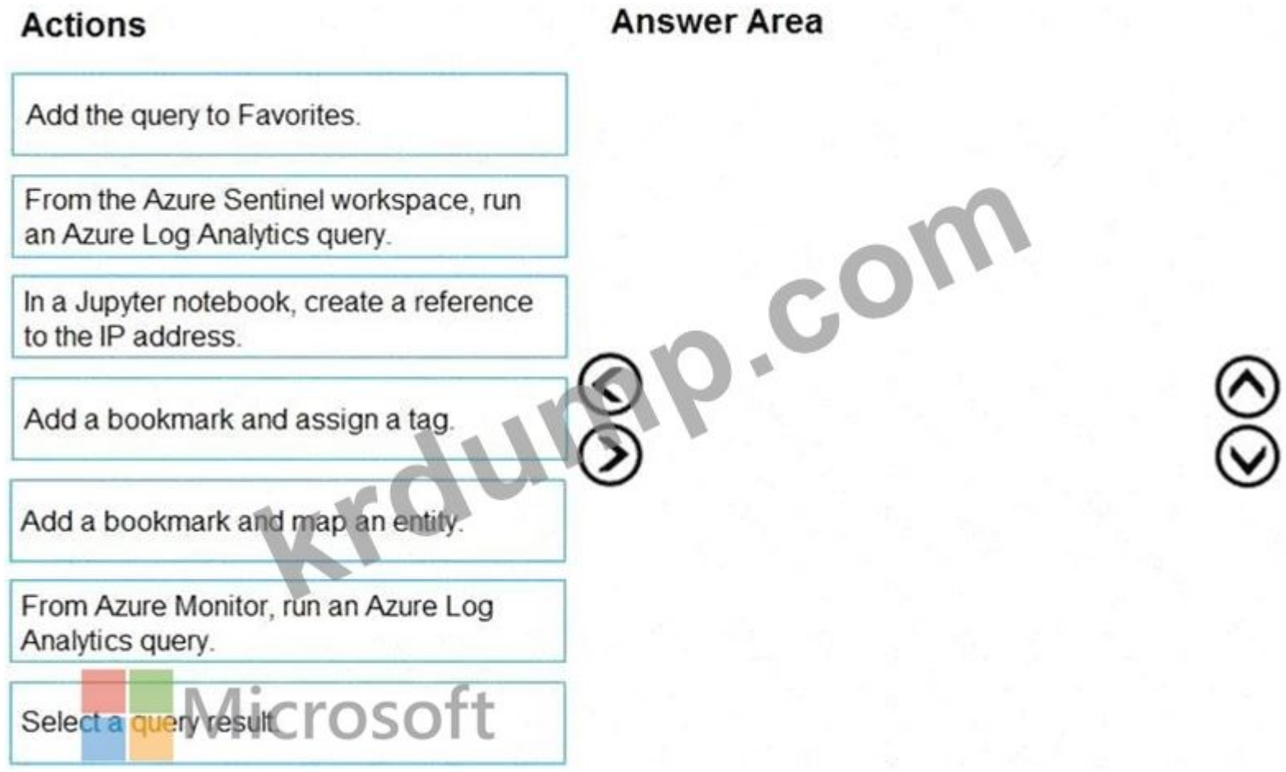


Reference:

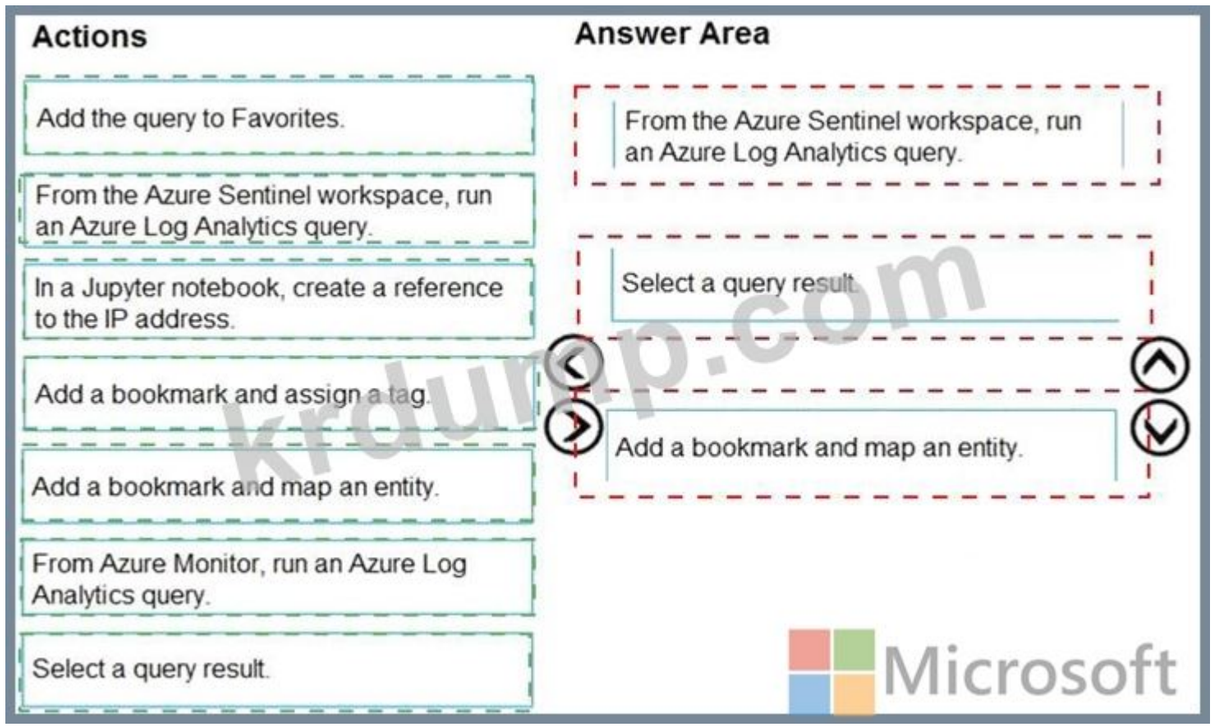
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

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

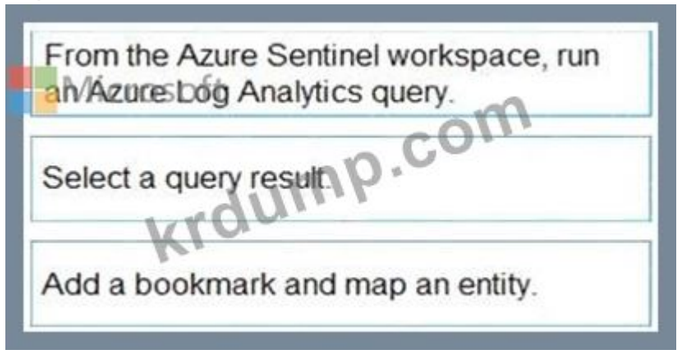
NEW QUESTION: 201
Azure Active Directory(Azure AD) □□□ □□□□ □□ Azure Sentinel □□ □□□ □□□□.
□□ IP □□□□ □□□□ □□□□□ □□□□ □□ □□□ □□□□ □□□□.
□□ □□□ □□□ □□ □□□□ □□□ □□ □□ □□□□ □□□ □ IP □□□ □□□ □ □□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:



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

NEW QUESTION: 202

□□ □□ □□□ □□ □□□□□ □□□ Azure □□□ □□□□.

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

□□ □□□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Answer:

Explanation:

NEW QUESTION: 203
contoso.com□□□ Microsoft Entra □□□□ □□ □ □□□□ User1□□□ □□□□ □□□□.
contoso.com□ App1□□□ □□ □□□□ Role1□□□ □ □□□ □□□□.
User1□ Role1□ □□□□ □□□.
Microsoft Entra □□ □□□ App1□ □□ Enterprise □□□□□□ □□□□□□ □□□ □□□□ □□□?
A. API □□
B. □□□ □ □□
C. □ □□
D. □□ □ □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 204
storage1□□□ □□□ □□□ □□□ □□ □□ □□□ □□□ Azure □□□ □□□□.
□□□ □□□ □□ □□□ □□□ Azure □□□ □□□□. □□ □□□ □□□□ □□□ □□ □□ □□ □□□□.

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

□□ □□□□ □□□□□ □□ □□ □□□ □□ □□□ □□□□□□ □□□□ □□□□.

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

storage1□ □□ □□ □□□ □ □□ □□□□ □□□ □□□□□.

* □□□ □□: □□□ □□□□
* □□ □□□□: VNET3\Subnet3
* □□□ - □□ □□: 52.233.129.0/24

□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.

□□: □□ 1□□ 1□□□□.

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: 205

□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

Name	Type
RG1	Resource group
VM1	Virtual machine

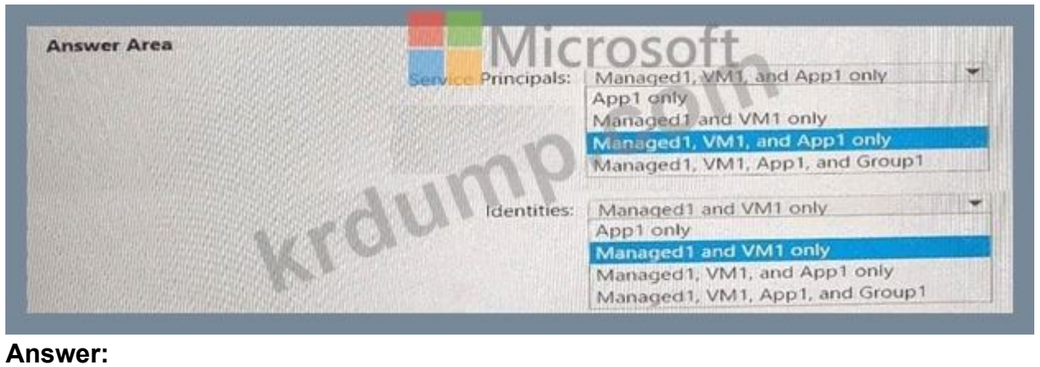
□□ □□□ □□□□□.

Managed1□□□ □□□ □□□ ID□ □□□□.

Group1□□□ □□□ Microsoft 365 □□□ □□□□.

RG1□ □□ □□ □□□ □□□ □□□□□ □□ ID□ □□ □□□ □□□ □ □□□ □□□□ □□□. □□□ □□□□ □□□? □□ □□□□ □□□ □□□ □□□□ □□□□□. □□:

□□□ □□ □□□ □□□ 1□□ □□□□□.



Answer:

Explanation:

NEW QUESTION: 206

□□ □□ □□ □□ Azure Firewall □□□ □□□ Azure □□□ □□□□.

Name	Type
Policy1	Standard
Policy2	Premium

□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Tier	Policy
FW1	Premium	Policy2
FW2	Premium	Policy1

□□□□ □□ □□ □□□ □□ □□□□□ □□□□ □□□□.

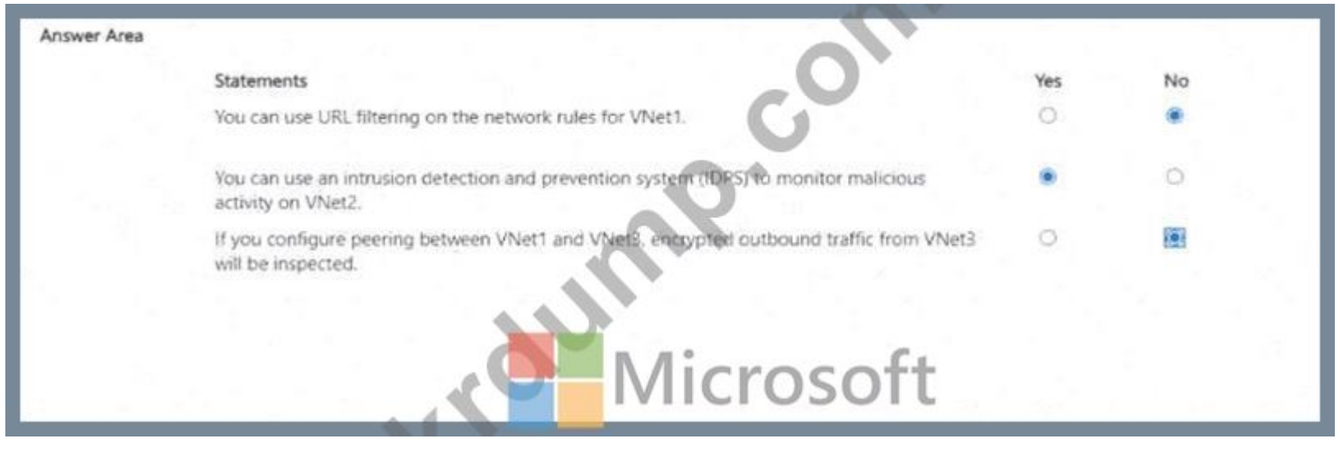
Name	Firewall
VNet1	FW1
VNet2	FW2
VNet3	None

□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.

□□: □□ 1□□ 1□□□□.

Answer:

Explanation:



NEW QUESTION: 207

Azure Storage □□□ □□ □□□ □□□□ □□□□. Azure Storage Analytics □□□ □□□□□ □□ □□□ □□□□ □□□ □□□□□□. □□ □□□ □□□□□ □□□ □□□□ □□□?

A. □□□□□ Microsoft Defender

B. AzCopy

C. Windows□ □□ □□□

D. □□□□□□□ □□□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 208

□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

Name	Type
storage1	Storage account
KeyVault1	Azure key vault

90□□□ □□ □□□□ □□□□□□ storage1□ □□□□ □□□. □□ cmdlet□ □□□□ □□□?

A. Add-AsKeyVaultmanageStorageAccount

B. Set-A;□□ □□ □□ □□

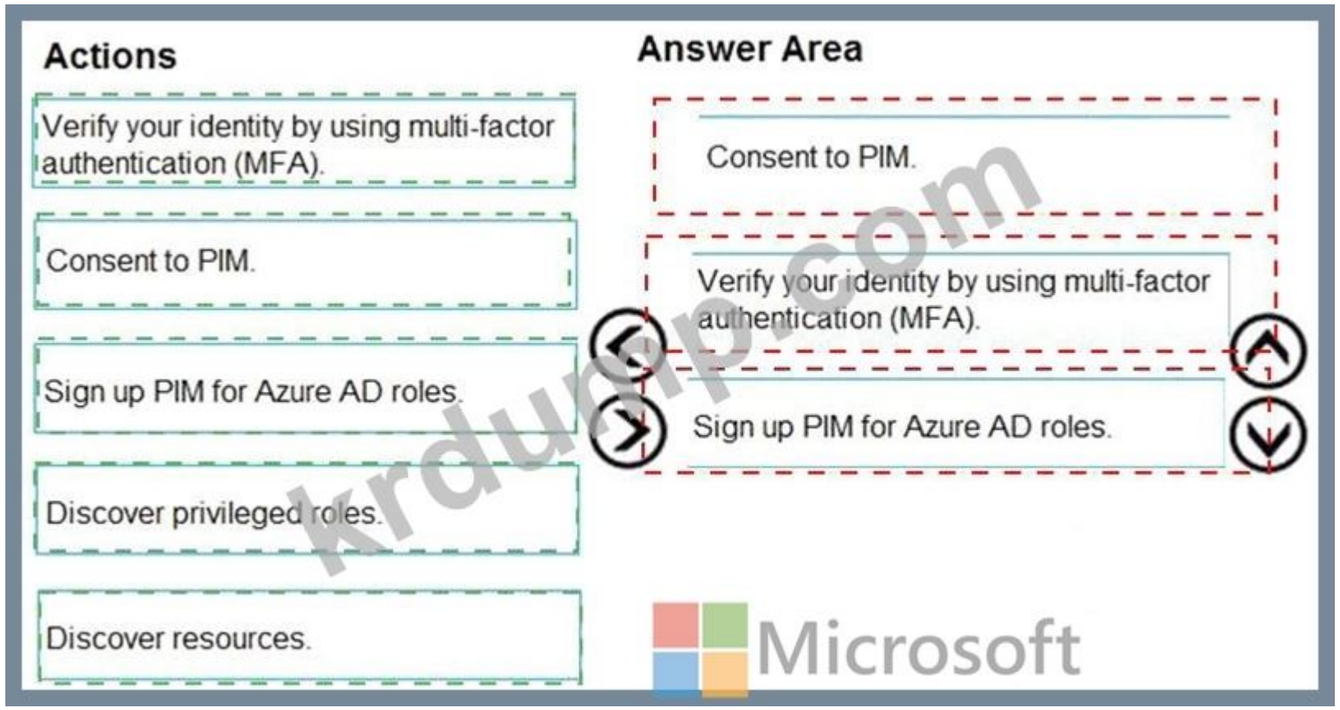
C. -A=StorageAccount□ □□□□□.

D. Add-A:StorogcAccountmanagementPolicyAction

Answer: A (LEAVE A REPLY)

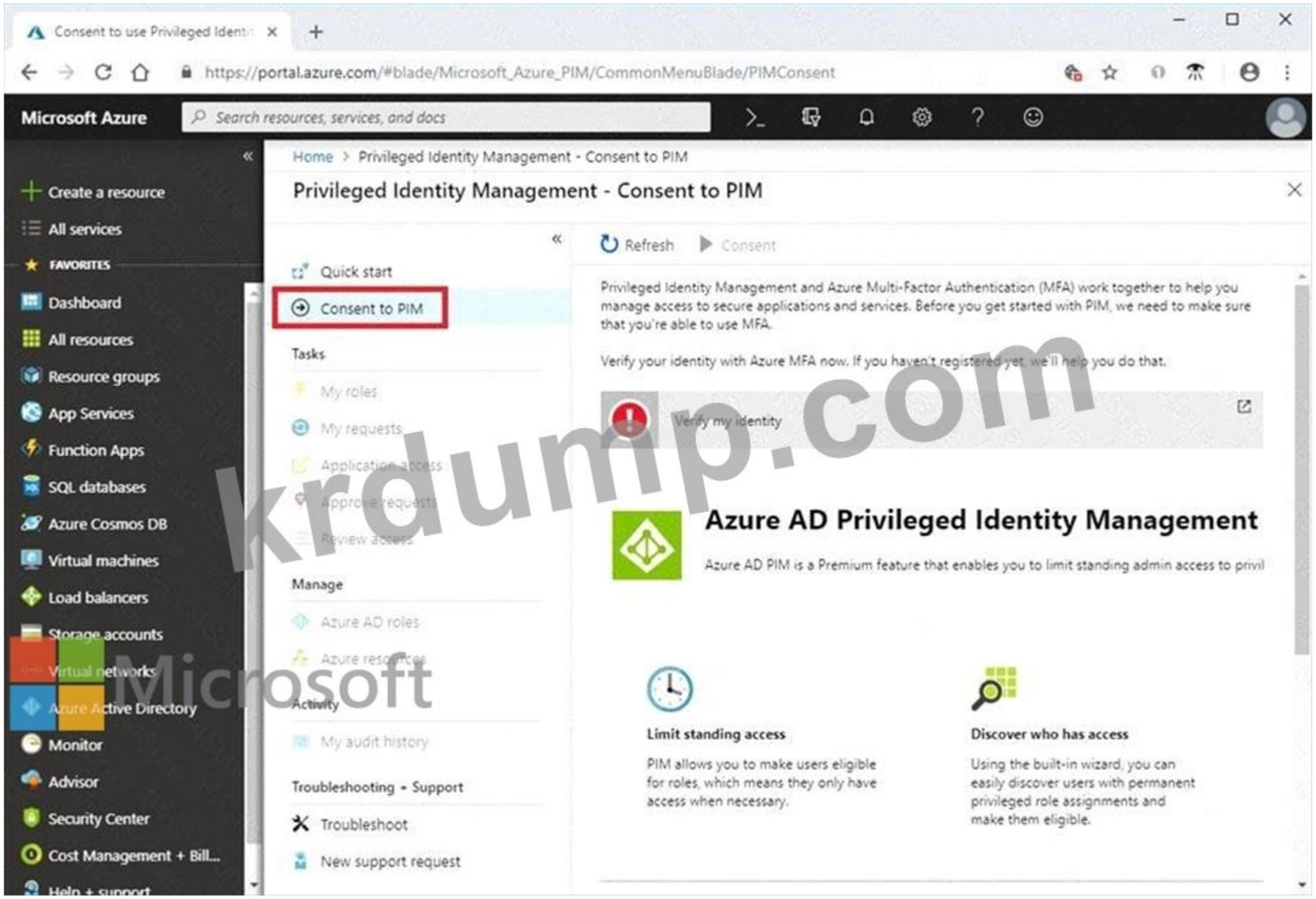
NEW QUESTION: 209
Azure □□□ □□□□.
Azure AD(Azure Active Directory) PIM(Privileged Identity Management)□ □□□□ Azure AD □□□ □□□ □ □□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.

Answer:



Explanation:

Step 1: Consent to PIM



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

Step 3: Sign up PIM for Azure AD roles

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

References:

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

NEW QUESTION: 210

Microsoft Graph□ □□□□ Azure Active Directory(Azure AD) □□□□ □□□ □□□□ □□ □□□□□ □□□. □□ Azure AD□ □□□□ □ □□□ □□□□ □□□. □□ □□□ □□□□ □□□?

A. □□□ □□ □□ □□ □□□ □□(RBAC) □□

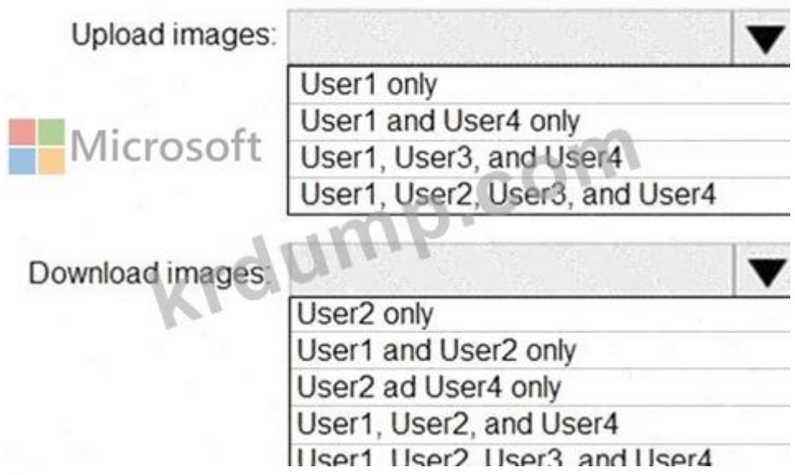
B. □□ ID

C. Azure AD □□□□□□ □□□
D. □ □□
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

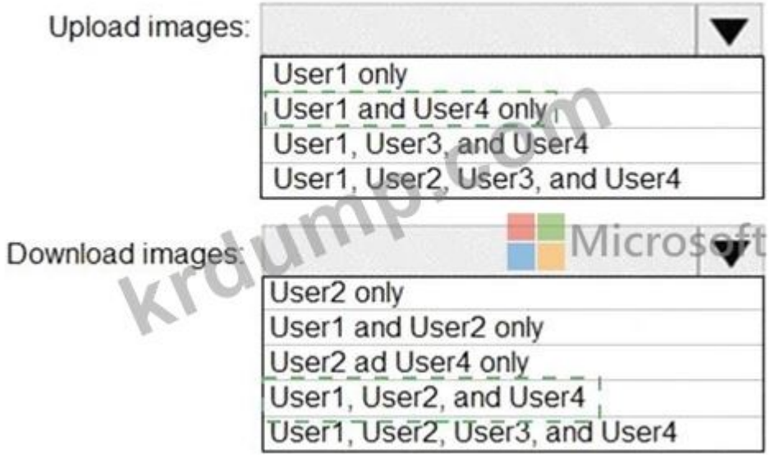
NEW QUESTION: 211
Registry1□□□ Azure Container Registry□ □□□□.
□□ □□ □□□ □□ Registry1□ □□ □□ □□□ □□□□□.

User	Role
User1	AcrPush
User2	AcrPull
User3	AcrImageSigner
User4	Contributor

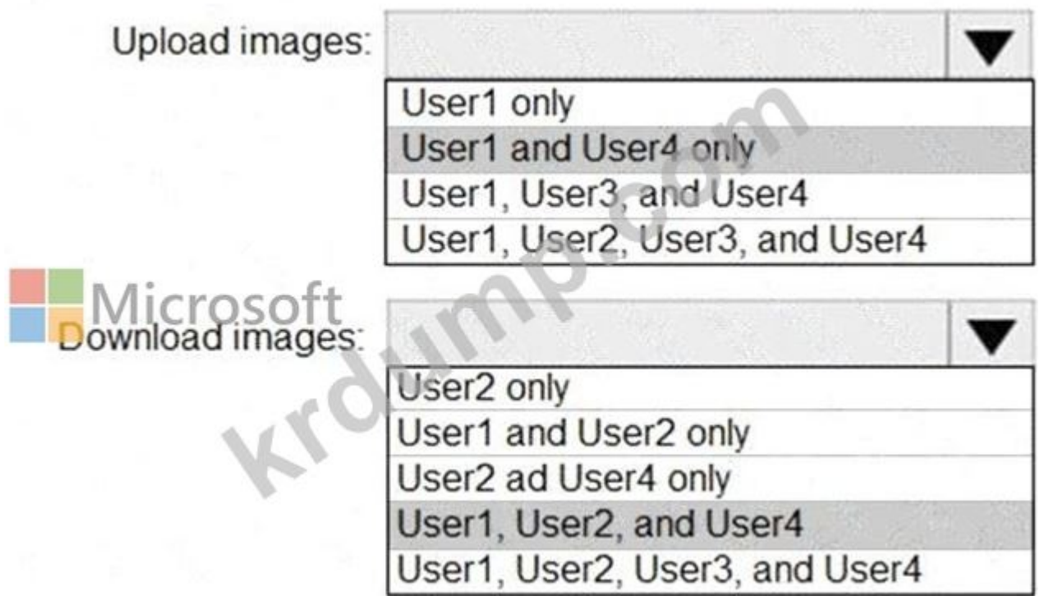
□□ □□□□ Registry1□ □□□□ □□□□□ Registry1□□ □□□□ □□□□□ □ □□□? □□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:



Box 1: User1 and User4 only

Owner, Contributor and AcrPush can push images.

Box 2: User1, User2, and User4

All, except AcrImagineSigner, can download/pull images.

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

References:

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

NEW QUESTION: 212

□□ □□ □□□ □□□□ □□□ Microsoft Entra □□□□ □□□□.

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

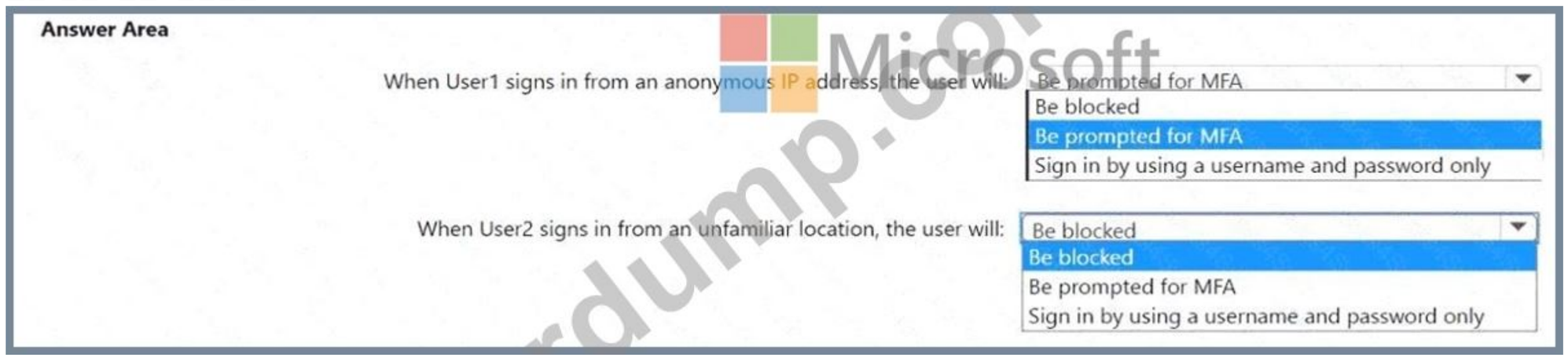
□□ □□□ □□□ Microsoft Entra Identity Protection □□□ □□ □□□ □□□ □□□□□.

* □□: □□1 □□, □□2 □□
* □□ : □□□ □□ □□ : □□ □□
* □□: □□ □□, □□ □□ □□

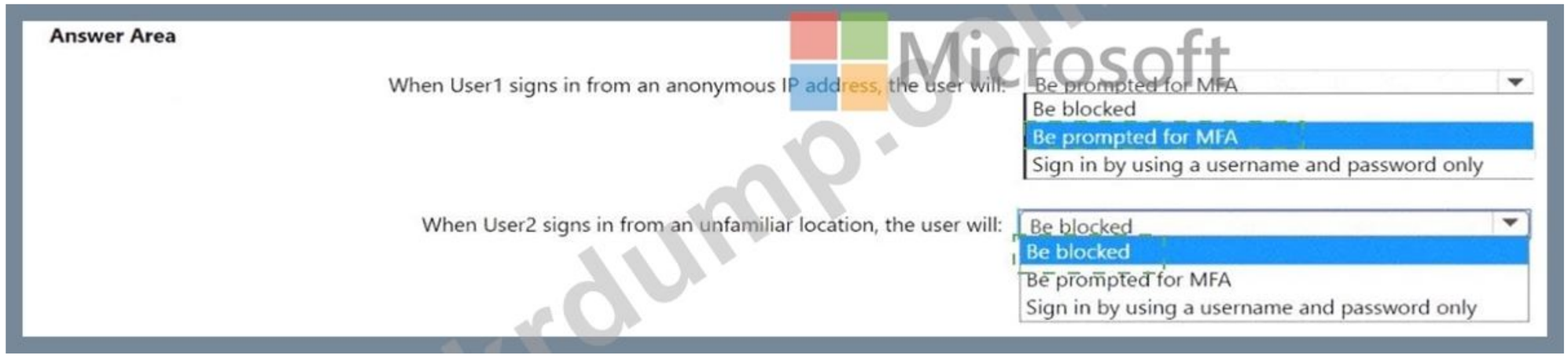
□□□□ Microsoft Entra ID□ □□□□ □ □□ □□ □□□□□ □□□□ □□□.

□ □□□□ □□ □□□ □□□□ □□□? □□ □□□□ □□□ □□□ □□□□ □□□□□.

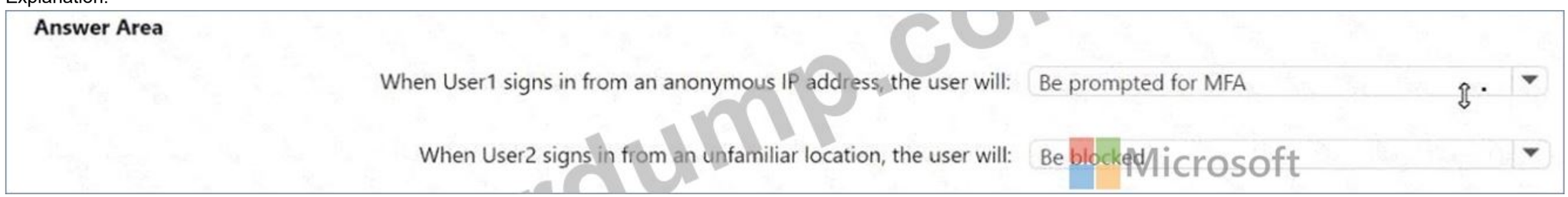
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 213

□□□ □□

□□□ □□ □□ □□□ □□ □□□ □□□□□.

□□□ □□□ □□□□□ □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.

□□□□□ □□□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□□□.

Azure □□□ □□: Userl -28681041@ExamUsers.com

Azure □□□□: GpOAe4@lDg

Azure Portal□ □□□□□ □□□□□ □□□□ □□□ CTRL-K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.

□□ □□□ □□ □□ □□□□□ □□□□□.

□□□ □□□□: 28681041

□□ 8

rg1lod28681041n1 Azure Storage □□□ □□ HTTP □□□ □□□□ □□□.

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.